SIEMENS

SIGUARD PDP
Phasor Data Processing

V2.11

Administrator Guide

E50417-H1076-C496-A2

NOTE

For your own safety, please observe the warnings and safety instructions contained in this manual.

Document version: E50417-H1076-C496-A2.00

Release status: 01.2012

Version of the product described: V2.11

Preface

Purpose of the Manual

This manual is a set of instructions for the software SIGUARD PDP. You obtain an overview of the possibilities for use and configuration.

Target Audience

This manual is addressed mainly to the operating crew, commissioning engineers, and quality managers who are responsible for the configuration, parameterization, and monitoring of power systems and their components.

Scope of Application of this Manual

This manual applies to SIGUARD PDP V2.10.

Standards

SIGUARD PDP was developed in compliance with guidelines in DIN EN ISO 9001:2008.

Additional Support

For questions about the system, please contact your Siemens sales partner.

Support

Our Customer Support Center provides a 24-hour service.

Tel.: +49 (1805) 24-7000

Fax: +49 (1805) 24-2471

E-mail: support.ic@siemens.com

Training Courses

Inquiries regarding individual training courses should be addressed to our Training Center:

Siemens AG

Siemens Power Academy

Humboldtstraße 59

90459 Nuremberg

Tel.: +49 (911) 433-7415

Fax: +49 (911) 433-5482

E-mail: td.power-academy.energy@siemens.com

Internet: http://www.siemens.com/energy/power-academy

Safety Information

This manual is not a complete index of all safety measures required for operation of the equipment (module, device). However, it comprises important information that must be noted for purposes of personal safety, as well as in order to avoid material damage. Information is highlighted and illustrated as follows according to the degree of danger.

DANGER

DANGER means that death or severe injury **will** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid death or severe injuries.

WARNING

WARNING means that death or severe injury **may** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid death or severe injuries.

CAUTION

CAUTION means that medium-severe or slight injuries **can** occur if the specified measures are not taken.

✧ Comply with all instructions, in order to avoid medium-severe or slight injuries.

NOTICE

NOTICE means that material damage **can** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid material damage.

NOTE

Important information about the product, product handling, or a certain section of the documentation, which must be given particular attention.

Table of Contents

1 Overview

1.1 General

This manual is intended for the system administrator working for the operator of the SIGUARD PDP system. It describes the network structure and gives instructions for improving the security in the network.

The manual consists of the following main parts:

- General rules for system security
- Instructions for network topology
- Installation of the SIGUARD PDP components
- Time synchronization
- Details on security settings

1.2 Recommended Actions that Make Your System More Secure

In order to make your SIGUARD system more secure, take note of the following points:

- Create a list of the services (ports and protocols) that are used in the IT system. You can use this list to configure the firewall in your system.
- Follow the recommendation to activate the Windows Desktop Firewall and go by the description of which ports must be opened for incoming data traffic.
- Deactivate all unnecessary services, for example, **File and Printer sharing for Microsoft networks**.
- Create a special Windows user group **Users** for your installed program. Only this user group may have the authorization to launch the corresponding program and to navigate to the folders. This user group may be granted only read access to the shared folder of the SIGUARD PDP Server.
- Create users who are members of the Windows user group **Users** and the defined user group, for example, **SIGUARD PDP Engineer**.

  Do not use an administrator account for normal work on the computer.

  Only the defined users may be authorized to use the installed program, but not normal Windows users. This procedure ensures a high degree of security and prevents intrusion of malware, such as foreign DLL or EXE files.
- If there is direct access to the Internet, always activate the automatic update function in Windows and update all software products from third parties, such as Adobe Acrobat Reader, for example, or the Oracle Java runtime environment. Many other programs offer an automatic update service. If there is no direct access to the Internet, you can update the software manually or run WSUS (Windows Server Update Service).
- In order to prevent intrusion of malware via storage media (CD-ROM, USB stick, among others) or via shared data usage, install an approved virus scanner on your system with the setting **on access**.

  If there is direct access to the Internet, then take note that only virus software updated daily with virus signatures ensures a high degree of security. For all systems, the virus signatures must be made available automatically or manually.
- To guarantee the completeness and the discretion of the data transmitted between the user interface and the SIGUARD PDP Server, the data can be encrypted. For this, the IPSec function implemented in Windows is used to make the data transmission more secure.

  Further information on this can be found in chapters *7.5.2.1 General* and *7.5.1.1 General*.
- In order to communicate with other partners, use the IPSec solution integrated in Windows for a secure and authenticated data connection, using simple text protocols. If you use a firewall, enable the IPSec protocol (ESP/UDP Port 500 or UDP Port 4500/UDP Port 500).

  Further information on this can be found in chapters *7.5.1.1 General* and *7.5.2.1 General*.
- Use the **Windows Task Scheduler** to back up the engineering data to an external drive or a shared folder on a regular basis. This ensures that the engineering data can be restored without or with little data lost in a system failure.
- Collect and store the protocol files within a certain time frame. Remote access to the protocol files of the SIGUARD PDP Server occurs via the **Remote Registry Service** available in Windows. The **Event Viewer**, a standard program by Microsoft, is used.

1.3 Recommended Rules for Improving the Security Process

To ensure the security process for your SIGUARD-System, adhere to the following rules:

- Never use the Windows user account **Guest**. Always deactivate this user account!
- Allow access only if absolutely necessary and only for the appropriate user groups. Delete the group for these access rights and add the correct user group. Set the read and write access with the **Security Function**.
- Do not use any account that belongs to the administrator group for normal work on your computer.
- Do not use any simple passwords for the user account. Adhere to the rules for passwords that apply in your company.
- If possible, change your password at regular intervals.
- Do not work in Windows without activating the Desktop Firewall, unless you have a reliable, limited security zone installed on your system.
- Furthermore, work only with Windows updated with patches if your system is not installed within a reliable and limited security zone.
- Do not work in Windows without a current virus scanner, unless your system is installed within a reliable, limited security zone.
- Whenever possible, do not use third-party software with known security gaps. If necessary, set up a reliable, limited security zone.
- Do not install any unreliable software on the system with which you are working.

■

2 Network Topology

2.1 Overview

In this chapter, you find an overview of the security configuration of the SIGUARD network. The SIGUARD network is not a self-standing network, but rather a distributed system. The system is connected to different network zones that must satisfy different security requirements.

For this reason, Siemens recommends implementing the concept for secured networks described here. If you have defined your own, limited security zones with strict security conditions, one or 2 security tunnels or mechanisms can be dispensed with, as necessary.

2.2 Network Configuration

The following figure shows an example of a network configuration for the SIGUARD system. Normally, the PMUs are distributed at station level statewide. A separation of the SIGUARD PDP Server, the SIGUARD PDP UI computer, and the SIGUARD PDP Engineer computer is possible. Alternatively, the configuration may consist of a system at the office level with a joint UI and Engineer environment.

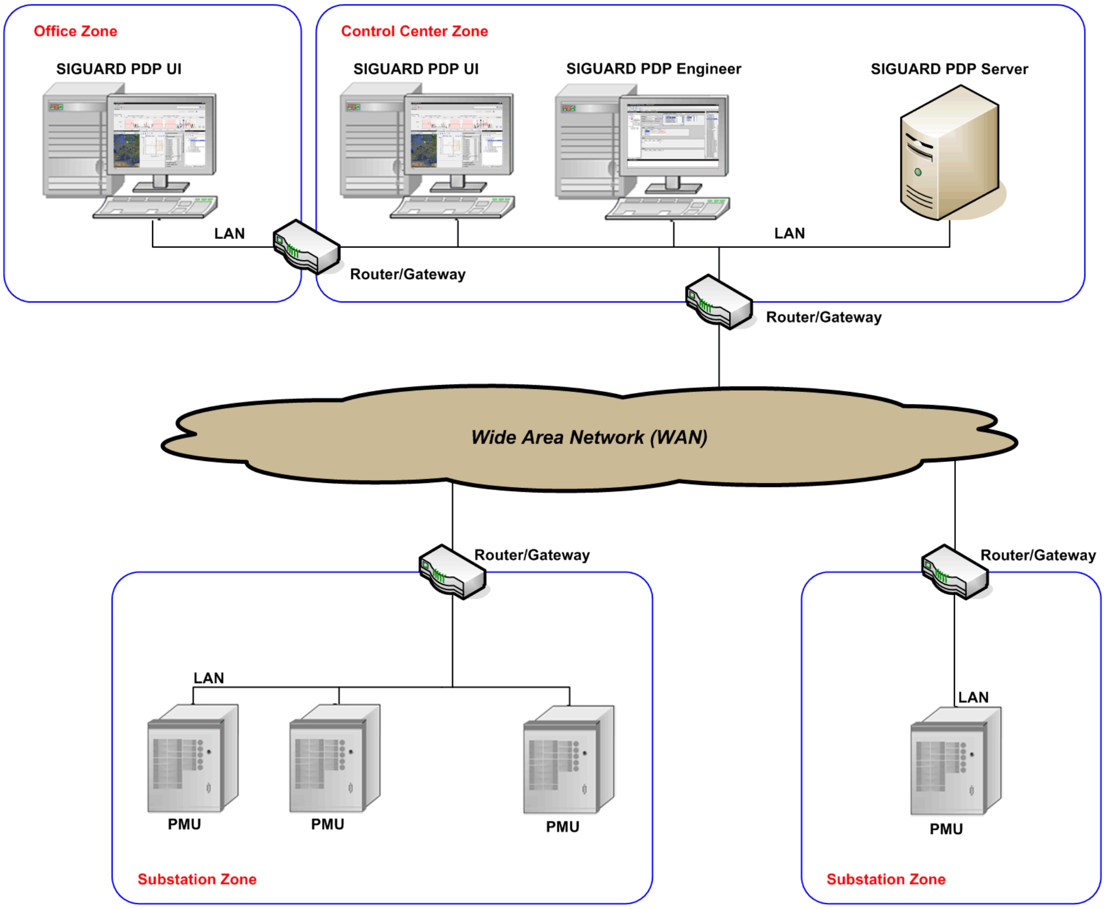


Figure 2-1 Network Configuration (Example)

2.3 Network Configuration with IPSec

With this configuration, you can achieve encrypted data traffic:

- Between the programs SIGUARD PDP UI, SIGUARD PDP Engineer, and SIGUARD PDP Server
- Between the PMU and the SIGUARD PDP Server

In many PMUs, IPSec is not supported directly in device communication. For this reason, additional hardware, the **Siemens Scalance S Security Module**, is required. Configuration and operation of the Scalance S Security Module is simple. The other security tunnels can be configured via a Windows-native application.

You can find more information on configuration in chapter *7.5.1.2 IPSec Configuration*.

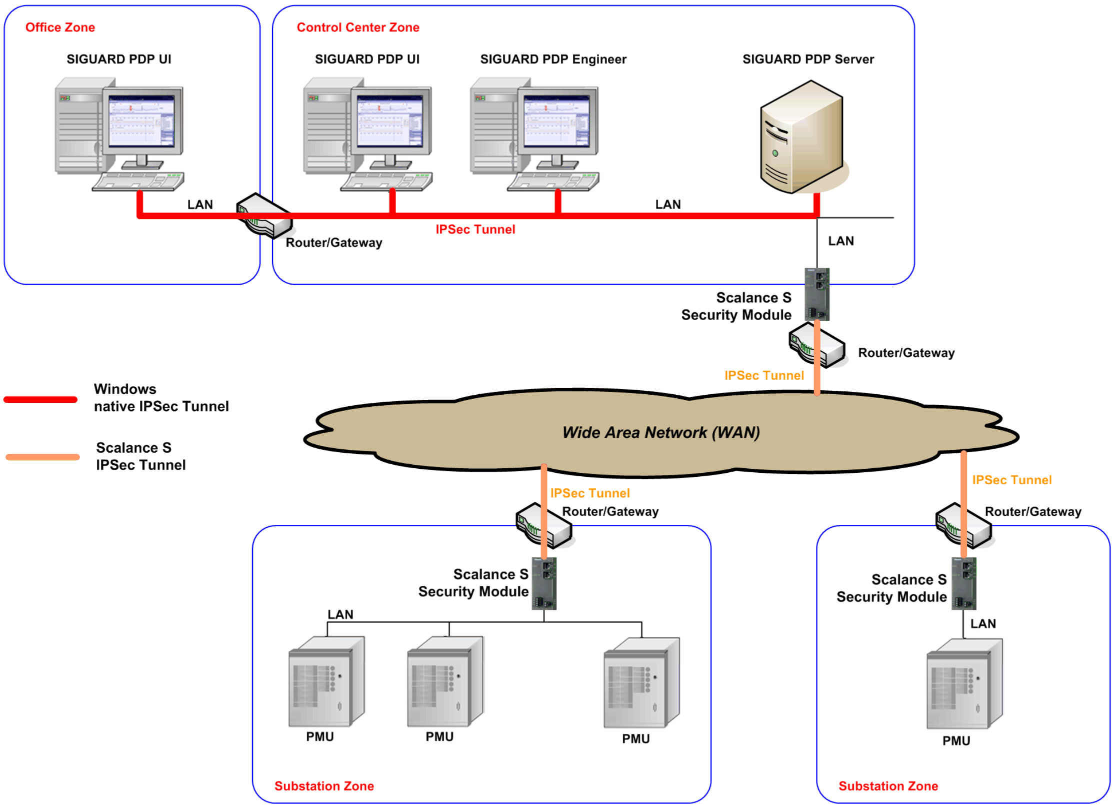


Figure 2-2 Network with Windows-Native IPSec Tunnel and Security Module Scalance S

2.4 Communication Protocols for the Use of a Firewall

The services that are used by the SIGUARD PDP Engineer/UI computer for external access to the SIGUARD PDP Server are listed in the following. Note that the Microsoft Network Discovery Service is optional. If you do not need a browser, deactivate this service via the function **Services** and/or via **Microsoft Desktop Firewall**.

NOTE

The TCP communication between SIGUARD PDP Server and PMU is freely definable via SIGUARD PDP Engineer. TCP communication is only an outgoing connection from the SIGUARD PDP Server.

Table 2-1 Communication Matrix

Service	Protocol Layer 4	Protocol Layer 7	From host (client)	From port (client)	To host (server)	To port (server)
Microsoft Network Discovery	TCP	Microsoft Network Browsing (http) Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	SIGUARD PDP Engineer/ UI computer		SIGUARD PDP Server	5357
SIGUARD Service Interface	TCP	SIGUARD Service Interface	SIGUARD PDP Engineer/ UI computer	> 1024	SIGUARD PDP Server	59152
File Sharing	TCP	netbios-ssn	SIGUARD PDP Engineer/ UI computer	> 1024	SIGUARD PDP Server	139
File Sharing	TCP	netbios-ssn	SIGUARD PDP Engineer/ UI computer	> 1024	SIGUARD PDP Server	445
PMU protocol (C37.118)	TCP	PMU protocol (C37.118)	SIGUARD PDP Server	> 1024	PMU	Freely definable

■

3 SIGUARD PDP System Installation

3.1 Installation Requirements

3.1.1 Hardware

The following hardware requirements apply to the SIGUARD system:

Table 3-1 Hardware Requirements for SIGUARD

Hardware		**Minimum Requirements**	**Recommended Requirements**
SIGUARD PDP Server	Processor	Dual Core	Quad Core
	Clock frequency	2.0 GHz	≥ 2.5 GHz
	Primary storage (32-bit operating system)	2 GB	4 GB
	Free hard disk space	4 GB (operating system) Archive, see below	
	Graphics card	Standard graphics card	DirectX V9.0c compatible
	USB port	USB 2.0	
	Network interface	100 Mbit/s	1 GBit/s
SIGUARD UI computer	Processor	Dual Core	Quad Core
	Clock frequency	2.0 GHz	≥ 2.5 GHz
	Primary storage (32-bit operating system)	2 GB	4 GB
	Primary storage (64-bit operating system)	4 GB	8 GB
	Free hard disk space	10 GB (UI, Google Earth)	
	Graphics card	DirectX V9.0c compatible	
SIGUARD PDP Engineer computer	See SIGUARD UI computer		

Disk Space for the Archive

For quick processing of the archive (saving, opening), the permanent archive and the ring archive should be placed on 2 separate physical hard disks.

The disk space requirement must be made available in accordance with the following conditions:

Table 3-2 Hardware Requirements for SIGUARD

Hardware		**Minimum Requirements**	**Recommended Requirements**
Ring archive		With the following boundary conditions	
	PMUs/with 8 channels each	8	14
	Channels	64	112
	Repetition rate (values/second)	10	10
	Storage period	7 days	7 days
	Free hard disk space	**Approx. 14 GB**	**Approx. 25 GB**

For storage of events, alarms, and time ranges, additional free hard disk space is required.

HINWEIS

The hard disk where the SIGUARD PDP archive is created must be formatted for the NTFS file system (New Technology File System).

3.1.2 Software

Operating System

The following operating systems are supported:

Table 3-3 Supported Operating Systems

Operating System	SIGUARD Computer		
	SIGUARD PDP Server	**SIGUARD PDP UI Computer**	**SIGUARD PDP Engineer Computer**
Windows XP Professional SP3 (32-bit)	X	X	X
Windows 7 Professional (32-bit)	X	X	X
Windows 7 Professional (64-bit)		X	X
Windows Server 2008 Standard Edition (32-bit)	X		

Other Software Requirements

Install **Google Earth** Version 6.0 (Version V 6.0.3.21790 has been tested).

NOTE

Adhere to the license requirements for the open source software that is used with SIGUARD PDP.

In the root directory of the SIGUARD PDP installations DVD, you find the PDF document **ReadMe_OSS.pdf.**

3.2 Installing the Software

3.2.1 Overview

You set up SIGUARD PDP on your computer via an installer. During installation, you transfer all the necessary data onto your computer:

- SIGUARD PDP
- Automation License Manager
- Service Controller Tool

In order to be able to use SIGUARD PDP, license SIGUARD PDP after installation via the Automation License Manager (see manual *Automation License Manager*).

The installation of the software components **OPC** and **ICCP** is performed during setup of SIGUARD PDP and for ICCP with an additional software add-on. Licensing is performed separately for each software component.

Notes on the installation of the software components can be found in the corresponding chapters in the *Administrator Manual*.

NOTE

You can install SIGUARD PDP and ICCP Add-on in whatever sequence you select.

3.2.2 Installation

Starting Installation

You install SIGUARD PDP as follows:

✧ Insert the DVD with **SIGUARD PDP** into your DVD drive.

The installation procedure starts automatically.

If the installation procedure does not start automatically, double-click the file **Setup.exe** in the root directory of the DVD.

✧ Follow the instructions of the installer.

Installation Type

During the installation, you must define the **Installation Type**.

NOTE

There must always be one server present in a SIGUARD PDP System. Up to 8 SIGUARD PDP UIs can be operated by this server.

NOTE

The SIGUARD PDP Engineer is installed along with SIGUARD PDP UI. There is no separate installation option with SIGUARD PDP Engineer.

- When installing a SIGUARD PDP System which is composed of several computers, first install the SIGUARD Server.
- Select between the installation types **Server** and **UI Client**.

When you install SIGUARD PDP UI, enter the computer name on which the SIGUARD Server is being installed.

- When you install SIGUARD PDP Server, select the software components **OCP** and/or **ICCP**, if you want to install them as well.

NOTE

If you want to operate a distributed system (1 server, several UI computers), set up the shares **\\<computername>\SIGUARD_Config** and **\\<computername>\SIGUARD_Export** on the server. Assign rights in accordance with your company policies.

- During installation, establish the path and the directory for the SIGUARD PDP.
- Establish the path for the program.
- Establish the path for the configuration file.
- Establish the CSV file.

NOTE

Siemens recommends saving the ring and the permanent archives on separate hard disks.

- Establish the path for the ring archive.
- Establish the path for the permanent archive.

Restart Computer

- Restart the computer after installation.

3.2.3 Licensing SIGUARD PDP

3.2.3.1 Prepare Licensing

You license the SIGUARD PDP product by transferring the license from one or more license USB stick(s) to your computer with the aid of the Automation License Manager (ALM) (see *Automation License Manager* manual).

Individual licenses for all SIGUARD PDP components or applications are necessary. The license keys are administered exclusively on the SIGUARD PDP Server, that is, the ALM must be installed there, and it is there that the licenses are queried by the SIGUARD PDP Server.

During the runtime, the SIGUARD PDP Server queries the licenses and creates a connection to the SIGUARD PDP UI computer only if the corresponding licensing is present. Licensing is also used to check how many SIGUARD PDP UI computers may be operated on the SIGUARD PDP Server.

NOTE

On a computer with licensing administration (SIGUARD PDP Server), you may not execute any programs which change the partitioning or structure of the hard-disk drives.

This includes programs for hard-disk drive maintenance, such as, for example, repair, defragmentation, or partitioning.

If you use such programs, you risk losing your license!

To prevent this, you must temporarily transfer the license key back to the license USB stick (see also *3.3.2 Removing the SIGUARD PDP License*).

NOTE

If it is not possible to access a USB interface on the SIGUARD PDP Server to which the licenses must be copied, then the licenses must first be installed on the SIGUARD PDP UI computer. To do this, install the Automation License Manager (ALM) on the SIGUARD PDP UI computer. In the root directory of the DVD, there is a link to set up the ALM.

If the licenses are installed on the SIGUARD PDP UI computer and there is a network connection to the SIGUARD PDP Server, they can be transferred with the ALM from the SIGUARD PDP UI computer to the SIGUARD PDP Server.

Access by the ALM that is installed on a SIGUARD PDP Server to a USB stick of a computer connected via a terminal session is no longer possible.

NOTICE

The **C:\AX NF ZZ** folder includes hidden files. You may not delete, move, or copy these files and folders. They contain data that are necessary for licensing your software!

Otherwise, you might lose the license irretrievably. To prevent irretrievable loss of your license, observe the following instructions:

✧ If you use an optimization program (for example, Scandisk/Defrag) that offers the possibility of moving fixed blocks of data, then you may only use this option only after you retransfer the licenses from the hard-disk drive back to the license USB stick.

✧ The license creates a cluster on the destination drive that is marked as defective. Do not attempt to restore this cluster.

✧ If overwriting a system with stored licenses (usually that is the SIGUARD PDP Server, but may also be another computer with licenses stored there) with a backup, you risk losing your license. Therefore, Siemens recommends removing all licenses or to exclude the directory **C:\AX NF ZZ** before creating a backup copy.

NOTE

There is a risk that the license USB stick is infected by viruses on the hard disks. You should therefore run a virus check on your computer every time you install or remove a license.

3.2.3.2 Executing Licensing

You license SIGUARD PDP as follows:

- Place the included license USB stick in the USB port of the SIGUARD PDP Server.
- Click **Start > Programs > Siemens Automation > Automation License Manager**.
- Transfer the license from the license USB stick to the hard disk of the SIGUARD PDP Server.

NOTE

If you have received multiple license USB sticks, then repeat these steps.

3.2.4 Assign Parameters of SIGUARD PDP

After the installation and licensing, create a new project with the tool **SIGUARD PDP Engineer**, parameterize, and activate it.

You can also expand functionalities of an existing project.

For instructions, see the manual *SIGUARD PDP - SIGUARD PDP Engineer - performance properties*.

3.2.5 Launching SIGUARD PDP

3.2.5.1 Overview

After parameterizing and activating a new project, the administrator must open the **Service Controller Tool** on the SIGUARD PDP Server and install and start the services required by **SIGUARD PDP**.

The **Service Controller Tool** must be executed after the reinstallation of the SIGUARD PDP Server. Administrator rights on the SIGUARD PDP Server are necessary to run the tool.

For details, also see *Administrator Manual - Service Controller Tool*.

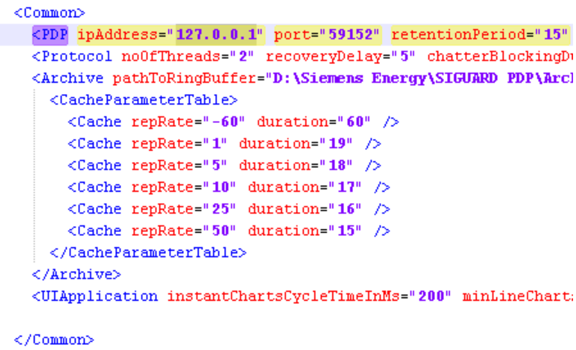
Then, it can be checked in the diagnostic tool **Communication UI**, whether all connections between SIGUARD PDP Server and PMUs has been correctly established and whether errors have occurred.

For this, also see *Administrator Manual - Diagnostic Tool Communication UI*.

3.2.5.2 Editing the Configuration File

If the SIGUARD PDP software is installed on a distributed system (SIGUARD PDP Server and UI-/Engineer computer are separated), then you must enter the IP address of the server in the configuration file. Proceed as follows:

- Open the configuration file **RT/PDP_config.xml** with an appropriate text editor.
- Instead of the IP address present, enter the IP address of the SIGUARD PDP Server.



```
<Common>
  <PDP ipAddress="127.0.0.1" port="59152" retentionPeriod="15"
  <Protocol noOfThreads="2" recoveryDelay="5" chatterBlockingD
  <Archive pathToRingBuffer="D:\Siemens Energy\SIGUARD PDP\Arc
    <CacheParameterTable>
      <Cache repRate="-60" duration="60" />
      <Cache repRate="1" duration="19" />
      <Cache repRate="5" duration="18" />
      <Cache repRate="10" duration="17" />
      <Cache repRate="25" duration="16" />
      <Cache repRate="50" duration="15" />
    </CacheParameterTable>
  </Archive>
  <UIApplication instantChartsCycleTimeInMs="200" minLineChart

</Common>
```

Figure 3-1 Change the IP Address

✧ Save the modified file.

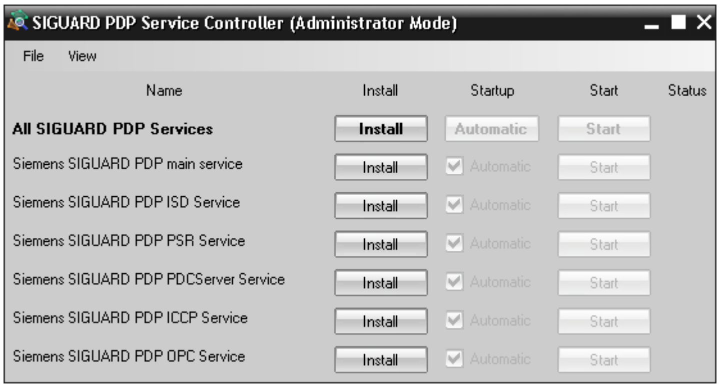
3.2.5.3 Service Controller Tool

The diagnostic tool **SIGUARD PDP Service Controller** can be opened independently of SIGUARD PDP. However, starting the services is a prerequisite for starting SIGUARD PDP.

You run the tool **Service Controller** as follows:

✧ Select **Start > Siemens Energy > SIGUARD PDP > Service Controller**.

The window **SIGUARD PDP Service Controller** is opened.



Name	Install	Startup	Start	Status
All SIGUARD PDP Services	Install	Automatic	Start	
Siemens SIGUARD PDP main service	Install	☑ Automatic	Start	
Siemens SIGUARD PDP ISD Service	Install	☑ Automatic	Start	
Siemens SIGUARD PDP PSR Service	Install	☑ Automatic	Start	
Siemens SIGUARD PDP PDCServer Service	Install	☑ Automatic	Start	
Siemens SIGUARD PDP ICCP Service	Install	☑ Automatic	Start	
Siemens SIGUARD PDP OPC Service	Install	☑ Automatic	Start	

Figure 3-2 Installation of SIGUARD PDP Service Controller, Services

✧ Click the **Install** button to start the service.

-- or --

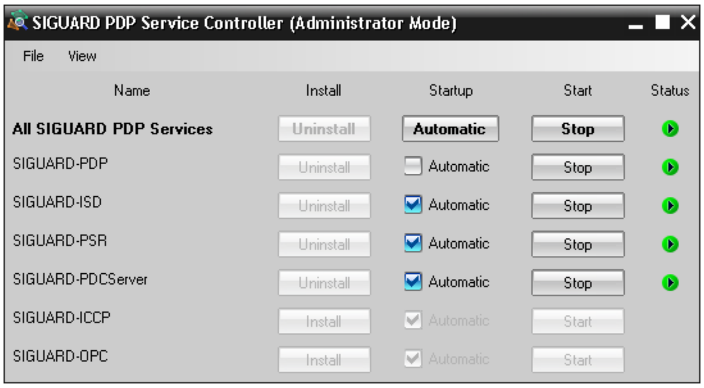
✧ Click the **Uninstall** button to uninstall a service.

An automatic start can be set for the services.

✧ Click the **Start** button to start a service.

-- or --

✧ Click the **Stop** button to stop a service.



Name	Install	Startup	Start	Status
All SIGUARD PDP Services	Uninstall	Automatic	Stop	▶
SIGUARD-PDP	Uninstall	☐ Automatic	Stop	▶
SIGUARD-ISD	Uninstall	☑ Automatic	Stop	▶
SIGUARD-PSR	Uninstall	☑ Automatic	Stop	▶
SIGUARD-PDCServer	Uninstall	☑ Automatic	Stop	▶
SIGUARD-ICCP	Install	☑ Automatic	Start	
SIGUARD-OPC	Install	☑ Automatic	Start	

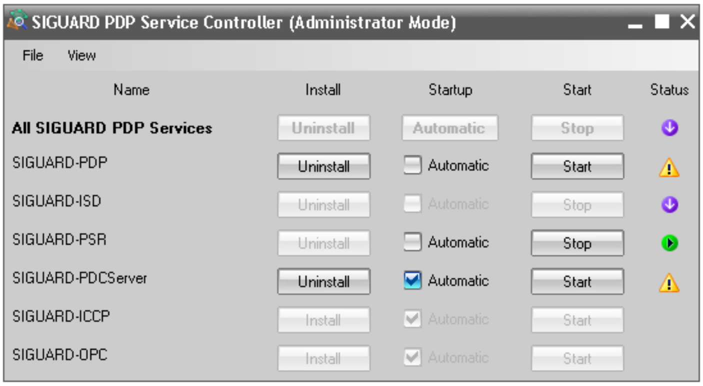
Figure 3-3 Service Controller, Services Installed and Started

The **Status** of the services is displayed in the last column:

Table 3-4 Status Displays of the Service Controller Tool

Status	Explanation
▶	This status indicates that this service is installed and started.
⬇	This status indicates that this service was started or stopped and the processing is still running.
⚠	This status indicates that this service was installed or stopped and an action (uninstall service or start service) is expected.

In the following example, some services are stopped.



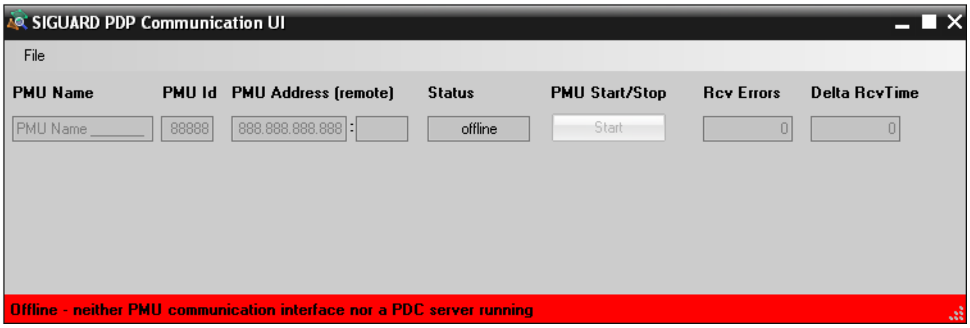
Name	Install	Startup	Start	Status
All SIGUARD PDP Services	Uninstall	Automatic	Stop	⬇
SIGUARD-PDP	Uninstall	☐ Automatic	Start	⚠
SIGUARD-ISD	Uninstall	☐ Automatic	Stop	⬇
SIGUARD-PSR	Uninstall	☐ Automatic	Stop	▶
SIGUARD-PDCServer	Uninstall	☑ Automatic	Start	⚠
SIGUARD-ICCP	Install	☑ Automatic	Start	
SIGUARD-OPC	Install	☑ Automatic	Start	

Figure 3-4 For Example: Service Controller with Stopped Services

3.2.5.4 Diagnostic Tool Communication UI

The **SIGUARD PDP Communication UI** is a diagnostic window that can be opened after the PDP starts.

When the **SIGUARD PDP Communication UI** is started before or during the SIGUARD PDP Server startup, then the following diagnostic window is opened:



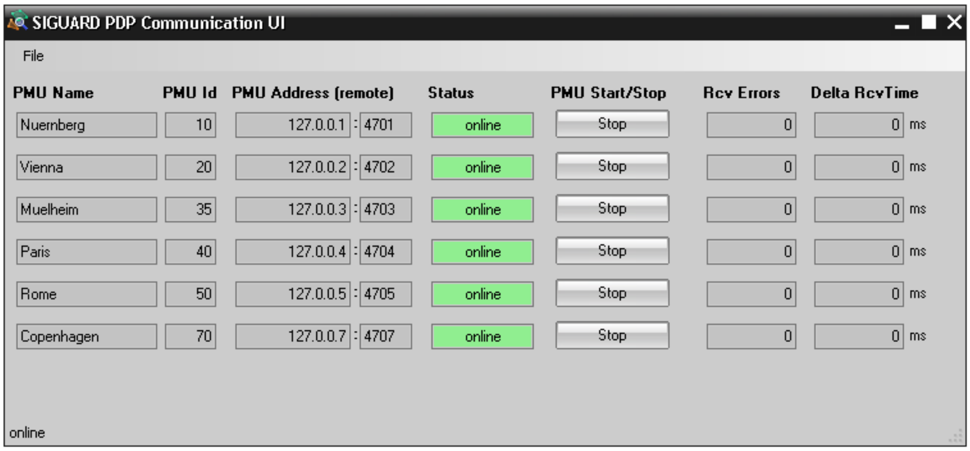
PMU Name	PMU Id	PMU Address (remote)		Status	PMU Start/Stop	Rcv Errors	Delta RcvTime
PMU Name	88888	888.888.888.888		offline	Start	0	0

Offline - neither PMU communication interface nor a PDC server running

Figure 3-5 Diagnostic Window without Started SIGUARD PDP Server

Since there is still no connection between PMU and SIGUARD PDP Server, no diagnostic data can be displayed (status: **offline**).

With the SIGUARD PDP Server started, the diagnostic window with all configured PMU connections is displayed:



PMU Name	PMU Id	PMU Address (remote)		Status	PMU Start/Stop	Rcv Errors	Delta RcvTime
Nuernberg	10	127.0.0.1	4701	online	Stop	0	0 ms
Vienna	20	127.0.0.2	4702	online	Stop	0	0 ms
Muelheim	35	127.0.0.3	4703	online	Stop	0	0 ms
Paris	40	127.0.0.4	4704	online	Stop	0	0 ms
Rome	50	127.0.0.5	4705	online	Stop	0	0 ms
Copenhagen	70	127.0.0.7	4707	online	Stop	0	0 ms

online

Figure 3-6 Diagnostic Window with Started SIGUARD PDP Server

All configured PMU connections to the SIGUARD PDP Server are established (status: **online**).

The Diagnostic Window

In the diagnostic window, a row is created for every PMU device that was created in the configuration. In every row, the following parameters are accepted from the configuration:

- PMU name

- PMU ID
- PMU Address (remote)

  The PMU address consists of the IP address and the port number.

The next field shows the status of the connection between PMU and SIGUARD PDP Server.

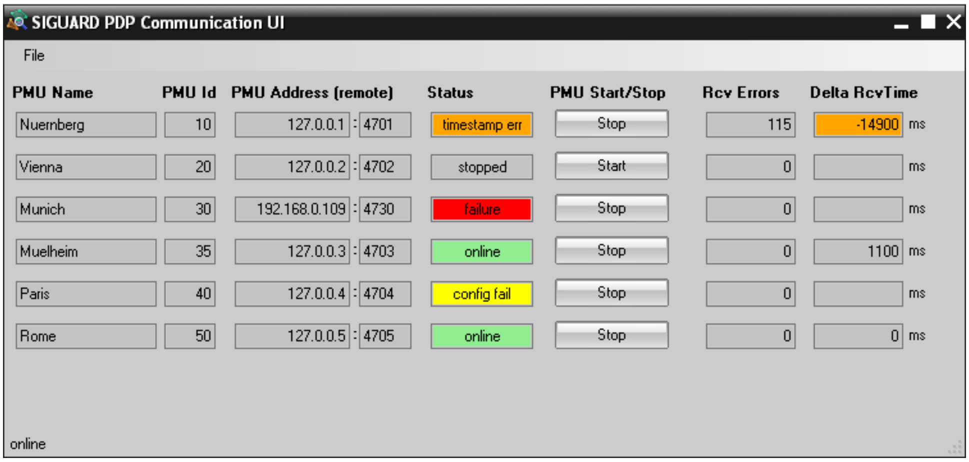
Table 3-5 Status Displays of Communication UI

Status	Explanation
offline	The status **offline** indicates that the diagnostic window was opened without the SIGUARD PDP Server being started.
online	The status **online** indicates that a correct connection between PMU and SIGUARD PDP Server exists by way of which the data is exchanged.
stopped	The status **stopped** indicates that the user has stopped any information evaluation of this physical PMU in the SIGUARD system, for example, via the button **Stop**, since it is not running optimally, for example. Only a stopped PMU can be activated via the button **Start**.
failure	The status **failure** indicates that the connection between PMU and SIGUARD PDP Server has failed or could not be established.
timestamp err	The status **timestamp err** indicates that the time stamp of the telegrams received from this PMU are invalid (too old, in the future or in incorrect grid).
config fail	The status **config fail** indicates that the native PMU configuration does not agree with the configuration from SIGUARD PDP Engineer.

In the field **Rcv Errors**, the telegram errors (for example, CRC errors) since the start of the SIGUARD PDP Servers are counted. Thus, a rough estimate concerning the quality of the connection is possible.

In the field **Delta RcvTime**, the difference between the currently received time stamps and the most recent time stamp (Δ = 0) is displayed.

In the following example, a **timestamp err** for the PMU Nürnberg is displayed, since the difference between the time stamp for the PMU Rome lies outside of the tolerance range (orange background in the field **Delta RcvTime**). The difference of the time stamp for PMU Mühlheim is not critical (white background in the field **Delta RcvTime**).



SIGUARD PDP Communication UI

File

PMU Name	PMU Id	PMU Address (remote)		Status	PMU Start/Stop	Rcv Errors	Delta RcvTime	
Nuernberg	10	127.0.0.1	4701	timestamp err	Stop	115	-14900	ms
Vienna	20	127.0.0.2	4702	stopped	Start	0		ms
Munich	30	192.168.0.109	4730	failure	Stop	0		ms
Muelheim	35	127.0.0.3	4703	online	Stop	0	1100	ms
Paris	40	127.0.0.4	4704	config fail	Stop	0		ms
Rome	50	127.0.0.5	4705	online	Stop	0	0	ms

online

Figure 3-7 For example: Diagnostic Window with Various Status Displays

3.3 Uninstalling the Software

3.3.1 Uninstalling SIGUARD PDP

You remove SIGUARD PDP from your computer via the uninstaller in the operating system. When doing so, you delete all data installed by the installer for SIGUARD PDP. You can decide during the uninstallation whether the archive and configuration files should be removed.

The **Automation License Manager** and the diagnostic software **BMC AppSight Black Box** are not removed when uninstalling SIGUARD PDP. These programs must be uninstalled separately. Do not uninstall these programs if they are still needed by other software.

Uninstalling the Services

To uninstall the services for SIGUARD PDP, proceed as follows:

- Open the Service Controller Tool with **Start > Siemens Energy > SIGUARD PDP > Service Controller Tool**.
- Stop the services.
- Uninstall the services.
- Close the Service Controller Tool.

Uninstalling SIGUARD PDP

You uninstall SIGUARD PDP as follows:

- Click **Start > Settings > Control Panel**.
- Open the list of the installed software programs.
- Select **Siemens SIGUARD PDP V2.10** and click the button **Remove**. The uninstallation process starts.
- Follow the instructions of the uninstaller.

NOTE

If the uninstallation fails in Windows 7, stop the **Network Time Protocol** service manually and repeat the uninstallation procedure.

A restart of the computer is necessary after uninstallation.

3.3.2 Removing the SIGUARD PDP License

NOTE

If the same software version of SIGUARD PDP is installed with a new software component, the license of SIGUARD PDP does not need to be removed.

You remove the license by transferring the license from your computer to the license USB stick.

NOTE

The license can also be transferred to another removable storage medium, for example, third-party USB stick.

Remove the licensing of SIGUARD PDP as follows:

- ✧ Place the included USB stick in the USB port.
- ✧ Click **Start > Programs > Siemens Automation > Automation License Manager**.
- ✧ Transfer the license or licenses from the hard disk to the license USB stick.

■

4 OPC

4.1 Overview

OPC is an open interface standard based on COM- and DCOM-technology (Distributed Component Object Model). This standard makes simple, standardized data exchange possible between automation/control applications, bay devices, and office applications.

In this way, you can send measured values from SIGUARD PDP to a SICAM PAS substation automation system and then have automation functions run there that are controlled by the phasor measured values.

First install the **OPC Server** and then configure the server according to your needs.

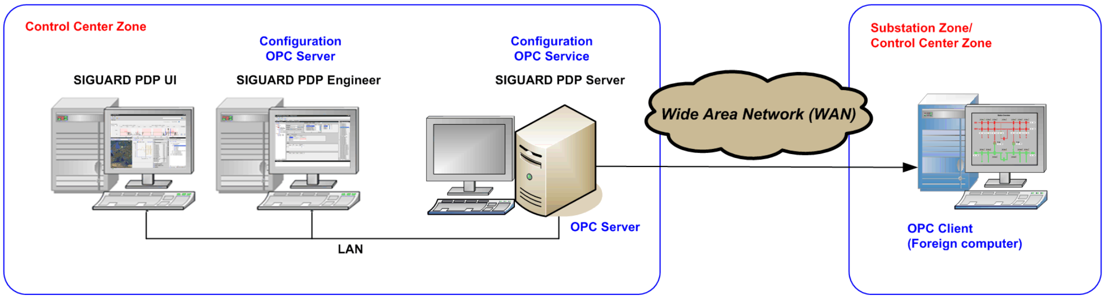


Figure 4-1 System Overview with OPC Server

4.2 OPC Server Installation

To install the **OPC Server**, proceed as follows:

- ✧ Uninstall SIGUARD PDP if it is already on your computer.
- ✧ Reinstall SIGUARD PDP with the option **OPC**.

Licensing the OPC Server

The **OPC** option must be licensed.

- ✧ Transfer the licenses from the license USB stick via the ALM.

4.3 OPC Server Configuration

When using the **OPC Server** function, setting changes for **DCOM** (Distributed Component Object Model) are necessary.

Configuring DCOM

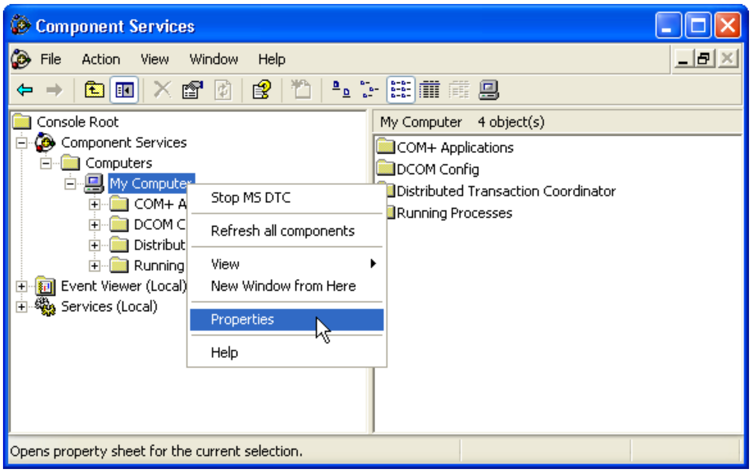
The configuration of DCOM is performed with the Microsoft tool **dcomcnfg.exe**.

To configure DCOM, proceed as follows:

- Open **Start > Run** via the window **Run**.
- Enter **dcomcnfg** and confirm with **OK**.

The window **Component Services** opens.

- Right-click **My Computer** and select the context menu **Properties**

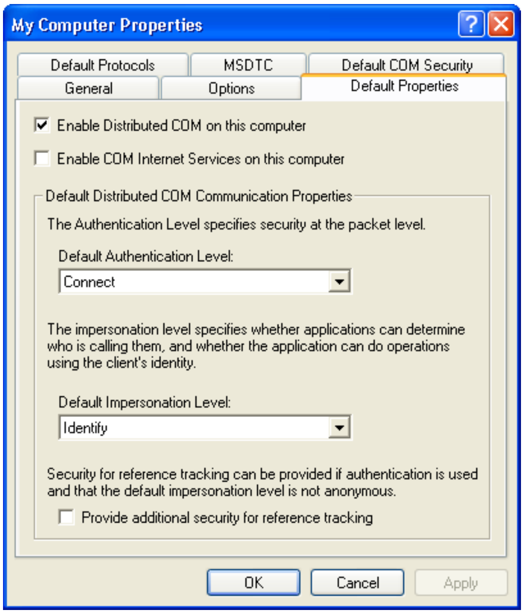


Opens property sheet for the current selection.

Figure 4-2 Component Services

The window **My Computer Properties** opens.

- ✧ Select the tab **Default Properties**.



☑ Enable Distributed COM on this computer

☐ Enable COM Internet Services on this computer

Default Distributed COM Communication Properties

The Authentication Level specifies security at the packet level.

Default Authentication Level:
Connect

The impersonation level specifies whether applications can determine who is calling them, and whether the application can do operations using the client's identity.

Default Impersonation Level:
Identify

Security for reference tracking can be provided if authentication is used and that the default impersonation level is not anonymous.

☐ Provide additional security for reference tracking

Figure 4-3 Default Properties

- ✧ Select **Enable Distributed COM on this computer**.
- ✧ Under **Default Authentication Level**, select the setting **Connect**.
- ✧ Under **Default Impersonation Level**, select the setting **Identify**

You do not need to perform settings in the other tabs.

- ✧ Close the dialog with **OK**.
- ✧ In the window **Component Services** under **My Computer**, check the entry **DCOM Config**.

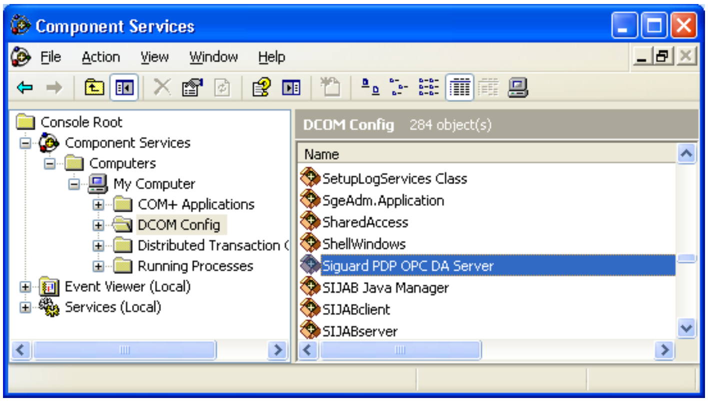
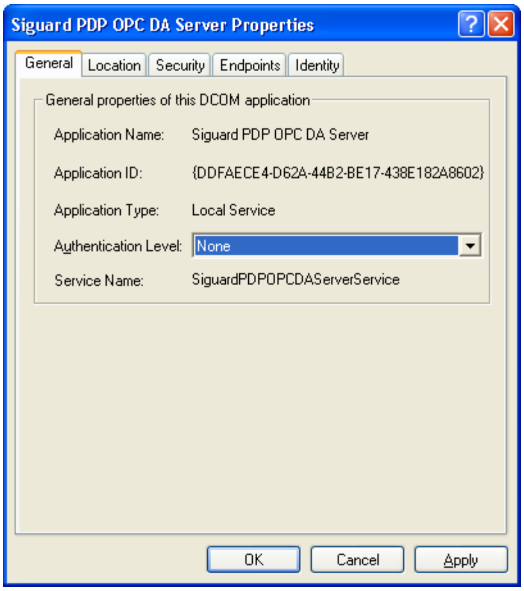


Figure 4-4 Opening the Properties of the SIEMENS SIGUARD PDP OPC DA Server

✧ Right-click **SIEMENS SIGUARD PDP OPC DA Server** and select the context menu **Properties**.

The dialog **SIEMENS SIGUARD PDP OPC DA Server Properties** opens.

✧ Select the tab **General**.



General properties of this DCOM application

Application Name: Siguard PDP OPC DA Server

Application ID: {DDFAECE4-D62A-44B2-BE17-438E182A8602}

Application Type: Local Service

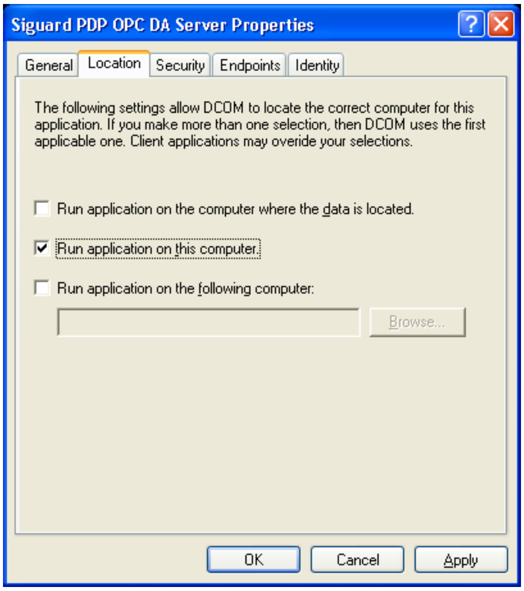
Authentication Level: None

Service Name: SiguardPDPOPCDAServerService

Figure 4-5 General

✧ Under **Authentication Level**, select the setting **None**.

✧ Select the **Location** tab.



The following settings allow DCOM to locate the correct computer for this application. If you make more than one selection, then DCOM uses the first applicable one. Client applications may overide your selections.

☐ Run application on the computer where the data is located.

☑ Run application on this computer.

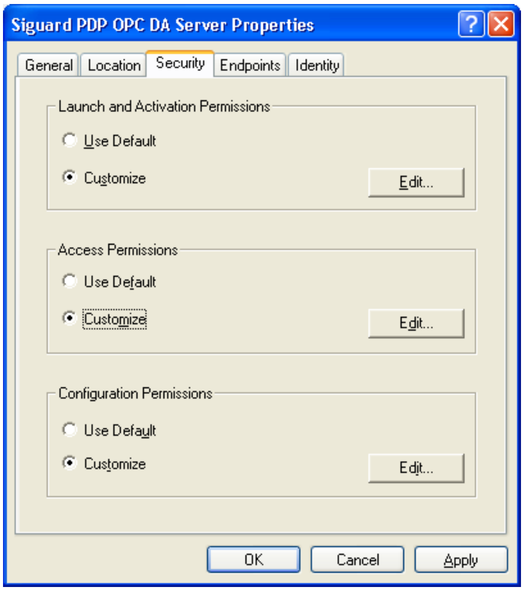
☐ Run application on the following computer:

Figure 4-6 Location

- ✧ Select **Run application on this computer**.

For DCOM, additionally assign start, access, and configuration rights for the user who logs on to the OPC Client and wants to access the OPC Server via a network connection.

- ✧ Select the tab **Security**.



Siguard PDP OPC DA Server Properties

General | Location | Security | Endpoints | Identity

Launch and Activation Permissions
○ Use Default
● Customize

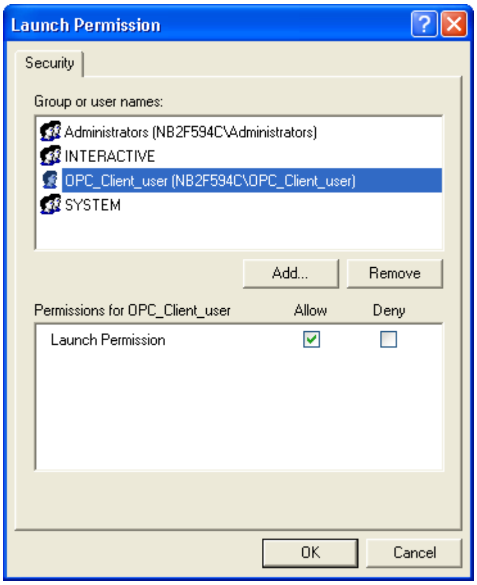
Access Permissions
○ Use Default
● Customize

Configuration Permissions
○ Use Default
● Customize

Figure 4-7 Security

- ✧ Under **Launch Permissions**, select the option **Customize**.
- ✧ Click **Edit...**.

The dialog **Launch Permission** opens.



Launch Permission

Security

Group or user names:
Administrators (NB2F594C\Administrators)
INTERACTIVE
OPC_Client_user (NB2F594C\OPC_Client_user)
SYSTEM

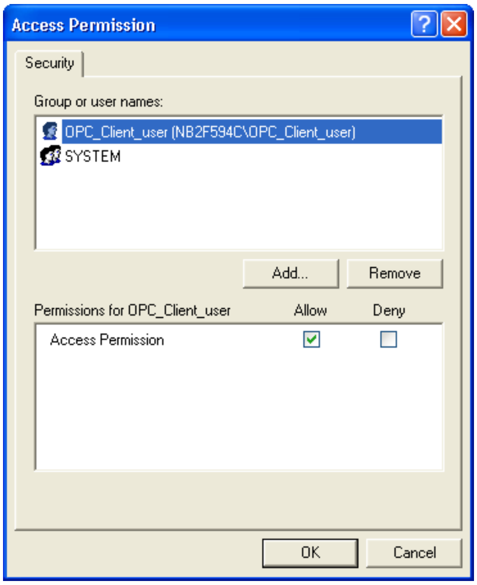
Permissions for OPC_Client_user	Allow	Deny
Launch Permission	☑	☐

Figure 4-8 Specifying the Start Permission

- Click **Add...** to add the user with which the OPC Server/Client shall work. To do this, you can also create a new user.
- For the **Launch Permission** user, select the option **Allow**.
- Close the dialog with **OK**.

- Under **Access Permissions**, select the option **Customize**.
- Click **Edit...**.

The dialog **Access Permission** opens.



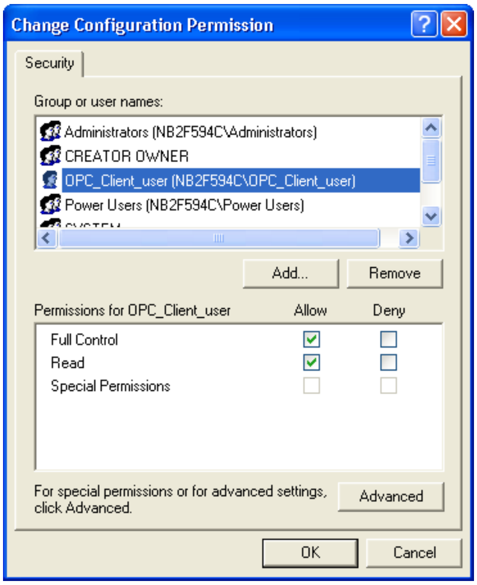
Group or user names:
OPC_Client_user (NB2F594C\OPC_Client_user)
SYSTEM

Permissions for OPC_Client_user	Allow	Deny
Access Permission	☑	☐

Figure 4-9 Specify the Access Rights

- Click **Add...** to add the user with which the OPC Server/Client shall work.
- Select the option **Allow** for the user.
- Close the dialog with **OK**.
- Under **Configuration Permissions**, select the option **Customize**.
- Click **Edit...**.

The dialog **Change Configuration Permission** opens.



Group or user names:

- Administrators (NB2F594C\Administrators)
- CREATOR OWNER
- OPC_Client_user (NB2F594C\OPC_Client_user)
- Power Users (NB2F594C\Power Users)
- SYSTEM

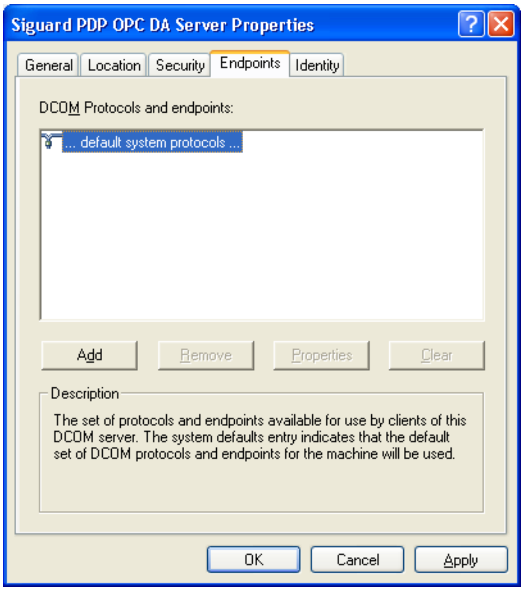
Permissions for OPC_Client_user	Allow	Deny
Full Control	☑	☐
Read	☑	☐
Special Permissions	☐	☐

For special permissions or for advanced settings, click Advanced.

Figure 4-10 Specifying the Configuration Permissions

- Click **Add...** to add the user with which the OPC Server/Client shall work.
- For the user, select the option **Allow** for **Full Control** and **Read**.
- Close the dialog with **OK**.
- Select the tab **End Points**.

  This tab includes a list of protocols and end points which may be used by the OPC Client. No settings are required.



DCOM Protocols and endpoints:

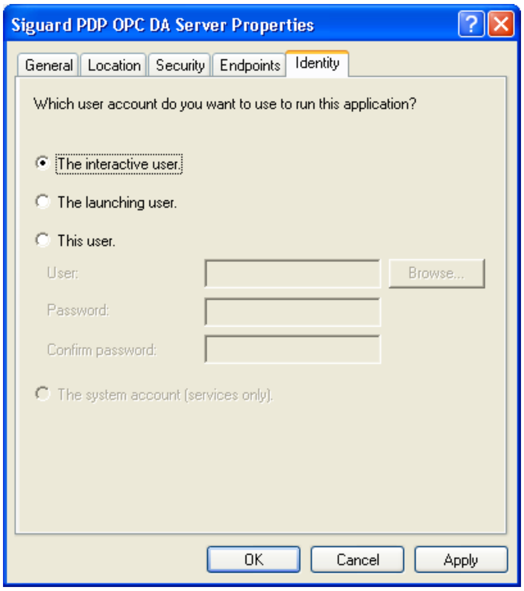
... default system protocols ...

Description

The set of protocols and endpoints available for use by clients of this DCOM server. The system defaults entry indicates that the default set of DCOM protocols and endpoints for the machine will be used.

Figure 4-11 Specifying the End Points

- ✧ Select the tab **Identity**.



Siguard PDP OPC DA Server Properties

Which user account do you want to use to run this application?

● The interactive user.
○ The launching user.
○ This user.
User:
Password:
Confirm password:
○ The system account (services only).

Figure 4-12 Identity

- ✧ Select **The interactive user**.
- ✧ Close the dialog with **OK**.
- ✧ Close the window **Component Services**.

NOTE

If the Microsoft Firewall is activated, perform additional settings for the OPC Server (see *2.4 Communication Protocols for the Use of a Firewall*).

■

5 ICCP

5.1 General

The ICCP Protocol

The ICCP protocol supports the exchange of network data via a network (WAN or LAN) between a local power utility network control center and

- Other power utilities (EVUs)
- Power Pools
- Regional Network Control Centers
- Non-EVU Generating Units

The protocol was standardized in accordance with IEC 61870-6 (TASE.2).

ICCP supports:

- Functions for the pre-processing of data
- A user interface for the display of error statistics with powerful testing and diagnostic functions

SIGUARD PDP uses the ICCP protocol to transfer measured values and events to a network control center.

Introduction

Using SIGUARD PDP Engineer, a configuration file **PDP_config.xml** is created which contains all data for the ICCP channels to control and parameterize the corresponding components. Every component of the network reads this XML file when starting.

Procedure

In order to be able to work with the ICCP, proceed as follows:

- Install the ICCP driver.
- License the ICCP driver.
- Edit the configuration file **osill2.cfg** of the ICCP driver.

5.2 Installation of the ICCP Driver

5.2.1 Installation Preparation

To install the ICCP driver, proceed as follows:

- Uninstall SIGUARD PDP if it is already on your computer.
- Install SIGUARD PDP with the option **ICCP**.

  You can find more information in chapter *3.2.2 Installation*.

5.2.2 Installation

Starting Installation

To install the SIGUARD PDP ICCP Add-on, proceed as follows:

- Insert the DVD with the **ICCP Add-on** into your DVD drive.

NOTE

The installation procedure does not start automatically.

- To start the installation procedure, double-click the **setup.exe** file from the root directory of the Add-on DVD.
- Follow the instructions of the installer.

Restart computer

- Restart the computer after installation.

NOTE

After the ICCP driver has been installed, you can find a sample configuration file **osill2.cfg** in the directory **C:\Program Files\SISCO\osill2\**. Information on editing the configuration file can be found in the corresponding chapters in the *Administrator Manual*.

5.3 Licensing the ICCP Driver

Activation of the ICCP Driver

- Open the window **SISCO MMS-EASE Activation** via the menu **Start > Programs > SISCO > MMS-EASE > Activate MMS-EASE**.

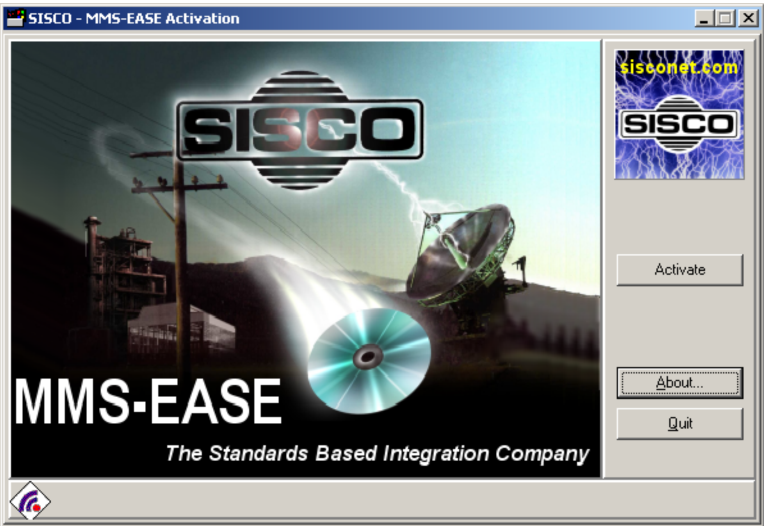
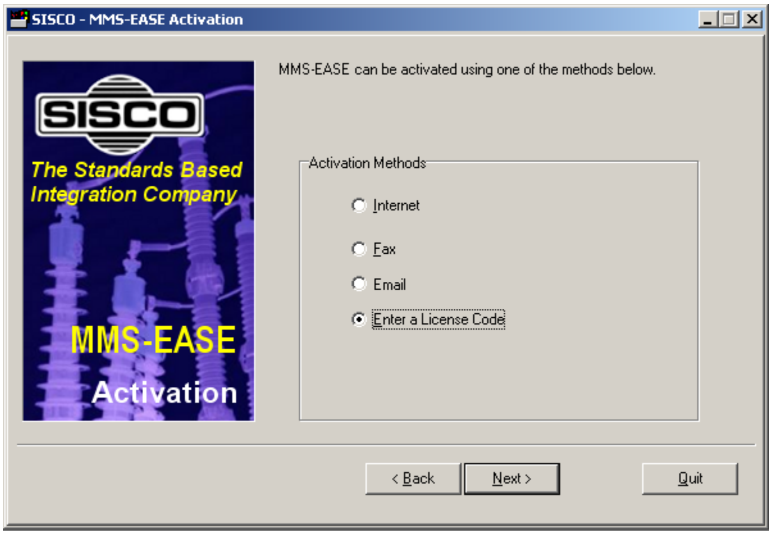

SISCO - MMS-EASE Activation
SISCO
MMS-EASE
The Standards Based Integration Company
sisconet.com
SISCO
Activate
About...
Quit

Figure 5-1 Licensing the ICCP Driver

- In order to activate the ICCP driver, click **Activate**.


SISCO - MMS-EASE Activation
SISCO
The Standards Based Integration Company
MMS-EASE
Activation
< Back
Next >
Quit

MMS-EASE can be activated using one of the methods below.

Activation Methods

○ Internet

○ Fax

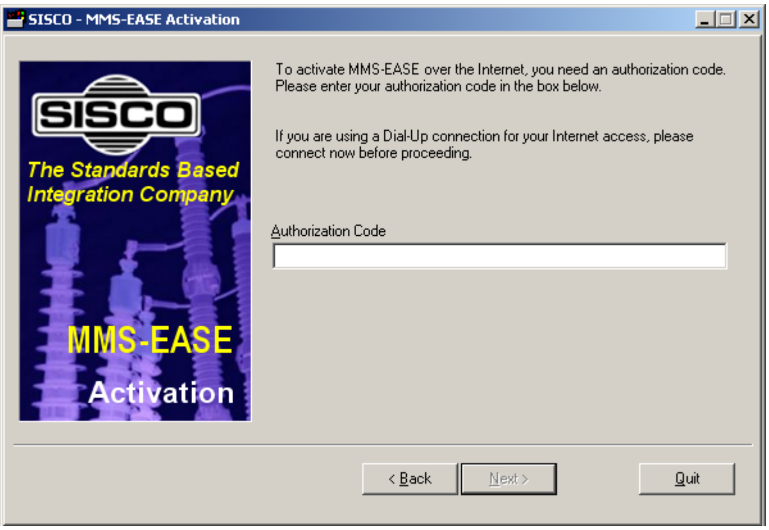
○ Email

● Enter a License Code

Figure 5-2 Licensing the ICCP Driver

You have various options to register the ICCP driver:

✧ Select the activation method **Enter a License Code**.



To activate MMS-EASE over the Internet, you need an authorization code. Please enter your authorization code in the box below.

If you are using a Dial-Up connection for your Internet access, please connect now before proceeding.

Authorization Code

SISCO - MMS-EASE Activation
SISCO
The Standards Based Integration Company
MMS-EASE
Activation
< Back
Next >
Quit

Figure 5-3 Entry of License Key

✧ Enter the license key that you received with the product.

NOTE

Do not enter the authorization code that is on the CD sleeve!

5.4 Editing the Configuration File

The fields **Local AR Name**, **Primary Remote AR Name**, **Alternate Remote AR Name**, **Third Remote AR Name**, and **Fourth Remote AR Name** are the aliases of the IP addresses for a connection between a local and a remote control center. These aliases are defined in a configuration file **osill2.cfg** in the path **C:\Program-Files\SISCO\osill2\**. In order to be able to connect a local with a remote control center, at least 4 fields within the configuration file must be defined for each connection:

- IP address (for TCP connections)
- P Selector (Local Presentation Selector)
- S Selector (Local Session Selector)
- T Selector (Local Transport Selector)

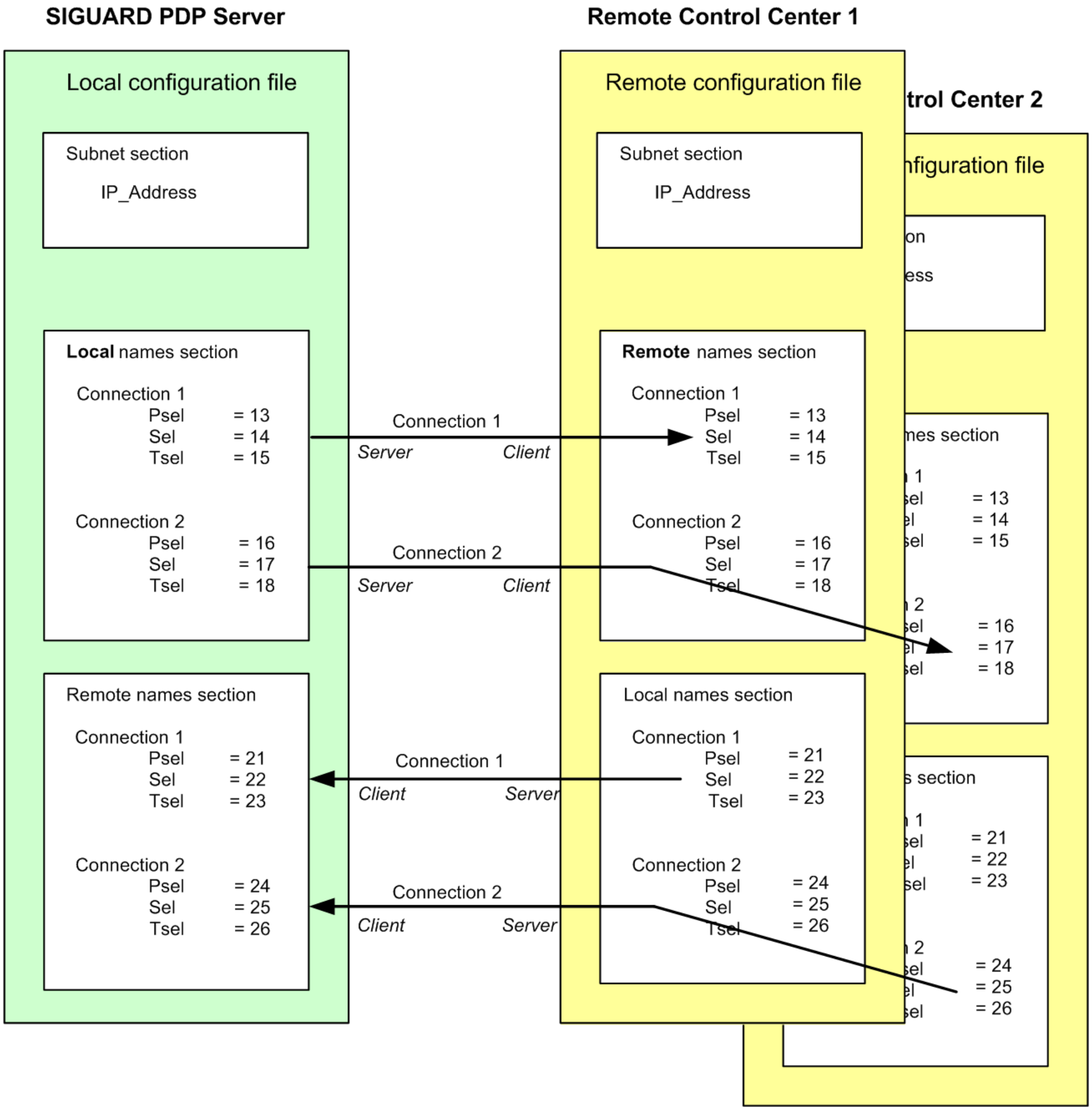
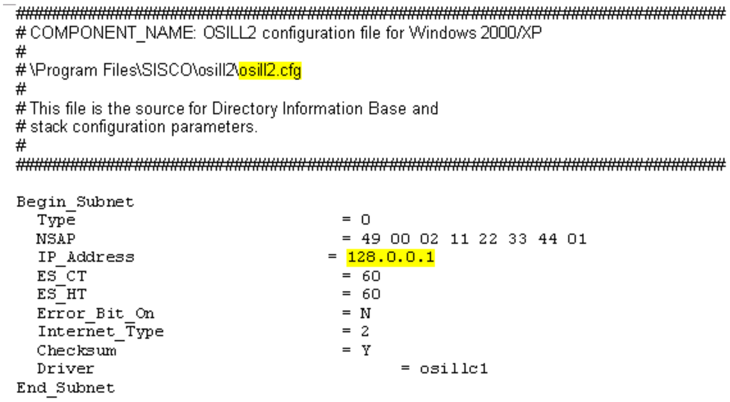


Figure 5-4 Overview of the Configuration Files

Adapt Subnet Range

- ✧ Open the configuration file **osill2.cfg**.
- ✧ Enter the IP address of the local computer in the **Subnet** area.



```
##########################################################################################
# COMPONENT_NAME: OSILL2 configuration file for Windows 2000/XP
#
# \Program Files\SISCO\osill2\osill2.cfg
#
# This file is the source for Directory Information Base and
# stack configuration parameters.
#
##########################################################################################

Begin_Subnet
  Type                            = 0
  NSAP                            = 49 00 02 11 22 33 44 01
  IP_Address                    = 128.0.0.1
  ES_CT                           = 60
  ES_HT                           = 60
  Error_Bit_On                    = N
  Internet_Type                   = 2
  Checksum                        = Y
  Driver                                = osillc1
End_Subnet
```

Figure 5-5 Setting the IP Address of the Local Computer

- ✧ Save the configuration file.

Adapt Local Names Section Area

- ✧ Adapt the parameter **AR_Name** in the area **Local Names Section** for every connection.

  The name can be assigned freely, for example, **LocalToICCPREM** (Local > ICCP-Remote).

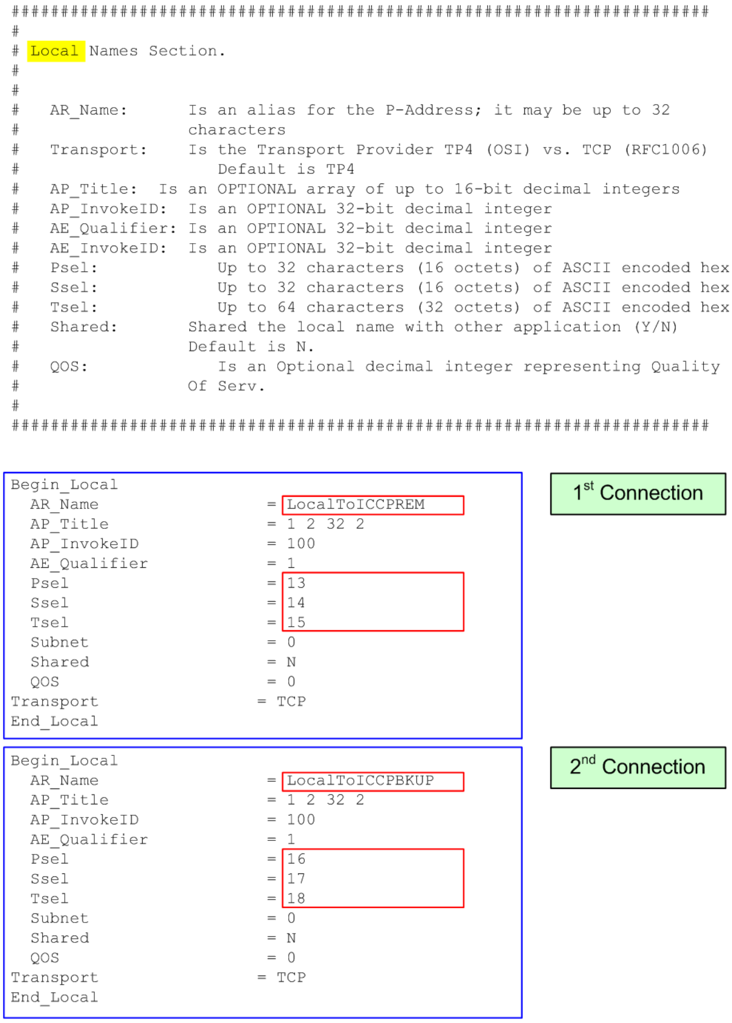
NOTE

The parameter must be identical to the name that is assigned in SIGUARD PDP Engineer.

- ✧ Assign values for the parameters **Psel**, **Ssel**, and **Tsel** that are unique in the SIGUARD system, for example, *13 / 14 / 15* for connection 1 or *16 / 17 / 18* for connection 2.

  These values must be identical to the values for the corresponding parameters in the configuration file of the Remote Control Center in agreement with its administrator. Agreement of the identical values is required for all connections.

  You can find further information in the *SISCO Installation Guide for MMS-EASE for Windows*.



```
#######################################################################
#
# Local Names Section.
#
#
#   AR_Name:      Is an alias for the P-Address; it may be up to 32
#                 characters
#   Transport:    Is the Transport Provider TP4 (OSI) vs. TCP (RFC1006)
#                    Default is TP4
#   AP_Title:  Is an OPTIONAL array of up to 16-bit decimal integers
#   AP_InvokeID:  Is an OPTIONAL 32-bit decimal integer
#   AE_Qualifier: Is an OPTIONAL 32-bit decimal integer
#   AE_InvokeID:  Is an OPTIONAL 32-bit decimal integer
#   Psel:            Up to 32 characters (16 octets) of ASCII encoded hex
#   Ssel:            Up to 32 characters (16 octets) of ASCII encoded hex
#   Tsel:            Up to 64 characters (32 octets) of ASCII encoded hex
#   Shared:       Shared the local name with other application (Y/N)
#                 Default is N.
#   QOS:             Is an Optional decimal integer representing Quality
#                 Of Serv.
#
#######################################################################
```

```
Begin_Local
  AR_Name                   = LocalToICCPREM
  AP_Title                  = 1 2 32 2
  AP_InvokeID               = 100
  AE_Qualifier              = 1
  Psel                      = 13
  Ssel                      = 14
  Tsel                      = 15
  Subnet                    = 0
  Shared                    = N
  QOS                       = 0
Transport                  = TCP
End_Local
```

```
Begin_Local
  AR_Name                   = LocalToICCPBKUP
  AP_Title                  = 1 2 32 2
  AP_InvokeID               = 100
  AE_Qualifier              = 1
  Psel                      = 16
  Ssel                      = 17
  Tsel                      = 18
  Subnet                    = 0
  Shared                    = N
  QOS                       = 0
Transport                  = TCP
End_Local
```

Figure 5-6 Local Names Section

Adapt Remote Names Section Area

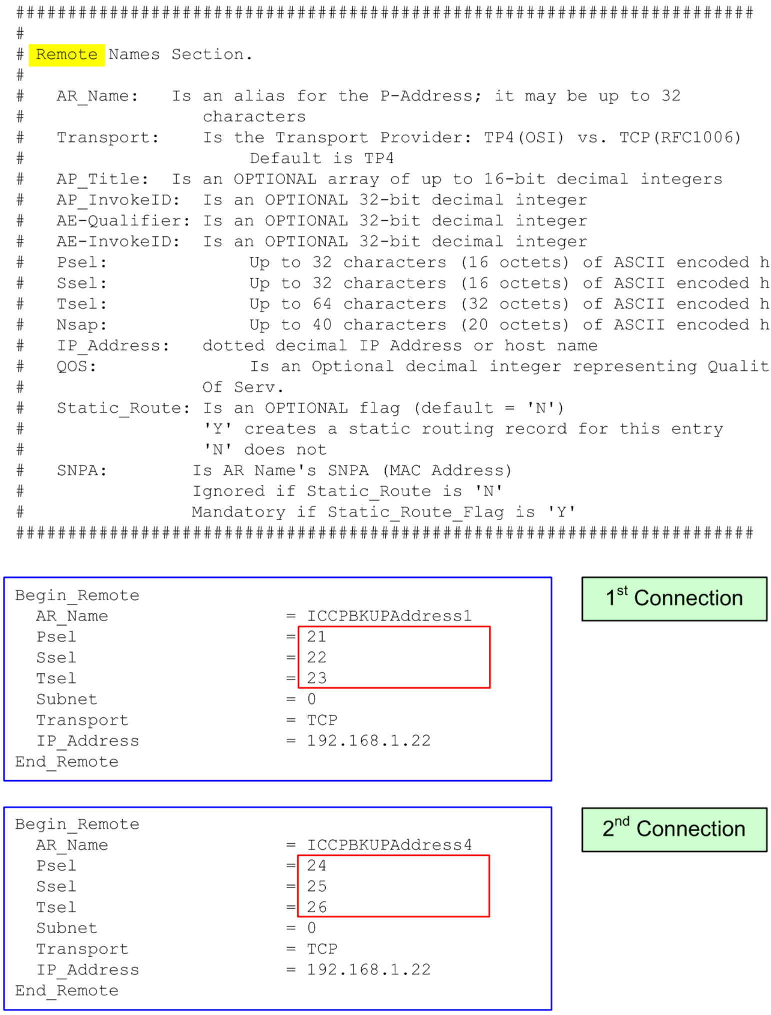
- ✧ Adapt the parameter **AR_Name** in the area **Remote Names Section** for every connection.

  The name can be freely assigned, for example, **ICCPBKUPAddress1**.

- ✧ Assign values for the parameters **Psel**, **Ssel**, and **Tsel** that are unique in the SIGUARD system, for example, *21 / 22 / 23* for connection 1 or *24 / 25 / 26* for connection 2.

  These values must be identical to the values for the corresponding parameters in the configuration file of the Remote Control Center in agreement with its administrator. Agreement of the identical values is required for all connections.

  You can find further information in the *SISCO Installation Guide for MMS-EASE for Windows*.



```
########################################################################
#
# Remote Names Section.
#
#   AR_Name:   Is an alias for the P-Address; it may be up to 32
#                 characters
#   Transport:    Is the Transport Provider: TP4(OSI) vs. TCP(RFC1006)
#                     Default is TP4
#   AP_Title:  Is an OPTIONAL array of up to 16-bit decimal integers
#   AP_InvokeID:  Is an OPTIONAL 32-bit decimal integer
#   AE-Qualifier: Is an OPTIONAL 32-bit decimal integer
#   AE-InvokeID:  Is an OPTIONAL 32-bit decimal integer
#   Psel:             Up to 32 characters (16 octets) of ASCII encoded hex
#   Ssel:             Up to 32 characters (16 octets) of ASCII encoded hex
#   Tsel:             Up to 64 characters (32 octets) of ASCII encoded hex
#   Nsap:             Up to 40 characters (20 octets) of ASCII encoded hex
#   IP_Address:   dotted decimal IP Address or host name
#   QOS:              Is an Optional decimal integer representing Quality
#                 Of Serv.
#   Static_Route: Is an OPTIONAL flag (default = 'N')
#                 'Y' creates a static routing record for this entry
#                 'N' does not
#   SNPA:        Is AR Name's SNPA (MAC Address)
#                Ignored if Static_Route is 'N'
#                Mandatory if Static_Route_Flag is 'Y'
########################################################################
```

```
Begin_Remote
  AR_Name                 = ICCPBKUPAddress1
  Psel                    = 21
  Ssel                    = 22
  Tsel                    = 23
  Subnet                  = 0
  Transport               = TCP
  IP_Address              = 192.168.1.22
End_Remote
```

1st Connection

```
Begin_Remote
  AR_Name                 = ICCPBKUPAddress4
  Psel                    = 24
  Ssel                    = 25
  Tsel                    = 26
  Subnet                  = 0
  Transport               = TCP
  IP_Address              = 192.168.1.22
End_Remote
```

2nd Connection

Figure 5-7 Remote Names Section

■

6 Time Synchronization

6.1 Overview

Siemens recommends operating the SIGUARD PDP Server, as with the PMUs, with time synchronization. If the SIGUARD PDP Server is not operated with time synchronization, it cannot be determined reliably whether the time stamps of the received telegrams lie within a permissible time slot. That is, it cannot be determined whether the received telegrams are too old or lie in the future. With an unsynchronized server time, telegrams with otherwise valid time stamps could be rejected, and then even those with a false time stamp could be recognized as valid and processed.

Time information within the SIGUARD PDP system can be synchronized as follows:

- **GPS receiver** Hopf6039 card

  The Hopf6039 card is a PCI card for the SIGUARD PDP Server.
- **NTP time server** (for example, SICLOCK, Hopf time server, Meinberg time server)

The time synchronization of SIGUARD PDP is based on the **NTP** (Network Time Protocol) and the corresponding service **NTPD** (Network Time Protocol Daemon) software. This service runs in the background in Windows.

During installation of SIGUARD PDP, this service is referred to as the **Network Time Protocol Service**. It is configured using the **ntp.conf** ASCII file.

You can find more information in chapter *6.5 Configuration File for the NTPD*.

During the installation of **SIGUARD PDP**, NTPD is also installed. It is activated upon a restart of the computer.

In a SIGUARD PDP system, several NTPDs can be active, for example, on the external radio clock and on the SIGUARD PDP Server. An NTPD can be configured as a Server or as a Client. Upon the request of a client, the server communicates its time information to the client.

Based on NTP, a precision of approximately 0.1 ms can be achieved under a Windows operating system. In order to achieve this high precision, the NTPDs of the system must perform extensive calculations. This process can take several hours after the system starts. If the current timing master fails, the NTPDs use the data received in an attempt to keep the time as accurate as possible for as long as possible.

Further information on NTP can be found under the following address: *http://www.ntp.org*.

6.2 Hopf Time Server Installation

Following the insertion of the Hopf6039 card, install the corresponding software first. Then you can initialize the Hopf6039 card.

During the installation of SIGUARD PDP, an NTPD (Network Time Protocol Daemon) is also installed. This NTPD enables even more precise time synchronization than the NTPD provided by Hopf.

To install a Hopf6039 card, proceed as follows:

- ✧ Insert the Hopf6039 card in the computer.
- ✧ Next, install the software for your Hopf6039 card. The software is required for the initialization of the card.
- ✧ Uninstall the NTPD of the Hopf6039 card (see *6.3 Uninstalling NTPD of the Hopf Card*).
- ✧ Install SIGUARD PDP. The NTPD delivered with SIGUARD PDP is automatically installed as well.

6.3 Uninstalling NTPD of the Hopf Card

To uninstall the NTPD of the Hopf6039 card, proceed as follows:

- ✧ Click **Start > Settings >Control Panel**.
- ✧ Double-click **Administrative Tools**. The **Administrative Tools** window opens.
- ✧ Double-click **Services**. The **Services** window opens.
- ✧ Right-click **Network Time Protocol** and select **End** from the context menu to end the service.
- ✧ Select **Start > Run**.
- ✧ To uninstall the service, enter **<Hopf installation path>\instsrv remove** and click **OK**.

6.4 NTP Daemon

To configure the NTPD, knowledge about its main functions is required. Some NTPD functions and terms are illustrated below.

Server, Client, and Peer

An NTPD can be configured as a **Server** or as a **Client**. The server uses the current time information received from a clock. The clients poll the time information from the server.

Besides this, an NTPD can be configured as a **Peer**. This is the case if several clocks with the same priority exist in a distributed system. The roles (server/client) of the individual NTPDs are not specifically defined. The peers communicate among each other to determine the quality of their time signal. The NTPD of the peer with the most precise time signal acts as the Server.

Stratum, Offset, and Dispersion

The NTP time distribution is based on a hierarchical structure. Time information is distributed from the top level down to the lower levels. A level is referred to as a **Stratum**. The clock is the top level and is referred to as stratum 0. The time server, which receives its time information directly from the clock, is assigned stratum 1. The server which acts as a client of this server is assigned stratum 2. Numbering is continued according to this pattern.

The **Offset** is the difference between the client clock and the server clock. The NTPD tries to keep the offset as small as possible. The offset is the most important criterion for the determination of the quality of time information.

The **Dispersion** is another criterion used for quality determination. The dispersion defines the upper limit for the deviation of the system time from the 'real' clock time. The smaller the dispersion, the higher is the quality of the time information.

Quality of Time Information

When determining the system time within the SIGUARD runtime, the time stamp received is assigned a **Quality**. The following 4 quality levels can be assigned:

- **High** means that the system time deviates from the 'real' clock time by less than 10 ms and that the quality of the time sources is sufficient for this determination. A dispersion of less than 10 ms is sufficient to meet the standard requirements in the field of automated energy supply.
- **Medium** means that the system time deviates from the 'real' clock time by less than 2 s and that the quality of the time sources is sufficient for this determination. This level of precision ensures that no low-quality time stamps are produced if a leap second is inserted and the clock therefore shows a temporary deviation of ~1 s.
- **Low** means that the available time information does not have the required precision and that the system must therefore be considered as 'out of synchronization'.
- **Unknown** is assigned if the system detects that no NTP service runs at all or that the service was not able to detect a time source.

For reasons of compatibility, the SIGUARD internal time stamp is assigned the **ClockSync** and **ClockValid** status bits. These bits are set based on the quality of the time stamp:

- **high**

  The status bits **ClockSync** and **ClockValid** are set.
- **medium**

  The status bit **ClockValid** is set.
- **low**

  No status bit is set.
- **unknown**

  No status bit is set.

6.5 Configuration File for the NTPD

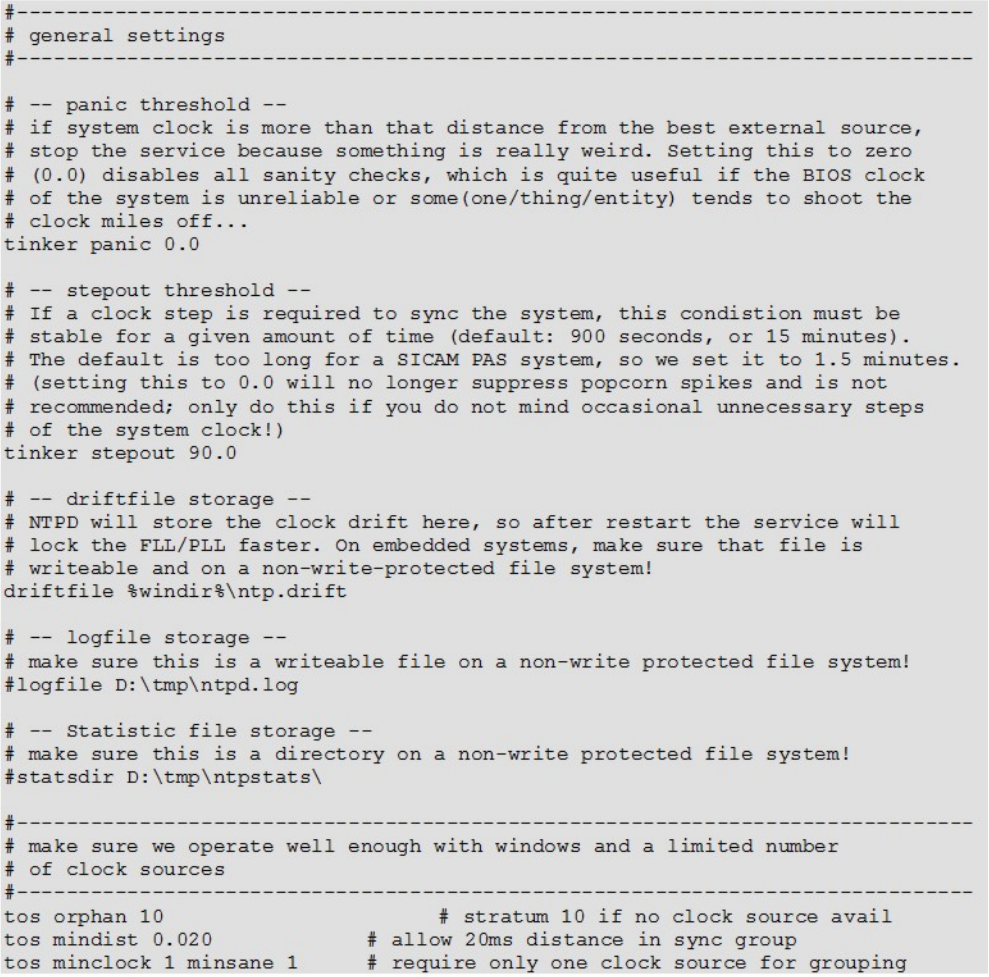
When installing **SIGUARD PDP**, an **ntp.conf** configuration file is copied into the directory **...\windows\system32\drivers\etc**. This file is used to configure the **NTPD**.

The time servers are indicated in the configuration files of the clients. However, the clients are not indicated in the configuration files of the servers. A time client can thus be added to a system in a simple way. Only the configuration file of the new client needs to be edited.

The configuration file includes some comments on its contents. This section provides information about important entries.

Further information can be found under the following address *http://www.ntp.org*.

General Settings



```
#-------------------------------------------------------------------------------
# general settings
#-------------------------------------------------------------------------------

# -- panic threshold --
# if system clock is more than that distance from the best external source,
# stop the service because something is really weird. Setting this to zero
# (0.0) disables all sanity checks, which is quite useful if the BIOS clock
# of the system is unreliable or some(one/thing/entity) tends to shoot the
# clock miles off...
tinker panic 0.0

# -- stepout threshold --
# If a clock step is required to sync the system, this condition must be
# stable for a given amount of time (default: 900 seconds, or 15 minutes).
# The default is too long for a SICAM PAS system, so we set it to 1.5 minutes.
# (setting this to 0.0 will no longer suppress popcorn spikes and is not
# recommended; only do this if you do not mind occasional unnecessary steps
# of the system clock!)
tinker stepout 90.0

# -- driftfile storage --
# NTPD will store the clock drift here, so after restart the service will
# lock the FLL/PLL faster. On embedded systems, make sure that file is
# writeable and on a non-write-protected file system!
driftfile %windir%\ntp.drift

# -- logfile storage --
# make sure this is a writeable file on a non-write protected file system!
#logfile D:\tmp\ntpd.log

# -- Statistic file storage --
# make sure this is a directory on a non-write protected file system!
#statsdir D:\tmp\ntpstats\

#-------------------------------------------------------------------------------
# make sure we operate well enough with windows and a limited number
# of clock sources
#-------------------------------------------------------------------------------
tos orphan 10                      # stratum 10 if no clock source avail
tos mindist 0.020            # allow 20ms distance in sync group
tos minclock 1 minsane 1     # require only one clock source for grouping
```

Figure 6-1 ntp.conf - General Settings

- **tinker panic**

  Time information is not synchronized if the clock concerned deviates by more than 7200 s from the best external clock. The NTPD stops automatically or does not start up.

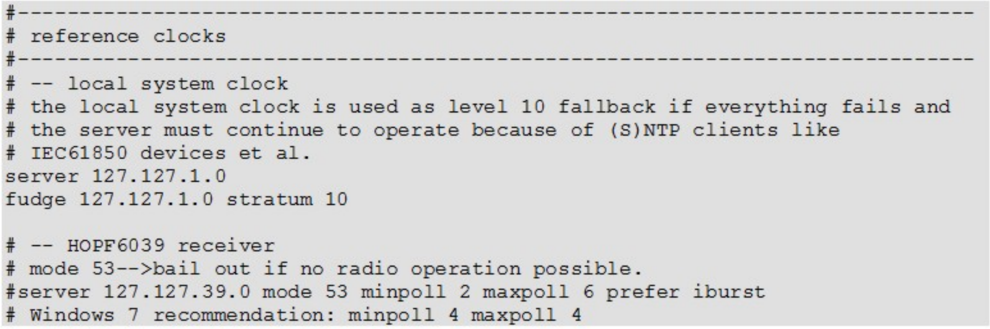
  The **Services-Manager** indicates whether the NTPD has started or not. Press **F5** to update the Services Manager. Set the local system time manually and start the NTPD.
- **driftfile, logfile, statsdir**

  In these rows, you can specify the storage location of the **drift** and **protocol files**. To do this, write access rights are required.

  Activate the **logfile, statsdir** rows for error detection only.

  The quartz drift determined is stored in the **ntp.drift** file. This allows faster synchronization after a system start, because the clock can be set to the correct speed based on the offset value. If no writeable (and reset-proof!) file system is available, the drift file can be disabled. In this case, optimum synchronization can be achieved only some time after a system start. This can take several hours.

Reference Clocks



```
#------------------------------------------------------------------------------
# reference clocks
#------------------------------------------------------------------------------
# -- local system clock
# the local system clock is used as level 10 fallback if everything fails and
# the server must continue to operate because of (S)NTP clients like
# IEC61850 devices et al.
server 127.127.1.0
fudge 127.127.1.0 stratum 10

# -- HOPF6039 receiver
# mode 53-->bail out if no radio operation possible.
#server 127.127.39.0 mode 53 minpoll 2 maxpoll 6 prefer iburst
# Windows 7 recommendation: minpoll 4 maxpoll 4
```

Figure 6-2 ntp.conf - Reference Clocks

Using the lines under **local system clock**, you can define the local clock as the timer. Define a high value for the stratum. The local time is used unless another, better time base is available.

In the lines under **Hopf6039** receiver, you can define the use of a **Hopf6039** card.

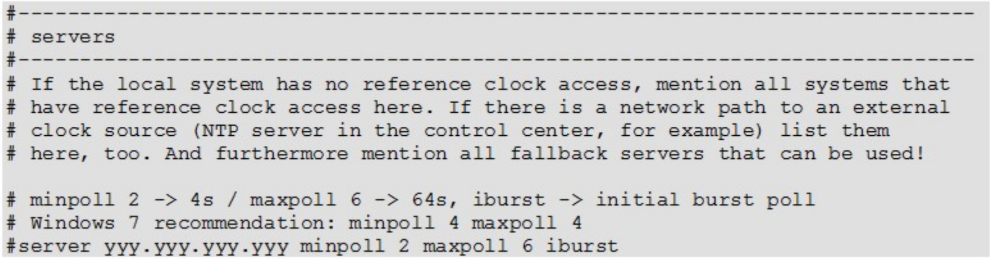
- **mode**

  With mode 53 (see *Table 6-2*), no time is polled from the card if it cannot receive data.
- **minpoll, maxpoll**

  The time is to be polled at intervals of between 4 s and 64 s. The values of minpoll and maxpoll are the exponents from a base of 2 ($2^2 = 4$, $2^6 = 64$).
- **iburst**

  The **iburst** parameter ensures that 5 values per second are read during the first poll. The internal filters enter a steady state, which ensures that synchronization can be achieved within an even shorter time.

Servers



```
#------------------------------------------------------------------------------
# servers
#------------------------------------------------------------------------------
# If the local system has no reference clock access, mention all systems that
# have reference clock access here. If there is a network path to an external
# clock source (NTP server in the control center, for example) list them
# here, too. And furthermore mention all fallback servers that can be used!

# minpoll 2 -> 4s / maxpoll 6 -> 64s, iburst -> initial burst poll
# Windows 7 recommendation: minpoll 4 maxpoll 4
#server yyy.yyy.yyy.yyy minpoll 2 maxpoll 6 iburst
```

Figure 6-3 ntp.conf - Servers

The following rows serve as examples for the definition of time servers. They are used for demo purposes only. In a "real" environment, the user must enter the parameters for real time servers.

server 139.25.31.13 minpoll 2 maxpoll 6 iburst

server 139.25.208.27 minpoll 2 maxpoll 6 iburst server ntp.lpz.siemens.de minpoll 2 maxpoll 6 iburst

6.6 Driver for the Hopf6039 Card

The Hopf6039 card is a PCI card with a DCF77 or GPS receiver with a clock function. With a clock time precision of 1 ms, the operating system can achieve a resolution of up to 1 ms. With the modified driver for the Hopf6039 card, the resolution can be improved in the edge polling mode.

The quartz oscillator integrated in the Hopf6039 card is more stable than the oscillator of a standard computer. By combining the Hopf6039 card with NTPD, a time precision of less than 1 ms can be maintained for another 2 hours even if no time signal can be received after a stabilization phase of several hours.

Different modes can be set on the modified driver in order to determine the behavior of the driver in case of error (that is, no time signal received from the clock). The driver can increase the value of the stratum and mark the clock as erroneous.

A typical line in the configuration file for a Hopf6039 card provides the following information types:

server 127.127.39.0 mode 53 minpoll 2 maxpoll 6 prefer iburst

The **mode 53** parameter must be interpreted as a bit pattern (decimal value). The following tables illustrate the significance of the bits.

Table 6-1 Bit Pattern of Mode 53

Bit	7	6	5	4	3	2	1	0
Bit pattern	0	0	1	1	0	1	0	1
Value	1			1	5			

Table 6-2 Parameter Mode 53

Bit position	Meaning
Bit 0 to 3	Stratum drop In case of error, this value is added to the stratum (see *Table 6-3*)
Bit 4	Edge polling mode The Hopf6039 card does not support interruptions. The card has a resolution of 1 ms, but maintains the clock time with far higher precision. During the first reading of the time stamp, a statistical error of +/- 0.5 is detected; due to repeated readings until the change of the value read, this error can be reduced to 1/10th of the original value. This method enables faster synchronization. If Bit 4 is set, repeated reading until the value changes is activated.
Bit 5 to 7	Dropout mode These bits determine the behavior in case of error (see *Table 6-3*).

Table 6-3 Parameter Mode

Dropout mode	Stratum drop	Meaning
0	0	The connection to the satellite is not checked, but rather the status of the internal clock. If the clock indicates that it is synchronized only by the internal quartz, the driver marks the clock as erroneous. The time signal is no longer polled. This behavior is identical with the behavior of the unmodified clock driver.
0	1 to 15	Time information is still polled, even if the clock is synchronized only by the internal quartz. However, the driver adds the **stratum drop** value to the stratum of the clock. The value of the stratum is limited to 15.

Dropout mode	Stratum drop	Meaning
1	1 to 15	The driver determines from how many satellites the clock receives time signals. If a clock does not receive time signals from any satellite, the **stratum drop** value is added to the stratum of the clock. The time signal is no longer polled if the clock is synchronized only by the internal quartz.
2	0	Time information is still polled, even if the clock is synchronized only by the internal quartz. This behavior is identical with the behavior of the unmodified clock driver, if the **fudge1** flag of this driver is set to **1**.
2	1 to 15	The driver determines from how many satellites the clock receives time signals. If a clock does not receive time signals from any satellite, the **stratum drop** value is added to the stratum of the clock. Time information is still polled, even if the clock is synchronized only by the internal quartz.

6.7 Sample Configurations

6.7.1 Overview

This chapter illustrates typical sample configurations. It describes the distribution of time information in the system and presents the configuration files of the NTPDs.

- In the first example, a Hopf PCI card is used. It is incorporated in a SIGUARD PDP Server.
- In the second example, the time is specified by an external radio clock or an NTP timer. The radio clock or an NTP timer is connected directly to the Ethernet.

6.7.2 PCI Card as Timer

The Hopf **FG6039GPS** PCI card is incorporated in the SIGUARD PDP Server and used as the timing master of the system. Other clocks can become the timing master only if the PCI card fails or if its time information is of poor quality.

The NTPD is active on the SIGUARD PDP UI computer as well as the SIGUARD PDP Engineer computer:

- On the SIGUARD PDP Server as server
- On the SIGUARD PDP UI computer and the SIGUARD PDP Engineer computer as client

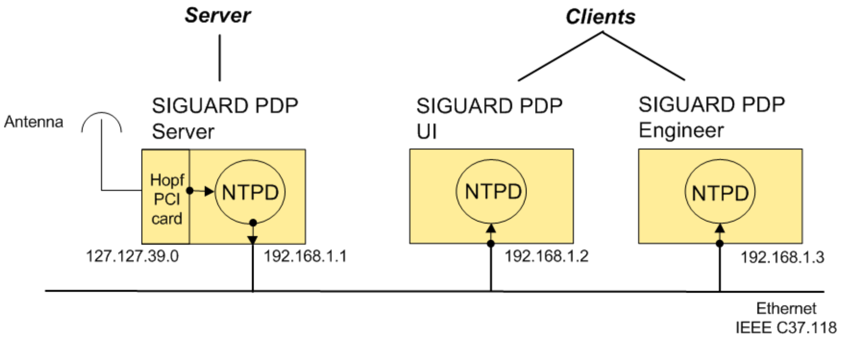


Figure 6-4 Time synchronization with the Hopf6039 card in the SIGUARD PDP Server (example)

NOTE

The time of the PMUs is synchronized via GPS at the control center (at the bay level).

Configuration Files

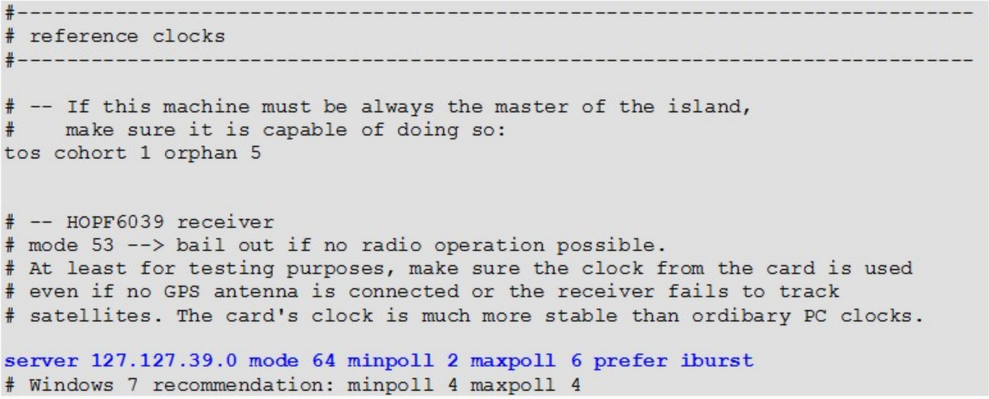
In the following sections, the configuration files **ntp.conf** for the SIGUARD PDP Server and the clients (SIGUARD PDP UI computer and SIGUARD PDP Engineer computer) are listed. The entries in the list have been customized for the example illustrated. Be aware that, in practice, the real system configuration (for example, IP addresses) must be considered.

Changes to the predefined configuration files have been highlighted.

6.7.3 PCI Card Configuration Files

6.7.3.1 Configuration File - Server

Configuration file for the **SIGUARD PDP Server**:



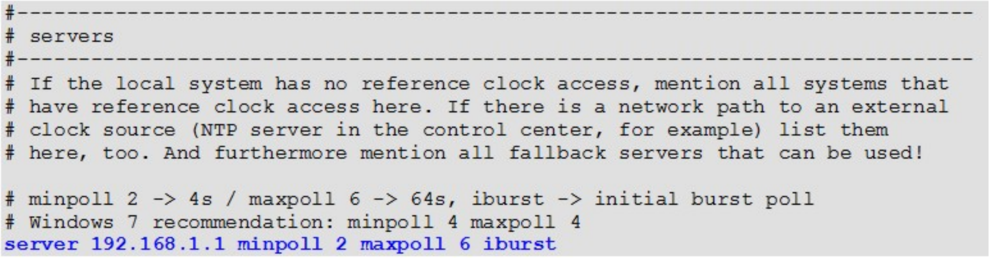
```
#------------------------------------------------------------------------------
# reference clocks
#------------------------------------------------------------------------------

# -- If this machine must be always the master of the island,
#    make sure it is capable of doing so:
tos cohort 1 orphan 5


# -- HOPF6039 receiver
# mode 53 --> bail out if no radio operation possible.
# At least for testing purposes, make sure the clock from the card is used
# even if no GPS antenna is connected or the receiver fails to track
# satellites. The card's clock is much more stable than ordibary PC clocks.

server 127.127.39.0 mode 64 minpoll 2 maxpoll 6 prefer iburst
# Windows 7 recommendation: minpoll 4 maxpoll 4
```

Figure 6-5 ntp.conf - Reference Clocks

In the row marked in blue, enter the IP address of the Hopf card (for example, 127.127.39.0).

6.7.3.2 Configuration File - Clients

Configuration file for the clients (**SIGUARD PDP UI computer** and **SIGUARD PDP Engineer computer**):



```
#------------------------------------------------------------------------------
# servers
#------------------------------------------------------------------------------
# If the local system has no reference clock access, mention all systems that
# have reference clock access here. If there is a network path to an external
# clock source (NTP server in the control center, for example) list them
# here, too. And furthermore mention all fallback servers that can be used!

# minpoll 2 -> 4s / maxpoll 6 -> 64s, iburst -> initial burst poll
# Windows 7 recommendation: minpoll 4 maxpoll 4
server 192.168.1.1 minpoll 2 maxpoll 6 iburst
```

Figure 6-6 ntp.conf - Servers

In the row marked in blue, enter the IP address of the SIGUARD PDP Server (for example, 192.168.1.1) as reference from the client to the server.

6.7.4 External Radio Clock or NTP Time Server as Timer

With this system configuration, an **external radio clock** (for example, SICLOCK, Meinberg, Hopf) or an NTP time server is used as timing master on the Ethernet. If this clock fails or if the quality of the time information is poor, another clock available in the system becomes the timing master. You can define which clock will be the new timing master in the configuration files of the NTPDs.

The NTPD is active on the SIGUARD PDP Server as well as on the SIGUARD PDP UI computer and the SIGUARD PDP Engineer computer. The NTPD of the radio clock or of the NTP time server is the time server, the NTPDs of the SIGUARD computers are the clients.

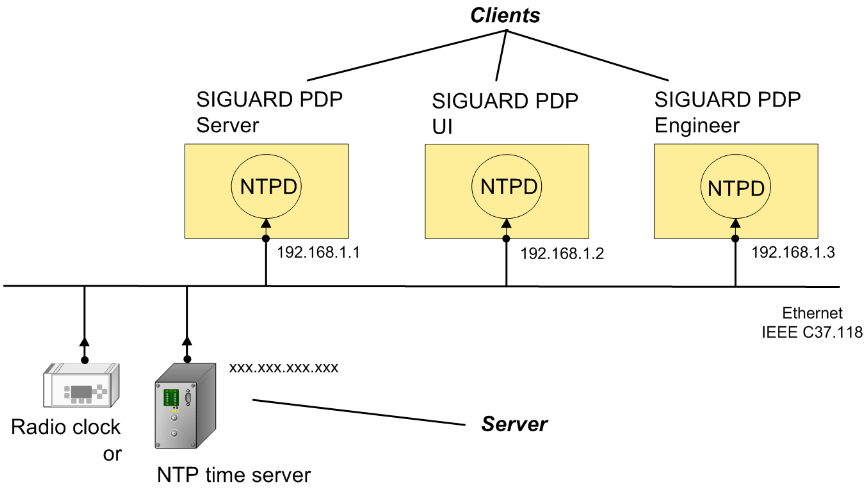


Figure 6-7 Time Synchronization via External Radio Clock or NTP Time Server

NOTE

The time of the PMUs is synchronized via GPS at the control center (at the bay level).

Configuration Files

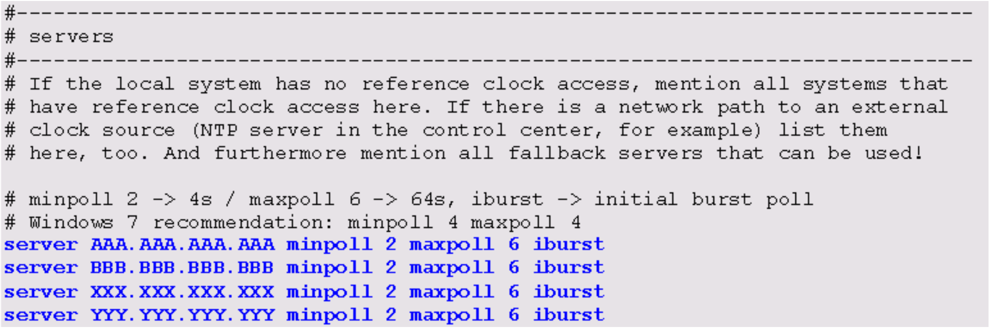
In the following sections, the configuration files **ntp.conf** for the NTP Clients are listed. The entries in the list have been customized for the example illustrated. Be aware that, in practice, the real system configuration (for example, IP addresses) must be considered.

Changes to the predefined configuration files have been highlighted.

6.7.5 NTP Configuration File

6.7.5.1 Configuration File - Clients

Configuration file for the Clients (**SIGUARD PDP Server**, **SIGUARD PDP UI computer** and **SIGUARD PDP Engineer computer**):



```
#------------------------------------------------------------------------------
# servers
#------------------------------------------------------------------------------
# If the local system has no reference clock access, mention all systems that
# have reference clock access here. If there is a network path to an external
# clock source (NTP server in the control center, for example) list them
# here, too. And furthermore mention all fallback servers that can be used!

# minpoll 2 -> 4s / maxpoll 6 -> 64s, iburst -> initial burst poll
# Windows 7 recommendation: minpoll 4 maxpoll 4
server AAA.AAA.AAA.AAA minpoll 2 maxpoll 6 iburst
server BBB.BBB.BBB.BBB minpoll 2 maxpoll 6 iburst
server XXX.XXX.XXX.XXX minpoll 2 maxpoll 6 iburst
server YYY.YYY.YYY.YYY minpoll 2 maxpoll 6 iburst
```

Figure 6-8 ntp.conf - Servers

In the rows marked in blue, enter the IP addresses of the available time servers. Only the entered time servers are polled.

NOTE

If a radio clock is used as a timer, then the settings of the respective manufacturer should be taken into account.

6.7.6 Completing Configuration

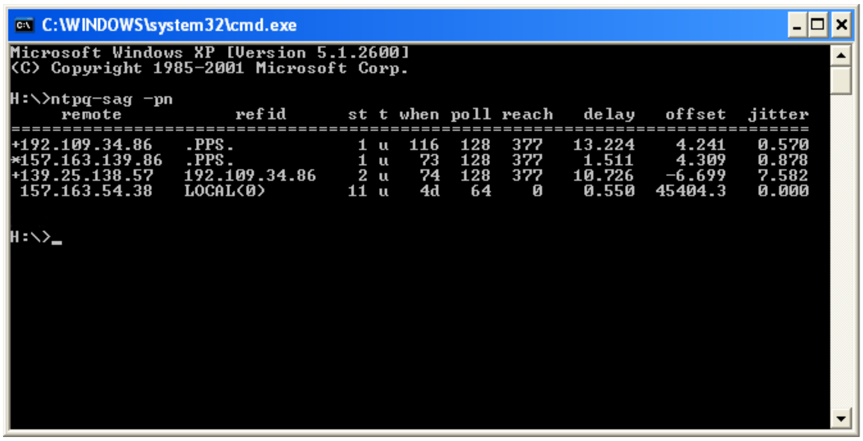
- Save the configuration files for servers and clients in the appropriate path of the computer.
- Start the **Network Time Protocol** service again.

  The procedure for starting the **Network Time Protocol** is the same as described in chapter *4.3 OPC Server Configuration*.

6.8 Poll NTP Driver

With the following command, you can poll the NTP driver, in order to see whether it is working properly:

- Open the input window.
- Enter the command **ntpq-seq -pn**.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

H:\>ntpq-sag -pn
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
+192.109.34.86   .PPS.            1 u  116  128  377   13.224    4.241   0.570
*157.163.139.86  .PPS.            1 u   73  128  377    1.511    4.309   0.878
+139.25.138.57   192.109.34.86    2 u   74  128  377   10.726   -6.699   7.582
 157.163.54.38   LOCAL(0)        11 u   4d   64    0    0.550  45404.3   0.000


H:\>_
```

Figure 6-9 Result of the NTP Driver Query

For each NTP time server entered, a row is shown as the result of the poll. The *** symbol** shows that this time server is currently being used. The **+ symbol** shows that there is a connection to these time servers as well, and that an analysis of their time is taking place.

The parameter **reach** shows how many successful polls with the time server have occurred. The value **377** should be attained.

For further information, see *http://www.ntp.org/documentation.html*

■

7 Security Settings

7.1 Overview

Many different aspects must be considered in order to protect a complex system (such as the SIGUARD PDP network). This chapter describes some important aspects which can provide additional protection of the network. Further information on security you can find in chapter *1.2 Recommended Actions that Make Your System More Secure* and in chapter *1.3 Recommended Rules for Improving the Security Process*.

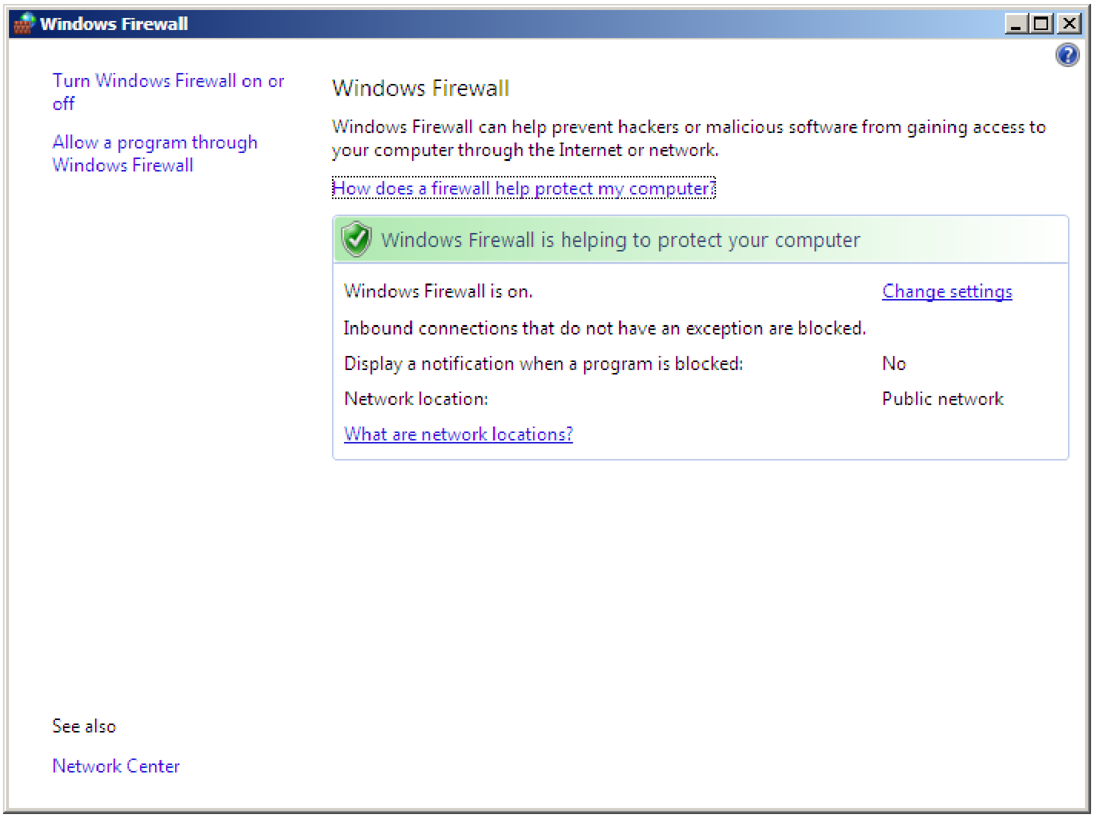
7.2 The Desktop Firewall

General

Siemens recommends activating the Windows Firewall on the SIGUARD PDP Server. For a pure SIGUARD PDP Server application, only some ports and service are required.

Setting up the Firewall

- On the SIGUARD PDP Server, open the window **Windows Firewall** via **Start > Settings > Control Panel > Windows Firewall**.


Windows Firewall
Turn Windows Firewall on or off
Allow a program through Windows Firewall
See also
Network Center

Windows Firewall

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

How does a firewall help protect my computer?

Windows Firewall is helping to protect your computer

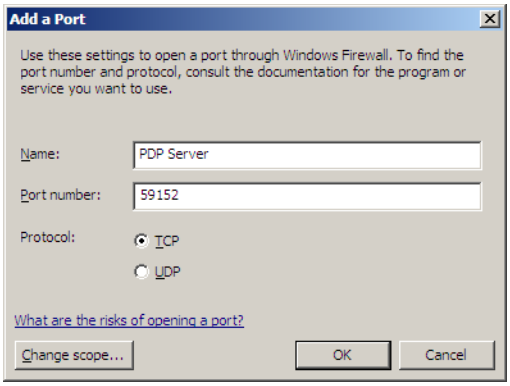
Windows Firewall is on.	Change settings
Inbound connections that do not have an exception are blocked.	
Display a notification when a program is blocked:	No
Network location:	Public network
What are network locations?	

Figure 7-1 Windows Firewall

- Select **Change settings**.
- Activate the firewall.

Add a port for the SIGUARD PDP Server which receives incoming connections.

- Open the window **Add a port**.



Add a Port

Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name: PDP Server

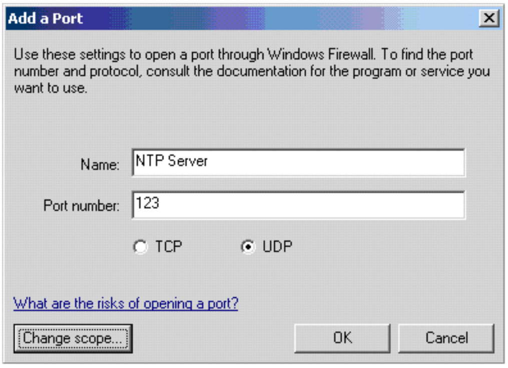
Port number: 59152

Protocol: ● TCP ○ UDP

Figure 7-2 Add TCP Port on the SIGUARD PDP Server

- Enter *PDP Server* as a name for the port.
- Assign the **Port number**, for example, *59152*.
- Set the protocol to **TCP**.
- Click **OK** to close the dialog.

If the SIGUARD PDP Server is used as **NTP Server**, incoming connections must also be accepted at UDP Port 123.



Add a Port

Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name: NTP Server

Port number: 123

○ TCP ● UDP

Figure 7-3 Add UDP Port on the NTP Server

- Enter *NTP Server* as a name for the port.
- Assign the **Port number**, for example, *123*.
- Set the protocol to **UDP**.
- Click **OK** to close the dialog.

In addition to the basic services of the network, exceptions must be defined for the firewall:

- File and Printer Sharing

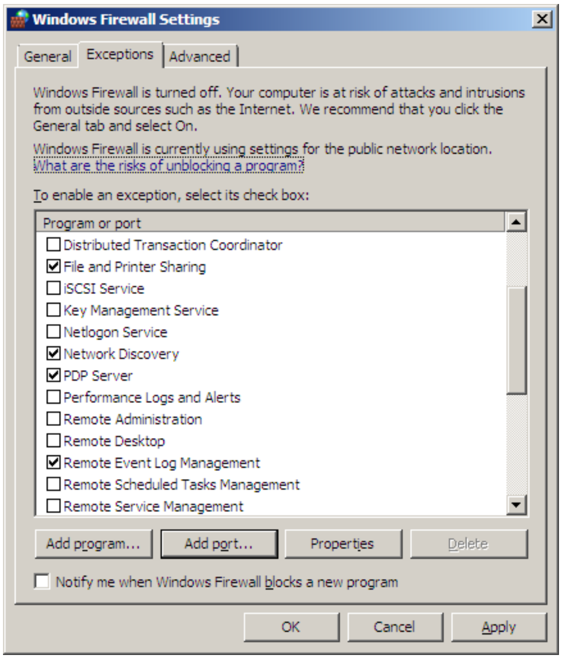
  File and Printer Sharing (Port 139/445) for a shared folder on the SIGUARD PDP Server
- Network Discovery

  Display of the network, if desired
- PDP Server

  The defined port for the SIGUARD PDP Server
- Remote Event Log Management

  For remote access to the events protocol file

✧ Open the window **Windows Firewall Settings**.



Windows Firewall is turned off. Your computer is at risk of attacks and intrusions from outside sources such as the Internet. We recommend that you click the General tab and select On.

Windows Firewall is currently using settings for the public network location.
What are the risks of unblocking a program?

To enable an exception, select its check box:

Program or port
☐ Distributed Transaction Coordinator
☑ File and Printer Sharing
☐ iSCSI Service
☐ Key Management Service
☐ Netlogon Service
☑ Network Discovery
☑ PDP Server
☐ Performance Logs and Alerts
☐ Remote Administration
☐ Remote Desktop
☑ Remote Event Log Management
☐ Remote Scheduled Tasks Management
☐ Remote Service Management

☐ Notify me when Windows Firewall blocks a new program

Figure 7-4 Exceptions

✧ Select the corresponding exceptions.

✧ Add the ports with **Add port...**.

✧ Click **OK** to close the dialog.

7.3 Logging

7.3.1 General

Regulations, such as NERC-CIP or BDEW Security Whitepaper, require records of changes and security-relevant activities. Changing the user password or a configuration change for retracing in the event of an error or foreign interventions count as security-relevant activities. Beyond this, the central recordings are a prerequisite for a good overview and for simplified fault search by Siemens.

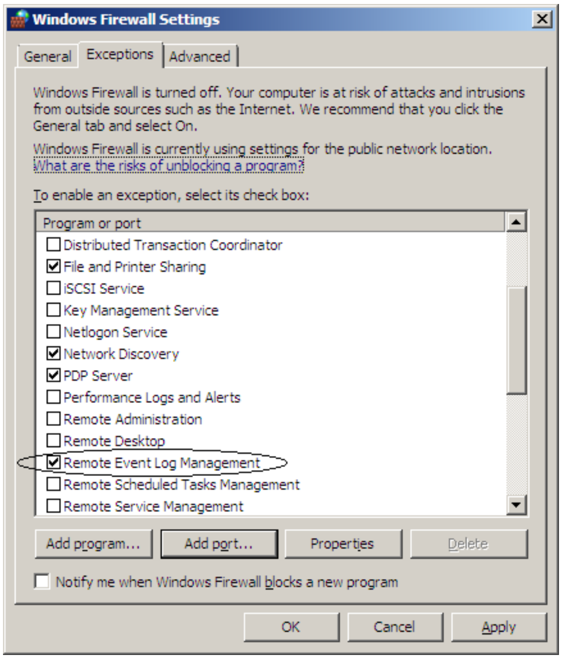
Central logging (recording of events in a protocol file) by Microsoft, which also contains system-native programs, is not so simple. It is not possible to record all relevant log data on a central Syslog Server. For this reason, a third-party software must be used, for example, **Datagram Syslog Agent**, which is distributed by Datagram Consulting as free software, see *website of Datagram Consulting*.

Microsoft Windows also supports remote access to recorded events via the included **Event Viewer**.

Note that some conditions must be satisfied in order to be able to view protocol files via remote access. In case of problems, see *Webpage Event Viewer Troubleshooting by Microsoft*.

- First, you need administrator rights on the remote computer, in order to be able to read protocol files. This user must also be created with the same password on the local computer. In order to attain the best security benefit, use **Run as**, in order to complete the process. Siemens recommends creating an audit administrator, who has administrator rights, on the remote computer and the local computer.
- In order to be able to view the designation and category fields in the properties window of an event recording, the **Remote Registry Service** must be started on some Windows operating systems.
- Once the firewall is activated as suggested, release the incoming data traffic for remote event recordings.

✧ Open the window **Windows Firewall Settings**.



Windows Firewall is turned off. Your computer is at risk of attacks and intrusions from outside sources such as the Internet. We recommend that you click the General tab and select On.

Windows Firewall is currently using settings for the public network location.
What are the risks of unblocking a program?

To enable an exception, select its check box:

Program or port
☐ Distributed Transaction Coordinator
☑ File and Printer Sharing
☐ iSCSI Service
☐ Key Management Service
☐ Netlogon Service
☑ Network Discovery
☑ PDP Server
☐ Performance Logs and Alerts
☐ Remote Administration
☐ Remote Desktop
☑ Remote Event Log Management
☐ Remote Scheduled Tasks Management
☐ Remote Service Management

☐ Notify me when Windows Firewall blocks a new program

Figure 7-5 Release Data Traffic for Remote Event Recordings

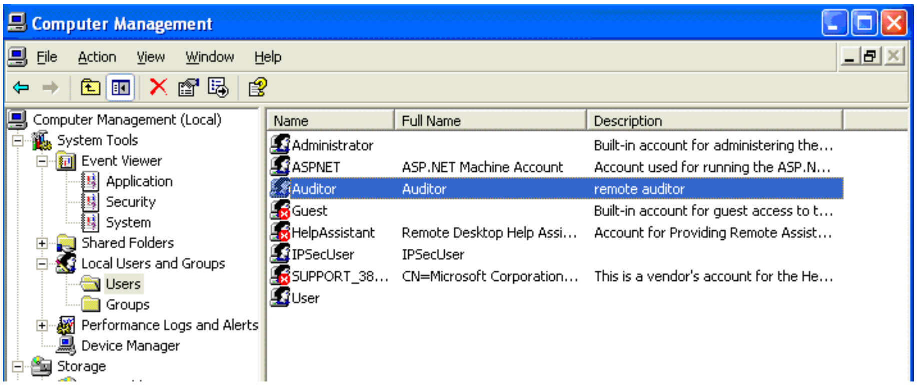
✧ Select **Remote Event Log Management**.

✧ Click **OK** to close the dialog.

7.3.2 Logging with the Event Viewer for Windows XP

Create User

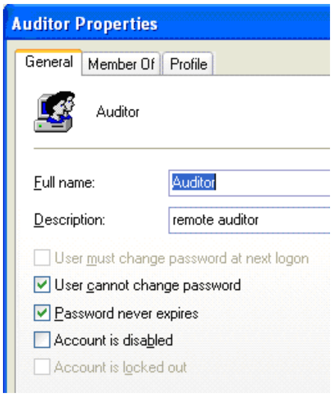
- ✧ Create a user with administrator rights on the local computer and the remote computer.
- ✧ Open the window **Computer Management** via the control panel.
- ✧ Select the user **Auditor**.



Name	Full Name	Description
Administrator		Built-in account for administering the…
ASPNET	ASP.NET Machine Account	Account used for running the ASP.N…
Auditor	Auditor	remote auditor
Guest		Built-in account for guest access to t…
HelpAssistant	Remote Desktop Help Assi…	Account for Providing Remote Assist…
IPSecUser	IPSecUser	
SUPPORT_38…	CN=Microsoft Corporation…	This is a vendor's account for the He…
User		

Figure 7-6 Computer Management with Selected User Auditor

- ✧ Double-click the properties window for this user.



Full name: Auditor

Description: remote auditor

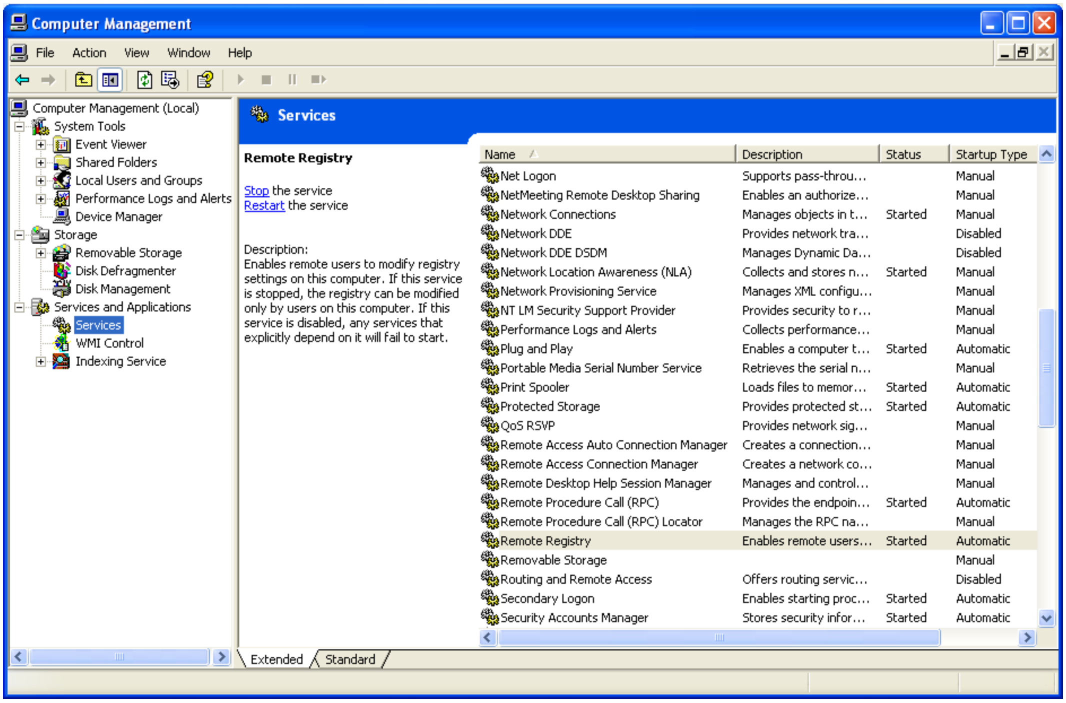
☐ User must change password at next logon
☑ User cannot change password
☑ Password never expires
☐ Account is disabled
☐ Account is locked out

Figure 7-7 Auditor Properties

- ✧ Establish the rights for this user on the tab **General**.
- ✧ Assign the new user in the user group on the tab **Member Of Administrators**.
- ✧ Next, click **OK** to confirm your settings.

Activate Remote Registry Service on the Remote Computer

- ✧ Open the window **Computer Management** via the control panel.
- ✧ Select the service **Remote Registry**.



Remote Registry

Stop the service
Restart the service

Description:
Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If this service is disabled, any services that explicitly depend on it will fail to start.

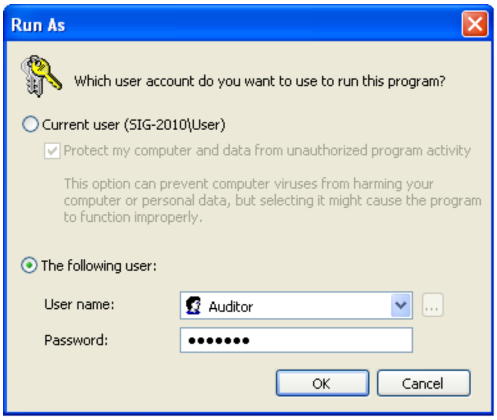
Name	Description	Status	Startup Type
Net Logon	Supports pass-throu...		Manual
NetMeeting Remote Desktop Sharing	Enables an authorize...		Manual
Network Connections	Manages objects in t...	Started	Manual
Network DDE	Provides network tra...		Disabled
Network DDE DSDM	Manages Dynamic Da...		Disabled
Network Location Awareness (NLA)	Collects and stores n...	Started	Manual
Network Provisioning Service	Manages XML configu...		Manual
NT LM Security Support Provider	Provides security to r...		Manual
Performance Logs and Alerts	Collects performance...		Manual
Plug and Play	Enables a computer t...	Started	Automatic
Portable Media Serial Number Service	Retrieves the serial n...		Manual
Print Spooler	Loads files to memor...	Started	Automatic
Protected Storage	Provides protected st...	Started	Automatic
QoS RSVP	Provides network sig...		Manual
Remote Access Auto Connection Manager	Creates a connection...		Manual
Remote Access Connection Manager	Creates a network co...		Manual
Remote Desktop Help Session Manager	Manages and control...		Manual
Remote Procedure Call (RPC)	Provides the endpoin...	Started	Automatic
Remote Procedure Call (RPC) Locator	Manages the RPC na...		Manual
Remote Registry	Enables remote users...	Started	Automatic
Removable Storage			Manual
Routing and Remote Access	Offers routing servic...		Disabled
Secondary Logon	Enables starting proc...	Started	Automatic
Security Accounts Manager	Stores security infor...	Started	Automatic

Figure 7-8 Remote Registry Service

- ✧ Stop the service with **Stop** or restart the service with **Restart**.
- ✧ Close the window **Computer Management**.

Start Event Viewer

- Since the Windows parameter **/auxsource** does not function here, start the **Event Viewer** manually the first time. Open the input window with the command **Start > Run > cmd** and enter the command **runas /netonly /user:auditor “mmc.exe /a eventvwr.exe"**.
- In the future, start the **Event Viewer** as the user **Auditor**. Right-click the object and select the program icon Event Viewer and select **Auditor** in the context menu.


Run As

Which user account do you want to use to run this program?

○ Current user (SIG-2010\User)

☑ Protect my computer and data from unauthorized program activity

This option can prevent computer viruses from harming your computer or personal data, but selecting it might cause the program to function improperly.

● The following user:

User name: Auditor

Password: •••••••

Figure 7-9 Logon as Auditor

- Select the user name *Auditor*.
- Enter the correct password.
- Click **OK** to close the dialog.

Establish a Connection with Another Computer

- In the window **Event Viewer**, select the main directory **Event Viewer**
- Right-click to open the context menu **Connect to another computer...**.

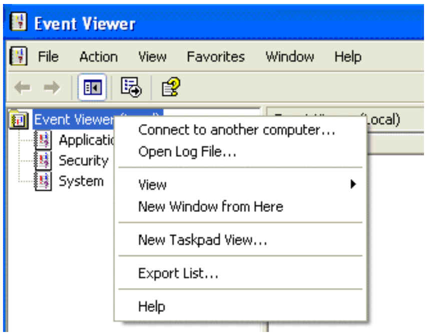
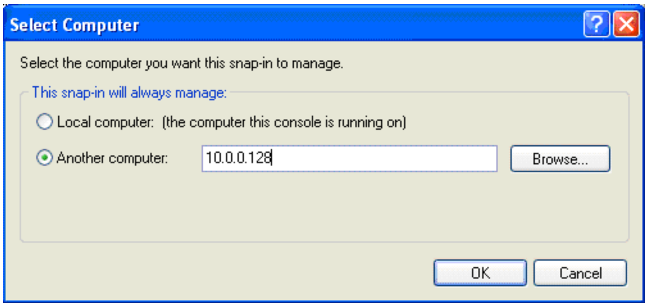


Figure 7-10 Context Menu Connect to another computer...

✧ Enter the **IP address** or the **Domain Name** of the remote computer.



Select the computer you want this snap-in to manage.

This snap-in will always manage:

○ Local computer: (the computer this console is running on)

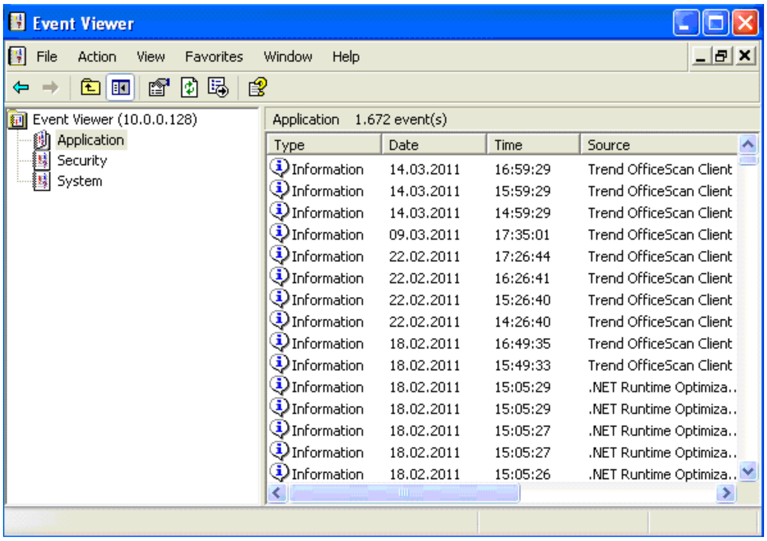
● Another computer: 10.0.0.128

Figure 7-11 Event Viewer, Set up Remote Connection

✧ Click **OK** to close the dialog.

View Protocol Files

✧ In the window **Event Viewer**, select the main directory **Application**



Application 1.672 event(s)

Type	Date	Time	Source
Information	14.03.2011	16:59:29	Trend OfficeScan Client
Information	14.03.2011	15:59:29	Trend OfficeScan Client
Information	14.03.2011	14:59:29	Trend OfficeScan Client
Information	09.03.2011	17:35:01	Trend OfficeScan Client
Information	22.02.2011	17:26:44	Trend OfficeScan Client
Information	22.02.2011	16:26:41	Trend OfficeScan Client
Information	22.02.2011	15:26:40	Trend OfficeScan Client
Information	22.02.2011	14:26:40	Trend OfficeScan Client
Information	18.02.2011	16:49:35	Trend OfficeScan Client
Information	18.02.2011	15:49:33	Trend OfficeScan Client
Information	18.02.2011	15:05:29	.NET Runtime Optimiza..
Information	18.02.2011	15:05:29	.NET Runtime Optimiza..
Information	18.02.2011	15:05:27	.NET Runtime Optimiza..
Information	18.02.2011	15:05:27	.NET Runtime Optimiza..
Information	18.02.2011	15:05:26	.NET Runtime Optimiza..

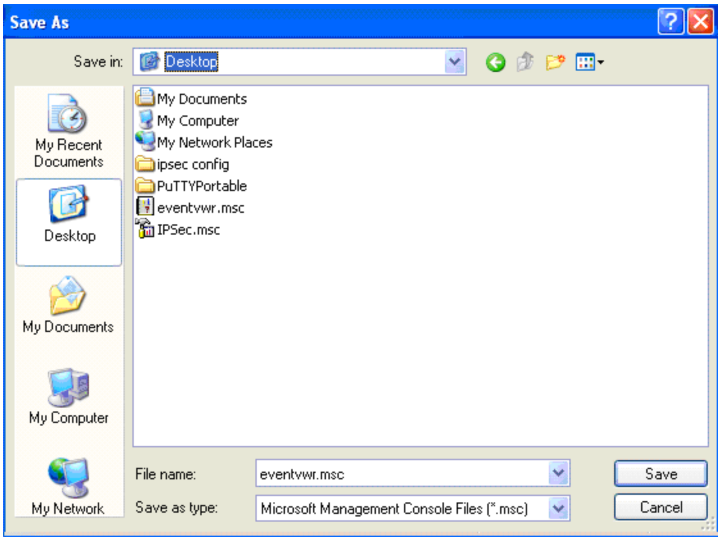
Figure 7-12 Event Viewer on the Remote Computer

All events are listed in the right-hand window section.

Save the Remote Access Configuration

Save this in order to get fast access to your configuration data in the future.

- In the Event Viewer, select the menu **File > Save As...**



Save in: Desktop

File name: eventvwr.msc

Save as type: Microsoft Management Console Files (*.msc)

Figure 7-13 Save Remote Access Configuration

- Select any path.
- Save by clicking **Save**.
- Click **OK** to close the dialog.

Save the Protocol Files

In this way, you can save protocol files via the **Event Viewer** in the format **.txt** or **.csv**.

- Select the directory **Application** in the **Event Viewer** and open the context menu **Save Log File As...**

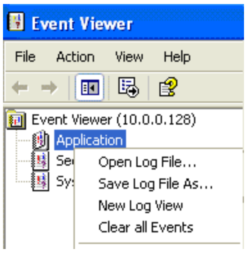


Figure 7-14 Context Menu Save Log File As...

- Enter any file name.
- Select any path.
- Save by clicking **Save**.

NOTE

Saving a protocol file in the format **.evt** is not possible during remote access.

7.3.3 Logging with the Event Viewer for Windows 7 (Local Computer) and Windows Server 2008 (Remote Computer)

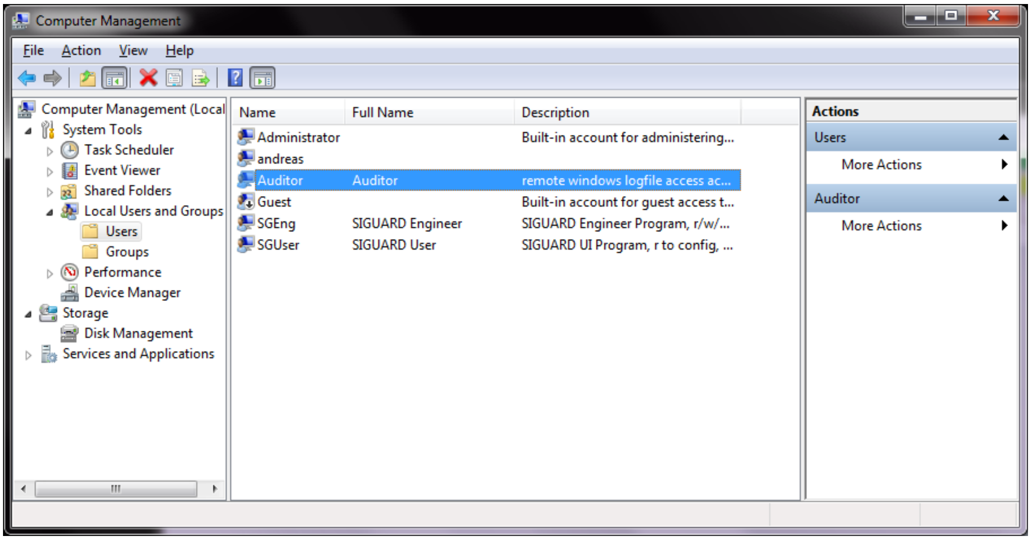
Create User

- Create a user **Auditor** with administrator rights on the local computer and the remote computer.

NOTE

For reasons of consistency, note that the same user name and the same password are always assigned on the local computer and on the remote computer.

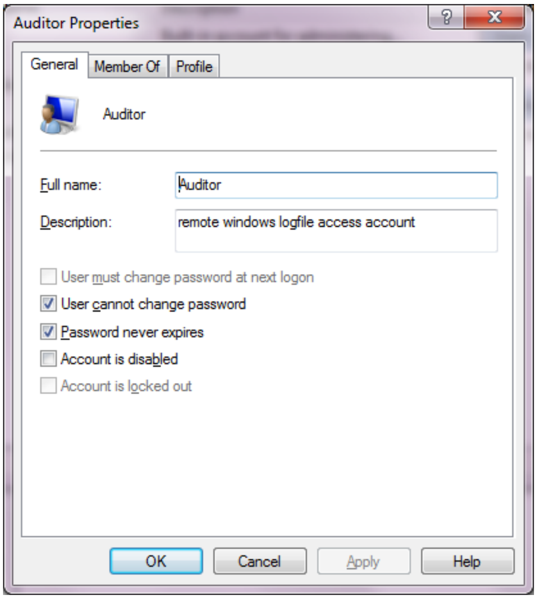
- Open the window **Computer Management** via the control panel.
- Select the user **Auditor**.



Name	Full Name	Description
Administrator		Built-in account for administering...
andreas		
Auditor	Auditor	remote windows logfile access ac...
Guest		Built-in account for guest access t...
SGEng	SIGUARD Engineer	SIGUARD Engineer Program, r/w/...
SGUser	SIGUARD User	SIGUARD UI Program, r to config, ...

Figure 7-15 Computer Management

- Double-click the properties window for this user.



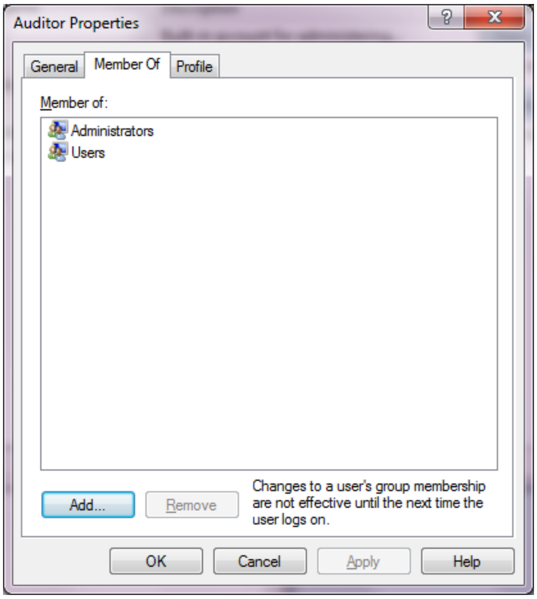
Full name: Auditor

Description: remote windows logfile access account

☐ User must change password at next logon
☑ User cannot change password
☑ Password never expires
☐ Account is disabled
☐ Account is locked out

Figure 7-16 Auditor Properties - General

- ✧ Establish the rights for this user on the tab **General**.
- ✧ To assign the new user in the user group **Administrators**, select the tab **Member Of**.



Member of:
Administrators
Users

Changes to a user's group membership are not effective until the next time the user logs on.

Figure 7-17 Auditor Properties - Member Of

The user **Auditor** is assigned to the user groups **Administrators** and **Users**.

- ✧ Next, click **OK** to confirm your settings.

Authorize the Remote Event Recordings

✧ In the window **Windows Firewall Settings**, select **Remote Event Log Management** on the tab **Exceptions**.

For further information, see *7.1 Overview*.

Start the Event Viewer

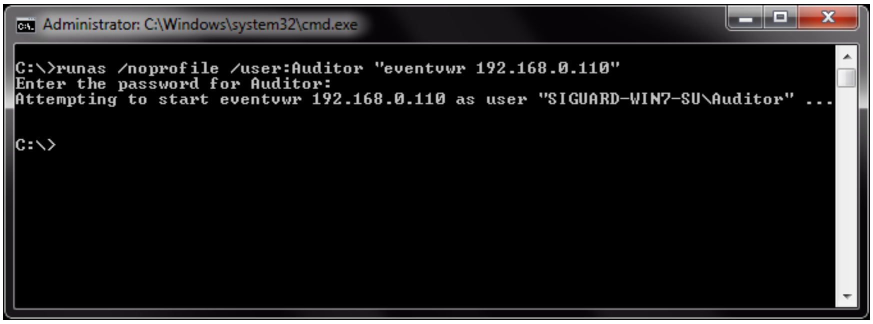
Under Windows 7/Server 2008, you can start the **Event Viewer** via the following elements:

- The user interface or
- The input window.

✧ At the user interface, start the **Event Viewer** from the menu **All Programs > Administrative Tools > Event Viewer**

-- or --

✧ Start the **Event Viewer** via the input window.



```
C:\>runas /noprofile /user:Auditor "eventvwr 192.168.0.110"
Enter the password for Auditor:
Attempting to start eventvwr 192.168.0.110 as user "SIGUARD-WIN7-SU\Auditor" ...

C:\>
```

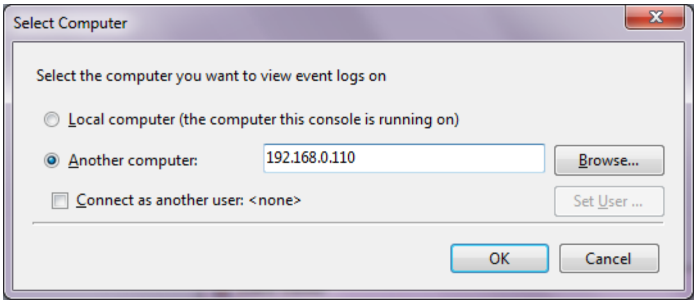
Figure 7-18 Starting the Event Viewer via the Input Window

The window **Event Viewer** opens.

Establish a Connection with Another Computer

✧ In the **Event Viewer**, open the menu **Action > Connect to another Computer...**.

✧ Select **Another Computer** and enter the IP address or the domain name of the remote computer.



Select the computer you want to view event logs on

○ Local computer (the computer this console is running on)

● Another computer: 192.168.0.110

☐ Connect as another user: <none>

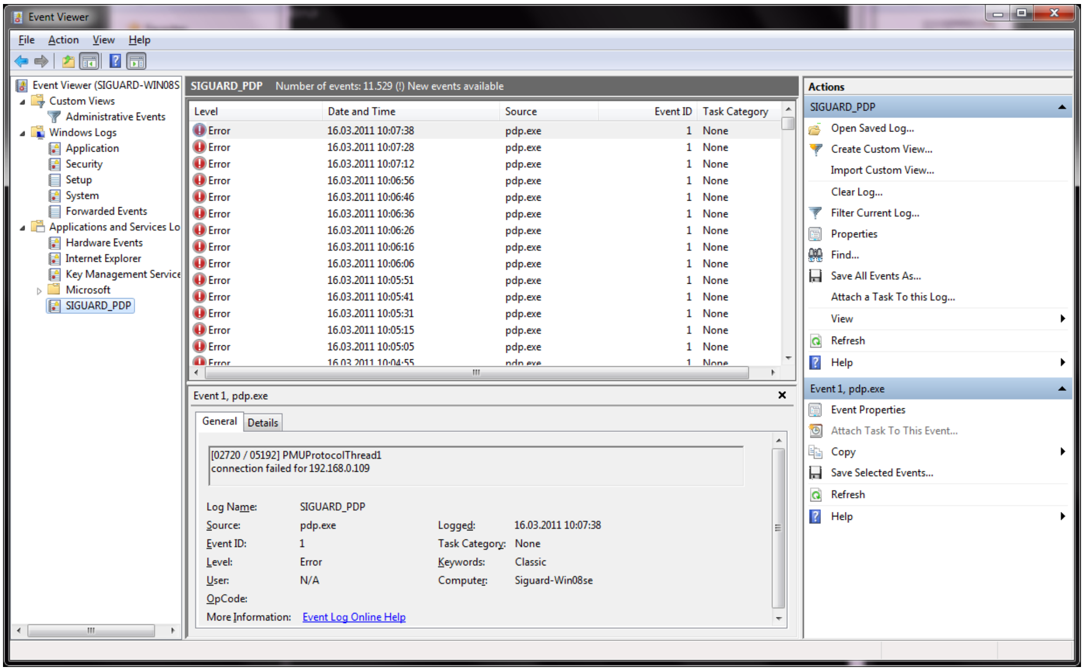
Figure 7-19 Event Viewer, Set Up Remote Connection

✧ Click **OK** to close the dialog.

View Protocol Files

The SIGUARD PDP Server has its own area where error messages can be displayed.

✧ Under **Applications and Services Logs**, select the subdirectory **SIGUARD_PDP**.



SIGUARD_PDP Number of events: 11.529 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Error	16.03.2011 10:07:38	pdp.exe	1	None
Error	16.03.2011 10:07:28	pdp.exe	1	None
Error	16.03.2011 10:07:12	pdp.exe	1	None
Error	16.03.2011 10:06:56	pdp.exe	1	None
Error	16.03.2011 10:06:46	pdp.exe	1	None
Error	16.03.2011 10:06:36	pdp.exe	1	None
Error	16.03.2011 10:06:26	pdp.exe	1	None
Error	16.03.2011 10:06:16	pdp.exe	1	None
Error	16.03.2011 10:06:06	pdp.exe	1	None
Error	16.03.2011 10:05:51	pdp.exe	1	None
Error	16.03.2011 10:05:41	pdp.exe	1	None
Error	16.03.2011 10:05:31	pdp.exe	1	None
Error	16.03.2011 10:05:15	pdp.exe	1	None
Error	16.03.2011 10:05:05	pdp.exe	1	None
Error	16.03.2011 10:04:55	pdp.exe	1	None

Event 1, pdp.exe

```
[02720 / 05192] PMUProtocolThread1
connection failed for 192.168.0.109
```

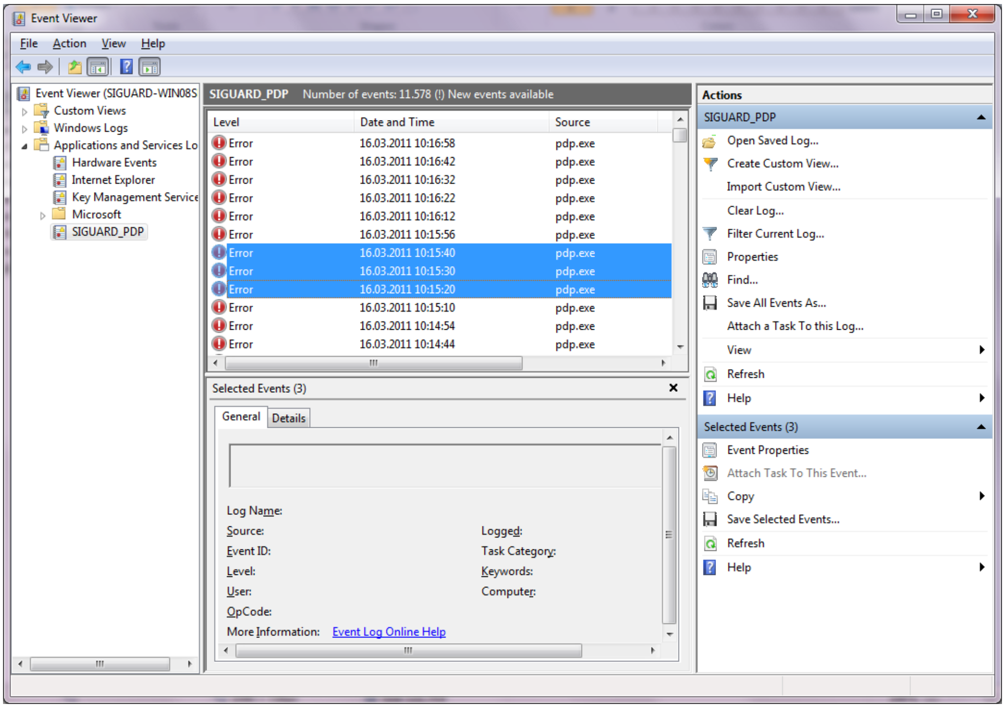
Log Name: SIGUARD_PDP
Source: pdp.exe
Logged: 16.03.2011 10:07:38
Event ID: 1
Task Category: None
Level: Error
Keywords: Classic
User: N/A
Computer: Siguard-Win08se
OpCode:
More Information: Event Log Online Help

Figure 7-20 Event Viewer in Remote Access

All SIGUARD PDP Server events are displayed here.

Save the Protocol Files

✧ In the **Event Viewer**, select error messages (rows) that you would like to save.



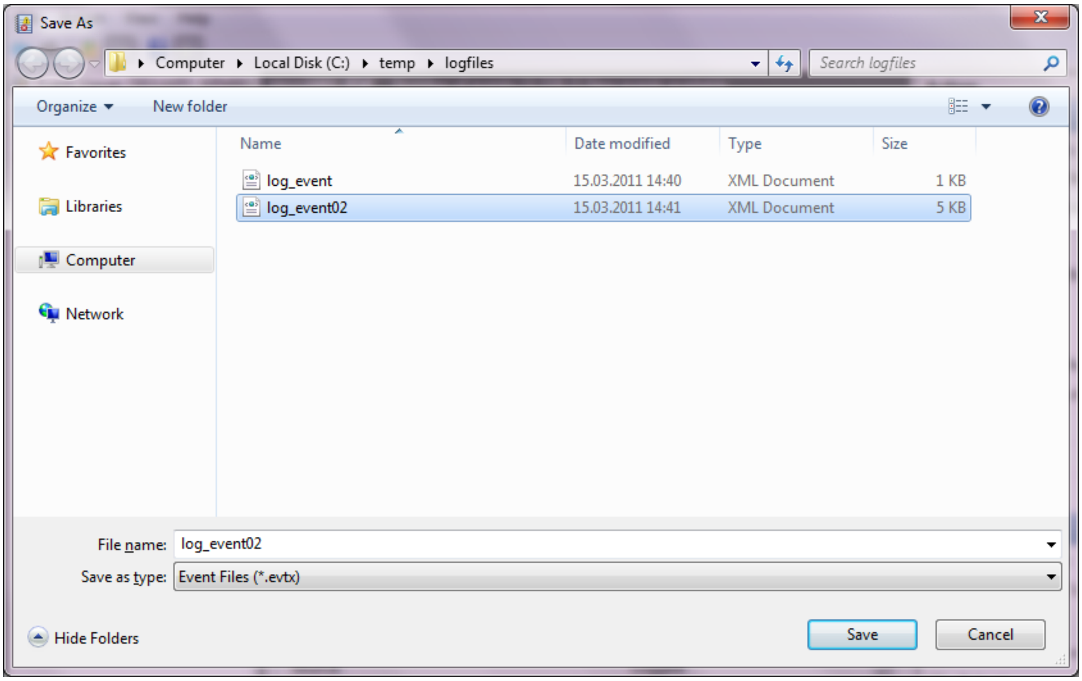
SIGUARD_PDP Number of events: 11.578 (!) New events available

Level	Date and Time	Source
Error	16.03.2011 10:16:58	pdp.exe
Error	16.03.2011 10:16:42	pdp.exe
Error	16.03.2011 10:16:32	pdp.exe
Error	16.03.2011 10:16:22	pdp.exe
Error	16.03.2011 10:16:12	pdp.exe
Error	16.03.2011 10:15:56	pdp.exe
Error	16.03.2011 10:15:40	pdp.exe
Error	16.03.2011 10:15:30	pdp.exe
Error	16.03.2011 10:15:20	pdp.exe
Error	16.03.2011 10:15:10	pdp.exe
Error	16.03.2011 10:14:54	pdp.exe
Error	16.03.2011 10:14:44	pdp.exe

Log Name:
Source: Logged:
Event ID: Task Category:
Level: Keywords:
User: Computer:
OpCode:
More Information: Event Log Online Help

Figure 7-21 Selected Error Messages

✧ In the window **Actions**, select the menu item **Save Selected Events...**



Name	Date modified	Type	Size
log_event	15.03.2011 14:40	XML Document	1 KB
log_event02	15.03.2011 14:41	XML Document	5 KB

File name: log_event02
Save as type: Event Files (*.evtx)

Figure 7-22 Save As...

✧ Enter a file name.

✧ Select the file format.

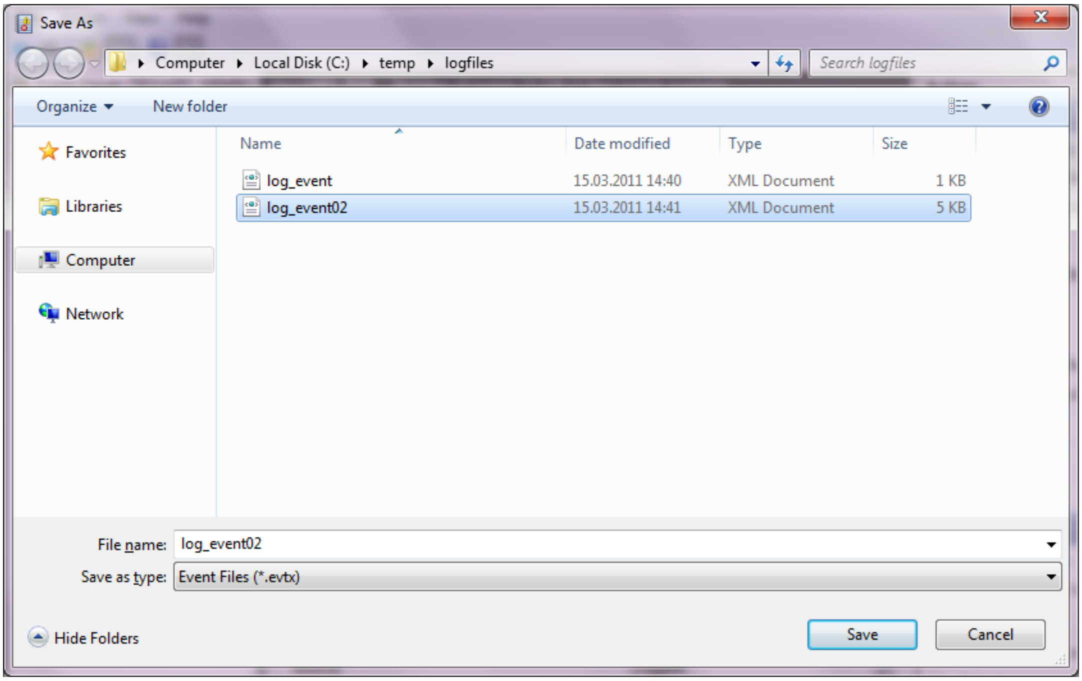
✧ Click **Save** to close the dialog.

Save Protocols in Text or XML Format

Protocol files can be saved in the following formats:

- Text format
- XML format

✧ In the window **Actions**, select the menu item **Save All Events As...**



Name	Date modified	Type	Size
log_event	15.03.2011 14:40	XML Document	1 KB
log_event02	15.03.2011 14:41	XML Document	5 KB

File name: log_event02

Save as type: Event Files (*.evtx)

Figure 7-23 Save As...

✧ Enter a file name.

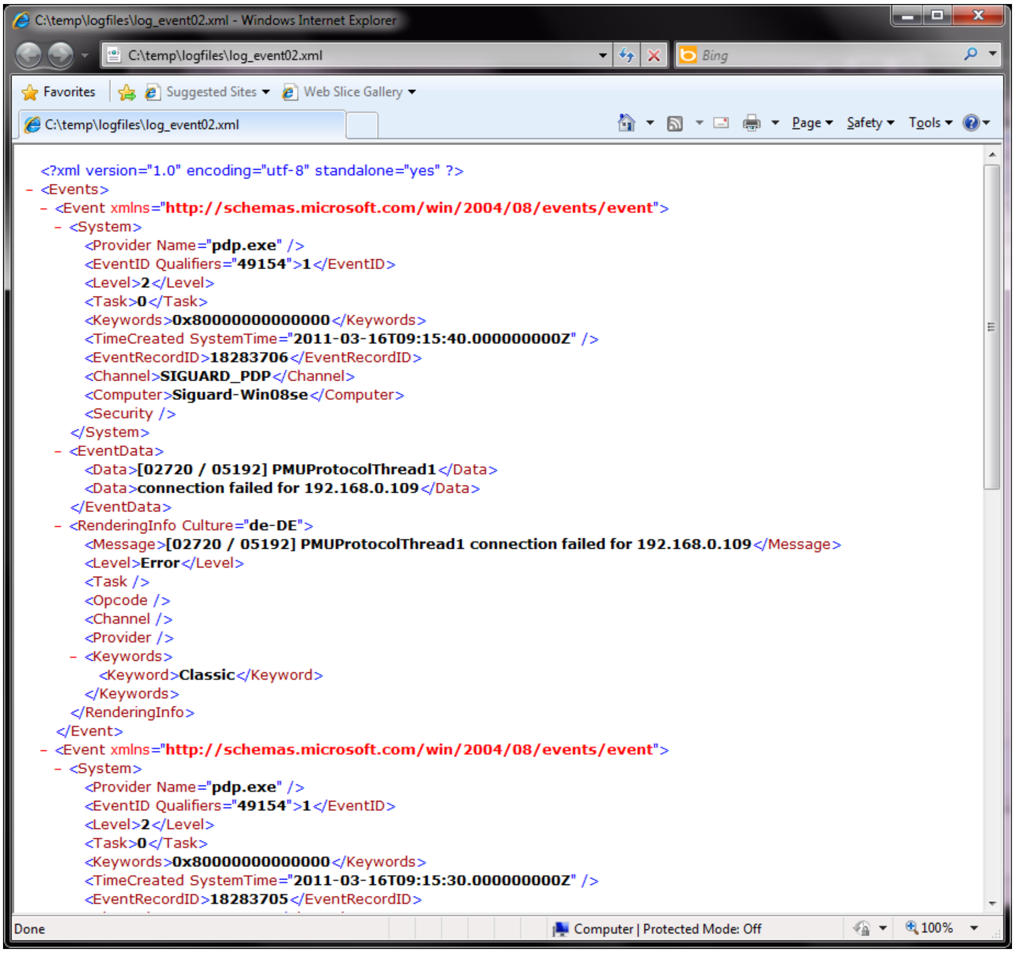
✧ Select the file format.

✧ Click **Save** to close the dialog.

View XML File

XML documents can be opened for later evaluations.

✧ Open an XML document by double-clicking the file name.



C:\temp\logfiles\log_event02.xml - Windows Internet Explorer
C:\temp\logfiles\log_event02.xml
Bing
Favorites
Suggested Sites
Web Slice Gallery
C:\temp\logfiles\log_event02.xml
Page
Safety
Tools
Done
Computer | Protected Mode: Off
100%

```
  <?xml version="1.0" encoding="utf-8" standalone="yes" ?>
- <Events>
  - <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
    - <System>
        <Provider Name="pdp.exe" />
        <EventID Qualifiers="49154">1</EventID>
        <Level>2</Level>
        <Task>0</Task>
        <Keywords>0x80000000000000</Keywords>
        <TimeCreated SystemTime="2011-03-16T09:15:40.000000000Z" />
        <EventRecordID>18283706</EventRecordID>
        <Channel>SIGUARD_PDP</Channel>
        <Computer>Siguard-Win08se</Computer>
        <Security />
      </System>
    - <EventData>
        <Data>[02720 / 05192] PMUProtocolThread1</Data>
        <Data>connection failed for 192.168.0.109</Data>
      </EventData>
    - <RenderingInfo Culture="de-DE">
        <Message>[02720 / 05192] PMUProtocolThread1 connection failed for 192.168.0.109</Message>
        <Level>Error</Level>
        <Task />
        <Opcode />
        <Channel />
        <Provider />
      - <Keywords>
          <Keyword>Classic</Keyword>
        </Keywords>
      </RenderingInfo>
    </Event>
  - <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
    - <System>
        <Provider Name="pdp.exe" />
        <EventID Qualifiers="49154">1</EventID>
        <Level>2</Level>
        <Task>0</Task>
        <Keywords>0x80000000000000</Keywords>
        <TimeCreated SystemTime="2011-03-16T09:15:30.000000000Z" />
        <EventRecordID>18283705</EventRecordID>
```

Figure 7-24 Protocol Opened in XML Format

7.4 User Management

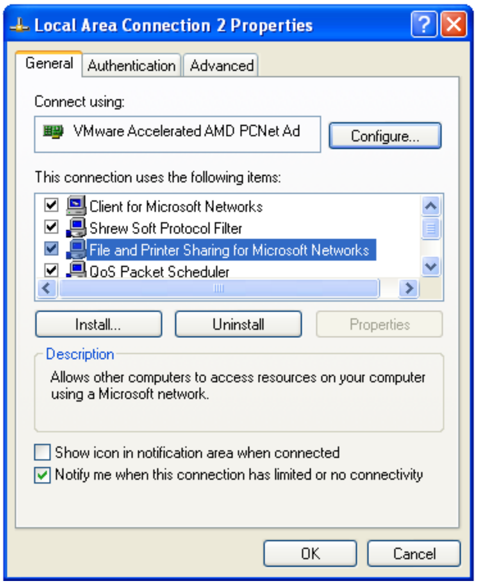
7.4.1 General

A SIGUARD PDP system consists of a SIGUARD PDP Server, the SIGUARD PDP Engineer, and the user interface, the SIGUARD PDP UI. If desired, all components can be subdivided onto a native system. To implement this, you need authorization on the SIGUARD PDP Server for remote access to the SIGUARD PDP Engineering and SIGUARD PDP UI.

✧ Switch on the function **File and Printer Sharing** for Microsoft networks in the configuration of your network card of your SIGUARD PDP system.

-- or --

✧ Permit incoming data traffic via the Desktop Firewall from Microsoft by selecting the function **File and Printer Sharing**.



Connect using: VMware Accelerated AMD PCNet Ad

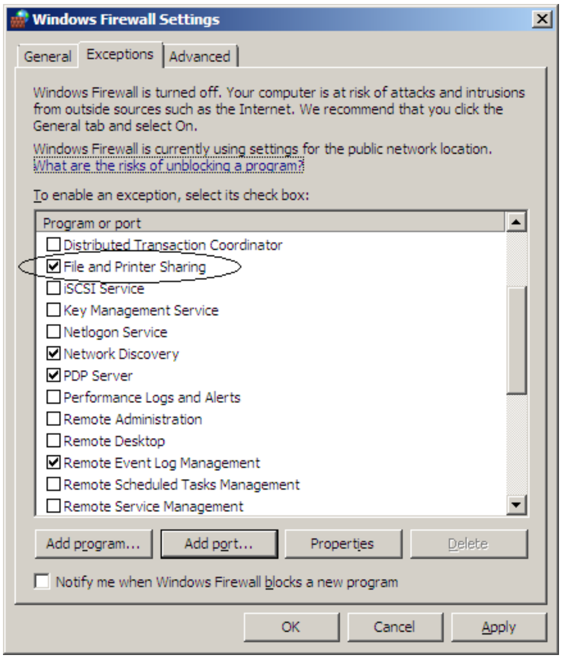
This connection uses the following items:

☑ Client for Microsoft Networks
☑ Shrew Soft Protocol Filter
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler

Description
Allows other computers to access resources on your computer using a Microsoft network.

☐ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

Figure 7-25 Configuration of the Network Card



Windows Firewall is turned off. Your computer is at risk of attacks and intrusions from outside sources such as the Internet. We recommend that you click the General tab and select On.

Windows Firewall is currently using settings for the public network location.
What are the risks of unblocking a program?

To enable an exception, select its check box:

Program or port
☐ Distributed Transaction Coordinator
☑ File and Printer Sharing
☐ iSCSI Service
☐ Key Management Service
☐ Netlogon Service
☑ Network Discovery
☑ PDP Server
☐ Performance Logs and Alerts
☐ Remote Administration
☐ Remote Desktop
☑ Remote Event Log Management
☐ Remote Scheduled Tasks Management
☐ Remote Service Management

☐ Notify me when Windows Firewall blocks a new program

Figure 7-26 Configuration via Windows Firewall Settings

When all systems are installed on a computer, no **File and Printer Sharing** is necessary.

Then deactivate the function **File and Printer Sharing** in the configuration of your network of your SIGUARD PDP systems or in the window **Windows Firewall Settings** on the tab **Exceptions**.

In any case, create user groups for SIGUARD PDP Engineer and SIGUARD PDP UI and assign users to corresponding groups. A user **SiguardRuntime** is created automatically on the SIGUARD PDP Server, during installation.

In the configuration described in the following, SIGUARD PDP Engineer and SIGUARD PDP UI are installed on the same computer. However, they have rights which enable SIGUARD PDP Engineer and SIGUARD PDP UI to be used by various users.

NOTE

For simpler administration and a secure password strategy, Siemens recommends using the Microsoft Domain Controller concept.

For the installation of **Active Directory Domain Services (ADDS)** on Windows Server 2008 or Windows 2008 R2, see *Webpage AD DS Installation and Removal Step-by-Step Guide by Microsoft*.

For installation of **Active Directory Domain Services (ADDS)** on Windows Server 2003, Windows Server 2003 with SP1 or Windows Server 2003 with SP2, see *Web page Installing a Domain Controller by Microsoft*.

7.4.2 Create Users and User Groups

In order to work with the SIGUARD PDP Server, create a SIGUARD PDP project. You create and update the configuration file and save it on the SIGUARD PDP Server. If you are editing the configuration on the SIGUARD PDP Server, authorization for remote access is required. Shared folders are very critical regarding security. Therefore, access to these shared folders should be limited by corresponding rights.

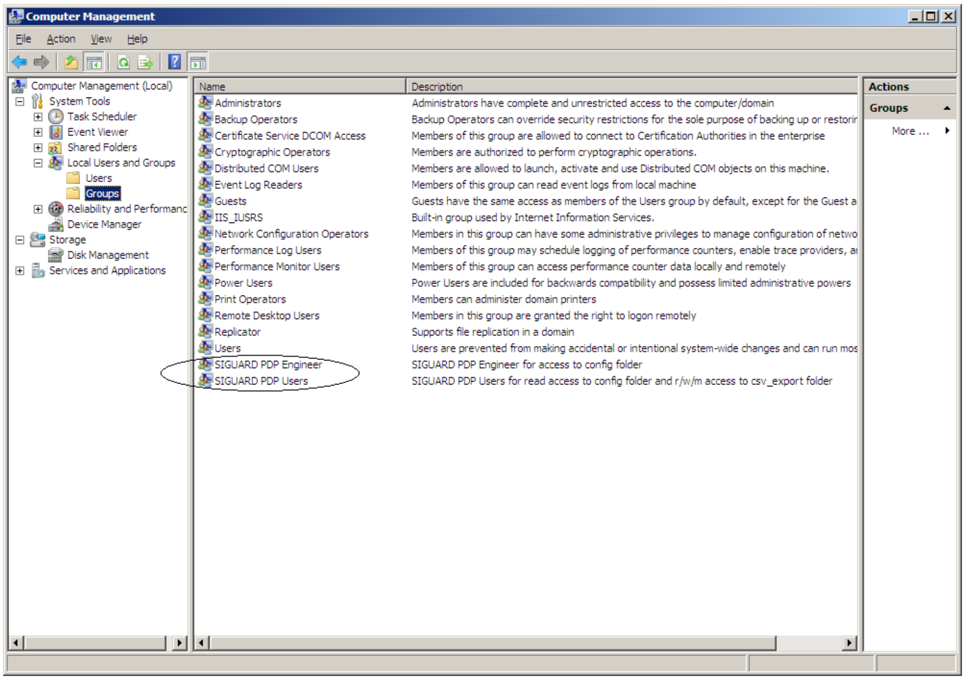
A SIGUARD PDP user may read only the configuration files on the SIGUARD PDP Server and create export files for SIGUARD PDP logging. Furthermore, a SIGUARD PDP user needs read and write access for a shared export folder on the SIGUARD PDP Server.

NOTE

All users and user groups must be created on the SIGUARD PDP Server and the local computer with the same password. The assignment of users to the user groups must be the same on all computers.

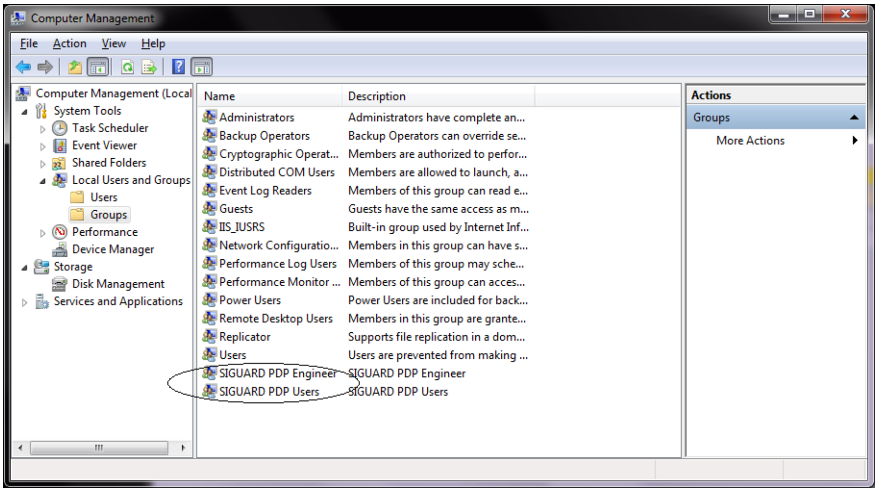
Creating a User Group

- ✧ Open the window **Computer Management** on the SIGUARD PDP Server and the local computer on which the SIGUARD PDP Engineer and SIGUARD PDP UI are installed.
- ✧ Open the folder **Local Users and Groups**.
- ✧ Create the user groups **SIGUARD PDP Engineer** and **SIGUARD PDP Users**.



Name	Description
Administrators	Administrators have complete and unrestricted access to the computer/domain
Backup Operators	Backup Operators can override security restrictions for the sole purpose of backing up or restorir
Certificate Service DCOM Access	Members of this group are allowed to connect to Certification Authorities in the enterprise
Cryptographic Operators	Members are authorized to perform cryptographic operations.
Distributed COM Users	Members are allowed to launch, activate and use Distributed COM objects on this machine.
Event Log Readers	Members of this group can read event logs from local machine
Guests	Guests have the same access as members of the Users group by default, except for the Guest a
IIS_IUSRS	Built-in group used by Internet Information Services.
Network Configuration Operators	Members in this group can have some administrative privileges to manage configuration of netwo
Performance Log Users	Members of this group may schedule logging of performance counters, enable trace providers, ai
Performance Monitor Users	Members of this group can access performance counter data locally and remotely
Power Users	Power Users are included for backwards compatibility and possess limited administrative powers
Print Operators	Members can administer domain printers
Remote Desktop Users	Members in this group are granted the right to logon remotely
Replicator	Supports file replication in a domain
Users	Users are prevented from making accidental or intentional system-wide changes and can run mos
SIGUARD PDP Engineer	SIGUARD PDP Engineer for access to config folder
SIGUARD PDP Users	SIGUARD PDP Users for read access to config folder and r/w/m access to csv_export folder

Figure 7-27 User Groups on the SIGUARD PDP Server



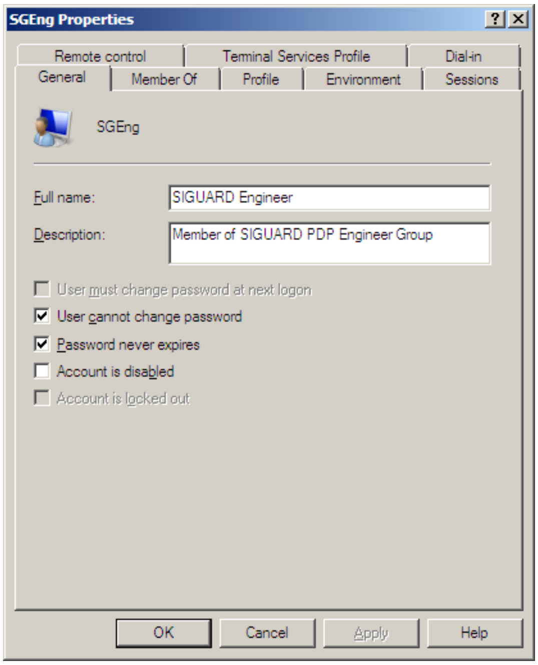
Name	Description
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Cryptographic Operat...	Members are authorized to perfor...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sche...
Performance Monitor ...	Members of this group can acces...
Power Users	Power Users are included for back...
Remote Desktop Users	Members in this group are grante...
Replicator	Supports file replication in a dom...
Users	Users are prevented from making ...
SIGUARD PDP Engineer	SIGUARD PDP Engineer
SIGUARD PDP Users	SIGUARD PDP Users

Figure 7-28 User Groups on the SIGUARD PDP Engineer/UI Computer

Create User SGEng on the SIGUARD PDP Server

In the configuration described, create a user **SGUser** on the SIGUARD PDP Server, who belongs to the user group **SIGUARD PDP Users**. Then create a user **SGEng**, who belongs to the user group **SIGUARD PDP Engineer**.

- Create the SIGUARD PDP Engineer user **SGEng**.
- Establish the properties for this user.



SGEng

Full name: SIGUARD Engineer

Description: Member of SIGUARD PDP Engineer Group

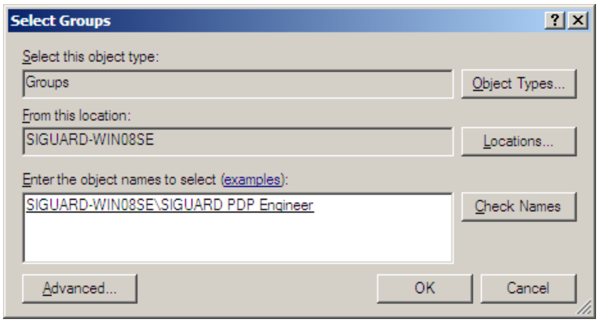
☐ User must change password at next logon
☑ User cannot change password
☑ Password never expires
☐ Account is disabled
☐ Account is locked out

Figure 7-29 General of the User SGEng

- Enter the name and the description for the new user.
- Establish the criteria for the password.

Assign User SGEng to the User Group SIGUARD PDP Engineer

- Select the tab **Member Of**, in order to assign the user **SGEng** to the user group **SIGUARD PDP Engineer**.
- Click **Add...**.



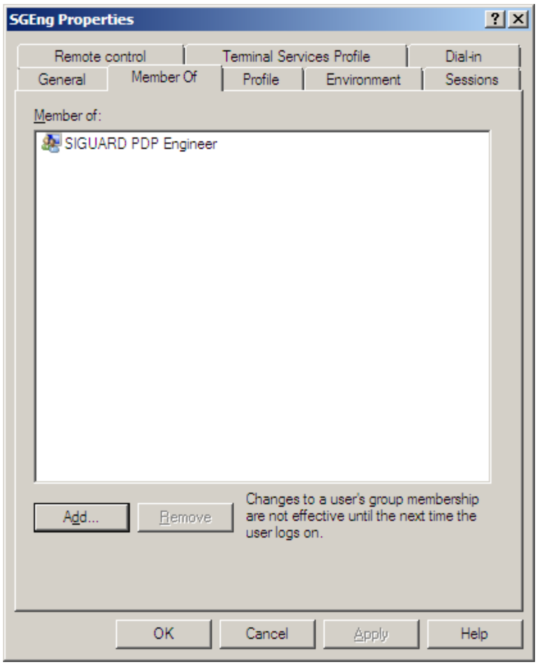
Select this object type:
Groups

From this location:
SIGUARD-WIN08SE

Enter the object names to select (examples):
SIGUARD-WIN08SE\SIGUARD PDP Engineer

Figure 7-30 Select Groups

- Select the user group **SIGUARD PDP Engineer**.
- Click **OK** to confirm your settings.



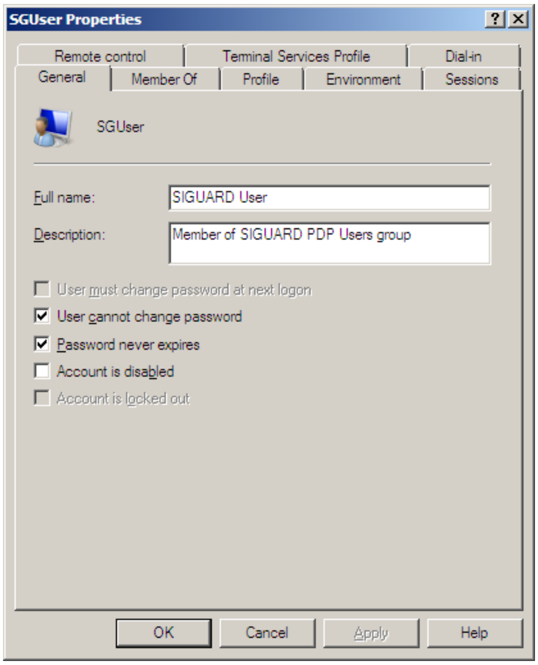
Member of:
SIGUARD PDP Engineer

Changes to a user's group membership are not effective until the next time the user logs on.

Figure 7-31 Member Of of the User SGEng

Create User SGUser on the SIGUARD PDP Server

- Create the SIGUARD PDP Engineer user **SGUser**.
- Establish the properties for this user.



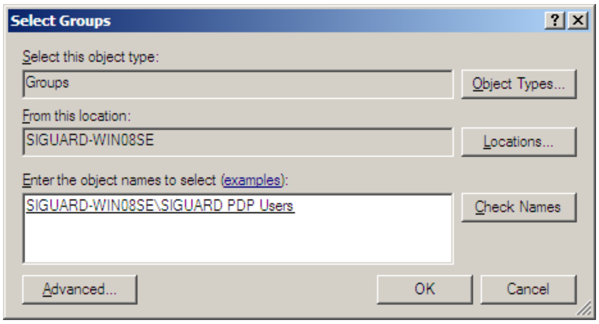
Full name: SIGUARD User
Description: Member of SIGUARD PDP Users group
☐ User must change password at next logon
☑ User cannot change password
☑ Password never expires
☐ Account is disabled
☐ Account is locked out

Figure 7-32 General of the User SGUser

- Enter the name and the description for the new user.
- Establish the criteria for the password.

Assign User SGUser to the User Group SIGUARD PDP User

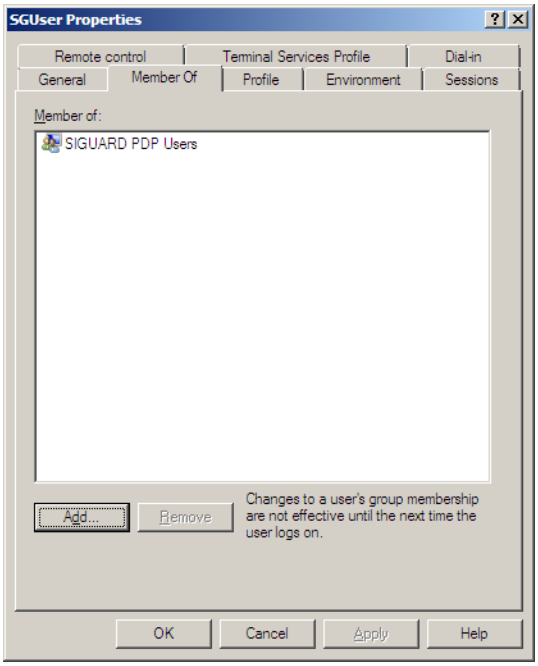
- Select the tab **Member Of**, in order to assign the user **SGUser** to the user group **SIGUARD PDP Users**.
- Click **Add...**.



Select this object type: Groups
From this location: SIGUARD-WIN08SE
Enter the object names to select (examples): SIGUARD-WIN08SE\SIGUARD PDP Users

Figure 7-33 Select Groups

- ✧ Select the user group **SIGUARD PDP Users**.
- ✧ Click **OK** to confirm your settings.



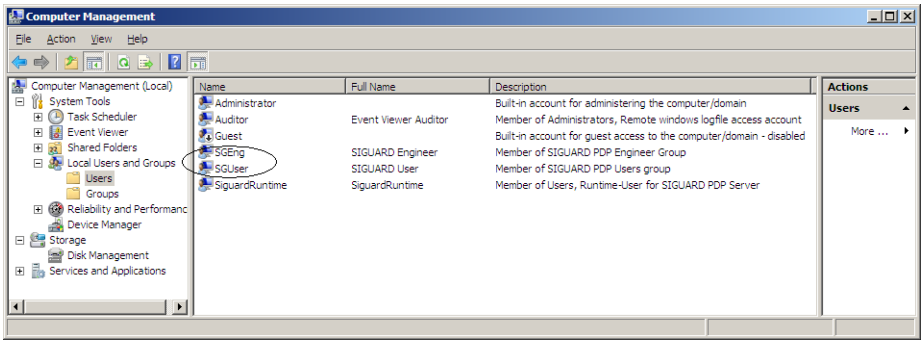
Member of:
SIGUARD PDP Users

Changes to a user's group membership are not effective until the next time the user logs on.

Figure 7-34 Member Of of the User SGUser

- ✧ Click **OK** to close the dialog.

The new users are included in the list **Users**.



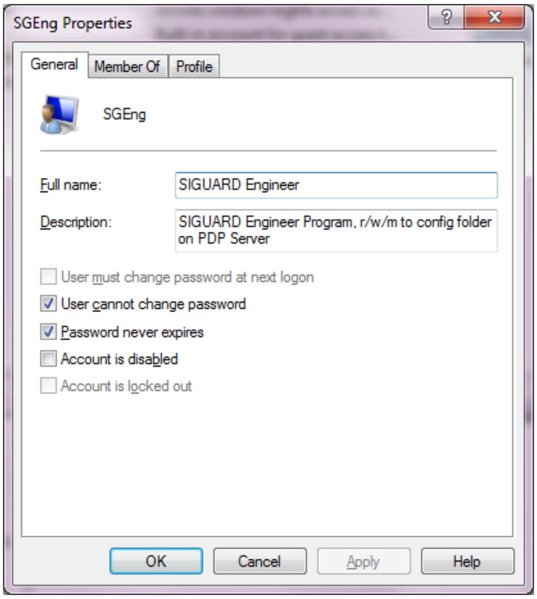
Name	Full Name	Description
Administrator		Built-in account for administering the computer/domain
Auditor	Event Viewer Auditor	Member of Administrators, Remote windows logfile access account
Guest		Built-in account for guest access to the computer/domain - disabled
SGEng	SIGUARD Engineer	Member of SIGUARD PDP Engineer Group
SGUser	SIGUARD User	Member of SIGUARD PDP Users group
SiguardRuntime	SiguardRuntime	Member of Users, Runtime-User for SIGUARD PDP Server

Figure 7-35 Users on the SIGUARD PDP Server

Create Users on the SIGUARD PDP Engineer/UI Computer

On the SIGUARD PDP Engineer/UI computer, create the same users as on the SIGUARD PDP Server. These users also belong to the Windows user group **Users**.

- Create the SIGUARD PDP Engineer user **SGEng**.
- Establish the properties for this user.



SGEng

Full name: SIGUARD Engineer

Description: SIGUARD Engineer Program, r/w/m to config folder on PDP Server

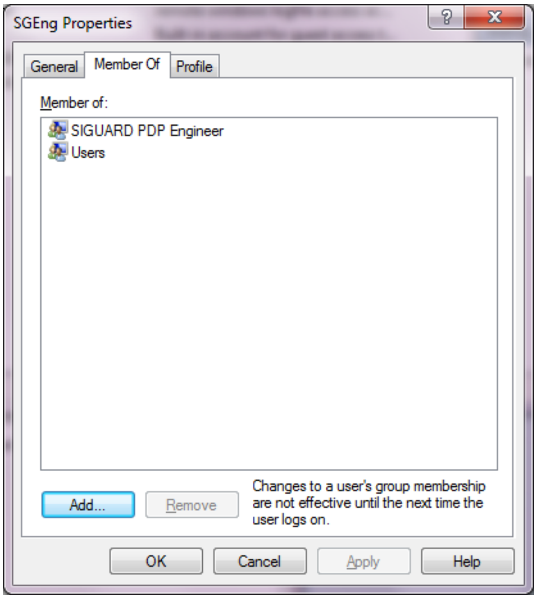
☐ User must change password at next logon
☑ User cannot change password
☑ Password never expires
☐ Account is disabled
☐ Account is locked out

Figure 7-36 General of the User SGEng

- Enter the name and the description for the new user.
- Establish the criteria for the password.

Assign User Group

- Select the tab **Member Of**, in order to assign the user **SGEng** to the user group **SIGUARD PDP Engineer** and to the user group **Users**.

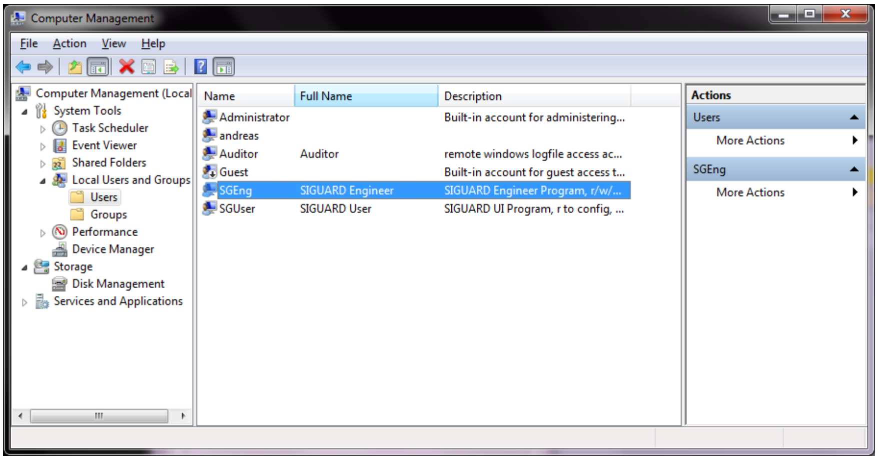


SIGUARD PDP Engineer
Users

Changes to a user's group membership are not effective until the next time the user logs on.

Figure 7-37 Assigned User Groups of the User SGEng

- Click **OK** to close the dialog.
- Repeat the assignment of the user **SGUser** to user group **SIGUARD PDP Users** and to user group **Users**.



Name	Full Name	Description
Administrator		Built-in account for administering...
andreas		
Auditor	Auditor	remote windows logfile access ac...
Guest		Built-in account for guest access t...
SGEng	SIGUARD Engineer	SIGUARD Engineer Program, r/w/...
SGUser	SIGUARD User	SIGUARD UI Program, r to config, ...

Figure 7-38 Assignment of the User SGUser

7.4.3 Create Access Rights on the Shared Folder on the SIGUARD PDP Server

General

On the SIGUARD PDP Server, there are 2 shared folders, **Config** and **CSV-Export**. It must be possible to access these 2 shared folders from the SIGUARD PDP Engineering/UI computer.

- Give the user group **SIGUARD PDP Engineer** read, write, and change rights for the shared folder **Config** and read access for the shared folder **CSV-Export**.
- Give the user group **SIGUARD PDP Users** read, write, and change rights for the shared folder **CSV-Export** and read access for the shared folder **Config**.
- In addition, authorize remote access to this shared folder **only** for these 2 user groups if the SIGUARD PDP Server is installed on a different computer than SIGUARD PDP Engineering/UI.

  The access rights for the 2 user groups to the shared folder may not be limited via the security settings.

Shared Folders Are Missing

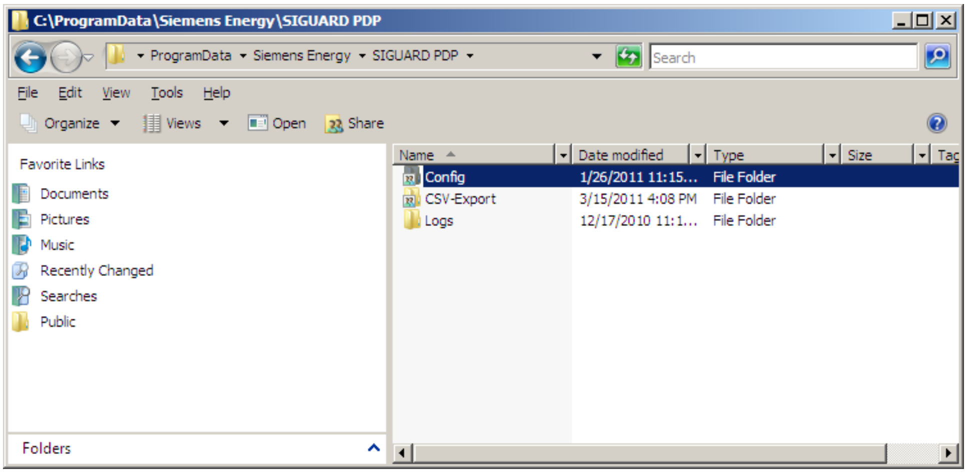
- If both of the folders are not yet present on your system, create them in the following paths:

  ..\ProgramData\Siemens Energy\SIGUARD PDP\Config and

  ..\ProgramData\Siemens Energy\SIGUARD PDP\CSV-Export
- Assign full access rights for both user groups as described below.

Set Up Access Rights for the Folder Config

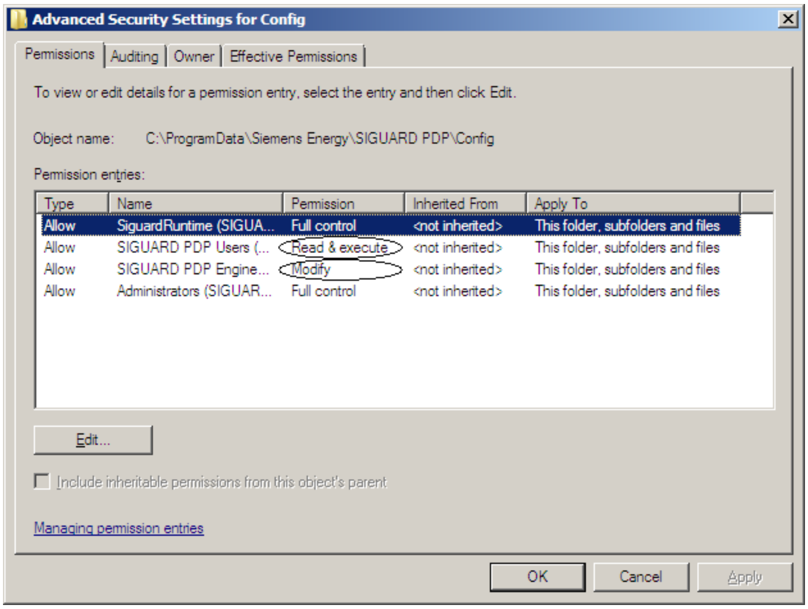
- Display the shared folder of the SIGUARD PDP Server.



Name	Date modified	Type	Size	Tag
Config	1/26/2011 11:15...	File Folder		
CSV-Export	3/15/2011 4:08 PM	File Folder		
Logs	12/17/2010 11:1...	File Folder		

Figure 7-39 Shared Folder Config on the SIGUARD PDP Server

- Right-click the folder **Config** and select the menu item **Advanced** in order to edit its security settings.



To view or edit details for a permission entry, select the entry and then click Edit.

Object name: C:\ProgramData\Siemens Energy\SIGUARD PDP\Config

Permission entries:

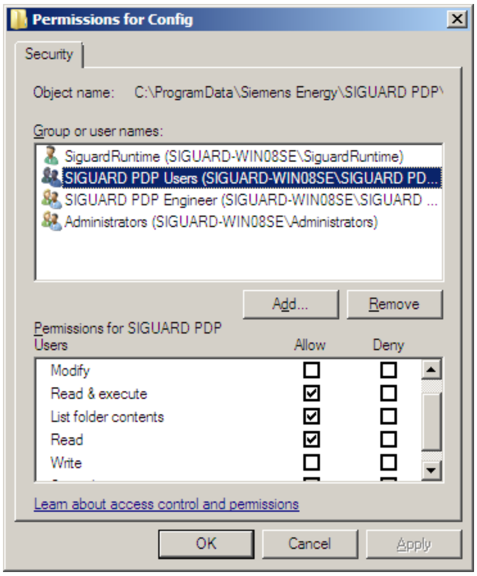
Type	Name	Permission	Inherited From	Apply To
Allow	SiguardRuntime (SIGUA...	Full control	<not inherited>	This folder, subfolders and files
Allow	SIGUARD PDP Users (...	Read & execute	<not inherited>	This folder, subfolders and files
Allow	SIGUARD PDP Engine...	Modify	<not inherited>	This folder, subfolders and files
Allow	Administrators (SIGUAR...	Full control	<not inherited>	This folder, subfolders and files

☐ Include inheritable permissions from this object's parent

Managing permission entries

Figure 7-40 Access Rights for the Folder Config

- ✧ In order to edit a security entry, select the corresponding entry on the tab **Permissions** and click **Edit...**



Object name: C:\ProgramData\Siemens Energy\SIGUARD PDP\

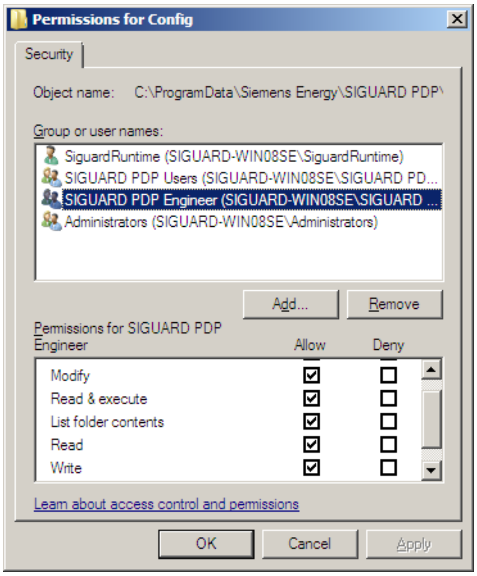
Group or user names:

SiguardRuntime (SIGUARD-WIN08SE\SiguardRuntime)
SIGUARD PDP Users (SIGUARD-WIN08SE\SIGUARD PD...
SIGUARD PDP Engineer (SIGUARD-WIN08SE\SIGUARD ...
Administrators (SIGUARD-WIN08SE\Administrators)

Permissions for SIGUARD PDP Users	Allow	Deny
Modify	☐	☐
Read & execute	☑	☐
List folder contents	☑	☐
Read	☑	☐
Write	☐	☐

Learn about access control and permissions

Figure 7-41 Access Rights for the User Group SIGUARD PDP Users



Object name: C:\ProgramData\Siemens Energy\SIGUARD PDP\

Group or user names:

- SiguardRuntime (SIGUARD-WIN08SE\SiguardRuntime)
- SIGUARD PDP Users (SIGUARD-WIN08SE\SIGUARD PD...
- SIGUARD PDP Engineer (SIGUARD-WIN08SE\SIGUARD ...
- Administrators (SIGUARD-WIN08SE\Administrators)

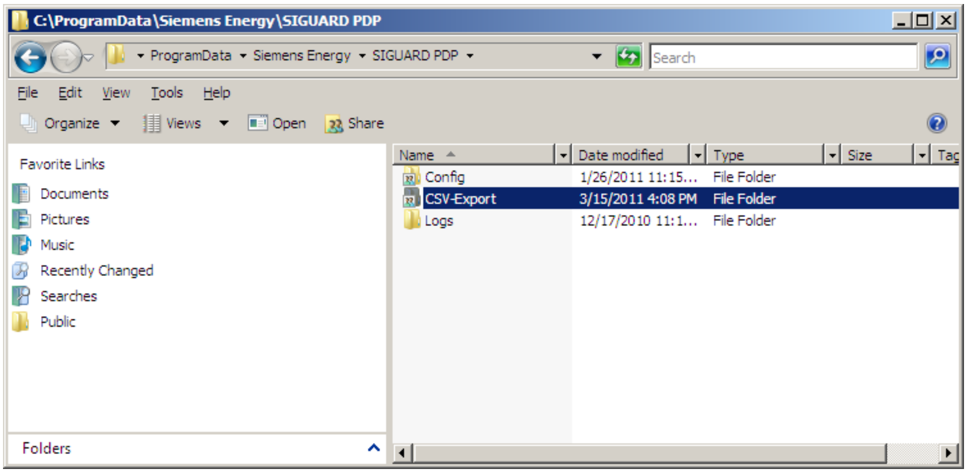
Permissions for SIGUARD PDP Engineer	Allow	Deny
Modify	☑	☐
Read & execute	☑	☐
List folder contents	☑	☐
Read	☑	☐
Write	☑	☐

Figure 7-42 Access Rights for the User Group SIGUARD PDP Engineer

✧ Close the dialog with **OK**.

Set Up Access Rights for the Folder CSV-Export

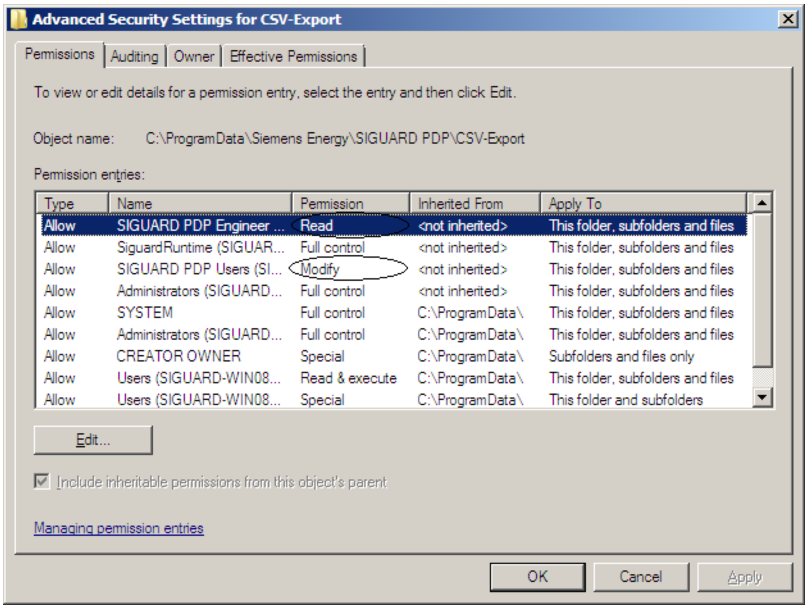
✧ Display the shared folder of the SIGUARD PDP Server.



Name	Date modified	Type	Size	Tag
Config	1/26/2011 11:15...	File Folder		
CSV-Export	3/15/2011 4:08 PM	File Folder		
Logs	12/17/2010 11:1...	File Folder		

Figure 7-43 Shared Folder CSV-Export on the SIGUARD PDP Server

✧ Right-click the folder **CSV-Export** and select the menu item **Advanced** in order to edit its security settings.



Advanced Security Settings for CSV-Export

To view or edit details for a permission entry, select the entry and then click Edit.

Object name: C:\ProgramData\Siemens Energy\SIGUARD PDP\CSV-Export

Permission entries:

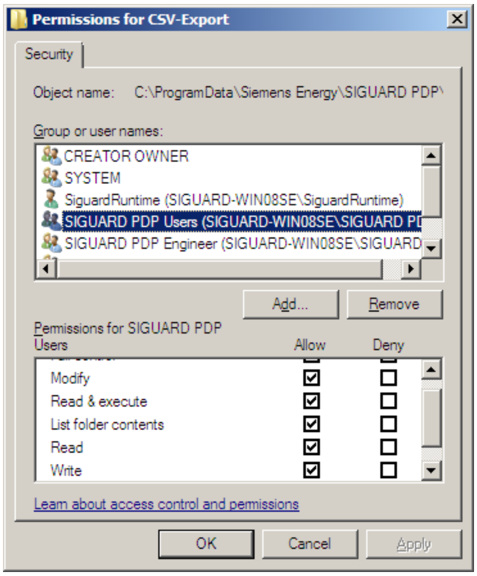
Type	Name	Permission	Inherited From	Apply To
Allow	SIGUARD PDP Engineer ...	Read	<not inherited>	This folder, subfolders and files
Allow	SiguardRuntime (SIGUAR...	Full control	<not inherited>	This folder, subfolders and files
Allow	SIGUARD PDP Users (SI...	Modify	<not inherited>	This folder, subfolders and files
Allow	Administrators (SIGUARD...	Full control	<not inherited>	This folder, subfolders and files
Allow	SYSTEM	Full control	C:\ProgramData\	This folder, subfolders and files
Allow	Administrators (SIGUARD...	Full control	C:\ProgramData\	This folder, subfolders and files
Allow	CREATOR OWNER	Special	C:\ProgramData\	Subfolders and files only
Allow	Users (SIGUARD-WIN08...	Read & execute	C:\ProgramData\	This folder, subfolders and files
Allow	Users (SIGUARD-WIN08...	Special	C:\ProgramData\	This folder and subfolders

☑ Include inheritable permissions from this object's parent

Managing permission entries

Figure 7-44 Access Rights for the Folder CSV-Export

- ✧ In order to edit a security entry, select the corresponding entry on the tab **Permissions** and click **Edit...**



Permissions for CSV-Export

Object name: C:\ProgramData\Siemens Energy\SIGUARD PDP\

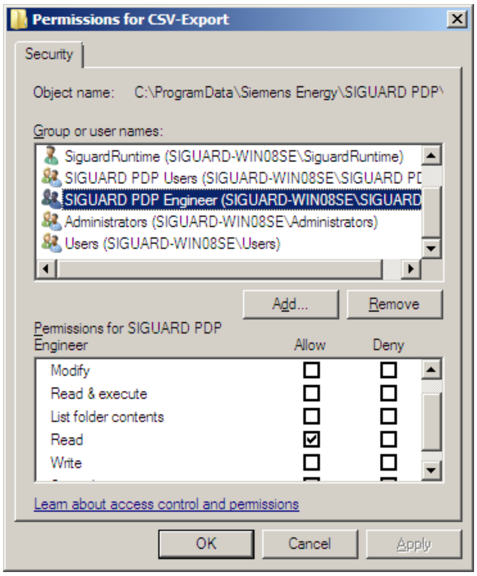
Group or user names:

- CREATOR OWNER
- SYSTEM
- SiguardRuntime (SIGUARD-WIN08SE\SiguardRuntime)
- SIGUARD PDP Users (SIGUARD-WIN08SE\SIGUARD P
- SIGUARD PDP Engineer (SIGUARD-WIN08SE\SIGUARD

Permissions for SIGUARD PDP Users	Allow	Deny
Modify	☑	☐
Read & execute	☑	☐
List folder contents	☑	☐
Read	☑	☐
Write	☑	☐

Learn about access control and permissions

Figure 7-45 Access Rights for the User Group SIGUARD PDP Users


Permissions for CSV-Export
Security
Add...
Remove
Learn about access control and permissions
OK
Cancel
Apply

Object name: C:\ProgramData\Siemens Energy\SIGUARD PDP\

Group or user names:

- SiguardRuntime (SIGUARD-WIN08SE\SiguardRuntime)
- SIGUARD PDP Users (SIGUARD-WIN08SE\SIGUARD PD
- SIGUARD PDP Engineer (SIGUARD-WIN08SE\SIGUARD
- Administrators (SIGUARD-WIN08SE\Administrators)
- Users (SIGUARD-WIN08SE\Users)

Permissions for SIGUARD PDP Engineer	Allow	Deny
Modify	☐	☐
Read & execute	☐	☐
List folder contents	☐	☐
Read	☑	☐
Write	☐	☐

Figure 7-46 Access Rights for the User Group SIGUARD PDP Engineer

✧ Click **OK** to close the dialog.

7.4.4 Set Local Access Rights

General

If **SIGUARD PDP Engineer** and **SIGUARD PDP UI** are installed on the same computer, set the access rights separately.

✧ Give the user group **SIGUARD PDP Engineer** access rights only to the program **SIGUARD PDP Engineer**.

✧ Give the user group **SIGUARD PDP Users** access rights only to the program **SIGUARD PDP UI**.

If the user assumes both tasks, both user groups are assigned to the user. These user groups require read and execute rights for the main directory **SIGUARD PDP** on the local computer (SIGUARD PDP Engineer/UI computer).

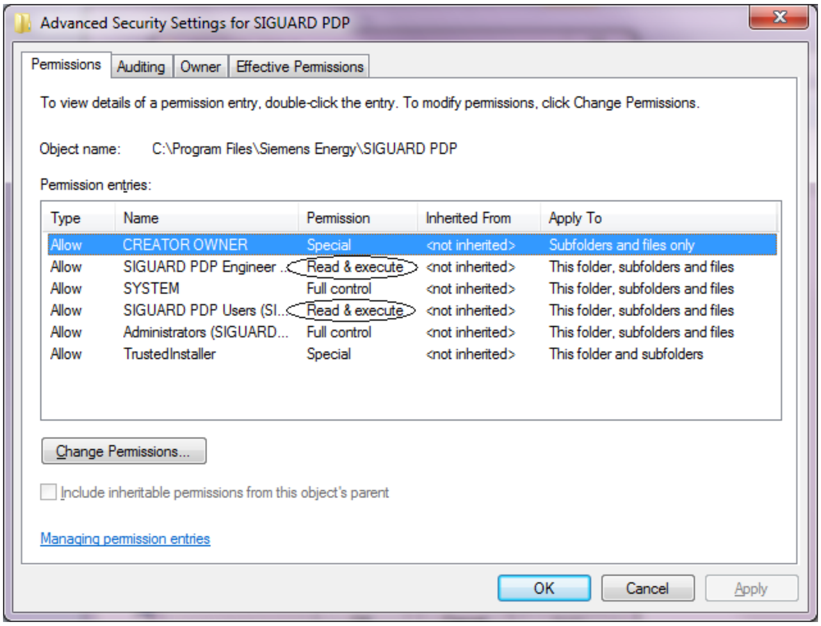
NOTE

If a SIGUARD PDP engineer requires access rights to the SIGUARD PDP UI computer, add the engineer as a member of the user group **SIGUARD PDP Users**.

Access Rights for the SIGUARD PDP Folder

For the folder **SIGUARD PDP** in the path **\Program Files\Siemens Energy** on the local computer, assign read, execute, and display rights for both SIGUARD user groups.

- ✧ Open the path **\Program Files\Siemens Energy**.
- ✧ For the folder **SIGUARD PDP**, open the window **Advanced Security Settings for SIGUARD PDP**.



Advanced Security Settings for SIGUARD PDP

To view details of a permission entry, double-click the entry. To modify permissions, click Change Permissions.

Object name: C:\Program Files\Siemens Energy\SIGUARD PDP

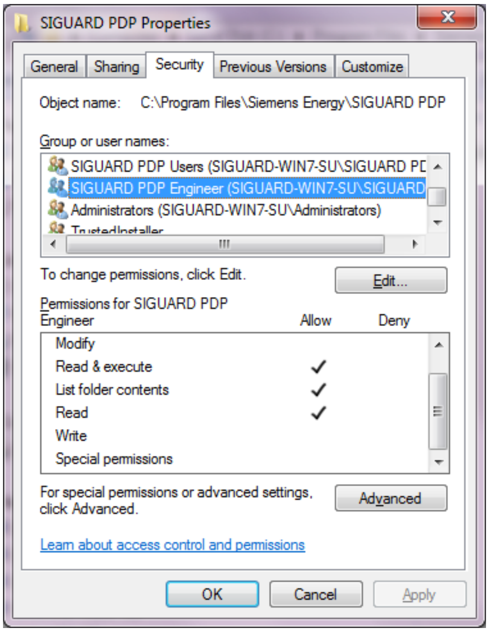
Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	CREATOR OWNER	Special	<not inherited>	Subfolders and files only
Allow	SIGUARD PDP Engineer ...	Read & execute	<not inherited>	This folder, subfolders and files
Allow	SYSTEM	Full control	<not inherited>	This folder, subfolders and files
Allow	SIGUARD PDP Users (SI...	Read & execute	<not inherited>	This folder, subfolders and files
Allow	Administrators (SIGUARD...	Full control	<not inherited>	This folder, subfolders and files
Allow	TrustedInstaller	Special	<not inherited>	This folder and subfolders

☐ Include inheritable permissions from this object's parent

Figure 7-47 Security Settings for the Local Folder SIGUARD PDP

- ✧ Select the corresponding entry and click **Change Permissions...**, to edit its access rights.



SIGUARD PDP Properties

Object name: C:\Program Files\Siemens Energy\SIGUARD PDP

Group or user names:

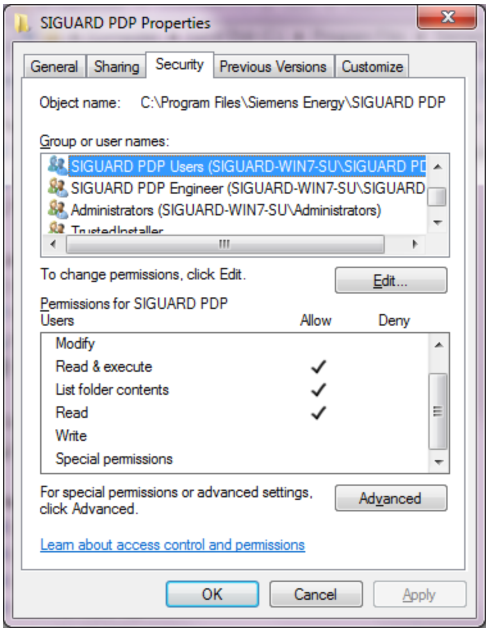
SIGUARD PDP Users (SIGUARD-WIN7-SU\SIGUARD PD
SIGUARD PDP Engineer (SIGUARD-WIN7-SU\SIGUARD
Administrators (SIGUARD-WIN7-SU\Administrators)
TrustedInstaller

To change permissions, click Edit.

Permissions for SIGUARD PDP Engineer	Allow	Deny
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write		
Special permissions		

For special permissions or advanced settings, click Advanced.

Figure 7-48 Access Rights of the User Group SIGUARD PDP Engineer to the SIGUARD PDP Folder



Object name: C:\Program Files\Siemens Energy\SIGUARD PDP

Group or user names:

SIGUARD PDP Users (SIGUARD-WIN7-SU\SIGUARD PD
SIGUARD PDP Engineer (SIGUARD-WIN7-SU\SIGUARD
Administrators (SIGUARD-WIN7-SU\Administrators)
TrustedInstaller

To change permissions, click Edit.

Permissions for SIGUARD PDP Users	Allow	Deny
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write		
Special permissions		

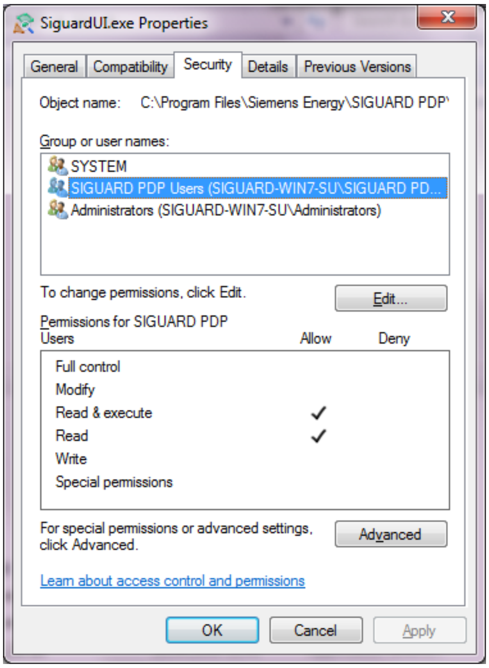
For special permissions or advanced settings, click Advanced.

Figure 7-49 Access Rights of the User Group SIGUARD PDP Users to the SIGUARD PDP Folder

- Click **OK** to close the dialog.

Editing Access Rights to the Program SIGUARD PDP UI

- Open the properties window of **SiguardUI.exe**.



Object name: C:\Program Files\Siemens Energy\SIGUARD PDP\

Group or user names:

SYSTEM
SIGUARD PDP Users (SIGUARD-WIN7-SU\SIGUARD PD...
Administrators (SIGUARD-WIN7-SU\Administrators)

To change permissions, click Edit.

Permissions for SIGUARD PDP Users	Allow	Deny
Full control		
Modify		
Read & execute	✓	
Read	✓	
Write		
Special permissions		

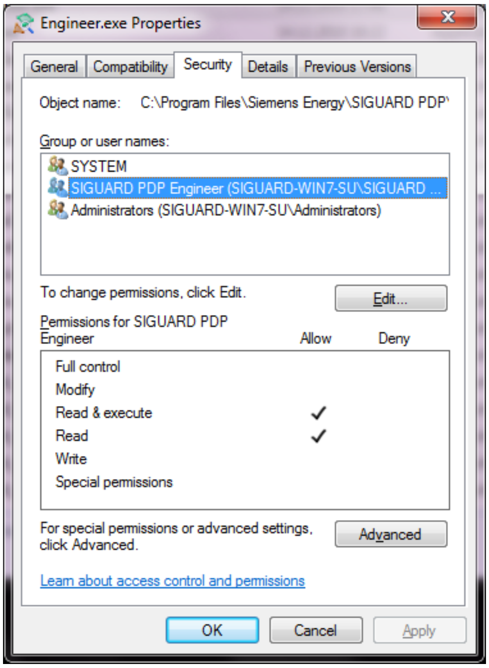
For special permissions or advanced settings, click Advanced.

Figure 7-50 Access Rights for SIGUARD PDP UI

- Select the user group and click **Edit...**, in order to change its rights.
- Select the user group and click **Advanced...**, in order to change its extended rights.
- Click **OK** to close the dialog.

Editing Access Rights to the Program SIGUARD PDP Engineer

- Open the properties window **Engineer.exe** and proceed as with SIGUARD PDP UI in order to change the program settings.



Object name: C:\Program Files\Siemens Energy\SIGUARD PDP\

Group or user names:
SYSTEM
SIGUARD PDP Engineer (SIGUARD-WIN7-SU\SIGUARD ...
Administrators (SIGUARD-WIN7-SU\Administrators)

To change permissions, click Edit.

Permissions for SIGUARD PDP Engineer	Allow	Deny
Full control		
Modify		
Read & execute	✓	
Read	✓	
Write		
Special permissions		

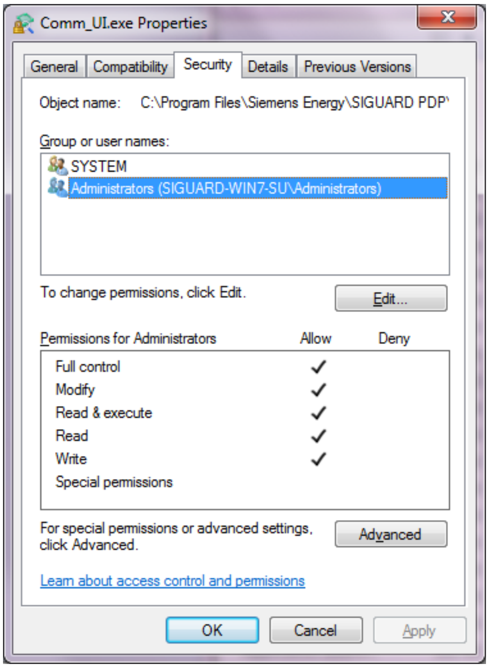
For special permissions or advanced settings, click Advanced.

Figure 7-51 Access Rights for SIGUARD PDP Engineer

Editing Access Rights to the Program SIGUARD PDP Communication UI

These settings are required only on the SIGUARD PDP Server.

✧ Open the properties window **Comm_UI.exe** and proceed as with SIGUARD PDP UI in order to change the program settings.



Object name: C:\Program Files\Siemens Energy\SIGUARD PDP\

Group or user names:

SYSTEM
Administrators (SIGUARD-WIN7-SU\Administrators)

To change permissions, click Edit.

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

For special permissions or advanced settings, click Advanced.

Figure 7-52 Access Rights for SIGUARD PDP Communication UI

7.5 IPSec Tunneling

7.5.1 IPSec Tunnel between SIGUARD PDP Server and Local Computer

7.5.1.1 General

Due to the data exchange of pure text between the SIGUARD PDP Server and the SIGUARD PDP Engineer/UI computer, Siemens recommends using a certified and trustworthy VPN connection tunnel (Virtual Private Network) from a third-party manufacturer that complies with the applicable guidelines.

IPSec (Internet Protocol Security) is a security protocol that guarantees the protection goals of trustworthiness, authenticity, and integrity for communication via IP networks. It is used for establishing Virtual Private Networks.

It is very easy to use this IPSec implemented in Windows. IPSec is included in Windows XP, Windows 7, and Windows Server 2008, among others.

In the following configuration, PSK authentication and ESP encryption are used.

Pre-shared key, or abbreviated, PSK, designates an encryption process in which the keys must be known to both participants before communication. Encapsulating Security Payload (ESP) ensures the authentication, integrity, and trustworthiness of IP packets. ESP is based directly on IP and uses the IP protocol number 50.

It is the simplest way to set up IPSec with PSK authentication for an administrator user account on a SIGUARD PDP Server and a SIGUARD PDP Engineer/UI computer, since only a few systems are integrated in SIGUARD. Do not install any further software for IPSec authentication/encryption. The completeness and trustworthiness of the data are guaranteed.

To do this, proceed as follows:

✧ Configure the IPSec Tunnel on the SIGUARD PDP Server.

✧ Export the configuration data.

✧ Import the configuration data on the local computer.

7.5.1.2 IPSec Configuration

Insert the IPSec Snap-In

- ✧ Start the **Configuration Management Console**.
- ✧ Select the menu **Add/Remove Snap-in...** .

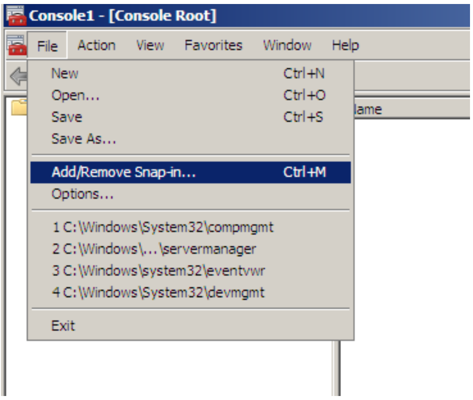
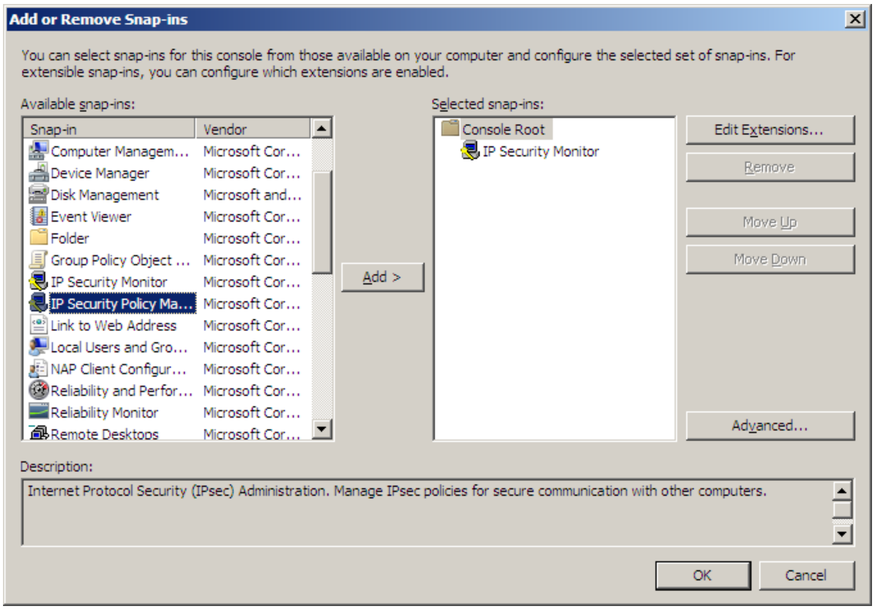

Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\System32\compmgmt
2 C:\Windows\...\servermanager
3 C:\Windows\system32\eventvwr
4 C:\Windows\System32\devmgmt
Exit
Name

Figure 7-53 Configuration Management Console

- ✧ Select the snap-in **IP Security Monitor** and **IP Security Policy Manager** and add these with **Add >** to the selected snap-ins.



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

Available snap-ins:

Snap-in	Vendor
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy Ma...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...
NAP Client Configur...	Microsoft Cor...
Reliability and Perfor...	Microsoft Cor...
Reliability Monitor	Microsoft Cor...
Remote Desktops	Microsoft Cor...

Selected snap-ins:

Console Root
  IP Security Monitor

Description:

Internet Protocol Security (IPsec) Administration. Manage IPsec policies for secure communication with other computers.

Figure 7-54 Adding IP Security Policy Snap-in

- ✧ Click **OK** to confirm your settings.

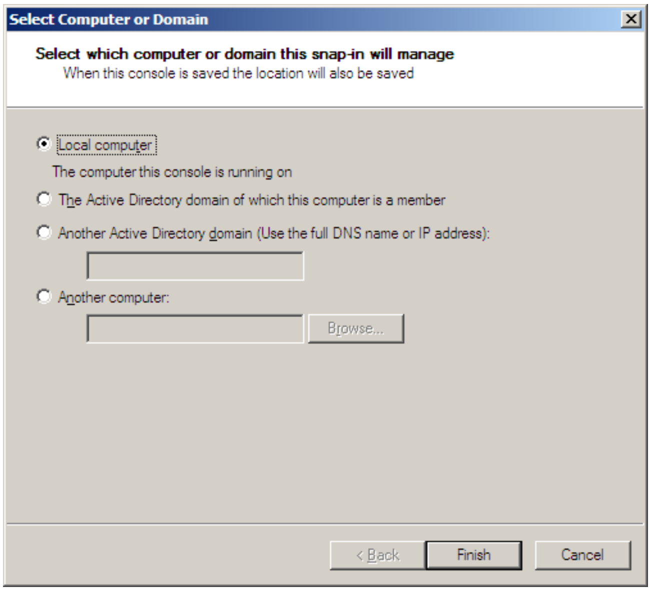

Select Computer or Domain
Select which computer or domain this snap-in will manage
When this console is saved the location will also be saved
● Local computer
The computer this console is running on
○ The Active Directory domain of which this computer is a member
○ Another Active Directory domain (Use the full DNS name or IP address):
○ Another computer:
Browse...
< Back
Finish
Cancel

Figure 7-55 Selection of the Local Computer

- ✧ Use **Local Computer** to select the computer on which this configuration is supposed to run.
- ✧ Click **Finish** to close the dialog.

Establishing a Security Strategy and Filter Settings

Use the wizard in the **Configuration Management Console** to set the following functions:

- Creation of an IPSec guideline with **Create IP Security Policy...**
- Filter settings for export with **Manage IP filter lists and filter actions...**

NOTE

Both transmission directions are always needed for the guidelines and filter settings.

- ✧ Right-click the snap-in **IP Security Policies on Local Computer**.

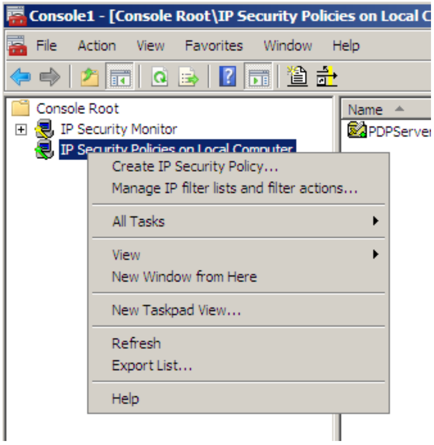
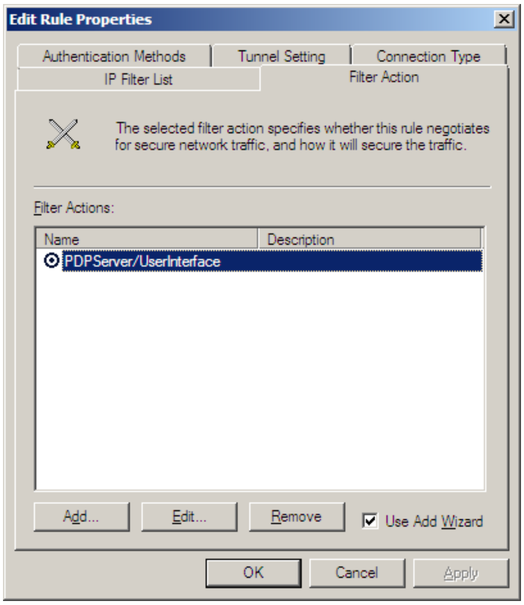

Console1 - [Console Root\IP Security Policies on Local C
File
Action
View
Favorites
Window
Help
Console Root
IP Security Monitor
IP Security Policies on Local Computer
Name
PDPServer
Create IP Security Policy...
Manage IP filter lists and filter actions...
All Tasks
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help

Figure 7-56 Calling up the Snap-Ins

Filter Editing

- ✧ Select the menu item **Manage IP filter lists and filter actions...**
- ✧ Select the tab **Filter Action**.



The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.

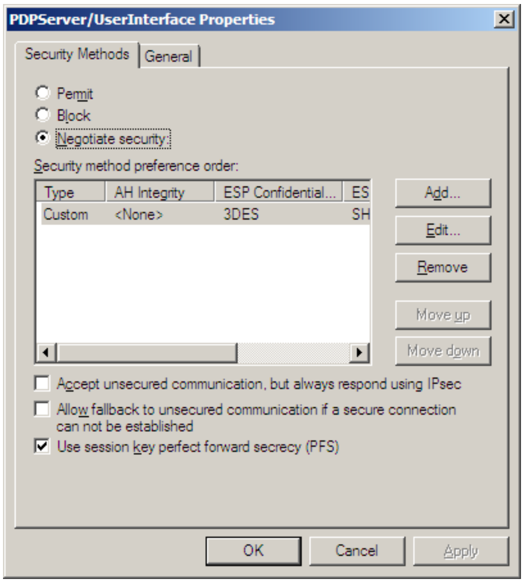
Filter Actions:

Name	Description
● PDPServer/UserInterface	

☑ Use Add Wizard

Figure 7-57 Add Filter and Edit Settings

- ✧ Select **Add...** in order to create a new filter.
- ✧ Select a filter and select **Edit...** in order to edit its properties.



○ Permit
○ Block
● Negotiate security:

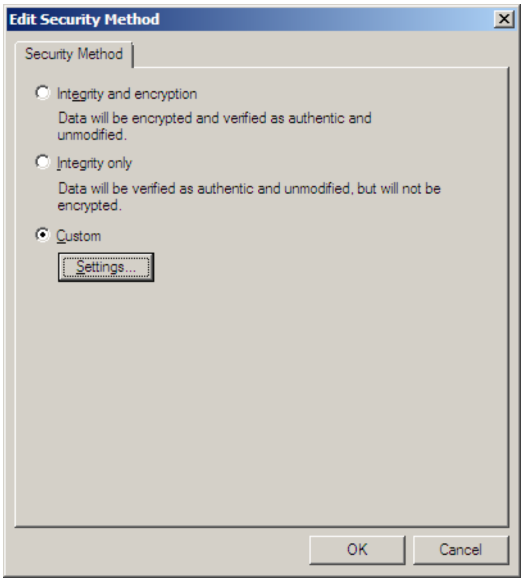
Security method preference order:

Type	AH Integrity	ESP Confidential...	ES
Custom	<None>	3DES	SH

☐ Accept unsecured communication, but always respond using IPsec
☐ Allow fallback to unsecured communication if a secure connection can not be established
☑ Use session key perfect forward secrecy (PFS)

Figure 7-58 Editing Filter Settings

- Select **Negotiate security**. The security rules for transmission are negotiated by the system, for example, which rules and which algorithms are used.
- Select **PFS (Perfect Forward Security)**. The filter uses a key with perfectly continuous secrecy, an encryption procedure in which previous and subsequent keys of a communication channel cannot be determined from an uncovered key.
- In order to establish the security method, select **Edit...**.



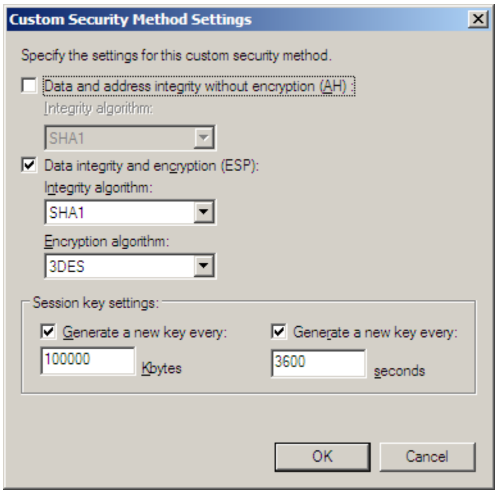
○ Integrity and encryption
Data will be encrypted and verified as authentic and unmodified.

○ Integrity only
Data will be verified as authentic and unmodified, but will not be encrypted.

● Custom

Figure 7-59 Establishing the Security Method

- In order to configure this security method, select **Settings...**.



Specify the settings for this custom security method.

☐ Data and address integrity without encryption (AH) :
Integrity algorithm: SHA1

☑ Data integrity and encryption (ESP):
Integrity algorithm: SHA1
Encryption algorithm: 3DES

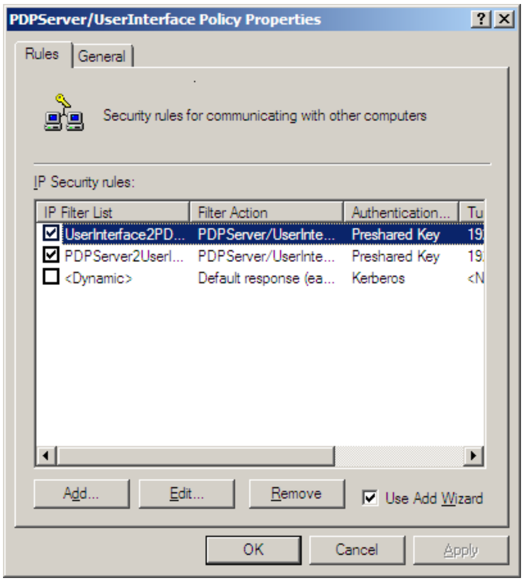
Session key settings:
☑ Generate a new key every: 100000 Kbytes
☑ Generate a new key every: 3600 seconds

Figure 7-60 Security Method Configuration

- Select **ESP** as the method for data encryption and data security.
- From the list box **SHA-1**, select the security algorithm and **3DES** as encryption algorithm.
- Keep the settings for **Session key**.
- Confirm your settings in the windows **Security Method Settings**, **Edit Security Method**,and **PDPServer/UserInterface Properties** with **OK**.

Definition of the IPSec Security Rules

- Select the menu **Create IP Security Policy...**.
- Select the tab **Rules**.



Security rules for communicating with other computers

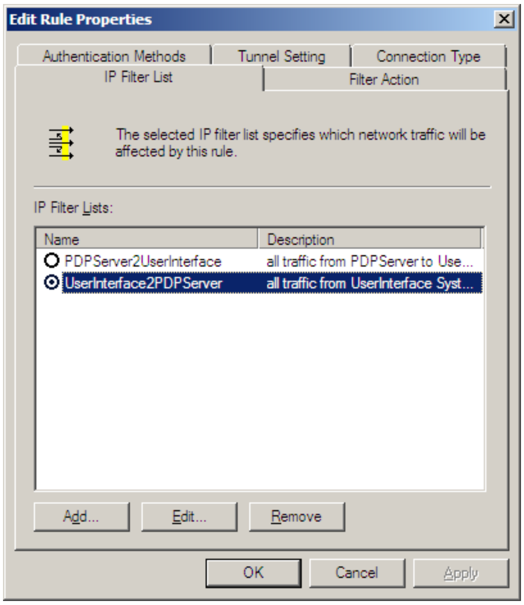
IP Security rules:

	IP Filter List	Filter Action	Authentication...	Tu
☑	UserInterface2PD...	PDPServer/UserInte...	Preshared Key	19
☑	PDPServer2UserI...	PDPServer/UserInte...	Preshared Key	19
☐	<Dynamic>	Default response (ea...	Kerberos	<N

☑ Use Add Wizard

Figure 7-61 IPSec Security Rule UserInterface2PDPServer

- In order to add 2 new security rules **Filter PDP Engineer/UI system (UserInterface) > PDPServer** and **PDPServer > UserInterface**, select **Add...**.
- Mark a checkmark in the check box, so that both rules work according to the PSK encryption process.
- Select a security rule and select **Edit...** in order to edit its properties.
- Select the tab **IP Filter List**.



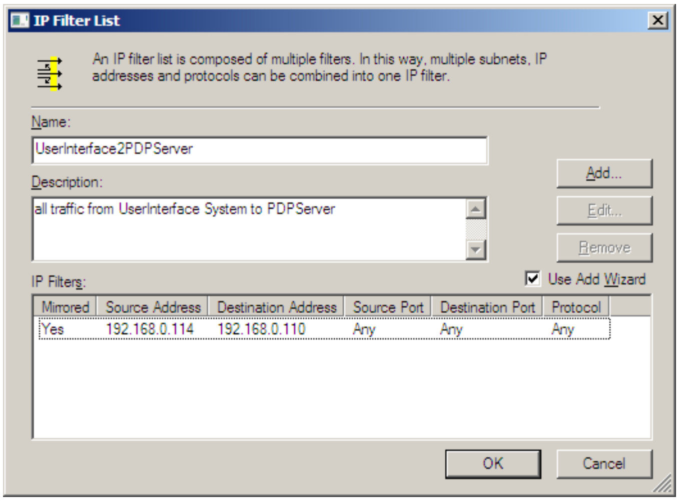
The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

	Name	Description
○	PDPServer2UserInterface	all traffic from PDPServer to Use...
●	UserInterface2PDPServer	all traffic from UserInterface Syst...

Figure 7-62 Editing the Security Rule UserInterface2PDPServer

- Select the filter **UserInterface2PDPServer** in order to edit its properties.



An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: UserInterface2PDPServer

Description: all traffic from UserInterface System to PDPServer

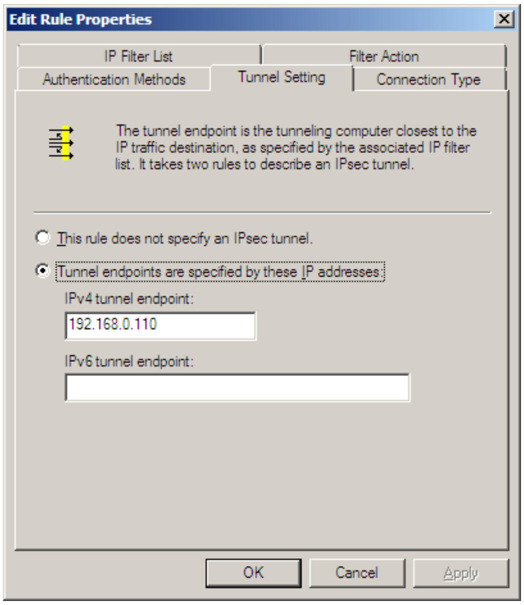
IP Filters:

☑ Use Add Wizard

Mirrored	Source Address	Destination Address	Source Port	Destination Port	Protocol
Yes	192.168.0.114	192.168.0.110	Any	Any	Any

Figure 7-63 IP Filter List

- Enter the IP address of the SIGUARD PDP Engineering/UI computer or its domain name as **Source Address**.
- Enter the IP address of the SIGUARD PDP Server or its domain name as **Destination Address**.
- Enter **Any** in the **Protocol** column, so that all protocols, for example, UDP, TCP, and Port 445 and 139, can pass through the IPSec tunnel.
- Click **OK** to close the dialog.
- Select the tab **Tunnel Setting**.



The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPsec tunnel.

○ This rule does not specify an IPsec tunnel.

● Tunnel endpoints are specified by these IP addresses:

IPv4 tunnel endpoint: 192.168.0.110

IPv6 tunnel endpoint:

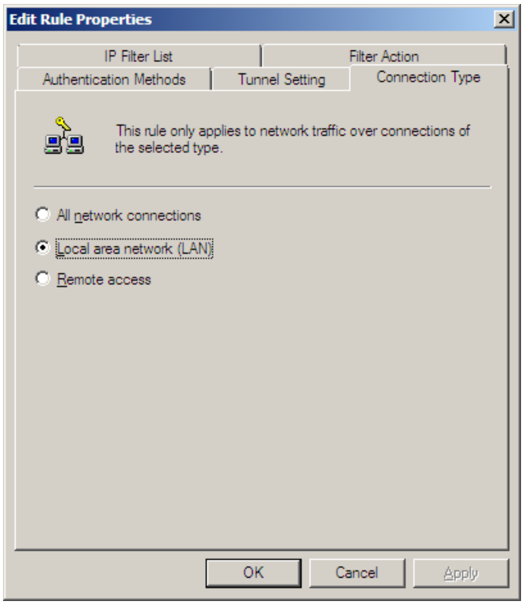
Figure 7-64 Settings for the IPSec Tunnel

✧ Select **Tunnel endpoints are specified by these IP addresses**.

In this entry in the IP filter list, the **Destination Address** is the tunnel endpoint of the SIGUARD PDP Server.

✧ Click **OK** to close the dialog.

✧ In the tab, select **Connection Type** in order to set the connection type.



This rule only applies to network traffic over connections of the selected type.

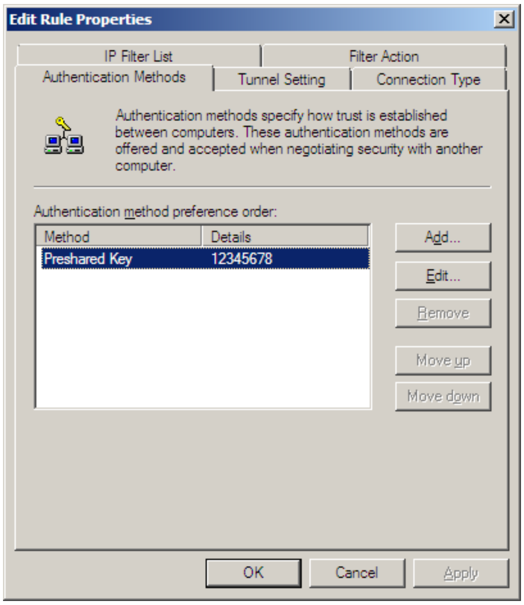
○ All network connections

● Local area network (LAN)

○ Remote access

Figure 7-65 IPSec Connection Type

- Select **Local Area Network (LAN)**.
- Click **OK** to close the dialog.
- Select the tab **Authentication Methods**.



Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Preshared Key	12345678

Figure 7-66 IPSec Authentication

- Select **Add..** in order to add a new IPSec authentication.
- Select an authentication method and select **Edit...** in order to edit its properties.
- Enter the method **Preshared Key**.
- Under **Details**, enter your personal security key.

  Change the given sequence of numbers. Select a security key that is at least 10 characters long and which includes alphanumeric characters and special characters.

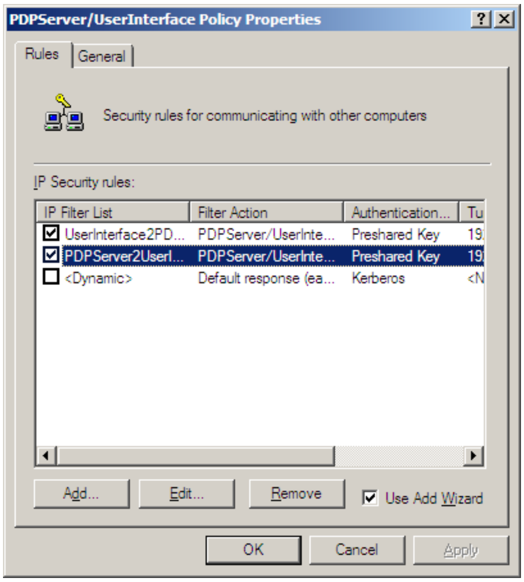
NOTE

The security key must not be given to the users. If the exported configuration file for installation on the local computer is transferred via a secure communication path, no security key must be entered. Therefore, use a long, complex security key.

- Click **OK** to close the dialog.

Configuration for the other Transmission Direction

✧ Select the **IP Filter List** for the other transmission direction.



Security rules for communicating with other computers

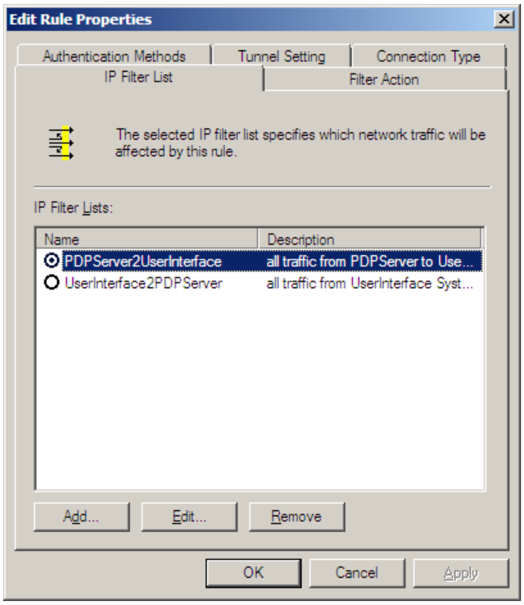
IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ UserInterface2PD...	PDPServer/UserInte...	Preshared Key	19
☑ PDPServer2UserI...	PDPServer/UserInte...	Preshared Key	19
☐ <Dynamic>	Default response (ea...	Kerberos	<N

☑ Use Add Wizard

Figure 7-67 IPSec Security Rule PDPServer2UserInterface

✧ Select the tab **IP Filter List**.



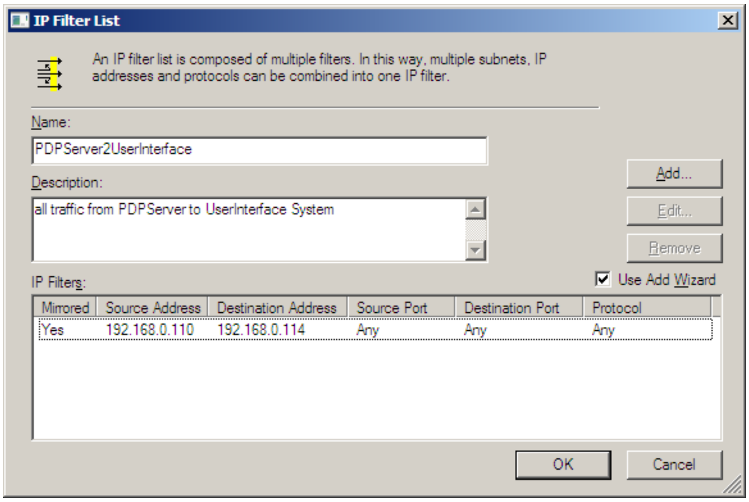
The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

Name	Description
● PDPServer2UserInterface	all traffic from PDPServer to Use...
○ UserInterface2PDPServer	all traffic from UserInterface Syst...

Figure 7-68 Editing the Security Rule PDPServer2UserInterface

- Select the filter **PDPServer2UserInterface** in order to edit its properties.



IP Filter List

An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: PDPServer2UserInterface

Description: all traffic from PDPServer to UserInterface System

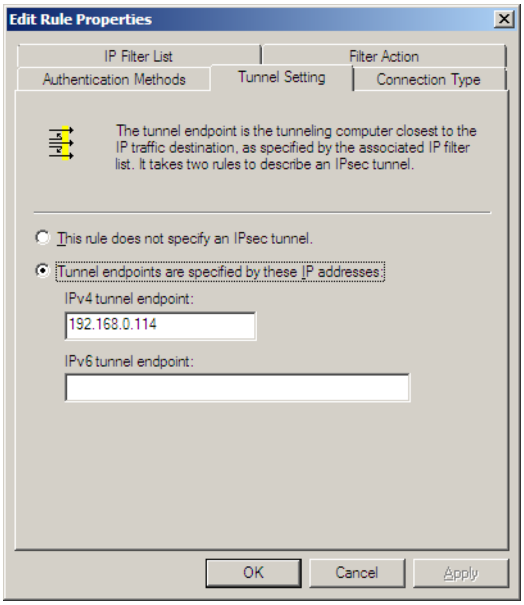
☑ Use Add Wizard

IP Filters:

Mirrored	Source Address	Destination Address	Source Port	Destination Port	Protocol
Yes	192.168.0.110	192.168.0.114	Any	Any	Any

Figure 7-69 IP Filter List

- Enter the IP address of the SIGUARD PDP Server or its domain name as **Source Address**.
- Enter the IP address of the SIGUARD PDP Engineer/UI computer or its domain name as **Destination Address**.
- Enter **Any** in the **Protocol** column, so that all protocols, for example, UDP, TCP, and Port 445 and 139, can pass through the IPSec tunnel.
- Select the tab **Tunnel Setting**.



Edit Rule Properties

The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPsec tunnel.

○ This rule does not specify an IPsec tunnel.

● Tunnel endpoints are specified by these IP addresses:

IPv4 tunnel endpoint: 192.168.0.114

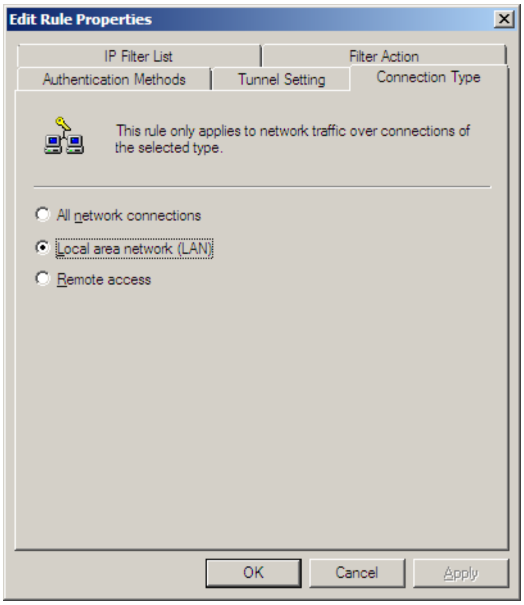
IPv6 tunnel endpoint:

Figure 7-70 Settings for the IPSec Tunnel

✧ Select **Tunnel endpoints are selected by these IP addresses**.

In this entry in the IP filter list, the **Destination Address** is the tunnel endpoint of the SIGUARD PDP Engineer/UI computer.

✧ In the tab, select **Connection Type** in order to set the connection type.



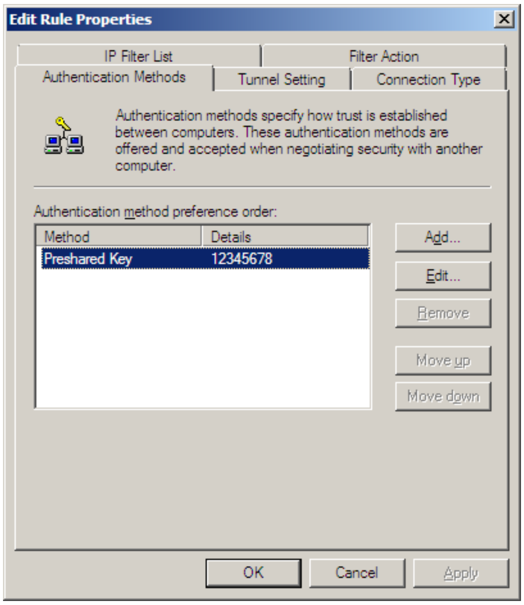
This rule only applies to network traffic over connections of the selected type.

○ All network connections
● Local area network (LAN)
○ Remote access

Figure 7-71 IPSec Connection Type

✧ Select **Local Area Network (LAN)**.

✧ Select the tab **Authentication Methods**.



Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Preshared Key	12345678

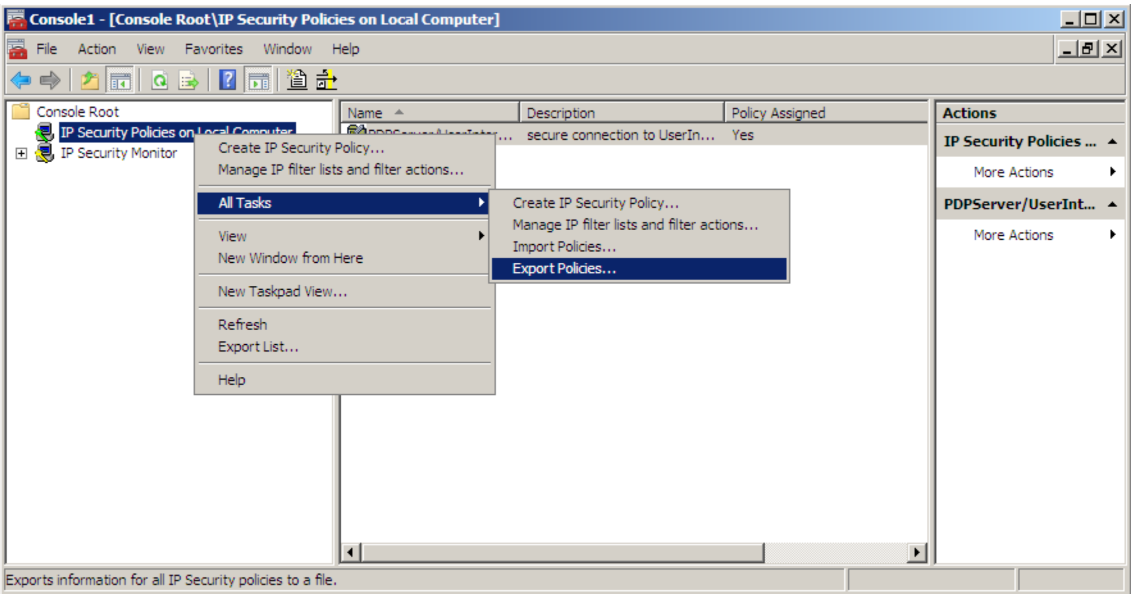
Figure 7-72 IPSec Authentication

- Enter the method and the security key as for the other transmission direction.
- Click **OK** to close the dialog.

Exporting the Configuration File

The configuration file which was created on the SIGUARD PDP Server is exported here in the format **Ipsec**. This file is overwritten and imported on the local computer via a **secure path**. Then, activate the security settings of **both** systems, on the SIGUARD PDP Server and on the local computer.

- Open the **Configuration Management Console**.
- Right-click the snap-in **IP Security Policies on Local Computer** and select the menu item **All Tasks > Export Policies...**.


Console1 - [Console Root\IP Security Policies on Local Computer]

Name	Description	Policy Assigned
PDPServer/UserInter...	secure connection to UserIn...	Yes

Exports information for all IP Security policies to a file.

Figure 7-73 Requesting Export of the Configuration File

- Assign a name for the configuration file.
- Click **Save As...** to close the dialog.
- Transfer the configuration file to the local computer via a **secure path**.

Importing the Configuration File

The configuration file is imported on the local computer.

- Insert the snap-ins in the **Configuration Management Console** of the local computer.
- Right-click the snap-in **IP Security Policies on Local Computer** and select the menu **All Tasks > Import Policies...**.

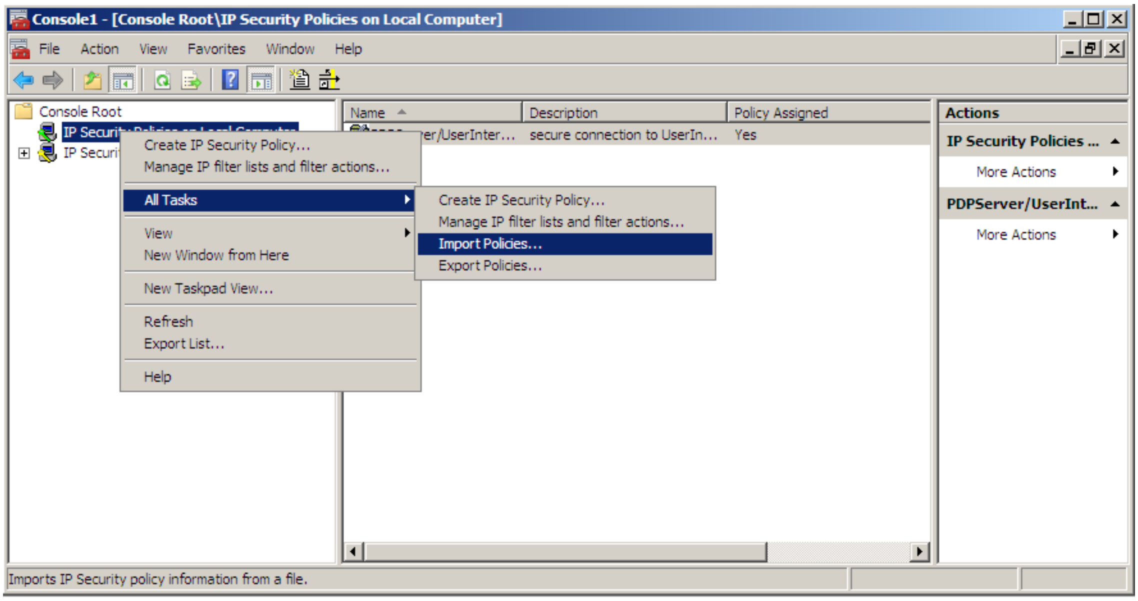


Figure 7-74 Requesting Import of the Configuration File

- Select the configuration file.
- Complete the import with **Open...**.

Activation of the Security Settings

Activate the security settings on both systems.

- Under **IP Security Policies on Local Computer**, right-click the entry **PDPServer/UserInterface Policy** and select the menu item **Assign**.

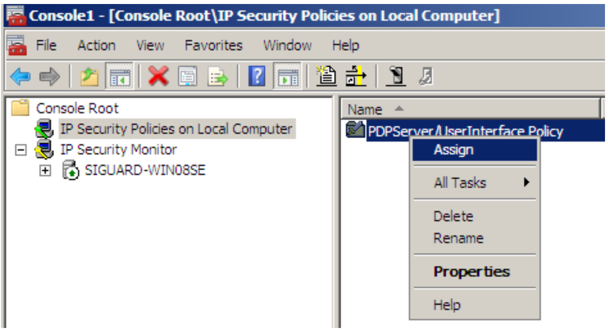
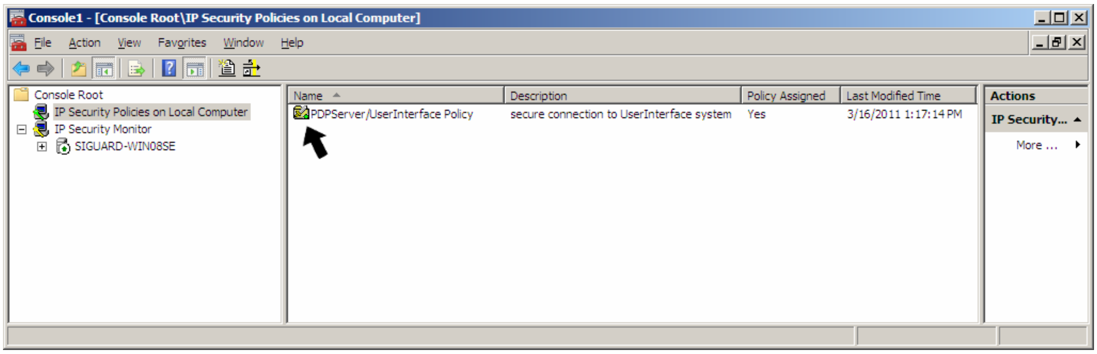

Console1 - [Console Root\IP Security Policies on Local Computer]
File
Action
View
Favorites
Window
Help
Console Root
IP Security Policies on Local Computer
IP Security Monitor
SIGUARD-WIN08SE
Name
PDPServer/UserInterface Policy
Assign
All Tasks
Delete
Rename
Properties
Help

Figure 7-75 Activation of the IPSec Security Settings



Name	Description	Policy Assigned	Last Modified Time
PDPServer/UserInterface Policy	secure connection to UserInterface system	Yes	3/16/2011 1:17:14 PM

Figure 7-76 IPSec Security Settings are Activated

As soon as the security settings are loaded, a green arrow appears in the icon for the configuration file.

Now, all IP data traffic between the SIGUARD PDP Server and the SIGUARD PDP Engineer/UI computer is encrypted. This setting is also retained, in case the system is restarted and a normal user logs on to the SIGUARD PDP Engineer/UI computer.

NOTE

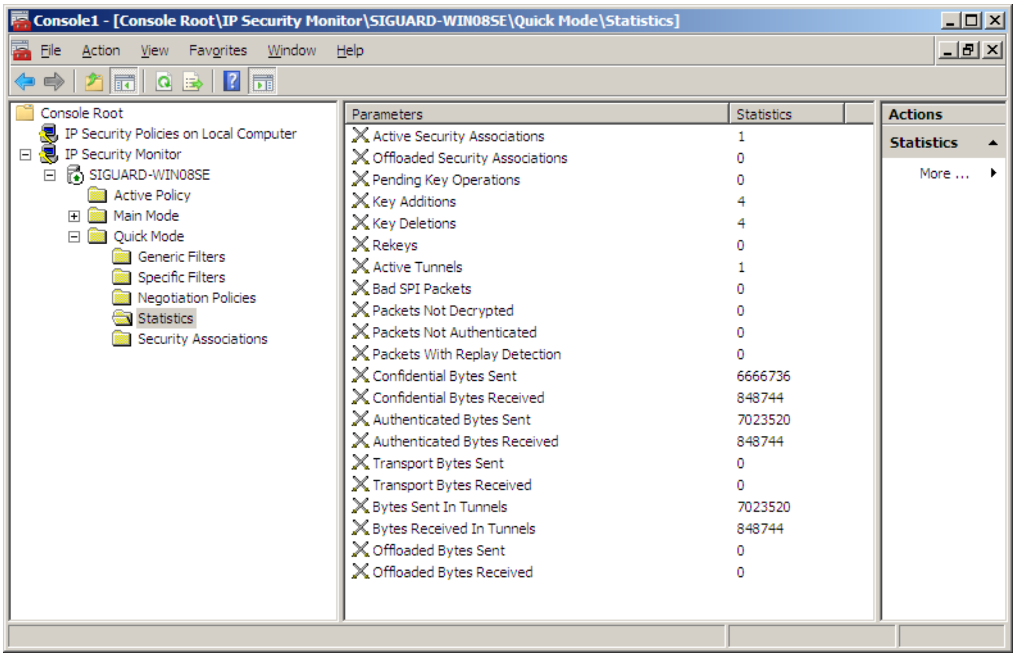
Additional security strategies can be added on both systems, either for access to other SIGUARD PDP Servers or for access via the SIGUARD PDP Engineer/UI computer to a server. The principle is the same.

✧ If you are uncertain whether the system is configured well, use the monitoring snap-in.

IPSec Monitoring

The current configuration can be monitored on the SIGUARD PDP Server.

- In the window **Configuration Management Console**, select the path **Console Root > IP Security Monitor > SIGUARD-WIN08SE > Quick Mode > Statistics**.



Parameters	Statistics
Active Security Associations	1
Offloaded Security Associations	0
Pending Key Operations	0
Key Additions	4
Key Deletions	4
Rekeys	0
Active Tunnels	1
Bad SPI Packets	0
Packets Not Decrypted	0
Packets Not Authenticated	0
Packets With Replay Detection	0
Confidential Bytes Sent	6666736
Confidential Bytes Received	848744
Authenticated Bytes Sent	7023520
Authenticated Bytes Received	848744
Transport Bytes Sent	0
Transport Bytes Received	0
Bytes Sent In Tunnels	7023520
Bytes Received In Tunnels	848744
Offloaded Bytes Sent	0
Offloaded Bytes Received	0

Figure 7-77 IPSec Monitoring

The most important parameters are **Bytes Sent In Tunnels** and **Bytes Received In Tunnels**. The IPSec tunnels are what is meant by tunnels.

7.5.2 IPSec Tunnel between PMU and SIGUARD PDP Server

7.5.2.1 General

If you use unsecure third-party communication networks, Siemens recommends using an IPSec tunnel between the PMUs and the SIGUARD PDP Server. To be able to use this IPSec tunnel, an additional security component, for example, SIEMENS **Scalance S**, must be used.

To do this, proceed as follows:

- Install the security module **Scalance S**.

  For details, also see *Figure 2-2*.

- Install the software **Security Configuration Tool**.
- Configure the security module **Scalance S**.

7.5.2.2 IPSec Configuration

If firewalls and/or routers are used between the SIGUARD PDP Server and the PMUs, the Scalance S modules are installed behind the corresponding inputs. Since the IPSec protocol is conducted over the firewalls, ESP data traffic must be authorized and UDP Port 500 must be enabled. If NAT-T (Network Address Translation Traversal) is used, UDP Port 4500 must be enabled and instead of **ESP**, **Encapsulated ESP** must be authorized.

Since the PMU protocol may be defined freely, Siemens recommends authorizing all data traffic between the SIGUARD PDP Server and the PMUs. Define a VPN group for the Scalance S network between the SIGUARD PDP Server and the PMUs.

NOTE

All Scalance S modules must be set up according to a global **IP Default Drop Firewall** policy. This policy must be set up as the last in the firewall configuration of a Scalance S module. Without this policy, all data traffic is permitted to pass through the IPSec tunnel.

A graphic interface (Security Configuration Tool) is available to configure the Scalance S modules. For operation and configuration of the Scalance S Security modules, see the SIEMENS Industry Manual, which you can download at the following address: *Download of the manual*.

7.6 Protection against Malware

7.6.1 General

The SIGUARD PDP Server and SIGUARD PDP Engineer/UI computer work with the Windows operating system. Therefore, Siemens recommends installing antivirus software, the virus signatures of which are continually updated, as protection against the infection by malware. Siemens recommends **Trend Micro OfficeScan** as antivirus software.

NOTE

Ensure that the antivirus software is configured in the manner recommended by Siemens.

To avoid an infection via USB devices, such as USB sticks or USB hard drives, the autostart function must be deactivated. This prevents the automatic execution of the software. It is also recommended to scan all USB devices with updated antivirus software for malware, before they are connected to the system. The antivirus software must be configured in the operating mode **on-access**. The same procedure applies to CDs or DVDs.

In addition to infection by malware via USB devices, infection can also occur through e-mail or browsing on the Internet. Therefore, Siemens recommends installing antivirus software that offers the following options:

- Checking e-mail
- Preventing access to unsecure Internet sites
- Preventing the use of unsecure e-mail servers

The computer must be configured such that infection by malware is prevented reliably. A secure configuration also includes the continuous updating of all installed third-party components.

System administrators must be trained such that the systems (for example, domain controller, file server, etc.) which they administer are used exclusively for administrative purposes.

In particular, SIGUARD PDP Servers which are used for administrative purposes must not be used for the following tasks:

- Browsing the Internet or playing any multimedia content
- Testing or installing untrustworthy software from dubious sources (for example, Internet, CD-ROM with shareware)
- Experimenting with SIGUARD PDP systems

7.6.2 Virus-Scanner System

Virus scanners are available in various designs:

- Self-standing product
- Client-Server configuration

  An example of this can be found in the following figure.

The setup data, configuration, and the updated virus signatures are distributed using a virus-scanning server. With the mechanisms **Push or Pull**, the information or the software is passed on to the systems.

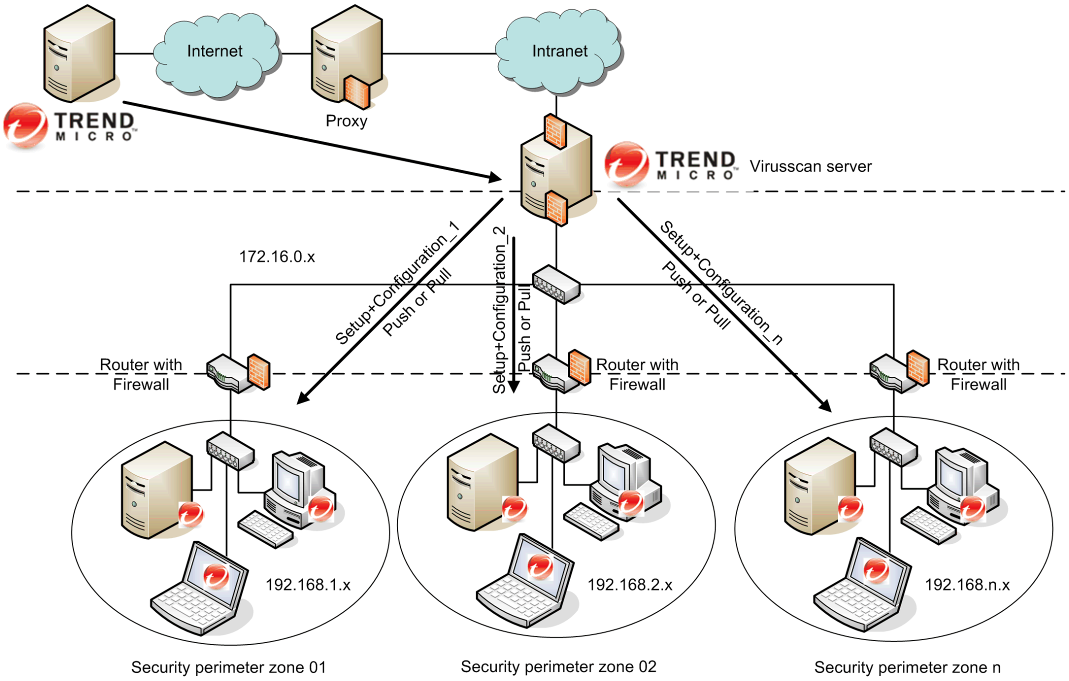


Figure 7-78 Virus-Scanner System by TrendMicro

The virus-scanner system by TrendMicro is tested and is recommended by Siemens.

7.7 Patch and Update Information

Security in the case of patch and update information is important over the entire lifespan of a product. The administration of patches for software is an essential part of this process. If possible, always activate the automatic update function of the installed software, for example, for Microsoft Windows, Adobe Acrobat, or Oracle Java. If Internet access is not authorized or is not available, install the security patches for the installed software manually.

If you do not have direct access or proxy access to the Internet, set up your own WSUS server (Windows Server Update Services). With WSUS, you can distribute all Microsoft patches in your Windows system. The method is comparable to the Client-Server from Virus Scan. The entire system receives the patches via an automated update mechanism in Windows. The significant difference is the server that makes the patches available.

Not all software producers offer an update system like the update system of Microsoft with which you can work via remote access. If you do not have direct access or proxy access to the Internet, install the security patches for the installed software manually. Inform yourself regularly on the homepage of the corresponding manufacturer in this regard.

■

Index