SIEMENS

SIMATIC

Process Control System PCS 7 Compendium Part F - Industrial Security (V8.0)

Configuration Manual

Valid for PCS 7 V8.0 (updated for V8.0 SP1)

11/2013
A5E32334449-AB

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
Industry Sector
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E32334449-AB
Ⓟ 11/2013 Technical data subject to change

Table of contents

Preface 1

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 project 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 to the product documentation covering SIMATIC PCS 7. The basic tasks for creating and configuring the project are described in the form of instructions with numerous illustrations.

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

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 with SIMATIC PCS 7 automation systems and projects.
The configuration guide is valid as of SIMATIC PCS 7 V8.0 (updated for V8.0 SP1).

SIMATIC PCS 7 Manual Collection

The complete documentation of PCS 7 is available to you free of charge and in multiple languages in MyDocumenationManager as a manual collection from the website http://support.automation.siemens.com/WW/view/en/59538371 or in PDF format via www.siemens.com/pcs7-documentation.

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 are of secondary importance.
Industrial Security must not be reduced to simply 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. If 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 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 to the product documentation for SIMATIC PCS 7. The basic tasks for creating and configuring the project are described in the form of instructions with numerous illustrations.

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.

Additional support

If you have any questions about using the products described in the manual, contact your Siemens representative in the sales and service locations that are responsible for your company.

You can locate your contact at http://www.siemens.com/automation/partner.

The guide that provides details of the technical documentation offered for the individual SIMATIC products and systems is available at http://www.siemens.com/simatic-tech-doku-portal.

The online catalog and online ordering system are available at http://mall.automation.siemens.com/.

Training center

Siemens offers a number of training courses to familiarize you with the SIMATIC PCS 7 process control system. Contact your regional Training Center or the central Training Center in D-90327 Nuremberg (http://www.sitrain.com).

Technical Support

You can contact Technical Support for all Industry Automation and Drive Technology products using the Support Request Web form http://www.siemens.com/automation/support-request.

Additional information on our Technical Support is available on the Internet at http://support.automation.siemens.com/WW/view/en/16604318.

Industry Online Support on the Internet

In addition to our documentation options, our expertise is also available to you online (http://support.automation.siemens.com).

Here you will find:

- Overview of the most important technical information and solutions for PCS 7 under http://www.siemens.com/industry/onlinesupport/pcs7.
- The newsletter, which will keep you constantly up-to-date with the latest information about our products.
- The right documents for you via the search function in our Industry Online Support portal.
- A forum in which users and experts from all over the world exchange ideas and experiences.
- Your local contact partner for Industry Automation and Drive Technology.

Information about local service, repairs, spare parts. The "Services" section offers even more options.

Security strategies 2

2.1 General information

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) encourages plant operators in their security advisories to take additional defensive measures to protect against cybersecurity risks. ICS-CERT recommends:

- Minimizing network exposure for all control system devices. Critical devices should not have direct access to the Internet.
- Placing control system networks and remote devices behind firewalls and isolating them from the company network.
- Using secure methods such as Virtual Private Networks (VPNs) when remote access is required. Keep in mind that VPN is only as secure as the connected devices.

2.2 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:

- 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.

The physical and organizational security measures are summarized under the heading "Plant Security".

- Division into security cells
  A sufficiently secured network architecture subdivides the instrumentation and control network into different task levels.
  Perimeter zone techniques should be employed. In this case, this means using exported data and not data used directly for process control that are available on a system (data memory database). The system is located between the main access point for data input (front-end firewall) and the deeply embedded access point for data input (back-end firewall), or the third network section of a triple-homed firewall (located in three networks).
- Securing access points to the security cells
  A single access point to each security cell (should be a firewall system) for the authentication of users, employed devices and applications, for the direction-based access control and the assignment of access permissions as well as for detection of break-in attempts.

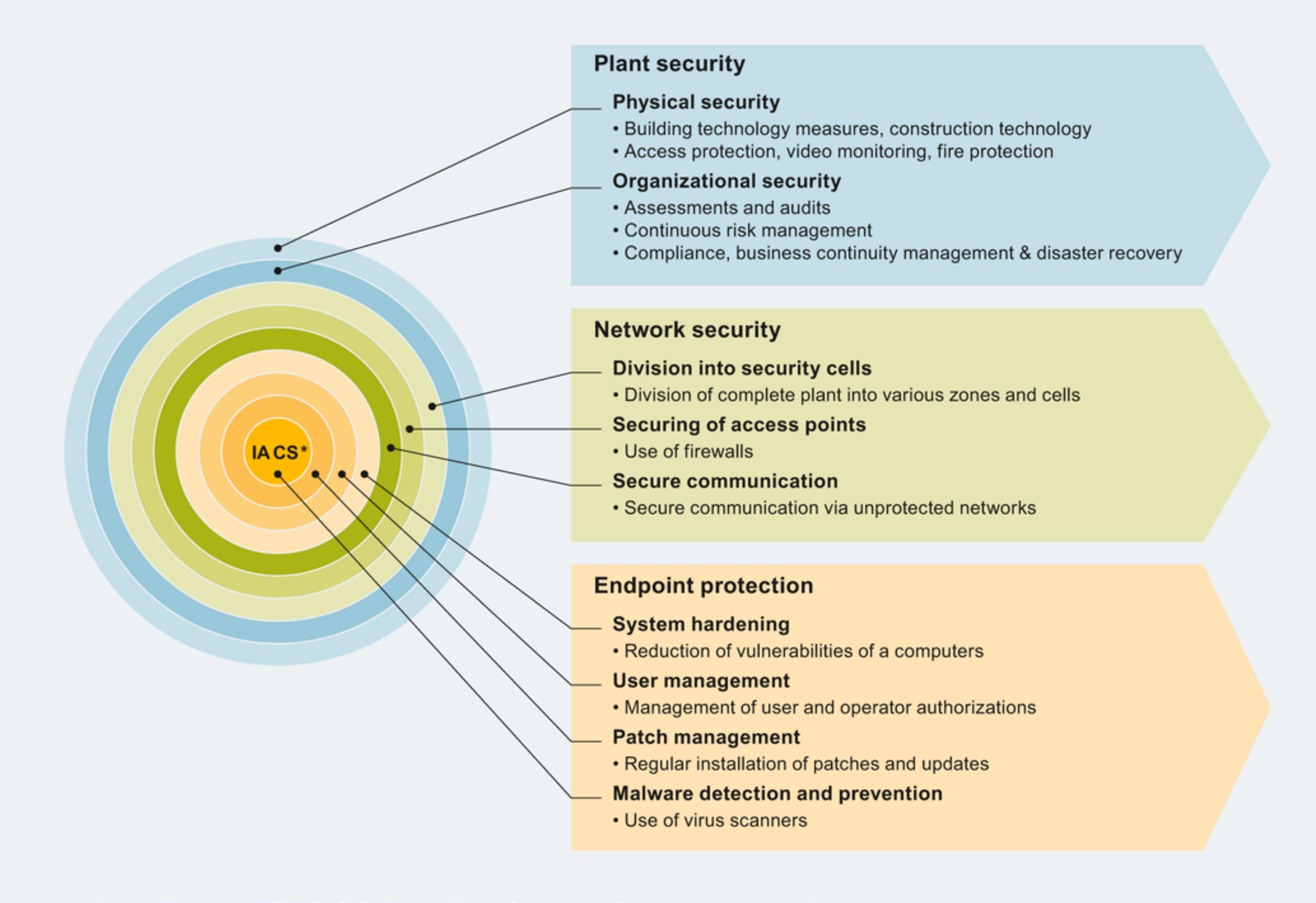
  The single access point functions as main access point to the network of a security cell and serves as the first point of a control for access rights to network levels.
- Securing the communication between two security cells using an "unsecured" network
  Certificate-based authenticated and encrypted communication should always be used when the perimeter zone technique or standard application layer filtering technique is not available. This can take place using tunneling protocols such as PPTP (Point-To-Point Tunneling Protocol), L2TP (Layer Two Tunneling Protocol) or IPSec (IP Security) filtering or even via channels that are also secured by server-based certificates, for example RDP (Remote Desktop Protocol), a Windows Server terminal server securely published via HTTPS or Windows Server Web server via the firewall using SSL (Secure Sockets Layer) technology.

The measures concerning the security cells, such as forming security cells, securing access points and the secure communication between different security cells, are summarized under the heading "Network Security".

- System hardening
  System settings of a computer that make it more resistant to attacks by malware.
- User management and role-based operator authorizations
  Task-based operation and access authorizations (role-based access control)
- Patch management
  Patch management is a regular procedure for installing patches on plant computers.
- Malware detection & prevention
  Use of suitable and correctly configured virus scanners

Measures such as "system hardening", "user and patch management" as well as "malware detection & prevention" are summarized under the heading "Integrity Protection or Endpoint Protection".

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


Plant security
Physical security
• Building technology measures, construction technology
• Access protection, video monitoring, fire protection
Organizational security
• Assessments and audits
• Continuous risk management
• Compliance, business continuity management & disaster recovery
Network security
Division into security cells
• Division of complete plant into various zones and cells
Securing of access points
• Use of firewalls
Secure communication
• Secure communication via unprotected networks
Endpoint protection
System hardening
• Reduction of vulnerabilities of a computers
User management
• Management of user and operator authorizations
Patch management
• Regular installation of patches and updates
Malware detection and prevention
• Use of virus scanners
IA CS*

*IA CS: Industrial Automation Control System

2.3 Example configuration

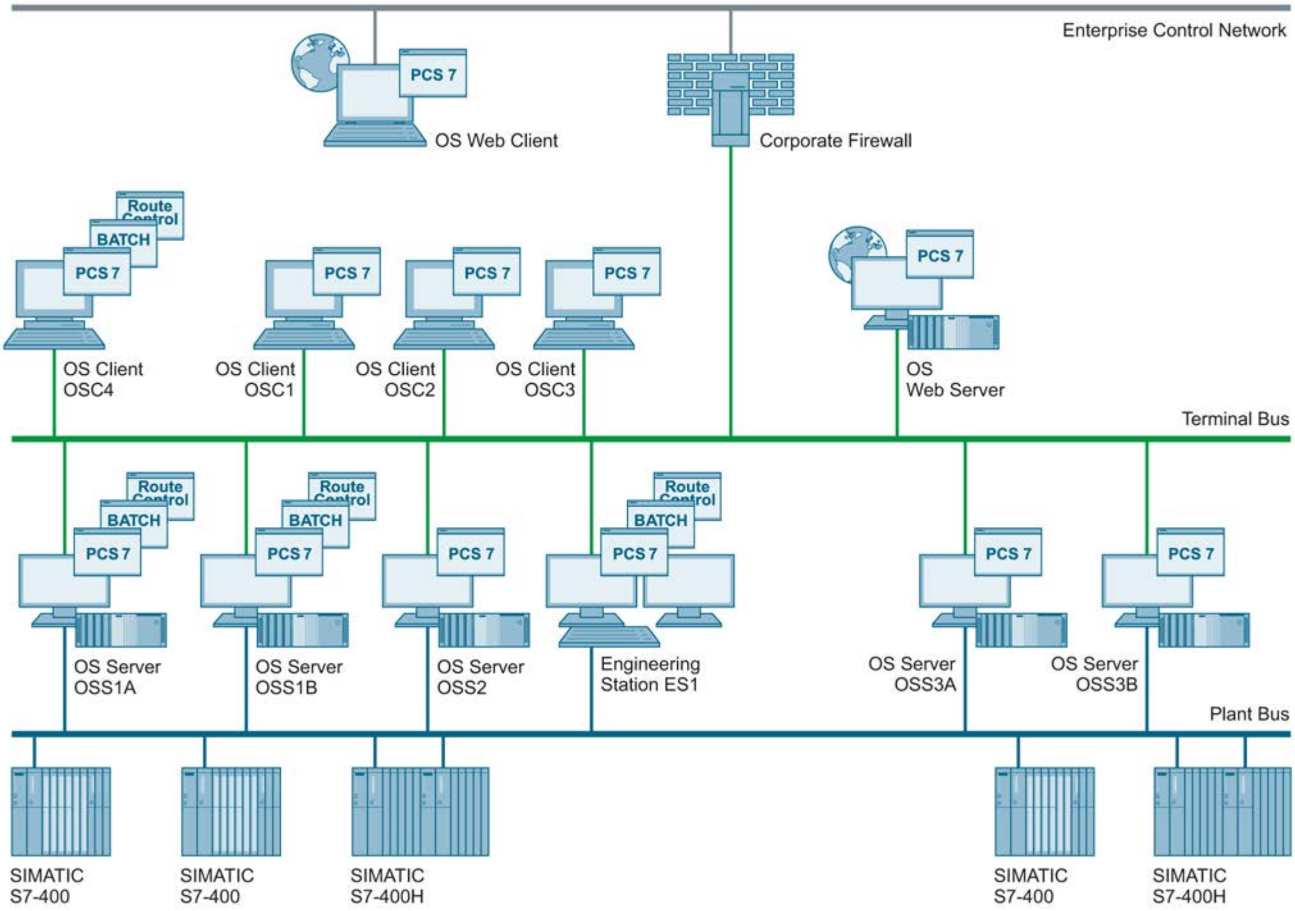
This compendium orients itself on the concept of defense-in-depth in its design and structure. In line with the concept, the individual sections are divided into the measures of network security (division into security cells, securing access points and secure communication between components in different security cells) and the measures of system integrity. 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.

Example configuration

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

3

3.1 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:

- Security concept PCS 7 & WinCC (Basic) (http://support.automation.siemens.com/WW/view/de/60119725/0/en)
- Security Concept PCS 7, Recommendations and Information (http://support.automation.siemens.com/WW/view/en/22229786)

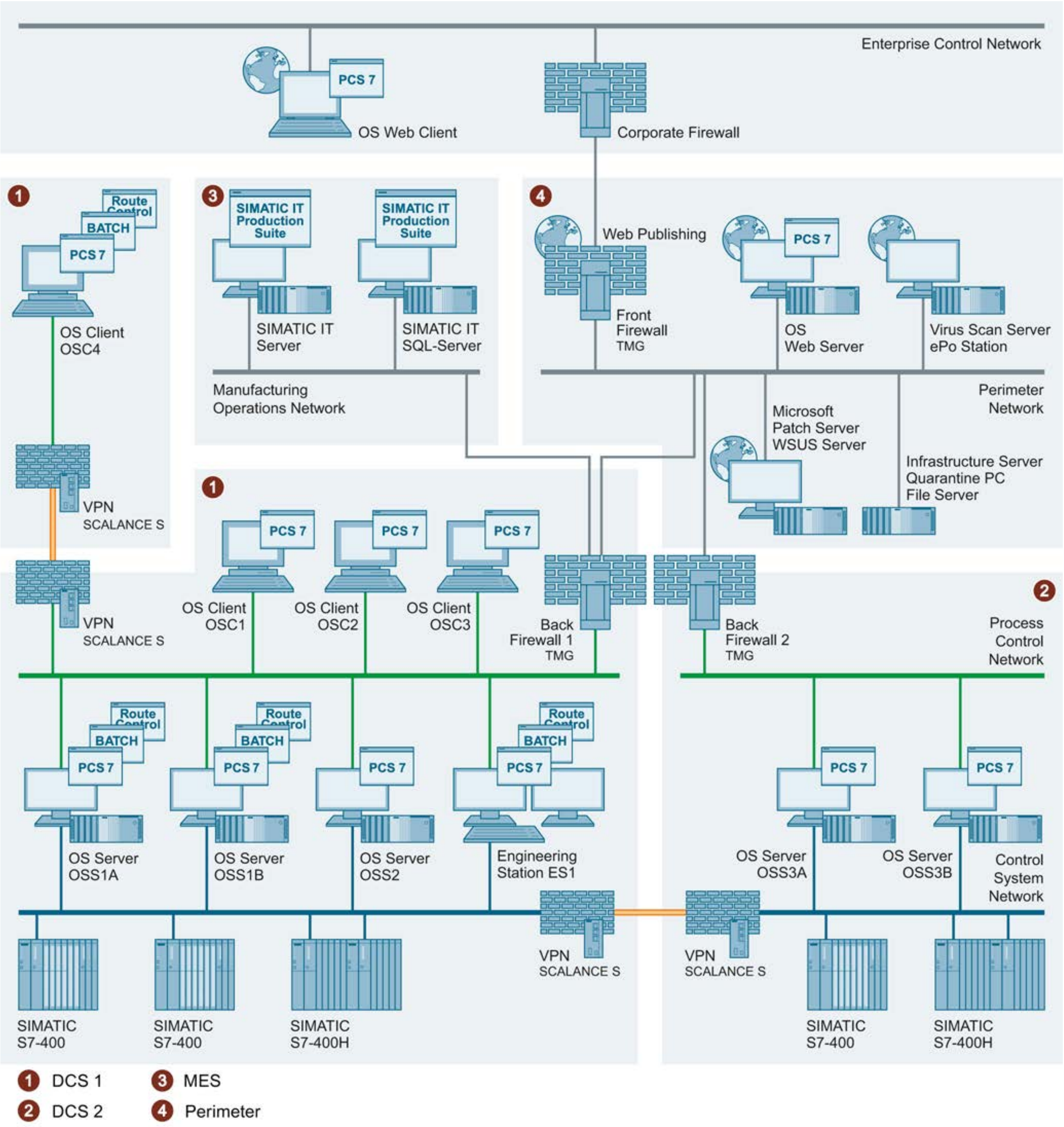
Example configuration: Division into security cells

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 the data exchange (project data/project backup) between the security cells.

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



3.2 Addressing and segmenting

IP address

Note

The term "IP Address" is used in this document in the sense of an IPv4 address. The opposite of this is an IPv6 address. This document does not deal with the IPv6 address.

Source: http://www.microsoft.com/germany/technet/datenbank/articles/600667.mspx?pf=true

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

Subnets

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
Network 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

Network classes

Source: http://www.microsoft.com/germany/technet/datenbank/articles/600667.mspx?pf=true

The address classes are defined by the Internet Assigned Numbers Authority (IANA) to systematically assign address prefixes to networks of varying size. The class of addresses indicates how many bits were used for the network ID and how many bits were used for the host ID. The address classes also determine the number of networks possible and the number of hosts per network. Of the five address classes, Class 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

3.2.1 Example configuration: Division into subnets

Addresses from the private IP address range for Class C shall be used for addressing the automation networks in the example configuration (CSN plant bus, PCN terminal bus, 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 must be 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
```

This results in the following networks:

- Network 1: Manufacturing Operations Network (IP addresses of the MON)

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

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

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

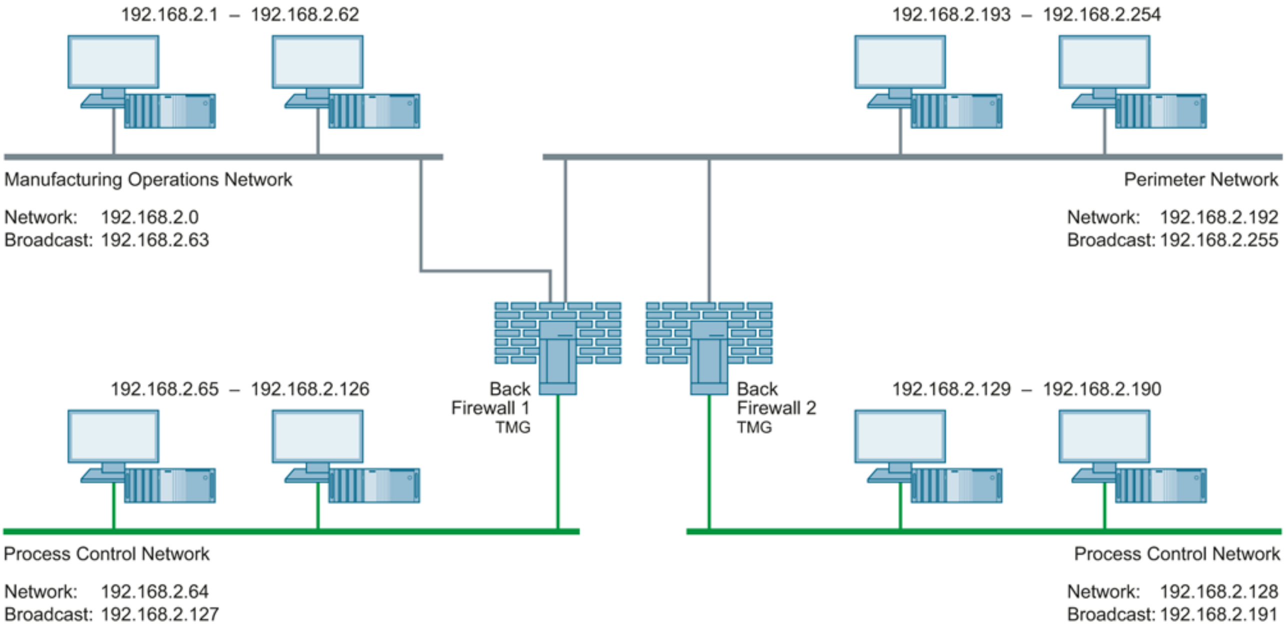
- Network 3: Process Control Network 2 (IP addresses of the PCN2 - Unit B)

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

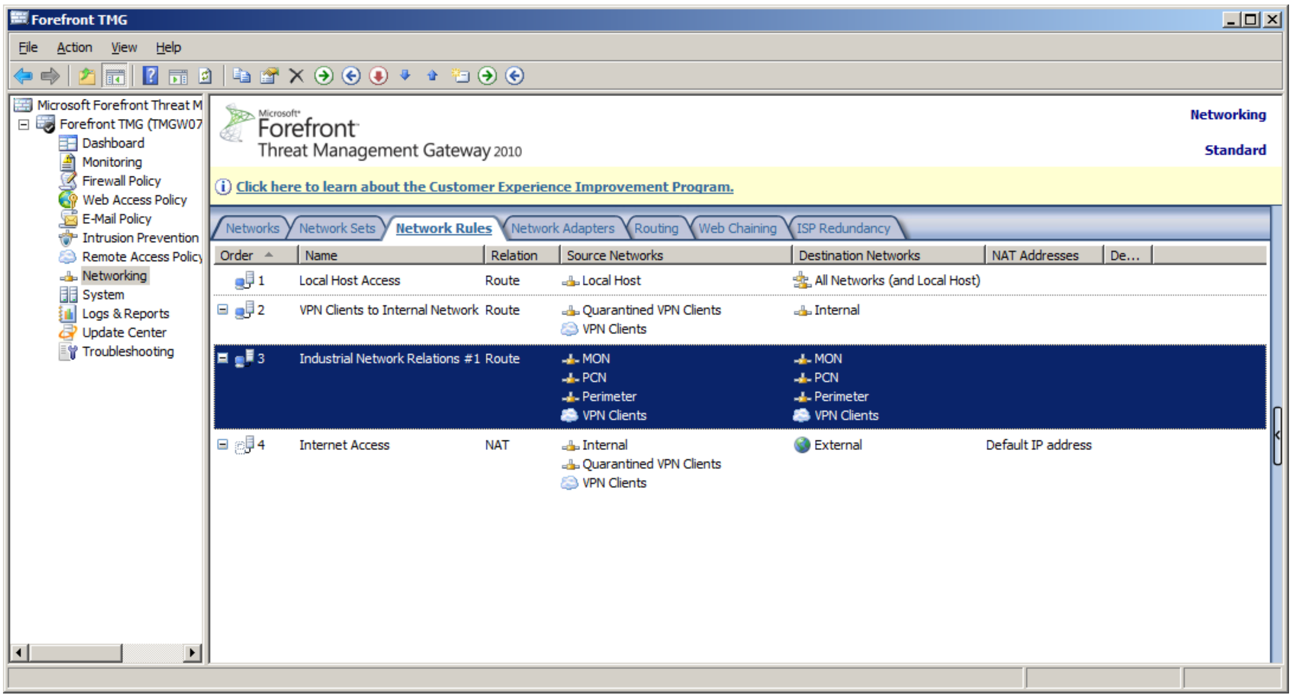
- Network 4: Perimeter Network (IP address of the Perimeter network)

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 various networks is performed by the two back-end firewalls in the aforementioned configuration. This requires establishing an appropriate network rule within the firewall used. The following figure shows an example of this rule in the Microsoft Forefront TMG Management:



Order	Name	Relation	Source Networks	Destination Networks	NAT Addresses	De...
1	Local Host Access	Route	Local Host	All Networks (and Local Host)		
2	VPN Clients to Internal Network	Route	Quarantined VPN Clients VPN Clients	Internal		
3	Industrial Network Relations #1	Route	MON PCN Perimeter VPN Clients	MON PCN Perimeter VPN Clients		
4	Internet Access	NAT	Internal Quarantined VPN Clients VPN Clients	External	Default IP address	

This network rule performs the routing between the PCN, MON and Perimeter networks in the example configuration. The data traffic between the security cells of units A and B is routed through the two back-end firewalls.

3.2.2 Example configuration: Setting of IP addresses and subnet mask

Procedure

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

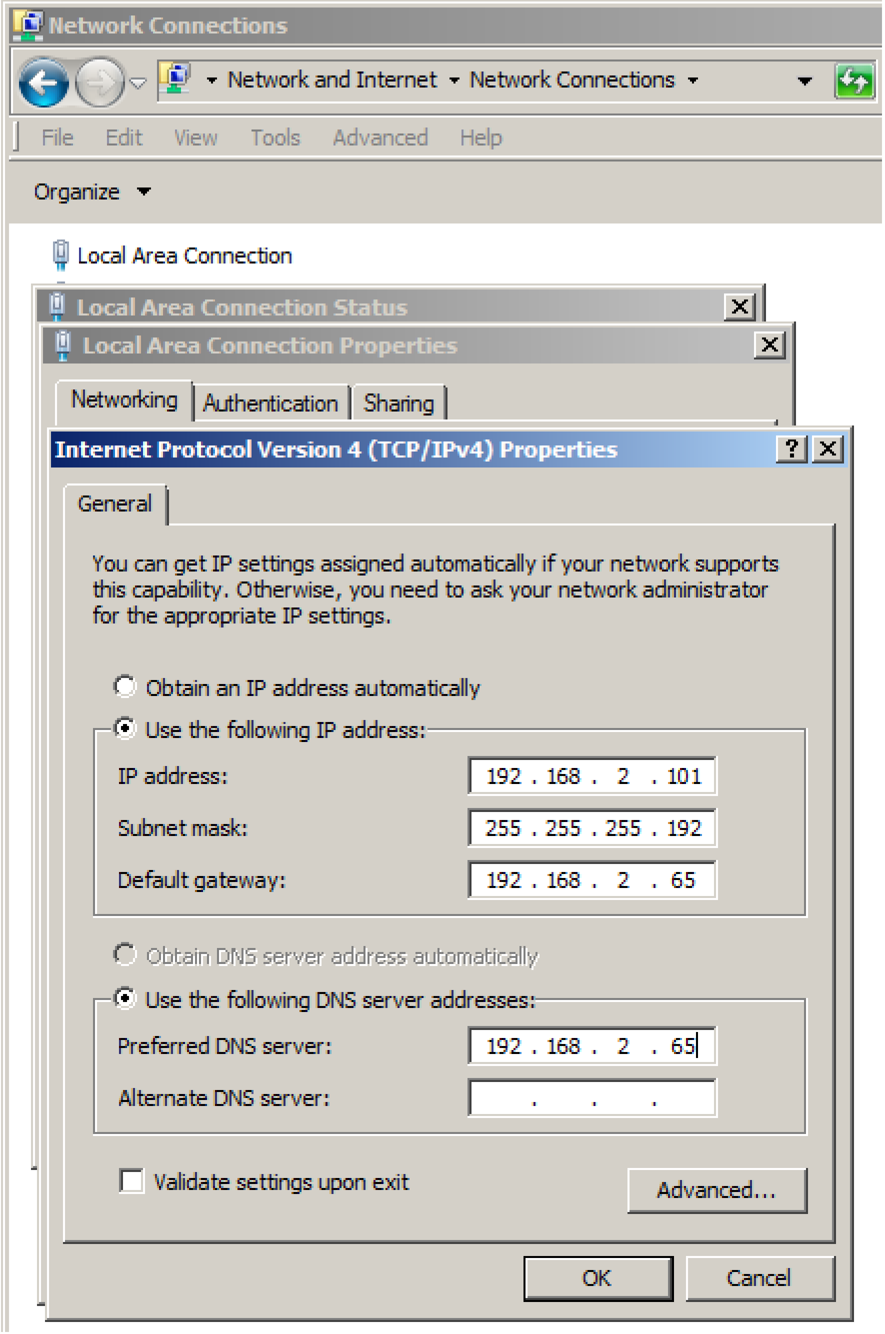
To set the IP address, subnet mask and default gateway, follow these steps:

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.


Network Connections
Network and Internet ▸ Network Connections
File Edit View Tools Advanced Help
Organize
Local Area Connection
Local Area Connection Status
Local Area Connection Properties
Networking Authentication Sharing
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 . 101

Subnet mask: 255 . 255 . 255 . 192

Default gateway: 192 . 168 . 2 . 65

○ Obtain DNS server address automatically

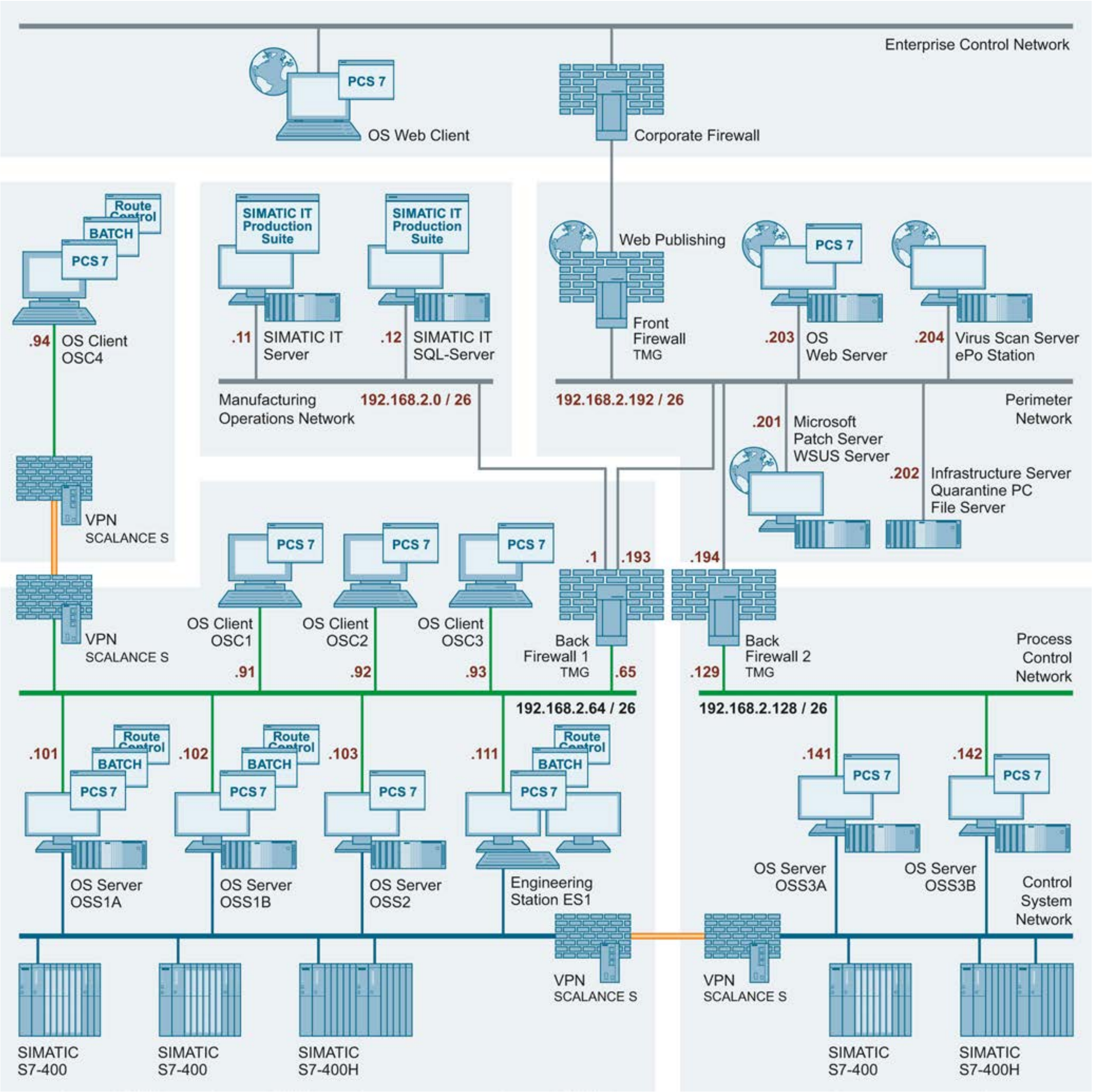
● Use the following DNS server addresses:

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.



3.3 Name resolution

Computer name

The computer name is used to uniquely identify a computer within a network. 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. Inadvertent double allocation of computer names can cause unpredictable behavior during communication.
Since the NetBIOS name is derived from the computer name (see NetBIOS name) and the NetBIOS name must be unique for NetBIOS name resolution, the computer name may not be longer than 15 characters.
The computer name must be unique and should allow an inference to be made about the function of the computer.

Note

You can learn about the rules for assigning the computer name in the installation manual "SIMATIC Process Control System PCS 7 PC Configuration and Authorization" (http://support.automation.siemens.com/WW/view/en/68157327).

Refer also to the following documents:

- FAQ "Why is the underscore character not permitted in computer names in PCS 7?" (http://support.automation.siemens.com/WW/view/en/67794552)
- 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" (http://support.automation.siemens.com/WW/view/en/68157345) section "Rules for naming in the PH"
- Online help WinCC Information system "Working with projects > Appendix > Invalid characters"
- "Projects.pdf" file. You can find this file in the installation folder of the SIMATIC product range of Siemens AG.

Changing the computer name

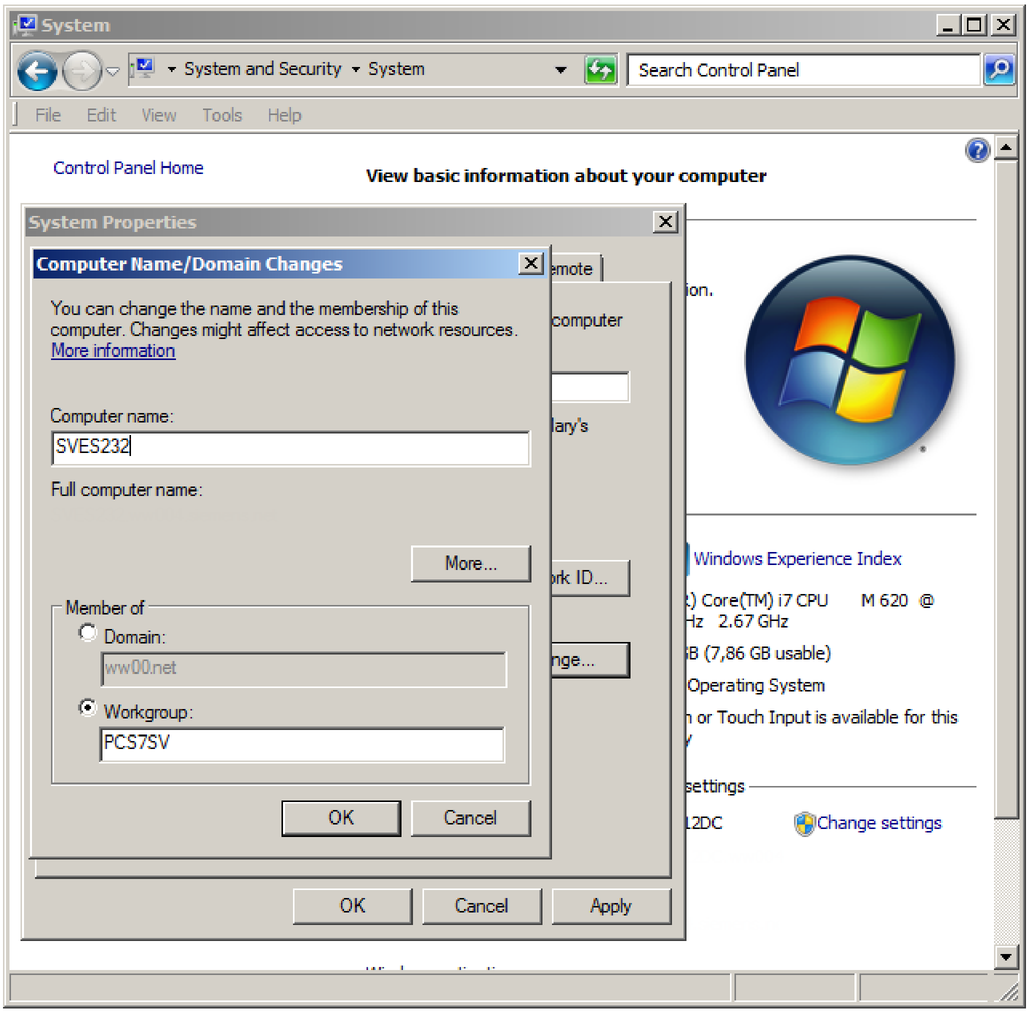
NOTICE
The computer name may be changed only prior to the installation of SIMATIC PCS 7 and prior to the initial opening of the WinCC Explorer.

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.



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: SVES232

Full computer name:

Member of
○ Domain: ww00.net
● Workgroup: PCS7SV

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.

Fully Qualified Domain Name

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

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:

- Default methods for the NetBIOS name resolution

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.

- Additional Microsoft-specific methods for the NetBIOS name resolution

Method	Description
Lmhosts files	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.

NetBIOS name resolution by using 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. 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.

To avoid network broadcasts, the entries in the Lmhosts file must be made with the keyword #PRE. The keyword #PRE specifies which entries should be loaded into the NetBIOS name cache as permanent entries at the beginning. With previously loaded entries, the network broadcasts are reduced since names could possibly be resolved via the cache instead of via broadcast queries.

Example:

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

NetBIOS name resolution with 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.

On a computer under Windows Server 2003 or Windows XP, three attempts are made to locate the primary NBNS server. If no response is received or a negative NetBIOS name query response message indicates that the name resolution has failed, a computer under 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.

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. A freely selectable name is an alias name for an IP address that can be assigned and used by individual persons. A domain name is a structured name in a hierarchically organized namespace that is referred to as DNS (Domain Name System). An example for a domain name is www.microsoft.com.

Freely selectable names are resolved via entries in the "Hosts" file. This file is located in the folder "systemroot\System32\Drivers\etc".

To resolve domain names, DNS name queries are sent to a configured DNS server. The DNS server is a computer on which entries with assignments of domain names to IP addresses or information about other DNS servers are stored. The DNS server resolves the queried domain name into an IP address and returns the result.

You have to configure your computers with the IP address of the responsible DNS server to resolve domain names. You have to configure Active Directory-based computers under Windows or operating systems of the Windows Server product family with the IP address of a DNS server.

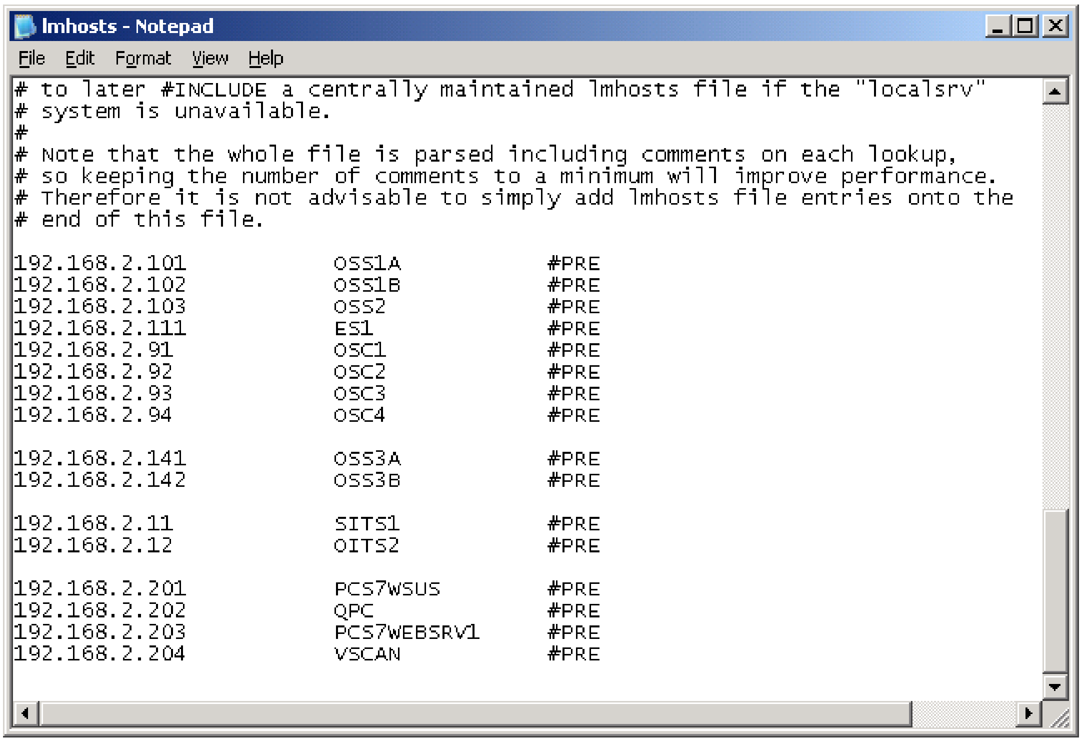
Example configuration: Name resolution

The example configuration was divided into four or five security cells (DCS1, DCS2, MES and Perimeter). None of these security cells contains a WINS server for the NetBIOS name resolution. A DNS server for the host name resolution is also lacking in every security cell. The "lmhosts" file should be configured on every computer to ensure an error-free name resolution.

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 the installation of SIMATIC PCS 7 and prior to the initial opening of the WinCC Explorer.

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 "MES", "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.

3.4 Managing networks and network services

The management of the network settings and required network services of a process control system can be organized in a distributed or central way. Mixed configurations of central and distributed management are possible.

Central management (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 or WINS
- Time synchronization (NTP, SNTP)

Distributed management (Windows workgroups)

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 a part of the MS Active Directory. You can find information on the configuration of RADIUS options for network devices in the manuals for the Scalance X network devices.

DHCP

DHCP (Dynamic Host Configuration Protocol) allows client computers and other TCP/IP-based network devices to be assigned valid IP addresses automatically. The additional configuration parameters required by these clients and devices, for example, DNS server, WINS server, default gateway, subnet mask can also be provided.

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

- Large networks with frequently changing topology.
- Users who simply want to have "a network connection" and do not want to deal with the network configuration in any detail.

Both of these application scenarios do not apply to an automation system. Using DHCP involves several security risks that cannot be outweighed by the benefits of an automation plant.

Note

Using a DHCP server

The use of a DHCP server for automatic network configuration (IPv4 address, subnet mask, etc.) is not recommended for security reasons.

If a DHCP server is used, address reservations must be used.

3.5 Access points to the security cells

3.5.1 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)" (http://support.automation.siemens.com/WW/view/en/60119725).

3.5.2 Automation Firewall Appliance

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

The current solution for the automated firewall is based on the firewall solution from Microsoft (Microsoft Forefront Threat Management Gateway 2010). An optimized rule base can be created using the Industrial Wizard and integrated SecureGUARD Appliance Management.

Note

The current solution of the automation firewall is based on the Microsoft Forefront TMG 2010. As of December 2012, this Microsoft product ceased to be available. An alternative firewall solution is currently being evaluated. However, a final result was not available at the time of this document's publication.

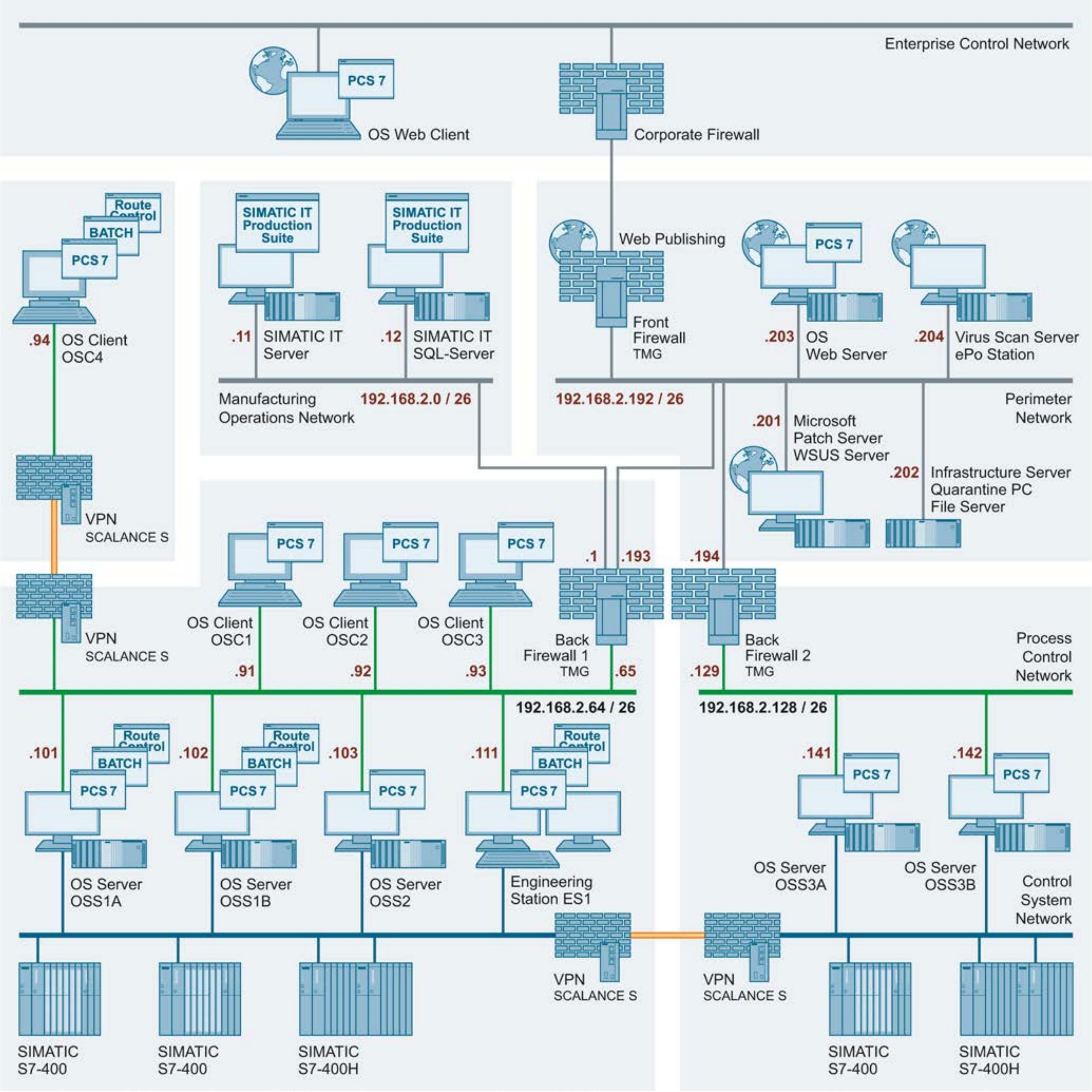
For this reason, the required firewall rules have been neutrally formulated over the course of development.

You can find the complete range of products for automation firewalls in the PCS 7 Add-on catalog. You can download this catalog from the SIMATIC PCS 7 website (https://www.automation.siemens.com/mcms/process-control-systems/en/simatic-pcs-7/Pages/simatic-pcs-7.aspx).

3.5.3 Example configuration: Access rules

Access rules

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



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

The following table features the required cross-security cell data exchange:

Security cell	Security cell	Via	Purpose
Perimeter	DSC1	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 • Communication between PCS7WEBSRV1 and OSS1A/B, OSS2 and ES1 • File transfer between QPC and ES1
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 • Communication between PCS7WEBSRV1 and OSS3A/B
Perimeter	MES	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
MES	DCS1		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
Perimeter WSUS to PCN1 OS Server #1	Allow	HTTP, HTTPS	[WSUS] [192.168.2.201]	[OS Server] [192.168.2.101, 192.168.2.102] [OS Server] [192.168.2.103]
PCN1 OS Server to Perimeter WSUS #1	Allow	HTTP, HTTPS	[OS Server] [192.168.2.103]	[WSUS] [192.168.2.201]
PCN1 OS Server to Perimeter WSUS #2	Allow	HTTP, HTTPS	[OS Server] [192.168.2.101, 192.168.2.102]	[WSUS] [192.168.2.201]
Perimeter Virus Scan Server to PCN1 OS Server #1	Allow	HTTP, HTTPS	PatternUpdate] [192.168.2.204]	[OS Server] [192.168.2.101, 192.168.2.102] [OS Server] [192.168.2.103]
PCN1 OS Server to Perimeter Virus Scan Server #1	Allow	HTTP, HTTPS	[OS Server] [192.168.2.103]	[PatternUpdate] [192.168.2.204]
PCN1 OS Server to Perimeter Virus Scan Server #2	Allow	HTTP, HTTPS	[OS Server] [192.168.2.101, 192.168.2.102]	[PatternUpdate] [192.168.2.204]
PCN1 OS Server to Perimeter OS WebNavigator #1	Allow	IPSec[1]	[OS Server] [192.168.2.103]	[OS WebNavigator] [192.168.2.203]
PCN1 OS Server to Perimeter OS WebNavigator #2	Allow	IPSec[1]	[OS Server] [192.168.2.101, 192.168.2.102]	[OS WebNavigator] [192.168.2.203]
Allow Web servers to access PCN1 #1	Allow	IPSec[1]	[OS WebNavigator] [192.168.2.203]	[OS Server] [192.168.2.101, 192.168.2.102] [OS Server] [192.168.2.103]
[1] The use of the "IPSec" protocol type requires a certificate-based signed connection via IPSec conforming to the security policy between the components in the various security cells. If there is no such connection, "All outbound traffic" can also be set. However, this dispenses the port filtering for such a FW rule.				

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

Name	Action	Protocols	From	To
Perimeter WSUS to PCN2 OS Server #1	Allow	HTTP, HTTPS	[WSUS] [192.168.2.201]	[OS Server] [192.168.2.141, 192.168.2.142]
PCN2 OS Server to Perimeter WSUS #1	Allow	HTTP, HTTPS	[OS Server] [192.168.2.141, 192.168.2.142]	[WSUS] [192.168.2.201]
Perimeter Virus Scan Server to PCN2 OS Server #1	Allow	HTTP, HTTPS	[PatternUpdate] [192.168.2.204]	[OS Server] [192.168.2.141, 192.168.2.142]
PCN2 OS Server to Perimeter Virus Scan Server #1	Allow	HTTP, HTTPS	[OS Server] [192.168.2.141, 192.168.2.142]	[PatternUpdate] [192.168.2.204]
PCN2 OS Server to Perimeter OS WebNavigator #1	Allow	IPSec[1]	[OS Server] [192.168.2.141, 192.168.2.142]	[OS WebNavigator] [192.168.2.203]
Allow Web servers to access PCN1 #1	Allow	IPSec[1]	[OS WebNavigator] [192.168.2.203]	[OS Server] [192.168.2.141, 192.168.2.142]
[1)] The use of the "IPSec" protocol type requires a certificate-based signed connection via IPSec conforming to the security policy between the components in the various security cells. If there is no such connection, "All outbound traffic" can also be set. However, this dispenses the port filtering for such a FW rule.				

The example configuration contains only one engineering station in security cell DCS1 which is also being used for the configuration of the OS servers OSS3A and OSS3B. To ensure the configuration steps, specifically loading the OS, you also have to manually configure the following access rules:

Name	Action	Protocols	From	To
PCN2 OS Server to PCN 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 certificate-based signed connection via IPSec conforming to the security policy between the components in the various security cells. If there is no such connection, "All outbound traffic" can also be set. However, this dispenses the port filtering for such a FW rule.				

It should also be possible to operate and monitor the OS servers OSS3A and OSS3B from the OS clients in the PCN. To ensure this, you need to configure the following access rules:

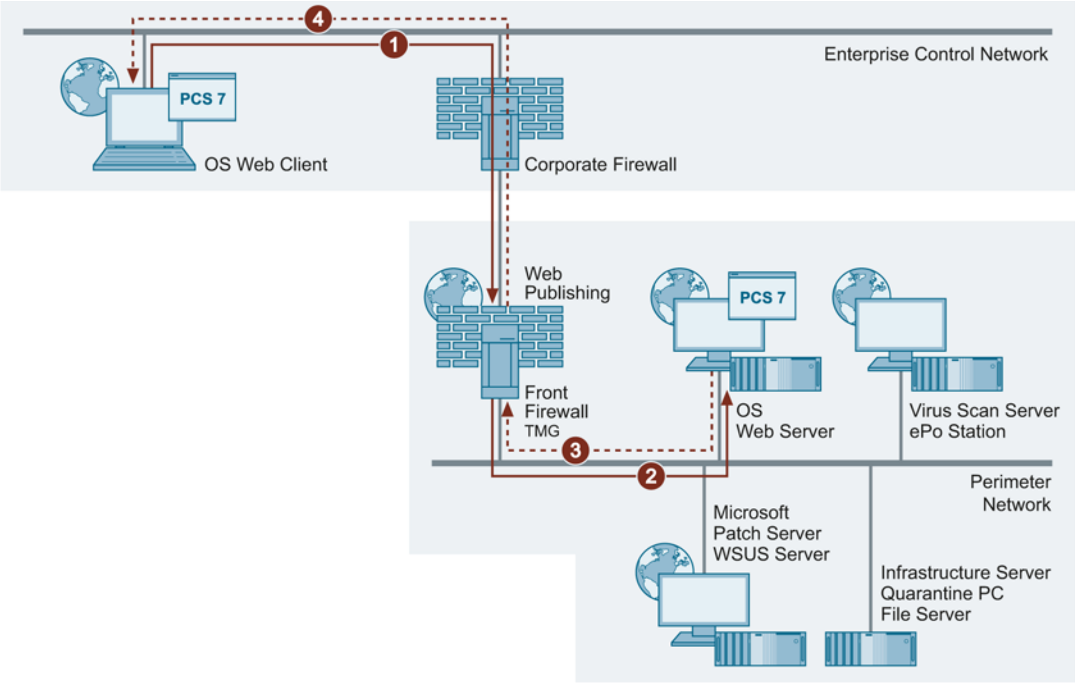
Name	Action	Protocols	From	To
PCN2 OS Server to PCN OS Client #1	Allow	IPSec[1]	[OS Server] [192.168.2.141, 192.168.2.142]	[ES Client] [192.168.2.91]
PCN2 OS Server to PCN OS Client #2	Allow	IPSec[1]	[OS Server] [192.168.2.141, 192.168.2.142]	[ES Client] [192.168.2.92]
PCN2 OS Server to PCN OS Client #3	Allow	IPSec[1]	[OS Server] [192.168.2.141, 192.168.2.142]	[ES Client] [192.168.2.93]
PCN2 OS Server to PCN OS Client #4	Allow	IPSec[1]	[OS Server] [192.168.2.141, 192.168.2.142]	[ES Client] [192.168.2.94]
PCN OS Client to PCN2 OS Server #1	Allow	IPSec[1]	[ES Client] [192.168.2.91]	[OS Server] [192.168.2.141, 192.168.2.142]
PCN OS Client to PCN2 OS Server #2	Allow	IPSec[1]	[ES Client] [192.168.2.92]	[OS Server] [192.168.2.141, 192.168.2.142]
PCN OS Client to PCN2 OS Server #3	Allow	IPSec[1]	[ES Client] [192.168.2.93]	[OS Server] [192.168.2.141, 192.168.2.142]
PCN OS Client to PCN2 OS Server #4	Allow	IPSec[1]	[ES 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 certificate-based signed connection via IPSec conforming to the security policy between the components in the various security cells. If there is no such connection, "All outbound traffic" can also be set. However, this dispenses the port filtering for such a FW rule.

Example configuration: Web publishing of a PCS 7 web server at the front-end firewall

To access a Web server in the Perimeter network from an external network, it must be published via the front-end firewall. The technique of Web publishing, which is supported by the automation firewall and is used here, offers better security than the obsolete technique of Web tunneling or Web forwarding. Opening port 80 or 443 and subsequently simply passing the queries through the front-end firewall directly to the Web server, as called for in this technique, should no longer be applied.

During Web publishing (see the following figures), the Web client does not directly access the Web server from the external network. Instead, it directs its query to the automation firewall (1). The automation firewall forwards this 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).



Only HTTPS should be allowed between Web client and automation firewall. This ensures the authenticity of the TMG via server certificate is guaranteed and encrypts the communication between Web client and firewall, thereby protecting it against manipulation. Depending on the desired internal security, either HTTP or HTTPS can be used for the automation firewall access to the Web server.

If Web clients from an external network are to access the Web server, it must be published at the front-end firewall. If Web clients from an MES network (MON) should be allowed access, however, the publishing is performed at the back-end firewall.

Note

The steps for configuring the OS Web server and the settings of the Web Client are described in the manual "SIMATIC Process Control System PCS 7 V7.0 PCS 7 OS Web Option" (http://support.automation.siemens.com/WW/view/en/24496095).

Example configuration: Web publishing of a PCS 7 web server at the front-end firewall

In order to reach the PCS 7 Web server that is located in the Perimeter network from another internal network, for example, from the Manufacturing Operations Network (MON) via a Web client, the Web server must first be published at the back-end firewall 1.
Since this functionality is not implemented in the Industrial Wizard, you need to perform the publishing rule using the Microsoft Forefront TMG Management Console in the back-end firewall.

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 Network Inspection System (NIS) in Microsoft Forefront TMG 2010 is an implementation of the IDS/IPS functionality. NIS is designed specifically for detecting and preventing attacks on Microsoft operating systems and applications. NIS is based on signatures developed by the Microsoft Malware Protection Center (MMPC) and distributed via Windows Update or WSUS.

NIS in Microsoft Forefront TMG 2010 offers protection against known attacks using low-level network protocol inspection. Each data packet is analyzed for protocol status, structure and content of the message. NIS checks the received data packet only after it has been checked by the firewall policy and any assigned Web or application filters.

Additional information

You can find the complete range of products for automation firewalls in the PCS 7 Add-on catalog. You can download this catalog from the SIMATIC PCS 7 website (https://www.automation.siemens.com/mcms/process-control-systems/en/simatic-pcs-7/Pages/simatic-pcs-7.aspx).

3.6 Secure communication between security cells

3.6.1 Overview

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

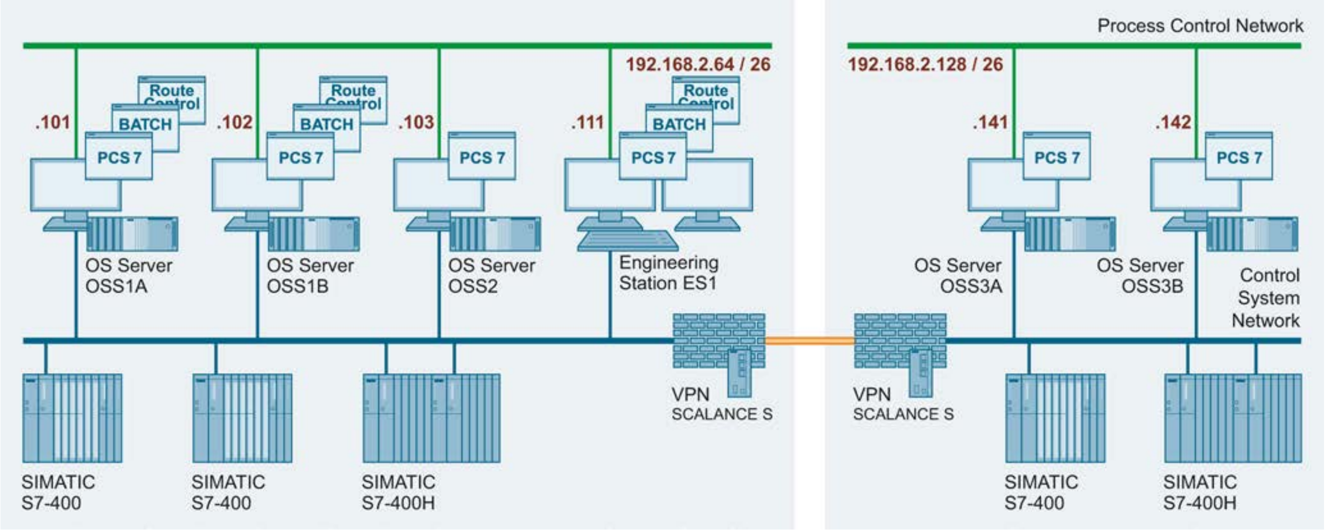
- Data exchange on the CSN level
  Data exchange between automation systems in different security cells
- Data exchange on the PCN level
  Data exchange for operating and monitoring with remote OS clients, which means OS clients located in other security cells than the corresponding OS server(s).

3.6.2 Data exchange between automation systems

3.6.2.1 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 an example of communication between automation systems in different security cells:



In the internal networks protected by SCALANCE S, IPSec tunnels provide the node for a secured data connection through the unsecured external network.

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

SCALANCE S uses the IPSec protocol for tunneling (tunnel mode of IPSec).

Note

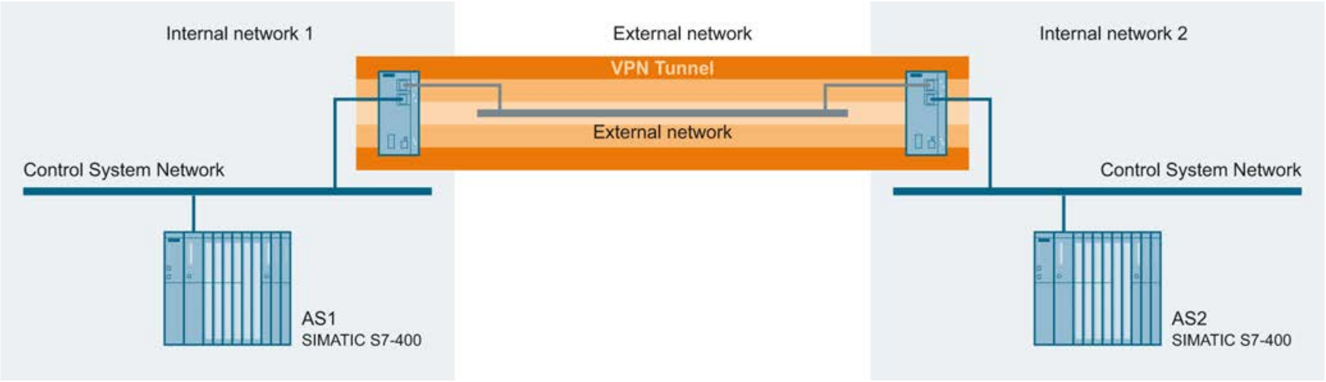
You can find additional information on SCALANCE S in the manual "SCALANCE S and SOFTNET Security Client" (http://support.automation.siemens.com/WW/view/en/21718449).

3.6.2.2 Example configuration: Establishing secure communication between security cells with SCALANCE S

Introduction

In this example, 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"). In the internal network, the network node is represented by an automation system in each case which is connected to the "internal network" port 2 (Port 2 = green) of a SCALANCE S module.

- AS1: Represents a node of the CSN in security cell 1 (internal network 1)
- AS2: 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 ("unsecured network") is connected to the "external network" port (Port 1 = red) of the SCALANCE S module.

Overview of configuration steps

1. Configuring SCALANCE S and networks
2. Configuring IP settings of automation systems
3. Create project and module
4. Configure tunnel function
5. Loading the configuration in SCALANCE S
6. Test

Configuring SCALANCE S and networks

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

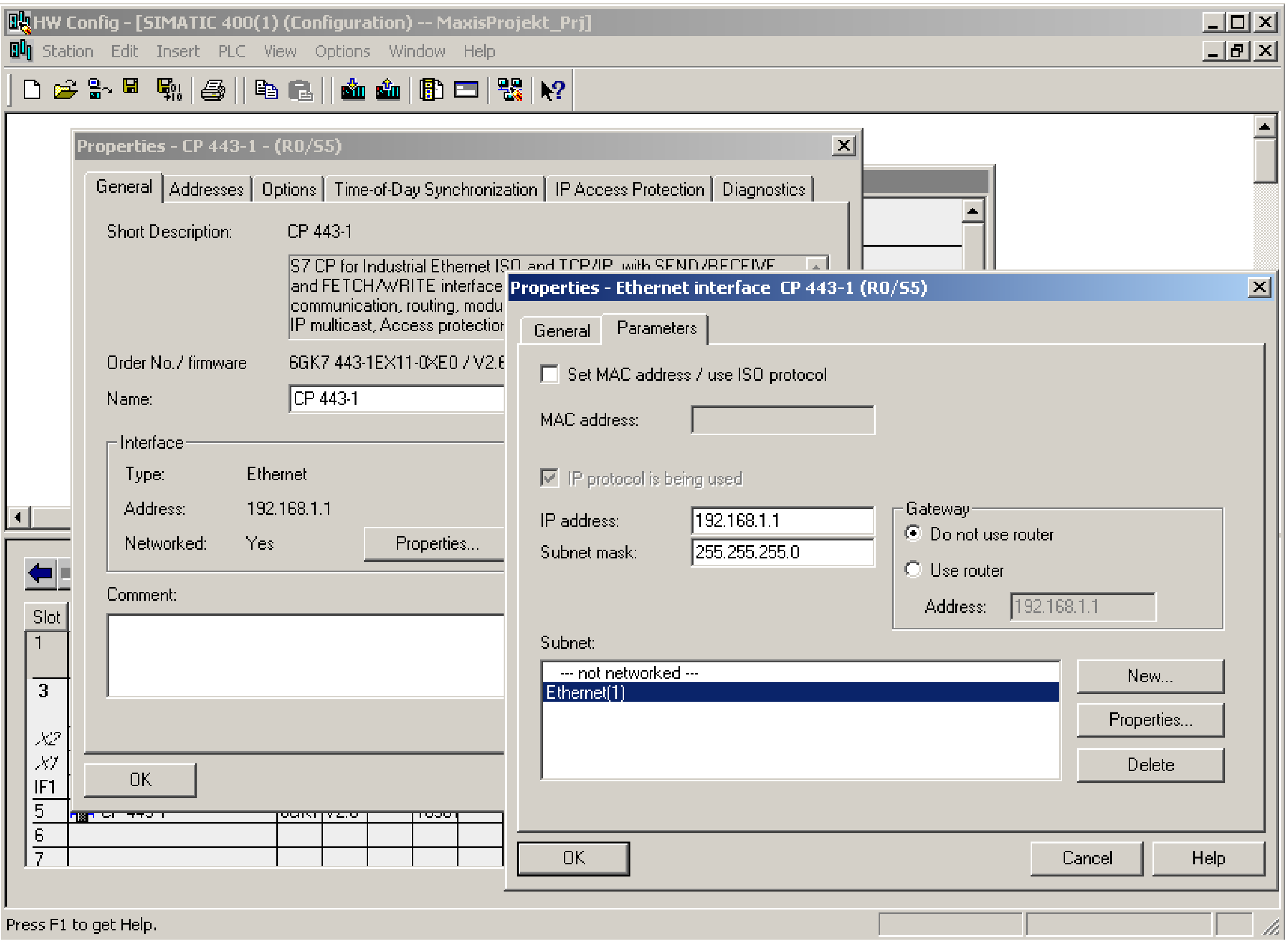
1. Start up the SCALANCE S according to the operating instructions.
2. Establish the physical network connections by inserting the connectors of the network cables into the ports (RJ45 sockets):
   - Connect Control System Network 1 with Port 2 of Module 1 and Control System Network 2 with Port 2 of 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
AS 1	192.168.1.1	255.255.255.0
AS 2	192.168.2.1	255.255.255.0

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



Short Description: CP 443-1

S7 CP for Industrial Ethernet ISO and TCP/IP with SEND/RECEIVE and FETCH/WRITE interface, communication, routing, modu IP multicast, Access protection

Order No./ firmware: 6GK7 443-1EX11-0XE0 / V2.6

Name: CP 443-1

Interface
Type: Ethernet
Address: 192.168.1.1
Networked: Yes

Comment:

☐ 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: 192.168.1.1

Subnet:
--- not networked ---
Ethernet(1)

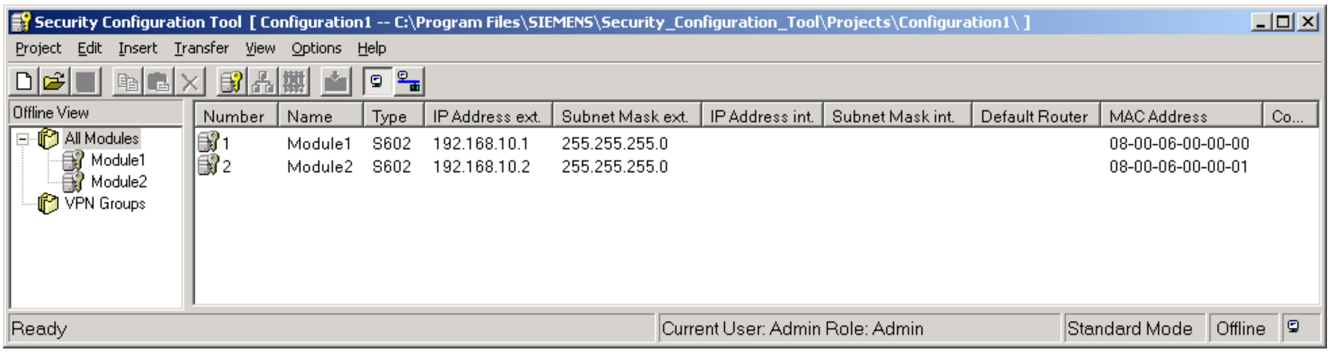
Creating project and modules

The SCALANCE S612 and S613 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 following command: "Project > New"
   You are prompted to enter a user name and a password. The user entry you define here is assigned the role of an administrator.
3. Enter a user name and a password and confirm your entry.
   A new project is created.
4. Click "All Modules".

5. Create a second module with the command "Insert > Module".
   This module automatically obtains a name based on the defaults for the project and any preset parameter values. The IPv4 address is incremented from "Module 1" and is different.


Security Configuration Tool [Configuration1 -- C:\Program Files\SIEMENS\Security_Configuration_Tool\Projects\Configuration1\ ]
Project
Edit
Insert
Transfer
View
Options
Help
Offline View
All Modules
Module1
Module2
VPN Groups

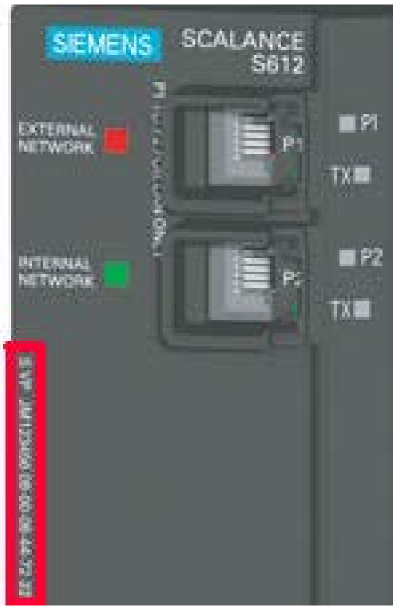
Number	Name	Type	IP Address ext.	Subnet Mask ext.	IP Address int.	Subnet Mask int.	Default Router	MAC Address	Co...
1	Module1	S602	192.168.10.1	255.255.255.0				08-00-06-00-00-00	
2	Module2	S602	192.168.10.2	255.255.255.0				08-00-06-00-00-01	

Ready | Current User: Admin Role: Admin | Standard Mode | Offline

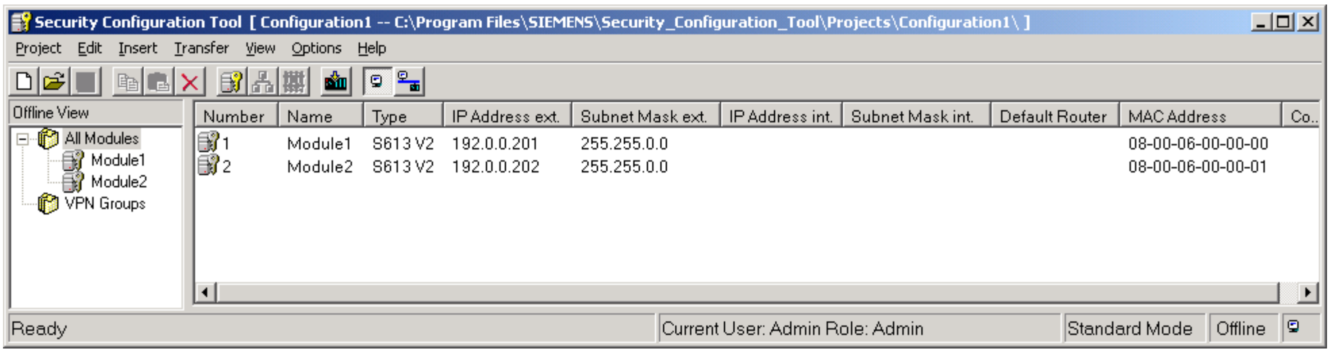
6. Select the entry "Module 1".

7. Click on the "Type" column and select the type of the module used.

8. In the "MAC address" column, enter the MAC address of the module in the specified format.
   You can find the MAC address on the front of the SCALANCE S module.



9. In the "IP address ext." column, enter the IPv4 address of the module in the specified format and adapt the subnet mask:
   – For Module 1: IPv4 address: 191.0.0.201 Subnet mask: 255.255.0.0
   – For Module 2: IPv4 address: 191.0.0.202 Subnet mask: 255.255.0.0


Security Configuration Tool [Configuration1 -- C:\Program Files\SIEMENS\Security_Configuration_Tool\Projects\Configuration1\ ]
Project
Edit
Insert
Transfer
View
Options
Help
Offline View
All Modules
Module1
Module2
VPN Groups
Ready
Current User: Admin Role: Admin
Standard Mode
Offline

Number	Name	Type	IP Address ext.	Subnet Mask ext.	IP Address int.	Subnet Mask int.	Default Router	MAC Address	Co..
1	Module1	S613 V2	192.0.0.201	255.255.0.0				08-00-06-00-00-00	
2	Module2	S613 V2	192.0.0.202	255.255.0.0				08-00-06-00-00-01	

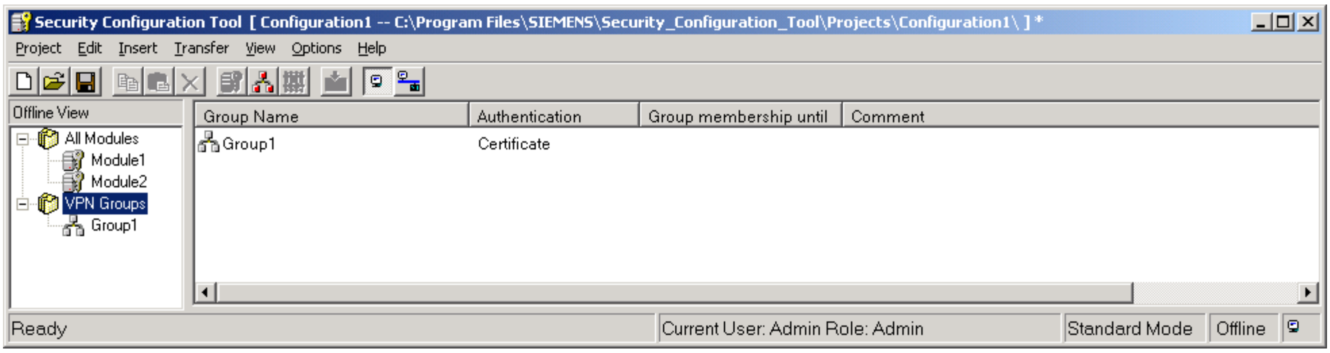
10. Repeat steps 6 to 9 for "Module 2".

Configuring the tunnel connection

Two SCALANCE S can establish one and only one 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. Select the "All Groups" navigation pane in the "Security Configuration Tool".
2. Create a new group with the command "Insert > Group".
   The group is inserted and automatically named "Group 1".



Security Configuration Tool [Configuration1 -- C:\Program Files\SIEMENS\Security_Configuration_Tool\Projects\Configuration1\ ] *

Group Name	Authentication	Group membership until	Comment
Group1	Certificate		

Ready | Current User: Admin Role: Admin | Standard Mode | Offline

3. In the content area, select the SCALANCE S module "Module 1" and drag it onto "Group 1" in the navigation pane.
   The module is now also assigned to "Group 1". The color of the key symbol of the module icon changes from gray to blue.
4. In the content area, select the SCALANCE S module "Module 2" and drag it onto "Group 1" in the navigation pane.
   The module (Module 2) is also assigned to "Group 1".
5. Save the project under a suitable name with the command "Project > Save As ...".
   This concludes the configuration of the tunnel connection.

Loading the configuration in SCALANCE S

To load the configuration created in the SCALANCE S modules, follow these steps:

1. Select the command "To all modules ..." in the "Transfer" menu.

Note

You can find more information about configurations and application possibilities of SIMATIC security products under http://support.automation.siemens.com/WW/view/en/67329379 or in the Siemens Industry Online Support Portal.

3.6.3 Quarantine station (file server)

Introduction

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 quarantine station is therefore important when the recommendations relating to system hardening are implemented, particularly for blocking the USB ports in the automation system (see section Working with mobile data media (Page 76)). As a central data communication point, the quarantine station should be especially protected from a security point of view. Therefore, the local security measures (for example, firewall, virus scanner, etc.) should be configured more strictly for it.

As shown in the example configuration, the quarantine station should be positioned in the Perimeter network. A corresponding rule must be stored in the back-end firewall(s) to ensure communication between the quarantine station and the computers in security cells DCS1 and DCS2 via the back-end firewall(s).

Firewall rules

If the automation firewall is used as back-end firewall, the quarantine station (FTP server) at the back-end firewall can be published for the security cells DCS1 and DCS2 (see Web publishing of the PCS 7 Web server at the front-end firewall or Web publishing of the PCS 7 Web server at the back-end firewall). For this purpose, a corresponding publishing rule (FTP forwarding) must be configured with the "Publish Non-Web Server Protocols" task in the automation firewall (Microsoft Forefront TMG Management Console):

Name	Action	Traffic	From	To	Networks
Publish FTP server	Allow	FTP server	Anywhere	IP address of quarantine station	PCN1

This FTP publication of the FTP server (quarantine station) achieves a higher security compared to a pure port release.

Note

You can find the complete range of products for automation firewalls in the PCS 7 Add-on catalog. You can download this catalog from the SIMATIC PCS 7 website (https://www.automation.siemens.com/mcms/process-control-systems/en/simatic-pcs-7/Pages/simatic-pcs-7.aspx).

If a firewall is used that does not offer the possibility of an FTP publication, the following tables show the required firewall rules:

- Front-end firewall

Name	Action	Protocols	From	To
ECN computer to perimeter Q-PC	Allow	FTP / 21	IP address of the computer in the Office network	IP address of the Q-PC in the Perimeter network
Perimeter Q PC to ECN computer	Allow	FTP / 21	IP address of the Q-PC in the Perimeter network	IP address of the computer in the Office network

The rules in the front-end firewall are only required if FTP data access from the ECN (Enterprise Control Network) to the quarantine station is planned in the Perimeter network.

- Back-end firewall

Name	Action	Protocols	From	To
Perimeter Q-PC to PCN ... #1	Allow	FTP / 21	IP address of the Q-PC in the Perimeter network	IP address of the computer in PCNx (e.g. ES1)
PCN … to Perimeter Q-PC #1	Allow	FTP / 21	IP address of the computer in PCNx (e.g. ES1)	IP address of the Q-PC in the Perimeter network

FTP server configuration

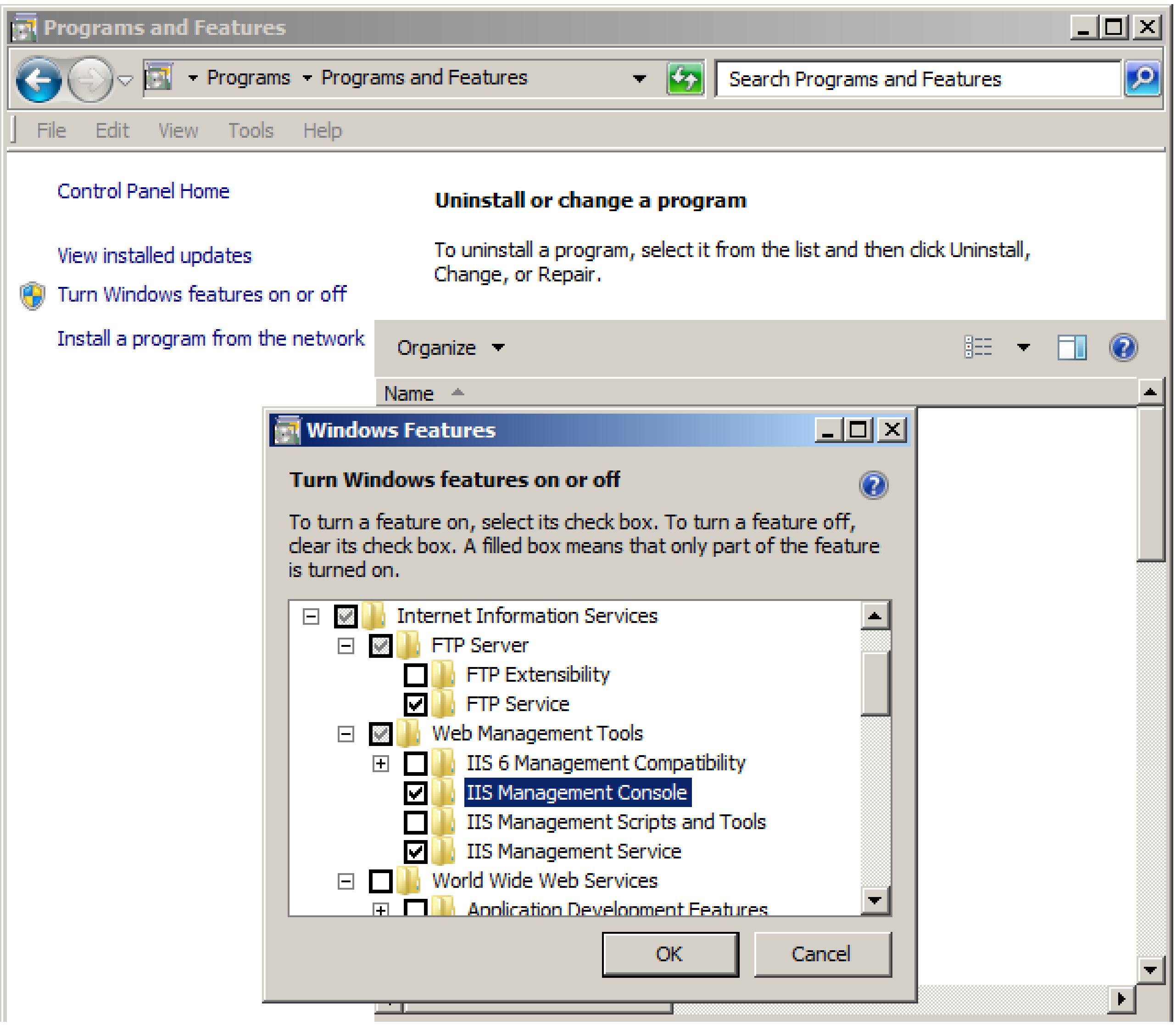
Enabling FTP Service

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

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 "Turn Windows features on or off" 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
OK
Cancel

Uninstall or change a program

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

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.

- ▣ 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

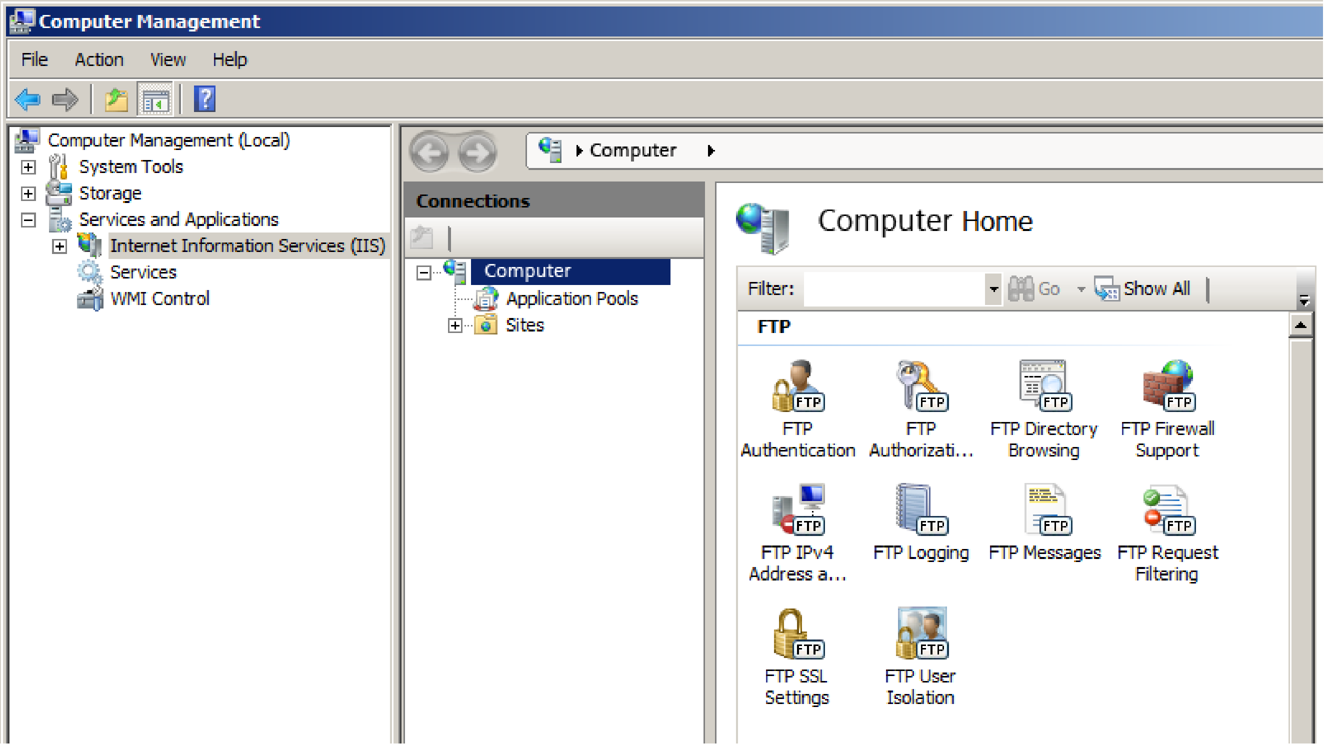
   If the property values differ, open the "Properties" dialog from the shortcut menu of the service and change the properties as described above.

Configuring the FTP server

To configure the FTP server, follows these steps:

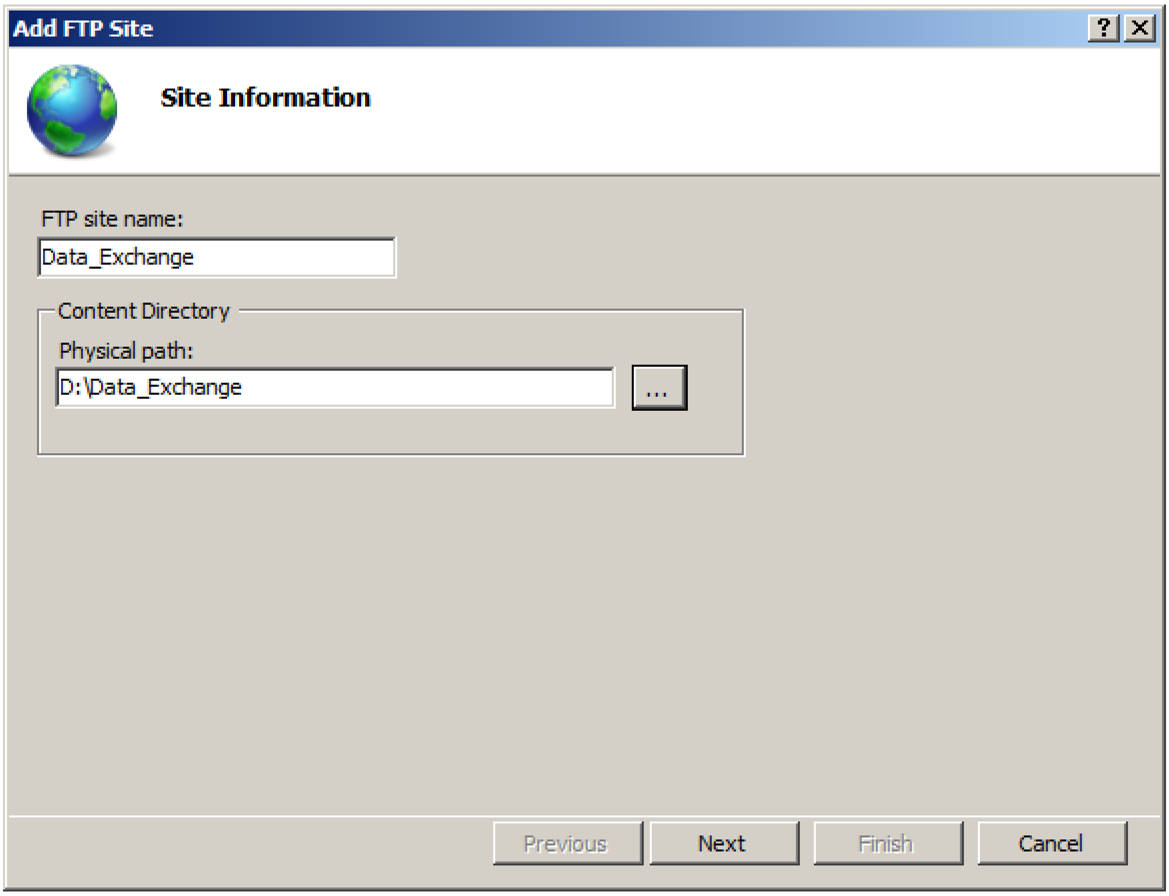
1. In the Windows Start menu, right-click on "Computer" and select the shortcut menu command "Manage".
   Enter the administrator password, if required. If you are already logged on as an administrator, confirm the execution of the application.
   The "Computer Management" dialog opens.

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

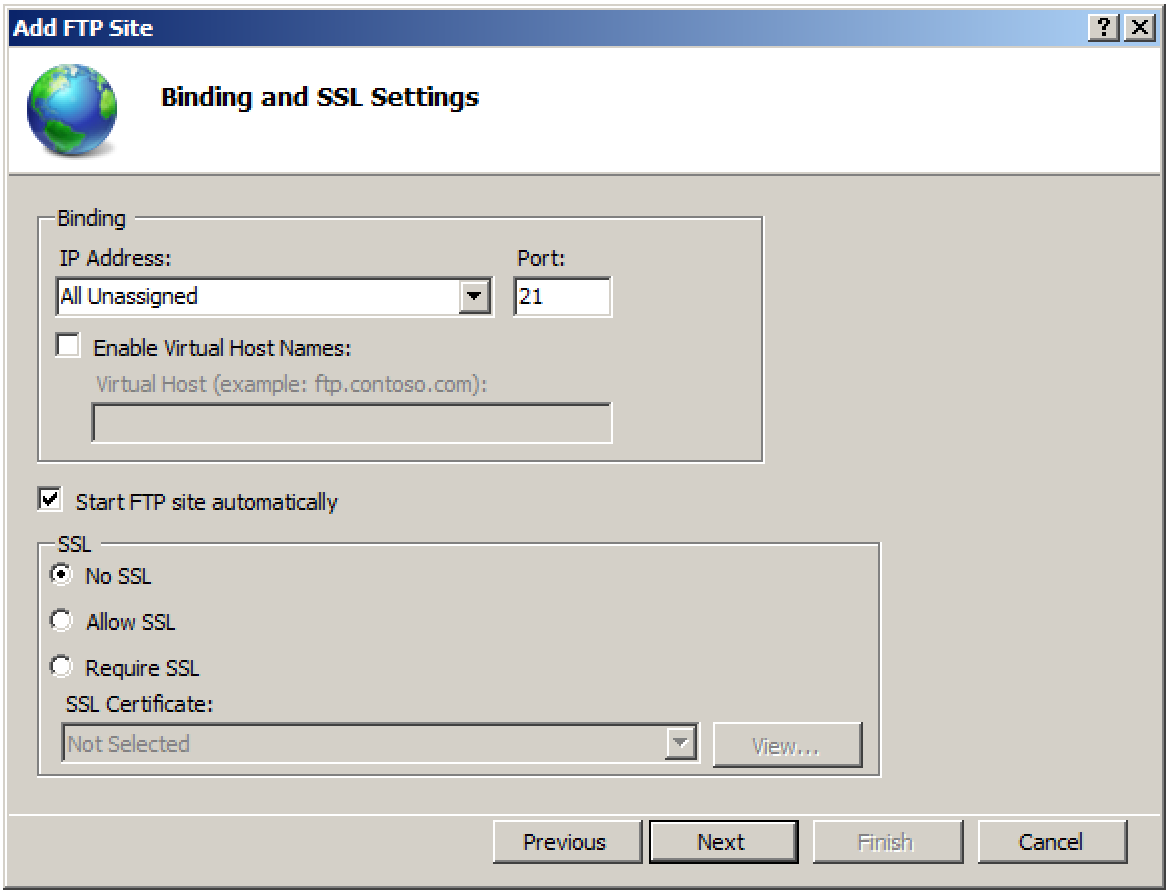
FTP site name: Data_Exchange

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 option "None".



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

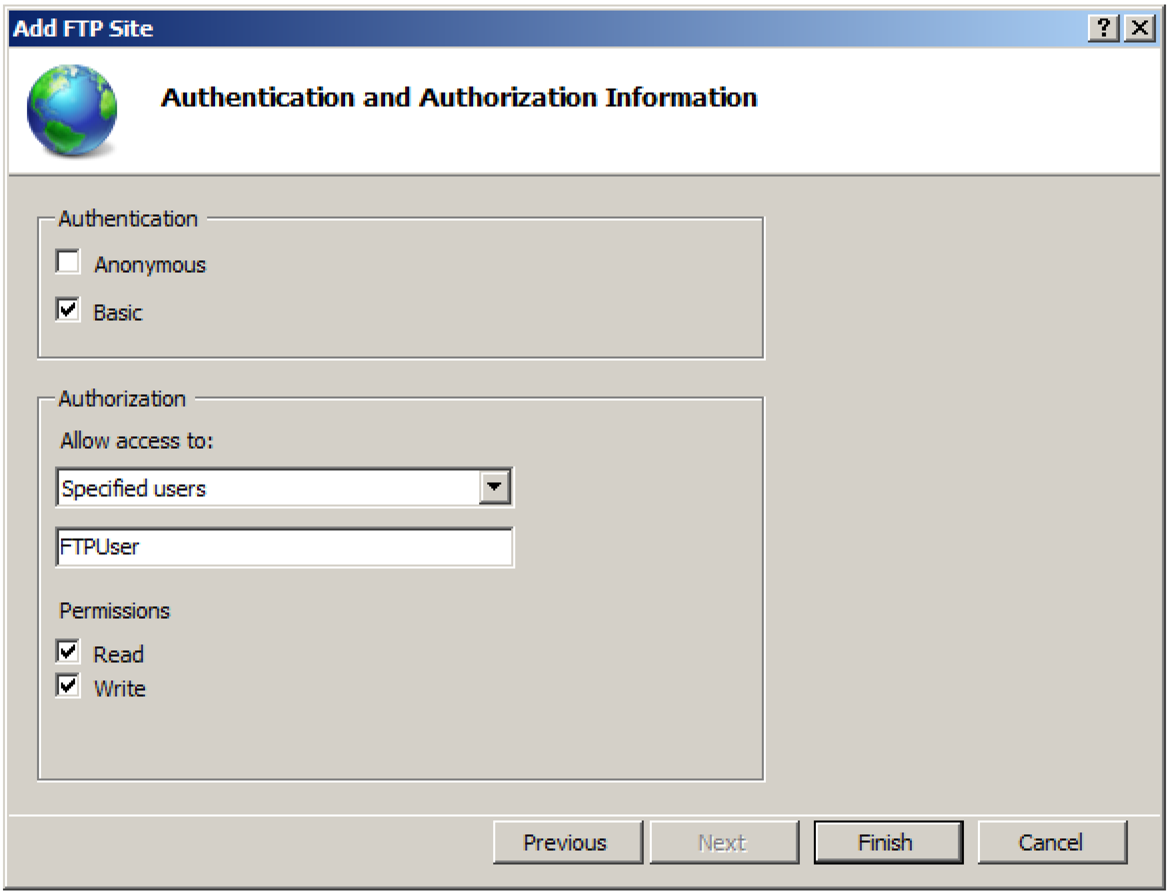
○ Allow SSL

○ Require SSL

SSL Certificate: Not Selected

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

9. Make the following settings in the "Authentication and Authorization Information" dialog:
   - "Authorization > Access allowed for" area: Select the entry "Specific users" from the drop-down list and enter the authorized users in the box below.
   - "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.

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. This is why this station must be integrated and included in the patch management and virus protection concept of the system. In other words, the quarantine station must regularly receive the latest Windows updates. The WSUS server, which is also located in the Perimeter network, can serve as update source. In addition, a current virus scanner must be installed on the quarantine station. The station receives current virus definitions via the virus scanner server, which is also located in the Perimeter network. Whitelisting is an additional protection that should also be implemented at the quarantine station (see the corresponding sections of this document).

3.7 Configuration of the SCALANCE X network components

It is especially important to observe the following points when configuring the network components (e.g. Ethernet switches):

- Disabling non-required ports
- Changing the preconfigured default password
- Disabling non-required protocols

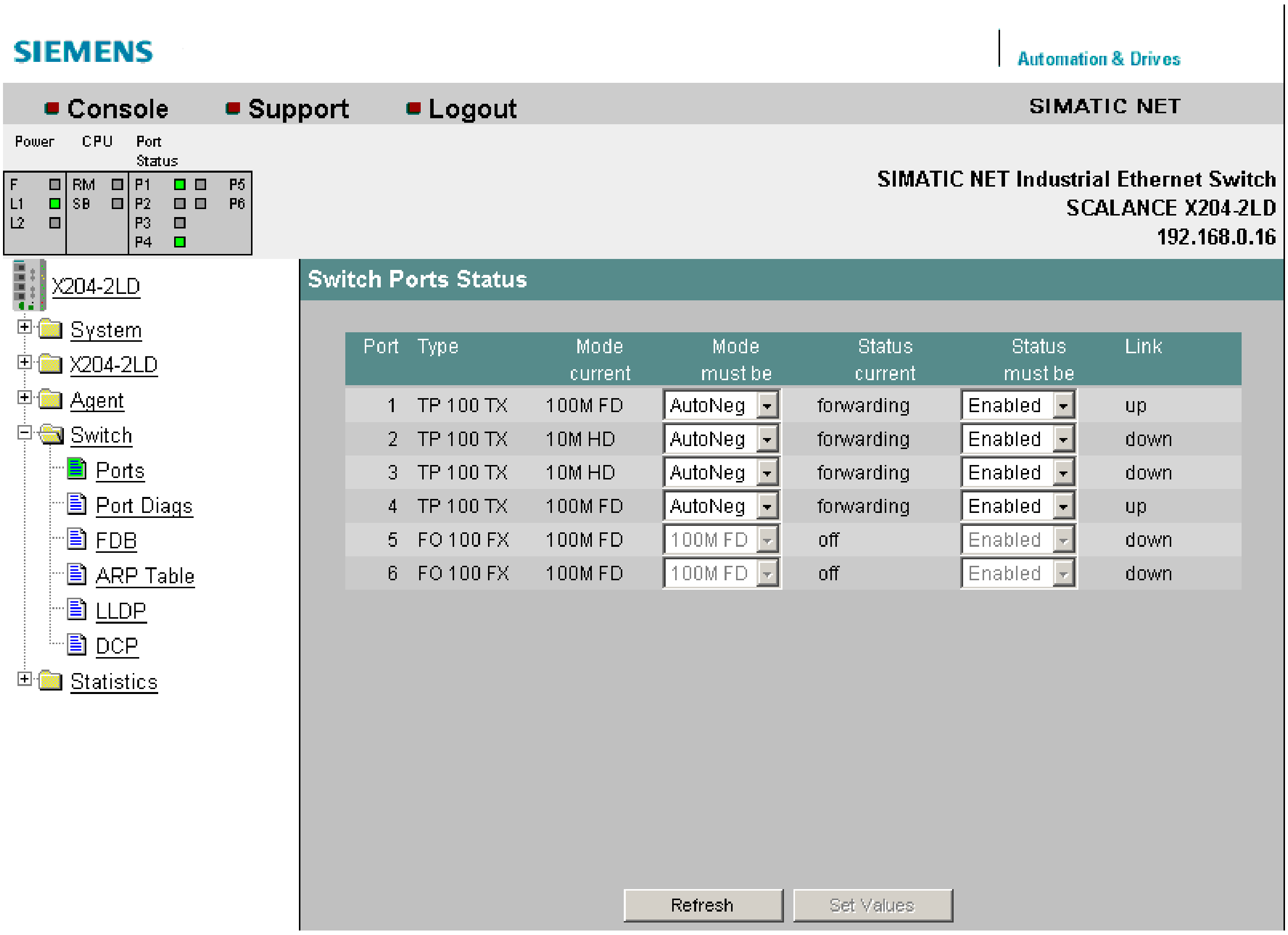
Note

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

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

Disabling non-required ports

Unused ports (ports of the Ethernet switch) that are not required and to which no terminal devices are connected must be disabled. To do this, go to the "Switch Ports" WBM menu and disable the non-required ports in this window.



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 auto-negotiation is enabled or disabled.
- Status: Indicates that the port is switched on.
- Link: Indicates the connection status to the network.

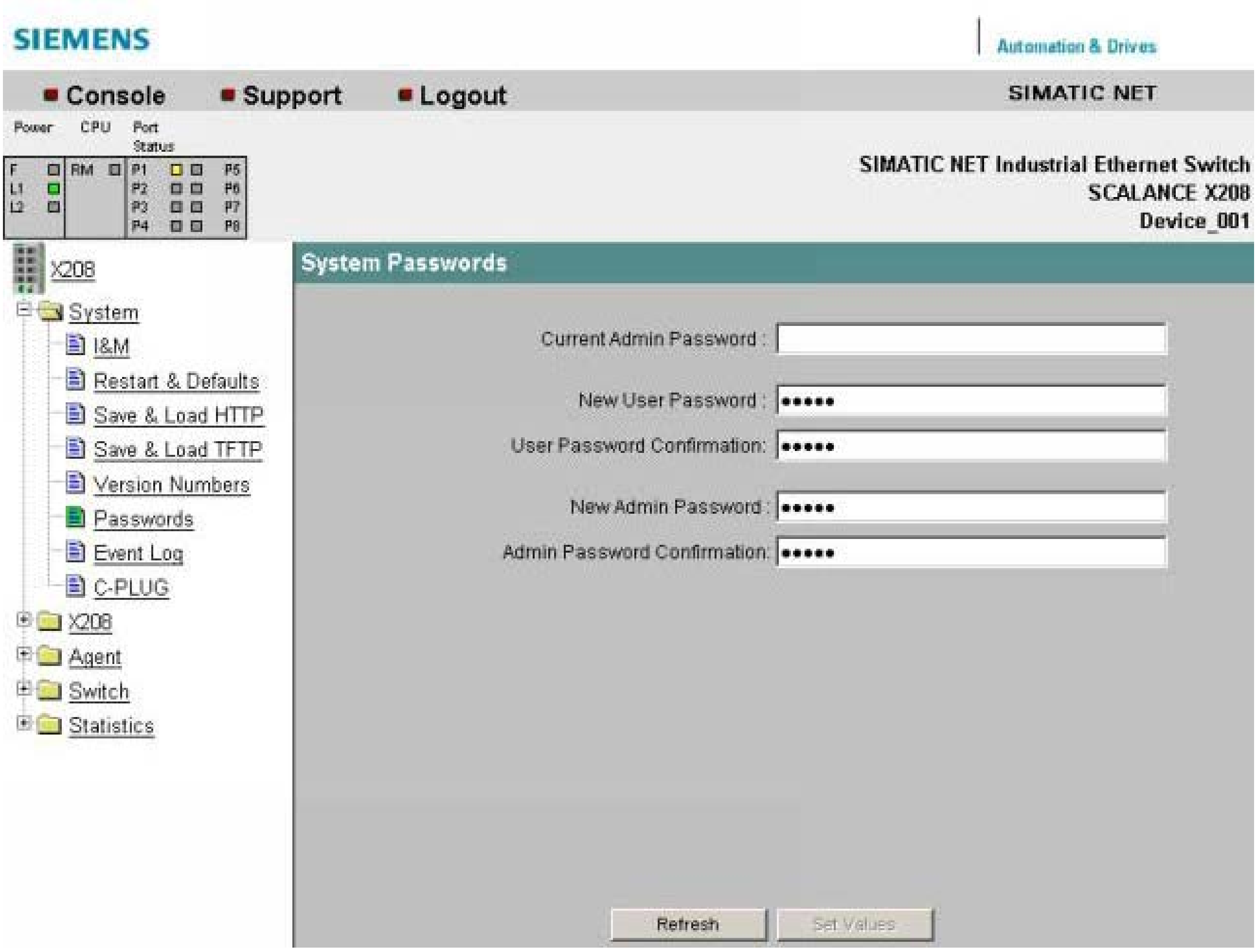
If a port is not used, the status of this port must be set to "Disabled".

System passwords

Change passwords for the users "Admin" and "User" in the "System Passwords" dialog. 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.



System Passwords

Current Admin Password :

New User Password : •••••

User Password Confirmation: •••••

New Admin Password : •••••

Admin Password Confirmation: •••••

Disabling non-required protocols

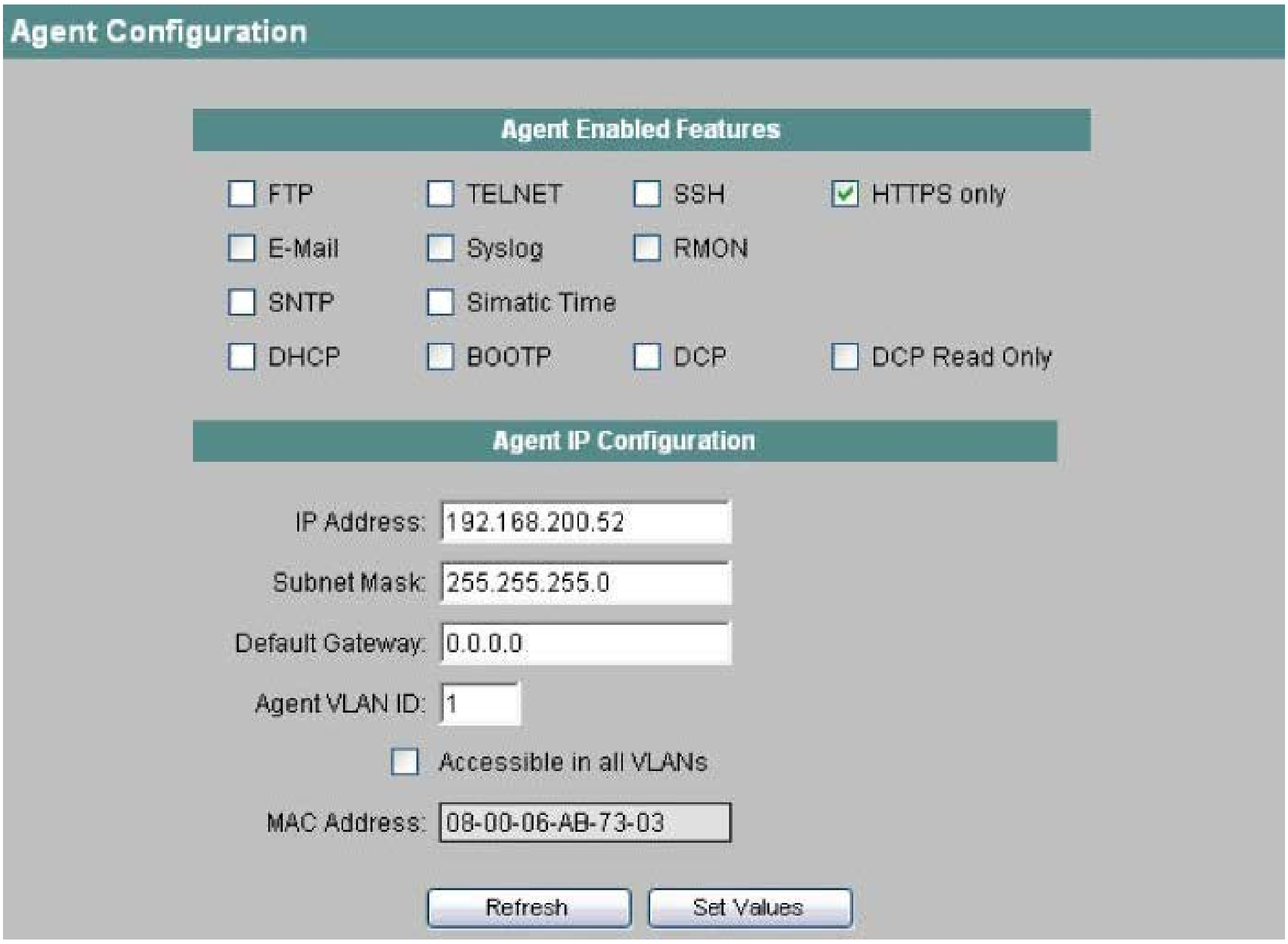
The access options to the IE switch are specified in the "Agent Configuration" dialog, which can be accessed via the "Agent" folder icon. Furthermore, the network configuration for the IE switch can be defined here.

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 31), subsection "DHCP (Dynamic Host Configuration Protocol)".

Specifying protocols

We recommend that you only specify the "HTTPS" protocol for accessing 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.



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: 192.168.200.52
Subnet Mask: 255.255.255.0
Default Gateway: 0.0.0.0
Agent VLAN ID: 1
□ Accessible in all VLANs
MAC Address: 08-00-06-AB-73-03

Additional information

You will find more information in the following manuals:

- SIMATIC NET Industrial Ethernet Switches SCALANCE X-400 (http://support.automation.siemens.com/WW/view/en/19625108)
- SIMATIC NET Industrial Ethernet Switches SCALANCE X-300 (http://support.automation.siemens.com/WW/view/en/67480000)
- SIMATIC NET Industrial Ethernet Switches SCALANCE X-200 Configuration Manual (http://support.automation.siemens.com/WW/view/en/63203259)
- SIMATIC NET Industrial Ethernet Switches SCALANCE X-200 Operating Instructions (http://support.automation.siemens.com/WW/view/en/63203773)

Support for realizing and implementing network security in your plant is available from the Industrial Security Services. You can find additional information and the corresponding contacts at http://www.industry.siemens.com/topics/global/en/industrial-security/services/Pages/Default.aspx.

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

System hardening 4

4.1 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
- Restrictive user management is implemented
- The local Windows Firewall is enabled and it is restrictively configured

4.2 Installing the operating system

Introduction

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

Note

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

- PCS 7 Readme (http://support.automation.siemens.com/WW/view/en/66807356)
- Manual "SIMATIC Process Control System PCS 7 PC Configuration and Authorization" (http://support.automation.siemens.com/WW/view/en/68157327)

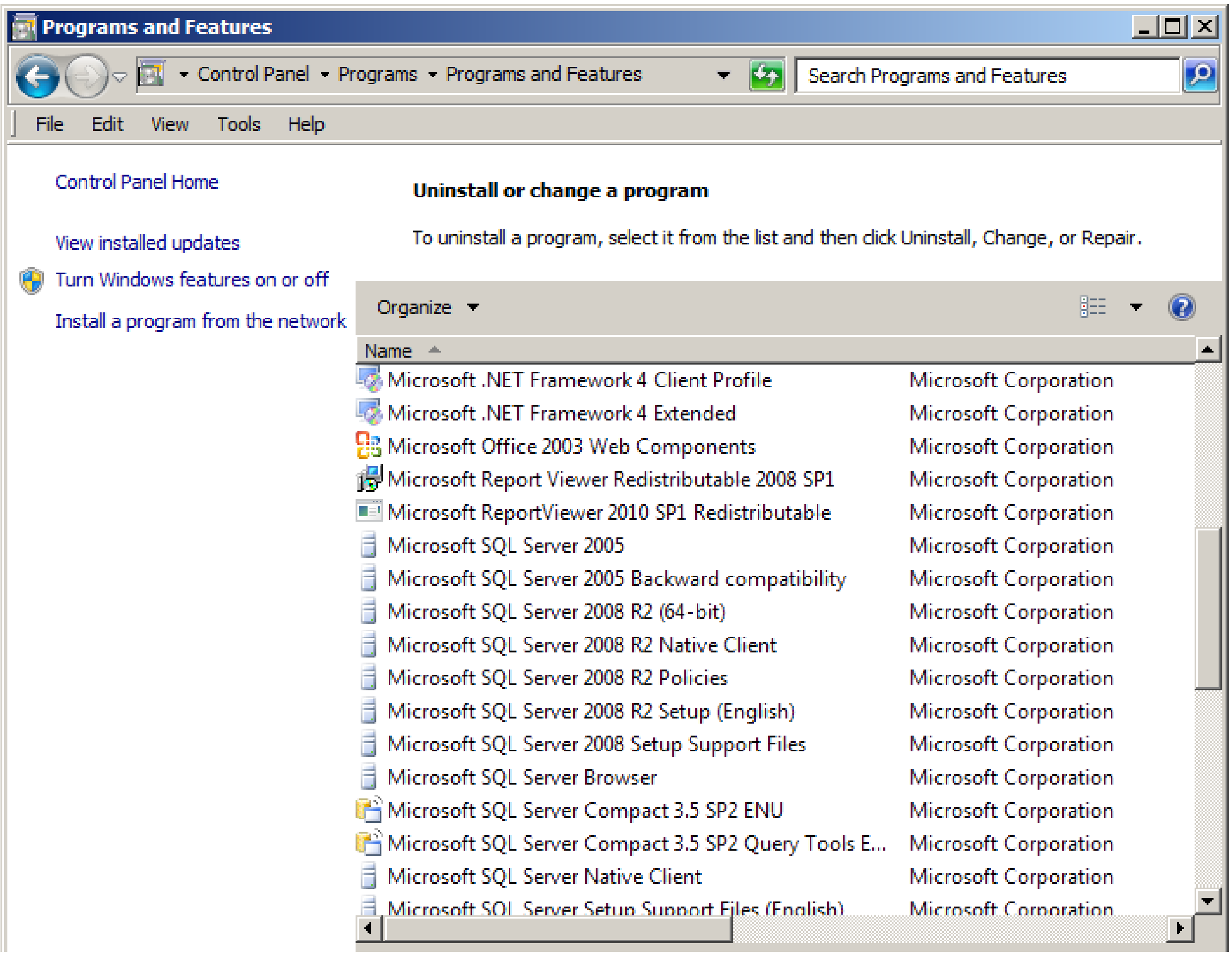
For a SIMATIC PCS 7 computer that fulfills a specific function in an automation plant (OS server, OS client, engineering station, etc.), some programs installed during the installation of the operating system may not be required. These programs should be removed. In most cases, this involves "Windows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

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.



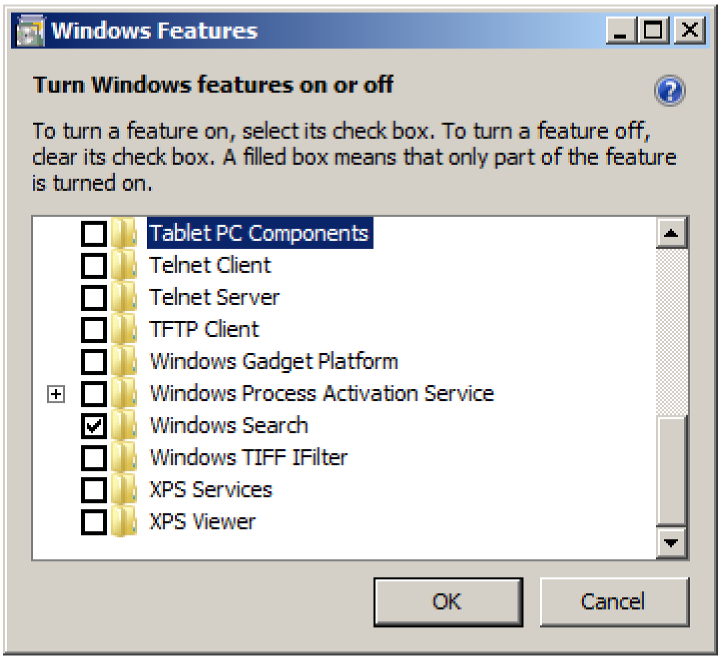
Programs and Features
Control Panel ▸ Programs ▸ Programs and Features
Search Programs and Features
File Edit View Tools Help
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Organize ▾

Uninstall or change a program

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

Name	
Microsoft .NET Framework 4 Client Profile	Microsoft Corporation
Microsoft .NET Framework 4 Extended	Microsoft Corporation
Microsoft Office 2003 Web Components	Microsoft Corporation
Microsoft Report Viewer Redistributable 2008 SP1	Microsoft Corporation
Microsoft ReportViewer 2010 SP1 Redistributable	Microsoft Corporation
Microsoft SQL Server 2005	Microsoft Corporation
Microsoft SQL Server 2005 Backward compatibility	Microsoft Corporation
Microsoft SQL Server 2008 R2 (64-bit)	Microsoft Corporation
Microsoft SQL Server 2008 R2 Native Client	Microsoft Corporation
Microsoft SQL Server 2008 R2 Policies	Microsoft Corporation
Microsoft SQL Server 2008 R2 Setup (English)	Microsoft Corporation
Microsoft SQL Server 2008 Setup Support Files	Microsoft Corporation
Microsoft SQL Server Browser	Microsoft Corporation
Microsoft SQL Server Compact 3.5 SP2 ENU	Microsoft Corporation
Microsoft SQL Server Compact 3.5 SP2 Query Tools E...	Microsoft Corporation
Microsoft SQL Server Native Client	Microsoft Corporation
Microsoft SQL Server Setup Support Files (English)	Microsoft Corporation

2. Click "Turn Windows features on or off" 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".

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.

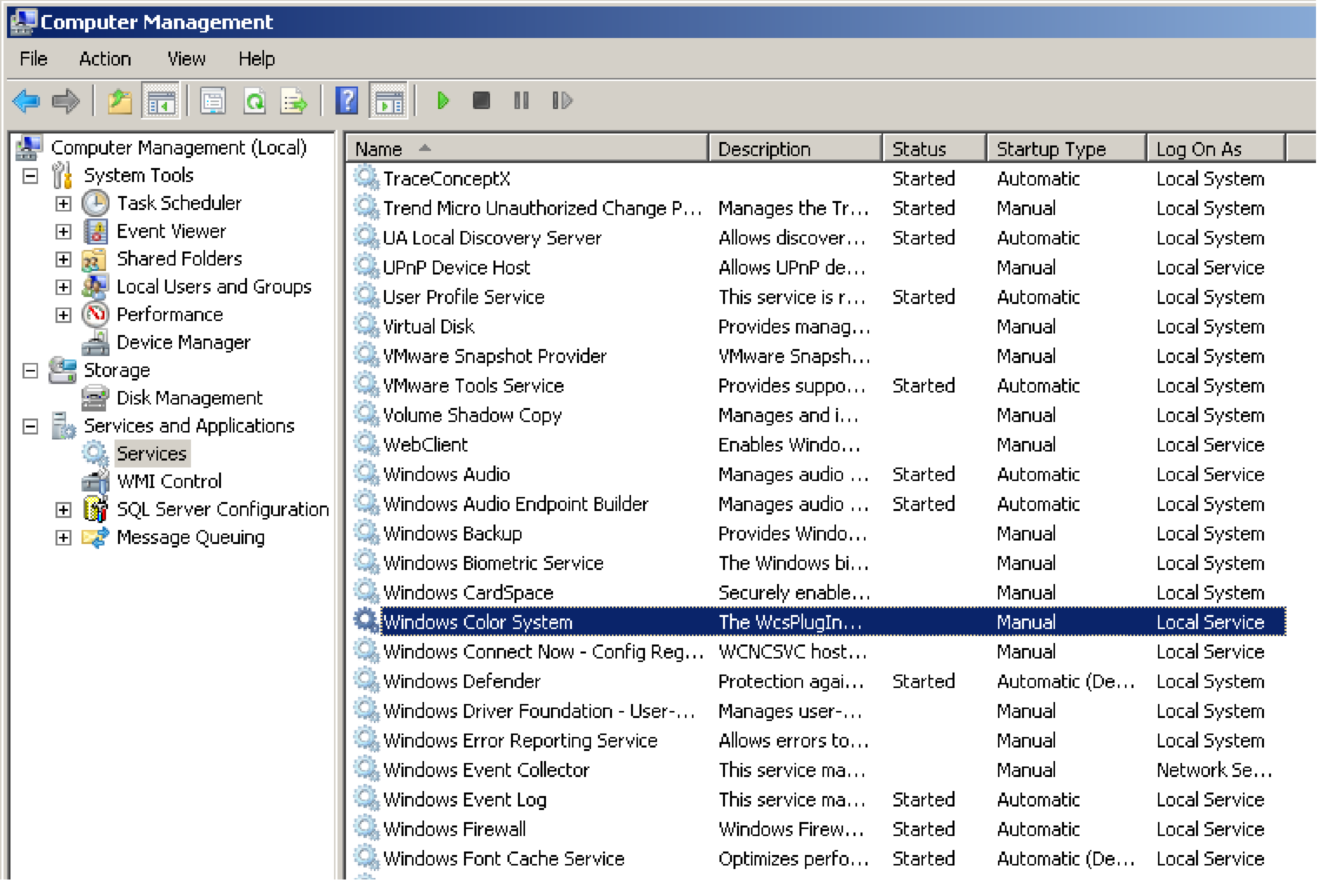
The following services can be disabled:

Service	Operating system
Certificate Propagation	Windows 7, Windows Server 2008 R2
Diagnostic Policy Service	Windows 7, Windows Server 2008 R2
Diagnostic Service Host	Windows 7, Windows Server 2008 R2
Windows Color System	Windows 7, Windows Server 2008 R2
Windows Connect Now - Config Registrar	Windows 7
Performance Logs and Alerts	All
Windows Presentation Foundation Font Cache	All
Help and Support	Windows XP, Windows Server 2003 R2
Wireless Zero Configuration	Windows XP, Windows Server 2003 R2
Terminal Services Session Directory	Windows Server 2003 R2

Procedure

To disable a service, 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" or "Automatic", or if the service has not been started, "Disabled".

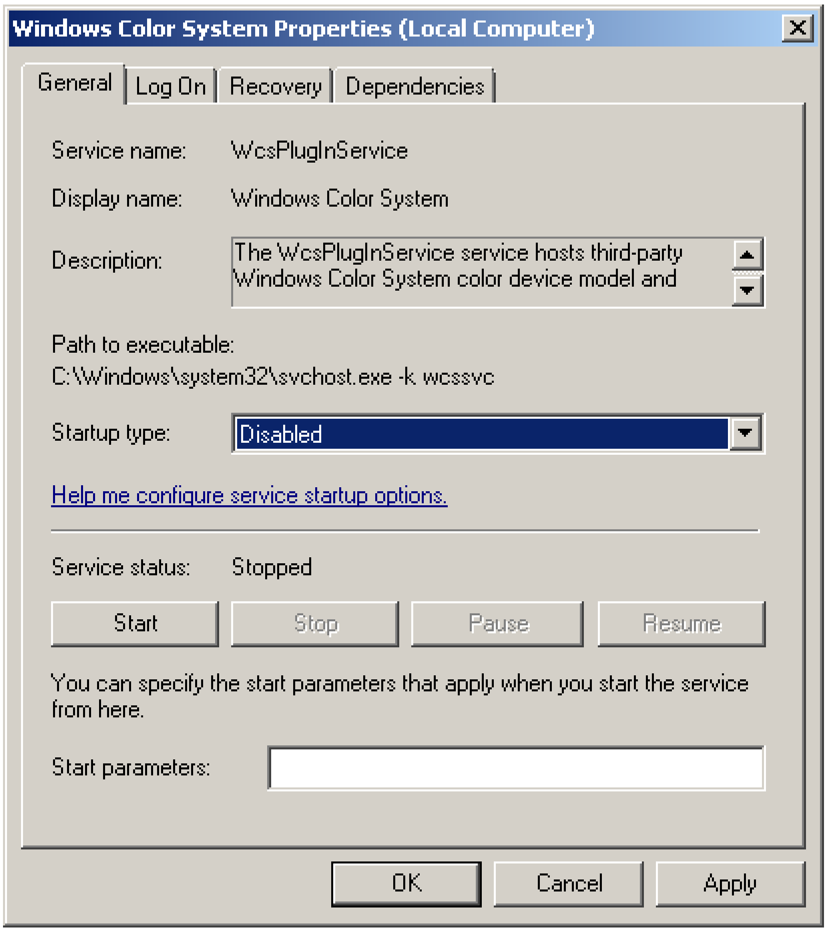


Computer Management (Local)
- System Tools
  - Task Scheduler
  - Event Viewer
  - Shared Folders
  - Local Users and Groups
  - Performance
  - Device Manager
- Storage
  - Disk Management
- Services and Applications
  - Services
  - WMI Control
  - SQL Server Configuration
  - Message Queuing

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:

4.3 Security Controller

The Security Controller (PCS 7 V8.0 or higher) or the SIMATIC Security Control (<PCS 7 V8.0) is a program that makes application-specific security settings. Security Controller (SC) or SIMATIC Security Control (SSC) is integrated by default in SIMATIC PCS 7 and SIMATIC WinCC.

The option enabling SC to automatically perform the settings must be explicitly confirmed when the program is 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 plant configuration or changing the roles of users, be aware that the local firewall configuration or the local group memberships must be adapted accordingly.

The Security Controller makes the following settings automatically:

- Group Settings (User Management – SIMATIC Logon)
- Registry settings
- Windows Firewall exceptions
- DCOM settings
- File and/or Directory Permissions

These settings are performed depending on the installation (PCS 7 OS Server, PCS 7 OS Client, ES, etc.) and for 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

Detailed information on this is also available in the manual "SIMATIC Process Control System PCS 7 PC Configuration and Authorization" (http://support.automation.siemens.com/WW/view/en/68157327).

4.4 Windows Firewall

Introduction

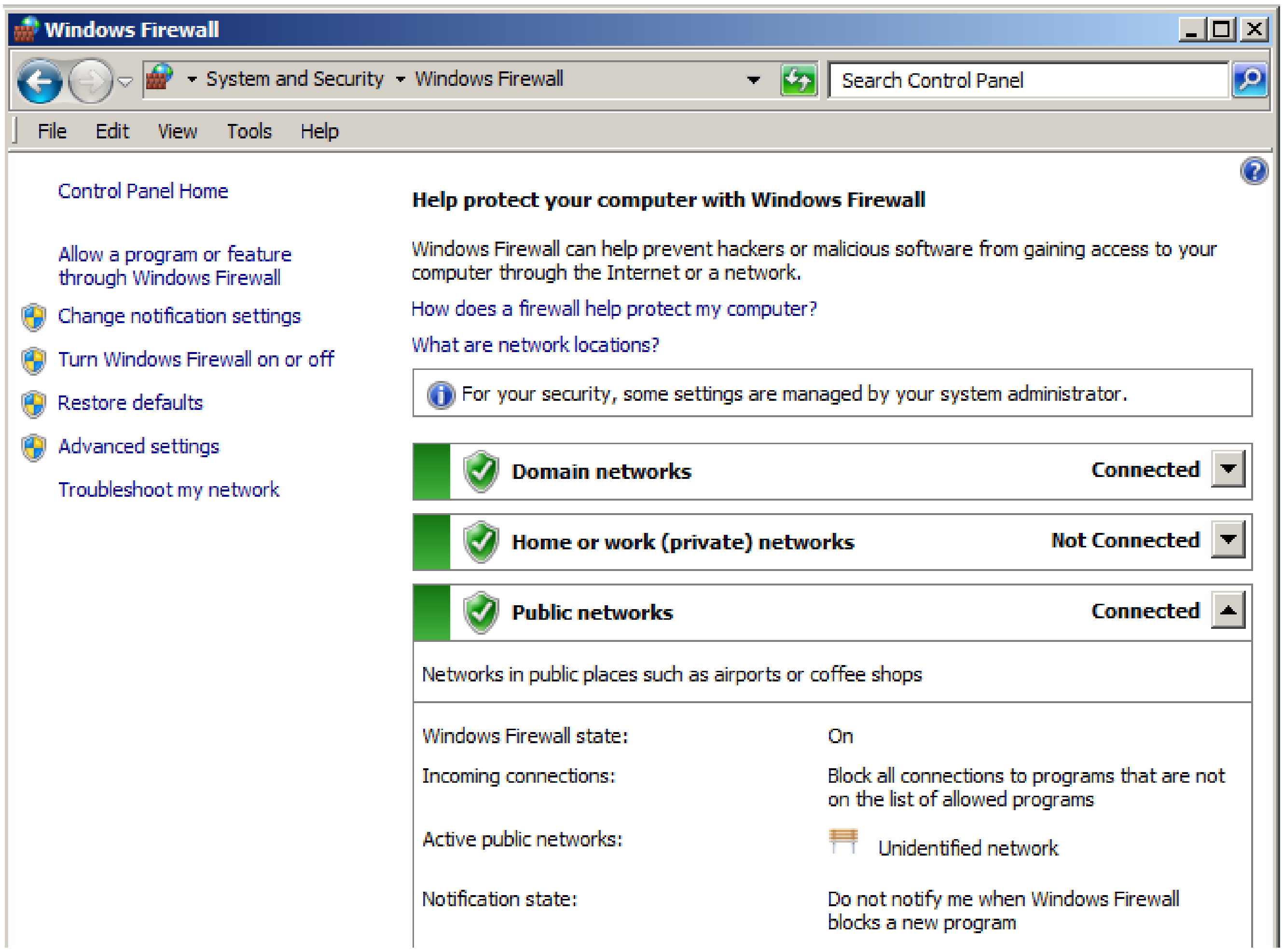
As described in the "Security Controller" (Page 66) section, Security Controller (as of PCS 7 V8.0) or SIMATIC Security Control (<PCS 7 V8.0) makes setting relating to the Windows Firewall. With respect to the example configuration in which communication of PCS 7 computers must be guaranteed among various subnets, the Windows Firewall needs to be manually adapted.

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 in the Windows Firewall or in the firewall rules:

1. Select the command "Start > Control Panel > System and Security > Windows Firewall":
   The "Windows Firewall" dialog opens.



Windows Firewall

System and Security ▸ Windows Firewall

Search Control Panel

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?

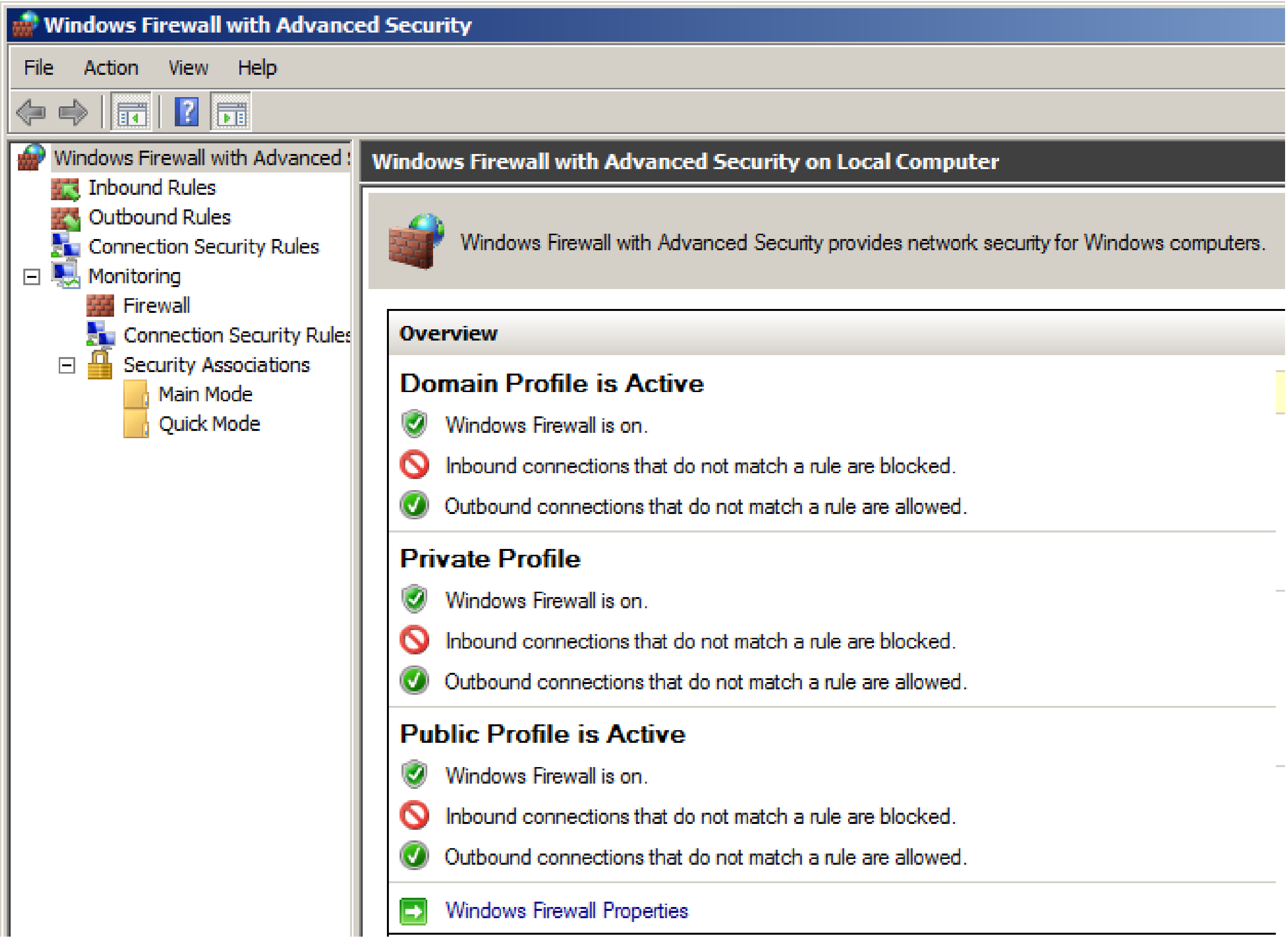
For your security, some settings are managed by your system administrator.

Domain networks	**Connected**
Home or work (private) networks	**Not Connected**
Public networks	**Connected**

Networks in public places such as airports or coffee shops

Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active public networks:	Unidentified network
Notification state:	Do not notify me when Windows Firewall blocks a new program

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 :
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
Overview
Windows Firewall Properties

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

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.

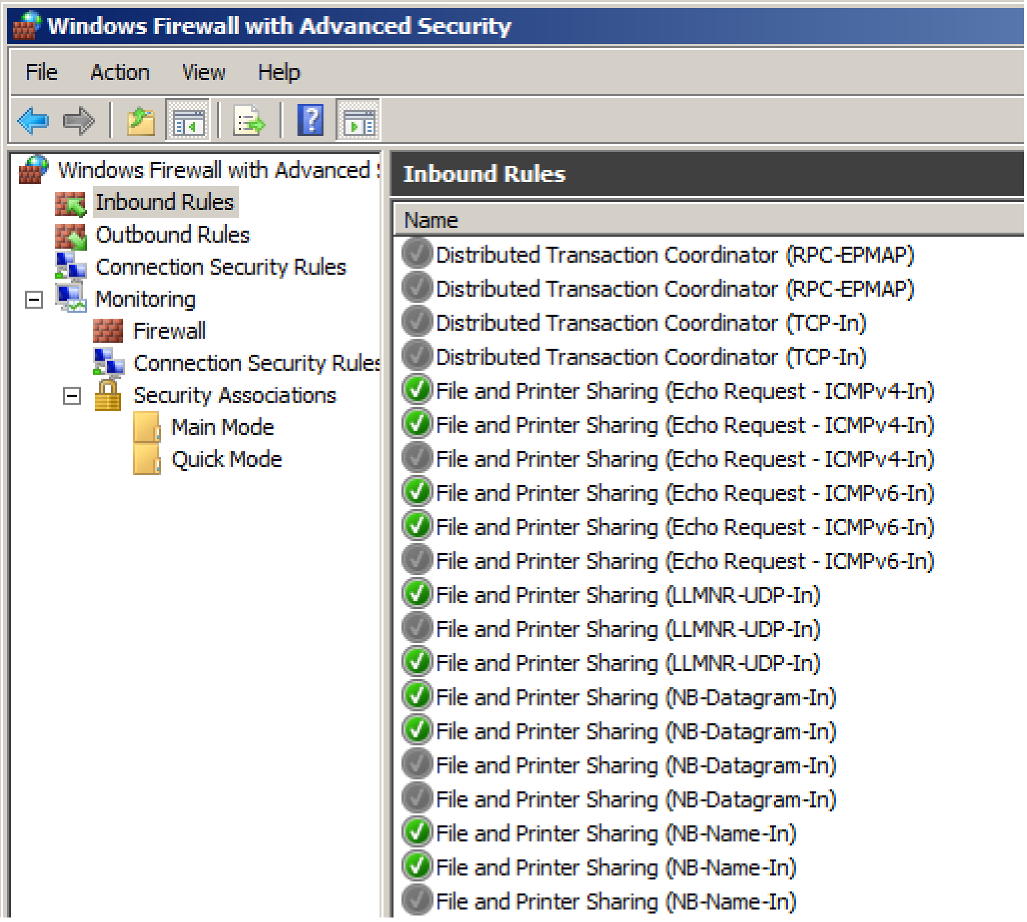
Public Profile is Active

✓ Windows Firewall is on.

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

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

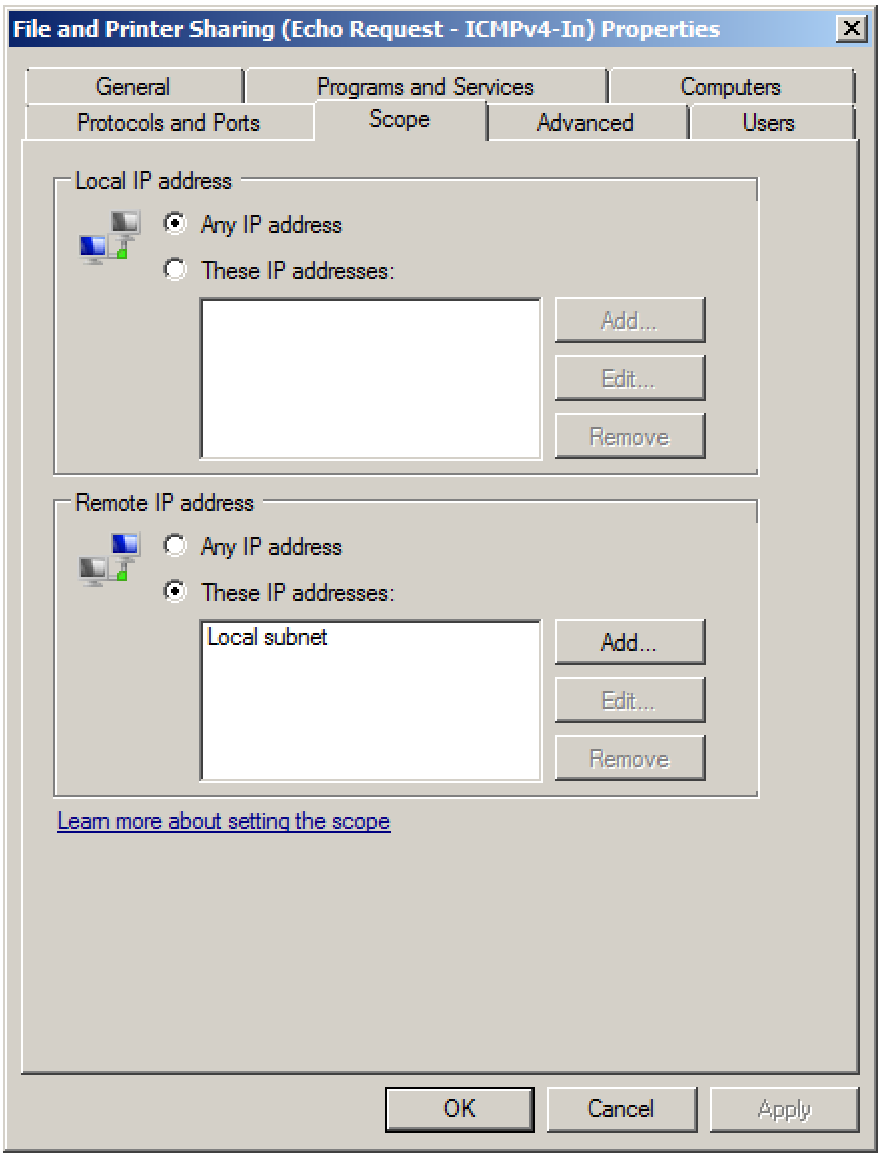
3. In the left navigation pane, click "Inbound Rules".
   The "Inbound Rules" are displayed.


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
○ 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 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 with computers in a different subnet is thus blocked.

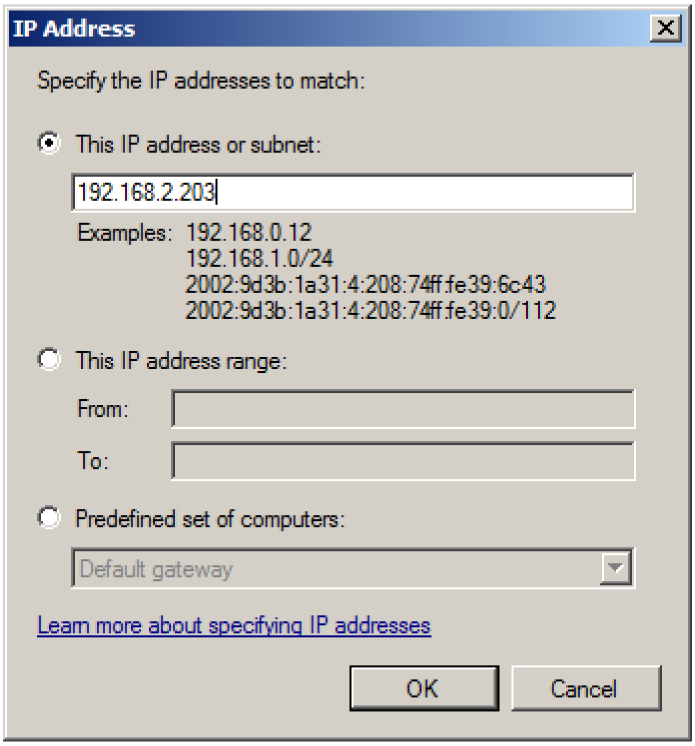


File and Printer Sharing (Echo Request - ICMPv4-In) Properties

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:

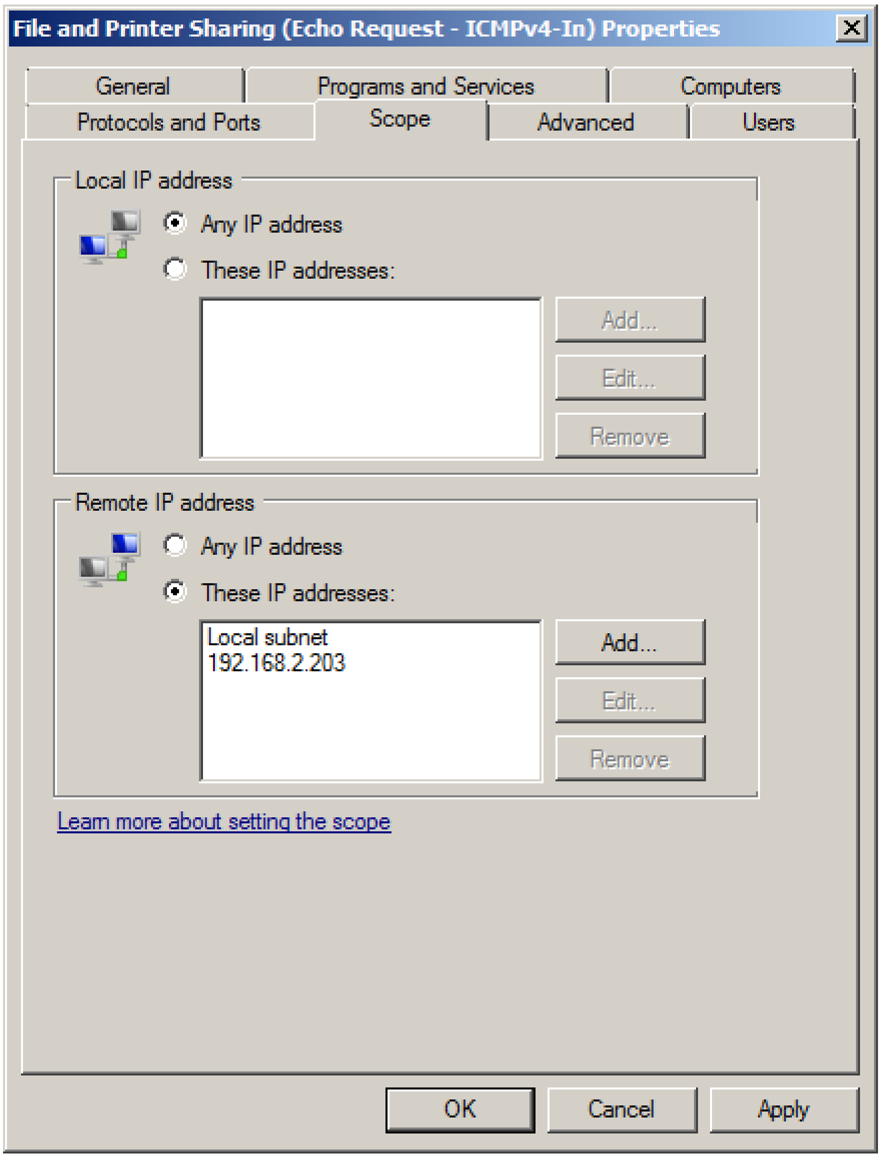
To:

○ Predefined set of computers:

Default gateway

Learn more about specifying IP addresses

7. Select the option "This IP address or subnet:" and enter the "IP address" of the communication partner. If 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:

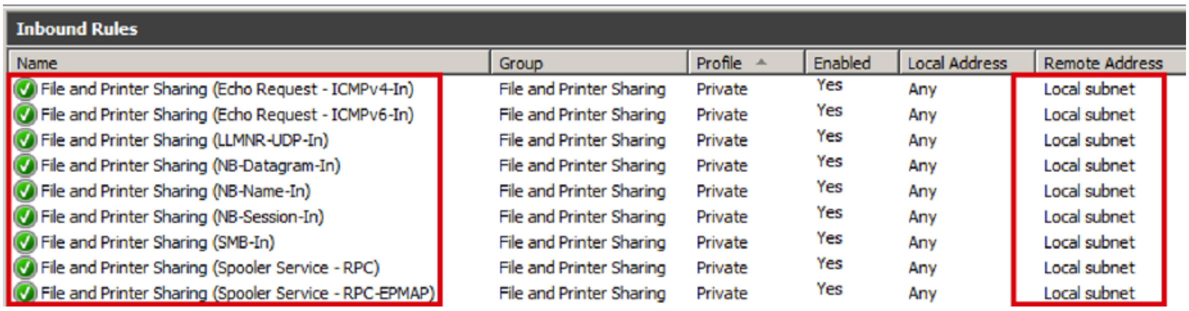
Remote IP address

○ 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 accordingly.



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

4.5 BIOS settings

The following BIOS settings should be performed on each computer in your plant:

- The access to the BIOS must be protected with a password. The password must be set by an administrator and handled as confidential.
- The boot sequence of the computer must be set in the BIOS in such a way that it boots from the hard drive. This means that the hard drive must be set as the first boot medium. This will make it more difficult to boot from other media, such as CD or USB.
- The startup order of the various media of the computer must be set in the BIOS in such a way that the hard disk is started first. This will make it more difficult to boot from other media, such as CD or USB.
- The USB ports must be disabled, unless they are required for peripheral devices, such as mouse or keyboard.

Note

The settings for a specific computer depend on the installed BIOS (for example, the manufacturer or version). The specific options of the setting can be found in the corresponding system description.

4.6 Working with mobile data media

4.6.1 Overview

Introduction

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.).

Definition of USB storage media

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

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.

Restricting user accesses to USB ports

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

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. This is why it is usually not practical to use a "USB Lock" or to disable the interface by other mechanical means. The use of interfaces should therefore be regulated by assigning appropriate rights on the operating system level or with the help of additional programs.

Working with USB ports

In addition to the BIOS settings for disabling the USB port (see section "Auto-Hotspot"), unwanted access can also be restricted using Windows settings. Blocking the USB ports via the BIOS settings or the hardware profile can prohibit unauthorized use of USB storage media.

Restricting access to USB storage media using Windows

The following describes various procedures that show how Windows resources can be used to prevent or restrict access to USB storage media:

- Restricting access to USB storage media using Windows XP or Windows Server 2003 on-board resources
  - When no USB storage medium has been installed
  - When a USB storage medium has been installed
- Blocking access to USB storage media using group policy in Windows 7 and Windows Server 2008
- Regulating the use of USB storage media using group policy in Windows 7 and Windows Server 2008
- Disabling the Autoplay function using group policy in Windows 7 and Windows Server 2008
- Disabling all Autorun functions using group policy in Windows 7 and Windows Server 2008
- Disabling the Autoplay function using group policy in Windows XP and Windows Server 2003

4.6.2 Restricting access using Windows XP or Windows Server 2003 on-board tools

Two procedures are available to prevent a user from establishing a connection to a USB storage medium:

- When no USB storage medium has been installed on the computer
- When a USB storage medium has been installed on the computer

Restriction when no USB storage medium has been installed on the computer

Source: http://support.microsoft.com/kb/823732/en

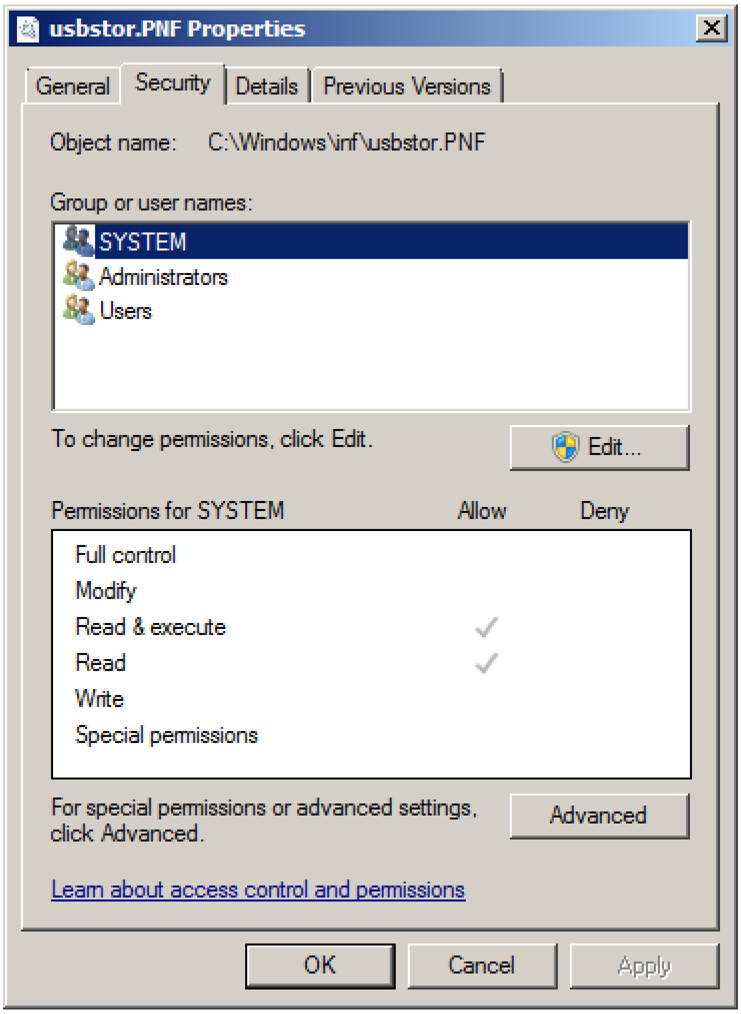
When no USB storage medium has been installed on the computer yet, assign the user or group and the local system account access restrictions for the following files:

- %SystemRoot%\Inf\Usbstor.pnf
- %SystemRoot%\Inf\Usbstor.inf

Afterwards, users can no longer install any USB storage medium on the computer. Proceed as follows to assign access restrictions to a user or group for the files Usbstor.pnf and Usbstor.inf:

1. Open the Windows Explorer and search for the folder "%SystemRoot%\Inf".
2. Right-click on the "Usbstor.pnf" file and then click "Properties".

3. Click on the "Security" tab.



Object name: C:\Windows\inf\usbstor.PNF

Group or user names:

- SYSTEM
- Administrators
- Users

To change permissions, click Edit.

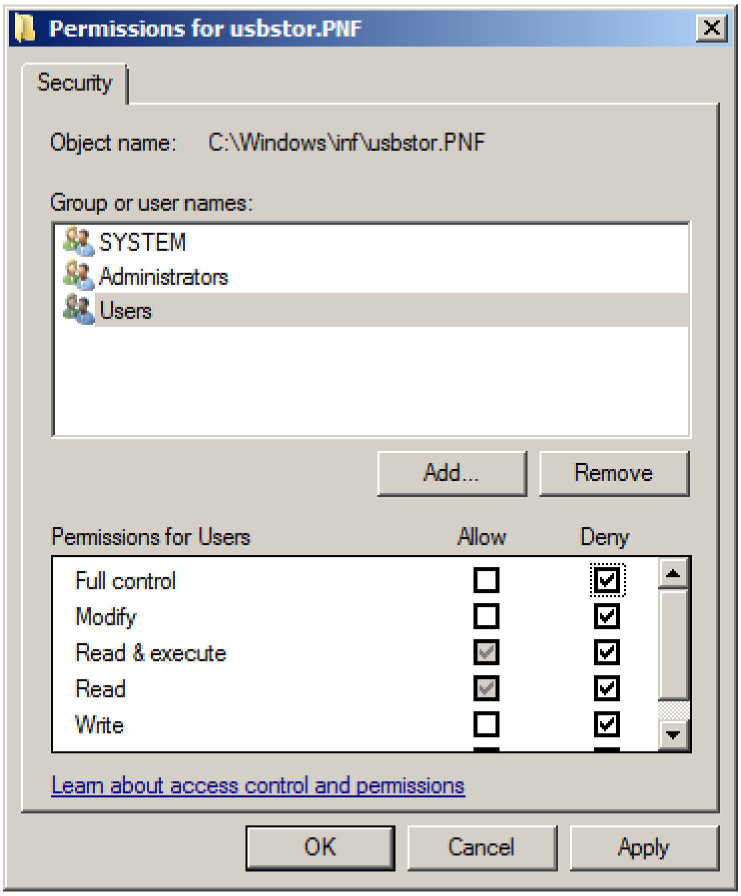
Permissions for SYSTEM	Allow	Deny
Full control		
Modify		
Read & execute	✓	
Read	✓	
Write		
Special permissions		

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

4. Add the user or group for whom you want to define access restrictions to the list Group or user names.

5. In the "Permissions for user or group names" list, select the "Deny" check box next to "Full Control".


Permissions for usbstor.PNF
Security
Add...
Remove
Learn about access control and permissions
OK
Cancel
Apply

Object name: C:\Windows\inf\usbstor.PNF

Group or user names:

- SYSTEM
- Administrators
- Users

Permissions for Users	Allow	Deny
Full control	□	☑
Modify	□	☑
Read & execute	☑	☑
Read	☑	☑
Write	□	☑

6. In addition, add the system account to the Deny list. To do this, select the "SYSTEM" account in the "Group or user names" list and enable the "Deny" check box next to "Full Control" in the "Permissions for SYSTEM". Then click "OK".

7. Repeat steps 1 - 6 for the "Usbstor.inf" file.

Restriction when a USB storage medium has been installed on the computer

Source: http://support.microsoft.com/kb/823732/en

NOTICE
Editing the registry
This section or the method or task description contains notes about editing the registry. An incorrect editing of the registry can lead to fatal problems. For this reason, it is important to exercise caution when executing the following steps. As a protective measure, you should create a backup copy before editing the registry. This ensures that you can restore the registry if a problem occurs.

When a USB storage medium is already installed on the computer, you can change the registry to ensure that the device is non-operational when the user connects it to the computer.

When a USB storage device is already installed on the computer, set the "Start" value in the following registry key to a value of 4:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor`

As a result, the USB storage medium will not work when the user connects the device to the computer.

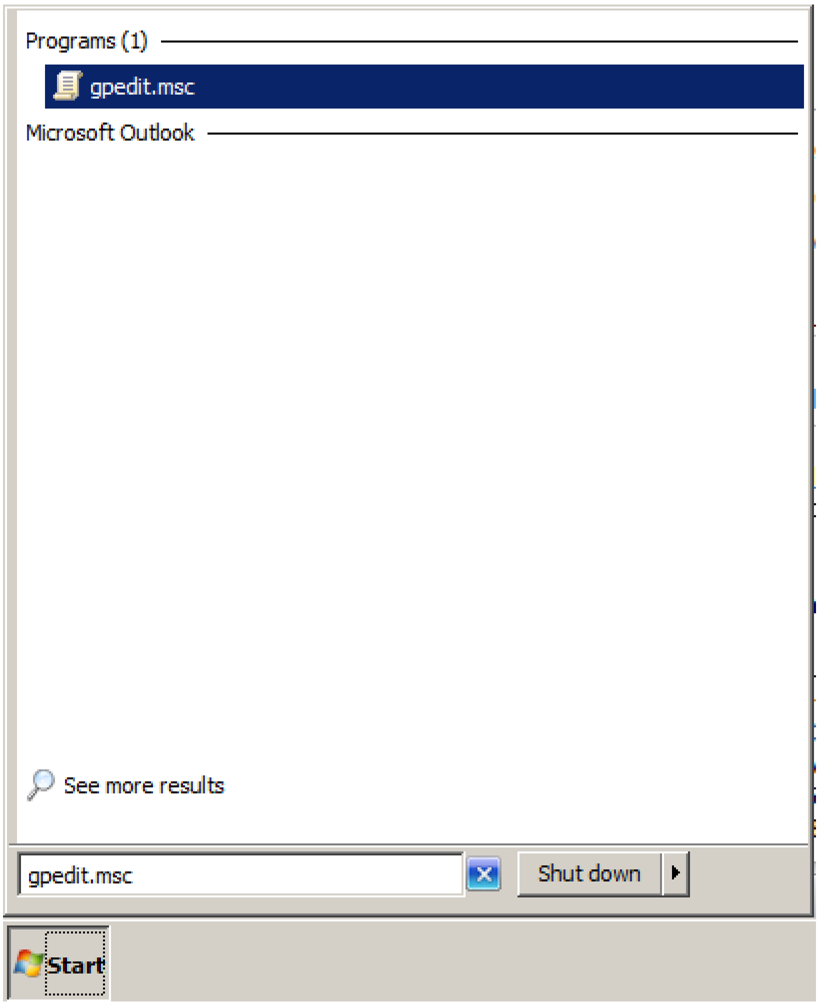
Follow these steps to set the "Start" value:

1. Click "Start" and then "Run".
2. In the "Run" box, enter the string "regedit" and click on OK.
3. Click on the following registry key:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor`
4. In the detail view, double-click "Start".
5. In the "Value data" box, enter the value 4, click on Hexadecimal (if this option is not already selected), and then click on OK.
6. Exit the registry editor.

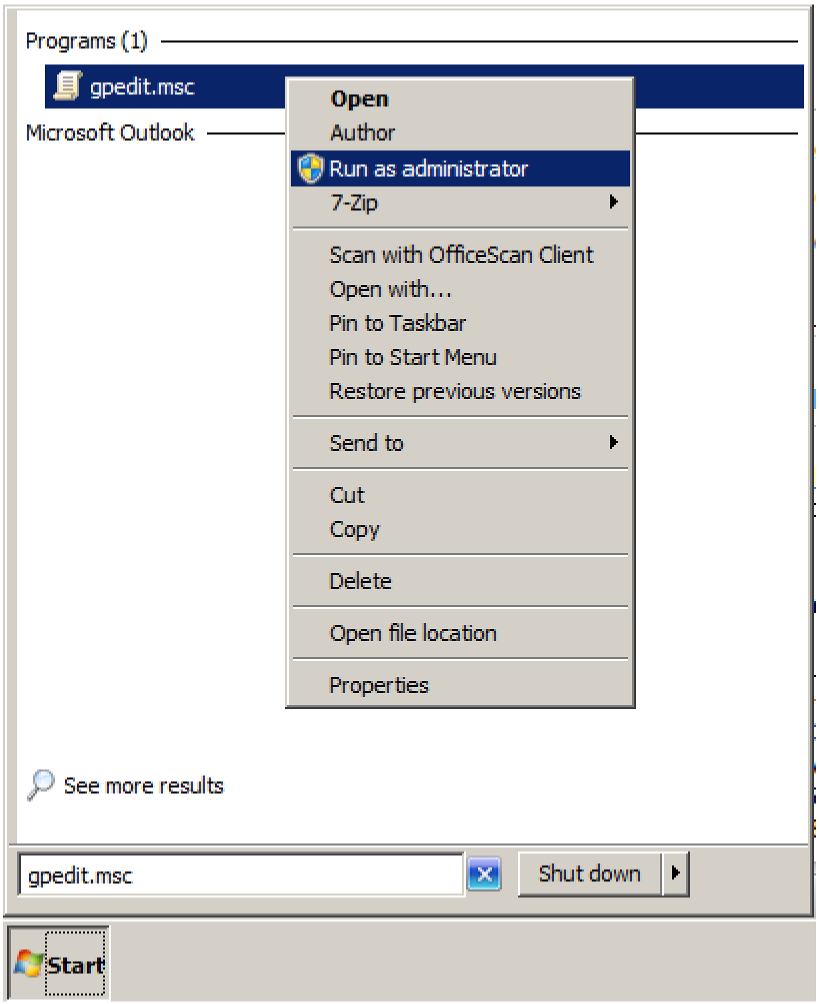
4.6.3 Blocking access to USB storage media using group policy in Windows 7 and Windows Server 2008

Procedure

1. Click "Start" and enter the string "gpedit.msc" in the "Search" box.



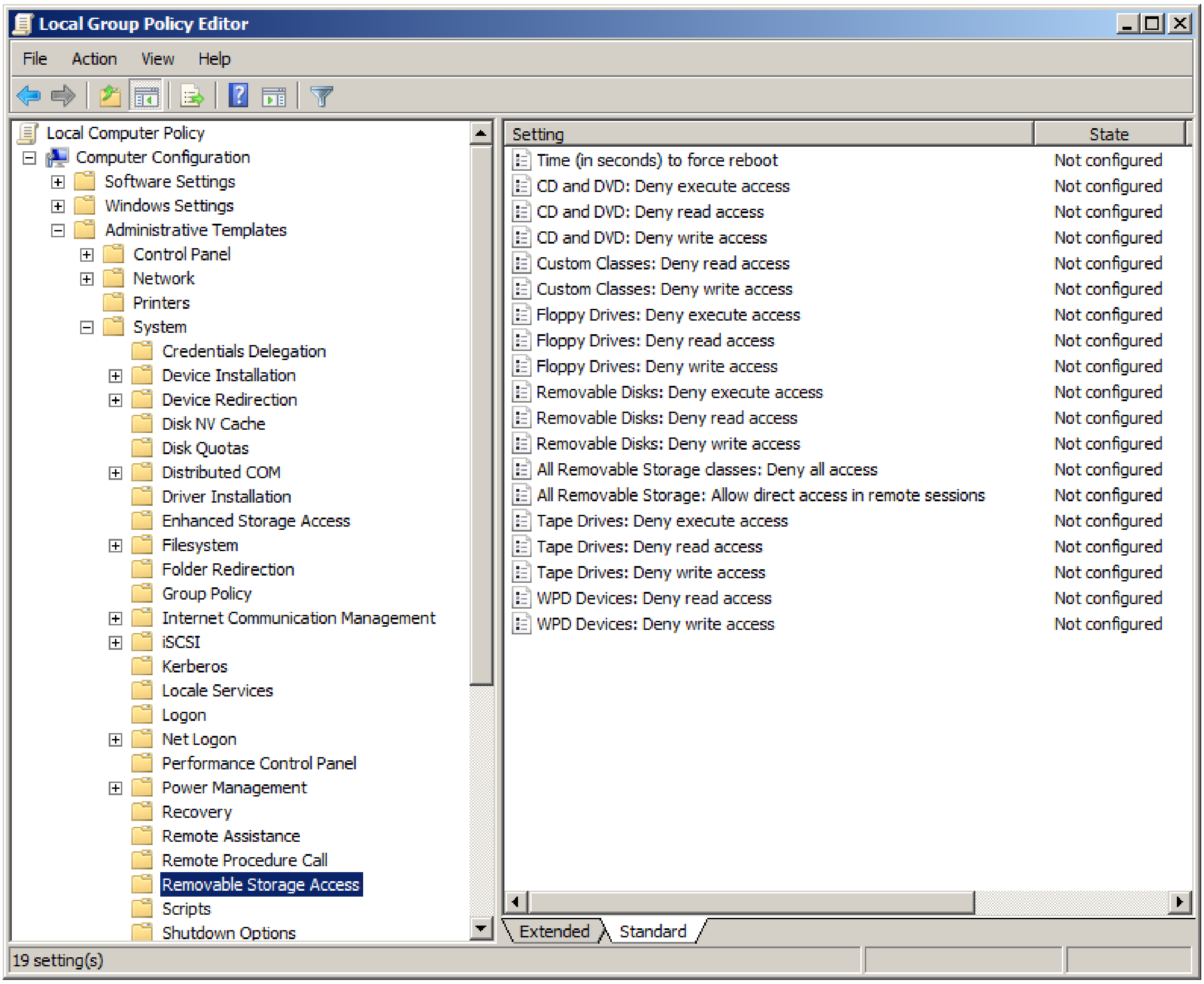
2. Start the group policy editor as an administrator.



This action requires administrator rights. For this reason, log in as administrator or start the group policy editor as administrator. Enter the administrator password, if required.

The group policy editor opens.

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



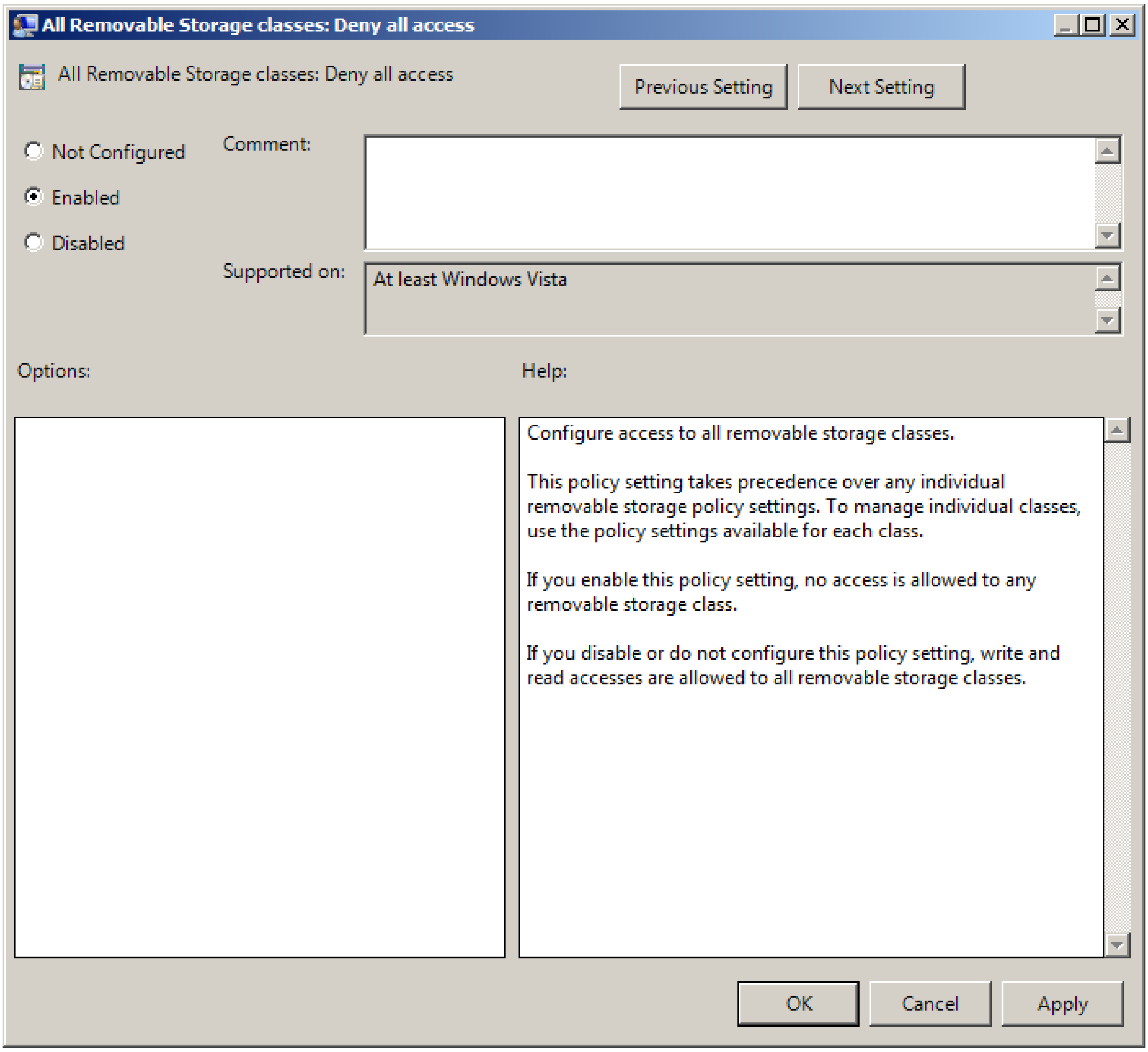
- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Control Panel
      - Network
      - Printers
      - System
        - Credentials Delegation
        - Device Installation
        - Device Redirection
        - Disk NV Cache
        - Disk Quotas
        - Distributed COM
        - Driver Installation
        - Enhanced Storage Access
        - Filesystem
        - Folder Redirection
        - Group Policy
        - Internet Communication Management
        - iSCSI
        - Kerberos
        - Locale Services
        - Logon
        - Net Logon
        - Performance Control Panel
        - Power Management
        - Recovery
        - Remote Assistance
        - Remote Procedure Call
        - Removable Storage Access
        - Scripts
        - Shutdown Options

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

Comment:

Supported on: At least Windows Vista

Options:

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

Access to USB storage media can also be locked using a global group policy in a central domain for all computers.

4.6.4 Regulating the use of USB storage media using group policy in Windows 7 and Windows Server 2008

To use a USB storage medium on a computer, the device must first be installed. This always occurs automatically when the device is initially connected to a computer. This installation can be influenced via group policies:

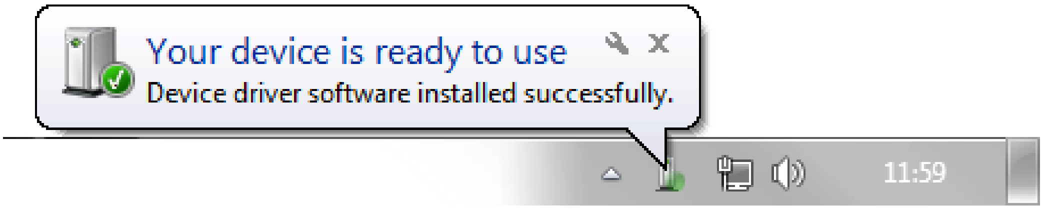
- The installation of explicitly defined devices by the user can be allowed (positive list)
- The installation of explicitly defined devices by the user can be disallowed (negative list)
- Read and write access to mobile data media, such as USB sticks, USB HDDs, diskettes, CD/DVD burners, can be configured.

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.

Determining the hardware ID of a device

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

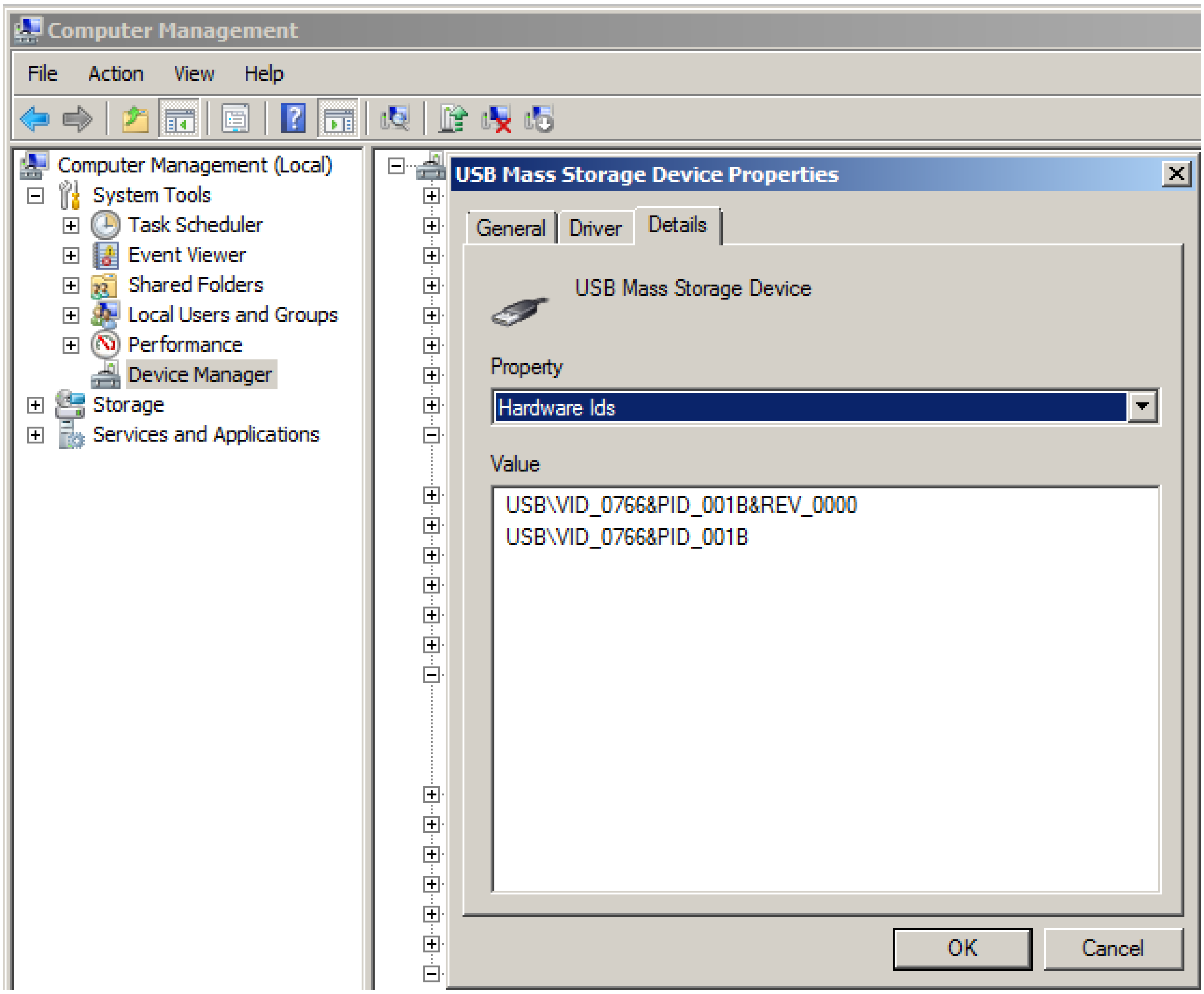
1. Connect the device with a Windows PC and wait until the installation of the corresponding driver finishes.
   Successful installation is indicated with the message "Your device is ready to use".



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
```

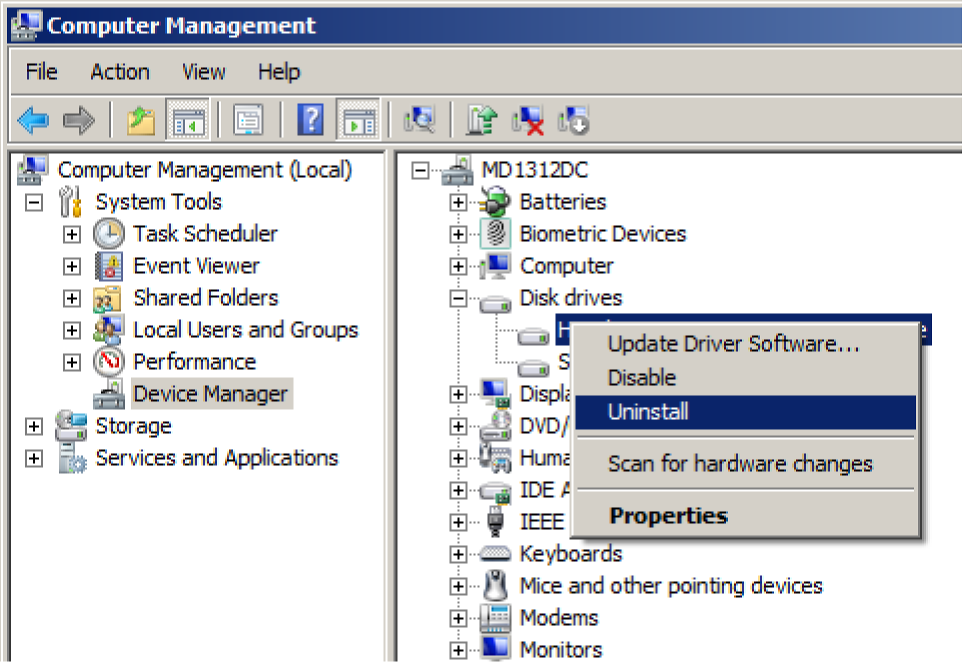
5. Select "Compatible IDs" from the drop-down list to display the compatible IDs of the device.
   You need the compatible IDs to configure the respective group policies.

Uninstalling the device

After determining the hardware ID, the device must be uninstalled. In a subsequent step, you explicitly permit the installation of the device via the group policies.

To uninstall the device, follow these steps:

1. Right-click on the device and select the command "Uninstall".



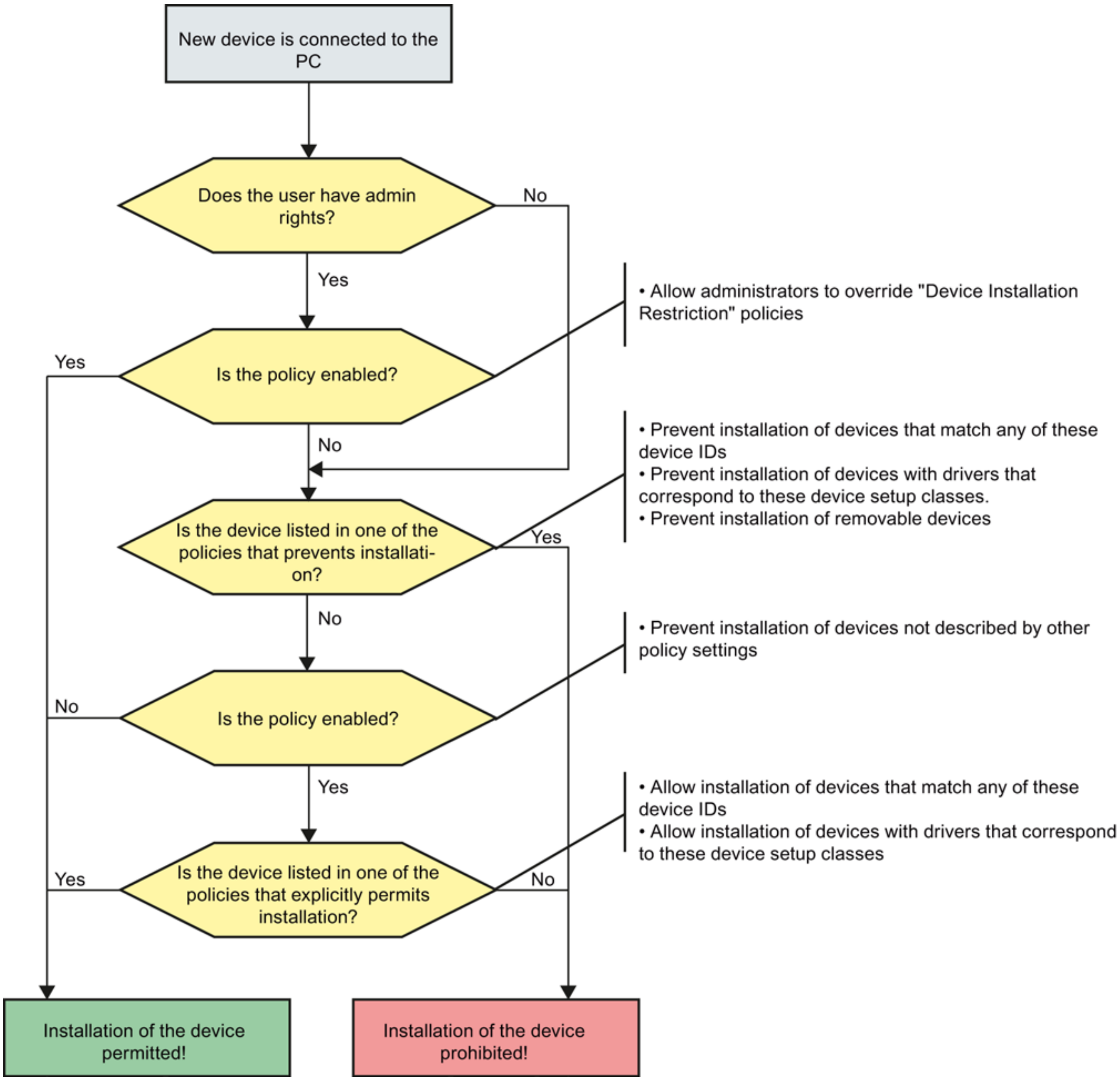
2. Click "OK" in the final dialog.

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!

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

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

To prevent the installation of all devices on the computer, proceed as follows:

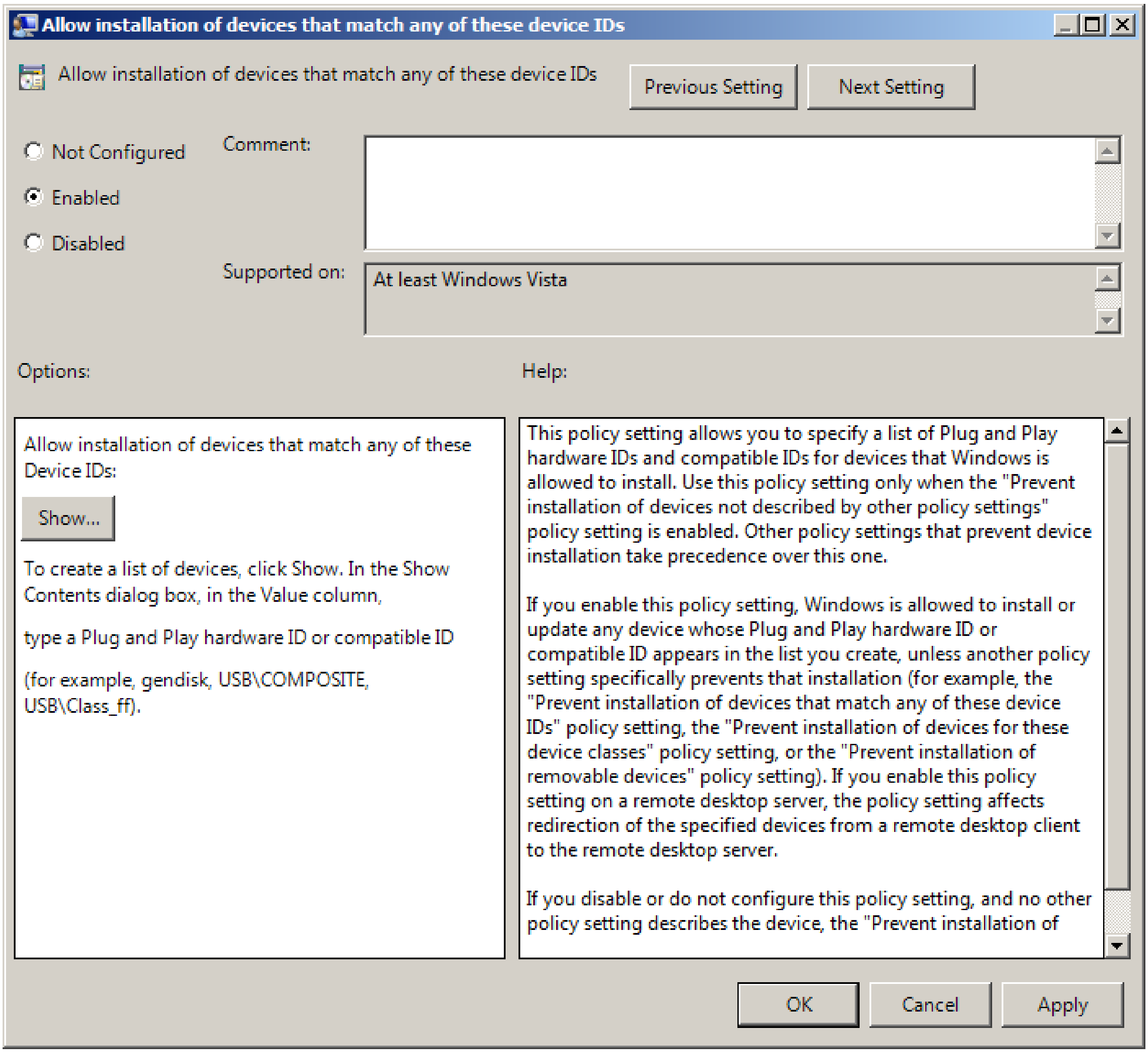
1. Ensure that all devices are uninstalled in the Device Manager.
2. Open the Group Policy Editor and navigate to the folder "Computer Configuration > Administrative Templates > System > Device Installation > Device Installation Restrictions".
   The group policies are displayed in the right pane of 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

○ 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).

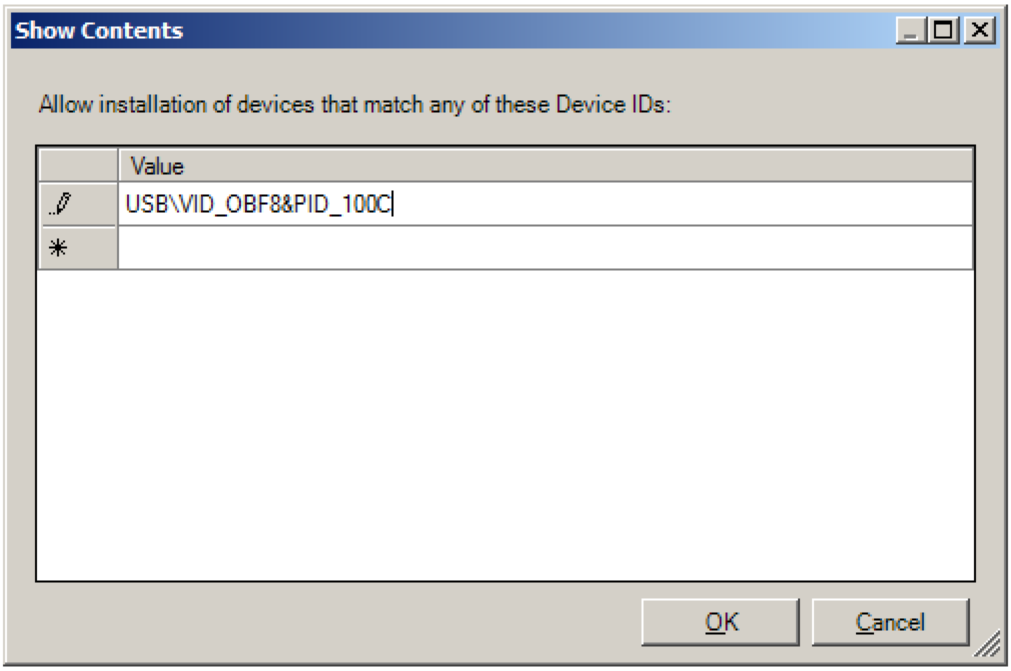
Help:

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.

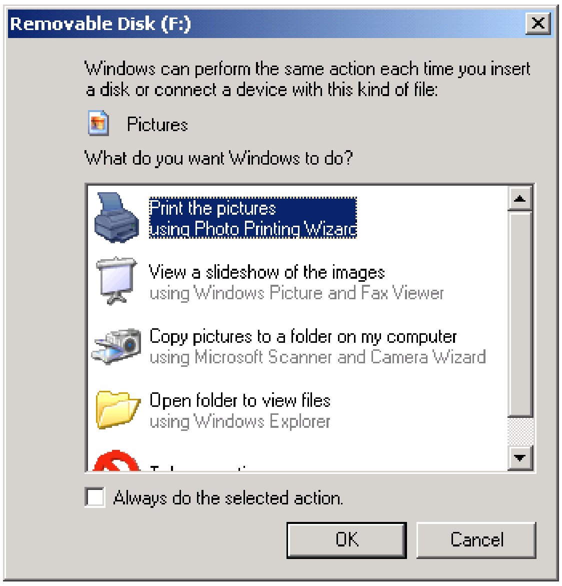
4.6.5 Disabling Windows Autorun / Autoplay for CD/DVD drives and USB storage media

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. However, this function can also be used to launch malicious software such as Trojans.



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.

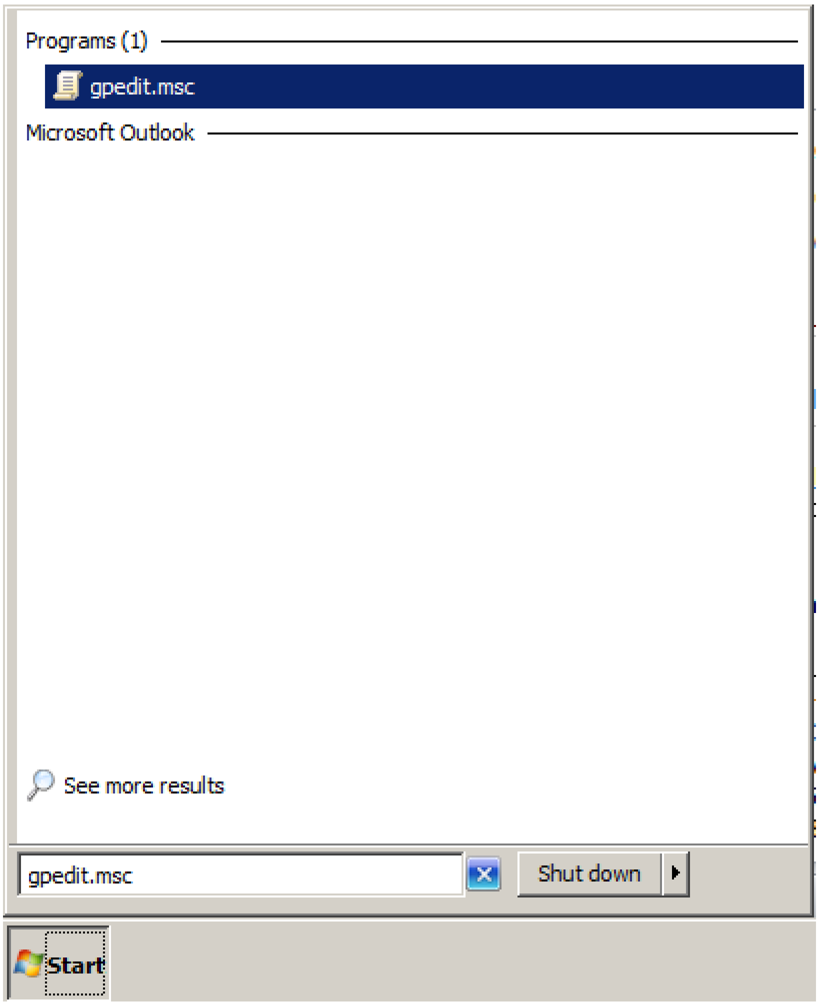
The "ShellHWDetection" service is responsible for Autorun as well as for Autoplay. Under Windows XP, the service can be disabled if Autorun has already been disabled.

4.6.5.1 Disabling the Autoplay function using group policy in Windows 7 and Windows Server 2008

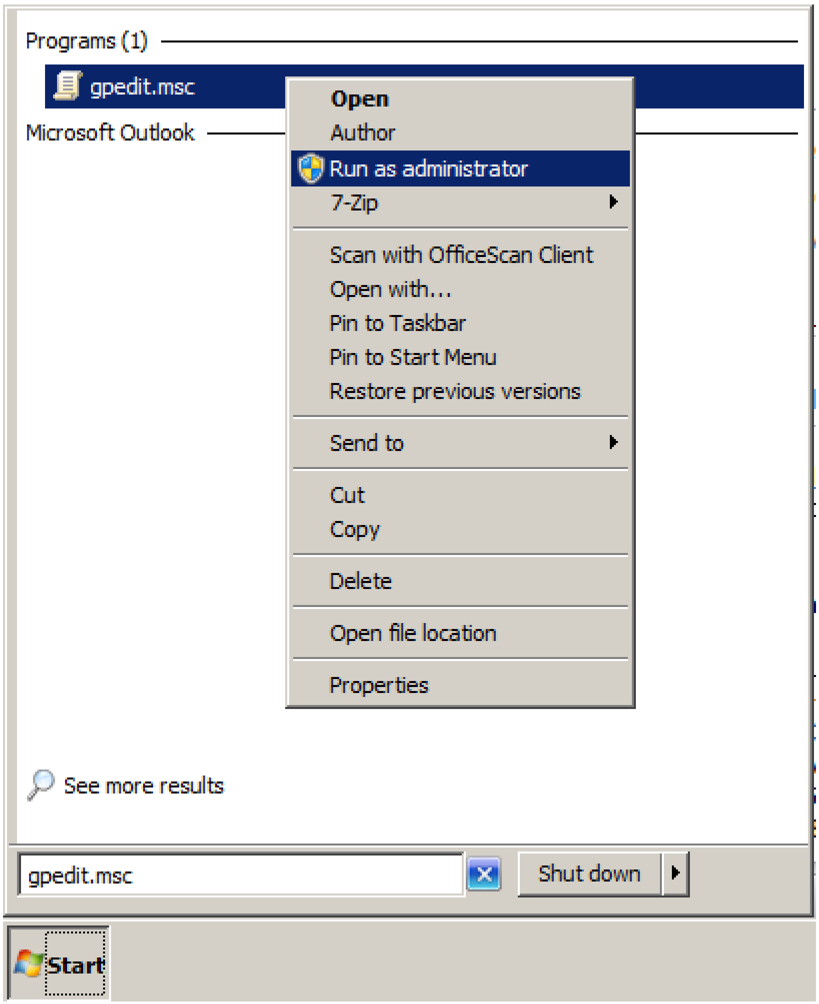
Procedure

To disable the Autoplay function, follow these steps:

1. Click "Start" and enter the string "gpedit.msc" in the "Search" box.



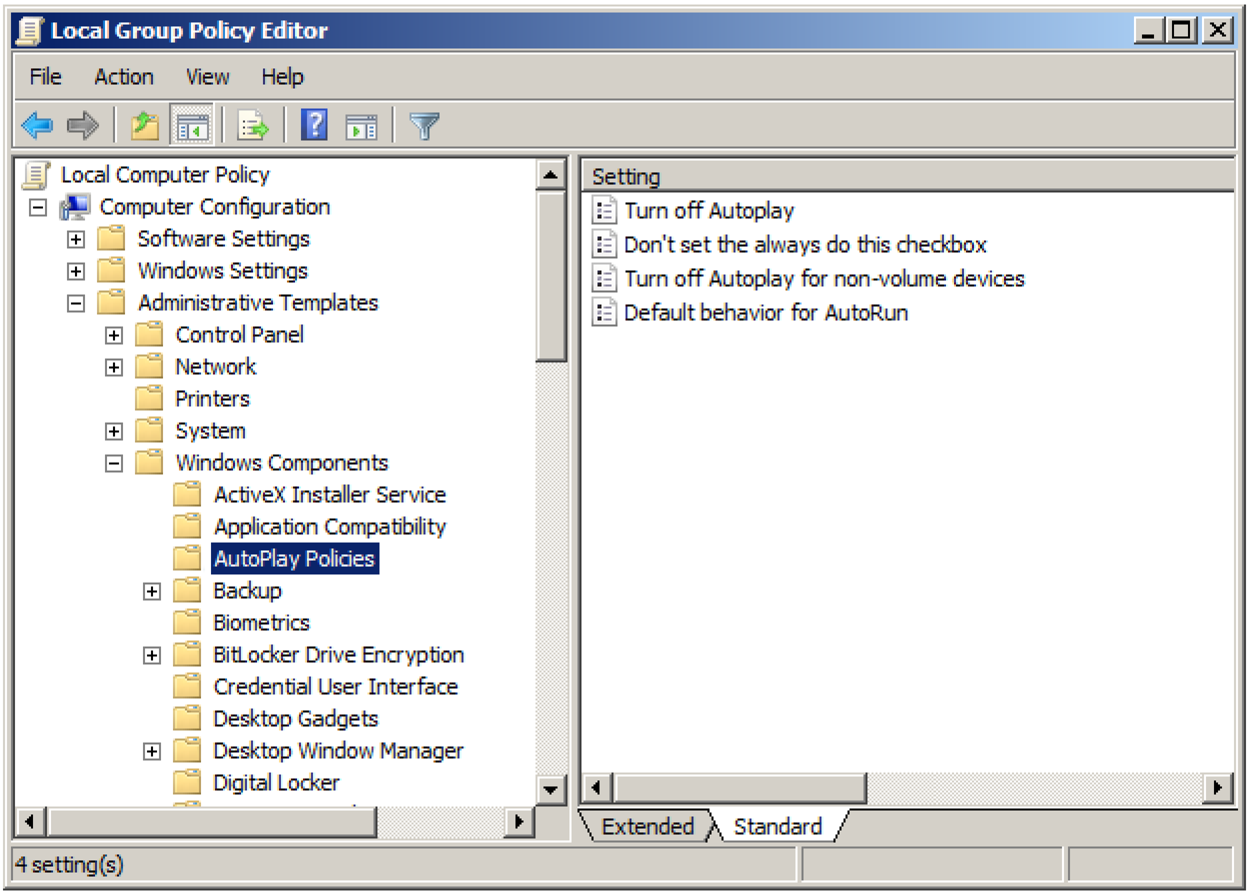
2. Start the group policy editor as an administrator.



This action requires administrator rights. For this reason, log in as administrator or start the group policy editor as administrator. Enter the administrator password, if required. The group policy editor opens.

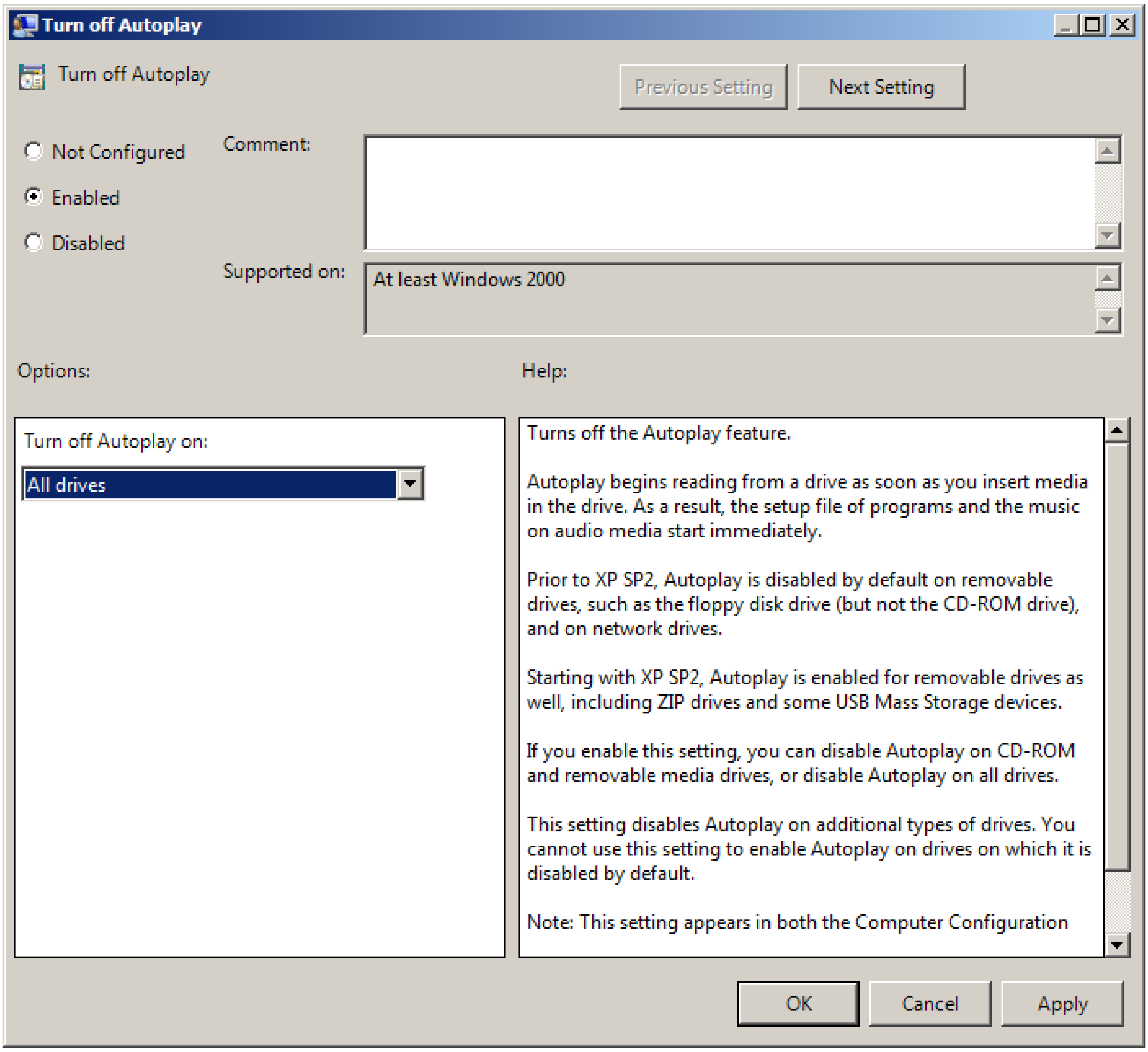
3. Select the folder "Computer Configuration > Administrative Templates > Windows Components > Autoplay Policies".

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



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 from the drop-down list.



Supported on: At least Windows 2000

Turn off Autoplay on: All drives

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.

4.6.5.2 Disabling the Autoplay function using group policy in Windows XP and Windows Server 2003

Procedure

To disable the Autoplay function, follow these steps:

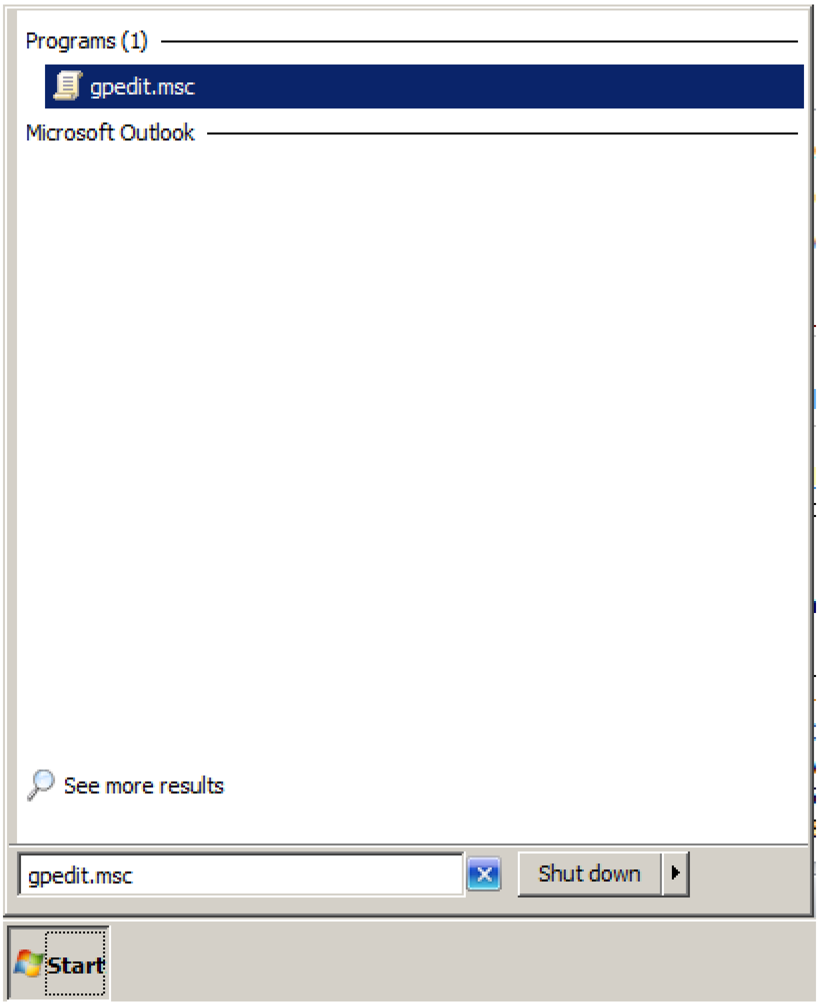
1. Click "Start" and then "Run".
2. In the "Run" box, enter the string "gpedit.msc" and click on OK.
   The Group Policy Editor opens.
3. Select the folder "Computer Configuration > Administrative Templates > System".
   The right pane of the editor shows the policies associated with the folder.
4. Double-click 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 from the drop-down list.
7. Confirm the settings with "OK".
8. Reboot the computer.

4.6.5.3 Disabling all Autorun functions using group policy in Windows 7 and Windows Server 2008

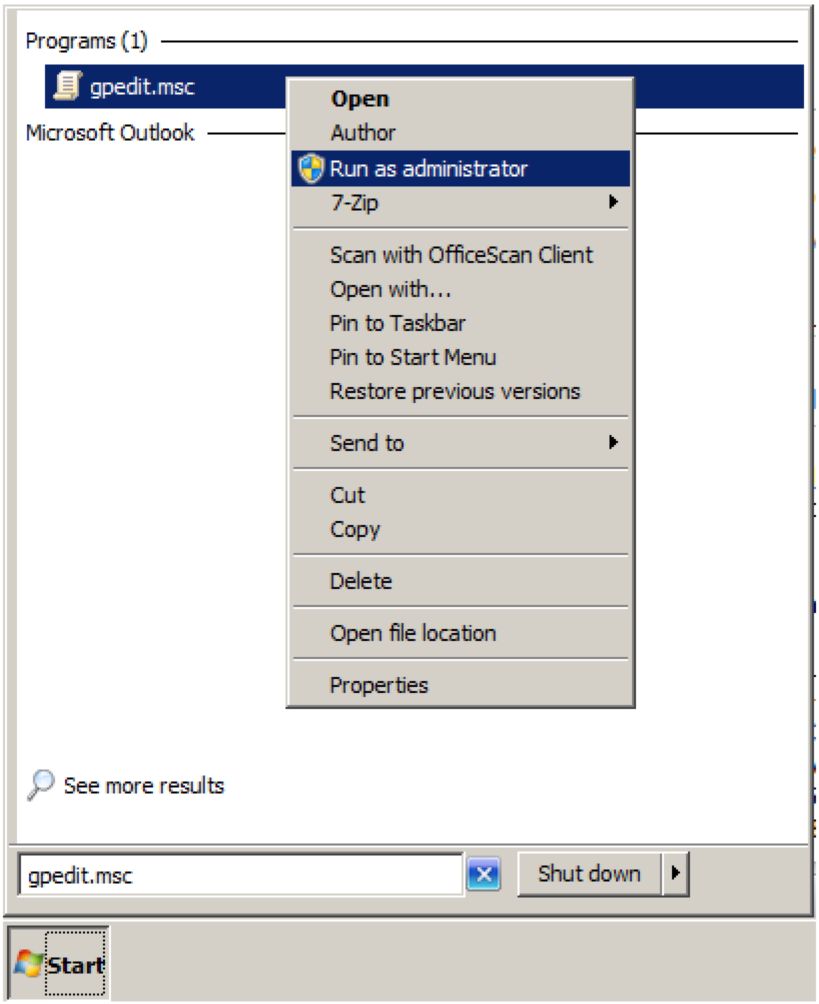
Procedure

To disable the Autorun feature, follow these steps:

1. Click "Start" and enter the string "gpedit.msc" in the "Search" box.



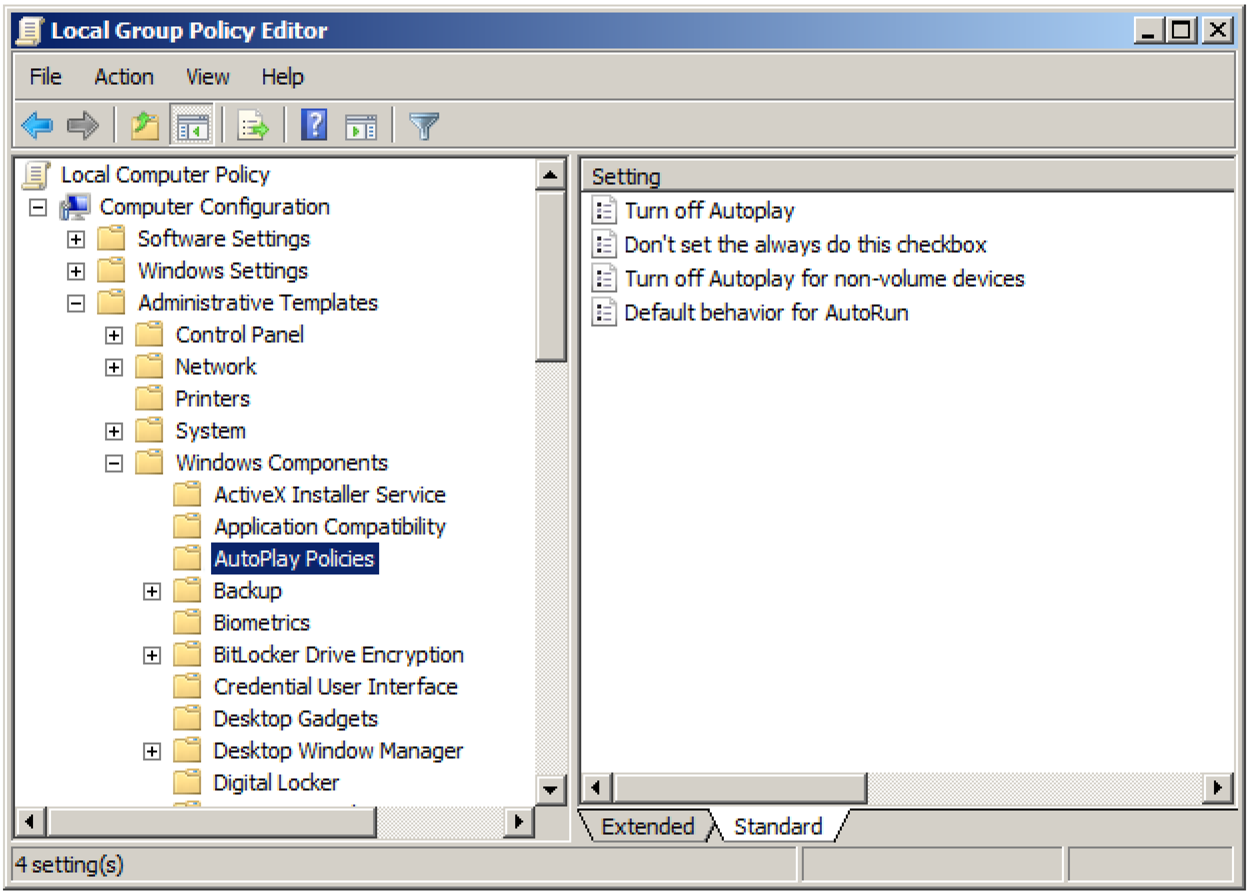
2. Start the group policy editor as an administrator.



This action requires administrator rights. For this reason, log in as administrator or start the group policy editor as administrator. Enter the administrator password, if required. The group policy editor opens.

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

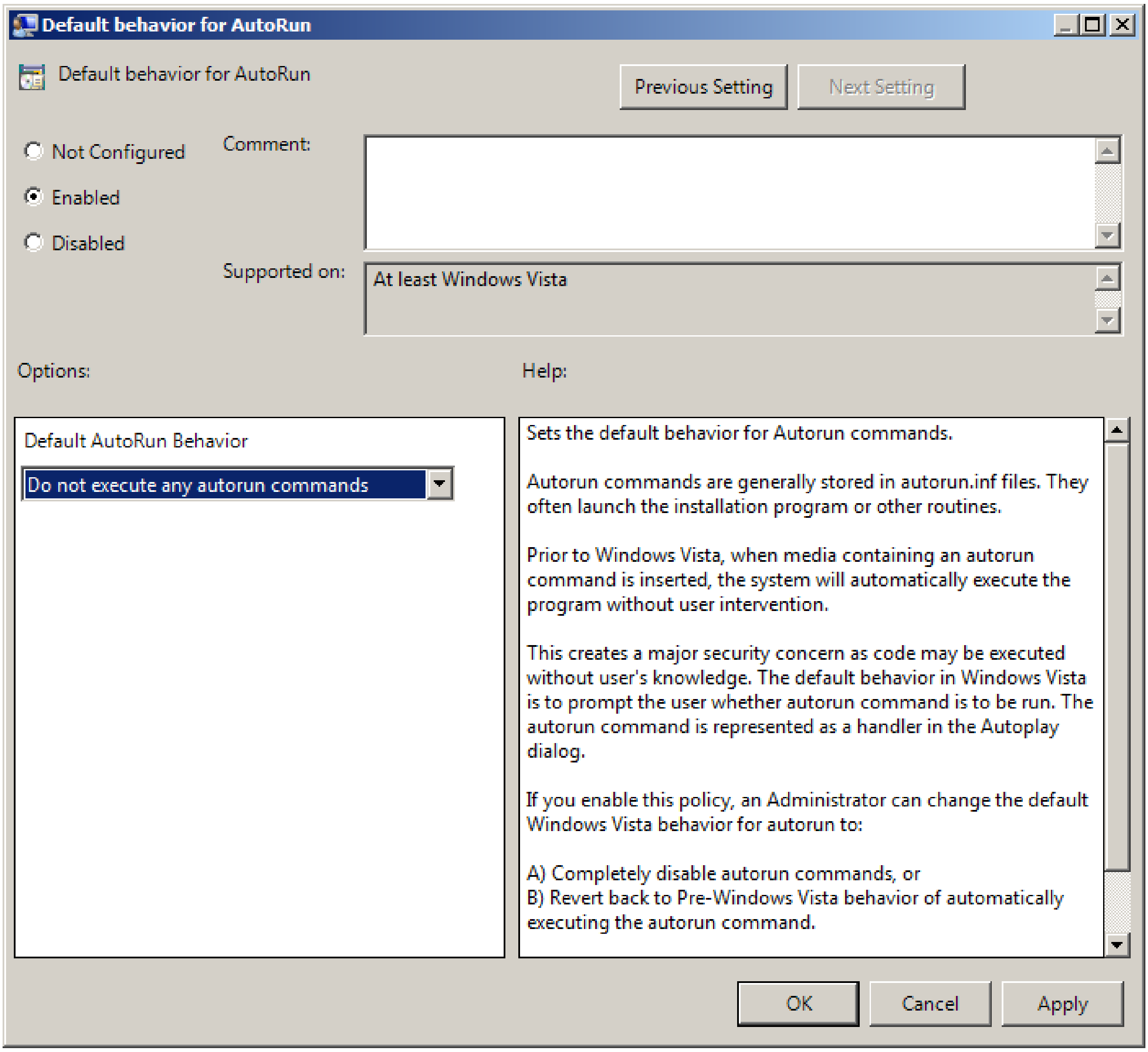
   The associated policies for the folder are displayed in the right pane of the editor.



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.



○ 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.

4.7 Whitelisting

Introduction

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). Since whitelisting is based on a positive list, there is no need for continuous updates to combat new malware threats.

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 (not on the whitelist) executable files 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 executables (exe, com, dll, bat, etc.) found during the scan are now protected against manipulation (modification, renaming, deletion, etc.). New files cannot be executed.

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 good documentation. McAfee Application Control can be operated conveniently using batch files or scripts.

Central administration of McAfee Application Control using McAfee ePO

McAfee ePO should be installed on a separate computer that contains the latest hardware. If the system already contains an infrastructure computer (e.g. WSUS, virus scan server), McAfee ePO can also be installed on this computer. McAfee ePO may not be installed on an automation device or a domain controller.

The central administration (installation, configuration and monitoring) is performed via McAfee ePO (McAfee ePolicy Orchestrator). 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.

Similar to an Active Directory Domain, central administration should be used in domains consisting of approx. 10 or more managed systems. All local commands and options of McAfee Application Control are also available remotely through ePO, some through pre-defined tasks and the remainder through remote command line options. By comparison to local administration, ePO offers superior monitoring functions and a clearly arranged event management.

Additional information

The whitelist solution from McAfee Application Control has been approved for different SIMATIC PCS 7 versions. You can find details about the compatibility with SIMATIC PCS 7 under http://support.automation.siemens.com/WW/view/en/2334224.

You can find a description of the recommended procedure with McAfee Application Control under http://support.automation.siemens.com/WW/view/en/51776157.

In addition to the system hardening options described above, there are options that relate to topics such as device hardening (of network devices and PLCs). They are part of the industrial security services. You can find additional information and the corresponding contacts http://www.industry.siemens.com/topics/global/en/industrial-security/Pages/default.aspx.

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

4.8 SIMATIC S7 CPUs

Since the S7-400 controllers are the most critical components in a PCS 7 configuration, it is recommended to configure a password and an appropriate protection level. 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.

You can find detailed information on protection levels of S7-400 CPUs under http://support.automation.siemens.com/WW/view/en/60458386.

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.

User Administration and Operator Permissions 5

5.1 Overview

Management of user and operator permissions involves the assignment of permissions in the Windows environment as well as the assignment of roles to users based on activities. 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 onto the operating system, users must obtain the permissions required for performing their tasks.

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

5.2 Windows workgroup or Windows domain

When Windows workgroups are used, the computers and users are managed decentralized and locally on each individual computer. Within Windows domains (Active Directory), centralized management of computers and users is possible.

When should plants be operated in Windows workgroups?

Operating a plant without centralized Windows management is recommended under the following conditions:

- The plant 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.
- When the uniformity of network settings, computer configurations, security policies, users and passwords can be guaranteed by meticulous, centralized plant documentation.

Special attention should be given to the following:

- The passwords of a user must always be changed on all affected computers.
- User accounts that are no longer needed must be removed everywhere.
- All computers in the plant must be configured with the same security policy (for example, use of the LanManager V2 protocol, signing of SMB communication, passport complexity and password age).
- A central record of assigned computer names and IP addresses must be created and kept up-to-date.
- When local LMHost and Host files are used to support name resolution, all files must always be updated at the same time.
- The operation of an entire plant can be seriously jeopardized by incorrect configuration of a single computer. Moreover, it is often difficult and time-consuming to locate the error in such cases.

When should plants be managed using a Windows domain (Active Directory)?

Configuration of centralized Windows management is recommended under the following conditions:

- The plant contains 10 or more computers, or the number of computers, accounts, and persons to be managed is very large.
- The plant undergoes changes on a routine basis (for example, adding new users, changing computers, introducing new security policies, changing passwords, etc.).
- Fault-tolerant logon and user management are required.
- Centralized configuration of the individual computers is required.
- The company has its own security policy that requires an Active Directory domain.

Additional criteria for centralized management:

- Legal requirements and guidelines must be met (for example, use of Kerberos as an authentication method or centralized logging of logon events, etc.).
- Centralized fault-tolerant IP address assignment (DHCP), centralized management of the name resolution and registration of computers (DNS/WINS) are required.

Note

A fault-tolerant DHCP is only possible with a DHCP server based on Windows Server 2008 (or later).

- The following requirements apply for a certificate server based on Active Directory services:
  - Secure Web services with encrypted communication via Secure Socket Layer (SSL)
  - Signatures for applications and documents
  - Authentication
  - Certificate-based IP security communication and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP).

5.3 Managing computers and users

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

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 by a domain, the AGLP principle (Access Global Local Permission) should be observed. According to this principle, the 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.

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 permanently used by different operators for process control.

Using "non-personalized" device-specific user accounts for the user accounts of these permanently used operator control and monitoring devices is recommended. Recommended accounts for this purpose are those that allow establishing a reference to the respective computer (e.g. OSClient_5). When using "Autologon" for logging onto the operating system, this account must be used. For an engineering station that is not permanently in operation but is used by different users/engineers for configuration, person-based user accounts are recommended for each user/engineer.

Note

Membership in the Administrators group is only relevant for the installation of PCS 7 and the configuration of the computer.

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 issuing the security settings since the respective user account or the group only has to be added to the local SIMATIC group. Depending on the SIMATIC products being installed, the number of added groups may differ.

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

SIMATIC WinCC

During the installation of SIMATIC WinCC, the following three new user groups are created for project shares and project file accesses:

- 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. Additional users must be added manually by an administrator of this group.
- SIMATIC HMI CS
  The members of this group may only perform configurations; they may not make direct changes to the runtime components. This group is empty by default and is reserved for later use.
- SIMATIC HMI VIEWER
  The members of this group may access configuration and runtime data only in read-only mode. This group is primarily used for the accounts of Web publishing services, e.g. IIS (Internet Information Services) for operating the WinCC Web navigator.

The first time a project is opened, a project share is automatically created and assigned the required share permissions and security settings. The project shares and project file accesses are managed automatically by the SIMATIC software.

SIMATIC NET

During the installation of SIMATIC NET via the frame setup of SIMATIC PCS 7, the following local user group is added to the user and group administration:

- SIMATIC NET
  All users working with PCS 7, PCS 7 OS or Route Control projects must be members of this group.

SIMATIC BATCH

For SIMATIC BATCH, the following new user group is created during the installation:

- 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 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.

SIMATIC Route Control

For SIMATIC Route Control, the following user groups are created additionally during the installation:

- RC_ENGINEER
- RC_MAINTENANCE
- RC_OPERATOR_L1
- RC_OPERATOR_L2
- RC_OPERATOR_L3

By default, the user account to be installed is added to the "RC_MAINTENANCE" group during the installation.

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.

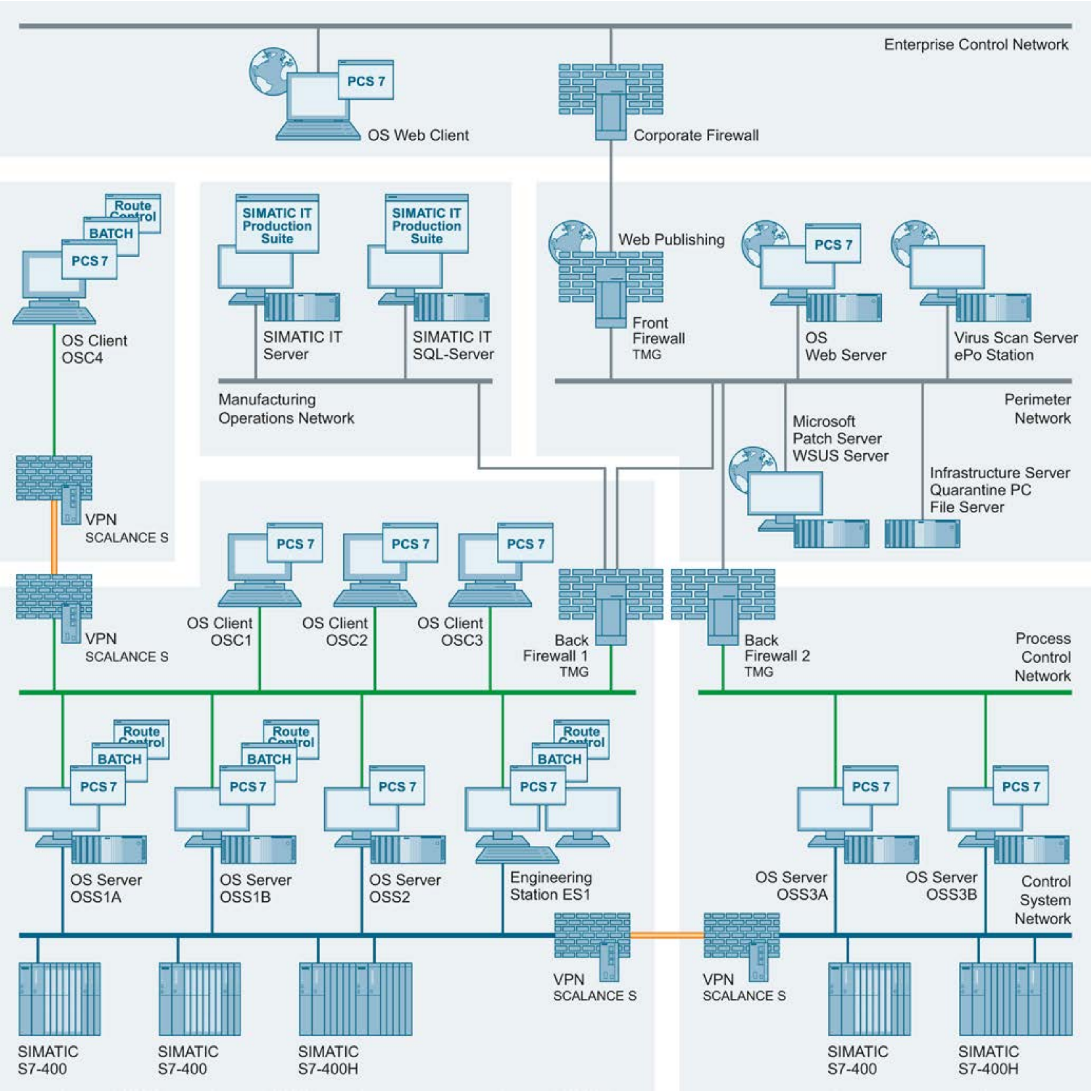
SIMATIC Management Console

The following user groups must be created for SIMATIC Management Console:

- SIMATIC Management Administrators
  Members of this group have unrestricted access to the Management Console and all permissions.
  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.
  Include users that are assigned to the "SIMATIC Management Administrators" user group on the Management Console computer in the "SIMATIC Management Users" user group as well.
- Windows logon on the Management Console computer
  All users of the Management Console must log on as an administrator (local "Administrators" group or computer-specific administrator in the domain).

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 to which different user groups the above users must be assigned:

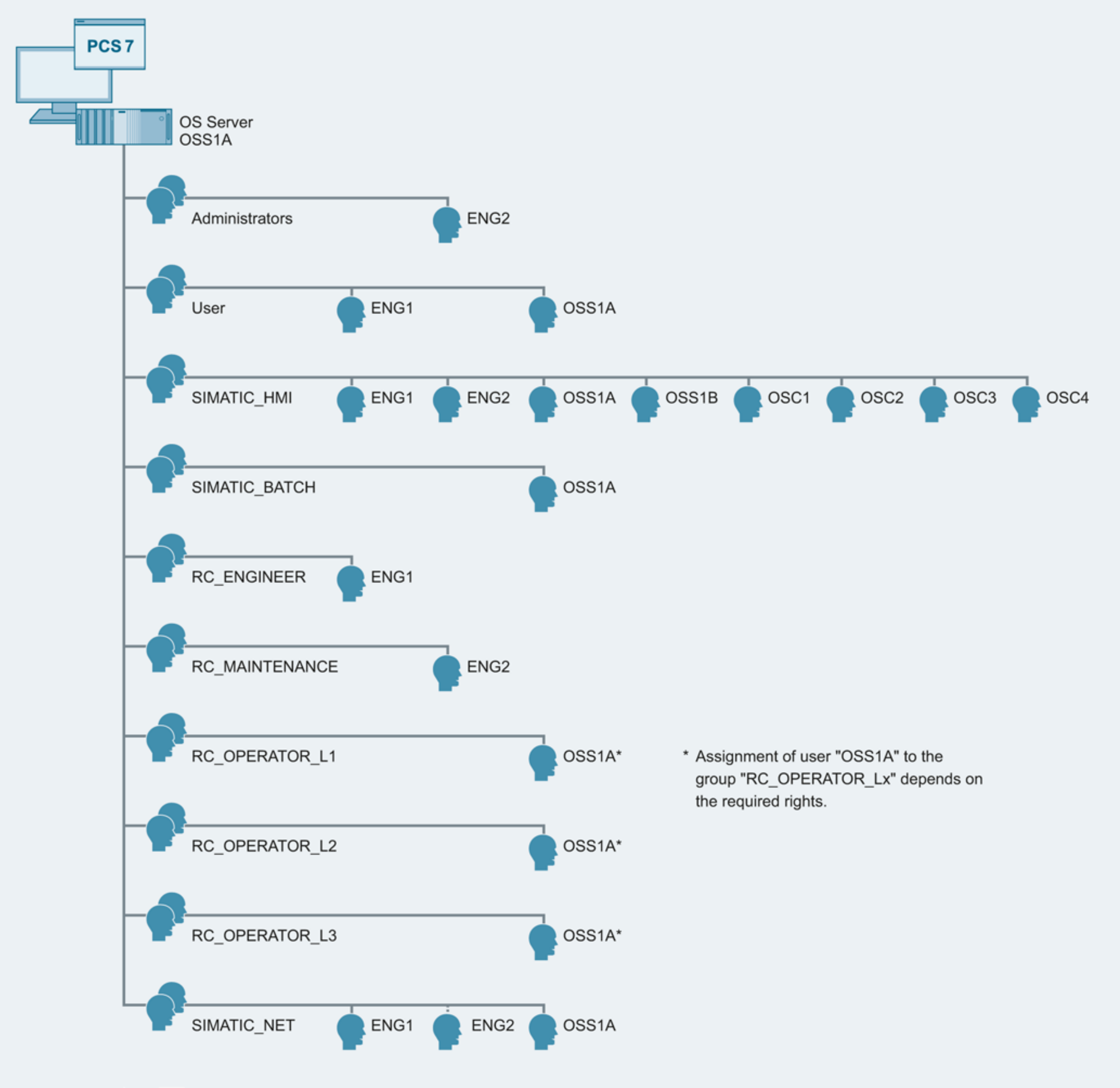
Computer/ Local group	ES1	OSC1	OSC2	OSC3	OSC4	OSS1A	OSS1B	OSS2	OSS3A	OSS3B
Administrators	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2
User	ENG1	OSC1 ENG1	OSC2 ENG1	OSC3 ENG1	OSC4 ENG1	OSS1A ENG1	OSS1B ENG1	OSS2 ENG1	OSS3A ENG1	OSS3B ENG1
SIMATIC HMI	ENG1 ENG2	ENG1 ENG2 OSC1 OSS1A OSS1B OSS2 OSS3A 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 more information on computer and user management in the document "Security Concept PCS 7 and WinCC - Basic document (Whitepaper)" (http://support.automation.siemens.com/WW/view/en/26462131).

Detailed information on this is available in the manual "SIMATIC Process Control System PCS 7 PC Configuration and Authorization” (http://support.automation.siemens.com/WW/view/en/68157327).

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 user manual "SIMATIC Process Control System PCS 7 SIMATIC Route Control” (http://support.automation.siemens.com/WW/view/en/68154021).

5.4 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 should to be changed at regular intervals (every 6 months at the latest).
- Minimum complexity
  A password should have a minimum complexity, which means it should meet the following requirements:
  - Minimum length of 8 characters
  - Contain at least 2 alphanumeric characters and at least 1 number, possibly a special character
- Password history
  A new password must differ significantly from the previous (old) password (by at least 3 characters).

Procedure

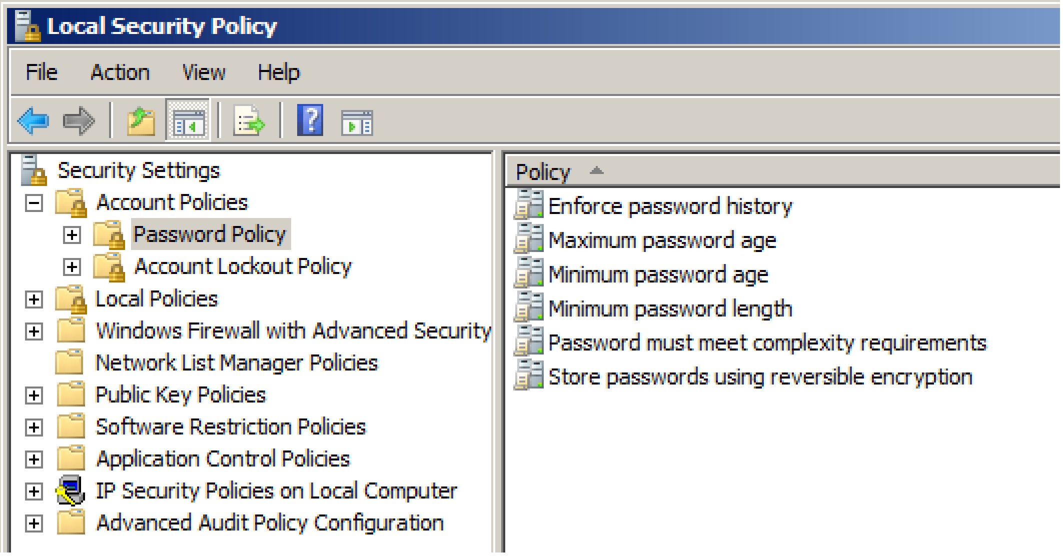
The following procedure is described using the example of the "Windows 7" operating system.

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.



- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
  - Windows Firewall with Advanced Security
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Computer
  - Advanced Audit Policy Configuration

Policy

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Password must meet complexity requirements
- Store passwords using reversible encryption

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.

5.5 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.

5.5.1 SIMATIC Logon

Systems automated with process control systems feature the following special/important 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 confirmations about important or critical actions.

SIMATIC Logon allows assigning individual, task-based permissions to SIMATIC applications and system areas.

SIMATIC Logon supports user management on a local computer and in a Windows domain. It is recommended to use SIMATIC Logon in the Active Directory in a domain to take advantage of the centralized group and user management features.

SIMATIC Logon offers a "Default user" function. This is automatically logged on at the start of the PCS 7 application or when a SIMATIC Logon user is logged off. For this user account, it is recommended to assign the minimum number of required user rights, for example, for emergency operation.

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

- Automation License Manager
- WinCC
- SIMATIC Batch
- STEP 7

You can find detailed information about SIMATIC Logon in the manual "SIMATIC Logon" (http://support.automation.siemens.com/WW/view/en/34519648).

5.5.2 Access protection for projects/libraries on the engineering station

Introduction

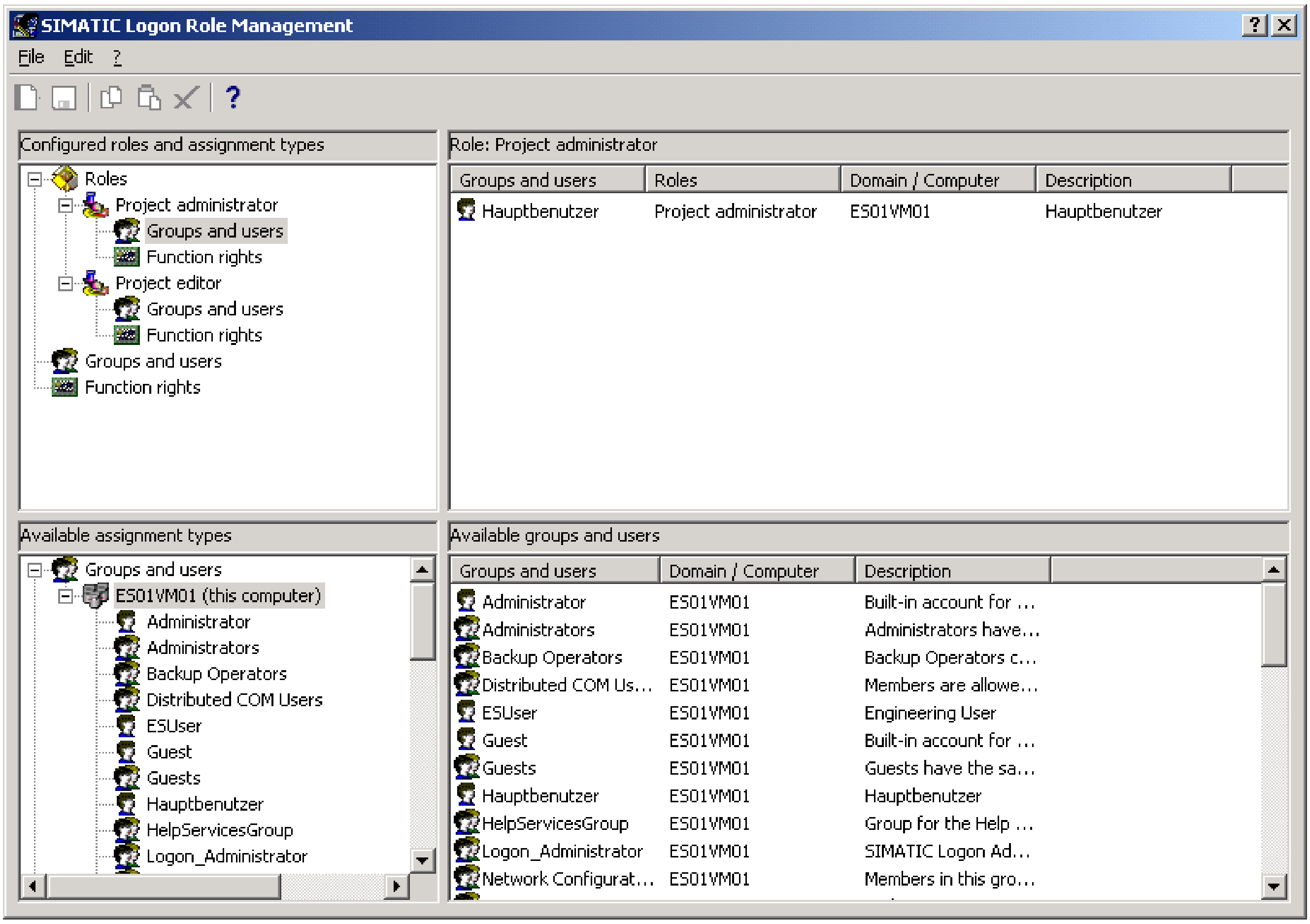
We recommend that you protect your projects and libraries against unwelcome access and that you log all access actions. This functionality requires that SIMATIC Logon is installed. The SIMATIC Logon software defines user roles for the engineering system and their assignment to the defined Windows users/groups.

These access-protected projects and libraries can then only be opened and edited by Windows users with 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 defines the users for the "Project editor" roles and the project password. He/she is entitled to activate and deactivate access protection. The project administrator can assign Windows users to one of the two user roles.

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 performed for each project and library in the SIMATIC Manger. 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 the project administrator or project editor.

The user currently logged on ("Project administrator" or "Project editor") is displayed in the status bar of the SIMATIC Manager. 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 on "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" (http://support.automation.siemens.com/WW/view/en/68157345).

5.5.3 Documenting changes in the change log

Introduction

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.

Procedure

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

5.5.4 Documenting changes in the ES log

Introduction

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.

Procedure

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

5.5.5 Access protection for operator stations

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

- On the one hand, the operator station must be protected against unauthorized access such as operator interventions or image selection if nobody is logged on to this station. This means when the operator logs off the station, either by pulling the smart card or with manual logoff, the station must switch to a state that makes it impossible for unauthorized persons to use it (screensaver mode). The screen selected at the time is therefore no longer displayed once an operator has logged off.
- On the other hand, the operator station must be "locked" in such a way that it is impossible for an unauthorized user to reach the Desktop of the operating system.

5.6 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 with key switches, protection level 1 is called "Key switch position". The position of the key switch (mode selection switch) determines the CPU protection:

- Key switch in STOP or RUN-P position: No restrictions
- Key switch in RUN position: Only read access possible

You can bypass the key switch protection by entering a password.

For standard CPUs whose operating mode switch is designed as a RUN-STOP switch rather than a key switch, protection level 1 is called "No protection". A password entry is not possible.

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" (http://support.automation.siemens.com/WW/view/en/68157345).

Patch management 6

6.1 Overview

Microsoft removes security gaps in its products and provides these corrections to its customers via official 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 WSUS
  Windows updates made available for all computers of the automation system from a separate Windows Server Update Service (WSUS)
- Manual update
  Manual installation of the "Security Patches" and "Critical Patches" after download from the Microsoft sites to all computers of the automation system.

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" (http://support.automation.siemens.com/WW/view/en/38621083)
- FAQ "How can you find out which Microsoft Patches are installed on the PC?" (http://support.automation.siemens.com/WW/view/en/48844294)
- FAQ "Which Microsoft Patches ("Security Patches" and "Critical Patches") have been tested for compatibility with SIMATIC PCS 7?" (http://support.automation.siemens.com/WW/view/en/22754447)

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

- http://technet.microsoft.com/en-us/
- http://www.microsoft.com/wsus

Support for implementing a 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:

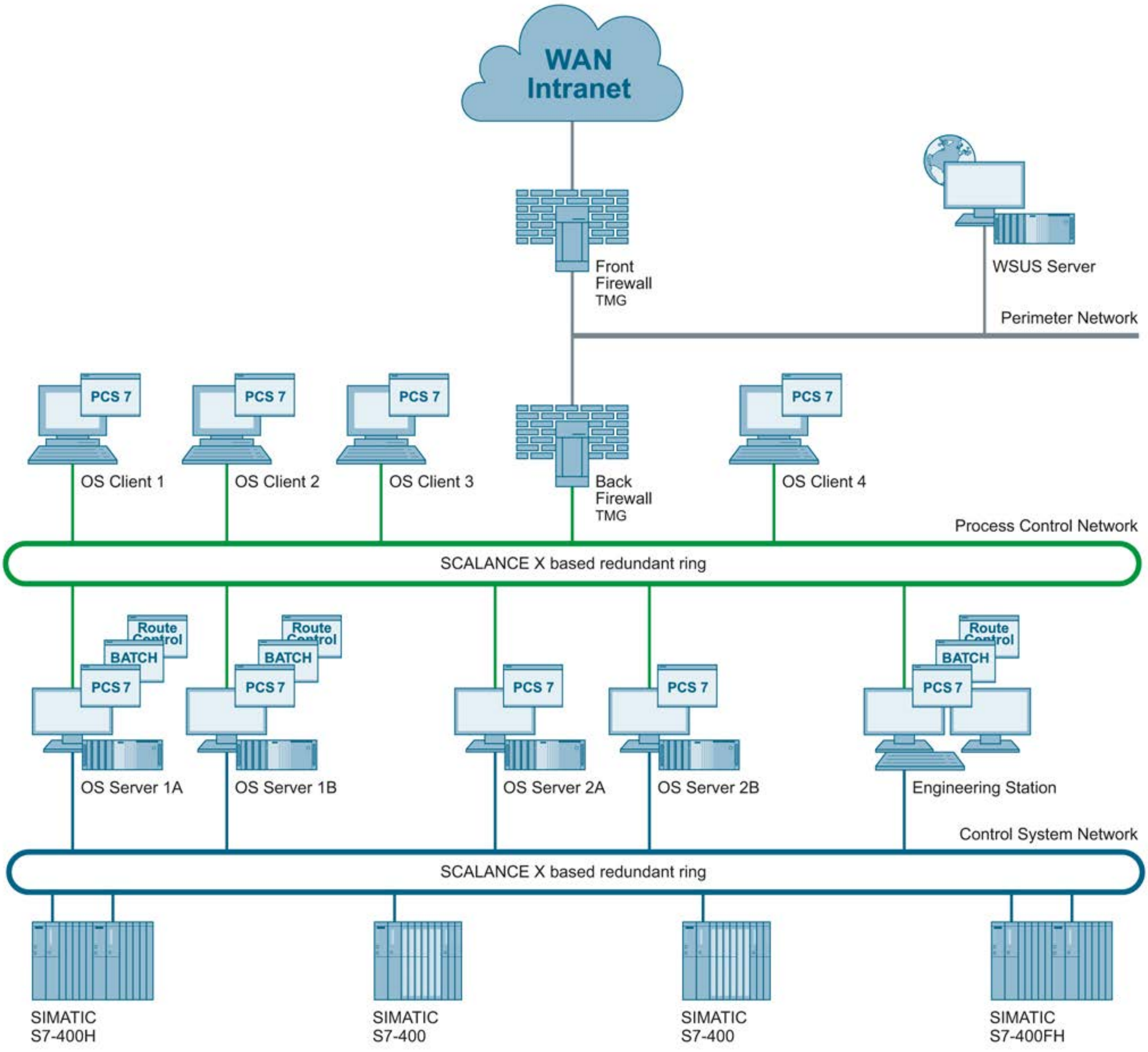
- http://www.industry.siemens.com/topics/global/en/industrial-security/Pages/default.aspx

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

6.2 Windows Server Update Service (WSUS)

WSUS server

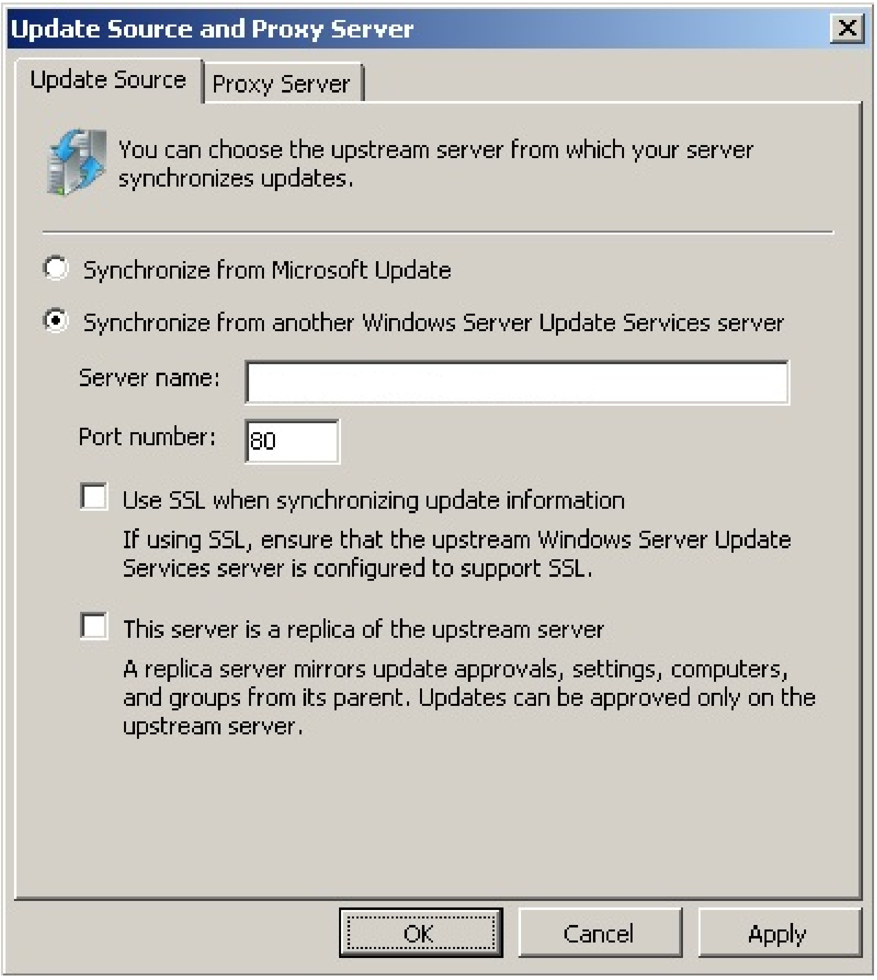
In accordance with the rules for dividing the components into security cells, the WSUS server must be singled out in a separate network (Perimeter network / DMZ). All solutions relating to securing access points to the security cells, such as front-end/back-end firewall or triple-homed firewall, can be used for the patch management or the WSUS server. The WSUS must be configured in the Perimeter network using the Industrial Wizard for configuring the access rules for the back-end firewall or the triple-homed firewall.



Update source

For the WSUS server, either an existing WSUS in a higher-level external network, such as the plant network or corporate network, or Microsoft Update on the Internet can be configured for synchronization. The decision not only affects the configuration of the firewall (frontend firewall or triple-homed firewall), but also the configuration of the WSUS server.

The corresponding update source must be configured in the WSUS configuration:



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.

6.2.1 Recommended procedure for patch management using the Microsoft Windows Server Update Service (WSUS)

Requirement

A WSUS is set up for your PCS 7 plant.

Configuring WSUS

To configure the WSUS, follow these steps:

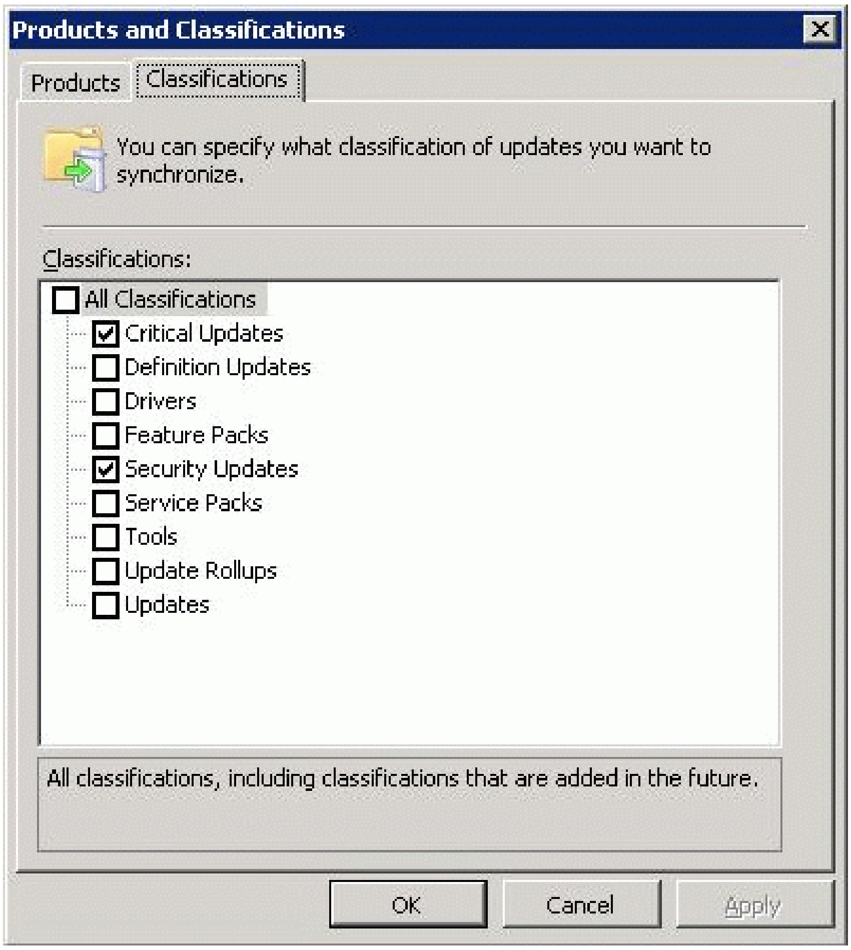
1. Open the WSUS Administration Console and click "Options".
2. Under "Products and Classifications", select all Microsoft products relevant to the plant in the "Products" tab.

Note

You can find information about the permitted Microsoft patches in the following FAQ:

Which Microsoft Security Patches ("Security Patches" and "Critical Patches") have been tested for compatibility with SIMATIC PCS 7?” (http://support.automation.siemens.com/WW/view/en/18490004).

3. Select the "Critical Patches" and "Security Patches" under "Products and Classifications" in the "Classifications" tab.



Products and Classifications

Products | Classifications

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

Classifications:

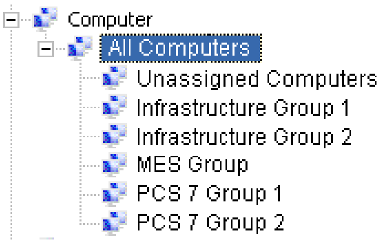
- □ All Classifications
  - ☑ Critical Updates
  - □ Definition Updates
  - □ Drivers
  - □ Feature Packs
  - ☑ Security Updates
  - □ Service Packs
  - □ Tools
  - □ Update Rollups
  - □ Updates

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

Note

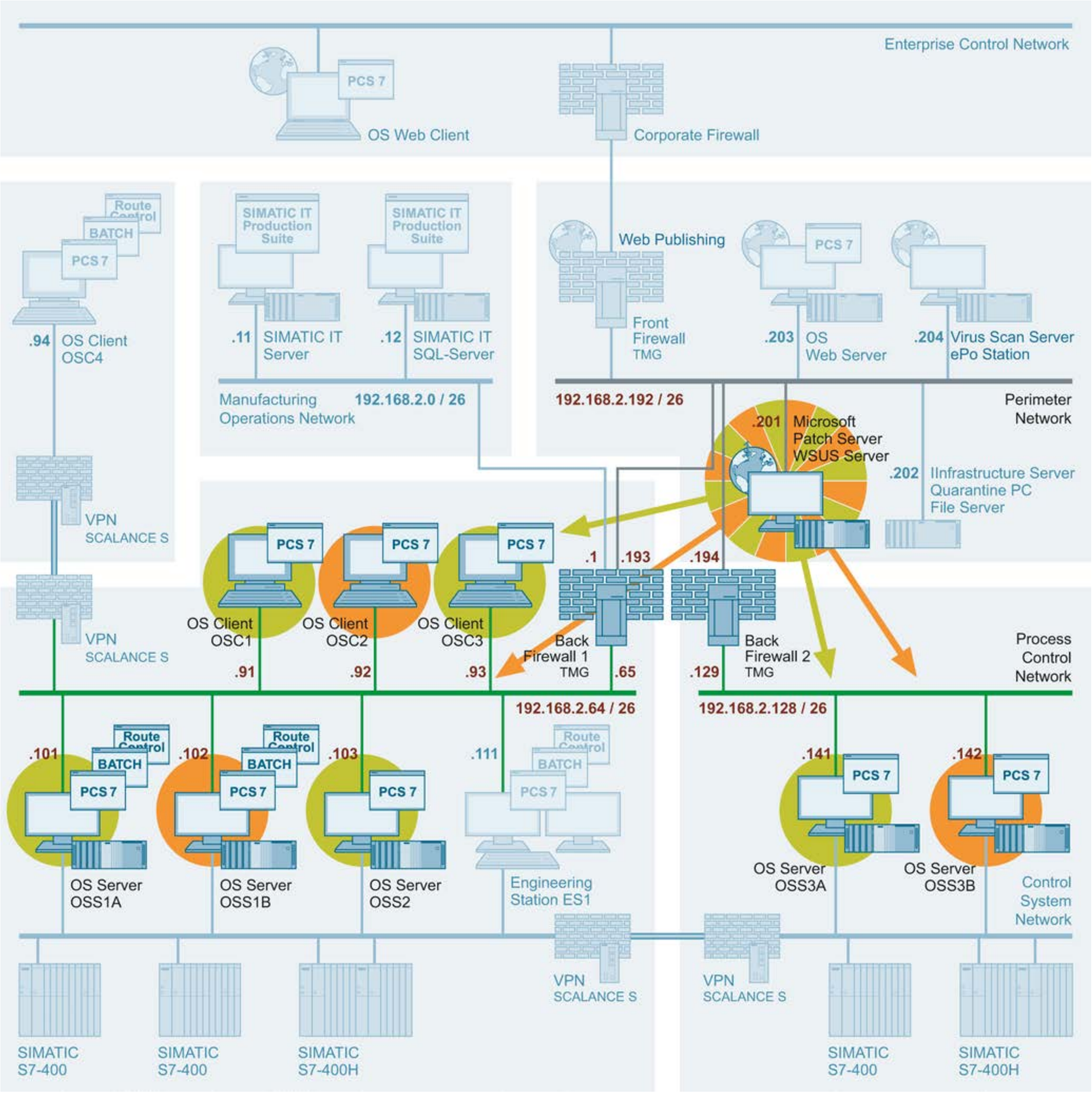
When using an Industrial Automation Firewall 200/1000 or Microsoft Forefront Threat Management Gateway (TMG) the "Definition updates" must also be selected under "Products and Classifications".

4. Create project-specific groups for the distribution of updates in the plant according to the redundancy concept, and assign the individual computer systems to these computer groups.

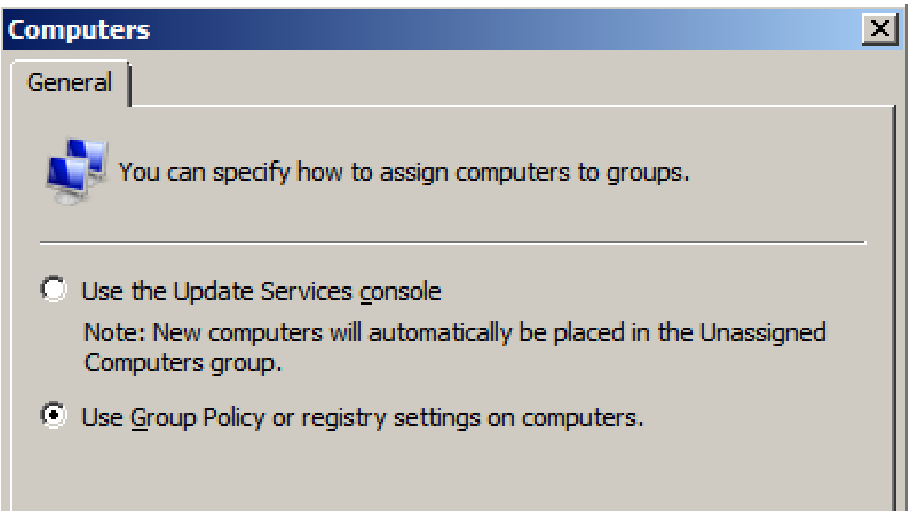


- Computer
  - All Computers
    - Unassigned Computers
    - Infrastructure Group 1
    - Infrastructure Group 2
    - MES Group
    - PCS 7 Group 1
    - PCS 7 Group 2

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".



In order to assign the computers directly to the correct computer groups, the following option must be selected, regardless of whether the administration is performed using Windows workgroups or domains.



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? (http://support.automation.siemens.com/WW/view/en/22754447)
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.

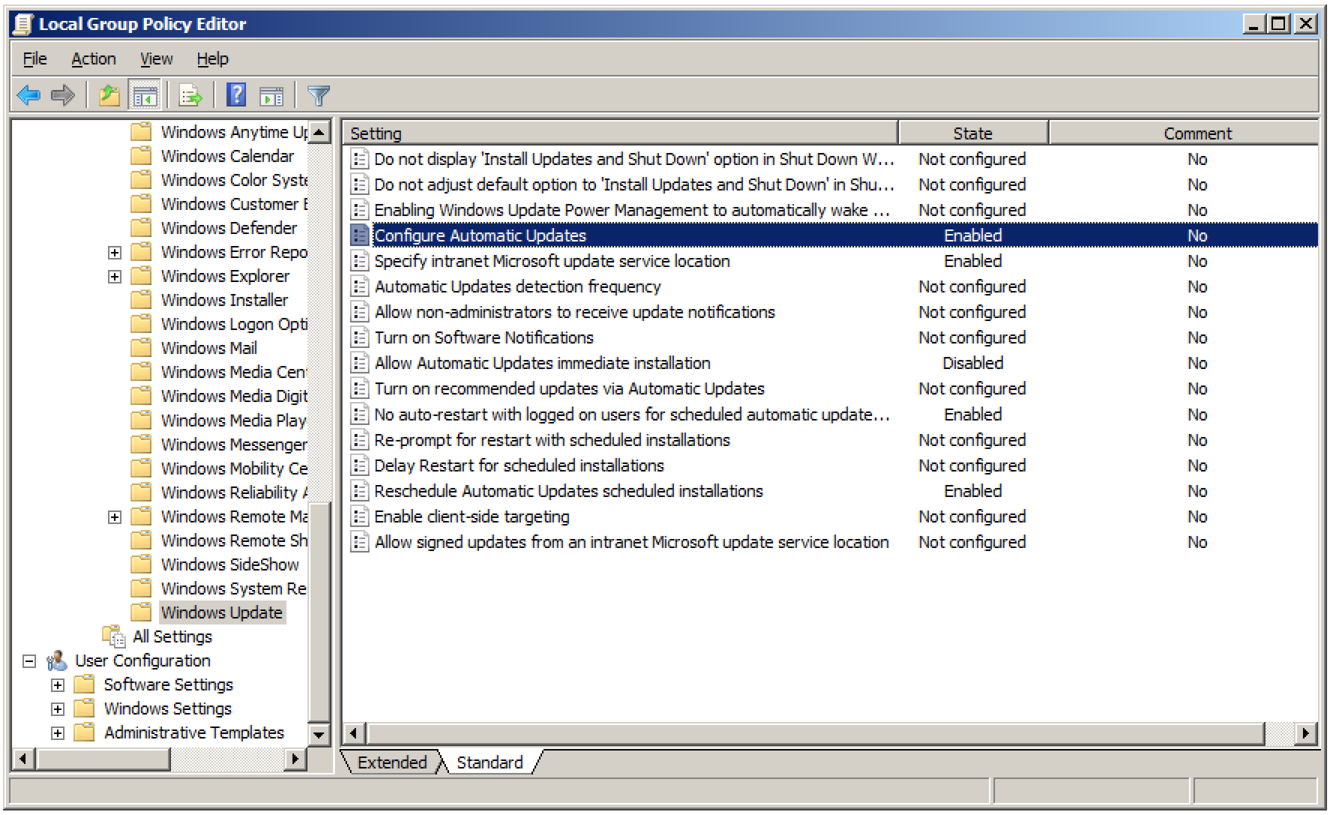
WSUS administration

1. Select all available updates in the "Critical Patches" and "Security Patches" categories and release them for installation in the created groups.
2. Use an administrative account to log on to the clients connected with the WSUS (the clients have been configured accordingly to receive the updates from the WSUS).
3. Run the updates offered.

6.2.2 Configuration of computer policies

The policies for the Windows Update service are defined via the editor for local group policies. When using a domain controller, the settings are performed centrally and distributed accordingly to all computer systems. If the administration is carried out using Windows workgroups, these settings must be made separately on every computer.

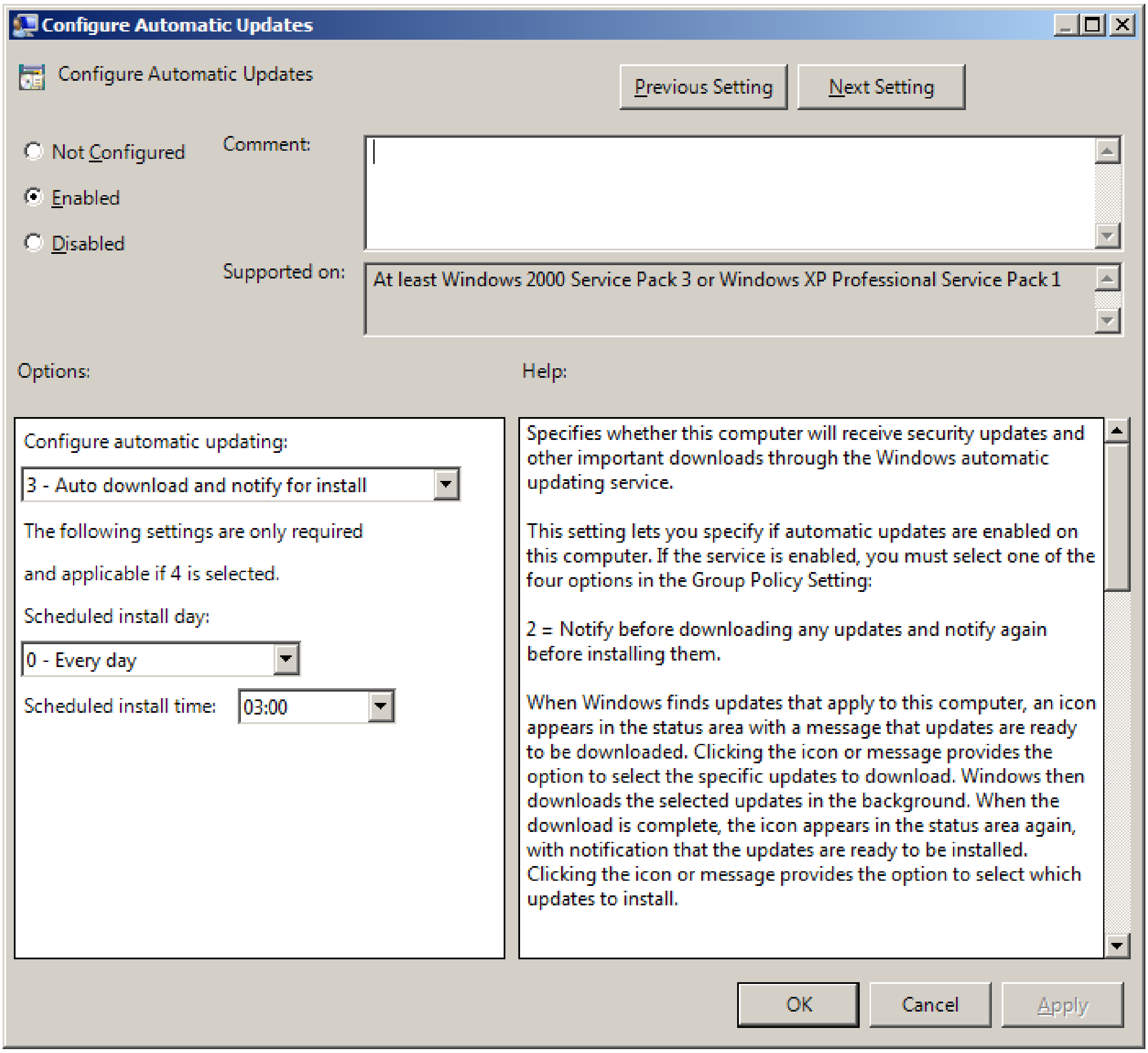
The following figure shows the editor for local group policies:



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 following group policies must be configured:

- "Configure Automatic Updates" policy
  The "Configure Automatic Updates" policy must be enabled. In the properties dialog of the policy, it must be stipulated that updates should be automatically downloaded but not installed.



○ 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: 3 - Auto download and notify for install

The following settings are only required and applicable if 4 is selected.

Scheduled install day: 0 - Every day

Scheduled install time: 03:00

Help:

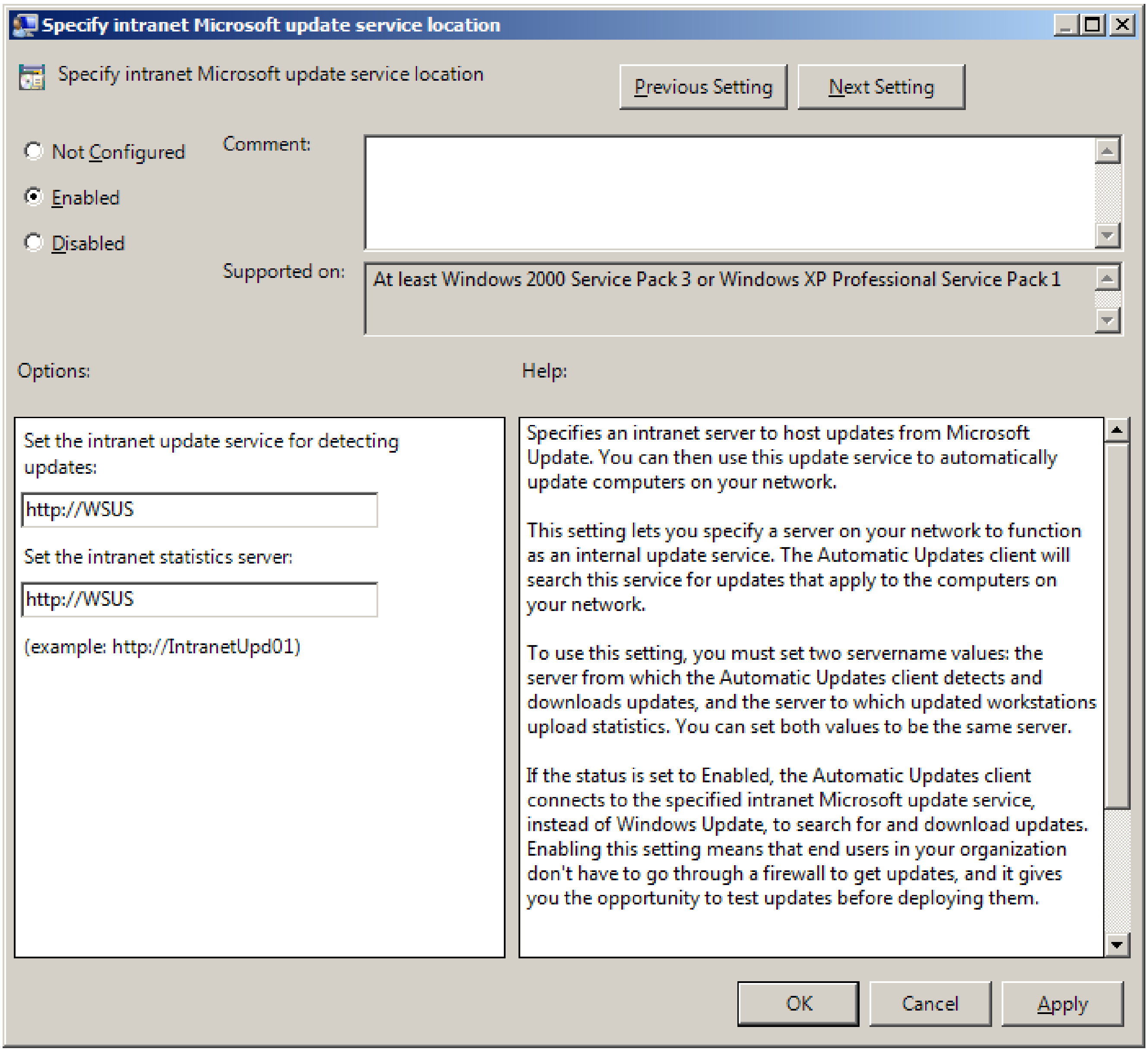
Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

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. If a separate upstream server in a higher-level, external network is used, the IP address or computer name of this WSUS server must be specified in the properties dialog of this policy.



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

Options:

Set the intranet update service for detecting updates:

http://WSUS

Set the intranet statistics server:

http://WSUS

(example: http://IntranetUpd01)

Help:

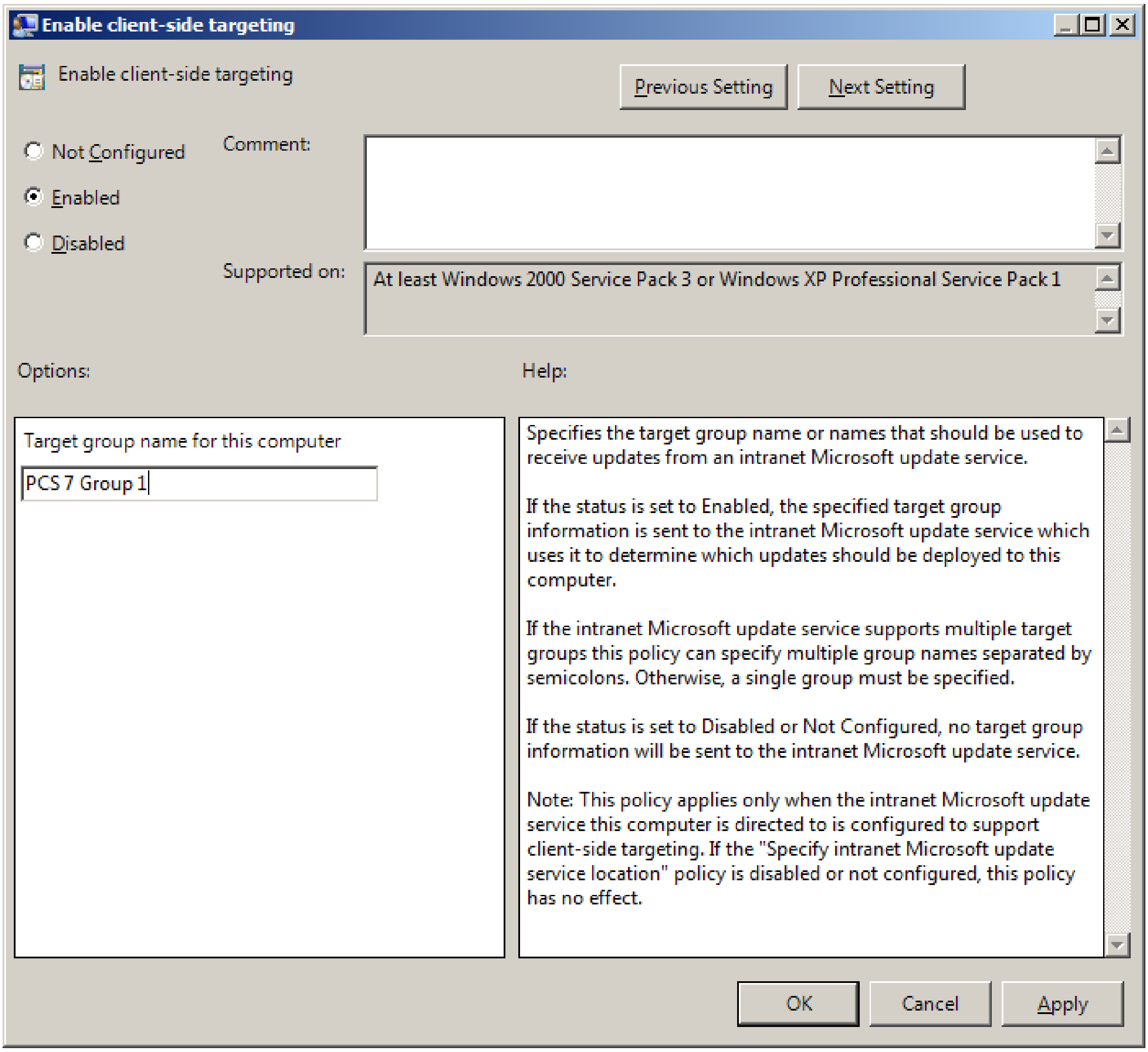
Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network.

This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network.

To use this setting, you must set two 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 destination assignment" policy
  The "Enable client destination assignment" 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.

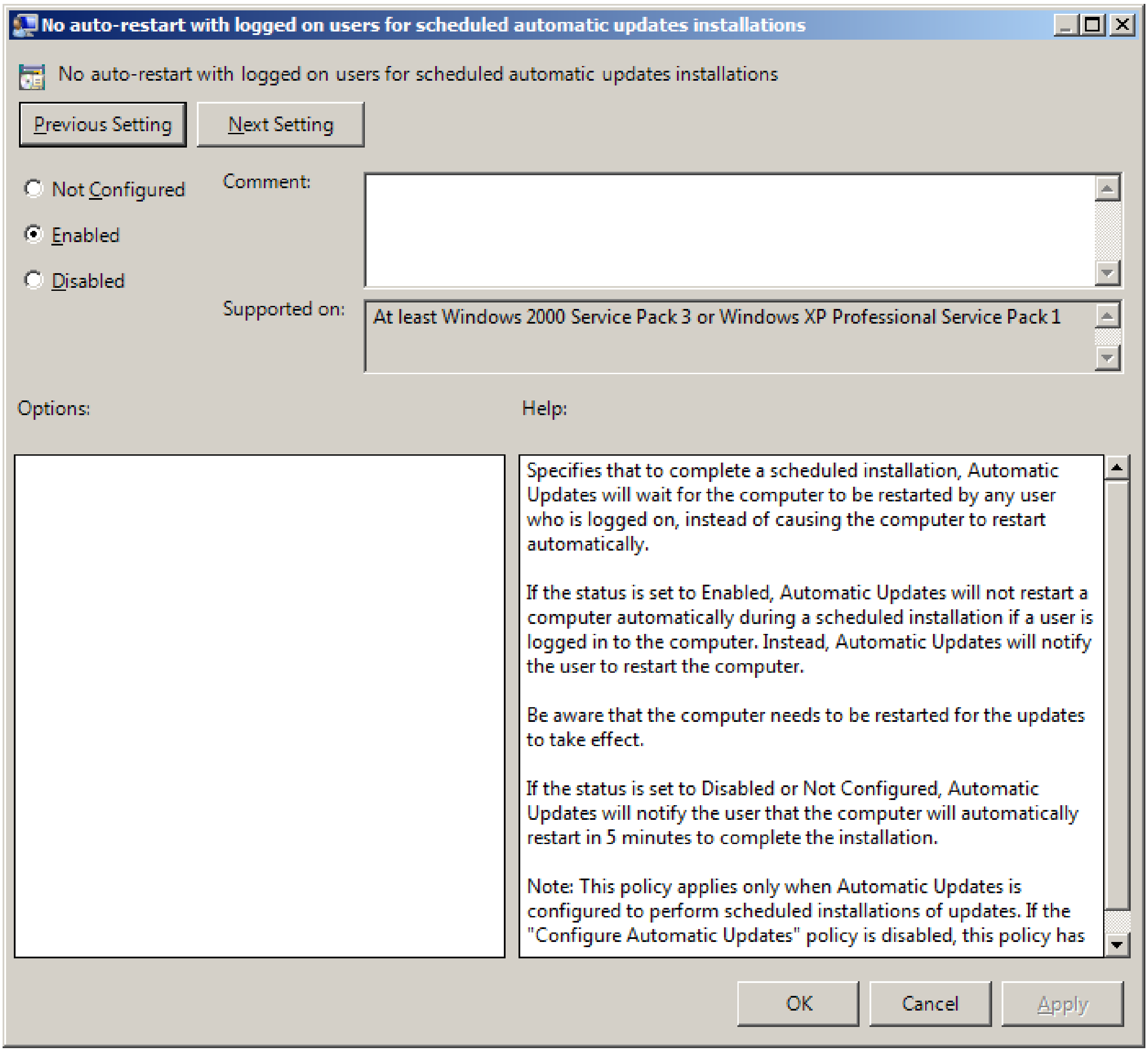
If the status is set to Enabled, the specified target group information is sent to the intranet Microsoft update service which uses it to determine which updates should be deployed to this computer.

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

6.2.3 Firewall rules

The following firewall rules apply to the access of the WSUS server in the Perimeter network to computers in the PCN via the back-end firewall or triple-homed firewall:

- Access rules between the WSUS server and a computer in the PCN

Name	Action	Protocols	From	To
Perimeter WSUS to PCN ... #1	Allow	HTTP HTTPS	IP address of WSUS server	IP address of client
PCN … to Perimeter WSUS #1	Allow	HTTP HTTPS	IP address of client	IP address of WSUS server

The following firewall rules are required for access of the WSUS server in the Perimeter network to the external network for downloading the security and critical updates via the front-end firewall or triple-homed firewall:

- Access rules for firewall rule for updating via the Microsoft pages

Name	Action	Protocols	From	To
Allow Windows Update access to WSUS or External	Allow	HTTP HTTPS	IP address of WSUS server	Microsoft Update Sites *.download.windowsupdate.com *.update.microsoft.com *.windowsupdate.com *.windowsupdate.microsoft.com

- Access rules for updating via a higher-level WSUS server

Name	Action	Protocols	From	To
Allow Windows Update access to WSUS or External	Allow	HTTP HTTPS	IP address of WSUS server	IP address of higher-level WSUS server

Note

You can find the complete range of products for automation firewalls in the PCS 7 Add-on catalog. You can download this catalog from the SIMATIC PCS 7 website (https://www.automation.siemens.com/mcms/process-control-systems/en/distributed-control-system-simatic-pcs-7/Pages/).

6.3 Manual update

For the manual update, the required updates must be downloaded first from the Microsoft Download Center to any existing computer. For this purpose, the correct operating system version (server operating system, Windows XP or Windows 7) must be ensured.

After the download and, if necessary, transfer of the updates to the target systems, the updates must be installed separately. Process management (WinCC Runtime) must be stopped before the installation with an OS server or OS client.
Run the setup and follow the instructions on the screen. A restart may be required after the installation.

Note

This guideline is valid only as of PCS 7 V6.1 SP1
The procedure described above does not apply to new Microsoft Service Packs, the use of which is still subject to an explicit release. If the updates require a later version of the Microsoft software, read the PCS 7 Readme or use the compatibility tool (http://support.automation.siemens.com/WW/view/en/2334224) to ensure that these later software versions or service packs have been approved for SIMATIC PCS 7.

Protection against malware using virus scanners 7

7.1 Overview

Introduction

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:

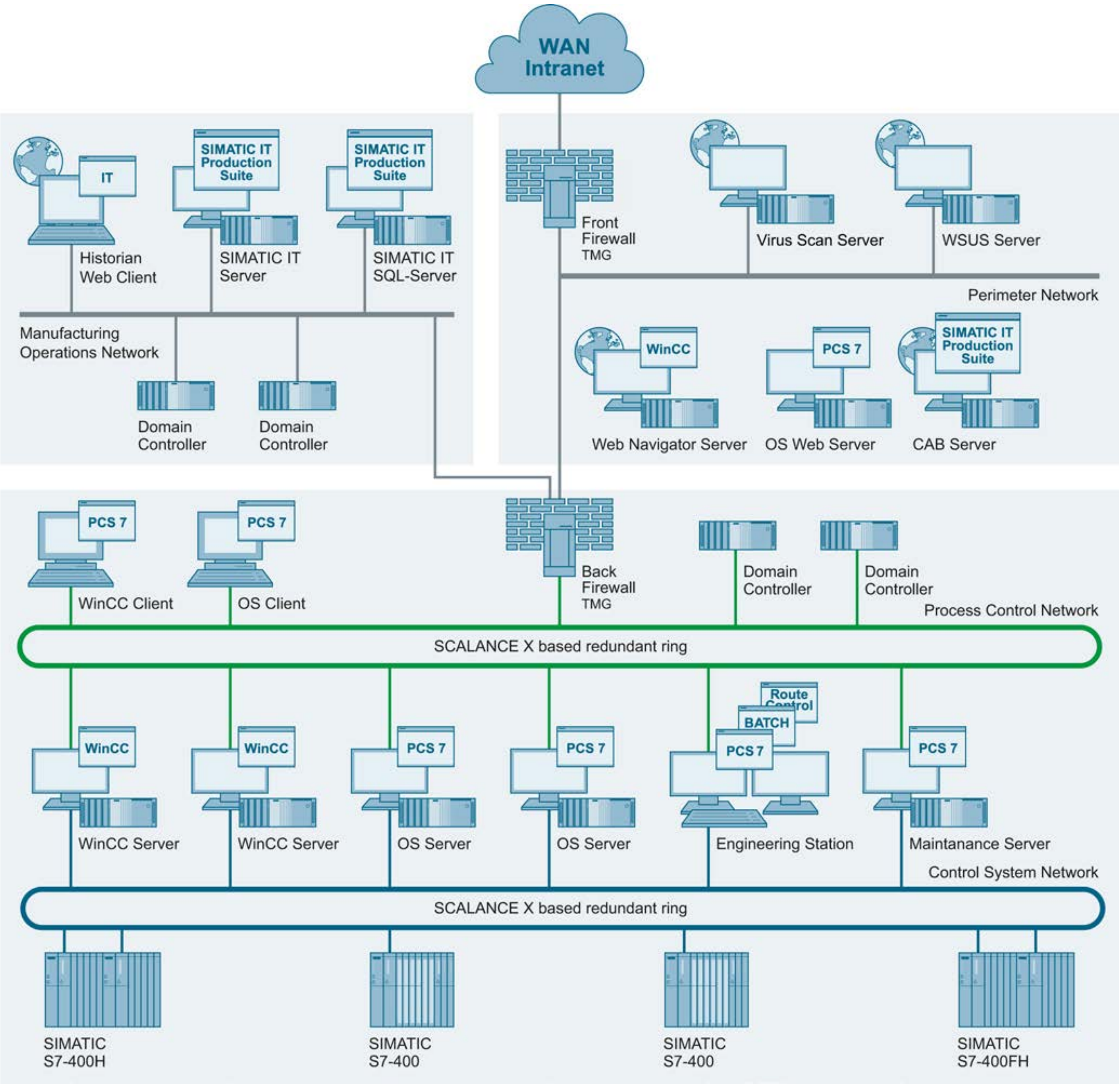
- Computer viruses
- Computer worm
- Trojan horse
- Other potentially dangerous programs, for example:
  - Backdoor
  - Spyware
  - Adware
  - Scareware
  - Grayware

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 scanner client is a computer that is checked for malware and managed by the virus scanner server. This means the PCS 7 OS server and OS clients as well as batch servers and batch clients are also virus scanner clients just like engineering stations or even maintenance servers.

In accordance with the rules for dividing the components into security cells, the virus scanner server must be singled out in a separate network (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 triple-homed firewall, can be used. The virus scanner server must be configured in the Perimeter network using the Industrial Wizard to configure the rule set for the back-end firewall or the triple-homed firewall.

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 triple-homed firewall), but also the configuration of the virus scanner server.

Firewall rules

For the virus scanner server in the Perimeter network to access the virus scanner clients in the PCN via the back-end firewall or triple-homed firewall, the following firewall rules apply.

- 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	HTTP HTTPS McAfee	IP address of virus scan server	IP address of virus scan client
PCN … to Perimeter virus scan server #1	Allow	HTTP HTTPS McAfee	IP address of virus scan client	IP address of virus scan server

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

- 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 overlapped Pattern Update Server or External	Allow	FTP over HTTP HTTPS	IP address of virus scan server	PatternUpdateSet ftp://ftp.nai.com http://update.nai.com

- 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 overlapped Pattern Update Server or External	Allow	FTP over HTTP HTTPS	IP address of virus scan server	PatternUpdateSet ftp://ftp.nai.com http://update.nai.com

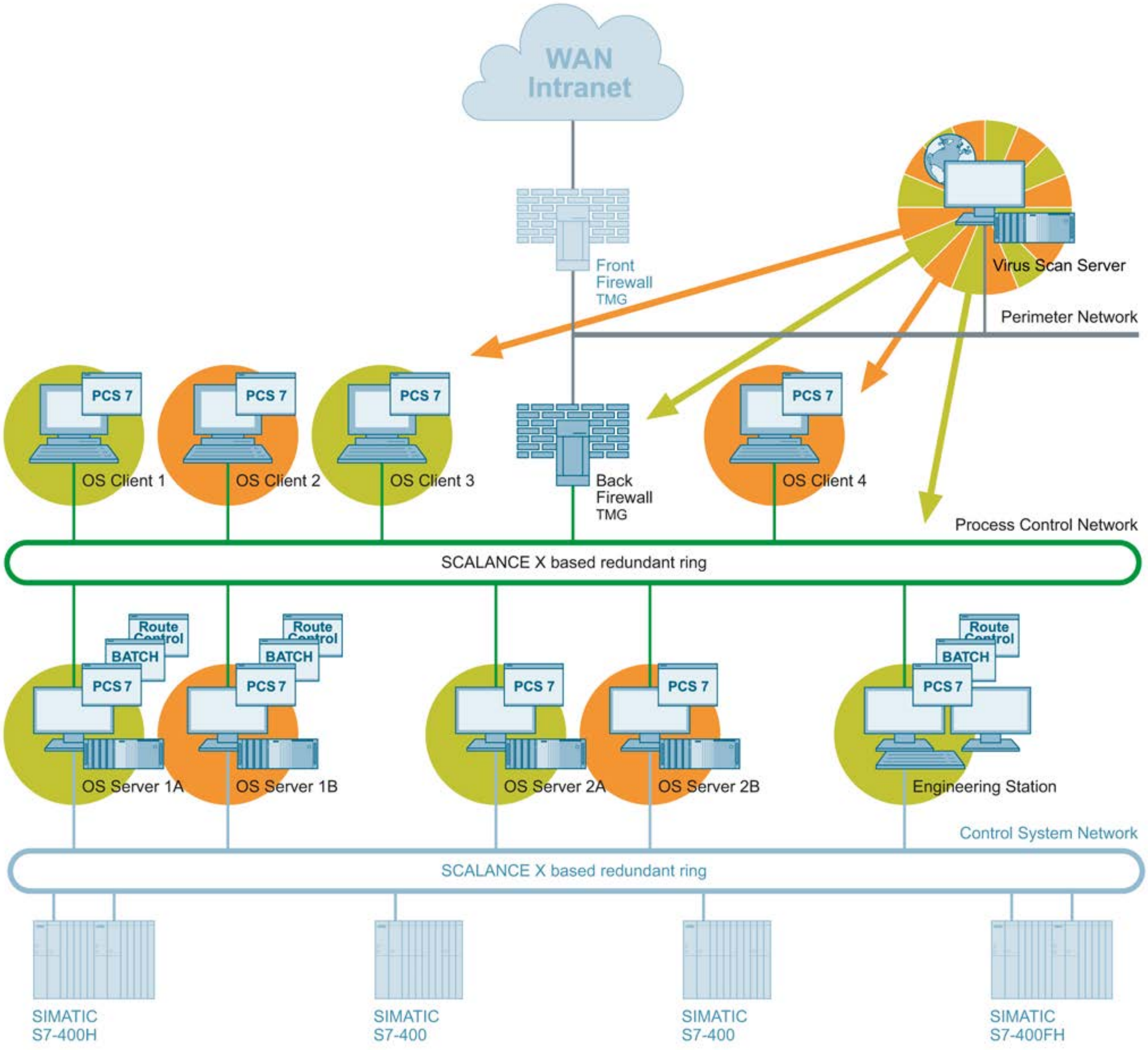
Note

You can find the complete range of products for automation firewalls in the PCS 7 Add-on catalog. You can download this catalog from the SIMATIC PCS 7 website (https://www.automation.siemens.com/mcms/process-control-systems/en/distributed-control-system-simatic-pcs-7/Pages/).

Distribution of virus signature files

To distribute the virus signature files from the virus scanner server to the virus scanner clients, we recommend forming project-specific computer groups (computer groups in patch management).

The following figure shows an example for forming 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" (http://support.automation.siemens.com/WW/view/en/38625951)
- FAQ "With what are SIMATIC PCS 7 V8.x, V7.x, V 6.x, V5.x and V4.x compatible?" (http://support.automation.siemens.com/WW/view/en/2334224)

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

- McAfee VirusScan (V8.5; V8.5i; V8.7) Configuration (http://support.automation.siemens.com/WW/view/en/38006821)
- McAfee VirusScan Enterprise 8.8 Configuration (http://support.automation.siemens.com/WW/view/en/66475606)
- Trend Micro OfficeScan 10.6 Configuration (http://support.automation.siemens.com/WW/view/en/59569279)
- Trend Micro OfficeScan V8.0 Configuration (http://support.automation.siemens.com/WW/view/en/38006929)
- Trend Micro OfficeScan V7.3 including Patch 2 Configuration (http://support.automation.siemens.com/WW/view/en/38006151)
- Symantec AntiVirus V10.2 configuration (http://support.automation.siemens.com/WW/view/en/38006339)
- Symantec Endpoint Protection 11.0 Configuration (http://support.automation.siemens.com/WW/view/en/38004530)

7.2 Procedure following a virus infection

Introduction

No general procedure can be recommended in the event of a virus 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) can also be used for this purpose.

Before loading an image, you should first check whether the storage location of the image is not infected as well. 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 shutdown phase
- 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 viral 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 (perhaps different antivirus solutions) for distributing data
  - Internet access via separate workstation with up-to-date virus scanner (perhaps different antivirus solutions)
- Listing of all network nodes and their tasks
  Backup of all the current data (engineering data, archives, backups, etc.) for each node.
- Import, scan, clean and archive the current data for each network node on the file server
- Planning the required redundancies (when cleaning during ongoing operation)
- Identify standby components; create a memory dump; analyze and examine the memory dump with the purpose of identifying the malware as well as its spreading mechanism
- Reinstall the component either from the system backup (if available and not harmful with respect to infection) or via original data medium (operating system recovery CD and automation components)
- Recommission the cleaned, reinstalled components in the quarantine network as the new master
- Transfer "clean" data (engineering data, archives, backups, etc.) from the file server to the cleaned, reinstalled component in the quarantine network
- Verify and adapt the security design of the plant
- Verify and adapt the security design in the "Quarantine" network
- Step-by-step "rebuilding" of the plant in the "Quarantine" network with cleaned, reinstalled components
- Expand the "Quarantine" network to the new automation network with the adapted measures of the security concept
- Step-by-step implementation of the measures from the security design in the "Quarantine" network

Additional information

Support for implementing a virus protection in form of virus scanners in your plant is available from the Industrial Security Services. You can find additional information and the corresponding contacts at http://www.industry.siemens.com/topics/global/en/industrial-security/Pages/default.aspx.

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

Backing up and restoring data 8

If a security incident, such as a malware infection, occurs (see section "Procedure for a virus infection" (Page 149)) or a storage medium fails (hard disk crash), regular creation of backups is absolutely necessary in order to purge the automation system and thereby re-establish the smooth and trouble-free operation as quickly as possible.

Two types of backups are differentiated here:

- Backup of engineering data (project backup)
- Backup of the system
  A system backup backs up the system partition. This means that the volume is backed up with the following data:
  - Hardware-specific files (for example "Ntldr", "Boot.ini" and "Ntdetect.com")
  - Windows operating system files
  - The installation of the operating system
  - The installation of all programs

8.1 Backup strategy

The backup strategy must be planned according to the type of defense-in-depth (see section "Concept of "defense in depth" (Page 11)") 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)
- Storage or storage location of backups
- Archiving of the backups

8.1.1 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, which means all data of the operating system (Windows XP, Windows 7, Windows Server 2003 or 2008R2)
- All installed programs, for example SIMATIC Manager and WinCC
- All required device-specific drivers, for example, for graphics, network

All these data are usually located on the system partition (C: \). A system backup therefore involves backing up the entire system partition (C: \).

8.1.2 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 to create a project backup therefore depends on the frequency of changes and should be set accordingly.

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 required 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, new software (e.g. a security update or a major update) is installed on a system component, a new system backup must be created for this system component.

Note

The product "Symantec System Recovery" has been tested for compatibility with SIMATIC PCS 7.

8.2 Storage location of backups

Project and system backups should be stored in a secure location. The criteria for "secure" locations must be determined in each case by the operator within the context of the organizational security (IT Security Management Plan). The following points should be taken into account in this regard:

- Buildings
- Fire zones or fire areas

8.3 Archiving

Backups, especially project backups should be archived. The requirements for archiving backups must be determined individually by the operator within the context of the organizational security (IT Security Management 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" (http://support.automation.siemens.com/WW/view/en/68157287), section "Data backup"
- Manual "SIMATIC Process Control System PCS 7 Compendium Part D – Operation and Maintenance"
- FAQ "How do you create a backup of the OS systems during operation?" (http://support.automation.siemens.com/WW/view/en/56897157).

Remote access 9

9.1 Secure remote maintenance based on the Siemens Remote Service platform

Introduction

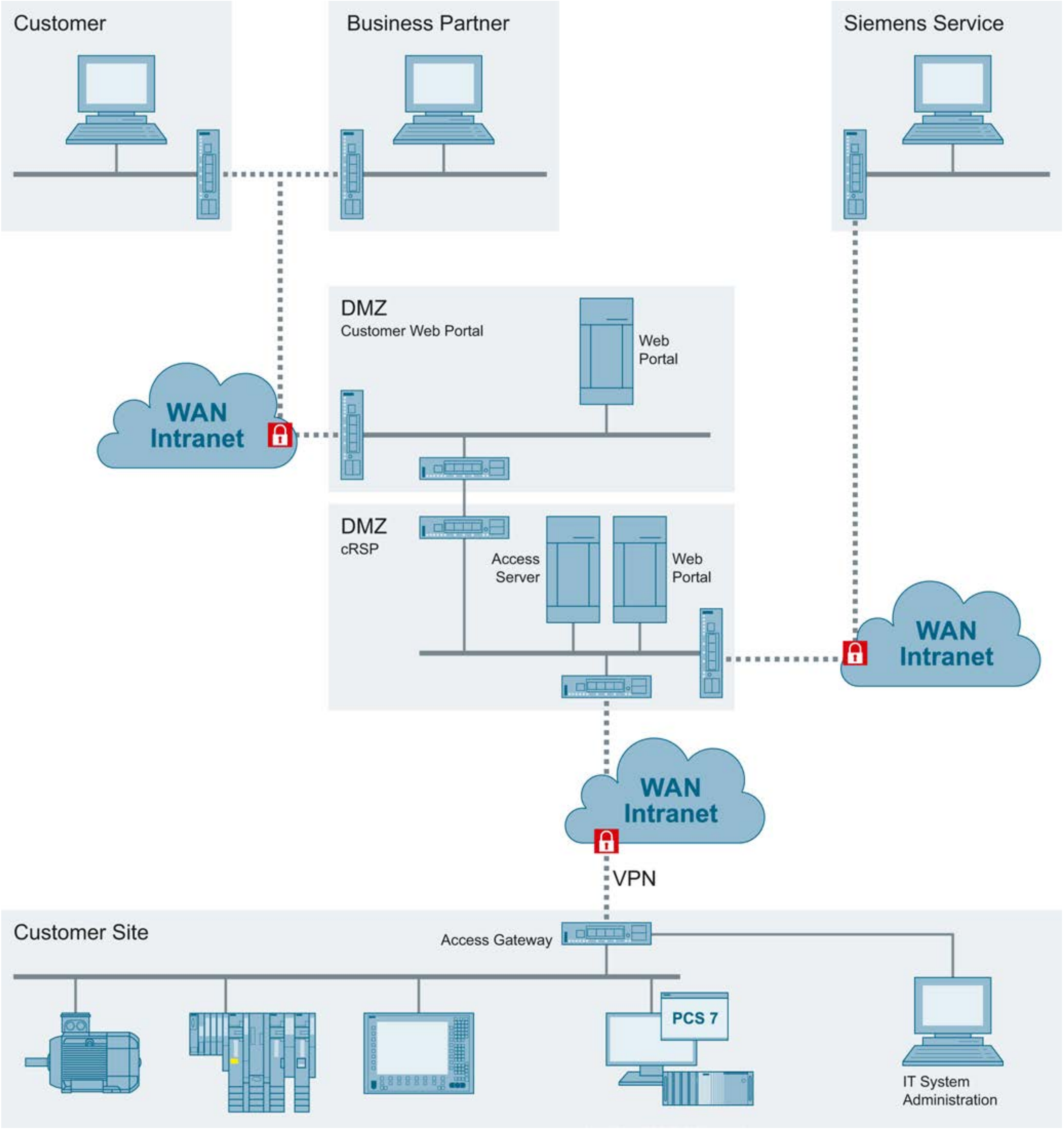
Optimal proactive, system-specific support for the automation system from remote locations: This is the idea behind the Siemens Remote Services platform. Thanks to its modular design, SIMATIC Remote Services can be optimally adapted to actual requirements. The available modules not only include those for remote infrastructure, but support and maintenance are possible as well.
Since the SIMATIC Remote Services are based on the SIEMENS Remote Service (SRS) platform, plant operators work with a safe, high-performance, and fault-tolerant platform for remote access to their SIMATIC automation systems.

The platform

The SIMATIC Remote Support Services are based on the Siemens Remote Service platform. This provides a secure, high-performance, and fault-tolerant remote connection.

- Tiered security and access concept
- Collaboration & Customer Web Portal
- Central monitoring, logging and reporting
- E-mail notification
- Transparent access at any time
- Hard authentication
- Encrypted communication using SSL and VPN

The following figure shows the architecture of the SIEMENS Remote Service platform:



9.2 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, 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 mapped electronically on the SIEMENS Remote Service platform and provide functional remote service access based on a minimalist design. 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.

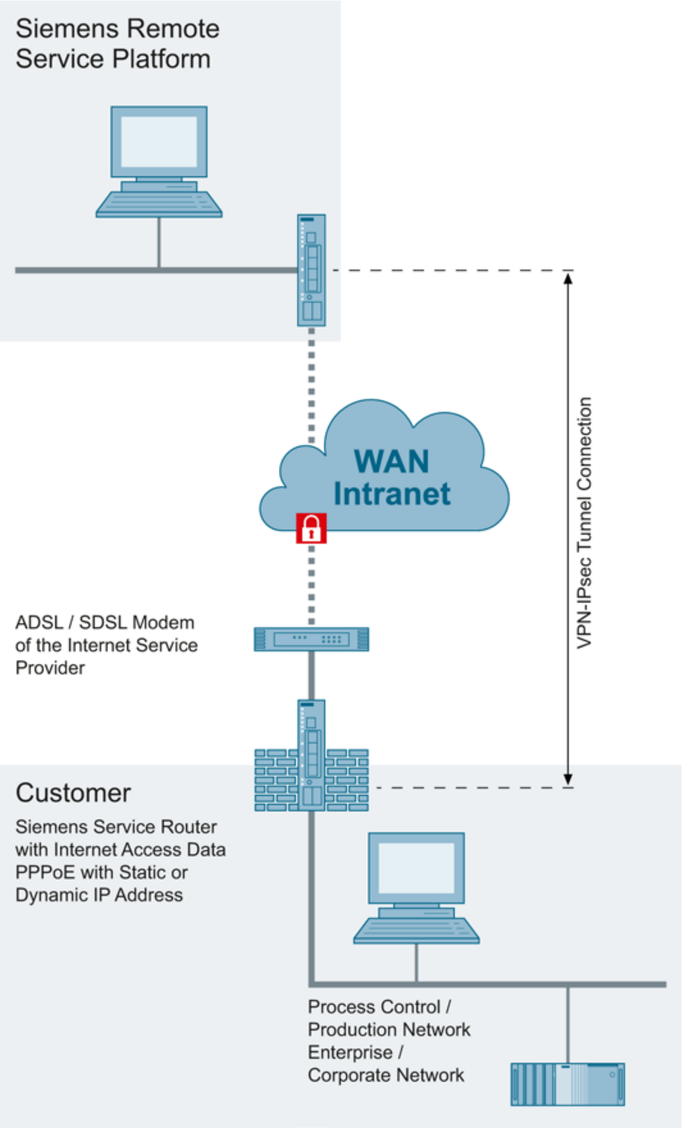
9.3 Connectivity to the Siemens Remote Service platform

The Siemens Remote Service platform provides a central infrastructure. The systems for remote maintenance only need to be connected. There are various access solutions available for this.

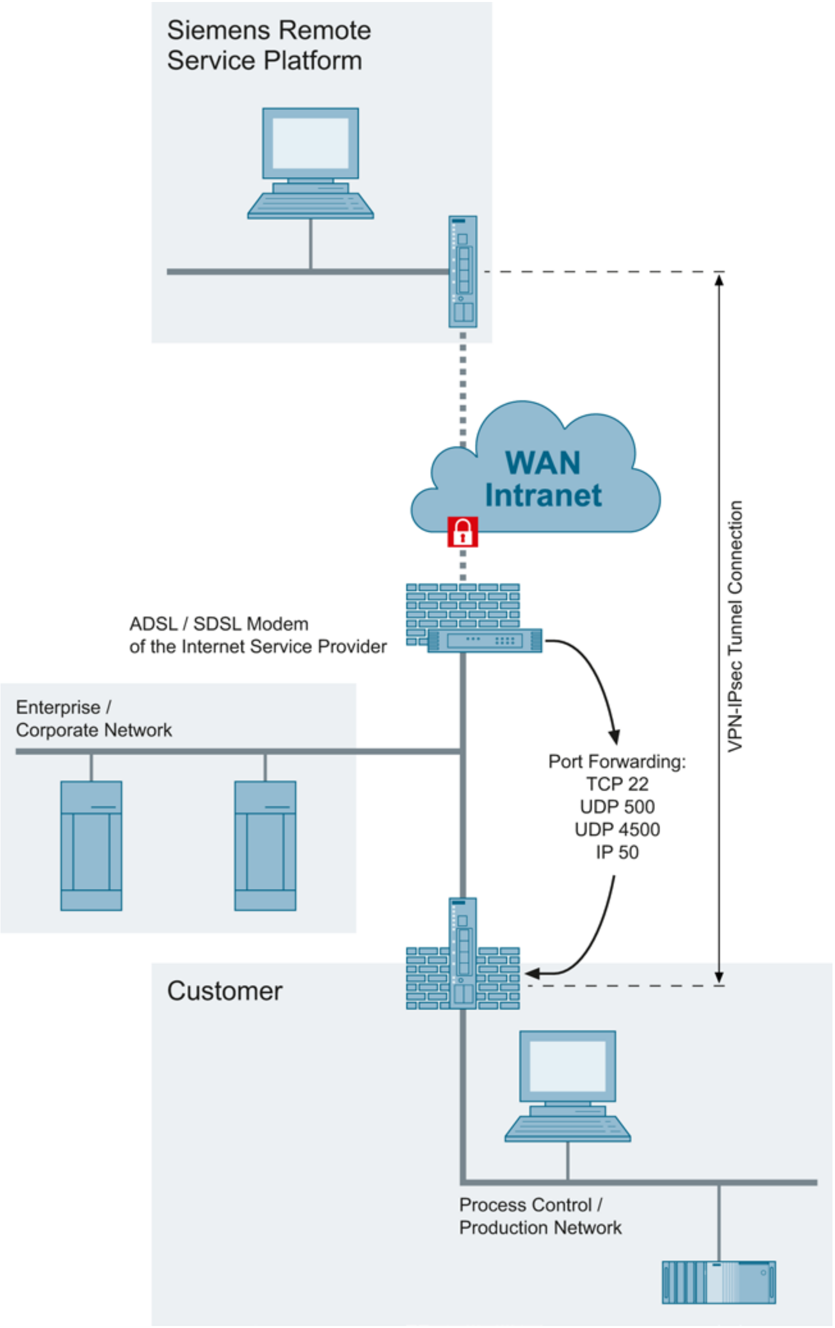
Connectivity installation (SRS DSL/UMTS access)

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

- Internet access via ADSL/SDSL modem
  A service router is supplied and is connected directly to the broadband network via an ADSL/SDSL modem. This connection is used as secure access to the Siemens Remote Service platform. The configuration of the access information for the PPPoE protocol and termination of the IPsec VPN tunnel connection is made in the Siemens service router. The Siemens service router in this case forms the IPsec tunnel endpoint of this connection.

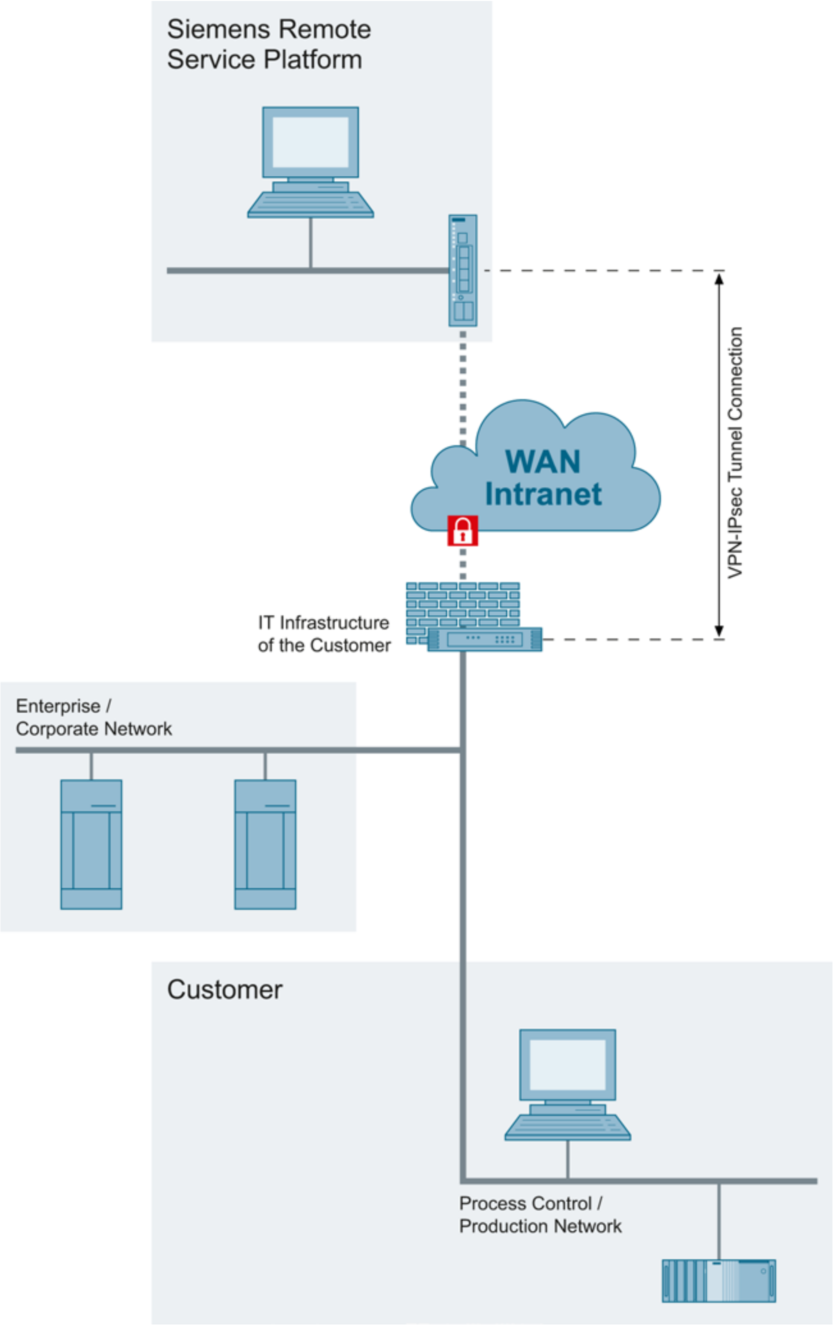


- Use of existing Internet access
  A service router is supplied and is connected to the broadband network via an existing Internet access point. This connection is used as secure access to the Siemens Remote Service platform. The VPN IPsec tunnel connection is terminated after the Internet access point of the customer. The Siemens service router in this case forms the IPsec tunnel endpoint of this connection. Secure transmission of data requires forwarding of the IPSec protected data from the Internet access point of the customer service to the Siemens service router (port forwarding to the SIEMENS service router).



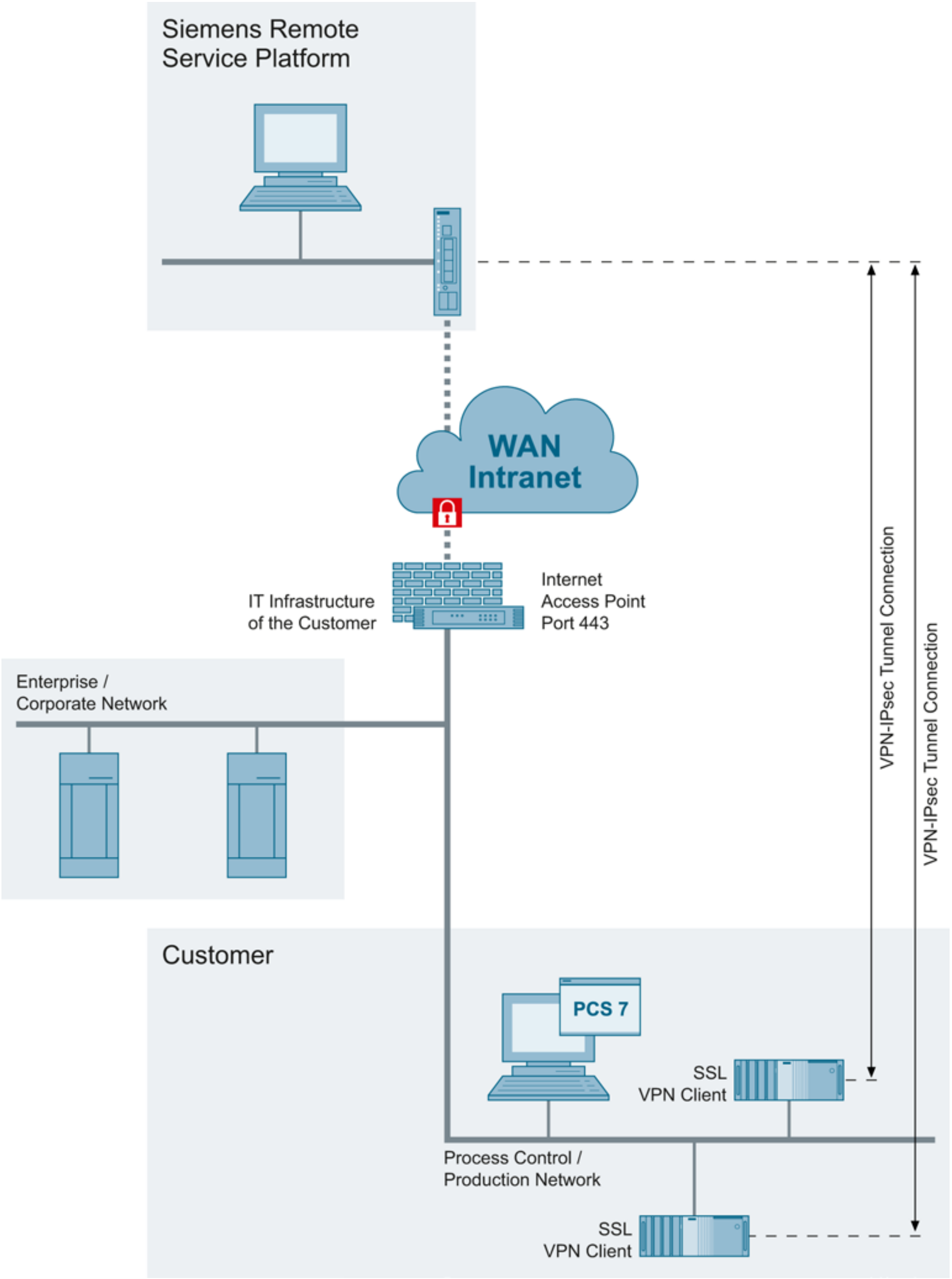
Connectivity installation (SRS customer own access)

An existing IT infrastructure is used as the connection partner to the Siemens Remote Service platform. The termination of the required VPN IPsec tunnel connection is made in the IT equipment of the customer. For secure transmission of data, there is a compliant, standard IPsec endpoint in which a pre-shared secret based IPsec connection can be set up in tunnel mode.


Siemens Remote Service Platform
WAN Intranet
VPN-IPsec Tunnel Connection
IT Infrastructure of the Customer
Enterprise / Corporate Network
Customer
Process Control / Production Network

Connectivity installation (SRS SSL client access)

An SSL VPN client software is provided, which establishes a connection to the Siemens Remote Service platform via an Internet access (port 443) using the existing IT infrastructure. The VPN IPsec tunnel connection is terminated on the client system after the Internet access point. The SSL VPN client installed on the target system in this case forms the IPsec tunnel endpoint of this connection. The connection is established from the SSL VPN client to Siemens Remote Service platform.


Siemens Remote Service 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

10 Definitions and Abbreviations

The following table shows the abbreviations used in this document:

Abbreviation/acronym	Explanation
Active Directory	Directory service of Microsoft Windows Server
CSN	Control System Network (plant bus)
DC	Domain Controller
DCS	Distributed Control System
DMZ	Demilitarized Zone
DNS	Domain Name System
ECN	Enterprise Control Network
ERP	Enterprise Resource Planning
ES	PCS 7 Engineering Station
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
PCN	Process Control Network (terminal bus)
PCN1	Production cell 1
PCN2	Production cell 2
PCS 7	Process Control System from Siemens
PN	Perimeter Network
SC	Security Controller
SCT	Security Configuration Tool
SSC	SIMATIC Security Control
TMG	Microsoft Forefront Threat Management Gateway
WINS	Windows Internet Naming Service
WSUS	Windows Server Update Services