SIEMENS

SICAM
SICAM PAS/PQS

V8.20

Installation

E50417-M8976-C432-C7

NOTE

For your own safety, observe the warnings and safety instructions contained in this document, if available.

Document version: E50417-M8976-C432-C7.00

Edition: 11.2022

Version of the product described: V8.20

Preface

Purpose of the Manual

This manual describes how to install the SICAM PAS/PQS software system. It contains instructions for installing the SICAM PAS/PQS base software system.
Other manuals may be required if you wish to install additional options.

Target Audience

This manual is intended for personnel who install the SICAM PAS/PQS base software system.

Scope

This manual is valid for SICAM PAS/PQS.

Standards

SICAM PAS/PQS has been developed in compliance with ISO 9001:2008 standard.

Additional Support

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

Customer Support Center

Our Customer Support Center provides a 24-hour service.

Siemens AG
Smart Infrastructure – Protection Automation
Customer Support Center

Tel.: +49 911 2155 4466
E-Mail: *energy.automation@siemens.com*

Training Courses

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

Siemens AG
Siemens Power Academy TD
Humboldtstraße 59
90459 Nuremberg
Germany

Phone: +49 911 9582 7100
E-mail: *poweracademy@siemens.com*
Internet: *www.siemens.com/poweracademy*

Notes on Safety

This document is not a complete index of all safety measures required for operation of the equipment (module or device). However, it comprises important information that must be followed for personal safety, as well as 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 moderate or minor injuries.

NOTICE

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

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

NOTE

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

Qualified Electrical Engineering Personnel

Only qualified electrical engineering personnel may commission and operate the equipment (module, device) described in this document. Qualified electrical engineering personnel in the sense of this document are people who can demonstrate technical qualifications as electrical technicians. These persons may commission, isolate, ground and label devices, systems and circuits according to the standards of safety engineering.

Proper Use

The equipment (device, module) may be used only for such applications as set out in the catalogs and the technical description, and only in combination with third-party equipment recommended and approved by Siemens.

Problem-free and safe operation of the product depends on the following:

- Proper transport
- Proper storage, setup and installation
- Proper operation and maintenance

When electrical equipment is operated, hazardous voltages are inevitably present in certain parts. If proper action is not taken, death, severe injury or property damage can result:

- The equipment must be grounded at the grounding terminal before any connections are made.
- All circuit components connected to the power supply may be subject to dangerous voltage.

- Hazardous voltages may be present in equipment even after the supply voltage has been disconnected (capacitors can still be charged).
- Operation of equipment with exposed current-transformer circuits is prohibited. Before disconnecting the equipment, ensure that the current-transformer circuits are short-circuited.
- The limiting values stated in the document must not be exceeded. This must also be considered during testing and commissioning.

OpenSSL

This product includes software developed by the OpenSSL Project for use in OpenSSL Toolkit (*http://www.openssl.org/*).

This product includes software written by Tim Hudson (*tjh@cryptsoft.com*).

This product includes cryptographic software written by Eric Young (*eay@cryptsoft.com*).

Table of Contents

1 Introduction

All software components of SICAM PAS/PQS are stored on the SICAM PAS/PQS DVD or in the downloaded zip-file. The dongle included in the scope of delivery and the function-specific license keys, a Soft License or ALM-Licenses determine which features are enabled on the computer.

1.1 System Types

Depending on the structure and capacity of your system, you install SICAM PAS/PQS as a:

- Stand-alone system
- Distributed system

For configuration examples, refer to */1/ SICAM PAS, Overview* and */2/ SICAM PQS, Overview*.

Stand-Alone System

SICAM PAS/PQS as a **stand-alone system** runs on one single computer, the **Full Server**. The SICAM PAS/PQS **Full Server** holds the data distribution system of SICAM PAS/PQS, the relational database system and the user interface. Protocol drivers and additional SICAM PAS/PQS components are located on this computer.

Distributed System

SICAM PAS/PQS as a **distributed system** runs on several computers. The following rules apply in this configuration:

- One computer is the **Full Server**. The SICAM PAS/PQS data distribution system, the Relational Database Management System (RDBMS) and the user interface are located on this computer. Protocol drivers and certain other applications can also reside on this computer.
  Every distributed SICAM PAS/PQS configuration must have **exactly 1** Full Server.
- The other computers in this configuration are operated as **DIP**s (Device Interface Processors). These computers host the protocol drivers and additional functions such as the fault location function, the archive, and also the user interface.

Both types of SICAM PAS/PQS are installed using the same installation routine. The installation process for these 2 types of SICAM PAS/PQS is almost identical. During the installation, you only need to specify whether the computer is to be operated as a stand-alone system/Full Server or as a DIP. It is nevertheless essential to understand which type of system you are installing.
The data exchange between the **DIP** and the **Full Server** must be ensured during operation.

1.2 Installation Variants

You can install SICAM PAS/PQS as a

- Demo version
- Licensed version

The installation DVD of SICAM PAS/PQS includes all files of the software components. During the installation process, you must specify whether you want to install a licensed version or a demo version.

Demo Version

For the demo version, neither a dongle nor a Soft License nor ALM-Licenses are required.
In the demo version, SICAM PAS/PQS is installed as a **stand-alone system**, see *1.1 System Types*.
In the demo version, SICAM PAS/PQS runs for 3 hours. After 3 hours, the demo version – runtime is stopped. SICAM PAS/PQS UI – Configuration can be further used. After each restart of your computer, the runtime is available for another 3 hours.
Be aware of the following additional restrictions:

- Projects created in the demo version cannot be used in the licensed version.
- SICAM PAS/PQS cannot be operated as a distributed system.

With the demo version, only the following is saved:

- 1 fault record per device
- 1 transient record per device
- 1 slow-scan record per recorder (for example, SIMEAS R frequency/power record)
- Continuous PQ measuring data for 1 day
- Evaluation and compression results for 1 day
- PQ violation reports per measuring group for 1 day
- Maximum of 500 events
- 1 fault event per device

Licensed Version

The licensed version requires a dongle, Soft License, or an ALM License.
In the licensed version, SICAM PAS/PQS can be installed and operated both as a **stand-alone system** and as a **distributed system**.

2 Installation Requirements

SICAM PAS/PQS is a 32-bit application with specific requirements with regard to the hardware components and the operating system. Additionally, it must be ensured that the network has been properly installed.

2.1 Hardware Components

Computer equipped with:

- Processor:
  - Minimum: Intel Core 2 Duo 1.6 GHz
  - Recommended: Quad Core CPU 3 GHz
- Primary storage capacity:
  - Minimum: 2 GB
  - Recommended for engineering of large stations: ≥ 8 GB
- Hard disk capacity:
  - Minimum: 4 GB plus configured archive size
- Graphics card:
  - Minimum: 1024 x 768 pixel
  - Recommended: 1920 x 1080 pixel
- Monitor suitable for graphics card
- DVD drive
- Keyboard
- Mouse
- Network interface
- USB port

NOTE

SICAM PAS/PQS is released for computers with multi-core processors.
Computers with multi-processor main boards are supported when working in single-processor mode.

Optionally

- Time signal receiver
- Network adapter for Ethernet
- COM Expander
- PROFIBUS interface card CP5613 A3 or CP5623
- INSYS Modems analog/ISDN
- ISDN FRITZ!Card

2.2 Operating System

One of the following operating systems is required:

- Windows 11 Professional/Enterprise/IoT Enterprise (64-bit)
- Windows Server 2022 Standard with Desktop Experience (64-bit)

For existing projects which are migrated to the new SICAM PAS/PQS version, the following operating systems can continue to be used:

- Windows 7 Professional/Ultimate/Enterprise SP1 (32-bit or 64-bit)
- Windows 10 Professional/Enterprise/IoT Enterprise LTSC (64-bit)
- Windows Embedded 7 (SICAM Station Unit V2.40, 32-bit)
- Windows 8.1 Professional SP1 (64-bit)
- Windows Server 2008 R2 Standard SP1 (64-bit)
- Windows Server 2012 R2 Standard (64-bit)
- Windows Server 2016 Standard with Desktop Experience (64-bit)
- Windows Server 2019 Standard with Desktop Experience (64-bit)

NOTE

.NET Framework V4.7.2 or later is required. For operating systems like Windows 10 (earlier than 1803), Windows 2016 Server or earlier, install .NET Framework using the Windows update or the offline installer.

To download the offline installer, refer to *https://dotnet.microsoft.com/download/dotnet-framework/thank-you/net48-offline-installer*.

NOTE

If the **Windows Server 2008 R2 Standard SP1** is installed on the Full Server for a distributed SICAM PAS/PQS system (the Full Server and the DIP are different computers) or a redundant SICAM PAS/PQS system, the following must be observed for the Full Server:

- The DNS Client, function search and resource publishing, SSDP search, and UPnP device host services must have been enabled and started.

  If these services are not started, the automatic network share cannot be permanently enabled.
- The automatic network share must be enabled.
- The ports of the programs that are used for the communication between Full Server and DIPs must be opened in the firewall. This refers to the ports of the btiserver.exe, dbsrv17.exe, and DSIServer.exe programs.

NOTE

To install SICAM PAS/PQS on **Windows 7/Windows Embedded 7** (SICAM Station Unit V2.40, 32-Bit), you must download the KB2999226, KB3083324, and KB4499175 patches from *https://www.catalog.update.microsoft.com/Home.aspx* and execute them.

Windows Update

Siemens recommends you update the patches using the **Windows Update** service before installing/updating SICAM PAS/PQS. However, for an uninterrupted system operation, it is always recommended that you deactivate the automatic update of the operating system.

The applications of SICAM PAS/PQS use various network services, such as TCP/IP, SNTP, DCOM, and ODBC. Unsupervised operation of SICAM PAS/PQS is restricted by Windows Update because of the following reasons:

- The function of the network services could possibly be restricted by the Windows security updates.
- Manual intervention into the computer configuration is required (for example, other settings of the Windows firewall).
- The computer must be restarted after an update.
- The computer is connected with the Internet to perform the update, which involves a security risk.

NOTE

If the SSR service does not start after any Windows security updates, reinstall SICAM PAS/PQS.

Standby Mode

To operate SICAM PAS/PQS, it must be ensured that the operating system does not switch to standby mode.

✧ Select **Never** for **Standby** in the **Control panel**, **Energy options**, **Energy scheme** tab.

Automatic Maintenance

Automatic maintenance is a scheduled task in Windows 8.1 and later versions which performs many pre-defined tasks at specific time intervals. Automatic Maintenance stops all the running maintenance tasks and resumes them when the system is in idle state.
To avoid slowness or non-responsiveness:

✧ Perform **Automatic Maintenance** regularly on a system.
You change the scheduled time of all the maintenance tasks via
Control Panels > All Control Panels Items > Action Center.

Siemens recommends you deactivate the setting **Check for solutions to problem reports** under **Maintenance** to avoid sending the data to Microsoft and look for possible solution.

NOTE

For protection against malware infections, Siemens recommends to enable the latest virus patterns of Microsoft Security/Windows Defender.
If you use other antivirus software follow the instructions and recommendations of the manufacturer. Siemens recommends to specify the following directories in the list of exceptions:

- Archive directory
- %PAS_APPDATA%
- %ProgramData%\Siemens\SettingsManager

2.3 Configuring the Windows Network Operation

Be aware of the following when operating SICAM PAS/PQS:

- TCP/IP must be installed in any case, that is, even for a stand-alone system.
- **Your computer must be assigned a valid TCP/IP name.** Be aware that TCP/IP name conventions are stricter than Windows conventions. The host name must neither start with a number nor include a blank or special characters with the exception of _ and - . For example, **My PC** is a valid name under Windows. Due to the blank included, it cannot be used with TCP/IP.
- Before you install SICAM PAS/PQS, TCP/IP must be configured. SICAM PAS/PQS cannot be installed properly without a configured TCP/IP. An Ethernet adapter is required for the configuration of TCP/IP.
- **Power saving features:** Many hardware components have power saving features installed, usually as part of the BIOS on the computer. These features slow down or stop the system CPU during a period of inactivity. Additionally, the screen display enters the save mode and the hard disk stops rotating. As almost no industrial standards are available for these features, they may vary significantly depending on the individual manufacturer and model. For this reason, if these features have been enabled, SIEMENS cannot guarantee that the SICAM PAS/PQS software runs without any problems.

- If you operate **SICAM PAS/PQS** in a network with other computers, further configuration steps may be required: In addition to IP addresses and network connections, a mechanism for the assignment of computer names and IP addresses may be required in a TCP/IP network. The following 4 assignment options are available:
  - DNS <HELP=glossary.hlp TOPIC=gls_domain_namesystem>
  - WINS <HELP=glossary.hlp TOPIC=gls_WINS>
  - Broadcast name resolution
  - HOSTS and LMHOSTS <HELP=glossary.hlp TOPIC=gls_lmhosts> files

  In small networks in which IP addresses do not change, network connections can use a HOSTS or LMHOSTS file for the assignment of computer names and IP addresses. For more detailed information, refer to the corresponding Windows documentation.
- For a distributed SICAM PAS/PQS system, the Windows network interfacing must be configured on each computer in the system.
- For a SICAM PAS/PQS computer, it is recommended to configure Windows on the computer in such a way that the computer reboots automatically after a failure. Refer to your Windows/BIOS documentation for instructions.
- The **network share** must be permanently enabled. It is not enabled by default in all operating systems, for example, Windows Server 2008 R2.

2.4 Compatibility

SICAM Station Unit

The latest version of SICAM PAS/PQS can be used on the SICAM Station Unit V2.40.

SICAM PAS CC / SICAM SCC

For use with a redundant SICAM PAS CC/SICAM SCC V7.0x the appropriate SICAM PAS CC/SICAM SCC Hotfix (SICAM PAS CC V7.00 HF1, SICAM PAS CC V7.00 SP1 HF2, SICAM SCC V7.01 HF2 or later) must be installed on the SICAM PAS CC/SICAM SCC system.

When installing or uninstalling SICAM SCC V8.01 or earlier on the same computer after the installation of the latest version of SICAM PAS/PQS, the SICAM PAS/PQS latest version installation must be repaired afterwards.

SICAM SCC will support Unicode characters in a future version. Until then, do not use Unicode characters in projects with connection to SICAM SCC.

SICAM PQ Analyzer/SICAM SCC

To be able to connect to a SICAM PAS/PQS runtime archive, SICAM PQ Analyzer of the same version is required.

When installing or uninstalling SICAM SCC V8.01 or earlier on the same computer after the installation of the latest version of SICAM PQ Analyzer, the SICAM PQ Analyzer latest version installation must be repaired afterwards.

Siemens IEC 61850 Browser

The Siemens IEC 61850 Browser V4.0 is included on the DVD and must be installed separately.

OSCOP P

If you uninstall OSCOP P from the computer where both SICAM PAS/PQS and OSCOP P are installed you must reinstall SICAM PAS/PQS to ensure it functions properly.

SICAM Q80 Manager

Use SICAM Q80 Manger V3.22 and later on the SICAM PAS/PQS computer.

SICAM PQS NeQual Converter

Use the SICAM PQS NeQual Converter V2.03 with the latest version of SICAM PQS while using Unicode characters. You obtain the current version from the Customer Support Center.

SIGRA

After the installation of the latest version of SICAM PQS, if scheduled reports are configured and you repair SIGRA on the same computer, the SICAM PAS/PQS latest version installation must also be repaired.

Discontinuation

The **Windows XP** and **Windows 2003 Server** operating systems, as well as the **PROFIBUS FMS Master** application and the data transmission via an **X.21** interface are no longer supported by SICAM PAS/PQS V8.06 and later.

If you want to continue to use these functionalities, use SICAM PAS/PQS V8.05 and note the corresponding documentation.

2.5 Further Requirements

The following prerequisites must be met for the installation of the SICAM PAS/PQS software:

- You must be logged on as a user with **administrator rights**.
- To install SICAM PAS/PQS and SICAM SCC on the same computer, at least V7.00 must be installed for both of them.
- Install the TCP/IP network interfacing for Windows before installing SICAM PAS/PQS. For more detailed information on the installation of the network interface for Windows, refer to the Windows documentation.
- To configure SICAM PAS/PQS for the data exchange with PROFIBUS DP devices, install the PROFIBUS interface card (for example, CP5613/14) and the corresponding software components before installing SICAM PAS/PQS.
- If SICAM PAS/PQS is already installed on your computer and you want to perform a reinstallation or an upgrade, Siemens recommends you back up your database. During a reinstallation of SICAM PAS/PQS, the system prompts you to specify whether the existing database is to be maintained or overwritten.
- An SQL Anywhere database is created during the installation of SICAM PAS/PQS.

3 Installing SICAM PAS/PQS

3.1 General Information

The SICAM PAS/PQS DVD holds the SICAM PAS/PQS software with all required components and the following additional components:

- A readme file
- A note concerning the Open Source software used
- SIMEAS R PAR
- The demo project
- The device templates
- The manuals
- The Siemens IEC 61850 Browser
  For more information on the Siemens IEC 61850 Browser, refer to the online help and the readme file.

NOTE

Read the installation instructions carefully. Before you install SICAM PAS/PQS, check whether all system requirements are met, and in particular those for the installation and configuration of the TCP/IP network interfacing. After the installation and configuration of the TCP/IP network interfacing, you must reboot your computer.

NOTE

A **PDF reader** is required in order to be able to read the manuals.
Using the PDF reader, you can start a comprehensive search in all documents of a directory. To do this, use the **Advanced Search** function.
The documentation of SICAM PAS/PQS is stored in the **%PASINSTALLPATH%\Documentation\English** installation directory.

NOTE

If **DIGSI 5** is installed on your computer, you must uninstall it first before installing SICAM PAS/PQS. Perform a new installation of DIGSI 5 after installing SICAM PAS/PQS.

NOTE

If **SICAM PAS Secure Communication Add-on** is installed on your computer, you must uninstall it first before installing SICAM PAS/PQS.

3.2 Installation

The sequence of installation of SICAM PAS/PQS includes the following steps:

- Setting up a SQL Anywhere database and the system start parameters
- Configuring the ODBC data source names for SICAM PAS/PQS
- Installing the SICAM PAS/PQS software
- Installing the dongle driver
- Installing the Automation License Manager
- Installing the SICAM PAS/PQS documentation (PDF format)

SICAM PAS/PQS is installed via either of the following options:

- *3.2.1 Installation via DVD*
- *3.2.2 Silent Installation* that runs unattended with parameters defined in an XML file and is executed via command prompt

NOTE

The path of the **Setup** directory must not contain any special characters.

3.2.1 Installation via DVD

Proceed as follows in order to perform the installation:

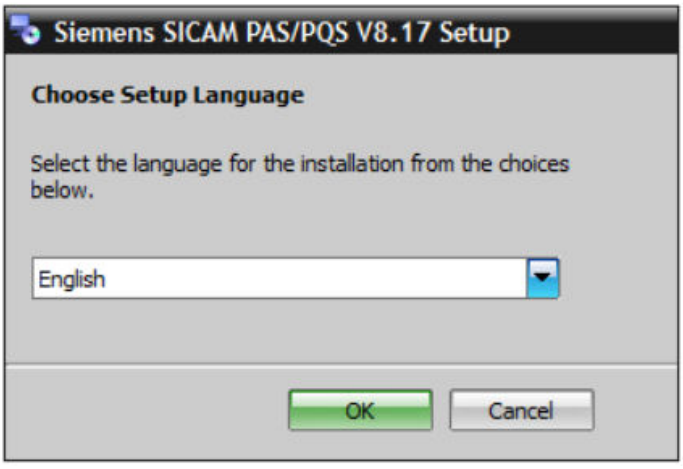
✧ Log on as an administrator user. If required, contact your local Windows administrator.

✧ Insert the DVD **SICAM PAS/PQS** into your DVD drive.

✧ Display the DVD content using the **Windows Explorer**.

✧ In the root directory of the DVD, double-click **Setup.exe**.

The installation is started.
The language selection dialog opens.

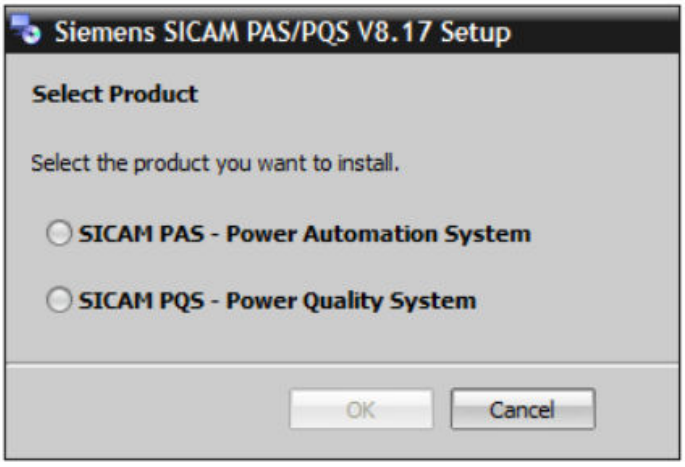


[sc_Setup_language, 10, en_US]

Figure 3-1 Language Selection

✧ Select the language to be used for the installation process and then click **OK** to confirm.

The product selection dialog opens.



[sc_Select_Product, 10, en_US]

Figure 3-2 Selecting the Product

NOTE

If **SICAM PAS V6.00** has already been installed on your computer, the system prompts you to uninstall it. Create a backup copy of your SICAM PAS/PQS database. Uninstall SICAM PAS/PQS and restart the installation.

When installing the latest version of SICAM PAS/PQS, **SICAM PAS/PQS V7.00 and later** is uninstalled automatically.

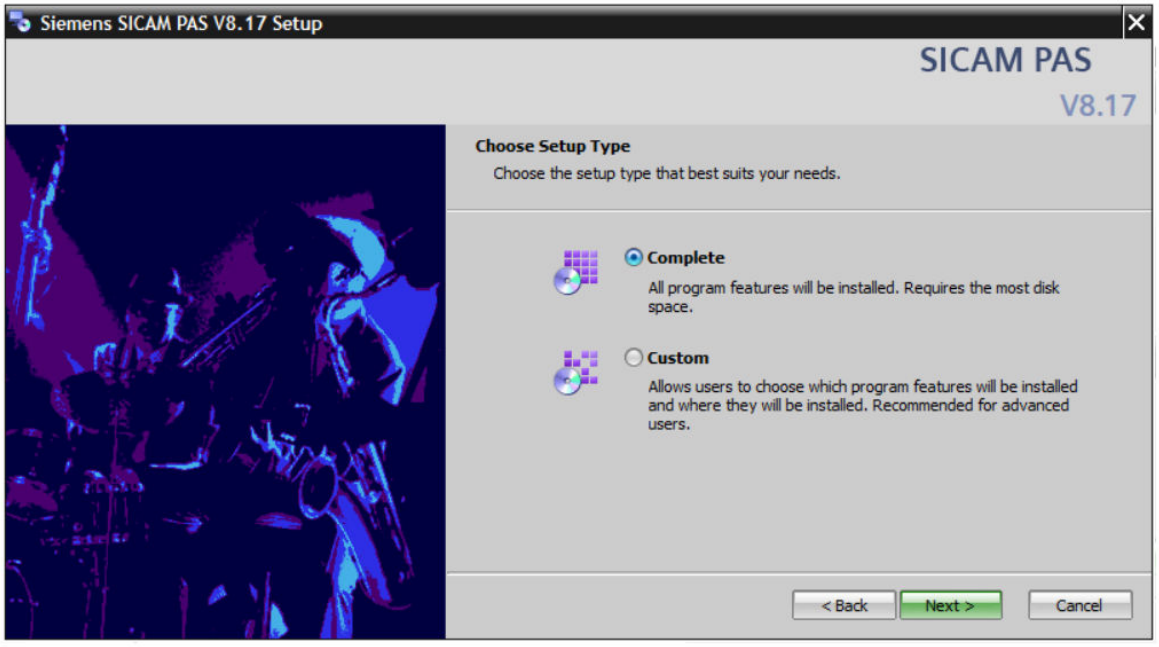
✧ Select the desired product and click **OK**.

NOTE

All further installation steps are identical for SICAM PAS and SICAM PQS. In this chapter, the installation is illustrated based on the example of SICAM PAS.

✧ In the dialog which opens, click **Next >**.

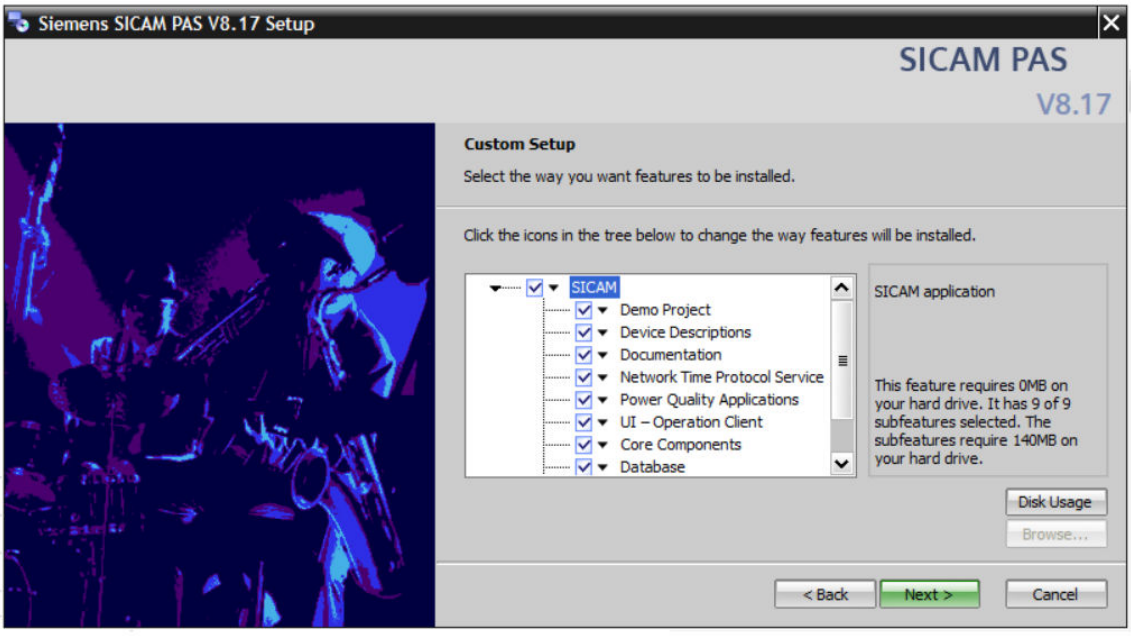
The **Choose Setup Type** dialog opens.



[sc_SICAMPAS_Setup_Type, 10, en_US]

Figure 3-3 Selecting the Setup Type

✧ Select the **Setup type**.
If you select **Complete**, the component selection dialog is skipped. All components are installed. In the dialog which opens next, you can specify the installation directory.
If you select **Custom**, the component selection dialog opens.



[sc_SICAMPAS_Custom_Setup, 10, en_US]

Figure 3-4 Selecting SICAM PAS/PQS Components

The following components are installed by default:

- **Demo Project**
  Configuration database of a demo project

- **Device Descriptions**
  Device templates
- **Documentation**
  SICAM PAS/PQS manuals in PDF format
- **Network Time Protocol Service**
  This component enables the time synchronization of individual computers in a SICAM PAS/PQS system, see *7 System Time*.
- **Power Quality Applications**
  Components for the Power Quality applications
- **UI – Operation Client**
  Access to SICAM PAS/PQS UI – Operation from a remote computer via browser
- **Core components**
  System files of the SICAM PAS/PQS software
- **Database**
  SQL Anywhere database system SQL scripts can be executed using Interactive SQL. You can customize the destination path of the database.
- **System Services**
  System files of the SICAM PAS/PQS software. You can customize the destination path of the system services.

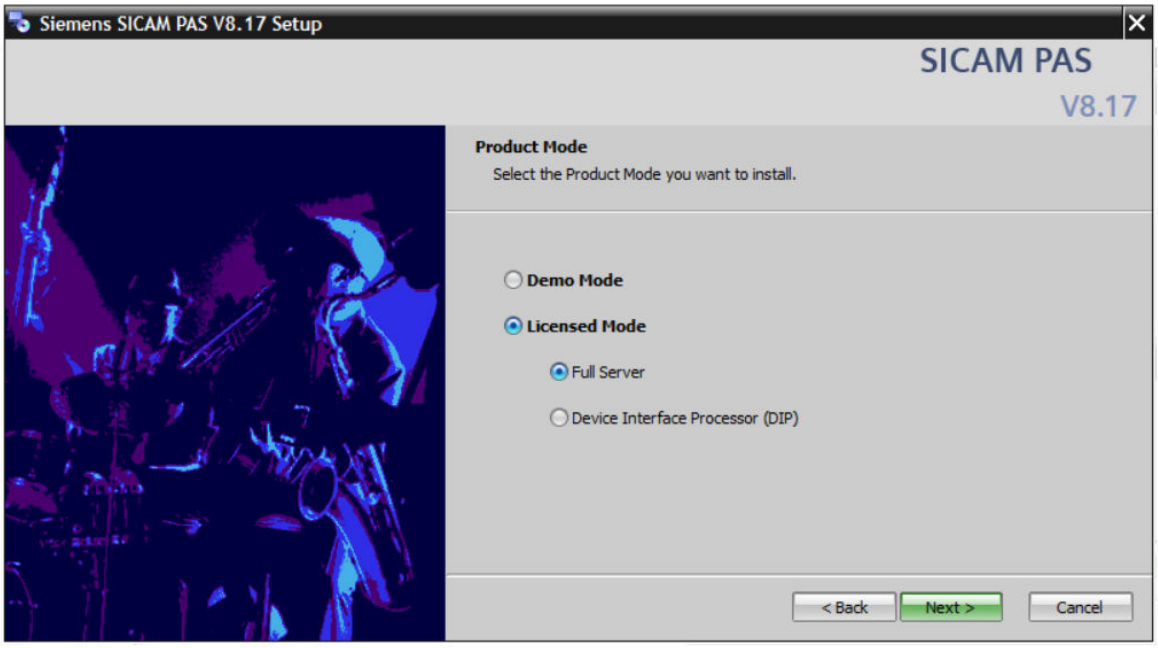
The components which are not displayed in gray (dimmed) can be deselected.

✧ Click **Disk Usage** in order to check whether sufficient free memory is available. If the memory capacity is not sufficient, deselect components or install them on another drive.

✧ Click **Browse** in order to change the installation path for a component.

✧ Apply the default settings (recommended) or select the components to be installed.

✧ Click **Next >**.



[sc_SICAMPAS_Product_Mode, 10, en_US]

Figure 3-5 Selecting the Product Mode (Licensed Version or Demo Version)

✧ Select **Demo Mode** if you have received SICAM PAS/PQS for demonstration purposes.

- or -

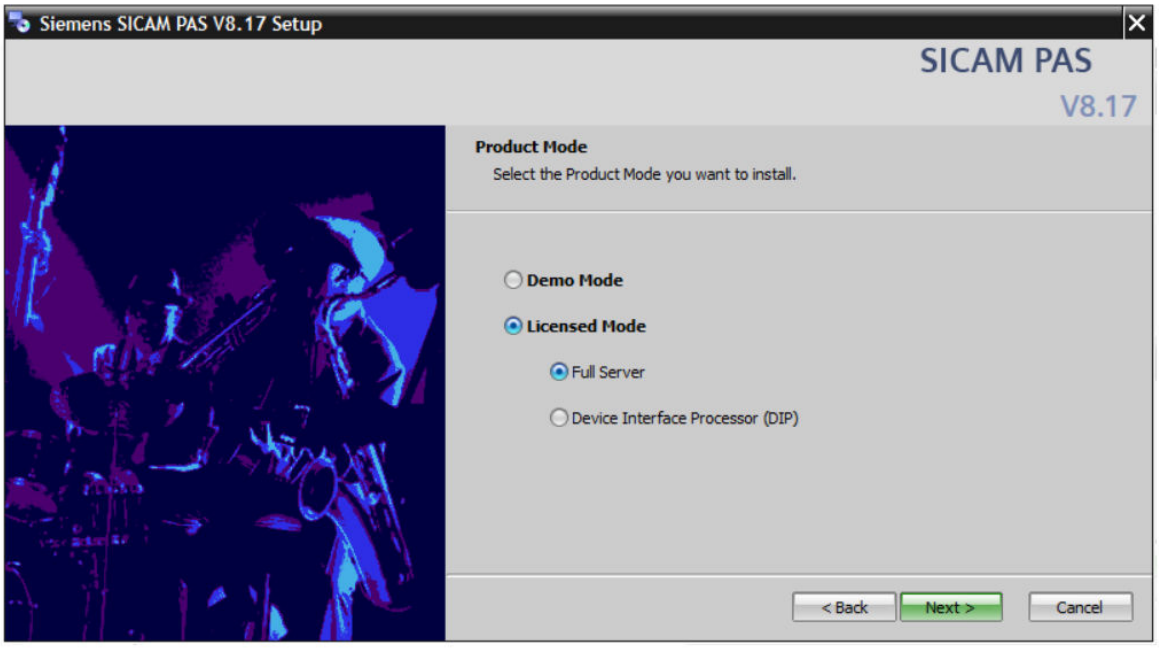
✧ Select **Licensed Mode** if you have purchased a full version of SICAM PAS/PQS.
If you select **Licensed Mode**, you can additionally specify whether you want to install a **Full Server** or a **DIP**.
If you are using the demo version of SICAM PAS/PQS, the **Full Server** is installed.

✧ Select **Full Server** if your computer is a stand-alone computer or is used as a server in a distributed SICAM PAS/PQS.
Every distributed SICAM PAS/PQS requires exactly one server.

- or -

✧ Select **Device Interface Processor (DIP)** if your computer is the DIP of a distributed SICAM PAS/PQS.
Every distributed SICAM PAS/PQS requires exactly one Full Server. The other computers in the system are DIPs.

✧ Click **Next >**.
If you are using SICAM PAS/PQS for the first time, a configuration database does not exist and the following dialog is not displayed.
If a database has already been installed under the specified path, the system prompts you whether the existing database is to be retained or overwritten. If you have updated SICAM PAS/PQS and want to use the existing database, the conversion is completed by executing the Feature Enabler.
It is possible that the database has been created using a SICAM PAS/PQS version that has previously been uninstalled.



[sc_SICAMPAS_Product_Mode, 10, en_US]
Figure 3-6 Database Query

✧ Select **Yes**, to lose all the current settings.

- or -

✧ Select **No**, to retain the existing database.

NOTE

An existing SICAM PAS/PQS database of version V5.1x and later is converted to the latest version upon the initial start-up of **SICAM PAS/PQS Feature Enabler**.

If you upgrade from an existing version of SICAM PAS/PQS to the latest version and select **No**, the database to be opened is created with an older version of SICAM PAS/PQS. Under this condition, **SICAM PAS/PQS UI – Operation Client** cannot be opened.

To open **SICAM PAS/PQS UI – Operation Client**:

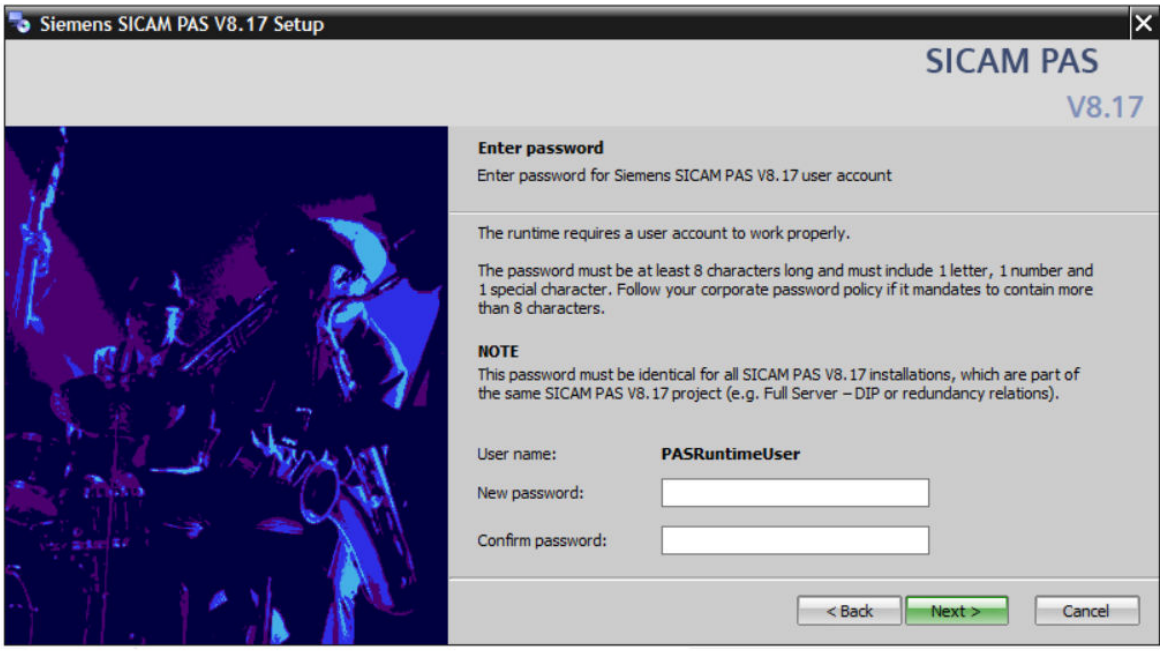
- Open **SICAM PAS/PQS UI – Configuration** or **SICAM PAS/PQS UI – Operation**.
  The Adapting the database dialog opens to enable you to execute the scripts which will allow you to use the database with the current version of SICAM PAS/PQS.
- Click **Yes**.
  The **Report** displays the progress and completion of the execution of the scripts. **SICAM PAS/PQS UI – Operation Client** can now be opened successfully.

✧ Select **Yes** to replace the existing database.

✧ Click **Next >**.

During the installation process, a new **PASRuntimeUser** is created.

This user is added to the **SICAM PAS PQS Users** (created during the installation) and **Users** groups.



[sc_SICAMPAS_Password, 10, en_US]

Figure 3-7 Creating the SICAM PAS User Account

NOTE

You can also use a different user instead of **PASRuntimeUser**, see *3.2.3 Using a Different User Account in PAS Runtime*.

Only the user that has been logged on to Windows during installation of SICAM PAS/PQS will automatically be added to the **SICAM PAS PQS Users** group by the installer. Further Windows users that should be able to work with SICAM PAS/PQS must be manually added to the **SICAM PAS PQS Users** group via **Computer Management > Local Users and Groups > Groups**.

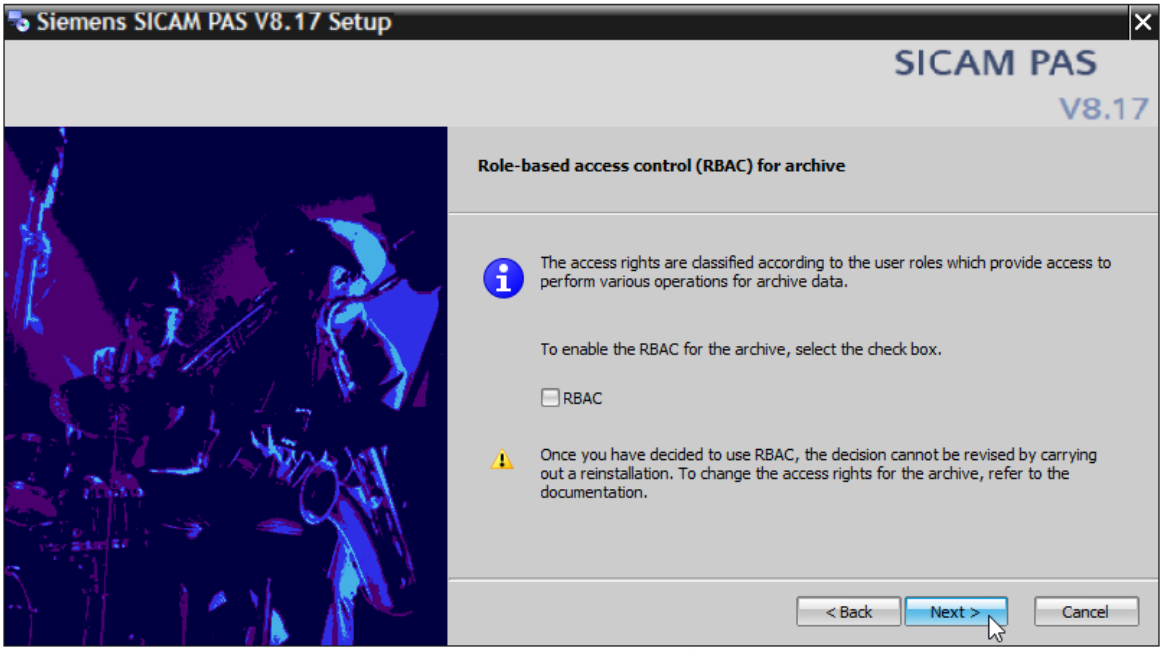
NOTE

The password must be at least 8 characters long and must include 1 letter, 1 number and 1 special character. Follow your corporate password policy if it mandates to contain more than 8 characters.

This password must be identical for all SICAM PAS/PQS installations that are part of the same SICAM PAS/PQS project (for example, Full Server-DIP or redundancy relations).

The entered password will be set as the password for the already existing **PASRuntimeUser** user.

✧ Enter a password and click **Next >**.



[sc_RBCA_FirstInstallation, 9, en_US]

Figure 3-8 Role-based Access Control for Archive

When installing SICAM PAS/PQS for the first time, Windows user groups are added to provide a role-based access control for the archive (RBAC) to perform various operations for the archive data.

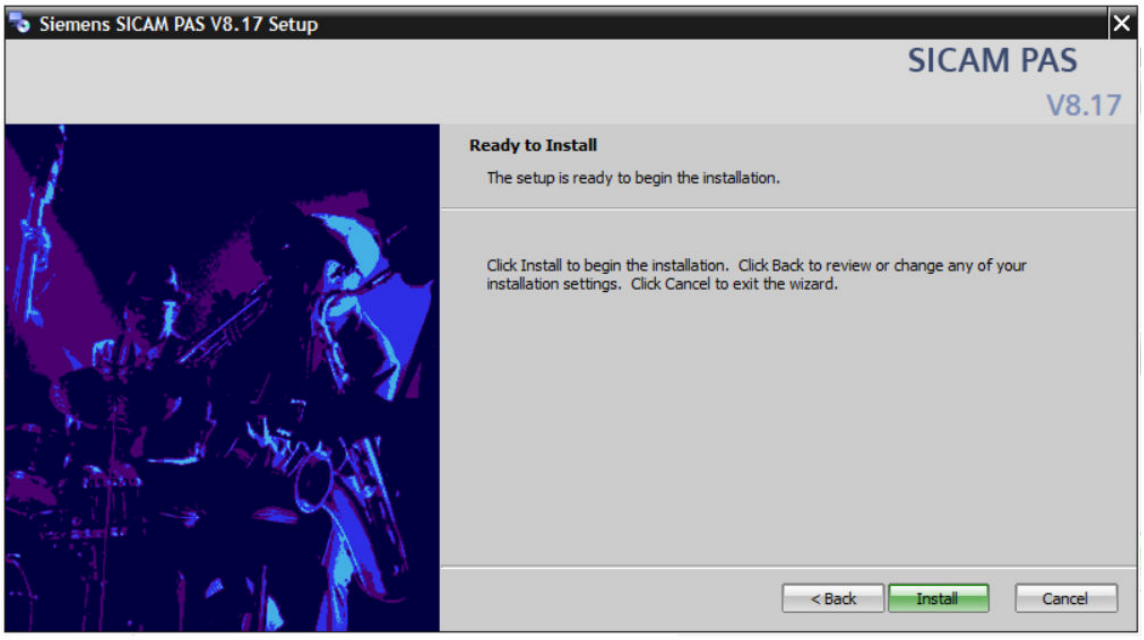
If you select the **RBAC** check box, the RBAC gets activated and your user account is added to the **SICAM PQ Analyzer ADMIN** user group with all rights.

If you do not select the **RBAC** check box, the user groups remain empty and any user has all the access rights for the archive.

To change this setting, a user account or a domain user group can be manually added to the **SICAM PQ Analyzer ADMIN**, **SICAM PQ Analyzer ENGINEER**, **SICAM PQ Analyzer OPERATOR**, or **SICAM PQ Analyzer VIEWER** user group via **Computer Management > Local Users and Groups > Groups**.

For more information on RBAC, refer to */13/ SICAM PQ Analyzer*.

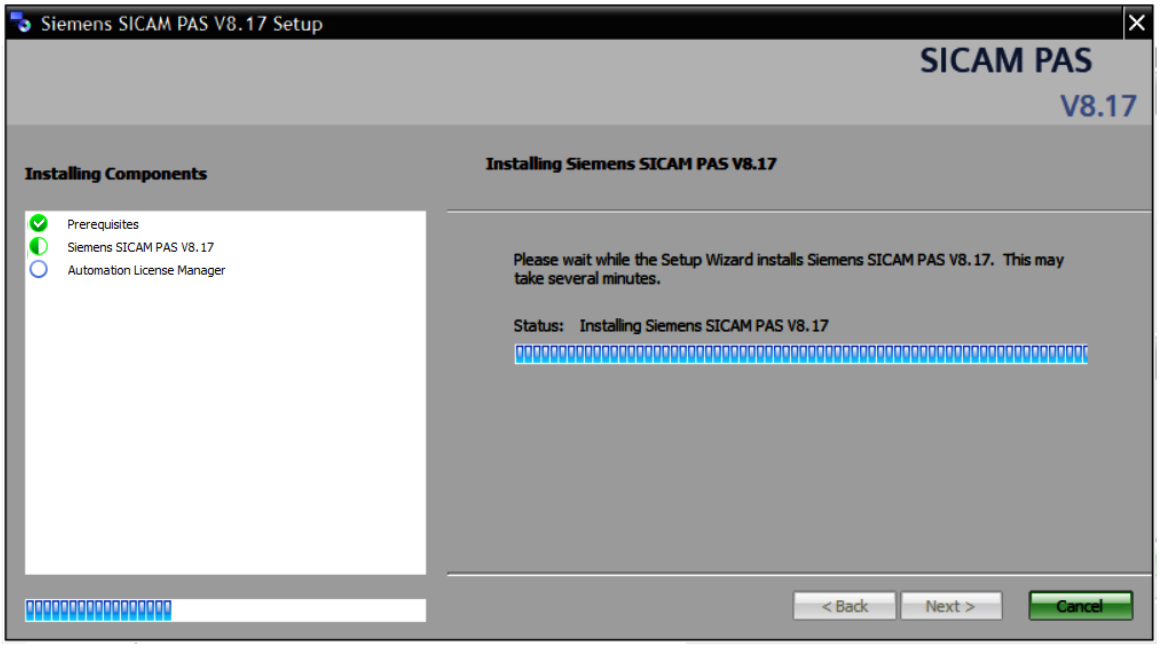
✧ Click **Next >**.



[sc_SICAMPAS_Ready_to_Install, 10, en_US]

Figure 3-9 Starting the Installation

✧ Click **Install**.



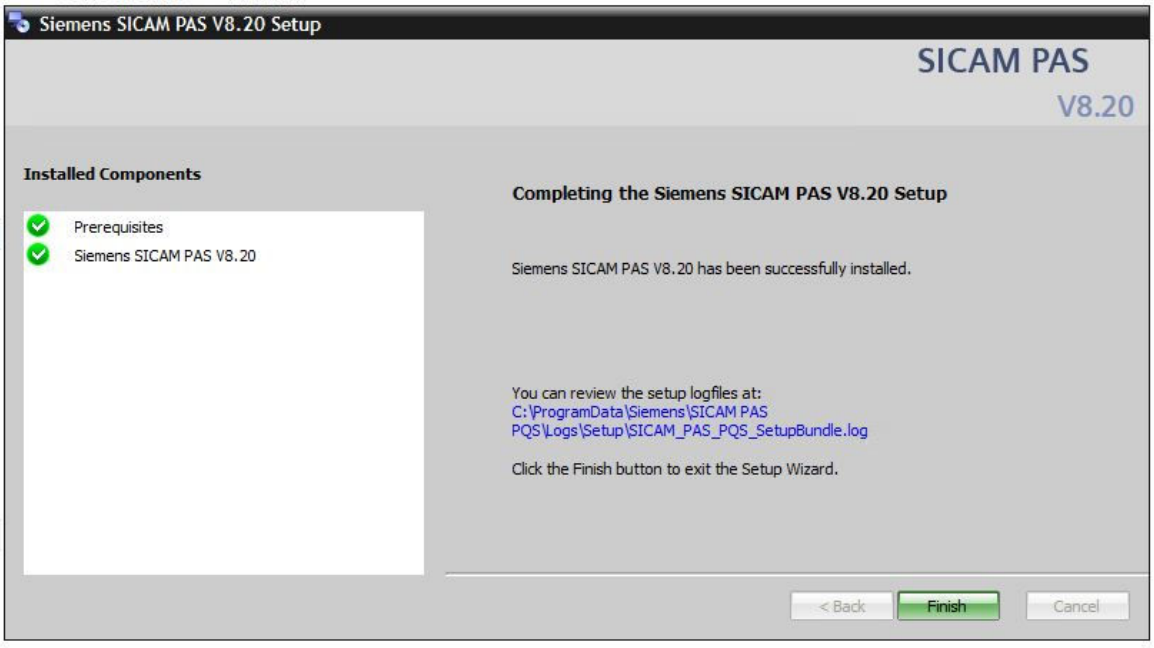
[sc_SICAMPAS_Install_Progress, 10, en_US]

Figure 3-10 Installation in Progress

This starts the installation process. The following steps are executed:

- The installer copies the SQL Anywhere software to the hard disk and creates the database required for the SICAM PAS/PQS software.
- The installer copies the SICAM PAS/PQS software to the hard disk.
- The installer creates the Windows Registry entries, which ensure that the SICAM PAS/PQS services (for example, SSR, IPCDaemon, SARAMonitoring, DfAgent) starts up automatically. Additionally, the installer customizes the system's PATH variable, creates Windows Services and program groups, inserts menu items in the Start menu, and starts individual services.

The following dialog is displayed as soon as the installation has been completed:

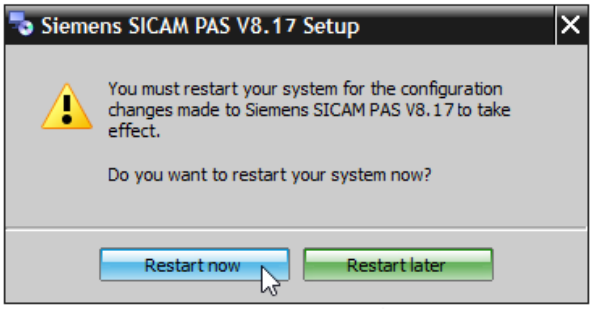


[sc_SICAMPAS_Installed_Components, 11, en_US]

Figure 3-11 Completing the Installation

✧ Click **Finish**.

After the installation, the system prompts you to restart the computer.



[sc_SICAMPAS_Restart, 10, en_US]

Figure 3-12 Restart

✧ Click **Restart now**.

The SICAM PAS/PQS installation is now complete. The computer is restarted.

NOTE

The dongle includes all the license keys ordered and enables the corresponding features. As an alternative to a dongle you can license the system via Internet for a computer or a virtualization solution and enable it via the Soft License, or by using the ALM license model.

In case of an upgrade or reinstallation of an existing system V8.01 or earlier (old dongle), the features must be enabled in the Feature Enabler. For more information, see *A.19 Using a Dongle to License a SICAM PAS/PQS System, V8.01 and Earlier*.

In case of an upgrade or reinstallation of an existing system V8.17 or later, ALM must be used for licensing. For more information, see *5.2 Using Online Software Delivery (OSD) to License a SICAM PAS/PQS System, V8.17 and Later*.

Be aware of the following:

- For the operation of a Full Server, the **Runtime - Small/Medium/Large** function must have been enabled.
- To configure a SICAM PAS/PQS system, the **Configuration** function must have been enabled.

NOTE

During the installation of SICAM PAS/PQS, the **%SR5_DATA%** directory is created and enabled with full permission for all users of the **SICAM PAS PQS Users** group.

The **Archive Server monitoring service**, **Defragmentation Agent**, **PowerCC IPC Daemon**, and **SSR** services run with the **PASRuntimeUser** login.

SICAM PAS/PQS saves configuration data in the **%SR5_DATA%** directory. In order to retrieve current configuration data, the other SICAM PAS/PQS computers must be able to access this directory.

NOTE

If the SSR service fails to start after restarting the computer, proceed as follows:

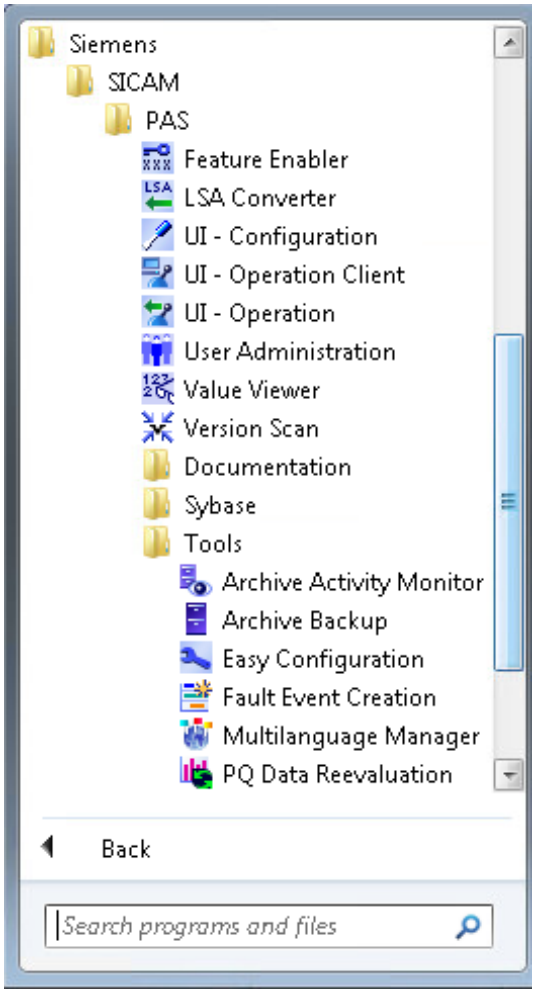
- Right-click the **ASRBaseAddressEditor.exe** application and select **Run as administrator** from the context menu. You will find this application in the SICAM PAS installation folder for binary files (%PAS_BIN%).
- Restart the computer.

NOTE

The following folders are provided security permission for the **Users** group with full permission:

- %commonappdata%Siemens\SettingsManager
- %commonappdata%Siemens\SICAM PAS PQS
- %commonappdata%Siemens\SICAM PQ Analyzer

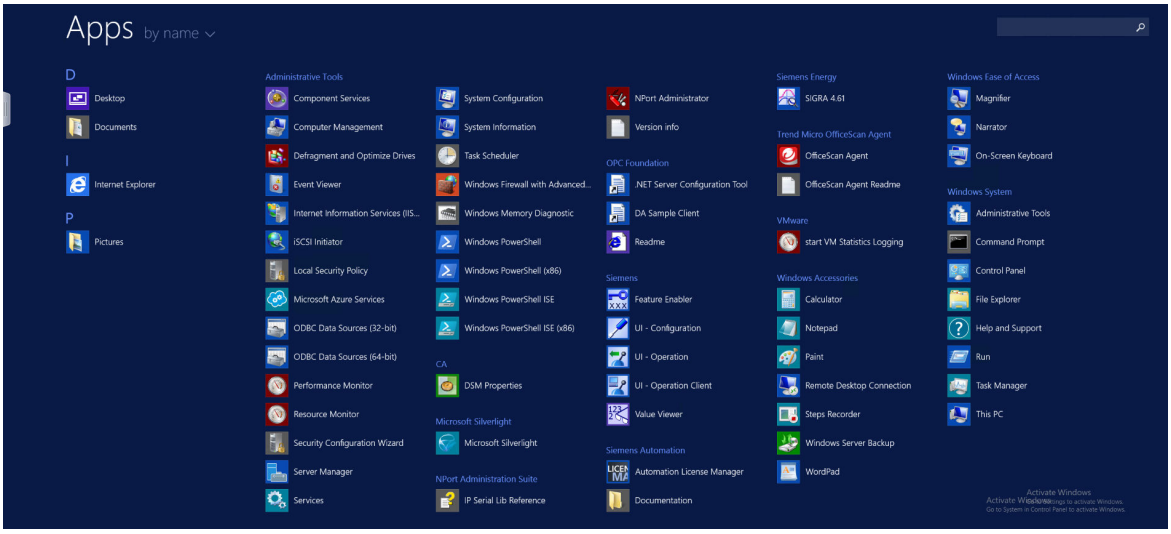
After the installation on Windows 7, shortcuts for SICAM components are created in the **All Programs** list and in the **SICAM PAS/PQS** directory.



[sc_Windows7, 4, en_US]

Figure 3-13 All Programs List - Windows 7

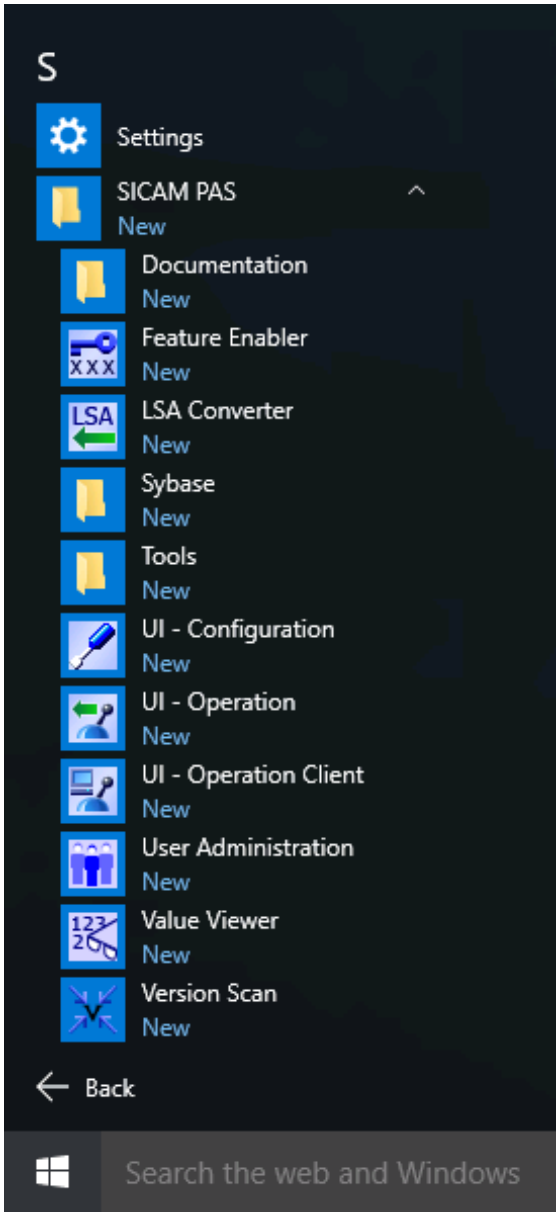
After the installation on Windows 8.1 or Windows Server 2012 R2, tiles/shortcuts for SICAM components are created in the **Apps** window and in the **SICAM PAS/PQS** directory on the desktop.



[sc_Apps_Window, 2, en_US]

Figure 3-14 Apps Window in Windows 8.1 or Windows Server 2012 R2

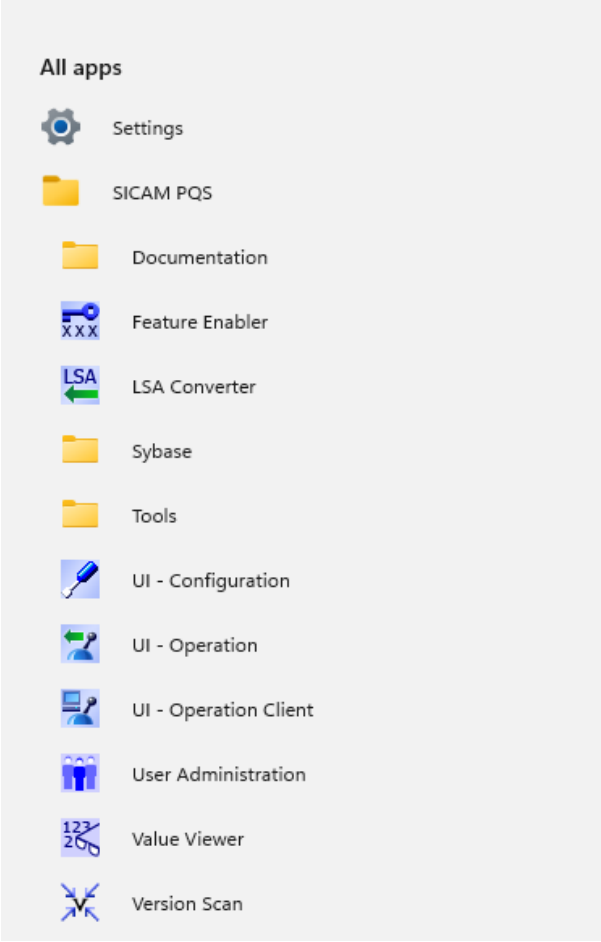
After the installation on Windows 10 or Windows Server 2016/2019, shortcuts for SICAM components are created in the **All Apps** list in the **SICAM PAS/PQS** directory.



[sc_Windows10, 1, en_US]

Figure 3-15 All Apps List - Windows 10 or Windows Server 2016/2019

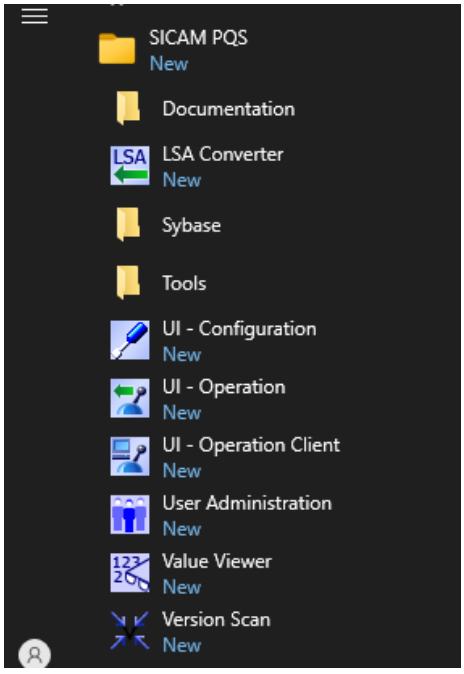
After the installation on Windows 11, shortcuts for SICAM components are created in the **All Apps** list in the **SICAM PAS/PQS** directory.



[sc_Windows11, 1, en_US]

Figure 3-16 All Apps List - Windows 11

After the installation on Windows Server 2022/21H, shortcuts for SICAM components are created in the **All Apps** list in the **SICAM PAS/PQS** directory.



[sc_WindowsServer2022, 1, en_US]

Figure 3-17 All Apps List - Windows Server 2022/21H

3.2.2 Silent Installation

The silent installation of SICAM PAS/PQS is performed in 2 steps:

- Editing the XML file that defines the:
  - Display of error messages
  - Product type
  - Installation location
  - Server type
  - Installation mode
  - Password for **PASRuntimeUser**
  - Replacement of existing database
  - Access control for archive
- Running the Setup.exe with parameters for:
  - Source
  - Language
  - Reboot

Editing the XML File

To edit the XML file:

✧ Copy the **Setup** folder from the DVD to a preferred location onto your local computer.

✧ Open the **SilentConfig.xml** file from the **SetupData\Configuration** folder using any text or XML editor (for example, Notepad++).

NOTE

The **SilentConfig.xml** is a read-only file by default.
To enable the edit permissions:

- Right-click the file and select **Properties**.
  The **Properties** dialog opens.
- Clear the **Read-only** check box.

✧ Modify the **SilentConfig.xml** file according to your individual needs:

Property name	Value	Description
<ShowErrorDialog>	true, false	Display of error messages If you set the value as **true**, error messages are displayed for each of the installation error encountered. If you set the value as **false**, error messages are not displayed. Errors encountered during the installation are logged in the log files at **%programdata%\Siemens\SICAM PAS PQS\Logs\Setup**.
BRAND	PAS, PQS	Product type SICAM PAS or SICAM PQS is installed based on the entered value.
INSTALLDIR		Installation location, default value: **%PASINSTALLPATH%**
SERVER_TYPE	FullServer, DIP	Server type If your computer is a stand-alone computer or is used as a Server in a distributed SICAM PAS/PQS, enter **FullServer**. If your computer is the DIP of a distributed SICAM PAS/PQS, enter **DIP**.
INST_MODE	Licence, Demo	Installation mode If you have received SICAM PAS/PQS for demonstration purposes, enter **Demo**. If you have purchased a full version of SICAM PAS/PQS, enter **Licence**.
PASSWORDFORSSR	PassWord123$	Password for the **PASRuntimeUser**. You must enter a password of at least eight characters that includes both alpha numeric and special characters.
INSTALLDATABASE	0, 1	Replacement of existing database The value **0** does not overwrite an existing database. The value **1** overwrites an existing database.
ENABLEUSERMANAGE-MENT	0, 1	Role-based access control for archive The value **0** does not provide role-based access control for the archive. The value **1** provides role-based access control for the archive.

✧ Save the changes made to the **SilentConfig.xml** file.

Running Setup.exe

✧ Open the **Command Prompt** with administrator rights.

✧ Execute the **Setup.exe** by using either of the following commands:
<Source>\Setup.exe /si /L <lang ID> or **<Source>\Setup.exe -si /L <lang ID>**
where:
<Source> indicates the location at which the **Setup** folder is copied onto the local computer.
L <lang ID> indicates the language ID that is passed as a command line argument for the language parameter. The IDs for English and German language are 1033 and 1031 respectively.
For example, **E:\SICAM_PAS_PQS\Setup\Setup.exe /si /L 1031**
The system restarts automatically to complete the installation.
If you want to avoid the restarting of the system, enter **/noreboot** as a command line argument. Restart the system manually to complete the installation.

NOTE

The command line argument **si** is case-sensitive.
SICAM PAS/PQS is localized as per the language ID. If the language parameter is not passed, English is the localized language by default.
If the command is executed with wrong command line arguments, the installer starts in the user-interactive mode.

✧ Verify the installation in the log files generated at:
%programdata%\Siemens\SICAM PAS PQS\Logs\Setup

NOTE

During the installation of SICAM PAS/PQS, if any of the installation prerequisites is not met, the installation is aborted. Also, the prerequisite that was not met is displayed in the log file.

3.2.3 Using a Different User Account in PAS Runtime

If you want to use a different account in PAS runtime instead of **PASRuntimeUser**, proceed as follows on all SICAM PAS/PQS systems:

✧ Add a new account to the **SICAM PAS PQS Users** group.

✧ Log on to the account to access the following services:

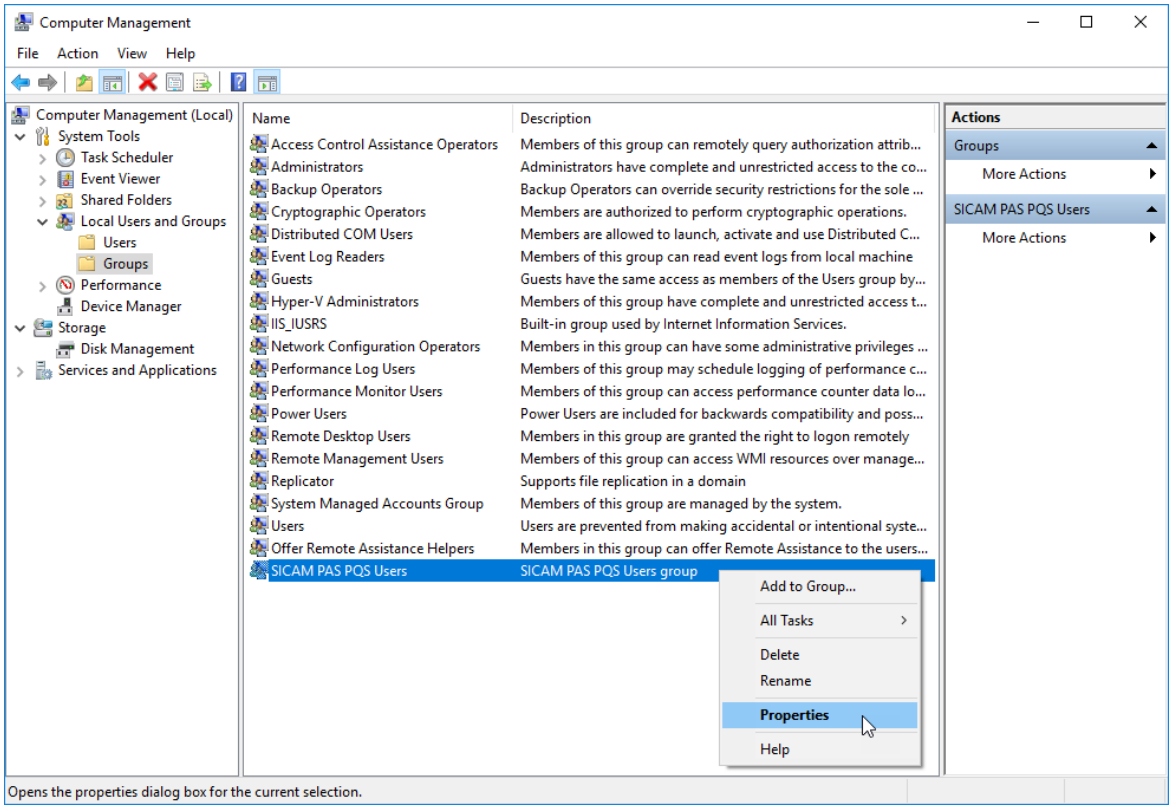
- **Archive Server monitoring service**
- **Defragmentation Agent**
- **PowerCC IPC Daemon**
- **SSR**

To add local users and domain users to the **SICAM PAS PQS Users** group:

✧ Click **Start**, type **Computer Management**, and confirm by pressing <Enter>.

The **Computer Management** window opens.

✧ In the navigation tree, select **Local Users and Groups > Groups**.

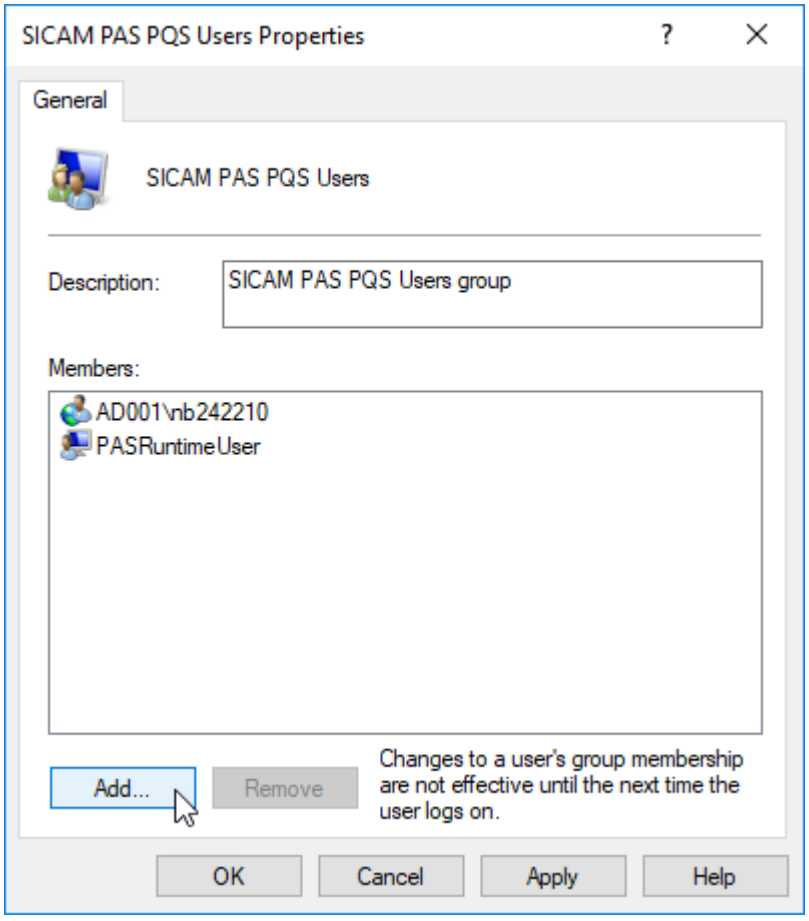


[sc_Computer_Management, 2, en_US]

Figure 3-18 Computer Management

✧ Select **SICAM PAS PQS Users** and select **Add to Group...** from the context menu.

The **SICAM PAS PQS Users Properties** dialog opens.

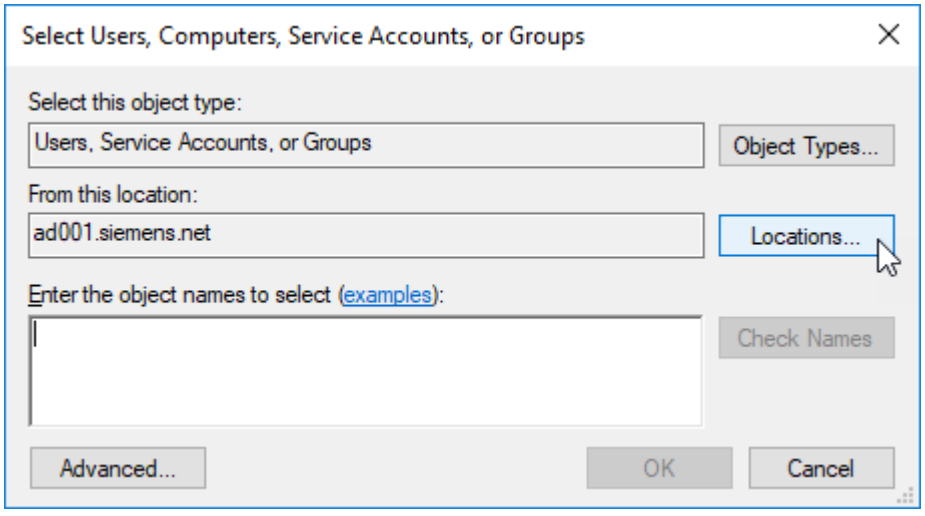


[sc_User_Properties, 2, en_US]

Figure 3-19 SICAM PAS PQS Users Properties

✧ Click **Add...** .

✧ If you use a domain account, click **Locations...** in the **Select Users, Computers, Service Accounts, or Groups** dialog.



[sc_Select_User_Comp_Serv_Acc_Grp, 2, en_US]

Figure 3-20 Selecting an Account

✧ Select the domain and click **OK**.

✧ Enter the account name and click **OK**.

✧ Click **OK** to close the **SICAM PAS PQS Users Properties** dialog.

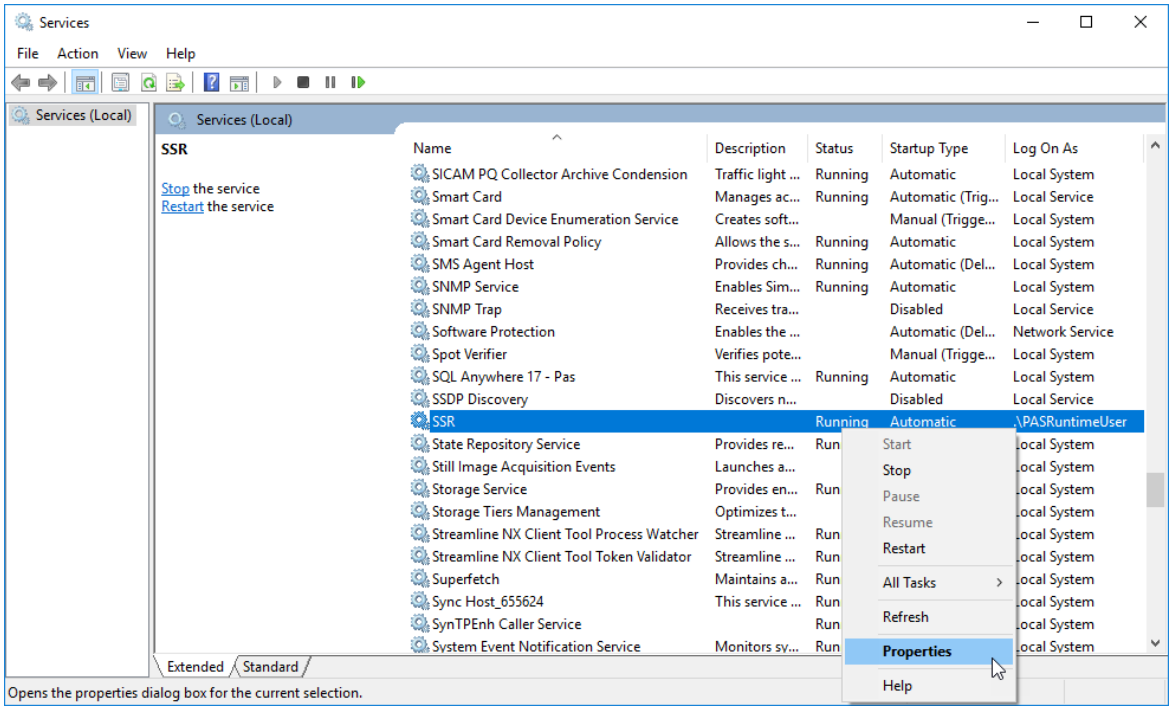
NOTE

If you add a user to the **SICAM PAS PQS Users** group who is already logged on to the system, make sure that the user logs off and logs on again to enable the changes made to user groups.

To logon with a new account to a service, for example **SSR**:

✧ Click **Start**, type **Services**, and confirm by pressing <Enter>.

The **Services** window opens.



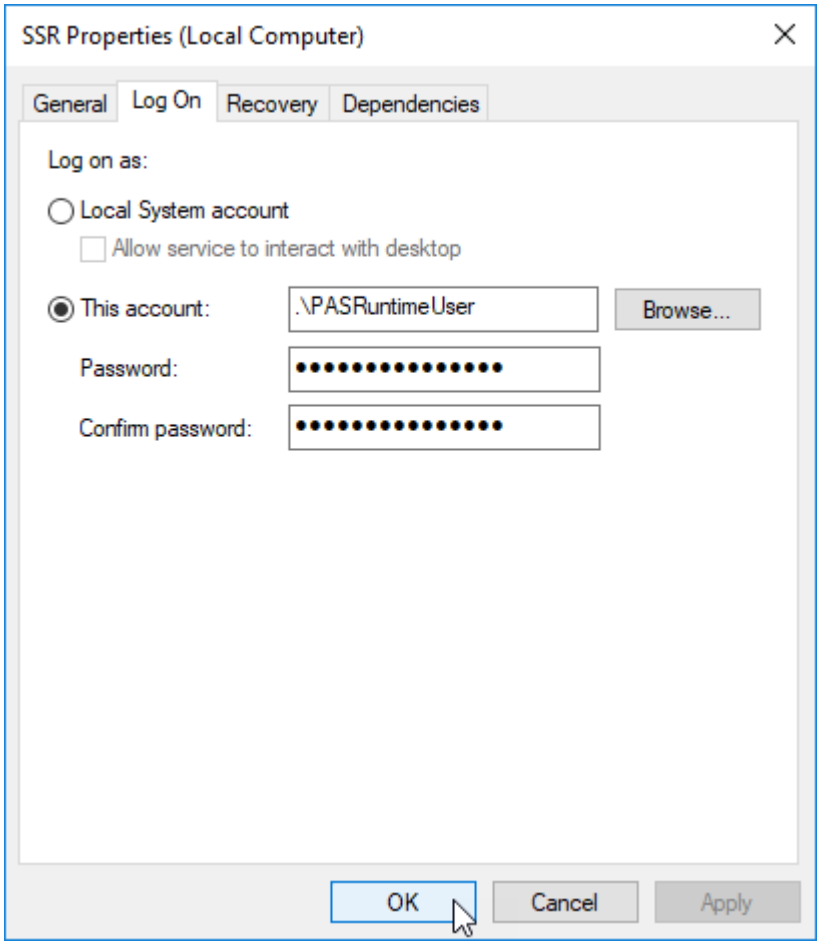
[sc_Services_Properties, 2, en_US]

Figure 3-21 Services Window

✧ Select **SSR** and select **Properties** from the context menu.

The **SSR Properties** dialog opens.

✧ Select the **Log On** tab.



[sc_SSR_Properties, 2, en_US]

Figure 3-22 Log On Tab

- ✧ Activate **This account**.
- ✧ Enter the desired user (assigned to the group **SICAM PAS PQS Users**).
  If you use a domain account, click **Browse...** to open the **Select user** dialog and navigate through **Locations...** to the domain.
- ✧ Enter the corresponding password, confirm it, and click **OK** to close the dialog.
- ✧ Repeat the login procedure for the following services:
  - **Archive Server monitoring service**
  - **Defragmentation Agent**
  - **PowerCC IPC Daemon**
- ✧ Close the **Services** window.

3.2.4 Modifying Login Details in the Application Pools

If a user password is modified from the **Computer Management**, which is used to log on to SICAM PAS/ PQS UI – Operation Client, the password must also be modified in the application pool of the Internet Information Services (IIS).

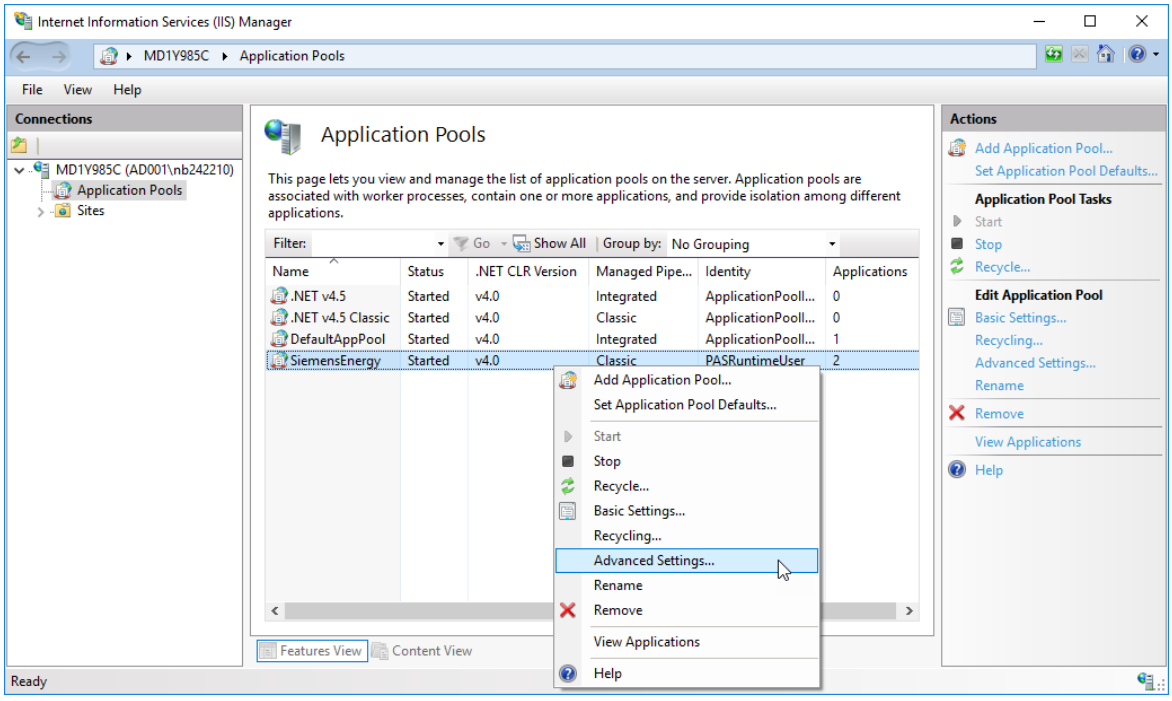
To modify the password in the application pool:

- ✧ Click **Start**, type **IIS**, and confirm by pressing <Enter>.

The **Internet Information Services (IIS) Manager** window opens.

✧ Select the **Application Pools** in the **Connections** section.

The **Application Pools** section is displayed.



[sc_IIS_Manager, 2, en_US]

Figure 3-23 Selecting Application Pools in the Connections Section

✧ Right-click **SiemensEnergy** and select **Advanced Settings...** from the context menu.

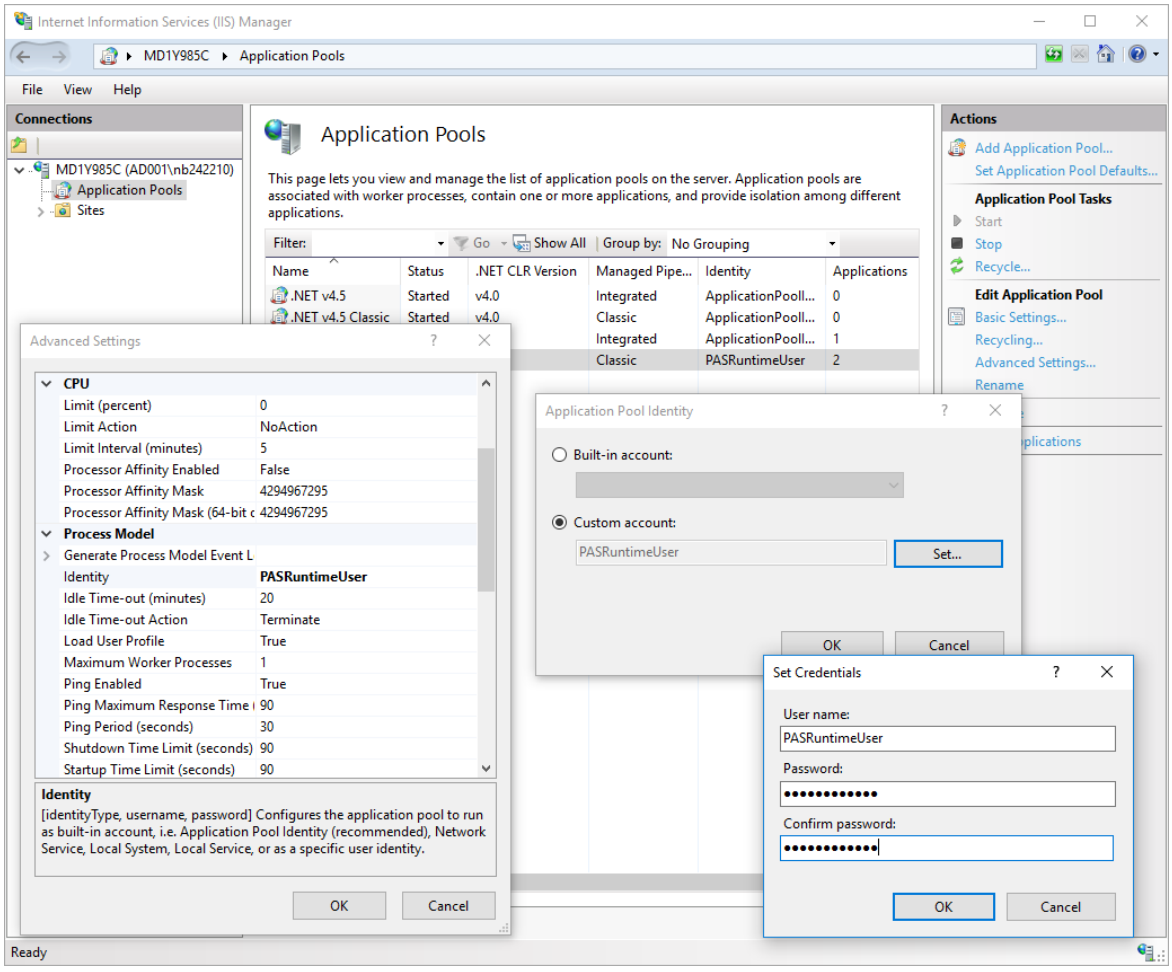
The **Advanced Settings** dialog opens.

✧ Select **Identity** from the **Process Model** section and click **...** .

The **Application Pools Identity** dialog opens.

✧ Select **Custom account** and click on **Set...** .

The **Set Credentials** dialog opens.



[sc_IIS_Maanger_Advanced_Settings, 2, en_US]

Figure 3-24 Setting Credentials

✧ Enter the **User name** and **Password** and click **OK** in all the open dialogs.

The User name and Password is set.

3.2.5 Viewing the Product Information in Micosoft Edge

You can view the **Product version**, **Installed hotfix version**, and **Copyright** product information from the **About** dialog in the **Microsoft Edge** web browser.

To do this, proceed as follows:

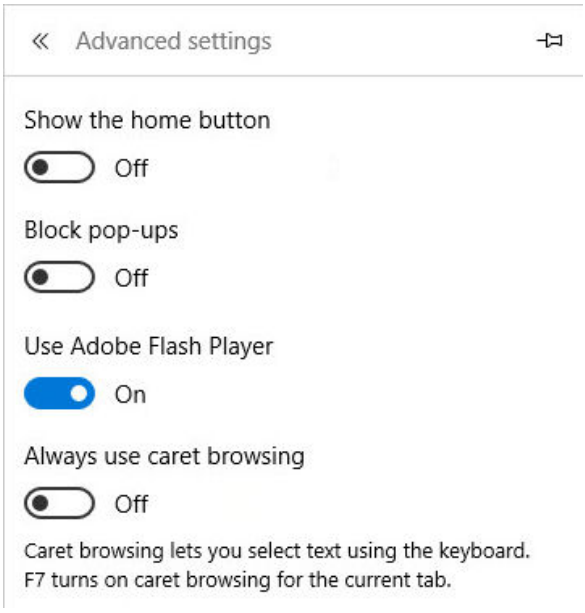
✧ Open SICAM PAS/PQS UI – Operation Client in Microsoft Edge and click the following symbol:

If you are unable to view the product information, change the Microsoft Edge settings as follows:

✧ In Microsoft Edge, click **...** on the top-right corner and select **Settings**.

✧ Click **View advanced settings**.

✧ Disable the **Block pop-ups** option.



[sc_Edge advanced settings, 1, en_US]

Figure 3-25 Microsoft Edge, Advanced Settings

Hiding the Address Bar in the About Dialog

The **About** dialog displays an additional address bar along with the product information.

To hide the address bar, proceed as follows:

✧ Click **Start** > **Control Panel** > **Internet Options**.

The **Internet Properties** dialog opens.

✧ In the **Security** tab, select **Internet** and click **Custom level...** in the **Security level for this zone** section.

The **Security Settings - Internet Zone** dialog opens.

✧ In the **Settings** section below the **Miscellaneous** topic, activate **Allow websites to open windows without address or status bars**.

✧ Click **OK** to apply the selected settings and and exit the dialogs.

The address bar in the **About** dialog is hidden.

3.3 Firewall Configuration

3.3.1 Understanding Windows Firewall

The Windows Firewall blocks attempts to access your system via TCP/IP or UDP/IP in order to protect your system against unauthorized use. The Firewall settings must be customized in order to provide SICAM PAS/PQS components access to the system while the **Firewall is active**.

Configure the Firewall after the installation of SICAM PAS/PQS.

NOTE

If your computers are installed behind a corporate firewall, you are protected against access from outside the company. In this case, you can deactivate the local Windows Firewall, and the Firewall configuration described below is not required.

NOTE

Some firewalls (for example, ZoneAlarm) prevent the establishment of connections from SICAM PAS/PQS components to the database server. Hence, release the connection establishment for the following components in the firewall:

- SICAM PAS/PQS Feature Enabler
- SICAM PAS/PQS UI – Configuration
- SICAM PAS/PQS UI – Operation / SICAM PAS/PQS UI – Operation Client
- SICAM PAS/PQS User Administration
- SICAM PAS/PQS Value Viewer

When are Settings Required?

Settings must be defined for the following system configurations, in case the Windows Firewall has been activated:

- SICAM PAS/PQS has been configured as a distributed system.
- A control center is connected via:
  - IEC 60870-5-104 Slave
  - IEC 61850 Server
  - DNP3 Slave
  - Modbus Slave
- The SNMP Manager component is used.
- A SICAM PAS/PQS computer is used as time server.
- The SoftPLC is used on the DIP.
- An OPC connection via DCOM is used.
- An OPC XML DA Server is used.
- SICAM PAS/PQS is configured redundantly.
- SICAM SCC is configured redundantly.
- SICAM SCC communicates with SICAM PAS/PQS.
- SICAM PAS/PQS communicates with the SICAM PQ Analyzer.

The following tables include a list of the programs/services with the corresponding ports on which you must deactivate the blocking by the Windows Firewall. The **Display name** of the service is shown in bold letters.

The programs/services can be components of:

- SICAM PAS/PQS
- SICAM SCC

The name of the computer on which you must configure the Firewall is indicated in the right-hand table column. Furthermore, the reason for the configuration is indicated in this column.

Additional configuration steps are required for the following system configurations, see *3.3.3 Additional Configurations for SICAM PAS/PQS Components*:

- SICAM PAS/PQS has been configured as a distributed system.
- The SoftPLC is used on the DIP.
- An OPC connection via DCOM is used.

SICAM PAS/PQS

Installation Directory[1]	Program/Service Display Name	Protocol	Port	Computer Remark
%ProgramFiles%\Siemens\Automation License Manager\almapp	almapp64x.exe **Automation License Manager Service**	TCP	4410	SICAM PAS/PQS computer or computer with Collector archive For remote installation of ALM licenses
\bin	btiserver.exe	TCP	10025	All SICAM PAS/PQS computers
\CFE\Bin	CfeDNP30Slave.exe	TCP	20000[2]	Full Server and/or DIP For communication with a control center via DNP3
\CFE\Bin	CfeIEC104Slave.exe	TCP	2404[2]	Full Server and/or DIP For communication with a control center via IEC 60870-5-104
\CFE\Bin	CfeIec61850Server.exe	TCP	102	Full Server and/or DIP For communication with a control center via IEC 61850 and publishing of GOOSE messages
\CFE\Bin	CfeModBusSlave.exe	TCP	502[2]	Full Server and/or DIP For communication with a control center via Modbus
\CFE\Bin	CfeSimeasRDM.exe	Proprietary	2010	Full Server and/or DIP For callback of devices
\CFE\Bin	CfeSnmpClient.exe	UDP	161, 162	On the computer which operates with the SNMP Manager For communication with SNMP Agents (for example, switches, routers, and SIPROTEC EN100)
\CFE\Bin	CfeTestandDiagnosisUI.exe	TCP	10600 to 10650	All SICAM PAS/PQS computers For test and diagnosis purpose
		UDP	11055	
\ASA\win32	dbsrv17.exe **SQL Anywhere 17 - Pas**	TCP	2638	Only Full Server If SICAM PAS/PQS has been configured as a distributed and redundant system
		UDP	2638	
\bin	DsiServer.exe	TCP	10500	Only Full Server
C:\Windows\System32	hasplms.exe **Sentinel LDK License Manager**	TCP	1947	All SICAM PAS/PQS computers For enabling the features (dongle)
C:\Siemens\SySrv\Bin	IpcDaemon.exe **PowerCC IPC Daemon**	TCP	19234	Full Server and/or DIP If SICAM PAS/PQS has been configured as a distributed and redundant system
\PlcUI	LanguageSwitchService.exe **LanguageSwitchService**	TCP	8089	Full Server and/or DIP For switching the SoftPLC program language

1 Default installation directory: **%PASINSTALLPATH**%

2 The predefined ports can be customized.

Installation Directory[1]	Program/Service Display Name	Protocol	Port	Computer Remark
[3]\NTP	ntpdssl-sag.exe **Network Time Protocol**	UDP	123	On the computer which operates as a time server
\bin	OPCServer.exe	TCP	135	Only Full Server For communication with a control center or a third-party device via OPC
\bin	OPCXmlDaServer.exe	TCP	8081	Full Server and/or DIP For communication with a control center or a third-party device via OPC XML DA
\bin	PasCCProxy.exe	TCP	10501[2]	Full Server and/or DIP For communication with SICAM SCC
C:\Siemens\SySrv\Bin	PowerCCSSR2.exe **SSR**	TCP	17824	Full Server and/or DIP If SICAM PAS/PQS has been configured as a distributed and redundant system
		UDP	31365 31366	
\bin	SARAServer.exe **Archive Server monitoring service**	TCP	4845 4846 4847[2]	Computer with archive For communication with SICAM PQ Analyzer, the following ports are defined: • Port 4845 for backup archive • Port 4846 for demo archive • Port 4847 for runtime/collector archive
[3]\SNMP	securesnmpagent.exe **Secure SNMP Agent**	UDP	161	Full Server and/or DIP For Asset Monitoring (SNMP Agent)
\bin	SoftPLC.exe	TCP	21950[2]	Full Server and/or DIP For a redundant SICAM PAS/PQS system
		TCP	23042	Full Server and/or DIP For SoftPLC Runtime Debugger, diagnosis port
NA	NA	HTTPS	443	Add as Inbound Rules in Full Server and/or DIP

1 Default installation directory: **%PASINSTALLPATH**%

3 Installation directory for a 32-bit operating system: **%CommonProgramFiles%\Siemens** – for a 64-bit operating system: **%CommonProgramFiles(x86)%\Siemens**

NOTE

If a predefined port on the SARA server (communication of SICAM PQ Analyzer/SICAM PQ Collector with the archive) must not be opened due to internal IT security policies or is already occupied by another software, for example, SIMATIC NET, change the port on all systems as follows:

In the SICAM PAS/PQS system:

- Open the **%PAS_BIN%** directory.
- Modify the port numbers in the **SARAServer.ini** file.

In the SICAM PQ Analyzer system:

- Open the **%PQA_BIN%** directory.
- Modify the port numbers accordingly in the files:
  - **SARAServer.ini**
  - **SARADataProviderConfiguration.ini**
  - **Siemens.Energy.PowerQuality.Analyzer.UI.Business.SARAClient.dll.config**

A subsequent installation overwrites the updated port number with the default value and you must re-enter the changed port number in the specified files.

If more than one network card is available on the SICAM PAS/PQS system, replace the **[NodeName]** string with either the hostname or the IP address in the **SARAServer.ini** file for the following line:

Url=opc.tcp://[NodeName]:4847/SARAServer

SICAM SCC

Installation Directory [4]	Program/Service	Protocol	Port	Computer Remark
\bin	Synchtool.exe	TCP	51119 [5]	For all SIMATIC WinCC Server computers For a redundant SICAM SCC

3.3.2 Configuring the Windows Firewall

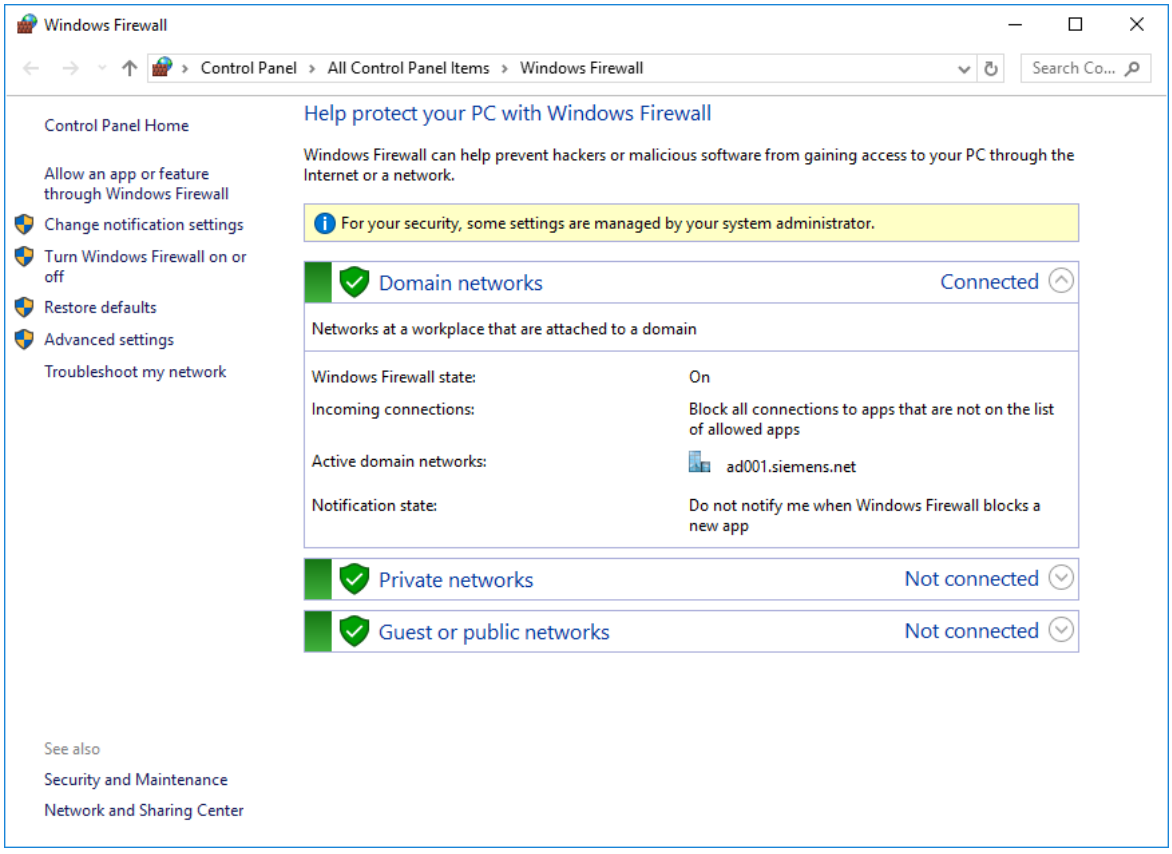
This chapter describes how to configure Windows Firewall in Windows 10.

To configure the Windows Firewall:

✧ Click **Start**, type **Windows Firewall**, and confirm by pressing <Enter>.

4 Default installation directory: **%PASINSTALLPATH**%

5 The predefined ports can be customized.



[sc_Windows_Firewall, 3, en_US]

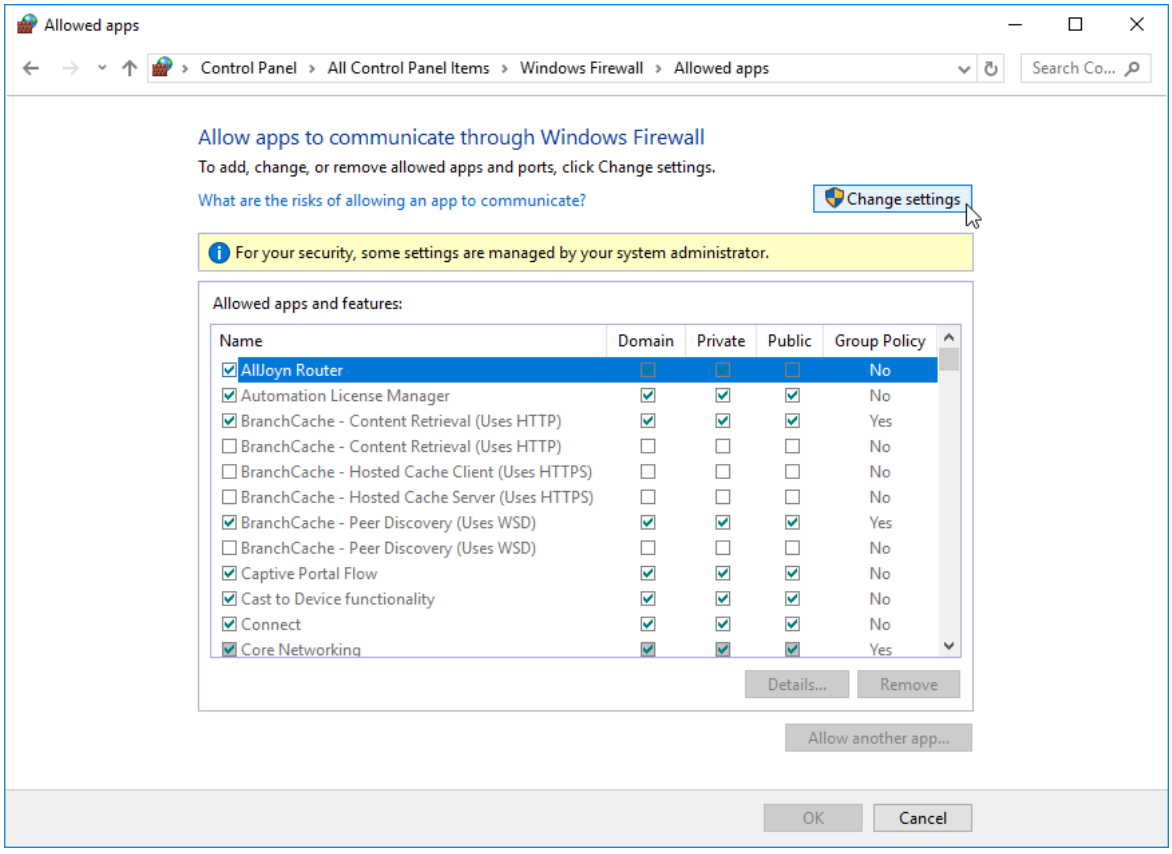
Figure 3-26 Windows Firewall Window

Allowing an App or a Service

To deactivate the blocking function for a program or a service:

✧ Select **Allow an app or feature through Windows Firewall** from the left section.

The **Allowed apps** window opens.



[sc_Allowed_Programs, 3, en_US]

Figure 3-27 Allowed Programs

✧ To be able to change the configured settings, click **Change settings**.

✧ Click **Allow another app...** .

The **Add an app** dialog opens.

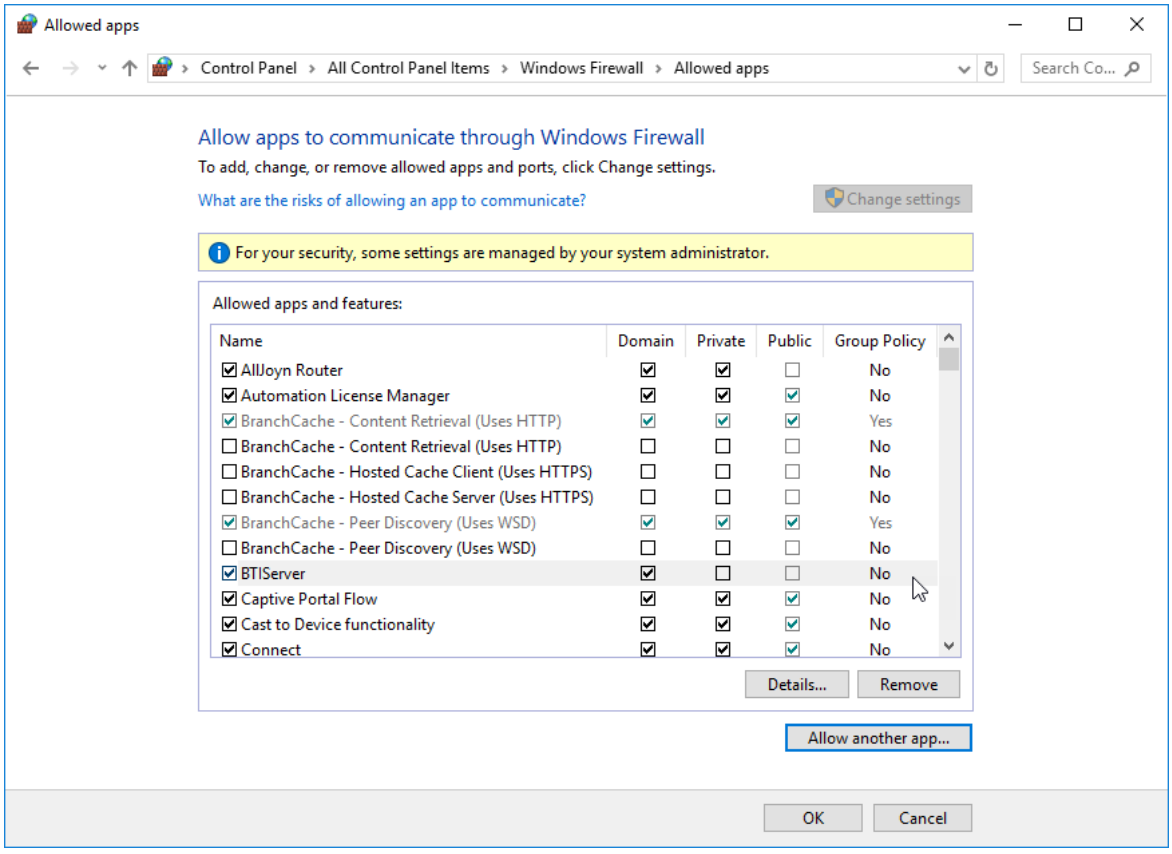
✧ Click **Browse...** .

The **Browse** dialog opens.

✧ Select, for example, the **btiserver.exe** file from the **%PAS_BIN%** directory and click **Open** to confirm.

✧ Click **Add** to close the **Add an app** dialog and to return to the **Allowed apps** window.

The **btiserver.exe** program is inserted and activated.



{sc_Allowed_Programs_BTIServer, 3, en_US}

Figure 3-28 Windows Firewall Window with BTIServer Allowed

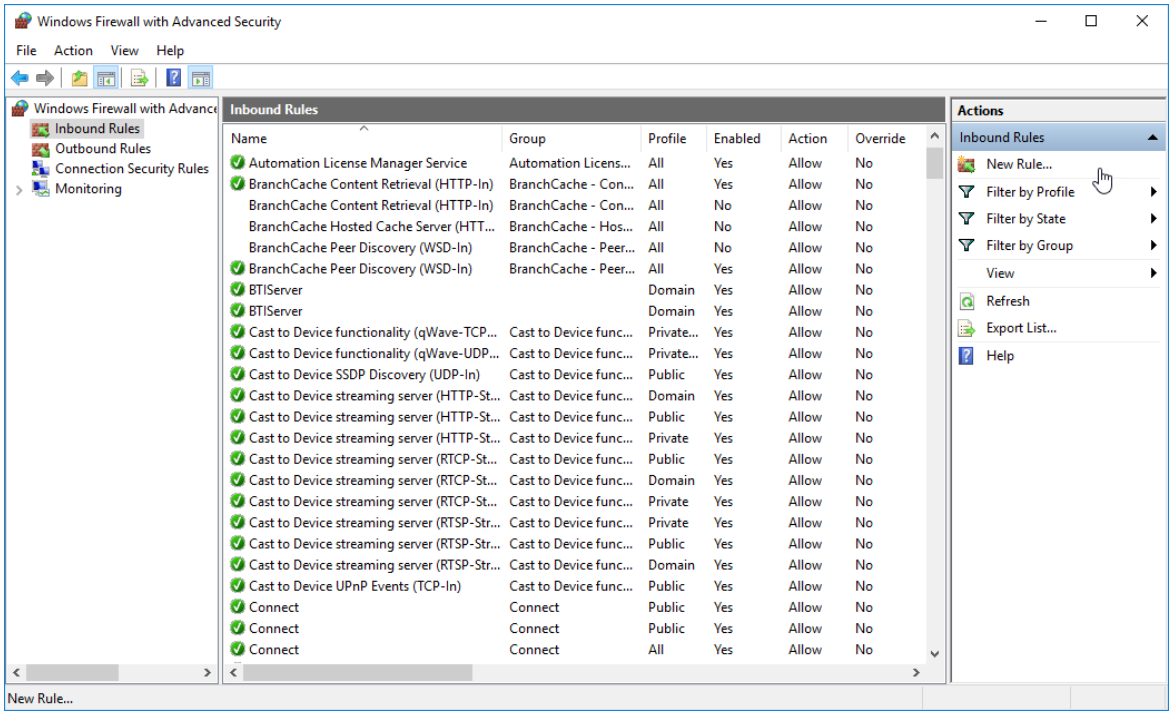
✧ Click **OK** to return to the **Windows Firewall** window.

Opening a Port

To deactivate the blocking of a port:

✧ Select **Advanced settings** from the left section of the **Windows Firewall** window.

The **Windows Firewall with Advanced Security** window opens.

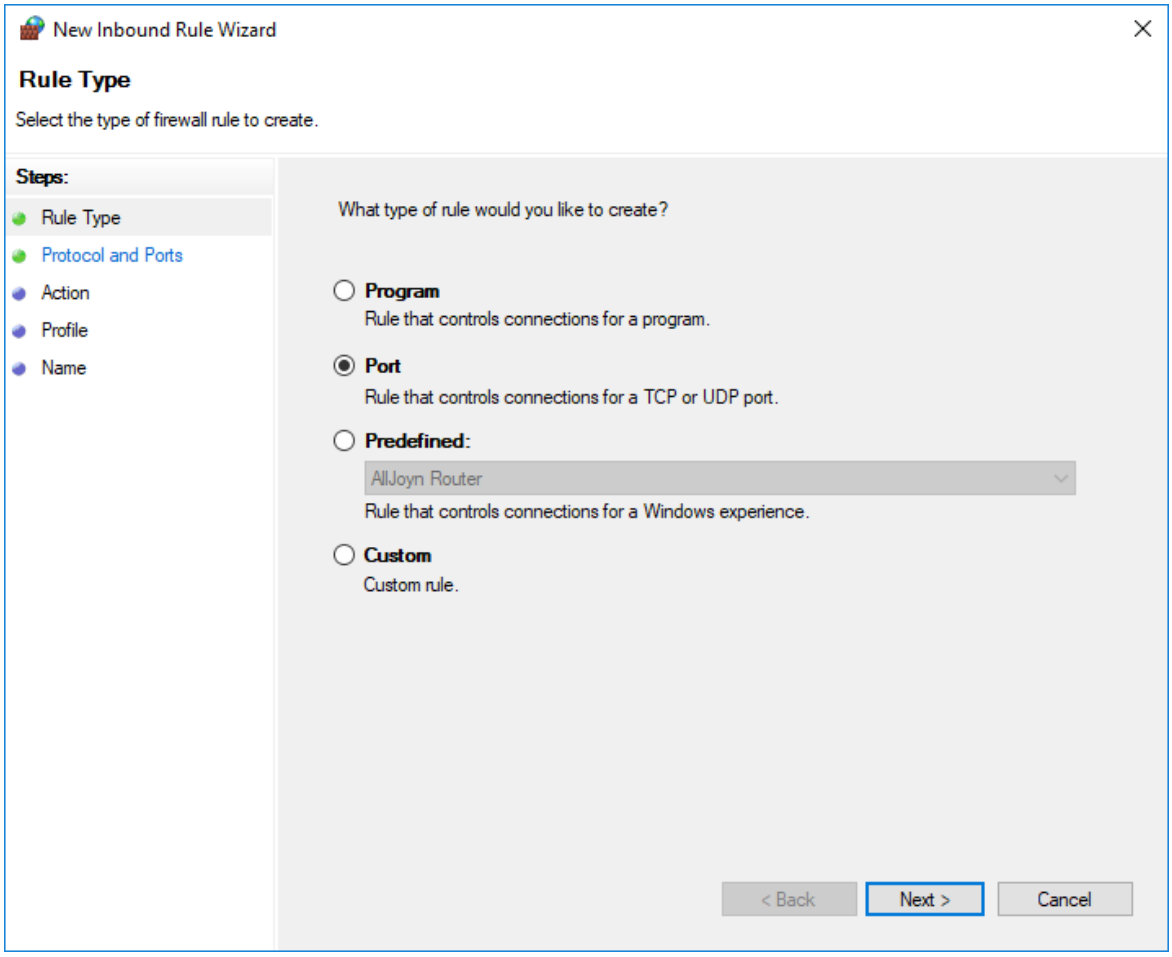


{sc_WindowsFirewall_Adv_Sec, 3, en_US}

Figure 3-29 Windows Firewall with Advanced Security Window

✧ Select **Inbound Rules** from the left section and click **New Rule...** from the **Actions** section.

The **New Inbound Rule Wizard** dialog opens.



[sc_New_Inbound_Rule, 3, en_US]

Figure 3-30 Configuring a Port

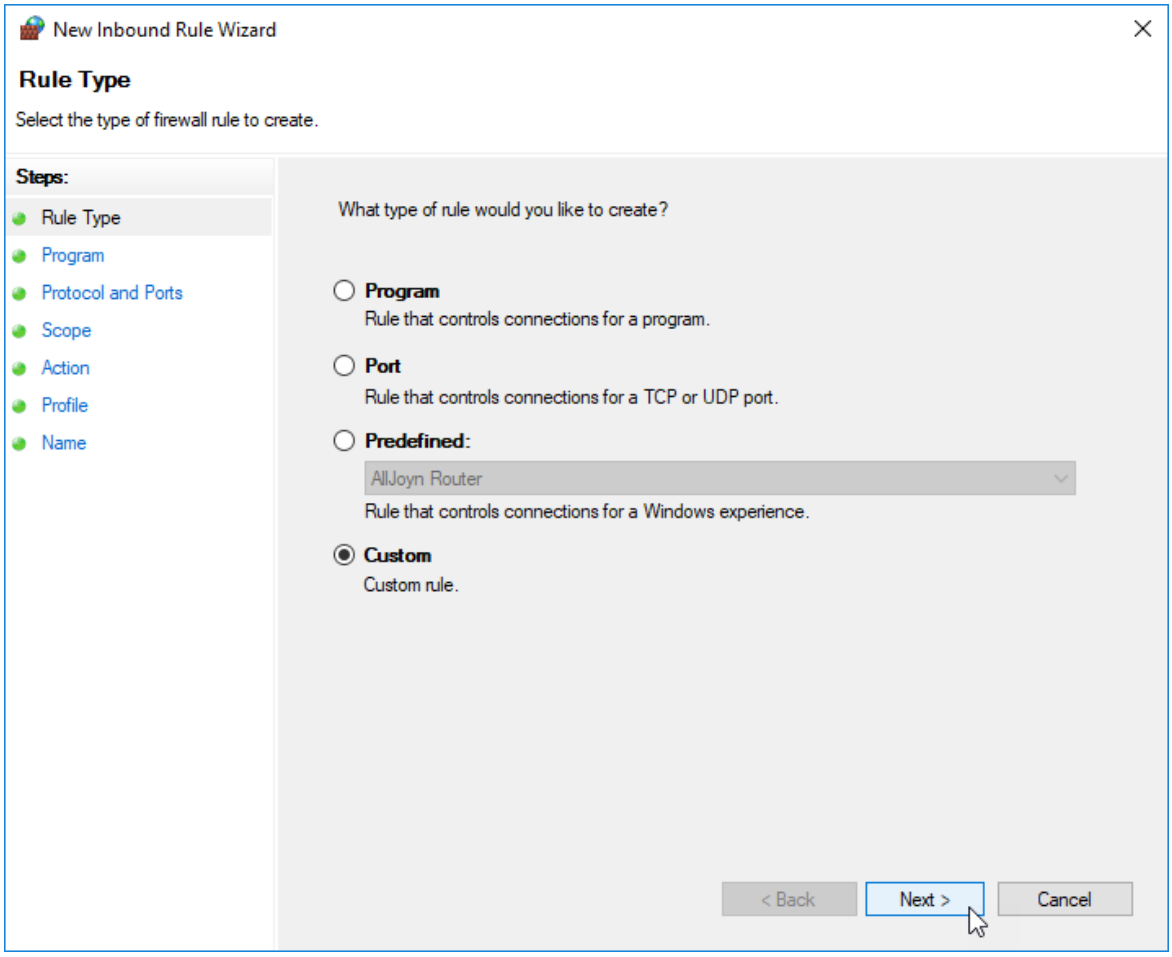
- ✧ In the **Rule Type** step, select **Port** and click **Next >** .
- ✧ Configure the port as required.
- ✧ Click **Finish**.

The blocking of the port has been deactivated.

Opening a Port for Specific IP Addresses

To deactivate the blocking of a port for specific IP addresses:

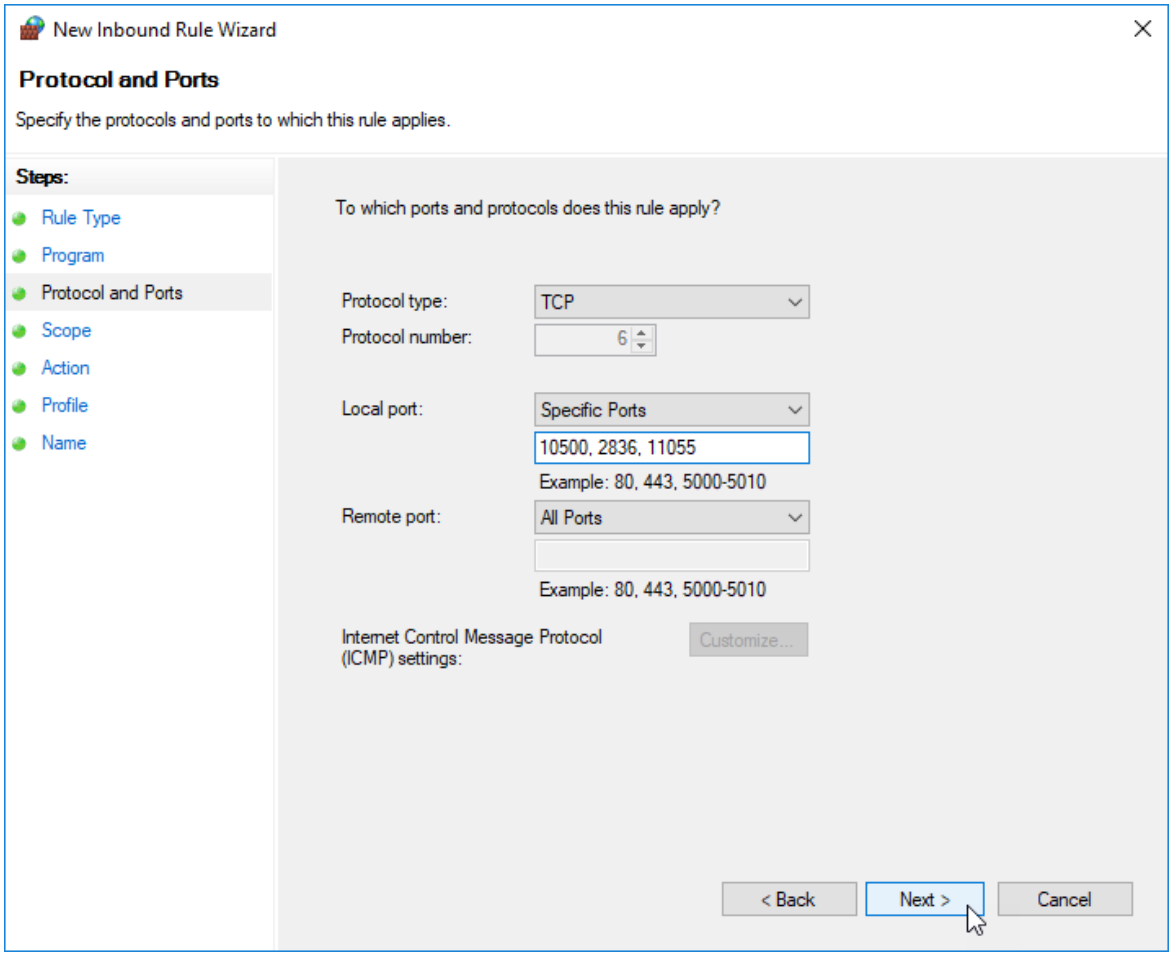
- ✧ In the **Windows Firewall with Advanced Security** window, open the **New Inbound Rule Wizard** dialog via **New Rule...**.
  If you additionally define **Outbound Rules**, use the same settings for ports and IP addresses.



[sc_Inbound_rules_rule_type_custom, 2, en_US]

Figure 3-31 Inbound Rule – Custom Rule Type

- ✧ In the **Rule Type** step, select **Custom** and click **Next >** .
- ✧ In the **Program** step, select **All program** and click **Next >** .
- ✧ In the **Protocol and Ports** step, specify the ports which you want to enable.

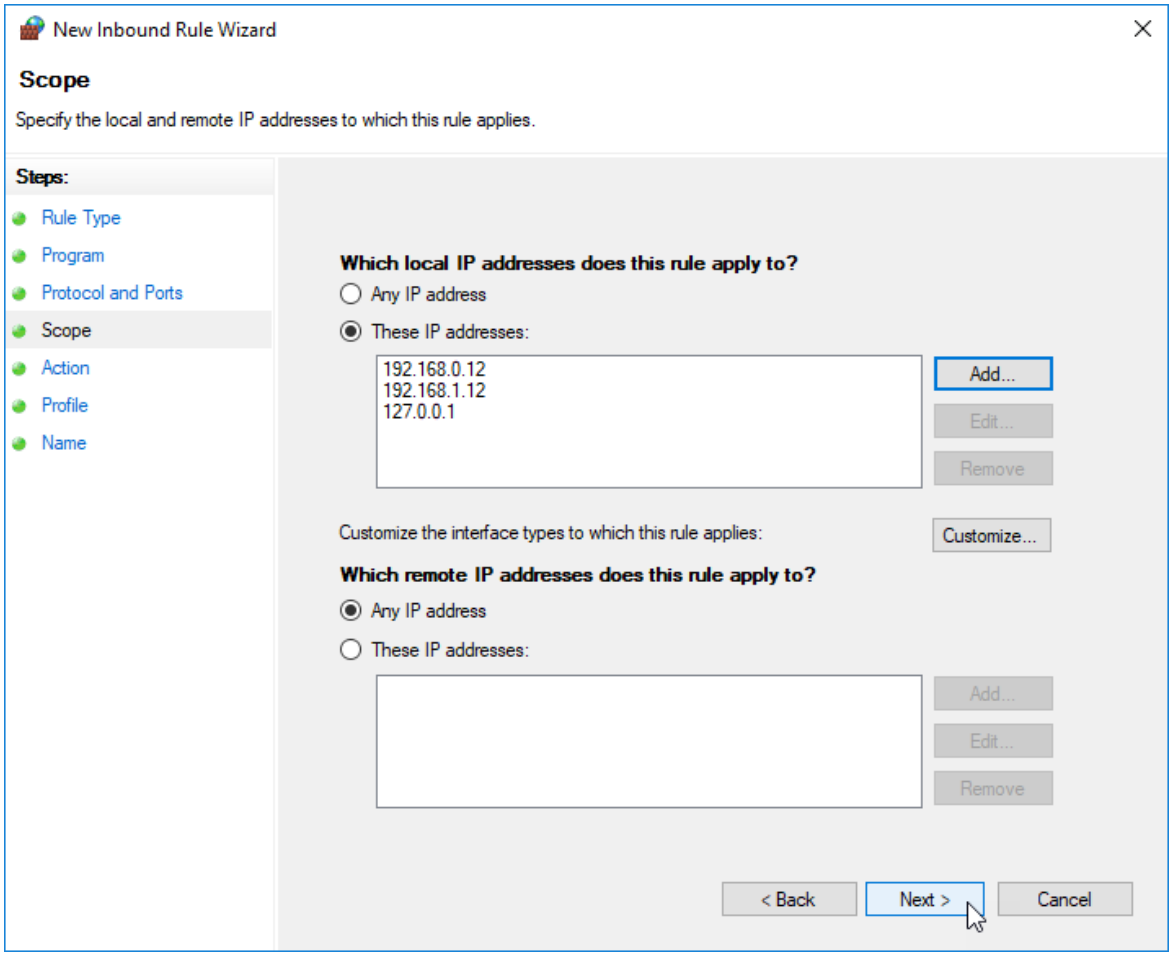


[sc_Inbound_rules_protocol_ports, 2, en_US]

Figure 3-32 Inbound Rule – Defining Protocol Type and Ports

✧ Click **Next >** .

✧ In the **Scope** step, you specify the IP addresses. If you configure the IP addresses for the local IP addresses, you additionally have to add the **127.0.0.1** IP address.



[sc_Inbound_rule_scope, 2, en_US]

Figure 3-33 Inbound Rule – Defining the IP Address Scope

- ✧ Click **Next >**.
- ✧ In the **Action** and **Profile** steps, adopt the default settings.
- ✧ In the **Name** step, enter a corresponding rule name and click **Finish**.

The blocking of the port for specific IP addresses has been deactivated.

3.3.3 Additional Configurations for SICAM PAS/PQS Components

This chapter describes the additional configurations which are only required for certain system configurations.

SICAM PAS/PQS as a Distributed System

To restart the Full Server from the DIP, the following configuration is required in the Windows Firewall:

- ✧ On the computer on which the Full Server has been installed, define the **File and Printer Sharing** function as an exception.

DIP with Automation (SoftPLC)

- ✧ In the **Windows Firewall** window, click **Advanced settings** from the left section.

The **Windows Firewall with Advanced Security** window opens.

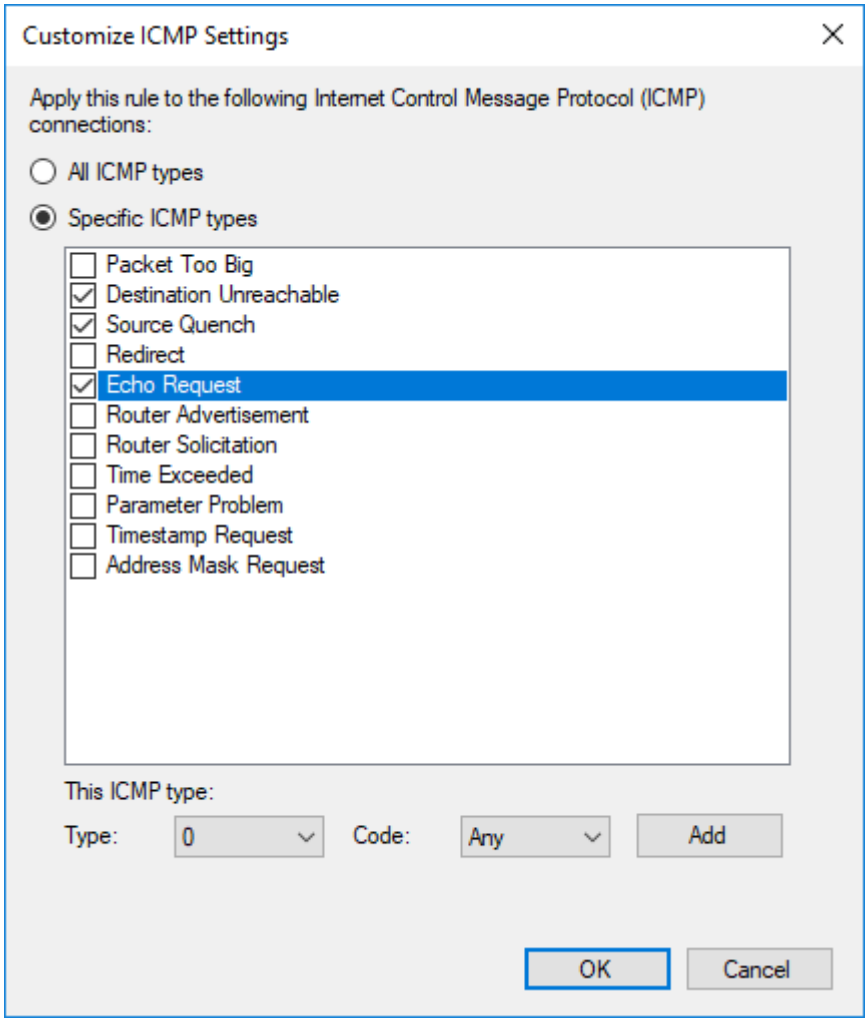
- ✧ Select **Inbound Rules** from the left section and click **New Rule...** from the **Actions** section.

The **New Inbound Rule Wizard** dialog opens.

- ✧ In the **Rule Type** step, select **Custom** and click **Next >**.
- ✧ In the **Programs** step, select **All programs** and select **Next >**.
- ✧ In the **Protocol and Ports** step, select **ICMPv4 i**n the **Protocol type** field and click **Customize...** .

The **Customize ICMP Settings** dialog opens.

- ✧ Select **Specific ICMP types** and enable the options as shown in the below figure.



[sc_Customize_ICMP_Settings, 2, en_US]

Figure 3-34 Customizing ICMP Settings

- ✧ Click **OK** to close the dialog.
- ✧ Configure the protocol as required.
- ✧ Click **Finish**.

The Windows Firewall configuration is complete.

OPC Connection via DCOM

- ✧ In the Windows Firewall, add the **OPCEnum.exe** program to the exceptions and activate it.

The **OPCEnum.exe** file is located in the **%windir%\SysWOW64** directory.
Additionally, you must configure access and start rights for DCOM, refer to *6.1.1 Starting the DCOM Configuration*.

3.4 Services Used

SICAM Services

The following table shows the services which are installed and used by SICAM PAS/PQS and SICAM PQ Analyzer.

Display Name	Required by	Installed by	Purpose
Archive Server monitoring service	SICAM PQ Analyzer	SICAM PAS/PQS SICAM PQ Analyzer	Ensures that the archive server of SICAM PAS/PQS or SICAM PQ Analyzer is running
Archive Server User Management service	SICAM PQ Analyzer	SICAM PAS/PQS SICAM PQ Analyzer	Provides user roles for SICAM PQ Analyzer and Collector application
Automation License Manager Service	SICAM PAS/PQS SICAM PQ Analyzer	SICAM PAS/PQS SICAM PQ Analyzer	Activates the licenses
Defragmentation Agent	SICAM PAS/PQS SICAM PQ Analyzer	SICAM PAS/PQS SICAM PQ Analyzer	For archive management
LanguageSwitchService	SICAM PAS/PQS	SICAM PAS/PQS	For switching the SoftPLC program language
Network Time Protocol	SICAM PAS/PQS	SICAM PAS/PQS	For time synchronization
PowerCC Application Dispatcher Service	SICAM PAS/PQS	SICAM PAS/PQS	Used by SICAM PAS/PQS runtime services
PowerCC IPC Daemon	SICAM PAS/PQS	SICAM PAS/PQS	For inter-process communication of the SICAM PAS/PQS services
Secure SNMP Agent	SICAM PAS/PQS	SICAM PAS/PQS	Provides the asset information and security notifications of SICAM PAS/PQS product via SNMP
Sentinel LDK License Manager	SICAM PAS/PQS	SICAM PAS/PQS	Enables the features (dongle)
SICAM Fault Event Manager	SICAM PAS/PQS SICAM PQ Analyzer	SICAM PAS/PQS SICAM PQ Analyzer	Manages the fault events in SICAM PAS/PQS or SICAM PQ Analyzer
SICAM PAS PQS Group Management	SICAM PAS/PQS	SICAM PAS/PQS	Manages the nested users pertaining to SICAM PAS/PQS users group. For example, you can create nested groups like switch operator, system engineer, guest, and so on.
SICAM PAS PQS Watchdog	SICAM PAS/PQS	SICAM PAS/PQS	Manages the memory of the SICAM PAS/PQS applications
SICAM PQ Collector Archive Condension	SICAM PQ Analyzer	SICAM PQ Analyzer	Condenses the traffic light of the Collector archive
SQL Anywhere 17 - Pas	SICAM PAS/PQS	SICAM PAS/PQS	Manages the SICAM PAS/PQS database
SSR	SICAM PAS/PQS	SICAM PAS/PQS	Start stop recovery service

NOTE

Be aware of the following while using **SICAMPASPQSGroupManagement** service:

- Login to the redundant system before **Update System with database copy** is performed from the main system
- Do not kill the service explicitly for any reason
- Do not manually stop or restart the **SICAMPASPQSGroupManagement** service
- If the system is in a workgroup, the service is not required, hence it will not start

Windows Services

The following services are provided by the operating system and used by SICAM PAS/PQS. Only services that can be started/stopped are listed.

Display Name	Required by	Purpose
SNMP Services	SICAM PQS	For monitoring the archive, refer to */4/ SICAM PAS/ PQS, Configuration and Operation*, chapter 5.
Workstation	SICAM PAS/PQS	Dependent Windows service for SSR
Network Store Interface Service	SICAM PAS/PQS	Dependent Windows service for SSR
IIS Admin Service	SICAM PAS/PQS	For SICAM PAS/PQS UI – Operation Client

4 Uninstalling SICAM PAS/PQS

4.1 Prerequisites

- Prior to uninstallation, create a backup copy of the SICAM PAS/PQS database.
- Always uninstall SICAM PAS/PQS using the Windows uninstallation routine and read the following instructions carefully. This prevents damage to the Windows Registry and unpredicatable problems in the operating system.
- Close all SICAM PAS/PQS components before uninstalling SICAM PAS/PQS.

4.2 Uninstallation

You can uninstall the SICAM PAS/PQS using either via the software management function of your operating system or via silent uninstallation.

Uninstallation via the Software Management Function

To uninstall the SICAM PAS/PQS via the software management functions:

✧ Click **Start**, type **Control Panel**, and confirm by pressing <Enter>.

✧ Click **Programs and Features**.

The **Programs and Features** window opens.

✧ From the list, right-click **Siemens SICAM PAS V8.xx** and select **Uninstall/Change** from the context menu.

This starts the uninstallation process.

✧ Follow the instruction of the uninstaller.

✧ After the uninstallation, restart your computer.

The uninstallation of SICAM PAS/PQS is now complete.

NOTE

The following software components are not uninstalled during the uninstallation of SICAM PAS/PQS and must be uninstalled separately:

- SICAM Q80 Shared Components
- Sentinel System Driver Installer
- OPC basic components
- ALM
- Microsoft Primary Interoperability Assemblies 2005
- Microsoft Visual C++ 2005 Redistributable
- Microsoft Visual C++ 2008 Redistributable
- Microsoft Visual C++ 2010 Redistributable
- Microsoft Visual C++ 2015 Redistributable
- Microsoft Visual C++ 2017 Redistributable
- WinPcap 4.1.3

NOTE

If you want to install a previous version of SICAM PAS/PQS with a new password for the **PASRuntimeUser** user, you must manually delete the **PASRuntimeUser** user and the **SICAM PAS PQS Users** user group via **Start > Control Panel > Administrative Tools > Computer Management > Local Users and Groups** before installation.

Silent Uninstallation

To uninstall the SICAM PAS/PQS via command prompt:

- ✧ Open the **Command Prompt** with administrator rights.
- ✧ Copy the **Setup** folder from the DVD to a preferred location onto your local computer.
- ✧ Execute the **Setup.exe** by using either of the following commands:
  <Source>\Setup.exe /sx or **<Source>\Setup.exe -sx**
  where: **<Source>** indicates the location at which the **Setup** folder is copied onto the local computer.
  For example, **E:\SICAM_PAS_PQS\Setup\Setup.exe /sx**.
  The system restarts automatically to complete the uninstallation.
  If you want to avoid the restarting of the system, enter **/noreboot** as a command line argument. Restart the system manually to complete the uninstallation.

NOTE

The command line argument **sx** is case-sensitive.
Uninstallation via command prompt is executed only if the same installation build is used that was used during the installation.
If the command is executed with wrong command line arguments, the installer starts in the user-interactive mode.

5 Licensing

5.1 Introduction

SICAM PQS is designed as an open and modular system whose components can be individually selected. Using the Automation License Manager (**ALM**), you can enable all the functions (features), which you require on your computer.

The different communication protocols, SICAM PQS UI – Configuration, and the Power Quality (PQ) functions are referred to as functions (features).

In addition, the **ALM** assists you in enabling functional upgrades.

The SICAM PQ Analyzer and the SICAM PQ Collector are activated through the **ALM**.

NOTE

For more information on upgrading protocol licenses, Dongle and Soft License users refer to *A.8 Licensing - General Information* and *A.18 Importing the License File*.

5.2 Using Online Software Delivery (OSD) to License a SICAM PAS/PQS System, V8.17 and Later

Installation for Download via OSD

Proceed as follows for installation:

- Open the **Online Software Delivery** (OSD: *https://www.automation.siemens.com/swdl/Login?lang=de*) in your Web browser.
- Log on with your login and your personal password.
  You can find your credentials in the download-notification e-mail.
- Confirm the delivery address and the export control clause.
  You are now logged on to the Online Software Delivery (OSD) and have access to all your data.
- Open the **Product Download** tab.
- Click **Certificate**.
  The certificate will be opened in your standard PDF viewer.
- Save the certificate for your personal documents.
- Open the **Product Download** tab again.
- Click **Download**.
  Confirm the product disclaimer if prompted.
- Download the ZIP file.
- Unpack the ZIP file to any folder.
- Double-click **SETUP.EXE**.
  The installation will be started.

Guided Installation

From now on, you are guided through the installation.

- Follow all further instructions of the installer.
- Restart your computer after the installation.

Authorization/Software Copy Protection

To execute the licensing procedure for **Download via OSD**:

- Ensure you are still logged on to OSD.
- Start the **Automation License Manager**.
- Select **Web License Key Download**.
- Transfer the license by dragging and dropping the **Transfer licenses** button into the navigation bar of the ALM.
  The license key is now on your local drive.

NOTICE

The **C:\AX NF ZZ**[6] folder contains hidden files. These files and the folder must neither be deleted, moved nor copied. They contain data which are necessary for the licensing of your software. If you do not observe these rules, the license may be irretrievably lost.

There is a risk of transferring a virus from the hard disk to a USB medium. You should therefore run a virus check on your PG/PC each time you install/remove a license.

In order to exclude the risk of an irretrievable loss of your license, observe the following rules:

- ✧ If you use an optimization routine (for example, Scandisk/Defrag) that can move fix memory blocks, only use this option once you have transferred the licenses from the hard disk to another partition/ drive/USB medium.
- ✧ When you install a license, a cluster which is marked as " defective " appears on the destination drive. Do not attempt to restore the defective cluster.
- ✧ Do not forget to uninstall the licenses before formatting, compressing or restoring your hard-disk drive or before installing a new operating system.
- ✧ If a back-up copy of your hard disk contains copies of licenses, these copies could possibly overwrite and destroy the valid installed licenses when you restore your back-up data on the hard disk. In order to prevent a valid license from being overwritten by a back-up copy, you are strongly recommended to either remove all licenses before making a back-up copy or to exclude the **C:\AX NF ZZ** folder from the back-up.

NOTE

You can transport the licenses via a USB medium or a network. For more detailed information, refer to the documentation of the **Automation License Manager**.

5.3 Connecting the DIP to the Full Server

In a distributed system you must connect a DIP to the Full Server. As a prerequisite, a network connection must have been set up to the Full Server and the Full Server must run.

To connect the DIP to the Full Server:

- ✧ Start the **ALM** on the DIP.
- ✧ Enter the **Computer name** and the **IP address** of the computer on which the Full Server to be connected to the DIP is running.
- ✧ Click **OK**.

6 Drive letter depends on drive where license is available.

6 OPC

The **OPC Server**, **OPC Client**, and the **OPC XML DA Server** functions (features) must be configured in addition to installation.

6.1 Setting up the OPC Server

To use the **OPC Server** function, set up **DCOM** (Distributed Component Object Model) and make sure that **SSR** is set as a Windows service with the desired user.
For more information on SSR, see *3.2.3 Using a Different User Account in PAS Runtime*.

6.1.1 Starting the DCOM Configuration

To perform the DCOM configuration, use the **dcomcnfg.exe** Microsoft tool.

NOTE

The **PASRuntimeUser** is used as a default user account while configuring DCOM in the following steps.

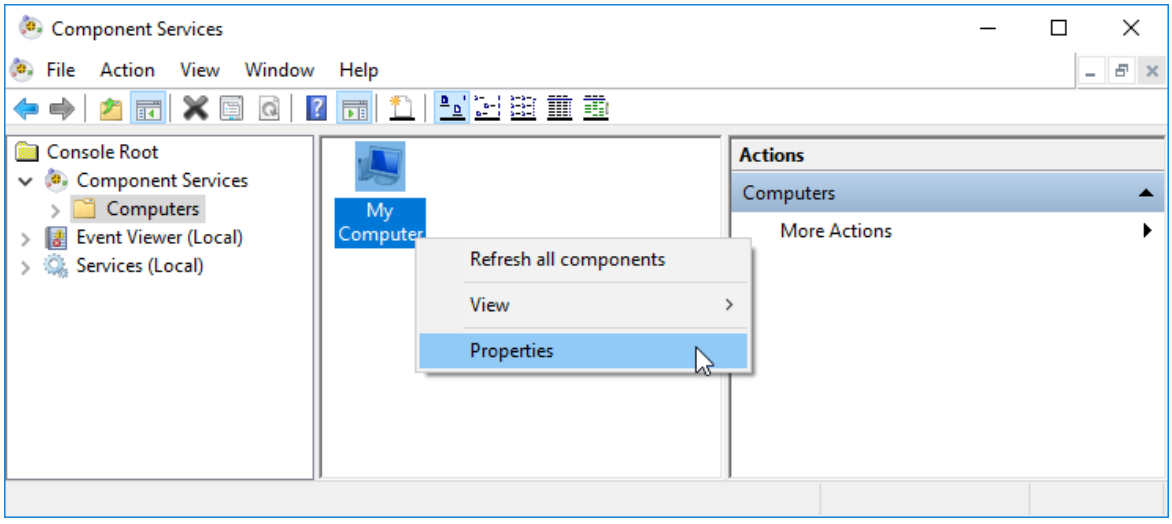
NOTE

In some cases you may have to reconfigure DCOM after a Windows update.

To configure DCOM:

✧ Click **Start**, type **dcomcnfg** and confirm by pressing <Enter>.

The **Component Services** window opens.

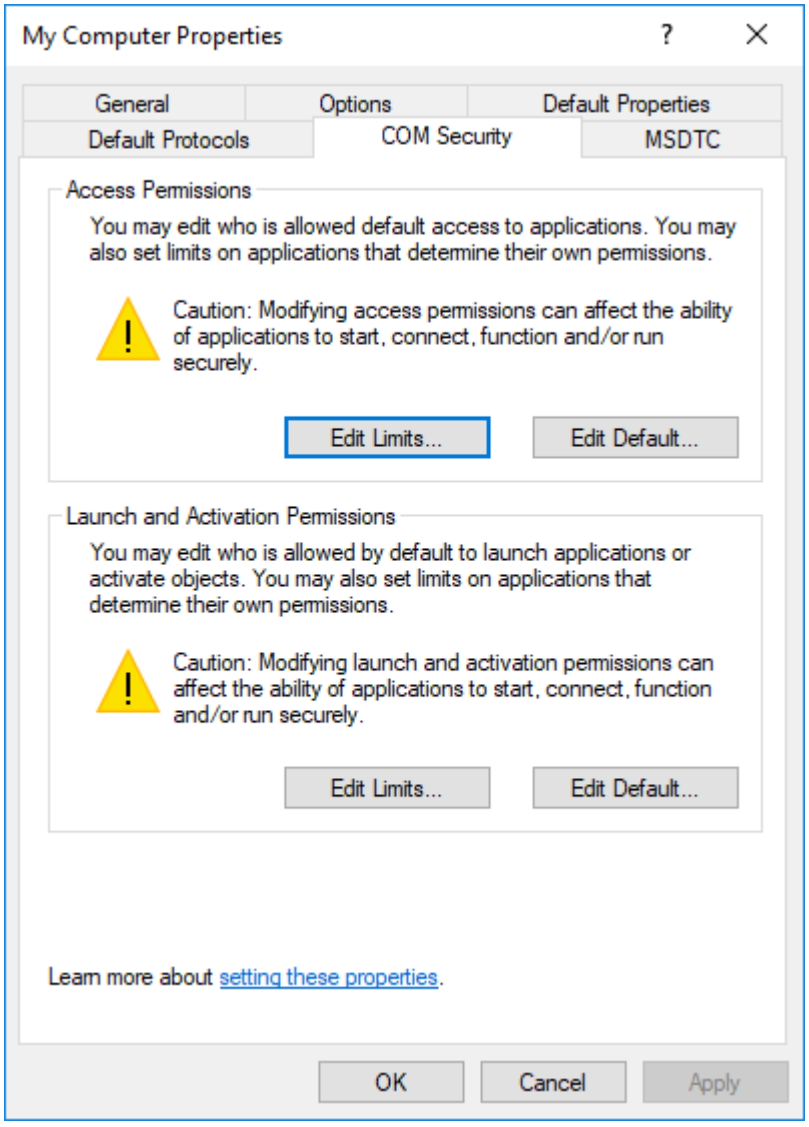


[sc_Component_Services, 2, en_US]

Figure 6-1 Component Services Window

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

The **My Computer Properties** dialog opens.



[sc_MyComputer_Properties, 2, en_US]

Figure 6-2 My Computer Properties Dialog

6.1.2 Configuring My Computer

In the **My Computer Properties** dialog, perform the following steps:

- *6.1.2.1 Granting Permissions for Everyone – Edit Limits*
- *6.1.2.2 Granting Access Permissions – Edit Default*
- *6.1.2.3 Granting Launch and Activation Permissions – Edit Default*
- *6.1.2.4 Configuring Default Properties*

6.1.2.1 Granting Permissions for Everyone – Edit Limits

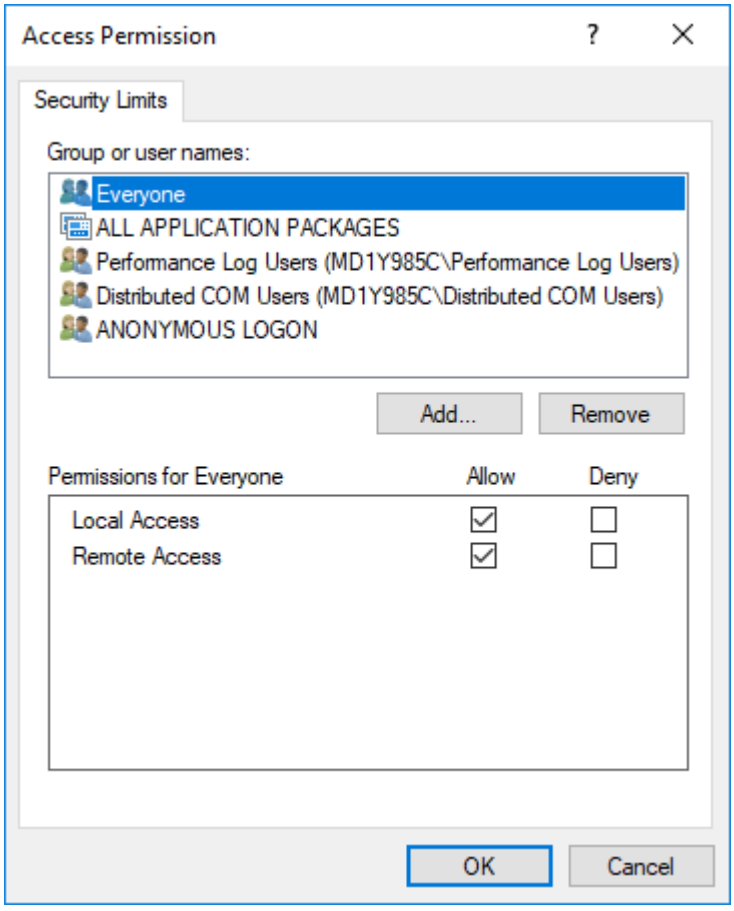
You must configure access, launch, and activation rights for DCOM, because the default settings would block any communication within the network.

To do this, proceed as follows:

✧ Select the **COM Security** tab.

✧ Under **Access Permissions**, click **Edit Limits...**.

The **Access Permission** dialog opens.

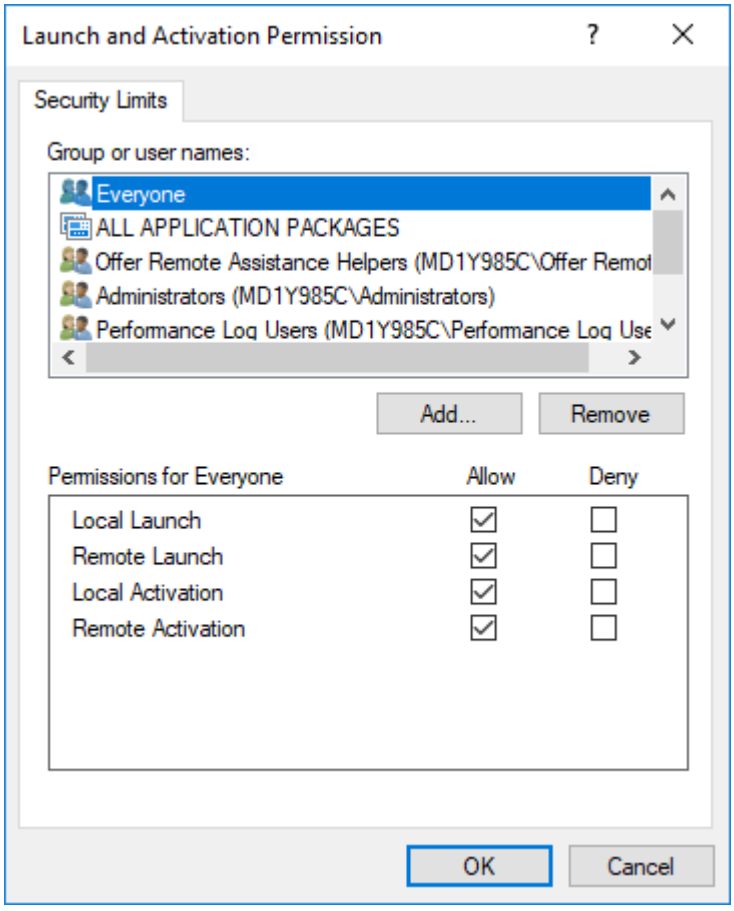


[sc_Access_Perm_Edit_Limits, 1, en_US]

Figure 6-3 Access Permission Dialog

- ✧ For **Everyone**, select **Allow** for the **Local Access** and **Remote Access** check boxes.
- ✧ For the **Distributed COM Users** and the **ANONYMOUS LOGON**, select the same permissions.
- ✧ Click **OK** to confirm.
- ✧ Under **Launch and Activation Permissions**, click **Edit Limits...** .

The **Launch and Activation Permission** dialog opens.



[sc_Launch_and_Activation_Perm_Edit_Limits, 1, en_US]

Figure 6-4 Launch and Activation Permission Dialog

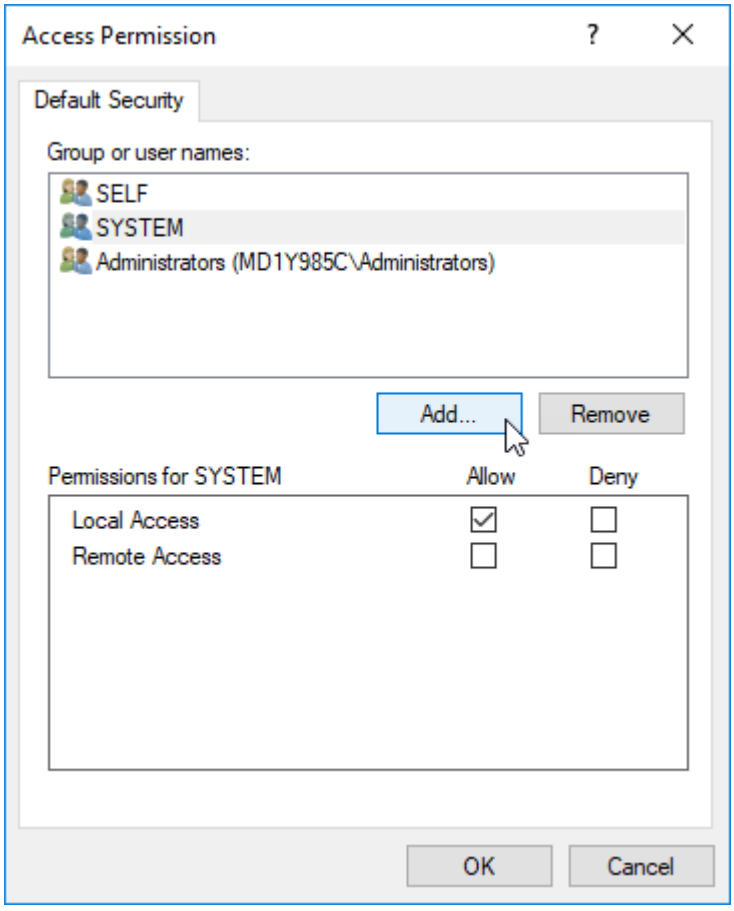
- ✧ For **Everyone**, select **Allow** for the **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation** check boxes.
- ✧ For the **Distributed COM Users** select the same permissions.
- ✧ Click **OK** to confirm.

6.1.2.2 Granting Access Permissions – Edit Default

To grant **Access Permissions** for a user, proceed with the following steps:

- ✧ Select the **COM Security** tab.
- ✧ In the **Access Permissions** field, click **Edit Default...** .

The **Access Permission** dialog opens.



[sc_Access_Perm_Edit_Default, 1, en_US]

Figure 6-5 Access Permission Dialog

Adding an User

✧ To add an user, for example, the **PASRuntimeUser**, click **Add...** .

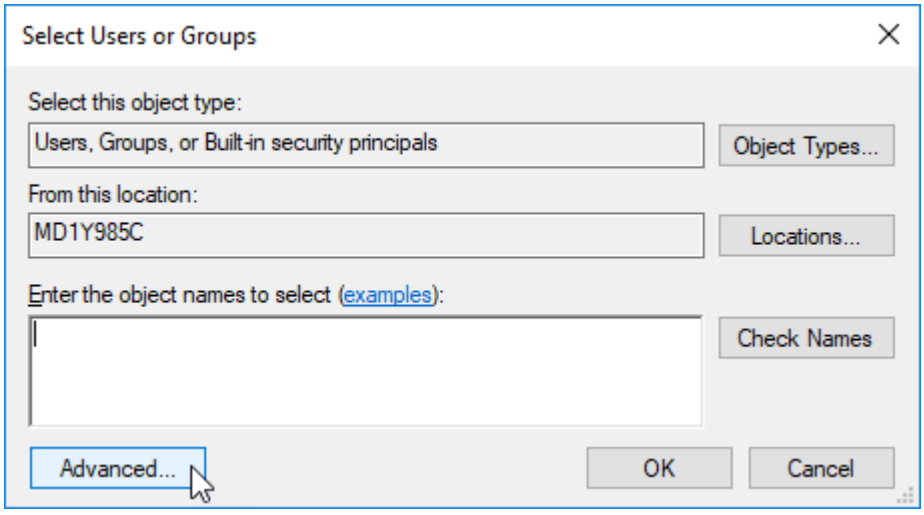
The **Select Users, Computers, or Groups** dialog opens.

✧ Click **Locations...** .

The **Locations** dialog opens.

✧ Select the name of your computer and click **OK**.

The **From this location** text box is updated.



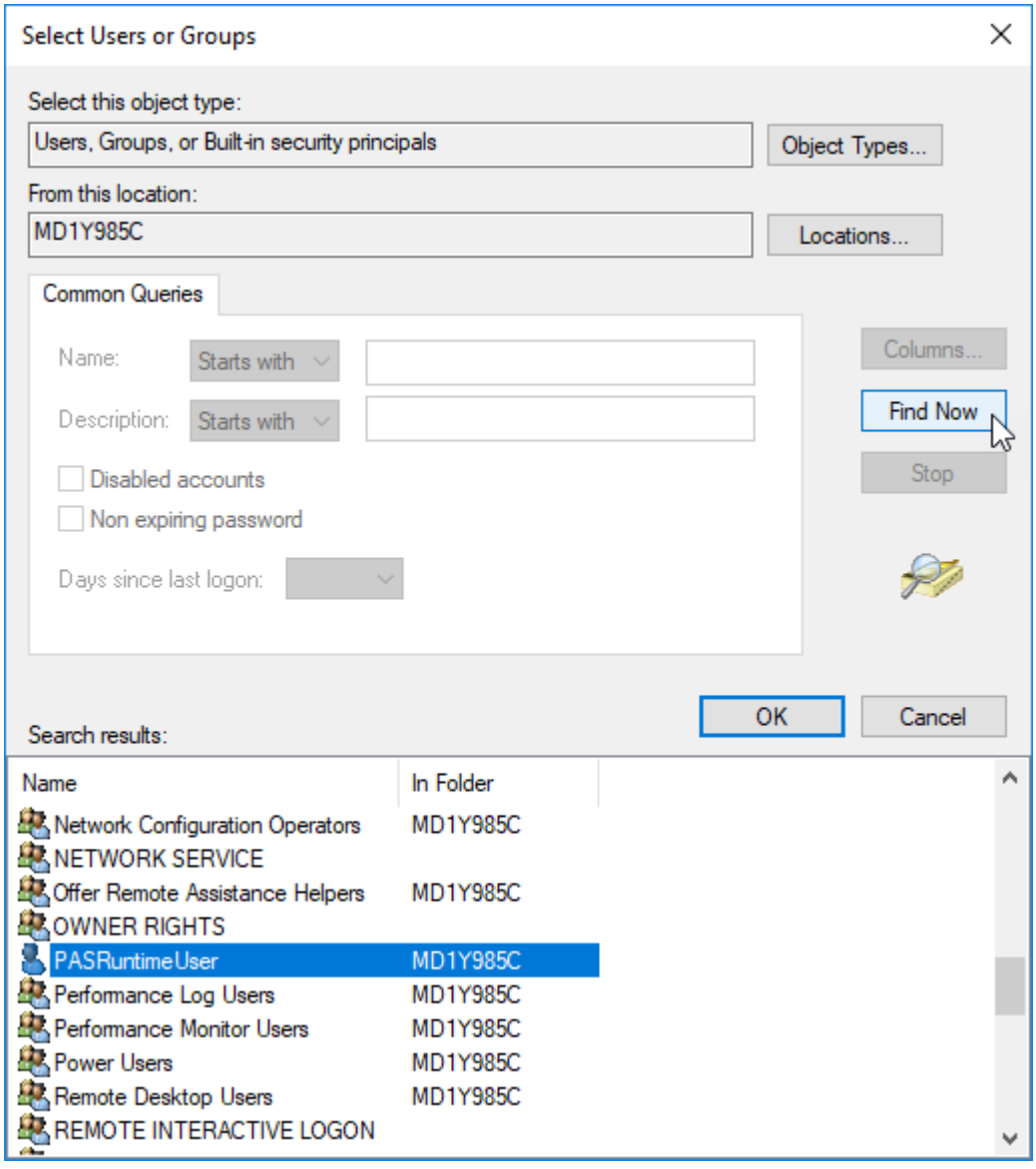
[sc_Select_Users_Comp_Serv_Acc_Grp, 2, en_US]

Figure 6-6 Select Users or Groups Dialog - Updated Location

✧ Click **Advanced...** to get access to the advanced settings.

✧ Click **Find Now**.

A list of all the users available from this location is displayed in the bottom section of the **Select Users or Groups** dialog.

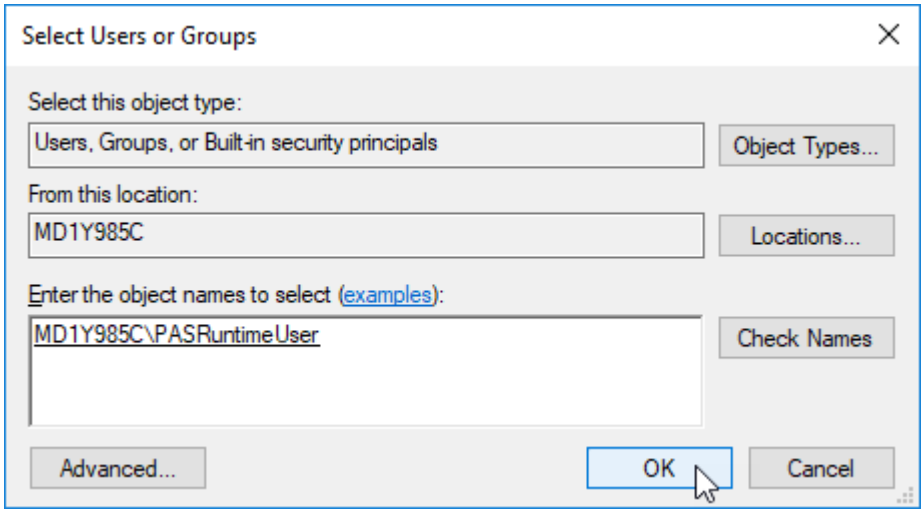


[sc_Select_Users_or_Groups, 2, en_US]

Figure 6-7 Select Users or Groups Dialog – List of Available Users

✧ Select the **PASRuntimeUser** and click **OK**.

The **Enter the object names to select** text box is updated.



[sc_Select_Users_or_Groups_PasRuntimeUser_added, 1, en_US]

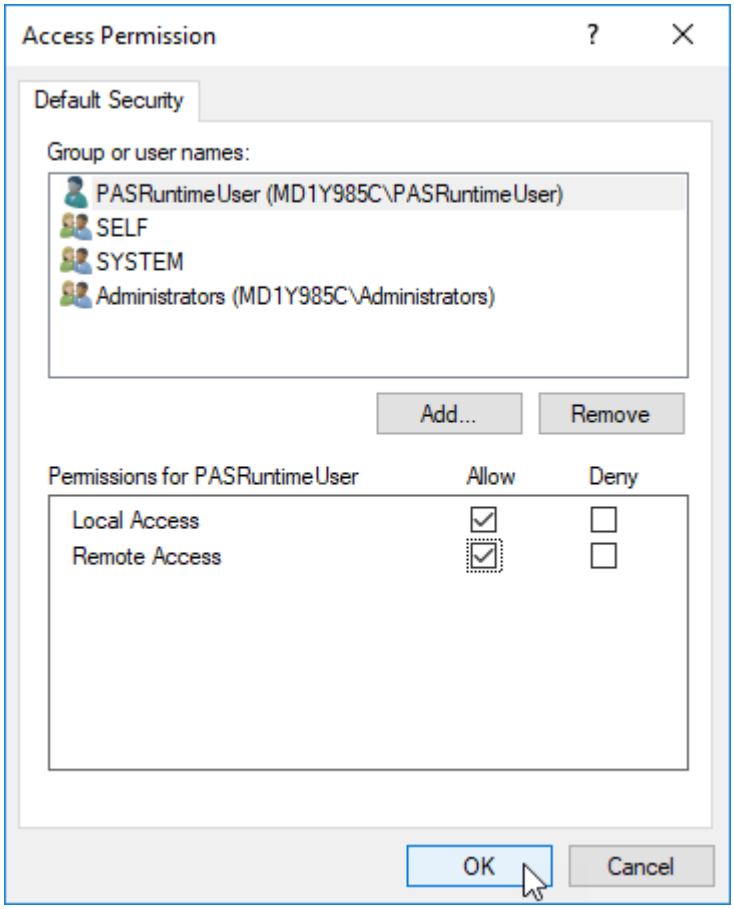
Figure 6-8 Select Users or Groups Dialog – Added PASRuntimeUser

✧ To close the dialog, click **OK**.

Granting Permissions

✧ In the **Access Permission** dialog, select the **PASRuntimeUser** from the **Group or user names**.

✧ Select **Allow** for the **Local Access** and the **Remote Access** check boxes.



[sc_Access_Perm_PASRuntimeUser, 1, en_US]

Figure 6-9 Access Permission Dialog

✧ To grant access permissions for the **PASRuntimeUser**, click **OK**.

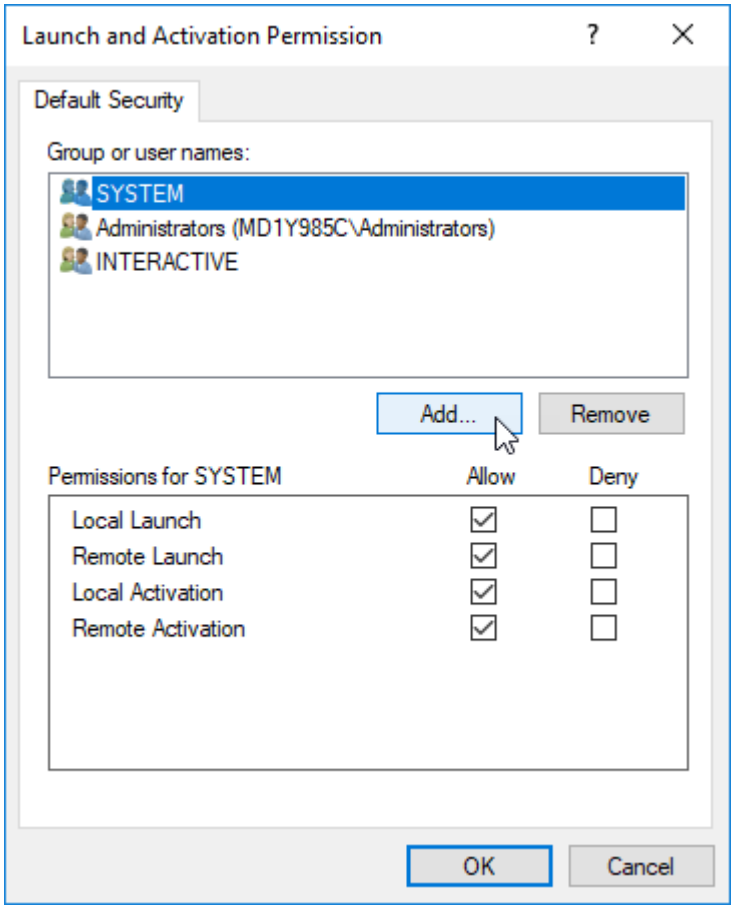
6.1.2.3 Granting Launch and Activation Permissions – Edit Default

To grant **Launch and Activation Permissions** for a user, proceed with the following steps:

✧ Select the **COM Security** tab.

✧ In the **Launch and Activation Permissions** field, click **Edit Default...** .

The **Launch and Activation Permission** dialog opens.



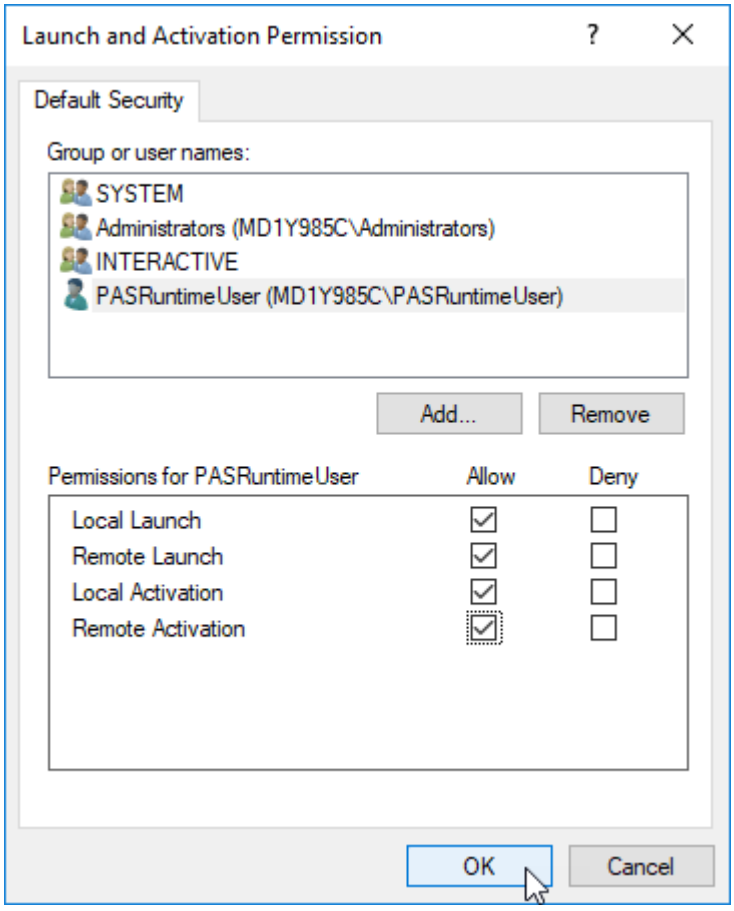
[sc_Launch_and_Activation_Perm_Edit_Default, 1, en_US]

Figure 6-10 Launch and Activation Permission Dialog

✧ Add the **PASRuntimeUser** as described in *Adding an User, Page 69*.

✧ Select the **PASRuntimeUser**.

✧ Next, select **Allow** for the **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation** check boxes.



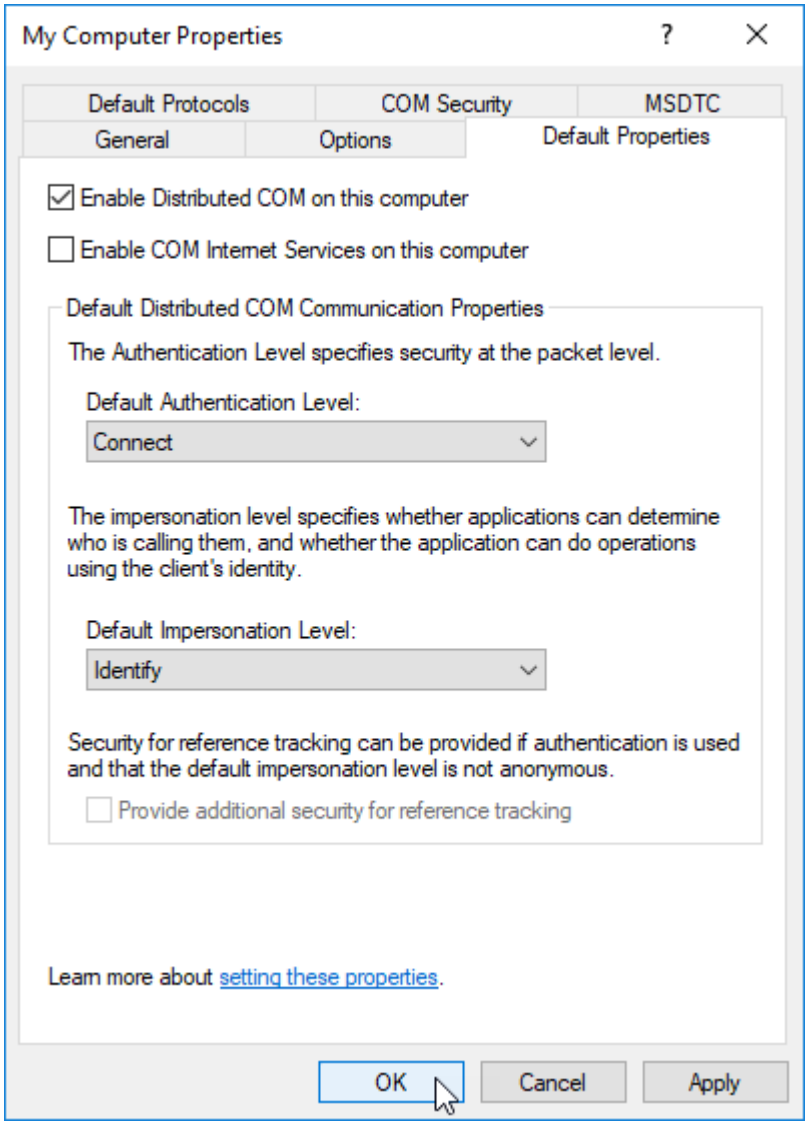
[sc_Launch_and_Activation_Perm_PASRuntimeUser, 1, en_US]

Figure 6-11 Launch and Activation Permission Dialog

✧ To grant the launch and activation permissions for the **PASRuntimeUser**, click OK.

6.1.2.4 Configuring Default Properties

✧ From the **My Computer Properties** dialog, select the **Default Properties** tab.



[sc_MyComputer_Properties_OPC_Default_prop, 1, en_US]

Figure 6-12 My Computer Properties Dialog – Default Properties Tab

- ✧ Select the **Enable Distributed COM on this computer** check box.
- ✧ Select **Connect** from the **Default Authentication Level** list box.
- ✧ Select **Identify** from the **Default Impersonation Level** list box.

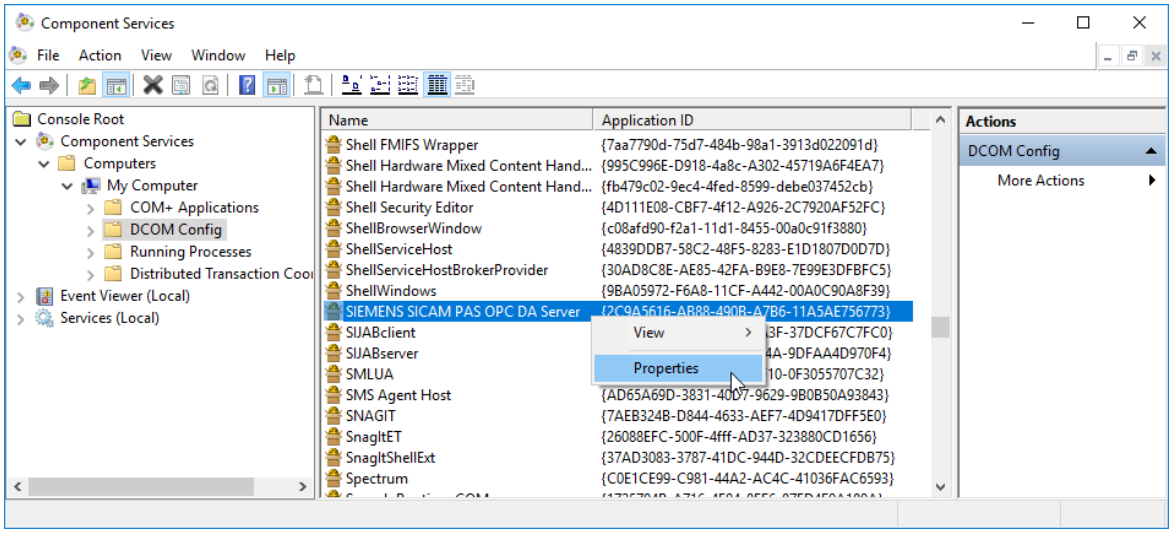
Settings do not need to be performed in the other tabs.

- ✧ Click **OK** to close the window.

6.1.3 Configuring SIEMENS SICAM PAS OPC DA Server

- ✧ In the **Component Services** window under **My Computer**, select **DCOM Config**.
- ✧ Right-click the **SIEMENS SICAM PAS OPC DA Server** and select **Properties** from the context menu.

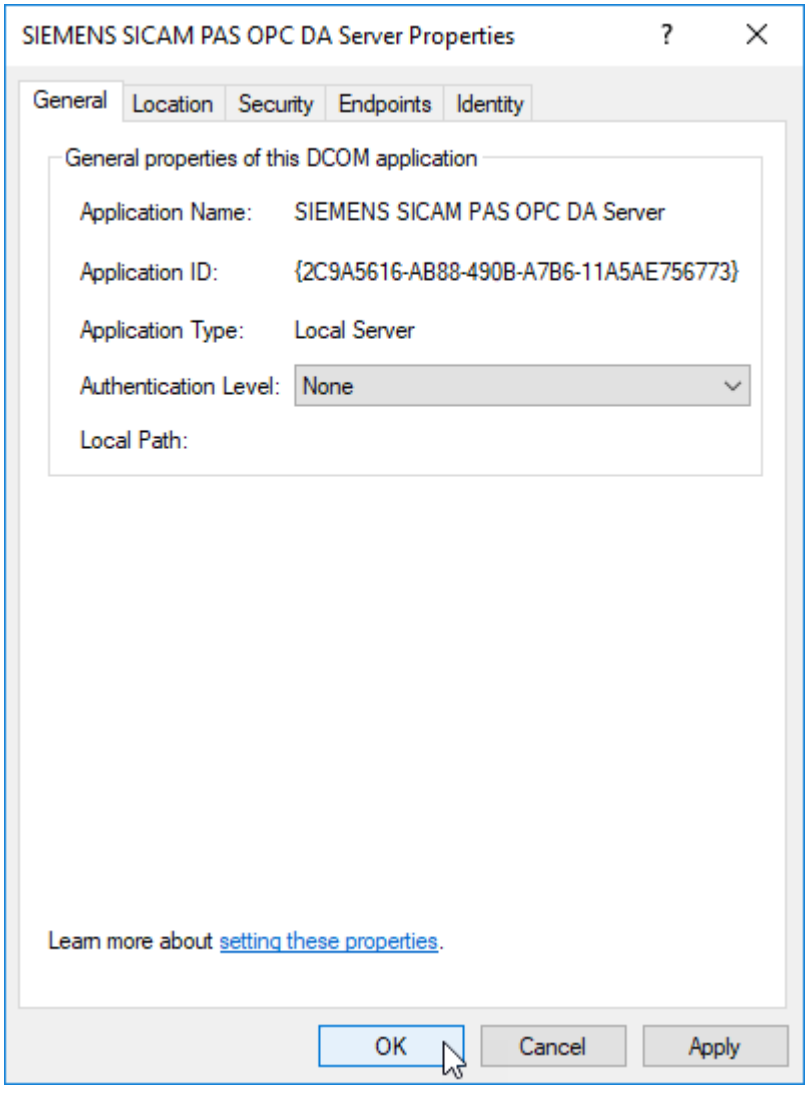
The **SIEMENS SICAM PAS OPC DA Server Properties** dialog opens.



[sc_Component_Services_OPCDA_Server, 2, en_US]

Figure 6-13 Selecting the Properties of the SIEMENS SICAM PAS OPC DA Server

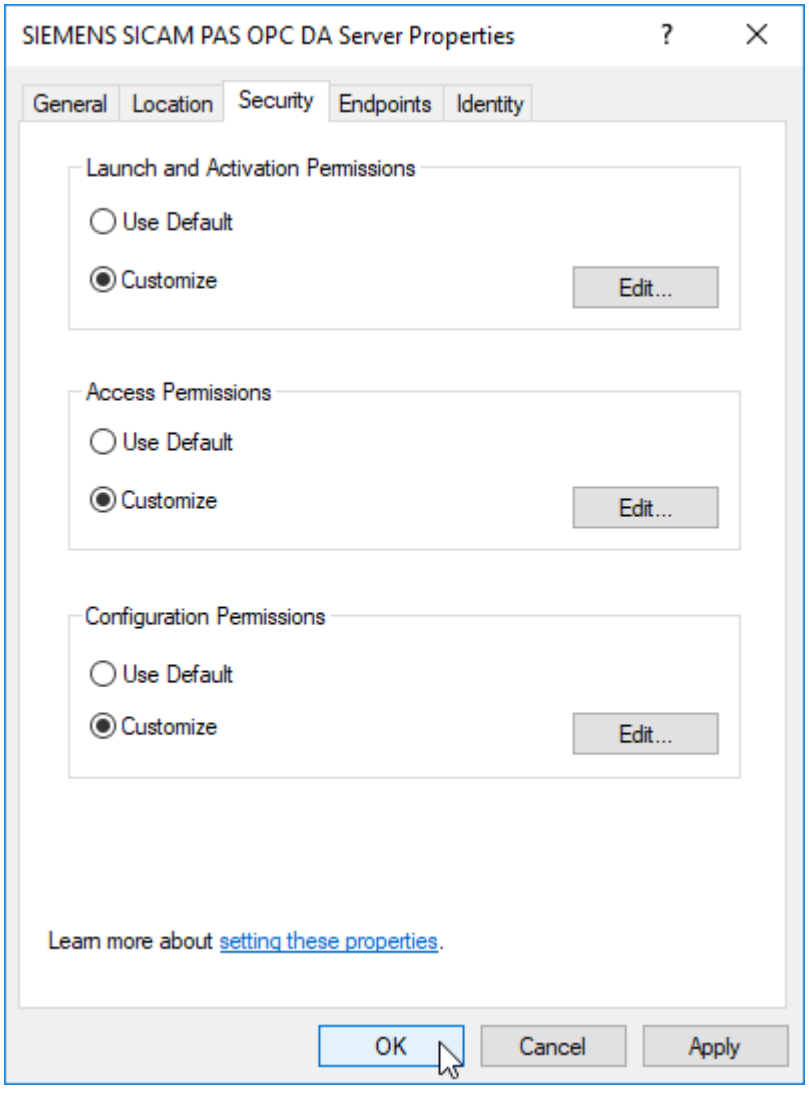
✧ Select the **General** tab.



[sc_OPC_DA_Properties_General, 2, en_US]

Figure 6-14 SIEMENS SICAM PAS OPC DA Server Properties Dialog – General Tab

- ✧ Select **None** from the **Authentication Level** list box.
  For DCOM, you must additionally assign the 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. For more detailed information on the configuration of the OPC Client, refer to *6.2 Checking the Settings of the OPC Client*.
- ✧ Select the **Security** tab.



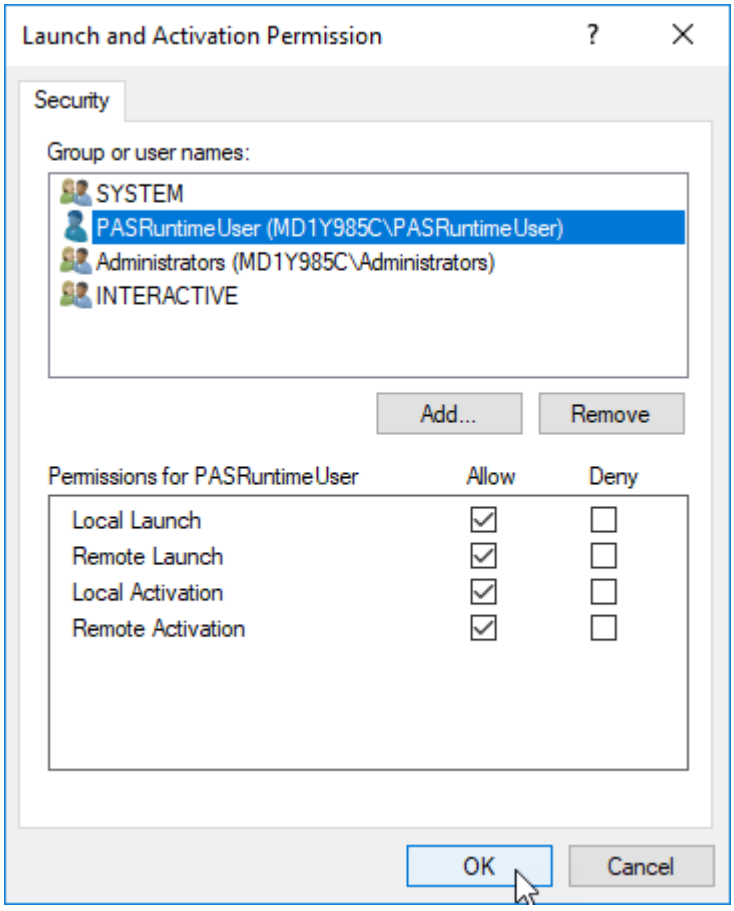
[sc_OPC_DA_Properties_Security, 2, en_US]

Figure 6-15 Security Tab

Granting Launch and Activation Permissions

- ✧ Select **Customize** under **Launch and Activation Permissions**.
- ✧ Click **Edit...** .

The **Launch and Activation Permission** dialog opens.



[sc_OPC_DA_Launch_and_Activation_Perm_PASRuntime, 1, en_US]

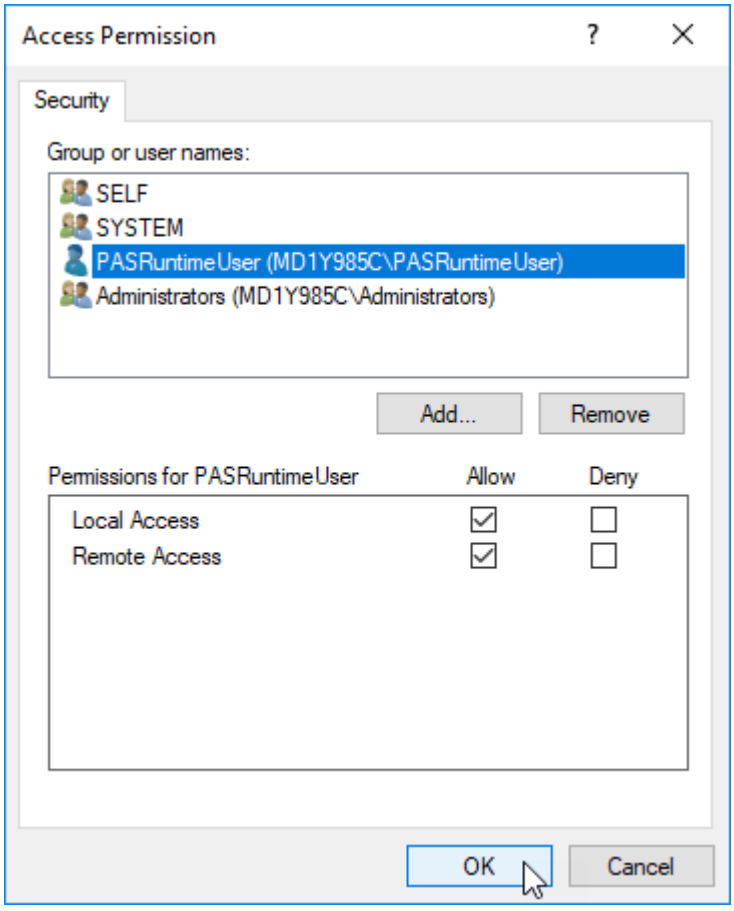
Figure 6-16 Specifying the Launch and Activation Permission

- ✧ Click **Add...** to add the user (with access permission for the OPC Server/Client).
- ✧ Select **Allow** for the **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation** check boxes.
- ✧ To grant launch and activation permissions for the **PASRuntimeUser**, click **OK**.

Granting Access Permissions

- ✧ Select **Customize** under **Access Permissions**.
- ✧ Click **Edit...** .

The **Access Permission** dialog opens.



[sc_OPC_DA_Access_Perm_PASRuntime, 1, en_US]

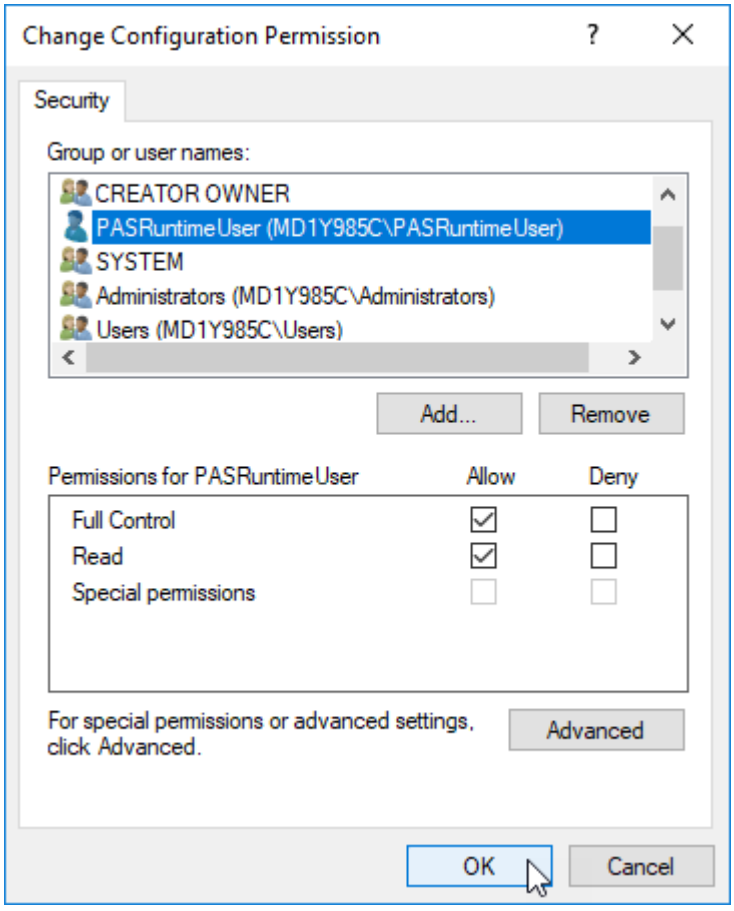
Figure 6-17 Specifying the Access Permission

- ✧ Click **Add...** to add the user (with access permission for the OPC Server/Client).
- ✧ Select **Allow** for the **Local Access** and **Remote Access** check boxes.
- ✧ To grant access permissions for the **PASRuntimeUser**, click **OK**.

Granting Configuration Permissions

- ✧ Select **Customize** under **Configuration Permissions**.
- ✧ Click **Edit...** .

The **Change Configuration Permission** dialog opens.



[sc_OPC_DA_Change_Config_Perm, 1, en_US]

Figure 6-18 Specifying Configuration Permissions

- ✧ Click **Add...** to add the user (with access permission for the OPC Server/Client).
- ✧ Select **Allow** for the **Full Control**, **Read**, and **Special Permissions**.

NOTE

Special Permissions is allowed only if the **Advanced** settings are configured.

- ✧ To grant configuration permissions for the **PASRuntimeUser**, click **OK**.

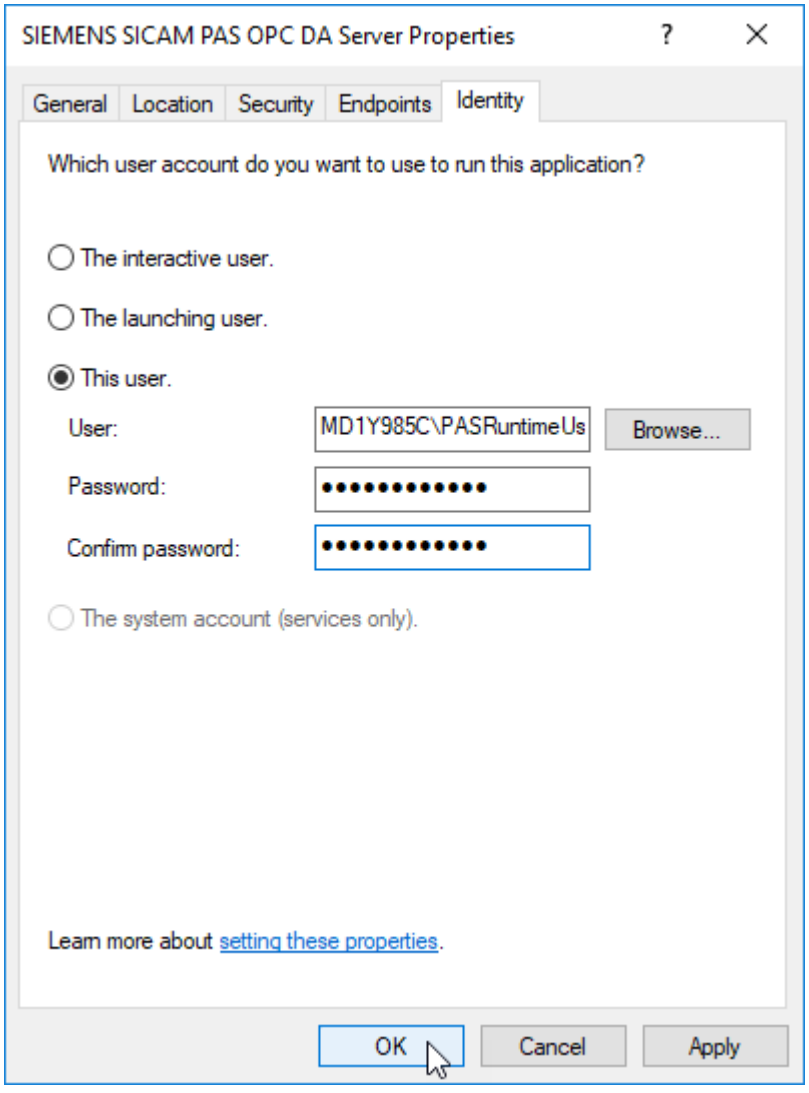
Endpoints Tab

This tab includes a list of protocols and endpoints, which may be used by the OPC Client.

- ✧ No settings are required.

Identity Tab

- ✧ Select the **Identity** tab.



[sc_OPC_DA_Properties_Identity, 1, en_US]

Figure 6-19 Identity Tab

- ✧ Select **This User** and enter the user name and password and confirm it.
- ✧ Click **OK** to close the dialog.
- ✧ Close the **Component Services** window.

NOTE

The entered user must be added to the **Distributed COM Users** group.

6.2 Checking the Settings of the OPC Client

SSR is set up as a Windows service for the OPC Client.

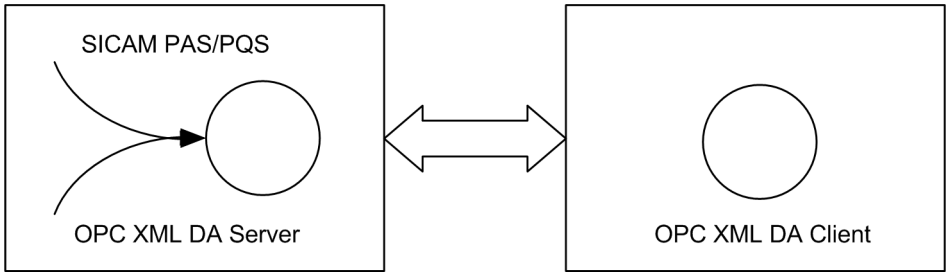
- ✧ To ensure that the OPC Client can access the OPC Server via a network, the OPC Client must log on with user rights for the OPC Server.
  This user does not need to be the user who is logged on to the local computer.

6.3 Setting up the OPC XML DA Server

The **OPC XML DA Server** is a protocol for SICAM PAS/PQS.
The data exchange of the SICAM PAS/PQS with an OPC XML DA Client takes place via this Server.
The OPC XML DA Server must be enabled using the **Feature Enabler**.

Communication

The OPC XML DA Server and OPC XML DA Client communicate via TCP/IP.



[dw_Comm_OPCXMLDA_Server_Client, 1, en_US]

Figure 6-20 Communication between the OPC XML DA Server and the OPC XML DA Client via Ethernet

This open communication is suitable for the data exchange between the SICAM PAS/PQS and other systems based on Microsoft Windows or also on other operating systems such as LINUX.
The OPC XML DA Server allows the exchange of structured information (station data) via the Internet using XML (EXtensible Markup Language).
Via the OPC XML DA Server, the OPC XML DA Client can set protocol parameters and read or write all the values, which have been mapped to OPC XML DA in SICAM PAS/PQS UI – Configuration.
The OPC XML DA Server can be accessed via *http://<hostname/ipaddress>:8081/da* from the OPC XML DA Client.

7 System Time

The time zone information for SICAM PAS/PQS can be updated using a download from the IANA Time Zone Database.

High-precision time synchronization is a prerequisite for the proper functioning of a SICAM PAS/PQS system. A radio clock can be used as the timer. The time information from this clock is distributed throughout the entire system. The distribution of time information is shown based on a sample configuration.

7.1 Updating Time Zones

The time zone information of the world is maintained in the IANA Time Zone Database. This reflects changes made by political bodies to time zone boundaries, UTC offsets, and daylight-saving rules. You can update the time zone information of the SICAM system using the download of this time zone information.

To do this, proceed as follows:

✧ Open the website *http://www.iana.org/time-zones*.

✧ Download the latest version of the time zone data file **tzdata20xxx.tar.gz**, for example, Time Zone Data v. 2014h (Released 2014-09-25) tzdata2014h.tar.gz (278.2kb).

✧ Open the directory where the program for updating the time zone information is located.

- For Windows 32-bit operating system:
  %CommonProgramFiles%\Siemens\TimeZoneCalculations\bin
- For Windows 64-bit operating system:
  %CommonProgramFiles(x86)%\Siemens\TimeZoneCalculations\bin

✧ Select the **TimeZoneDataUpdater.cmd** file and select **Run as adminstrator** from the context menu.

The command line tool opens.

✧ In the dialog that follows, navigate to the downloaded time zone data file and open it.

The time zone information is being updated.

✧ Click **OK** to exit the program.

After the update process is completed, the runtime system loads the time zone data within an hour. The system does not need to be shut down or be restarted.

7.2 Synchronizing Time

Time information within a SICAM PAS/PQS system can be synchronized via:

- an **NTP clock** (for example, SICLOCK, Hopf Time Server, and Meinberg Time Server), an external device connected to the SICAM PAS/PQS computer via Ethernet
- a **remote terminal interface** from the control center
  This time synchronization method is not relevant for SICAM SCC.

NOTE

The Hopf FG6039GPS receiver has been discontinued. If you want to continue to use this PCI card for the SICAM PAS/PQS computer, refer to the Installation manual of SICAM PAS/PQS V8.08.

The time synchronization of SICAM PAS/PQS is based on the **NTP** (Network Time Protocol) and the corresponding **NTPD** (Network Time Protocol Daemon) software. Under a Windows operating system, the NTPD service runs in the background. For the installation of SICAM PAS/PQS, it is referred to as the **Network Time Protocol Service**. It is configured by means of the **ntp.conf** ASCII file. To edit this configuration file, Siemens recommends a text editor with the YAML markup language support, for example, Notepad++. Using this editor, comments and entries are displayed in different colors. The configuration file is located in the Windows directory, subfolder **\drivers\etc**, for example: **C:\WINNT\system32\drivers\etc**.

NOTE

Windows 7 and higher does not allow to edit the **ntp.conf** file directly within the Windows directory.

If you use one of these operating systems, copy the **ntp.conf** file to another directory (outside of the Windows directory), for example to the desktop. Edit the copied file there and save it to the Windows directory afterwards, overwriting the existing file.

The NTPD is automatically installed together with **SICAM PAS** or **SICAM SCC**. It is activated upon a restart of the computer.

In a SICAM PAS/PQS system, several NTPDs are simultaneously active (for example, on the external radio clock, the SICAM PAS/PQS, and the SICAM SCC computer). 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 system's NTPDs must perform extensive calculations. This process can take several hours after the system starts. If the current Time Master fails, the NTPDs use the time data determined in order to keep an utmost level of time precision for as long as possible.

For more detailed information on NTP, refer to *http://www.ntp.org*.

7.2.1 Network Time Protocol Daemon

For the configuration of 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 in order to determine the quality of their time signal. The NTPD of the peer with the most precise time signal is 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.

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

During the SICAM PAS/PQS Runtime, the delivered time stamp is assigned a **quality** for the determination of the system time. 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 power automation.
- **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 switching second is inserted and the clock therefore shows a temporary deviation of ~1 second.
- **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 compatibility reasons, a SICAM PAS/PQS-internal time stamp includes the **ClockSync** and **ClockValid** status bits. These bits are set depending on the quality of the time stamp:

- **High**
  The **ClockSync** and **ClockValid** status bits are set.
- **Medium**
  The **ClockValid** status bits are set.
- **Low**
  No status bit is set.
- **Unknown**
  No status bit is set.

7.2.2 Time Synchronisation with Telecontrol Protocols

If SICAM PAS/PQS shall be time synchronized via

- telecontrol protocols only or
- a telecontrol protocol as a backup (in case the primary (NTP) clock source fails)

a shared memory clock driver must be used with the (basic) **mode 1**.

NOTE

When using telecontrol protocols for time synchronization, a system time accuracy below 10 ms is not ensured.

The **ntp.conf** configuration file consists of 4 blocks for time synchronization via telecontrol protocols. Thereby up to 4 telecontrol contol connections can be used for time synchronization. A typical block has the following structure:

server 127.127.28.0 mode 33 minpoll 2 maxpoll 6

fudge 127.127.28.0 stratum 5

Where:

- The 3rd address section (**28**) defines the type of clock driver (28 = shared memory clock driver).
- The 4th address section (**0**) is used to distinguish between clocks of the same type.
  The values 0, 1, 2, or 3 refer the maximal 4 control center connections configured in SICAM PAS UI – Configuration for time synchronization via telecontrol protocol.
- Time-out monitoring is automatically included (**mode 33**).
- The expected time synchronization interval with telecontrol protocol is between 4 seconds (**minpoll 2** = 2^2) and 64 seconds (**maxpoll 6** = 2^6).
- The **stratum** value **5** specifies the time synchronization via a telecontrol protocol.

Mode

For time synchronization via telecontrol protocols the mode values 1, 17, 33, or 49 (based on the basic mode 1) can be used.
The **mode** parameter must be interpreted as a bit pattern (decimal value). The tables below illustrate the significance of the bits, for example, if bit 0 and bit 5 are set, **mode 33** results from the bit pattern.

Table 7-1 Bit Pattern for Mode 33 (Example)

Bit	7	6	**5**	4	3	2	1	0
Bit pattern	0	0	**1**	0	0	0	0	1
Value			**32**		**1**			

Table 7-2 Meaning of the Individual Bits of the Mode Parameter

Bit position	Meaning
Bit 0 to 3	Bits 0 to 3 define the mode. This half byte must have the value **1** for the cooperation with the telecontrol protocols of SICAM PAS/PQS.
Bit 4 (bit value 16)	Setting the clock time If this bit is set, the clock driver initiates clock setting to the value present in the clock if the difference between the system time and the time available in the clock is more than 10 s. This difference value can be increased, but not reduced, by means of **fudge time2**.
Bit 5 (bit value 32)	Automatic time-out monitoring If this bit is set, the clock driver attempts to optimize the actual poll cycle within the limits predefined by **minpoll** and **maxpoll**.
Bit 7 (bit value 128)	Writing information in the system log file This bit is only relevant for diagnosis. All information, warning, and error conditions are written into the system log file. If this bit is not set, the driver does not attempt to perform any entries in the event list of the system (’ quiet mode ’).

If SICAM PAS is under normal conditions time synchronized with NTP clocks and time synchronization via telecontrol protocol will be used as backup (when NTP synchronization fails), mode 1 or mode 33 (recommended) shall be used.

- Mode 1
  without additional functional specifications
- Mode 33
  Automatic time-out monitoring is included (bit 5)

If SICAM PAS will be time synchronized only via telecontrol protocol, mode 17 and mode 49 (recommended) can be used. Both, mode 17 and mode 49, support “ Setting the clock time", that is, the clock driver immediately sets the system clock to the received value if the difference to the system time is more than 10 s respectively the value defined with **fudge time2** (bit 4 = 1).

Mode 17 specifies that “ Automatic time-out monitoring ” is not used (bit 5 = 0).

Minpoll, Maxpoll

If **Automatic time-out monitoring** (bit 5 = 1) is activated, the NTPD tries to set a polling interval within the limits selected via **minpoll** and **maxpoll**. If the telecontrol protocol did not provide any value within a defined interval, the polling interval is increased by one step. If more than 2 values are transmitted within an interval, the polling interval is reduced by one step.

If synchronization based on the telecontrol protocol fails, the polling interval increases until the maximum interval value has been reached. The clock is marked as faulty and the polling interval is set to the minimum value in order to detect a recovery of synchronization as quickly as possible.

The values for **minpoll** and **maxpoll** must be selected in such a way that they include the expected time synchronization interval of the telecontrol protocol. Minpoll and maxpoll are exponents referred to the basis of 2.

The following value range can be used: minpoll = 2 (2^2 = 4 s) to maxpoll = 10 (2^{10} = 1024 s = 17 min)

If mode 1 or mode 17 is used, the values for the **minpoll** and **maxpoll** parameters must be selected very carefully in order to match the synchronization frequency of the telecontrol center: the minpoll parameter

must be set in such a way that also $2^{minpoll}$ is greater than the expected time synchronization interval via telecontrol protocol.

Fudge

- **Time1**
  As with most clock drivers, this value is used in order to compensate a systematic (constant) offset. For example, the runtime of the telecontrol telegram between the control center and the substation can be corrected. The value is defined as a floating point value indicated in seconds.
  Example: An offset of 1 second results in **time1 1**.
- **Time2**
  The difference value for clock time setting can be increased to a value greater than 10 s, see **bit 4** in the description of **mode 33**, *Table 7-2*. The value is defined as a floating point value indicated in seconds.
  Example: The value can be set to 20 seconds with **time2 20**.

7.2.3 Configuration File for NTPD

When installing **SICAM PAS/PQS** or **SICAM SCC**, an **ntp.conf** configuration file is copied into the **%windir%\system32\drivers\etc** or **...\%windir%\SysWow64\drivers\etc** directory. The **%windir%** directory name depends on the operating system, for example, **Windows** or **WINNT**. 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 therefore be conveniently added to a system. Only the configuration file of the new Client needs to be edited.

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

For more detailed information, refer to the following web site: *http://www.ntp.org*.

Security Related Settings

```
#--------------------------------------------------------------------------
# -*- SECURITY RELATED SETTINGS -*-
#--------------------------------------------------------------------------
# DRDoS attack prevention (DRDoS -> distributed reflection denial of service)
# disable monitor
# ^^^^^^^^^^^^^ -- DO NOT CHANGE UNLESS YOU KNOW WHAT YOU'RE DOING!
# The 'mrulist' command can be used for a DRDoS attack unless a firewall can
# prevent access from outside the network. (But even then, an inside attacker
# could still use the response amplification to carry out an attack.) So the
# whole monitoring feature should be disabled by default, unless specific
# access rules and authentication are provided.
```

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 condistion 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. Note this also defines the stratum used if no time source
# is available/eligible for synchronisation.
#-----------------------------------------------------------------------
tos orphan 10 # stratum 10 if no clock source available
tos mindist 0.020 # allow 20ms distance in sync group
```

- **Tinker panic**
  If the clock concerned deviates by more than 7200 s from the best external clock, time information is not sychronized. 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 lines, you can specify the storage location of the drift and log files. To do this, write access rights are required.
  Activate the **logfile** and **statsdir** lines for error detection only.
  The quartz drift determined is stored in the **ntp.drift** file. This allows for 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 only be achieved some time (hours!) after a system start.

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.
#
# NOW OBSOLETED BY 'tos orphan 10' -- do not use this clock unless you know
# 'what you're doing! Change the 'tos orphan' line for different stratum settings
# obsolete# server 127.127.1.0
# obsolete# fudge 127.127.1.0 stratum 10 flag2 1

# GARMIN GPS18xLVC use 19200bd (32)
server 127.127.20.4 mode 32 minpoll 4 maxpoll 7 prefer
```

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.

Shared Memory Clocks

```
#-------------------------------------------------------------------------
# shared memory clocks ('iburst' is not useful here)
#-------------------------------------------------------------------------
# minpoll 2 -> 4s / maxpoll 6 -> 64s, mode 33 -> adaptive polling
# Windows 7 recommendation: minpoll 4 maxpoll 4, but do this only
# if your CC can sync the substation every 10..15 seconds;
# set the min/maxpoll of a clock to match the control center sync frequency.

# channel 1
server 127.127.28.0 mode 33 minpoll 2 maxpoll 6
fudge 127.127.28.0 stratum 5 #

# channel 2
server 127.127.28.1 mode 33 minpoll 2 maxpoll 6
fudge 127.127.28.1 stratum 5

# channel 3
server 127.127.28.2 mode 33 minpoll 2 maxpoll 6
fudge 127.127.28.2 stratum 5

# channel 4
server 127.127.28.3 mode 33 minpoll 2 maxpoll 6
fudge 127.127.28.3 stratum 5
```

These lines are required in order to use **shared memory clock drivers**. They are used for time synchronization through telecontrol protocols.

- **Mode**
  Through **mode 33**, see *Table 7-2*, you can define adaptive polling. During adaptive polling, the frequency of the poll is automatically adjusted to the poll result. If the result rarely changes, polls are performed less frequently.

- **Minpoll, maxpoll**
  The **minpoll** and **maxpoll** parameters must be specified in such a way that the range matches the current synchronization rate of the control center as precisely as possible.

Peers

```
#-------------------------------------------------------------------------
# peers: all time sync peers in a PAS installation
#-------------------------------------------------------------------------
# If the local system has reference clock access, mention all other systems
# (full servers and dips) in a PAS installation that can also access reference
# clocks. Peers will negotiate the leader of the pack...

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

If one Full Server and one or several DIPs are used, the synchronization sources can be distributed among the computers used. To do this, activate the **peer** line.
In this case, the computers must determine among each other which clock time is most suitable. Since the classical Server/Client relationship cannot be applied in this context, all the computers involved must be configured as **peers** (that is, **colleagues** with the same priority). Data is exchanged on a bidirectional basis in order to ensure that synchronization can be performed by both systems.

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
```

The following lines serve as examples for the definition of Time Servers. The information in these lines can be 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
```

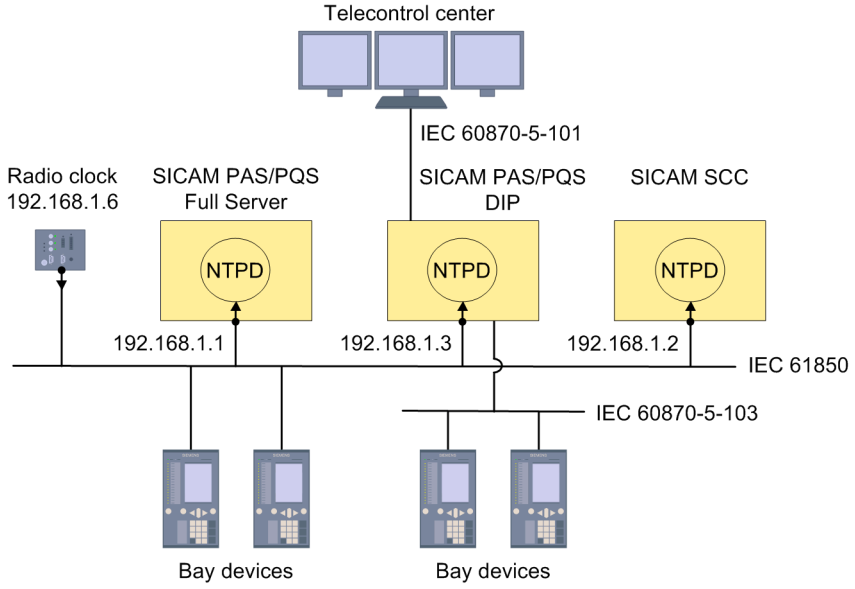
7.2.4 Example – External Radio Clock as Timer

For system configurations with an IEC 61850 Ethernet bay bus, an **external radio clock** (for example, SICLOCK, Meinberg, and Hopf) can be used as the Time 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 Time Master. In the NTPD configuration files, you can define which clock is to become the new Time Master.

The NTPD is active on both SICAM PAS/PQS computers (Full Server and DIP) and on the SICAM SCC computer. The NTPD of the radio clock is the Time Server; the NTPDs of the SICAM PAS/PQS computers are the Clients.

Additionally, time information can be transmitted from the telecontrol center.



[dw_Time_Synchronization_Ext_RadioClock, 2, en_US]

Figure 7-1 Time Synchronization through an External Radio Clock, Example

The bay devices on the IEC 61850 bus are Clients, which poll time information from the radio clock. Their configuration is not described in the present document. For more detailed information on this topic, refer to the documentation of the corresponding devices.

All other bay devices connected through IEC 60870-5-103 receive time information from the DIP.

Configuration Files

This paragraph provides a list of the ntp.conf configuration files for the SICAM PAS/PQS and the SICAM SCC computer. The entries in the list have been customized for the example illustrated. Be aware that the real system configuration (for example, IP addresses) of your own environment must be considered.

Changes to the predefined configuration files have been highlighted.

Configuration File of the SICAM PAS/PQS DIP

```
#--------------------------------------------------------------------------
# -*- SECURITY RELATED SETTINGS -*-
#--------------------------------------------------------------------------
# DRDoS attack prevention (DRDoS -> distributed reflection denial of service)
# disable monitor
# ^^^^^^^^^^^^^ -- DO NOT CHANGE UNLESS YOU KNOW WHAT YOU'RE DOING!
# The 'mrulist' command can be used for a DRDoS attack unless a firewall can
# prevent access from outside the network. (But even then, an inside attacker
# could still use the response amplification to carry out an attack.) So the
# whole monitoring feature should be disabled by default, unless specific
# access rules and authentication are provided.
```

```
#--------------------------------------------------------------------------
```

```
# 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.
tinker panic 7200.0
# -- 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\
#--------------------------------------------------------------------------
# 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
#--------------------------------------------------------------------------
# shared memory clocks ('iburst' is not useful here)
#--------------------------------------------------------------------------
# minpoll 2 -> 4s / maxpoll 6 -> 64s, mode 33 -> adaptive polling
# channel 1
server 127.127.28.0 mode 33 minpoll 2 maxpoll 6
fudge 127.127.28.0 stratum 5
# channel 2
server 127.127.28.1 mode 33 minpoll 2 maxpoll 6
fudge 127.127.28.1 stratum 5
# channel 3 server 127.127.28.2 mode 33 minpoll 2 maxpoll 6
fudge 127.127.28.2 stratum 5
# channel 4
server 127.127.28.3 mode 33 minpoll 2 maxpoll 6
fudge 127.127.28.3 stratum 5
#--------------------------------------------------------------------------
# peers: all time sync peers in a PAS installation
#--------------------------------------------------------------------------
# If the local system has reference clock access, mention all other systems
# (full servers and dips) in a PAS installation that can also access reference
# clocks. Peers will negotiate the leader of the pack...
# minpoll 2 -> 4s / maxpoll 6 -> 64s, iburst -> initial burst poll
peer 192.168.1.6 minpoll 2 maxpoll 6 iburst
```

The SICAM PAS/PQS DIP must be entered as a peer for the radio clock. If this is not possible, the radio clock **must not** be used as a peer, but as the Server.

```
#--------------------------------------------------------------------------
# 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
server 192.168.1.6 minpoll 2 maxpoll 6 iburst
```

Configuration file of the SICAM SCC computer and of the SICAM PAS/PQS Full Server

```
#--------------------------------------------------------------------------
# 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.
tinker panic 7200.0
# -- 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.drif
# -- 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\
#--------------------------------------------------------------------------
# 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
#--------------------------------------------------------------------------
# shared memory clocks ('iburst' is not useful here)
#--------------------------------------------------------------------------
# minpoll 2 -> 4s / maxpoll 6 -> 64s, mode 33 -> adaptive polling
# channel 1
server 127.127.28.0 mode 33 minpoll 2 maxpoll 6
fudge 127.127.28.0 stratum 5
# channel 2
```

```
server 127.127.28.1 mode 33 minpoll 2 maxpoll 6
fudge 127.127.28.1 stratum 5
# channel 3
server 127.127.28.2 mode 33 minpoll 2 maxpoll 6
fudge 127.127.28.2 stratum 5
# channel 4
server 127.127.28.3 mode 33 minpoll 2 maxpoll 6
fudge 127.127.28.3 stratum 5
#-------------------------------------------------------------------------
# peers: all time sync peers in a PAS installation
#-------------------------------------------------------------------------
# If the local system has reference clock access, mention all other systems
# (full servers and dips) in a PAS installation that can also access reference
# clocks. Peers will negotiate the leader of the pack...
# minpoll 2 -> 4s / maxpoll 6 -> 64s, iburst -> initial burst poll
# peer xxx.xxx.xxx.xxx minpoll 2 maxpoll 6 iburst
#-------------------------------------------------------------------------
# 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
server 192.168.1.3 minpoll 2 maxpoll 6 iburst
server 192.168.1.6 minpoll 2 maxpoll 6 iburst
```

A Appendix

Using the **VMware** software, several different SICAM PAS/PQS versions can be operated in parallel on the same computer.

A substation or a SIMEAS R device can be connected to SICAM PAS/PQS by means of a dial-up connection. The SICAM PAS/PQS computer must be equipped with a **modem** in this case.

A.1 Several SICAM PAS/PQS Versions on One Computer

General Information

NOTE

The installation of two SICAM PAS/PQS versions may only be performed on a computer which is used exclusively for the configuration of SICAM PAS/PQS systems.

VMware 5.x (or higher) enables you to operate several virtual computers ("virtual engines") on one single computer. Each virtual computer behaves like an autonomous computer with an individual audio/video and network interface card and an individual hard disk. You can switch between the virtual computers by clicking the mouse button.

Set up a virtual computer in order to operate 2 SICAM PAS/PQS versions (for example, SICAM PAS V7.00 and SICAM PAS/PQS V8.04) in parallel. On the real computer (with host operating system), install SICAM PAS/PQS V8.04; on the virtual computer (with guest operating system), install SICAM PAS V7.00. Alternatively, you can install both SICAM PAS/PQS versions on 2 virtual computers.

NOTE

For the virtual computer, you may only use the operating systems which have been released for SICAM PAS/PQS (see *2.2 Operating System*).

Since the use of special PC communications cards (CP5613/14, USB) is not supported by **VMware 5.x**, only the **SICAM PAS/PQS UI – Configuration** and **Feature Enabler** components can be executed. In order to ensure that the **SICAM PAS/PQS UI – Operation** and **Value Viewer** components and the **Runtime** operate properly, standard COM interfaces should be used.

Virtual Computer

VMware supports the following 3 different variants of virtual computers:

- **VMware Workstation**
- **VMware Server**
  With the VMware Server, the virtual computer is accessed via the **VMware Console**.
- **VMware Player**
  With the VMware Player, you can only run an existing virtual computer. However, you can neither create a new virtual computer nor modify an existing one, because the VMware Player has not been designed for these purposes.

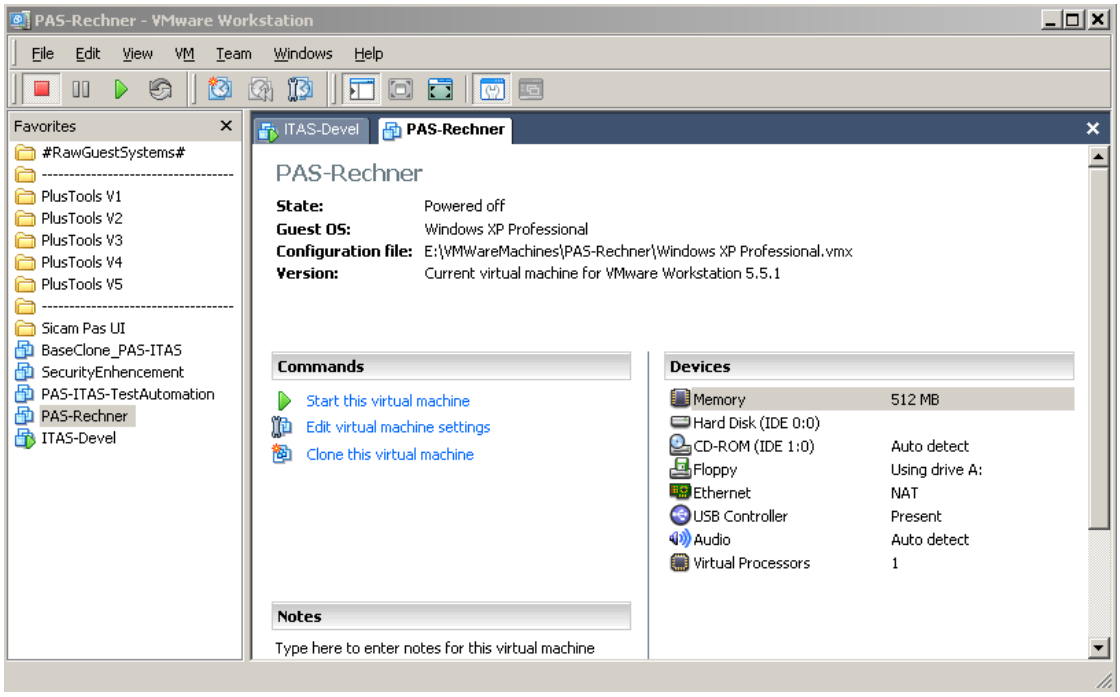
In order to be able to execute the steps described below, the **VMware Workstation** must have been installed according to the corresponding instructions. Additionally, an operating system released for SICAM PAS/PQS (see *2.2 Operating System*) is installed.

Setting up a Virtual Computer

To install SICAM PAS/PQS on a virtual computer, the following settings must be checked/performed on the **VMware Workstation**:

To perform the necessary settings:

- Start the **VMware Workstation**.



[sc_VMware_workstation_start, 1, en_US]

Figure A-1 VMware Workstation, Performing Settings

For more detailed information on the settings, refer to the **VMware** online help.

- Set the **CD ROM** to **Auto detect** in order to ensure that the virtual computer can use the DVD drive.
- Configure the Ethernet to meet your requirements.
  If the **NAT** or **Host only** options have been selected, VMware makes available an IP address to the virtual computer (guest system) via DHCP.
- Set the **USB Controller** to **Present** if you are using the USB dongle.
- Insert a **parallel port** if you are using a dongle for the parallel interface.
- Insert a **serial port** if you require a serial interface.

Installing SICAM PAS/PQS

For the installation of SICAM PAS/PQS, the virtual computer (guest operating system) must run and be able to access the SICAM PAS/PQS installation DVD.

Install SICAM PAS/PQS on the virtual computer as described in *3 Installing SICAM PAS/PQS*.

NOTE

You can install both the **Full Server** and a **DIP** on a virtual computer.

A.2 Virtualization Solutions

SICAM PAS/PQS has been released for use with virtualization solutions such as VMware and CITRIX. In addition, **VMware Workstation** and **VMware Player** can be used for the configuration of a SICAM PAS/PQS system.

NOTE

SICAM PAS/PQS can be used with the following CITRIX solutions:

- Pooled Desktop Catalog
- Remote PC Access Catalog

Please also note the following:

- In addition to the application software, the **Virtual Delivery Agent** (VDA) must be installed on every virtual machine.
- The receiver software must be installed on every client.

Hardware and software requirements

The hardware requirements defined by the designer of the virtualization solution must be fulfilled.

Furthermore, please note the software and hardware requirements of the product for the configuration of virtual machines.

As a rule the CPU utilization of a virtual machine should not exceed 50% during continuous operation, because the system stability can be impaired under high load scenarios. To check the CPU utilization, use either the options provided by the virtualization solution or the Task Manager on the guest system.

Thanks to its system architecture, SICAM PAS/PQS distributes the CPU load to several cores depending on the individual configuration. This means that the system performance can be improved by adding virtual CPU cores. However, adding virtual cores only makes sense if the capacity of all the existing cores is highly utilized (CPU utilization).

Siemens recommends providing more Random Access Memory (RAM) capacity than specified by the hardware requirements (e.g. an additional 2 GB or doubling the capacity specified), because the use of the swap file can affect the performance in virtual environments.

Licensing

Every guest system must be treated like a real installation and licensed accordingly.

A dongle (licenses) must be purchased for every virtual machine. The licenses must be specifically assigned to an individual virtual machine. To achieve this, a USB hub must be used. The USB hub and the virtual machine are connected via Ethernet LAN. In order to be able to assign a virtual machine a USB port, the USB hub must first be configured via the web interface of the hub. Furthermore, the software providing access to the corresponding USB ports (port groups) must be installed on every virtual machine which is to connect to the USB hub. The USB devices plugged into the ports communicate with the corresponding virtual machine via Ethernet LAN.

Please note that the dongles must be redundantly connected (via at least two USB hubs) in a redundant configuration.

NOTE

Prolonged network failures may cause the applications to stop working. To restart them, update the system.

Restrictions

SICAM PAS/PQS does **NOT** support multi-user scenarios (i.e. the simultaneous use of the product) on a virtual machine.

NOTE

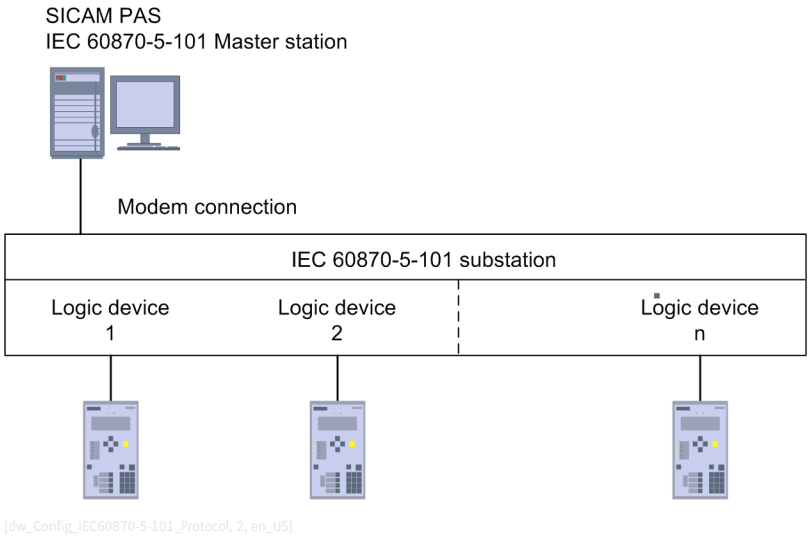
Especially when using virtual solutions in a redundant configuration, the fail-safe operation of core components such as network cards or hard disks must be ensured so as not to impair the availability of the overall system.

A.3 Connecting a Substation via IEC 60870-5-101

The IEC 60870-5-101 Master protocol is frequently used for the connection of remote telecontrol units.

In a typical configuration, SICAM PAS/PQS is the IEC 60870-5-101 Master station which communicates with a substation. This substation is the Master for different bay devices.

From the perspective of SICAM PAS/PQS, this RTU can be considered to be acting as a "proxy" for these bay devices.



[dw_Config_IEC60870-5-101_Protocol, 2, en_US]

Figure A-2 Example of a Configuration Using the IEC 60870-5-101 Protocol

In such a configuration, the substation can be communicate with SICAM PAS/PQS through a serial connection (COM port) using either a dedicated line or a dial-up connection (via modem).

If a modem connection is used, the modem must have already been installed on the SICAM PAS station computer. Modems can be installed via the Windows Control Panel.

The following modems can be used:

- ISDN card (for example, AVM FRITZ!Card PCI)
- Analog modem
- GSM modem

NOTE

Check that a modem driver for your operating system is available, before you buy a modem.

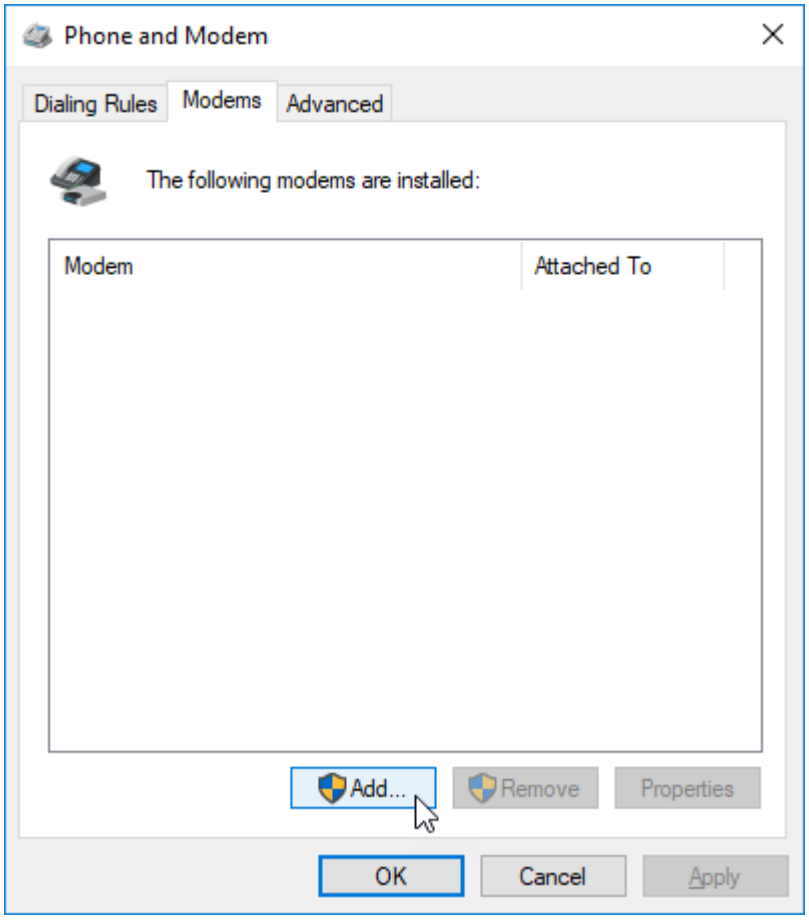
Installing a Modem

To install a modem for an IEC 60870-5-101 interface under Windows 10:

✧ Click **Start**, type **Phone and Modem**, and confirm by pressing <Enter>.

The **Phone and Modem** dialog opens.

✧ Select the **Modems** tab.

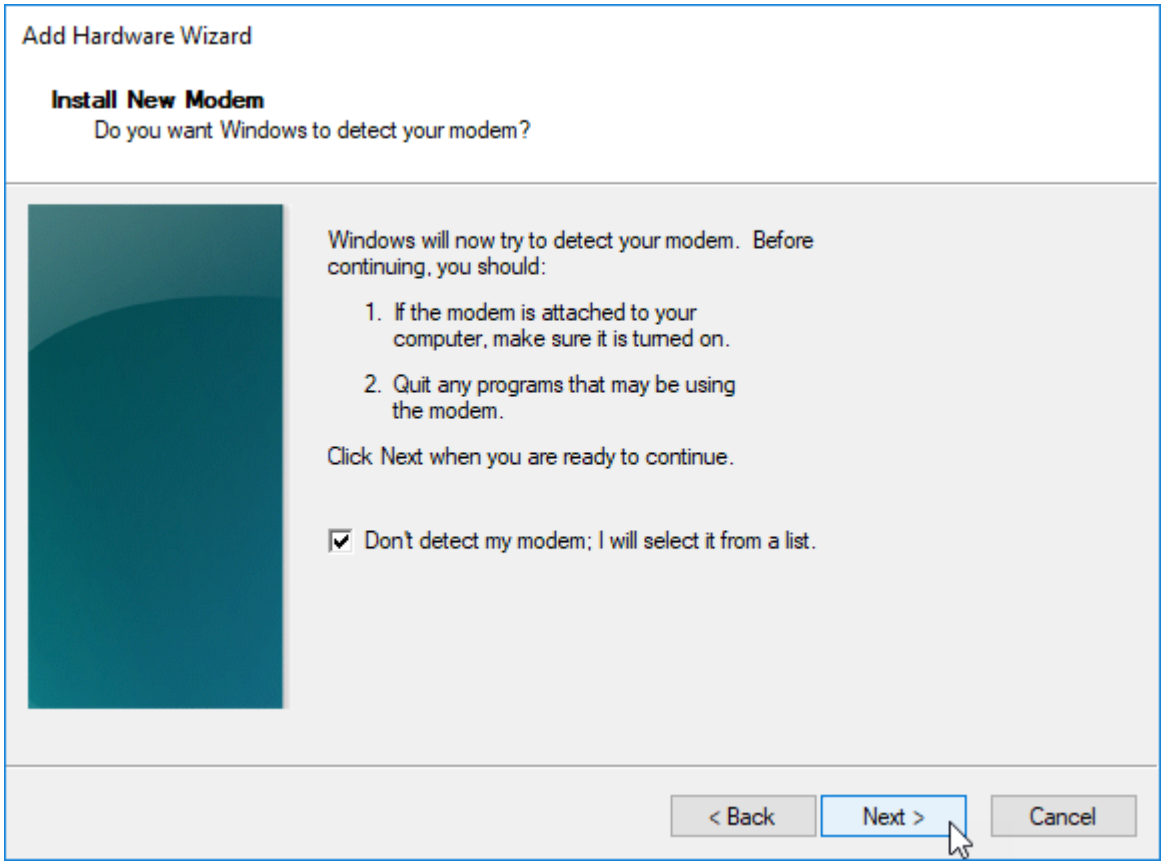


[sc_Add_Modem, 2, en_US]

Figure A-3 Adding a Modem

✧ Click **Add...**.

The **Add Hardware Wizard** dialog opens.

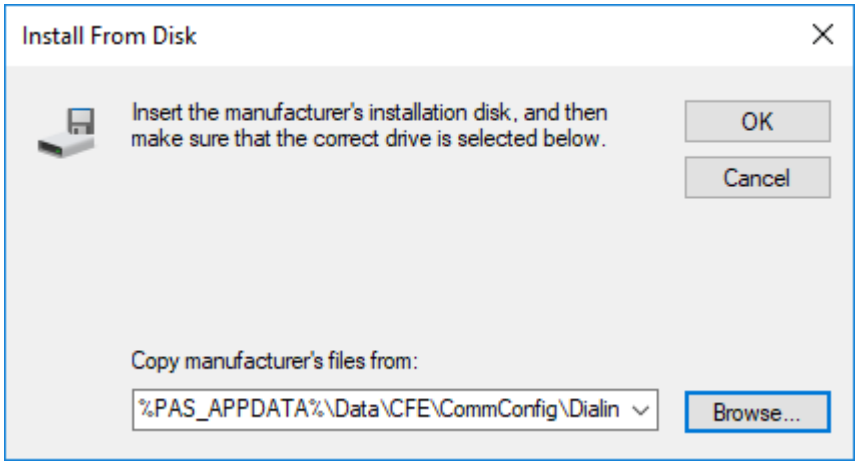


[sc_Install_Modem, 2, en_US]

Figure A-4 Installing a New Modem

- ✧ Activate **Don't detect my modem; I will select it from a list** and click **Next >**.
- ✧ In the next dialog, click **Have Disk...**.

The **Install From Disc** dialog opens.



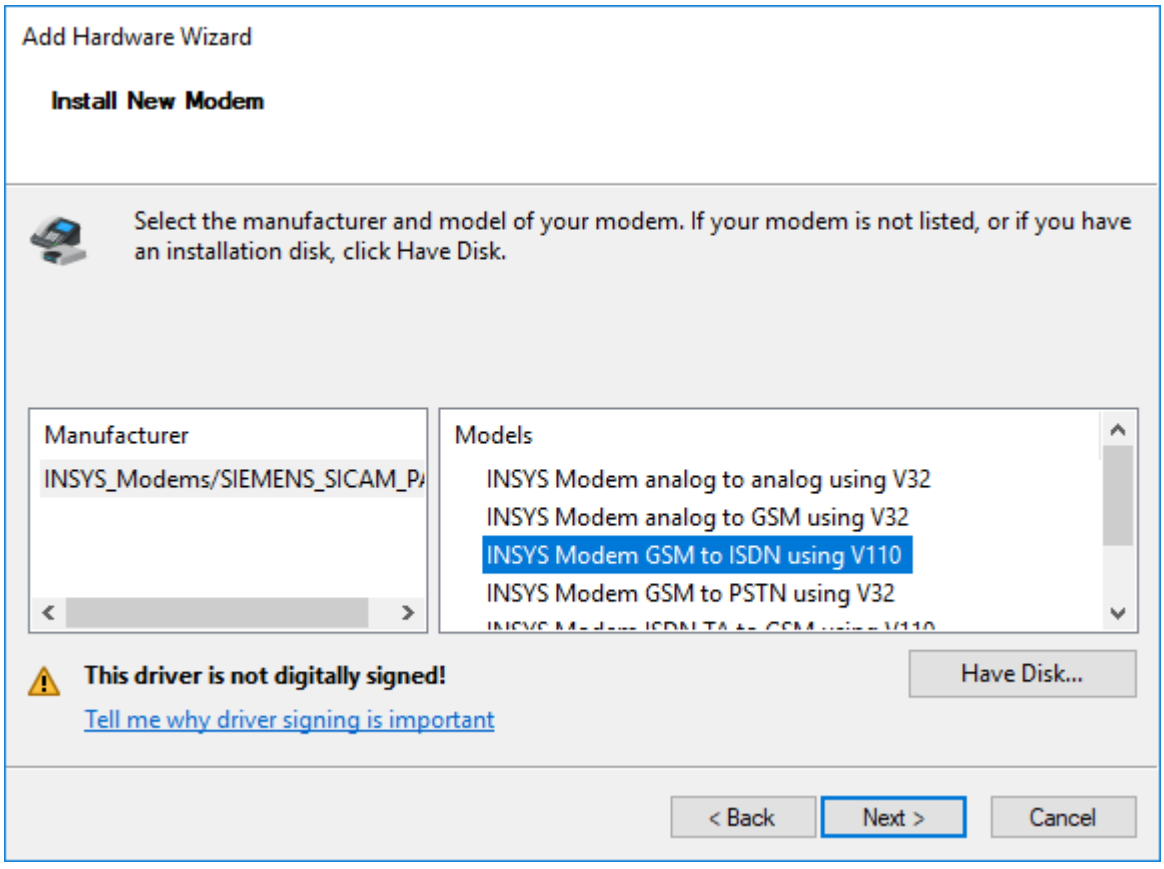
[sc_Install_From_Disk, 1, en_US]

- ✧ Enter **%PAS_APPDATA%\Data\CFE\CommConfig\Dialing** in the **Copy manufacture´s file from** field and click **Browse...**.
- ✧ Open the **Siemens_Modem_Insys.inf** file.

NOTE

The **Siemens_Modem_Insys.inf** file only considers Insys models.

- ✧ In the **Install from Disk** dialog, confirm your selection with **OK**.
- ✧ Select your modem (ISDN or analog modem) from the **Manufacturer** and **Models** sections.



[sc_Select_Modem, 2, en_US]

Figure A-5 Selecting a Modem

NOTE

Configure the modem connection of the substation/miniRTU in such a way that the INSYS modem uses the same data protocol as the modem on the SICAM PAS computer.

In the example above, the data protocol is V.110. In this case, the configuration string e.g. of an ISDN modem would be: **ATE0&KS0=1&C1&D2V1X0B0N4&WZ** (the most important value is B0, because it defines the type of protocol).

The configuration string must be modified accordingly if an analog modem is used (refer to the operating instructions of the analog modem).

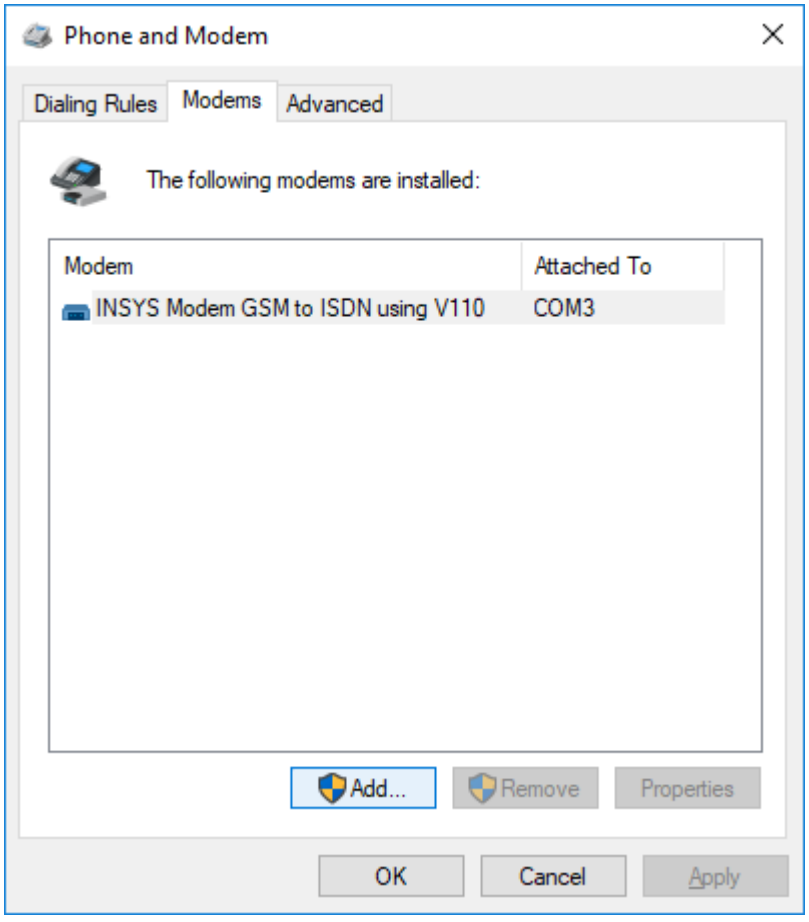
The following applies for the selection of the protocol:

Connect 2 ISDN modems based on the X.75 protocol. In the configuration string of the INSYS ISDN TA modem, the value B0 changes to B10.

Connect an ISDN modem to a GSM modem based on the V.110 protocol.

- ✧ Click **Next >**.
- ✧ Select the modem interface from the dialog and click **Next >**.
- ✧ In the dialog which opens, click **Finish** to complete the configuration of the modem.

The new modem is now listed in the **Modems** tab.



[sc_Modem_List, 2, en_US]

Figure A-6 Listed Modems

Using an ISDN card

An ISDN card (e. g. AVM FRITZ!CARD PCI) can be used as an alternative to a modem.

✧ To use the ISDN card with SICAM PAS/PQS, the AVM ISDN CAPI port driver must be installed.

NOTE

The AVM ISDN CAPI driver is only supported on the 32-bit edition of Windows 7.

The installation of the driver and of the virtual modem is described in detail in the card manufacturer ' s installation manual included in the scope of delivery of the ISDN card.

When installing the driver, you can select from numerous installable virtual modems.

For use under SICAM PAS/PQS, Siemens recommends you install modems working with the X.75 protocol, such as:

- AVM ISDN - ISDN (X.75)
- AVM ISDN Mailbox (X.75)

The virtual modems can be selected from the **Modem Parameters** dialog after their installation in order to use them under SICAM PAS/PQS.

NOTE

If the ISDN card is also used by other programs, these programs must be disabled before SICAM PAS/PQS communicates via this card. Otherwise, they might cause communication problems.

A.4 Connecting a SIMEAS R Device

Overview

You can connect a SIMEAS R device to a SICAM PAS/PQS station computer via:

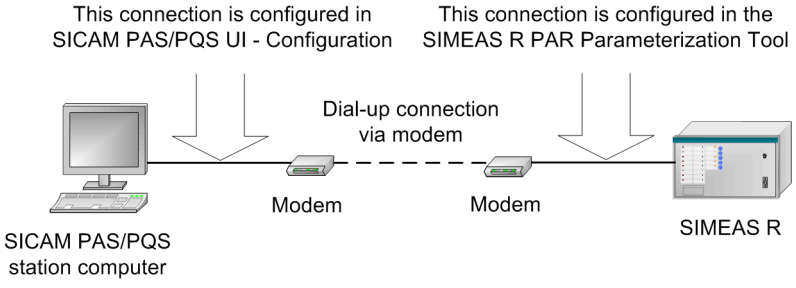
- Direct connection (null modem or star coupler)
- LAN
  Dial-up connection via modem
  - Hayes Compatible, Baud rate up to 115 200 bit/s
  - TAPI Interface, Baud rate up to 115 200 bit/s

The following modems can be used:

- Analog modem
- ISDN modem
- ISDN card (for example, AVM ISDN FRITZ!Card PCI V2.0)
- GSM modem

The ISDN/GSM modems must support the Hayes command set.

If you configure a modem (TAPI interface), Siemens recommends the use of an external analog **INSYS Modem 56k 4.2** for both the SIMEAS R device and the SICAM PAS/PQS station computer.



[dw_Modem_Connection, 1, en_US]

Figure A-7 Dial-up Connection via Modems and the Public Telephone Network

In order to ensure reliable communication, the modems of the SIMEAS R device and the SICAM PAS/PQS station computer must use the same **INIT string** and the same **baud rate**.

The steps to be carried out in order to set up a **dial-up connection via modems** are described depending on the interface type:

- *A.5 Modem (TAPI Interface)*
- *A.6 Modem via COM Port (Hayes Compatible)*

A.5 Modem (TAPI Interface)

Perform the following steps one after the other:

- *Installing the Modem on the SICAM PAS/PQS Station Computer, Page 107*
- *Configuring the Modem, Page 110*
- *Setting up a Modem Connection (TAPI Interface) in SICAM PAS/PQS, Page 114*
- *Setting up a Modem Connection in SIMEAS R PAR, Page 118*

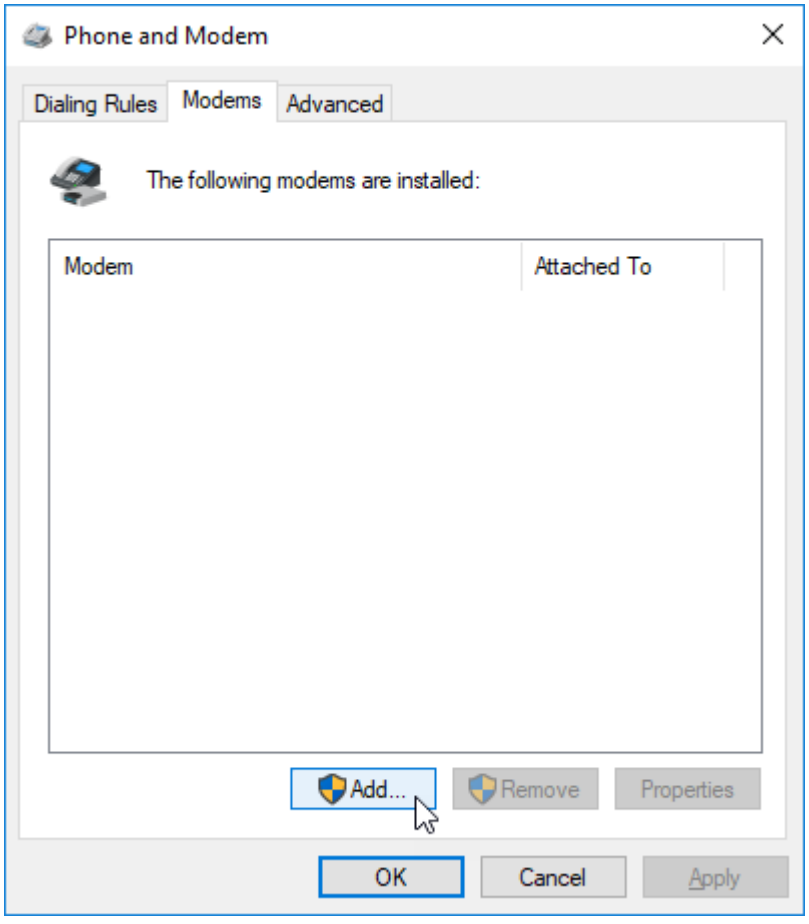
Installing the Modem on the SICAM PAS/PQS Station Computer

To install the **INSYS Modem 56k** in Windows 10 for a dial-up connection to a SIMEAS R device:

✧ Click **Start**, type **Phone and Modem**, and confirm by pressing <Enter>.

The **Phone and Modem** dialog opens.

✧ Select the **Modems** tab.



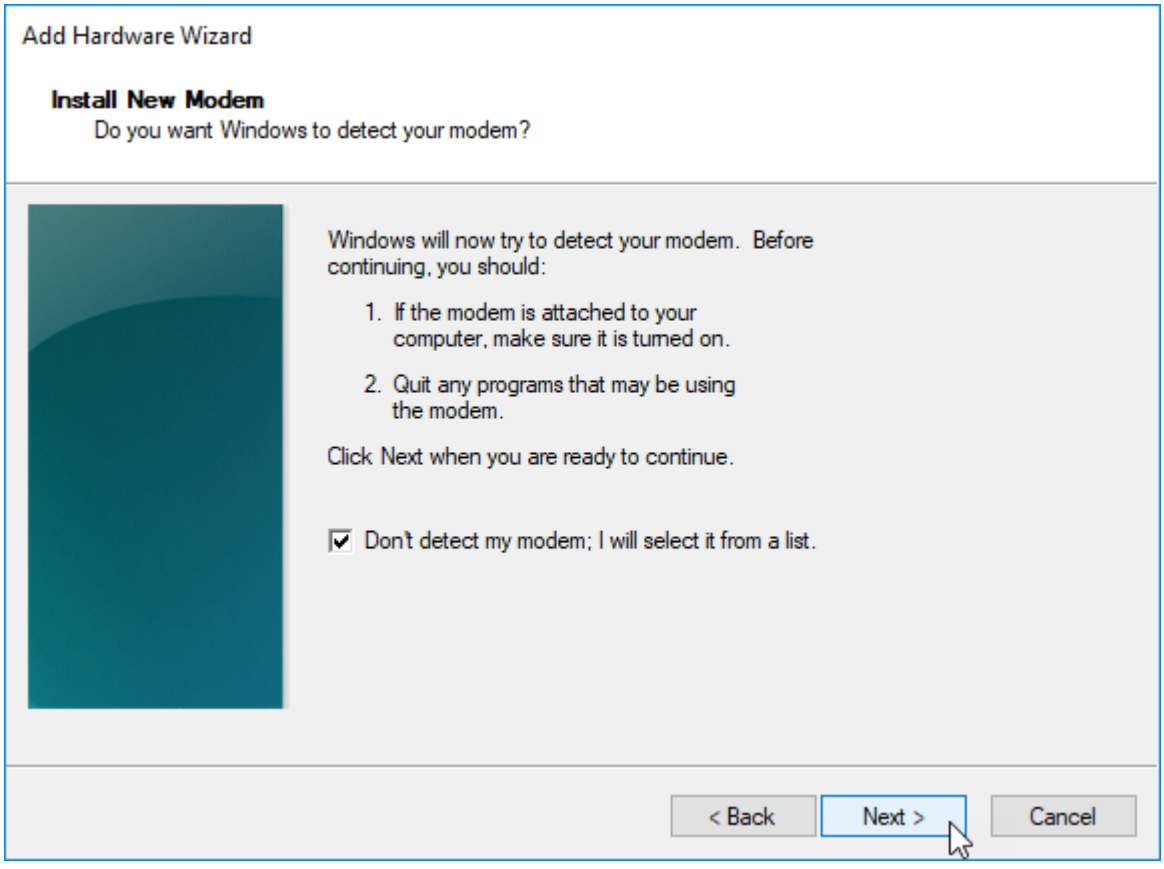
[sc_Add_Modem, 2, en_US]

Figure A-8 Adding a Modem

✧ Click **Add...**.

The **Add Hardware Wizard** dialog opens.

✧ Activate **Don't detect my modem; I will select it from a list** and click **Next >**.

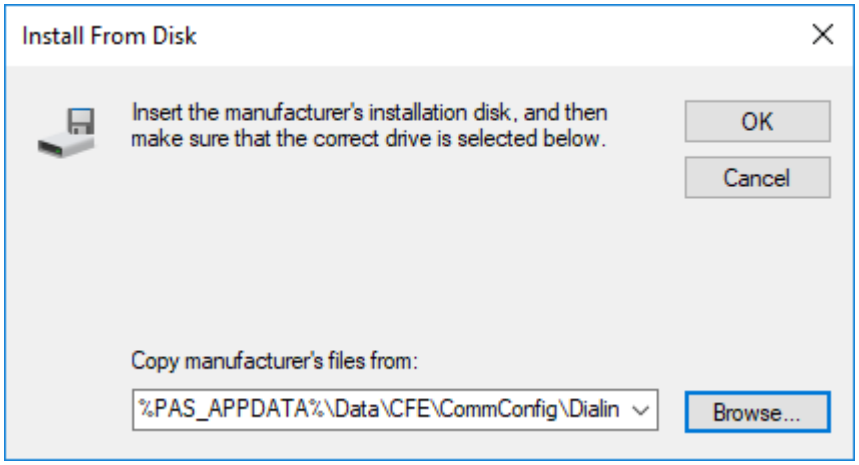


[sc_Install_Modem, 2, en_US]

Figure A-9 Installing a New Modem

✧ In the dialog which opens, click **Have Disk...**.

The **Install From Disk** dialog opens.



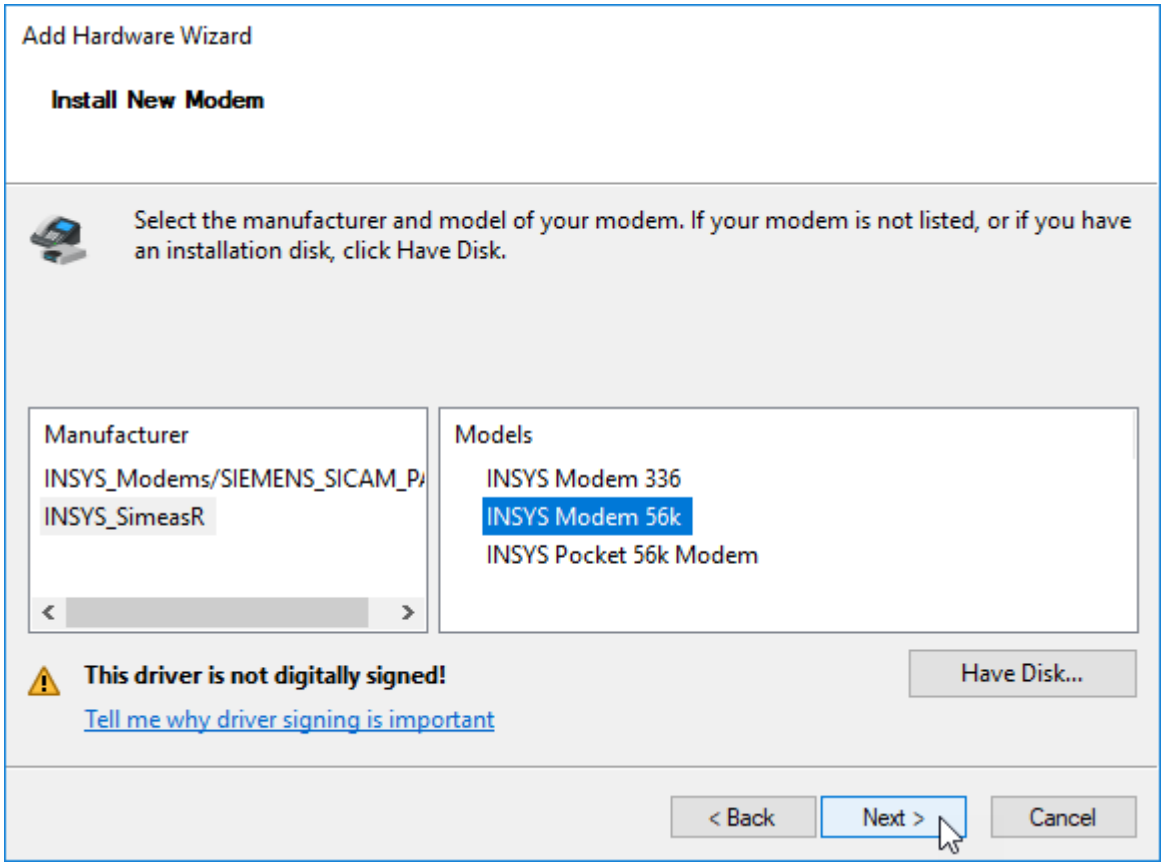
[sc_Install_From_Disk, 1, en_US]

✧ Enter **%PAS_APPDATA%\Data\CFE\CommConfig\Dialing** in the **Copy manufacturer´s file from** field and click **Browse...**.

✧ Open the **Siemens_Modem_Insys_SimeasR.inf** file.

The **Siemens_Modem_Insys_SimeasR.inf** file also includes the **INIT string** for the modem of the SICAM PAS/PQS station computer. For this reason, you do not need to define its parameters.

- ✧ In the **Install from Disk** dialog, confirm your selection with **OK**.
- ✧ Select **INSYS_SimeasR** from the **Manufacturer´s** section and **INSYS Modem 56k** from the **Models** section.

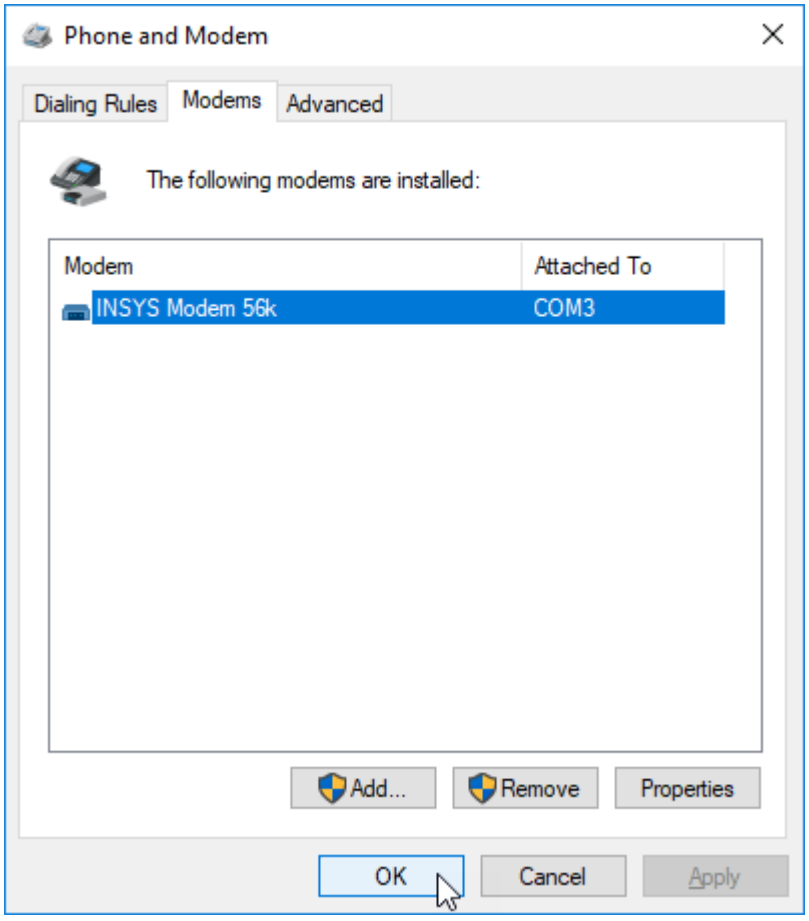


[sc_Select_Modem_Model, 2, en_US]

Figure A-10 Selecting a Modem

- ✧ Click **Next >**.
- ✧ Select the modem interface from the next dialog and click **Next >**.
- ✧ To finish the configuration of the modem, click **Finish**.

The new modem is listed in the Modems tab and can be inserted in SICAM PAS/PQS as a system resource.



[sc_Modem_List_New, 2, en_US]

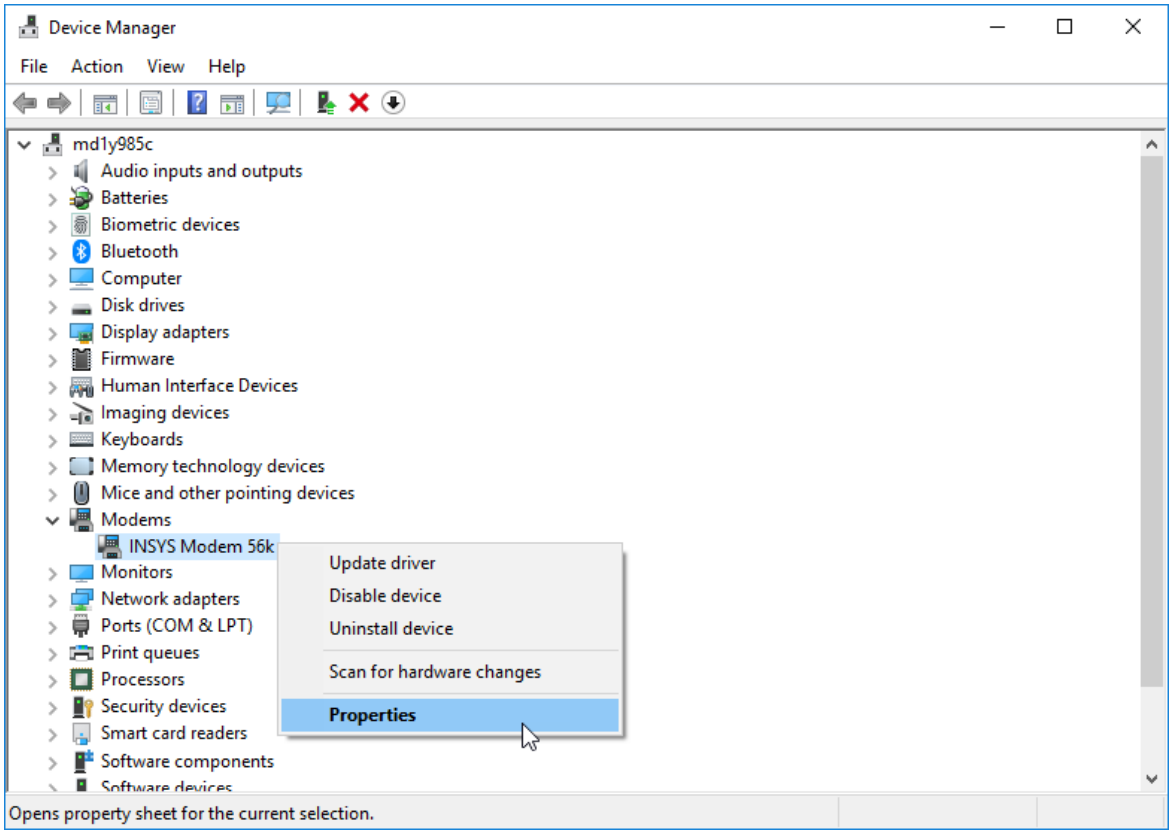
Figure A-11 Listed Modems

✧ Confirm with **OK**.

Configuring the Modem

✧ Click **Start**, type **Device Manager**, and confirm by pressing <Enter>.

The Device Manager opens.

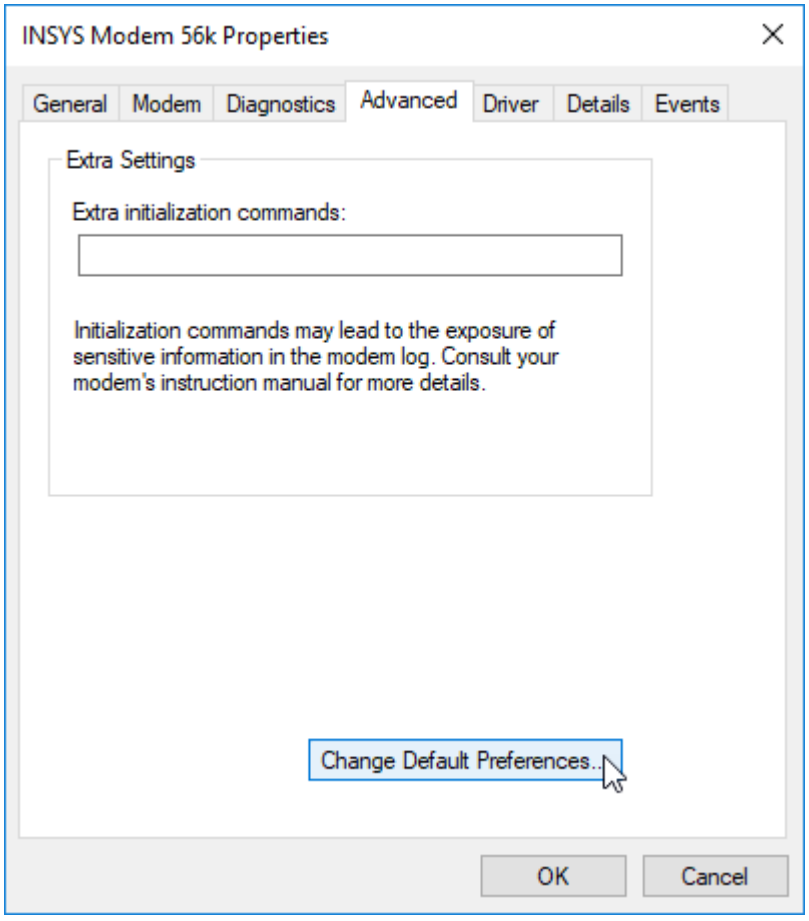


[sc_Modem_Properties, 2, en_US]

Figure A-12 Defining Modem Properties

✧ Select the **INSYS Modem 56k** modem and select **Properties** from the context menu.

The **INSYS Modem 56k Properties** dialog opens.

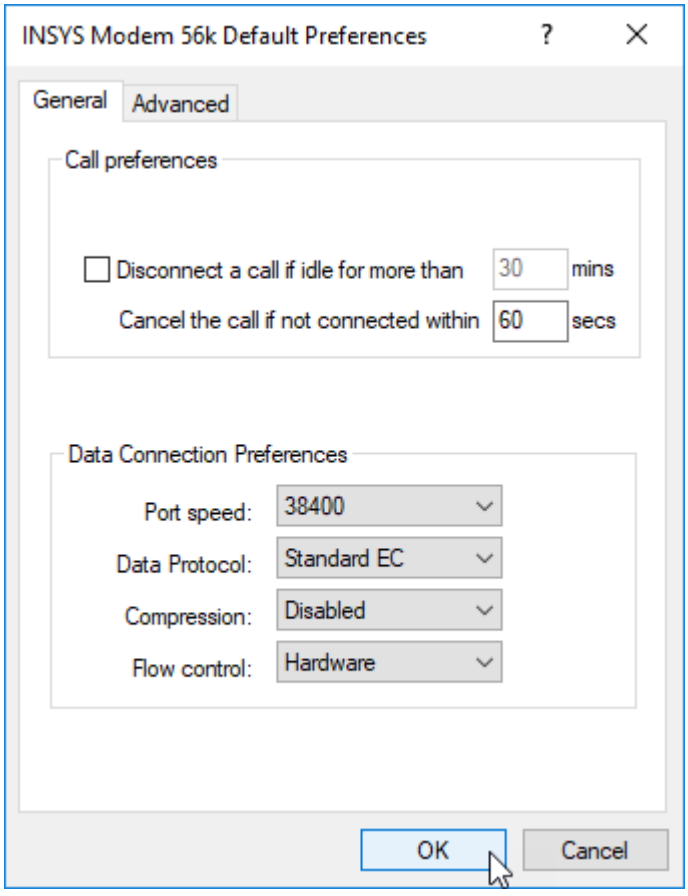


[sc_Modem_Properties_Advanced, 2, en_US]

Figure A-13 Changing Modem Default Preferences

✧ Select the **Advanced** tab and click **Change Default Preferences...**.

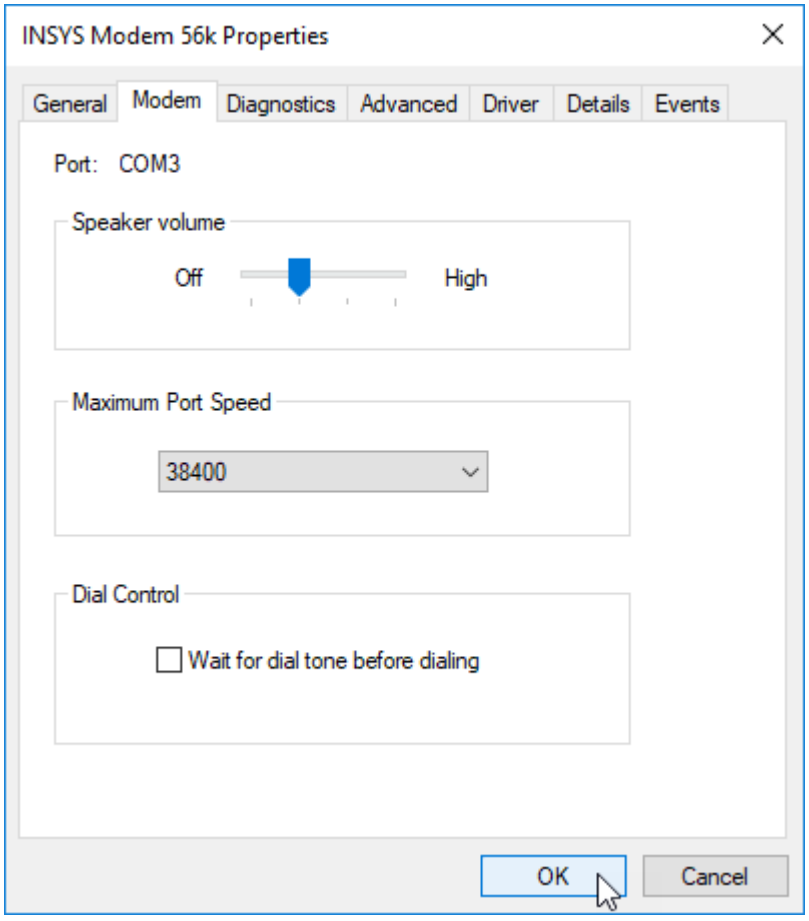
The **INSYS Modem 56k Default Preferences** dialog opens.



[sc_Change_Modem_Preferences, 2, en_US]

Figure A-14 Defining the Modem Parameters

- ✧ In the **General** tab, select the following settings:
  Port speed: **38400**
  Compression: Disabled
- ✧ Click **OK** to confirm your settings.
- ✧ Open the **Modem** tab.



[sc_Modem_Parameters, 2, en_US]

Figure A-15 Defining the Modem Parameters

- ✧ Change the **Maximum Port Speed** to **38400**.
- ✧ Deselect **Wait for dial tone before dialing**.
- ✧ Click **OK** to confirm your settings
- ✧ Close the **Device Manger**.

The modem of the SICAM PAS/PQS station computer is now installed and configured.

NOTE

If the modem/ISDN card is also used by other programs, these programs must be disabled before SICAM PAS/PQS communicates via this card. Otherwise, these programs might cause communication problems.

Setting up a Modem Connection (TAPI Interface) in SICAM PAS/PQS

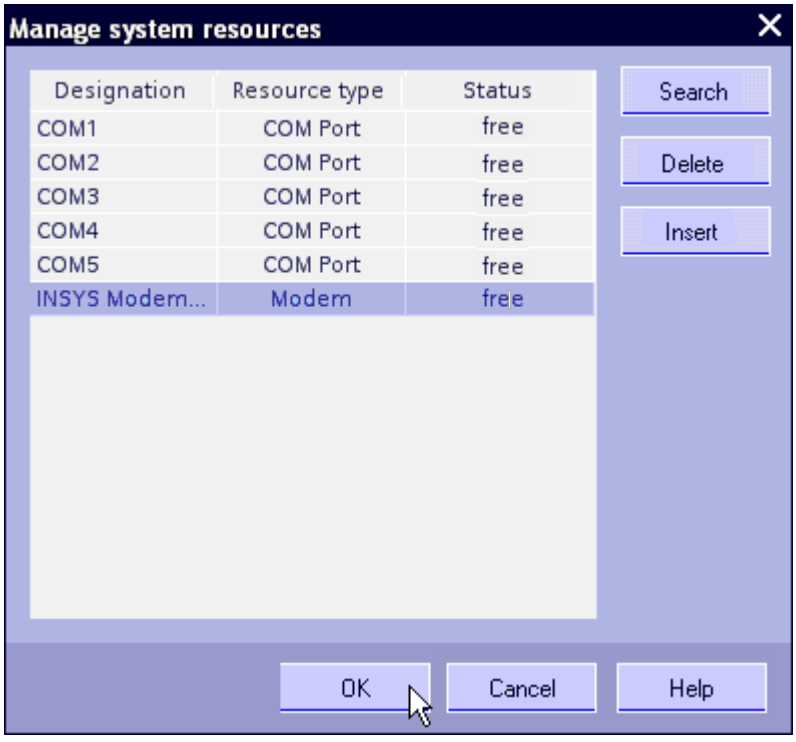
A **SIMEAS R Master** application **must be inserted in SICAM PAS/PQS UI – Configuration**.

Below the application, you must insert and parameterize an interface and a device for the modem. The device corresponds to the modem. A **system resource** is required for the interface.

For more detailed information on SICAM PAS/PQS UI – Configuration, refer to */4/ SICAM PAS/PQS, Configuration and Operation*.

Inserting a System Resource

- ✧ In **SICAM PAS/PQS UI – Configuration**, select the **Configuration** view.
- ✧ Insert the installed **INSYS Modem 56k** as a system resource of the **Modem** type in the system.

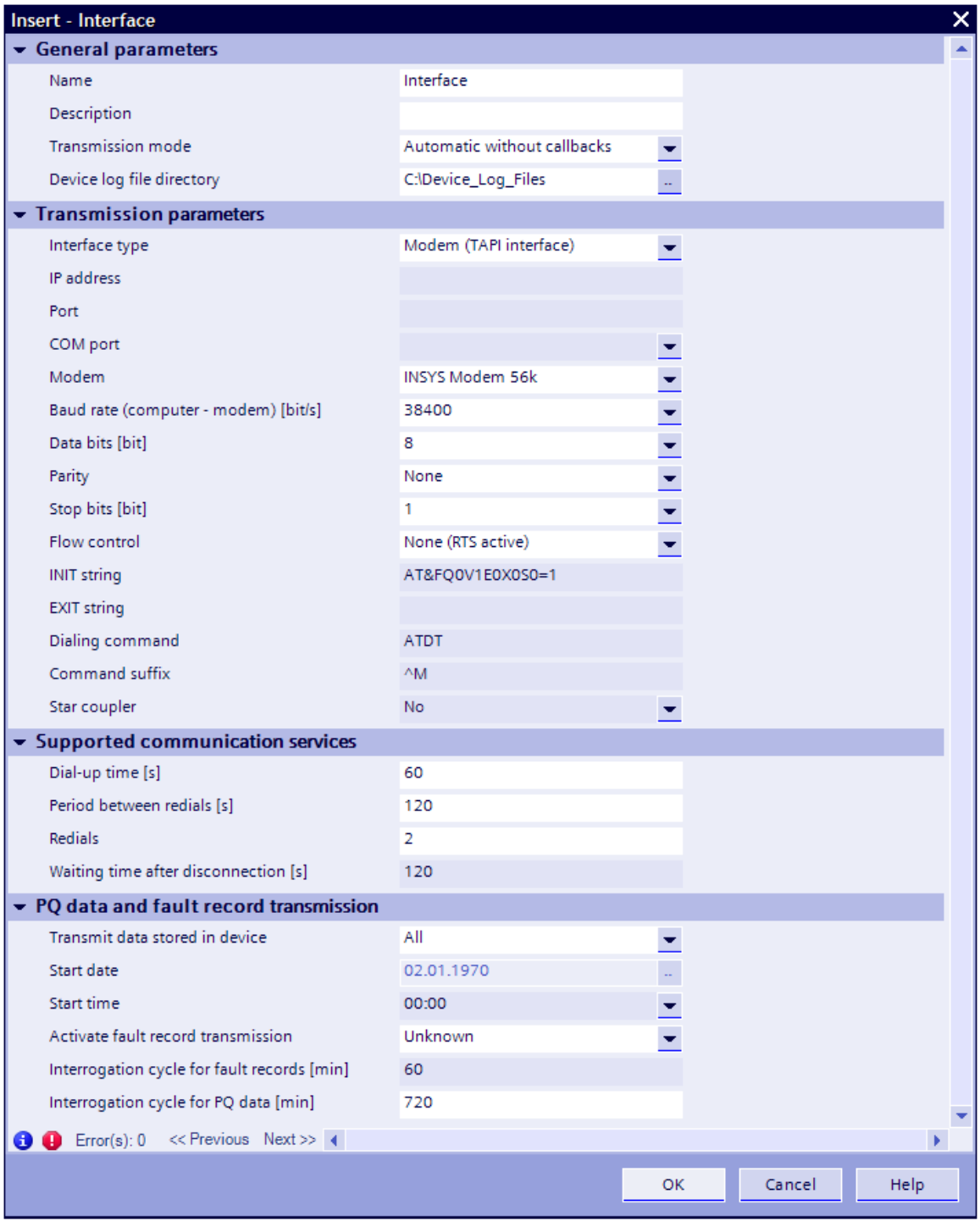


[sc_Insert_System_Resource_TAPI, 1, en_US]

Figure A-16 Inserting a System Resource

Inserting an Interface

✧ Select the **SIMEAS R Master** application and from the context menu, insert an **interface** for the modem.



[sc_Interface_Parameters_Definition_TAPI, 2, en_US]

Figure A-17 Defining Interface Parameters

- ✧ Enter the path of the **Device log file directory**.
- ✧ Select **Modem (TAPI interface)** from the interface type list box.
- ✧ Select **INSYS Modem 56k** from the modem list box.
- ✧ Define the **38400** baud rate.

NOTE

The definable **Baud rate** depends on the individual modem and the transmission line type.

✧ Under **Transmission parameters**, define **8 data bits** and **1 stop bit**.

✧ Check all other parameters.

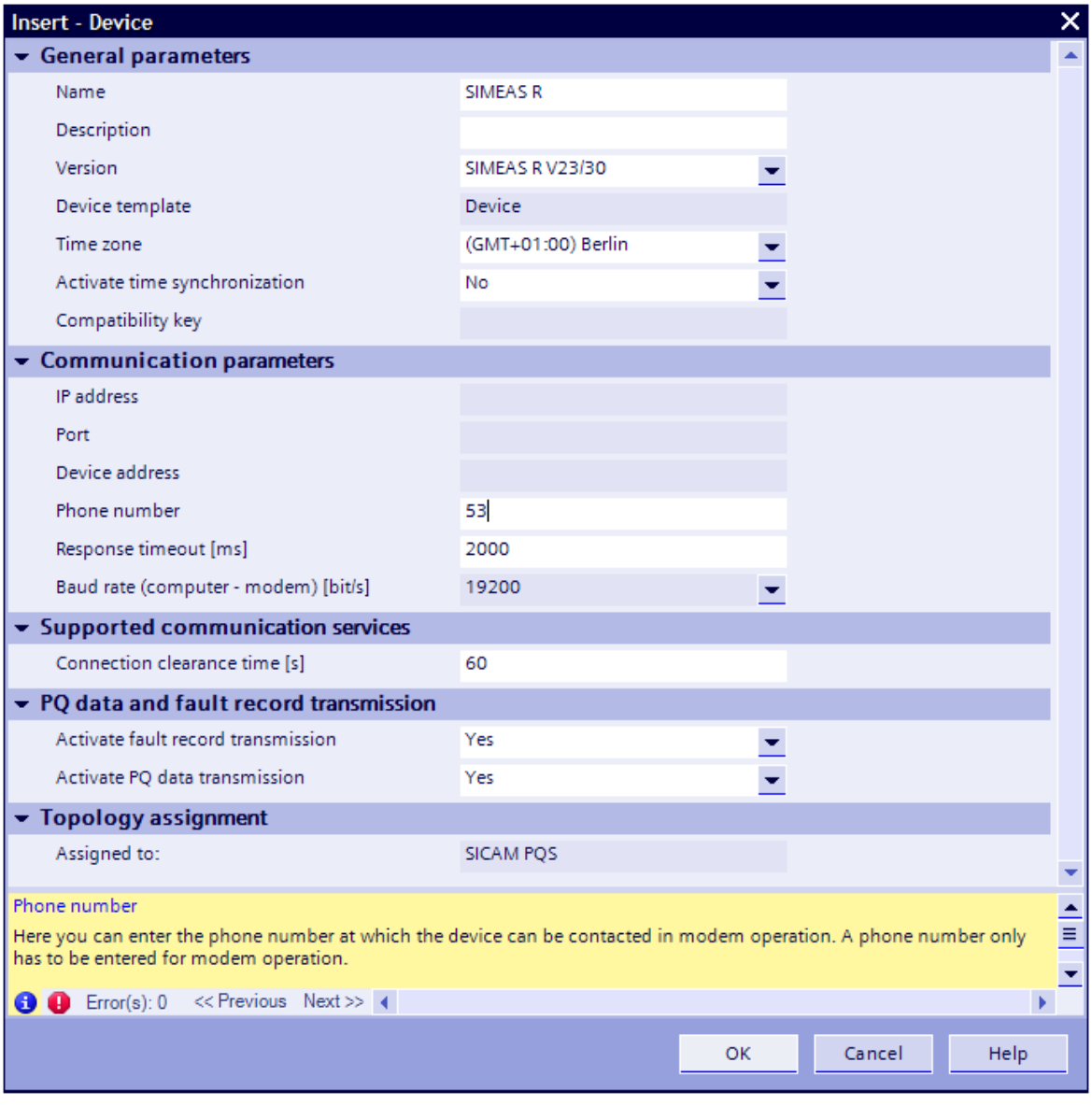
For the parameter description and their default values, refer to the online help.

✧ Click **OK** to close the dialog.

Inserting a Device

✧ Insert a device below this interface.

The device corresponds to the SIMEAS R device to be contacted via the dial-up connection.



[sc_Device_Parameters_Definition_TAPI, 1, en_US]

Figure A-18 Defining the Device Parameters

✧ Under **Communication parameters**, enter the **Phone number** under which the SIMEAS R device can be contacted later.

✧ Define all other parameters.

✧ Click **OK** to close the dialog.

Setting up a Modem Connection in SIMEAS R PAR

The transmission of parameters and measured data of a SIMEAS R-PMU device is carried out by a modem that is connected to the serial data interface on the back of the device.

With a SIMEAS R device V21/V23/V30, you can use an external modem as well as an internal modem (PCMCIA card).

For the initial setup of a device, connect the service interface on the front of the devices to the serial interface of the computer. The external modem does not need to be connected to the SIMEAS R device for parameterization.

For more detailed information on **SIMEAS R PAR** refer to */16/ SIMEAS R PAR, Parameterization Tool*.

To parameterize the data interface for the modem connection in SIMEAS R PAR:

✧ In **SICAM PAS/PQS UI – Configuration** in the **Configuration** view, select the **SIMEAS R** device and select **Open** from the context menu.

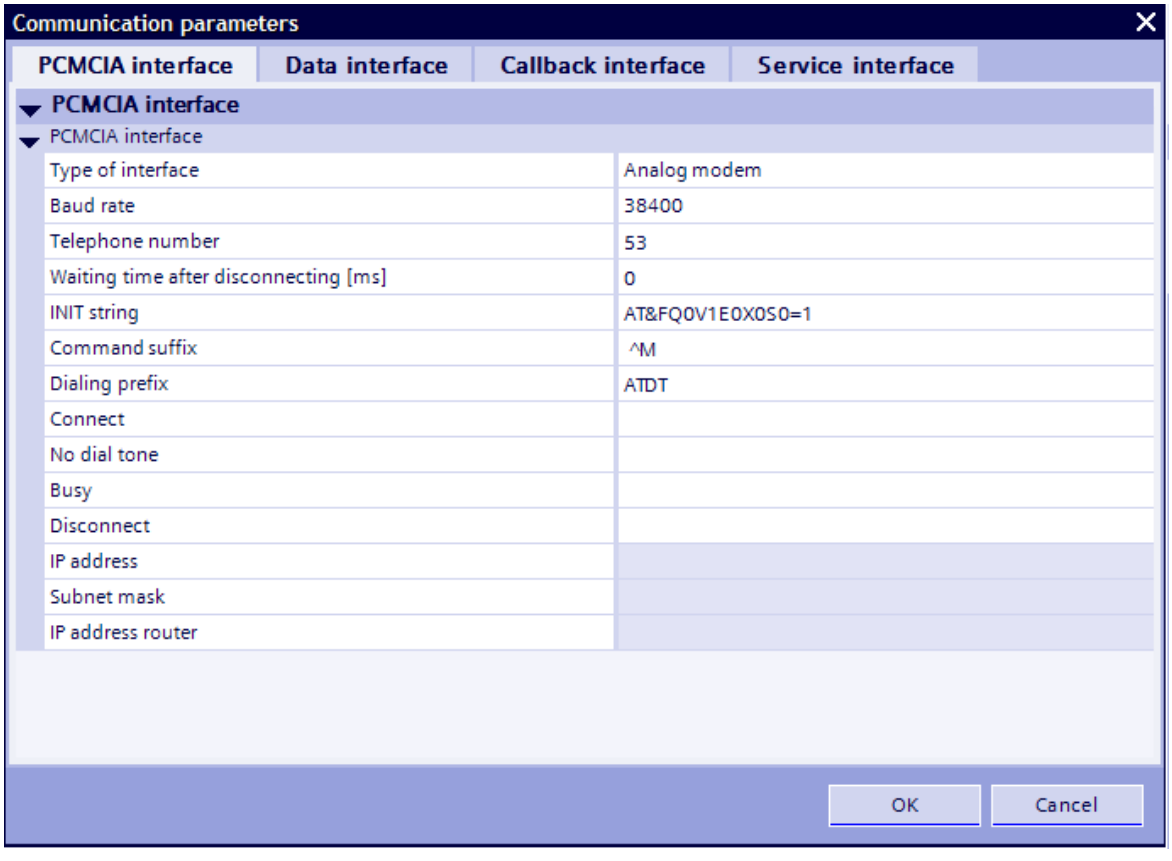
SIMEAS R PAR opens.

✧ Load the set of parameters from the device.

✧ Select **Device > Communication parameters...**.

The **Communication parameters** dialog opens.

✧ If you use an internal modem (PCMCIA), select the **PCMCIA interface** tab.
Using an external modem the settings are defined in the **Data interface** tab.



[sc_PCMCIA_Interface_Definition, 1, en_US]

Figure A-19 Defining the PCMCIA Interface (Internal Modem)

✧ From the **Type of interface** list box, select **Analog modem**.

- ✧ Enter the **Telephone number** under which the SIMEAS R modem can be contacted.
  This phone number is for information purposes only.
- ✧ Define the **Baud rate 38400**.
  The baud rate must be identical with the baud rate of the modem of the SICAM PAS/PQS station computer.
- ✧ Enter the **INIT string AT&FQ0V1E0X0S0=1**.
  The individual elements of the **INIT** string have the following meaning:
  AT: Attention - Start of each command sequence
  &F: Loading the factory default settings - the following elements can overwrite the factory default settings
  Q0: Modem messages are reported
  V1: Modem returns text messages in long form, such as "Connect" or "OK"
  E0: Echo off – does not return received AT commands (no mirroring)
  X0: Blind dialing – does not consider dial tone
  S0=1: Use the first ring to start the establishing of the connection. The value must be greater than or equal to 1, otherwise the SIMEAS R device does not establish a connection.
- ✧ Enter **^M** as **Commandsuffix**.
  ^M stands for <CR>.
- ✧ Click **OK** to close the dialog.
- ✧ Load the set of parameters into the device via the **Parameterset > Send to device...** menu item.
- ✧ Close SIMEAS R PAR.

NOTE

Connect the external modem to the SIMEAS R device at the place of destination and restart it. The modem is initialized during the restart.

A.6 Modem via COM Port (Hayes Compatible)

Perform the following steps one after the other:

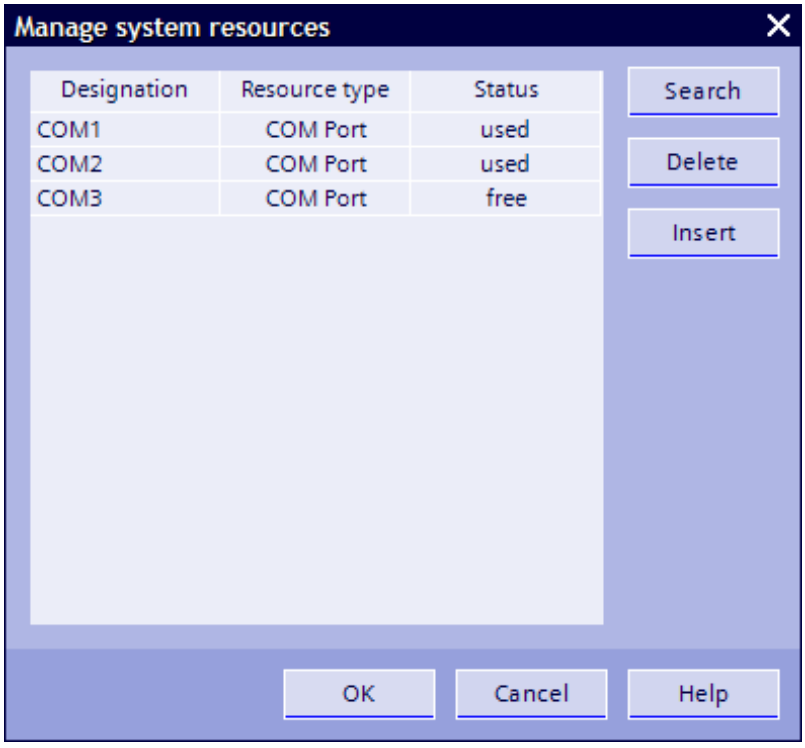
- *Setting up a Modem Connection (Hayes Compatible) in SICAM PAS/PQS, Page 119*
- *Setting up a Modem Connection in SIMEAS R PAR, Page 123*

Setting up a Modem Connection (Hayes Compatible) in SICAM PAS/PQS

A **SIMEAS R Master** application **must be inserted in SICAM PAS/PQS UI – Configuration**.
Below the application, you must insert and parameterize an interface and a device for the modem. The device corresponds to the modem. A **system resource** is required for the interface.
For more detailed information on SICAM PAS/PQS UI – Configuration, refer to */4/ SICAM PAS/PQS, Configuration and Operation*.

Inserting a System Resource

- ✧ In **SICAM PAS/PQS UI – Configuration**, select the **Configuration** view.
- ✧ As a system resource insert an interface of the **COM Port** type to which the Hayes compatible modem is connected.

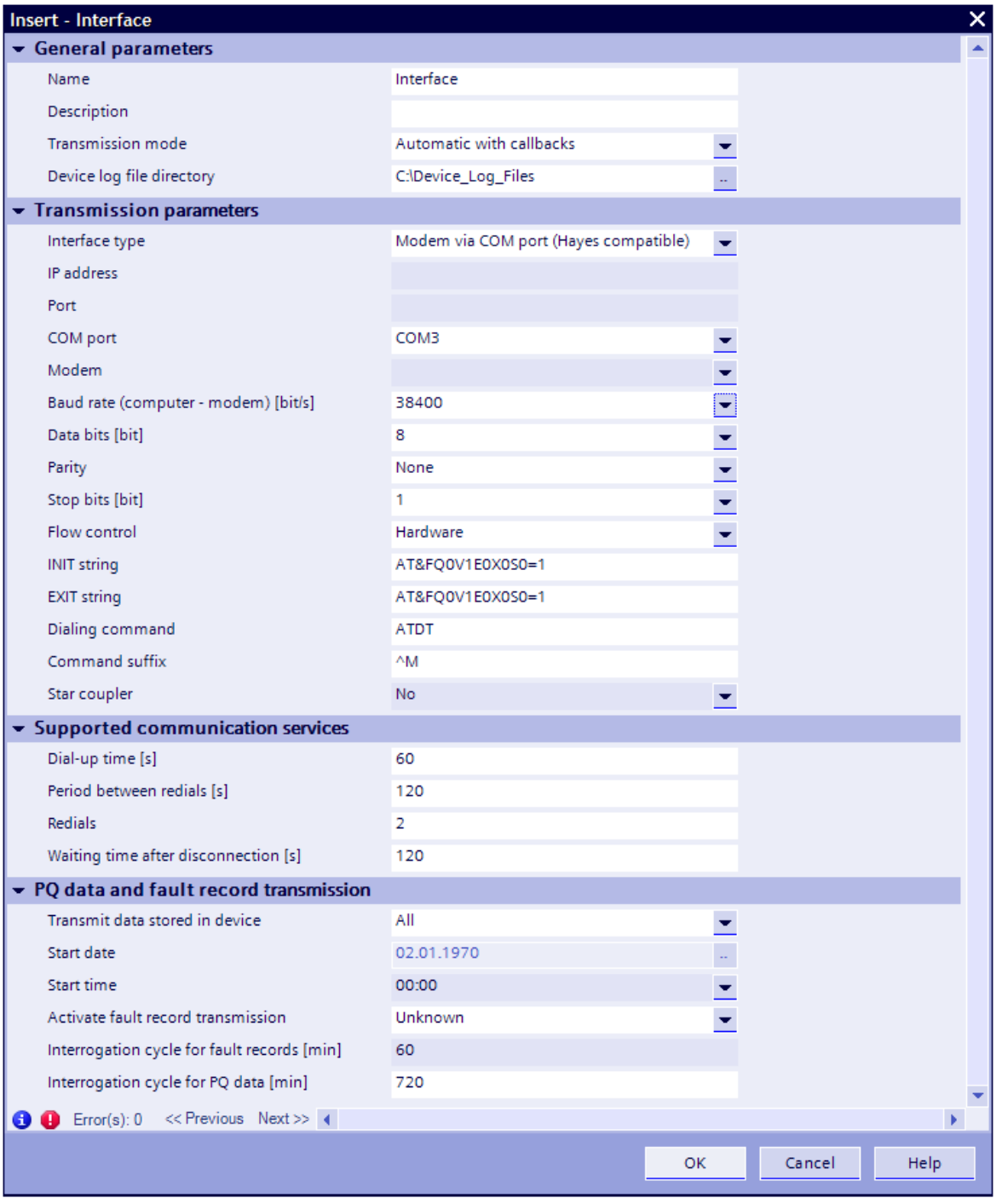


[sc_Insert_System_Resource, 2, en_US]

Figure A-20 Inserting a System Resource

Inserting an Interface

✧ Select the **SIMEAS R Master** application and from the context menu, insert an **interface** for the modem.



[sc_Interface_Parameters_Definition, 2, en_US]

Figure A-21 Defining Interface Parameters

- ✧ Select the **Transmission mode**.
- ✧ Enter the path of the **Device log file directory**.
- ✧ Select the **Modem via COM Port (Hayes-compatible)** from the interface type list box.
- ✧ Select the **COM port** to which the modem is connected.
- ✧ If you have selected the **Automatic with callbacks** transmission mode, you select under **Baud rate (computer - modem) [bit/s]** the highest common baud rate, which is supported by all the modems connected to this interface..

NOTE

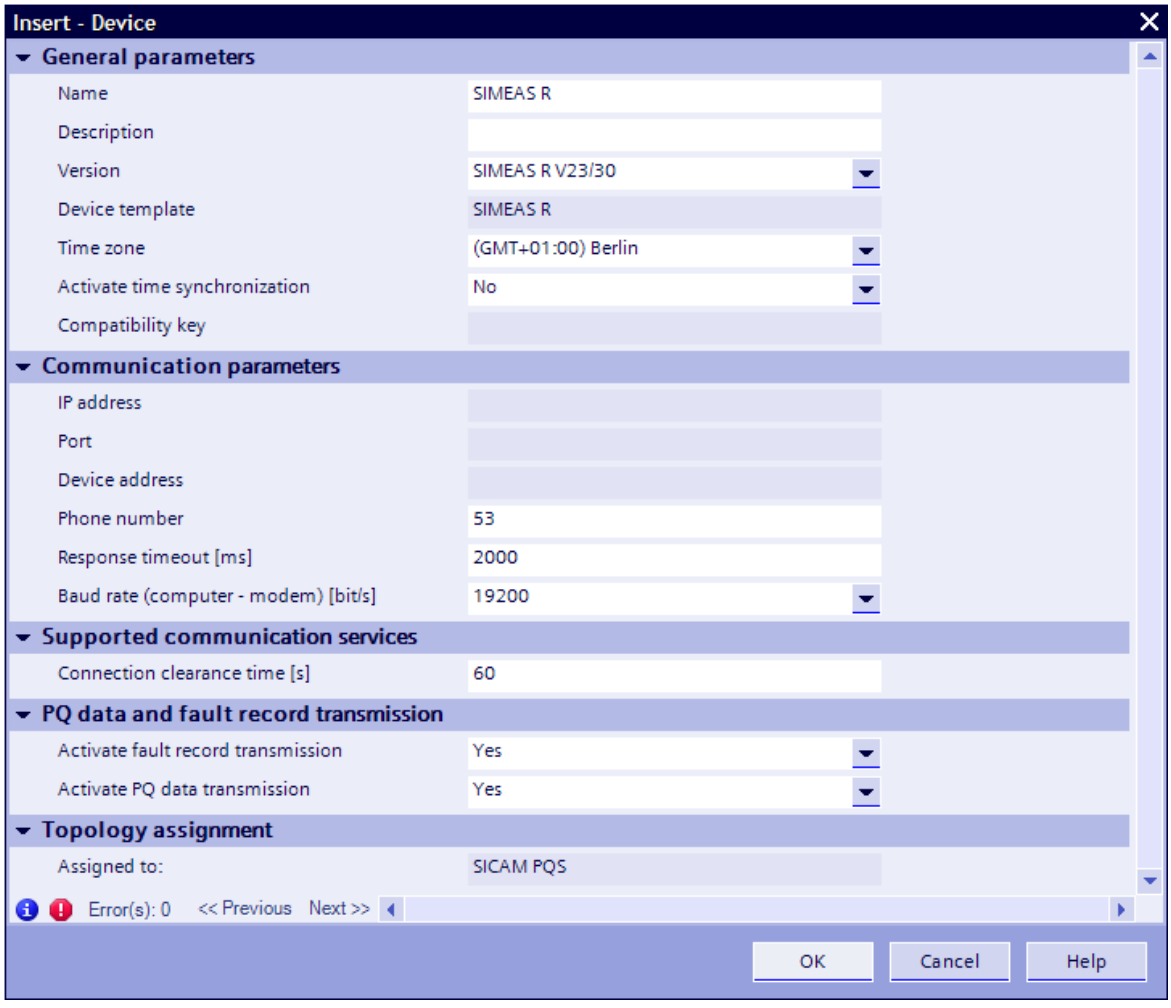
The definable **Baud rate** depends on the individual modem and the transmission line type.

- ✧ Define **8 data bits** and **1 stop bit**.
- ✧ Select **Hardware** from the flow control list box.
- ✧ Enter the **AT&FQ0V1E0X0S0=1 INIT** string.
- ✧ Enter an EXIT string, for example **AT&FQ0V1E0X0S0=1**. The EXIT string is used for communication of the modem after disconnection.
- ✧ Check all other parameters.
  For the parameter description and their default values, refer to the online help.
- ✧ Click **OK** to close the dialog.

Inserting a Device

- ✧ Insert a **device** below this interface.

The device corresponds to the SIMEAS R device to be contacted via the dial-up connection.



[sc_Device_Parameters_Definition, 2, en_US]

Figure A-22 Defining the Device Parameters

- ✧ Under **Communication parameters**, enter the **Phone number** under which the SIMEAS R device can be contacted later.

✧ Check all other parameters.
For the parameter description and their default values, refer to the online help.

✧ Click **OK** to close the dialog.

Setting up a Modem Connection in SIMEAS R PAR

The transmission of parameters and measured data of a SIMEAS R-PMU device is carried out by a modem that is connected to the serial data interface on the back of the device.

With a SIMEAS R device V21/V23/V30, you can use an external modem as well as an internal modem (PCMCIA card).

For the initial setup of a device, connect the service interface on the front of the devices to the serial interface of the computer. The external modem does not need to be connected to the SIMEAS R device for parameterization.

For more detailed information on **SIMEAS R PAR** refer to */16/ SIMEAS R PAR, Parameterization Tool*.

To parameterize the data interface for the modem connection in SIMEAS R PAR:

✧ In **SICAM PAS/PQS UI – Configuration** in the **Configuration** view, right-click the **SIMEAS R** device and select **Open** from the context menu.

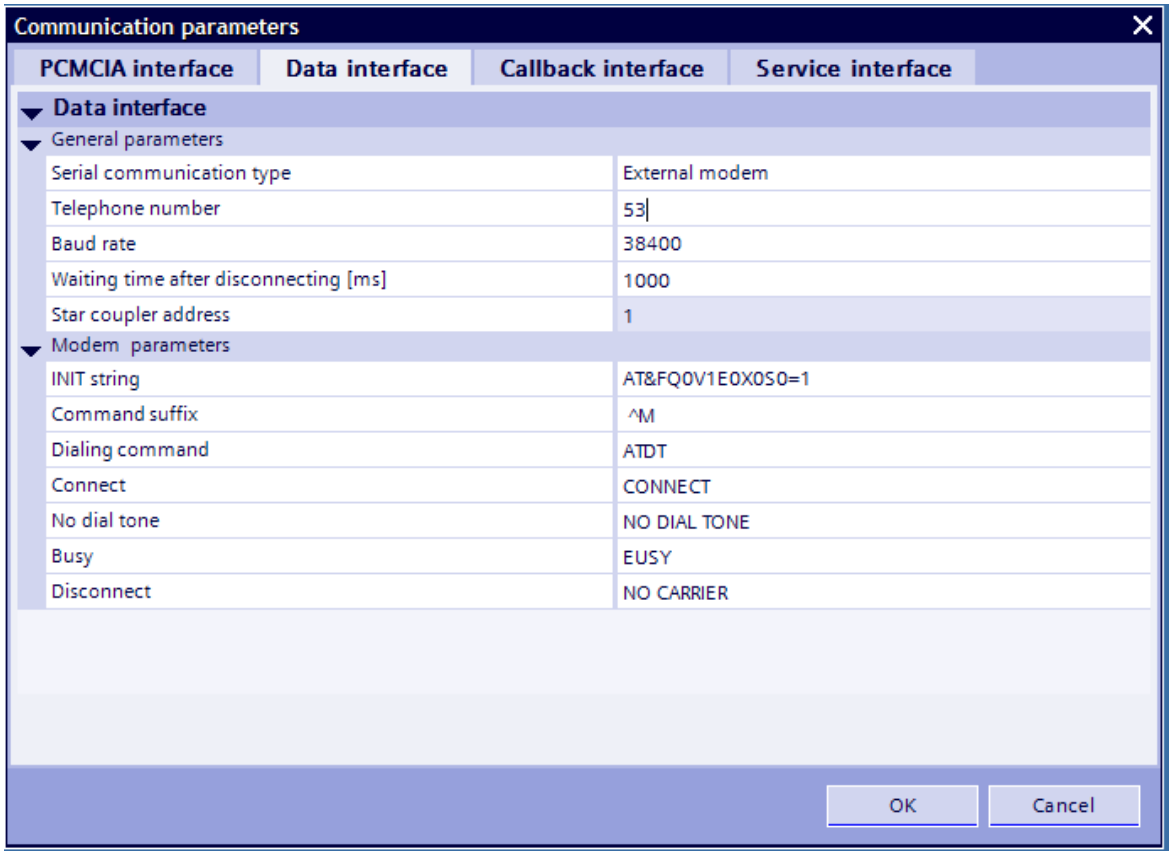
SIMEAS R PAR opens.

✧ Load the set of parameters from the device.

✧ Select **Device > Communication parameters...** .

The **Communication parameters** dialog opens.

✧ If you use an external modem, select the **Data interface** tab.
Using an internal modem (SIMEAS R V21/V23/V30 only) the settings are defined in the **PCMCIA interface** tab.



[sc_Data_Interface_Definition, 1, en_US]

Figure A-23 Defining the Data interface (External Modem)

- ✧ From the **Serial communication type** list box, select **External modem**.
- ✧ Enter the **Telephone number** under which the SIMEAS R modem can be contacted.
  This phone number is for information purposes only.
- ✧ Define the **Baud rate 38400**.
  The baud rate must be identical with the baud rate of the modem of the SICAM PAS/PQS station computer.
- ✧ Enter the **INIT string AT&FQ0V1E0X0S0=1** .
  The individual elements of the INIT string have the following meaning:
  AT: Attention - Start of each command sequence
  &F: Loading the factory default settings - the following elements can overwrite the factory default settings
  Q0: Modem messages are reported
  V1: Modem returns text messages in long form, such as "Connect" or "OK"
  E0: Echo off – does not return received AT commands (no mirroring)
  X0: Blind dialing – does not consider dial tone
  S0=1: Use the first ring to start the establishing of the connection. The value must be greater than or equal to 1, otherwise the SIMEAS R device does not establish a connection.
- ✧ Enter **^M** as **Commandsuffix**.
  ^M stands for <CR>.
- ✧ Click **OK** to close the dialog.
- ✧ Load the set of parameters into the device via the **Parameterset > Send to device...** menu item.
- ✧ Close **SIMEAS R PAR**.

NOTE

Connect the external modem to the SIMEAS R device at the place of destination and restart it. The modem is initialized during the restart.

A.7 Working with the Multilanguage Manager Tool

The Multilanguage Manager tool can be used for the translation of the SICAM PAS/PQS user interface and runtime language. The repository with the translated texts is deployed to the installed product.
To perform the translation, proceed as follows:

- Install SICAM PAS/PQS on a seperate computer for translation.
- Open the Multilanguage Manager tool, refer to *Starting the Multilanguage Manager Tool, Page 125*.
- Create a new language repository by using the existing reference language and make the necessary changes in the target language.
- Save the repository.
- To check your translation, create a project in SICAM PAS/PQS.
- Copy the repository to all computers (Full Server, DIPs, redundant systems).
- Open the Multilanguage Manager tool to deploy the repository.
- Set the new language in SICAM PAS/PQS on all computers.

Installation

The Multilanguage Manager tool is installed along with the installation of SICAM PAS/PQS or SICAM PQ Analyzer.

NOTE

The Multilanguage Manager tool needs no licensed version of SICAM PAS/PQS. However, to create a project for checking the translation, SICAM PAS/PQS must be installed as demo version or as licensed version.

Starting the Multilanguage Manager Tool

Operating System	Path
Windows 7	Select **Start** > **All Programs** > **Siemens** > **SICAM** > **PAS/PQS** > **Tools** > **Multilanguage Manager**
Windows 8.1	Double-click **Multilanguage Manager** from the **SICAM PAS/PQS** > **Tools** folder on the desktop.
Windows 10	Select **Start** > **All Apps** > **SICAM PAS/PQS**[7] > **Tools** > **Multilanguage Manager**.

Creating a New Language Repository

This feature allows you to use the existing reference language and translate the texts into the desired language. You can make the necessary changes to the target language texts before you save the repository.
The translation status has the following representations:

Status Icon	Description
	Requires translation
	Modified
	Error
	Translated

The repository is saved to a file with **.LRP** format. The default name for the repository is **<product name>_<product version>_<new language name>_<new language locale>.LRP**.
The default storage location is **%publicdocuments%Siemens\LanguageRepositories**.

Opening and Editing an Existing Repository

This feature allows you to open an existing repository (**.LRP** file). You can view the language texts that require translation, edit the target language texts, and save the repository. The translation status is displayed appropriately.

Upgrading an Existing Repository

This feature allows you to upgrade an existing repository created from earlier versions to the current version so that the available texts and the newly added texts can be translated.

NOTE

You can open the existing repository for an upgrade when the reference language is available in the installed directory and the operating system supports the locale of the repository.

The upgrade repository operation is product specific. For example, you can upgrade the repository created from an earlier version of SICAM PAS only if the latest version of SICAM PAS is installed on the system. To upgrade an earlier translated version to the current version, open the repository for an upgrade and save it with the default name or with the new name.

7 SICAM PQ Analyzer, if SICAM PQ Analyzer has been installed first

Deploying an Existing Repository

This feature allows you to deploy an existing language repository with the same version as the installed SICAM products. You can use the new deployed language in the user interface and/or runtime. The deploy operation creates a new language folder or overwrites the existing language folder (only if the **new language name** and the **new language locale** match) in the product environment, except for English and German languages.

The deployed language is now available in the language setting dialogs.

NOTE

Before you deploy the language repository, close all the SICAM system components on the target system.

For deploying the language files to the installed product, you must run the tool as an administrator.

Ensure that the deployed language is same in Full Server, DIPs, and the redundant system.

A.8 Licensing - General Information

Software Protection for SICAM PAS/PQS

The SICAM PAS/PQS features are distributed among several software modules, most of which are optional. In order to facilitate the installation of the SICAM PAS/PQS software, the software modules of the basic system and all optional features are available on the DVD included in the scope of delivery.

Which functions can be used for a system is determined by:

- Dongle with the feature-specific license keys
  – or –
- Soft License

Dongle

For the basic system (licensed version) you require a dongle which enables optional features via license keys. These license keys only apply to a single dongle. If you purchase several SICAM PAS/PQS you receive a separate kit including one dongle for each computer together with the corresponding license keys.

Before SICAM PAS/PQS software components start up they verify that the license key you entered matches the information in the dongle. During operation the system checks at regular intervals whether the dongle is still present.

If the dongle is missing or removed during operation, the feature for which no license key has been found will be disabled after approximately 5 minutes.

If the system has been running for at least 21 days it will run for another 14 days after the first dongle failure. During this time, dongle errors are ignored (password mismatches are not ignored). You can configure that a message will be transmitted to the control center in case of a dongle error. This ensures that you can order a new dongle if the existing one fails while the system is still running.

Soft License

A computer or a virtualization solution is defined by a license status and the desired features are enabled and licensed for the system in combination with a product key.

The Soft License only applies to 1 system.

A.9 Feature Enabler

The following information is displayed in the Feature Enabler:

- All the features which must be enabled
- The status of the system features
- Dongle errors if the necessary dongle is not plugged or defective

The Feature Enabler serves for the following licensing tasks:

- Enabling the system with all features when using a Soft License
- Extending the system by:
  - Importing the license file when using a Soft License or a dongle for SICAM PAS/PQS V8.02 and later
    A.18 Importing the License File
  - Entering the license key when using a dongle for SICAM PAS/PQS V8.01 and earlier
    A.19 Using a Dongle to License a SICAM PAS/PQS System, V8.01 and Earlier

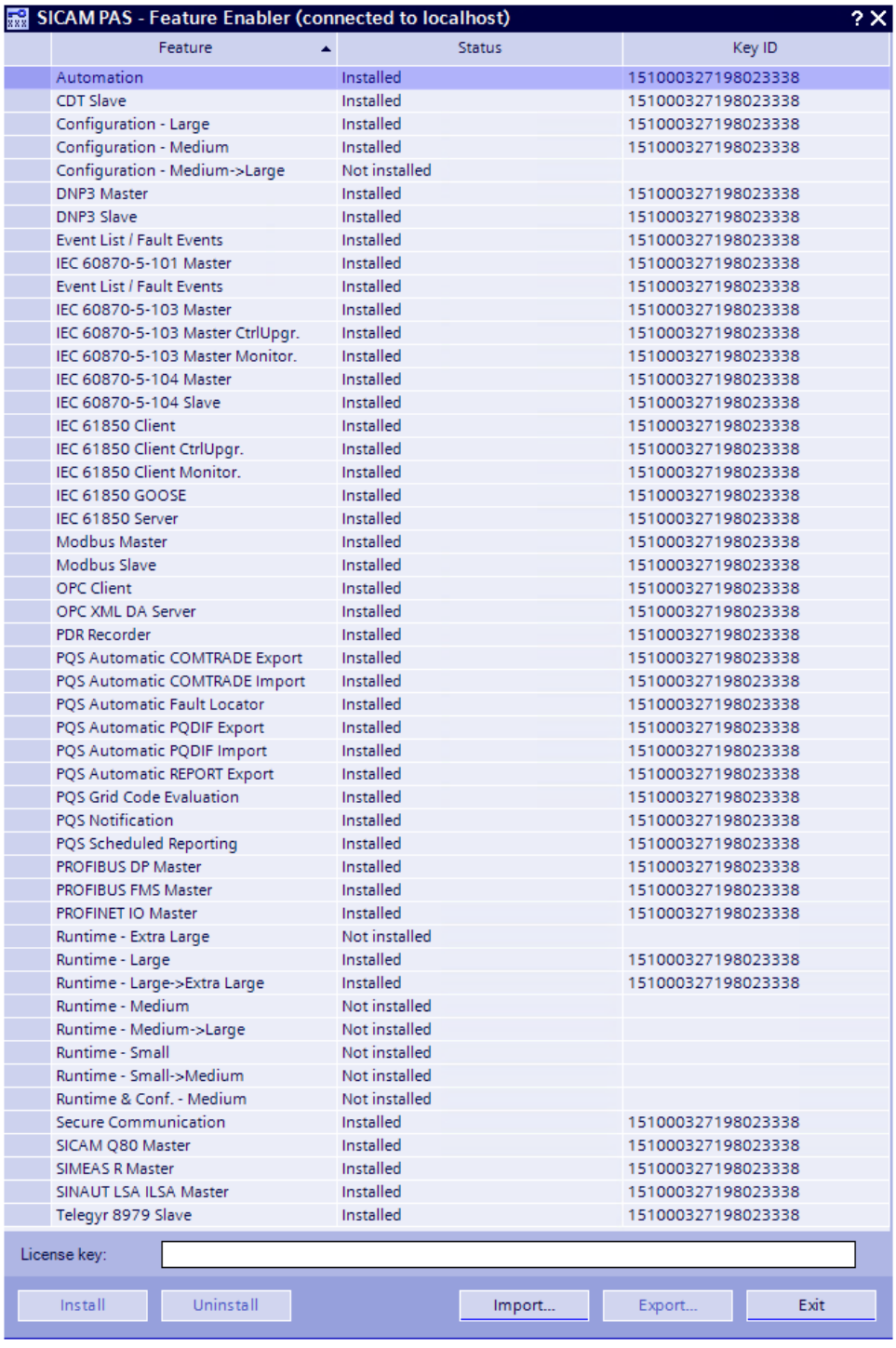
Starting the SICAM PAS/PQS – Feature Enabler

Start the Feature Enabler from the Windows Start menu.

✧ Select **Start** and scroll through the app list.

✧ Select **Feature Enabler** from the **SICAM PAS/PQS** folder.

The SICAM PAS/PQS – Feature Enabler opens.



[sc_Feature_Enabler_soft_license, 2, en_US]

Figure A-24 Feature Enabler, Status of all Features and Key ID

NOTE

When ordering additional features, you must specify the Key ID.

NOTE

For a distributed SICAM PAS/PQS system you must connect the DIP to the Full Server before enabling features on a DIP, see *A.20 Connecting the DIP to the Full Server*.

NOTE

If you use the **OPC Client** feature you must define further settings after the installation of your features.
For more detailed information see *6.2 Checking the Settings of the OPC Client* and *6.3 Setting up the OPC XML DA Server*.

A.10 Using a Dongle for Licensing

The dongle includes all the license keys ordered by the customer and enables the corresponding features.

NOTE

Since version V8.07, the **Runtime – Large** feature is limited to the use of 180 devices. The **Runtime – Extra Large** feature is required for a system configured for more than 180 devices. When performing an upgrade, the new **Runtime – Extra Large** feature is enabled instead of the **Runtime – Large** license.

Extending the System

If you extend the system by additional options you import a license file (V2C file) in the **Feature Enabler** which includes the licenses for the new features.

NOTE

With each extension of the license the counting index at the end of the file name is incremented by 1.
The license files must be imported without any gap in ascending order.

✧ Enable additional features in the **Feature Enabler**, see *A.18 Importing the License File*.

The dongle is extended by the imported features.

A.11 Using a Soft License for Licensing

NOTICE

Changing the computer configuration during the licensing process of the soft-license

The soft license becomes invalid.

✧ Once the licensing process has been started, do not perform any changes to the SICAM PAS/PQS computer which is to be licensed. This means, for example, that you must neither change any hardware, nor install any software, nor store/restore a backup file, before the license file has been imported via the Feature Enabler.

A.12 Software Licensing - General Information

An installed SICAM PAS/PQS system can be enabled and licensed via Internet using a product key.
The product key serves to enable the features ordered by the customer.

The system is enabled via the **SICAM PAS/PQS Soft License Manager** when entering the product key.

If the system is not connected to the Internet, it is defined by a license status file (C2V file). The features are enabled on a computer connected to the Internet.

The license file (V2C file) generated when enabling the features is imported in the **SICAM PAS/PQS Feature Enabler**. The system features are now enabled.

NOTE

Contact **Customer Support Center** in case the installed soft license needs to be transferred to another system.

Special Aspect to Be Considered for Installation on a Virtualization Solution

If you install SICAM PAS/PQS on a virtualization solution, perform the following steps after the setup:

- ✧ Open the **hasplm.ini** file in the **C:\Program Files (x86)\Common Files\Aladdin Shared\HASP** directory.
- ✧ Check the **bind_local_only = 0** entry. Change the value to **0** if required.
- ✧ Save the file.

NOTE

The license status file includes the fully qualified domain name (FQDN) of the specific computer for which you activate your system. Once the product key has been activated and the hostname or the domain name is changed afterwards, the soft license becomes invalid.

Opening the SICAM PAS/PQS Soft License Manager on a Computer with the System Installed

Start the SICAM PAS/PQS – Soft License Manager tool from the Windows Start menu:

- ✧ Select **Start** and scroll through the app list.
- ✧ Select **SICAM PAS/PQS > Tools**.

The **Tools** folder opens.

- ✧ Double-click **Soft License Manager**.

The **SICAM PAS/PQS – Soft License Manager** tool opens.

Opening the SICAM PAS/PQS Soft License Manager on a Computer without the System Installed

The Soft License Manager with the online help is located in the root directory of the **SICAM PAS/PQS** DVD in the **SoftLicenseMgr** directory.

- ✧ Copy the **SoftLicenseMgr** directory on the computer without a SICAM PAS/PQS installation.
- ✧ Open the **SoftLicenseMgr** directory and double-click the **SoftLicenseMgr.exe** file.

The Soft License Manager opens and the online help is available.

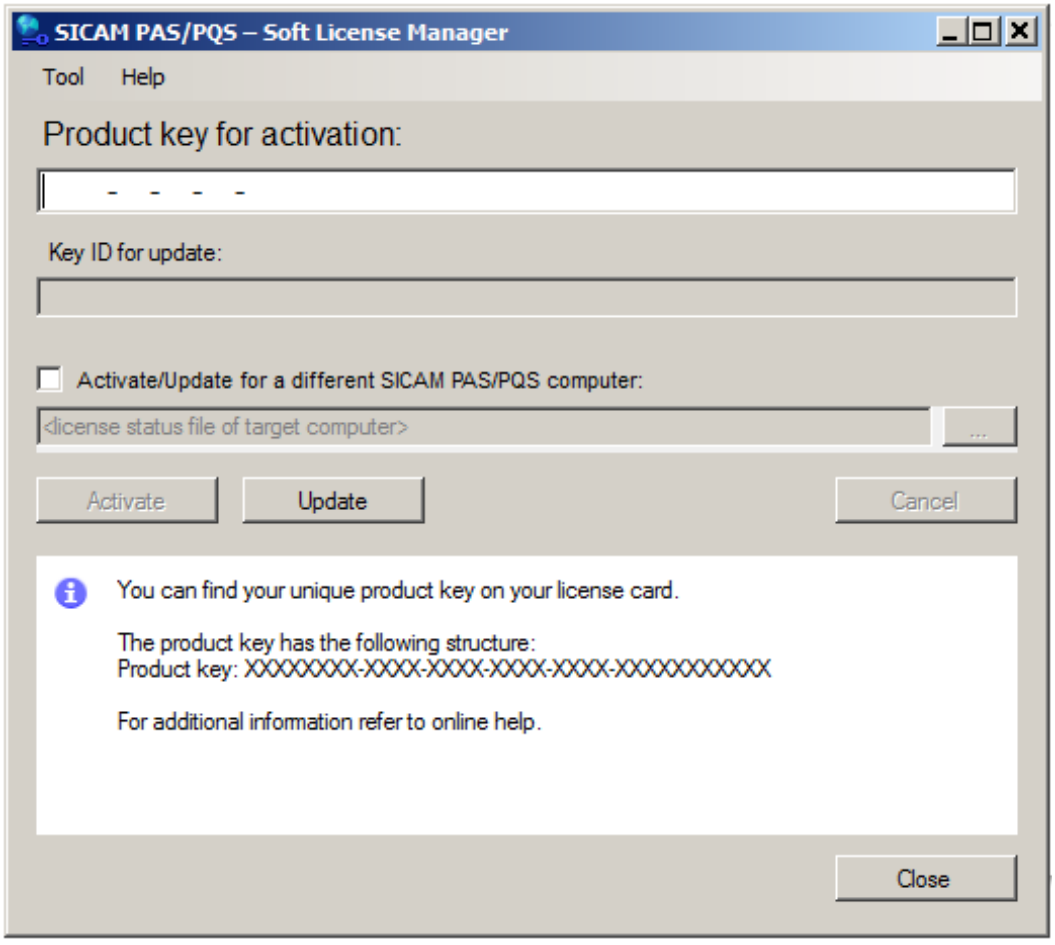
A.13 Licensing a System with Internet Access

The following steps must be performed in order to license a system **with** Internet access:

- Activating the product key
- Enabling the features

Activating the Product Key

- ✧ Install SICAM PAS/PQS.
- ✧ Start the Soft License Manager.



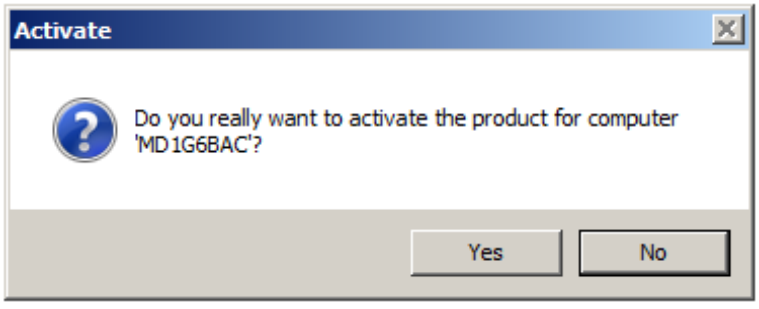
[sc_SLM_PAS_installed, 1, --_--]

Figure A-25 Soft License Manager with the System Installed

✧ In order to activate the product key enter the product key.
Once the product key has been entered, the **Activate** button is enabled.

✧ Click **Activate**.

The name of the computer for which the product key must be activated is displayed.



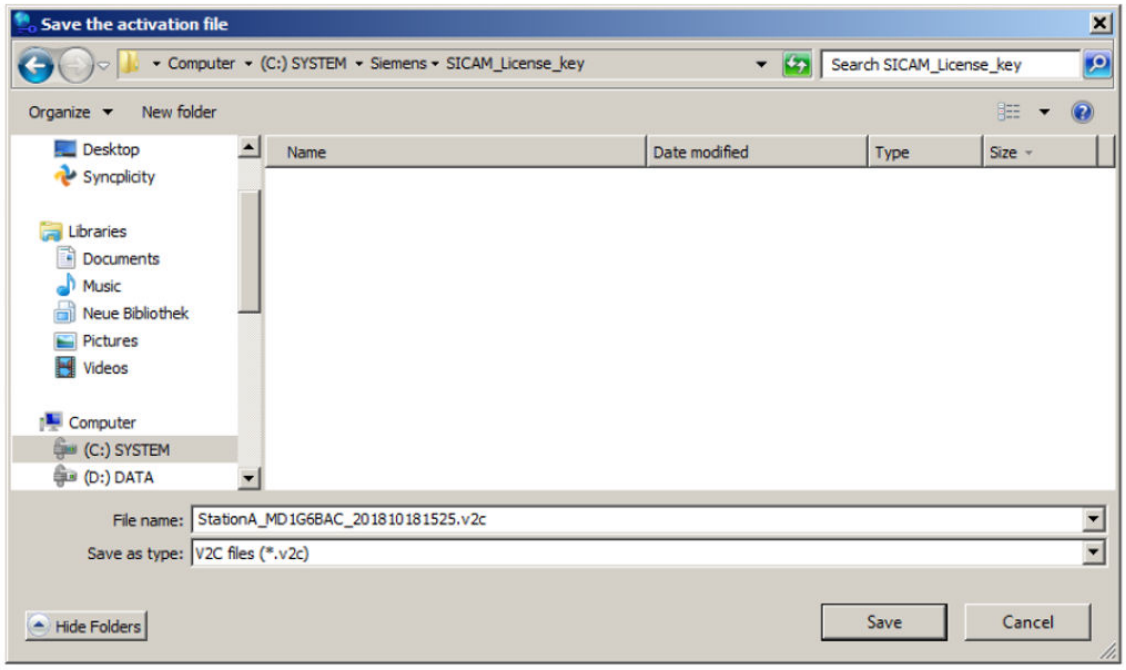
[sc_confirm_activation, 1, en_US]

Figure A-26 Confirmation Box

✧ Check the name of the computer for which you want to activate the product key.
The activation can neither be undone nor transferred.

- Click **No** to cancel the process.
- Click **Yes** to continue the activation.

The **Save the activation file** dialog opens after the activation.

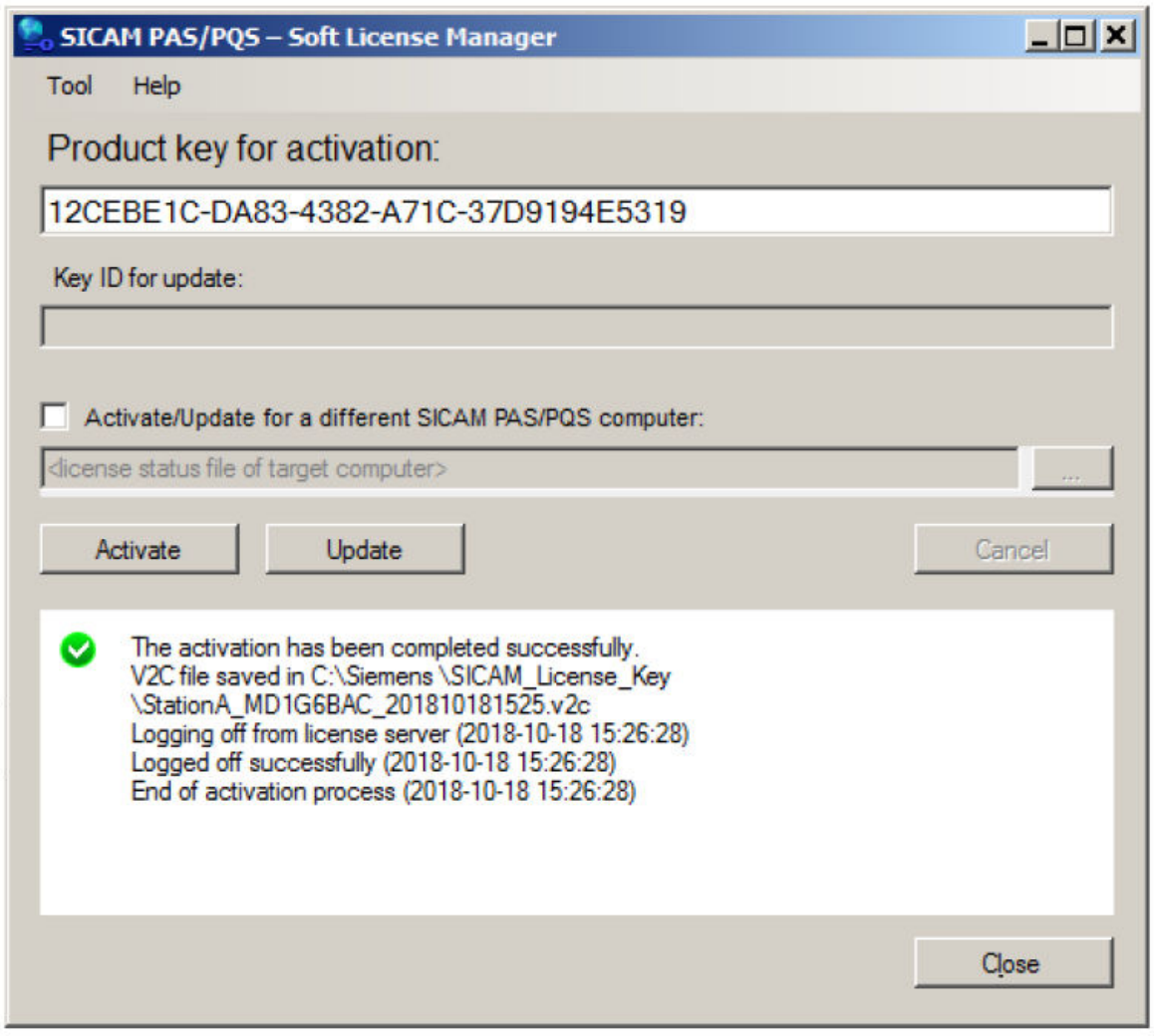


[sc_save_V2C_online, 3, en_US]

Figure A-27 Saving the License File

✧ Save the V2C license file with a unique name.

A message informs you that the activation has been successful.



[sc_system_activated_online, 3, --_--]

Figure A-28 Activation Completed

Enabling the Features

✧ Enable the features in the Feature Enabler, see *A.18 Importing the License File*.

A.14 Licensing a System without Internet Access

The following steps must be performed in order to license an installed system **without** Internet access:

- Creating a license status file for the system to be licensed (destination system)
- Activating the product key for the destination system on a computer **with** Internet access
- Enabling the features on the destination system using the Feature Enabler

Creating a License Status File

To create a license status file for the destination system on which SICAM PAS/PQS is installed:

✧ Start the Soft License Manager on the destination system.

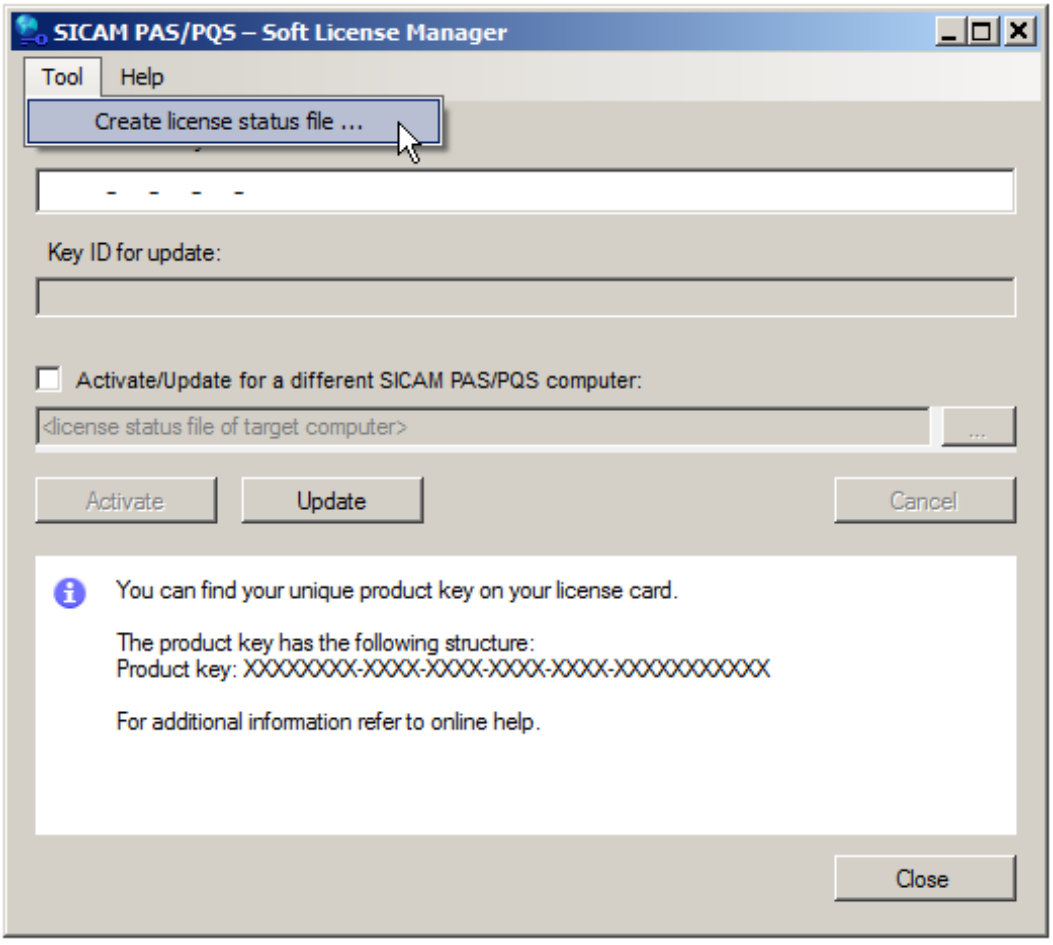
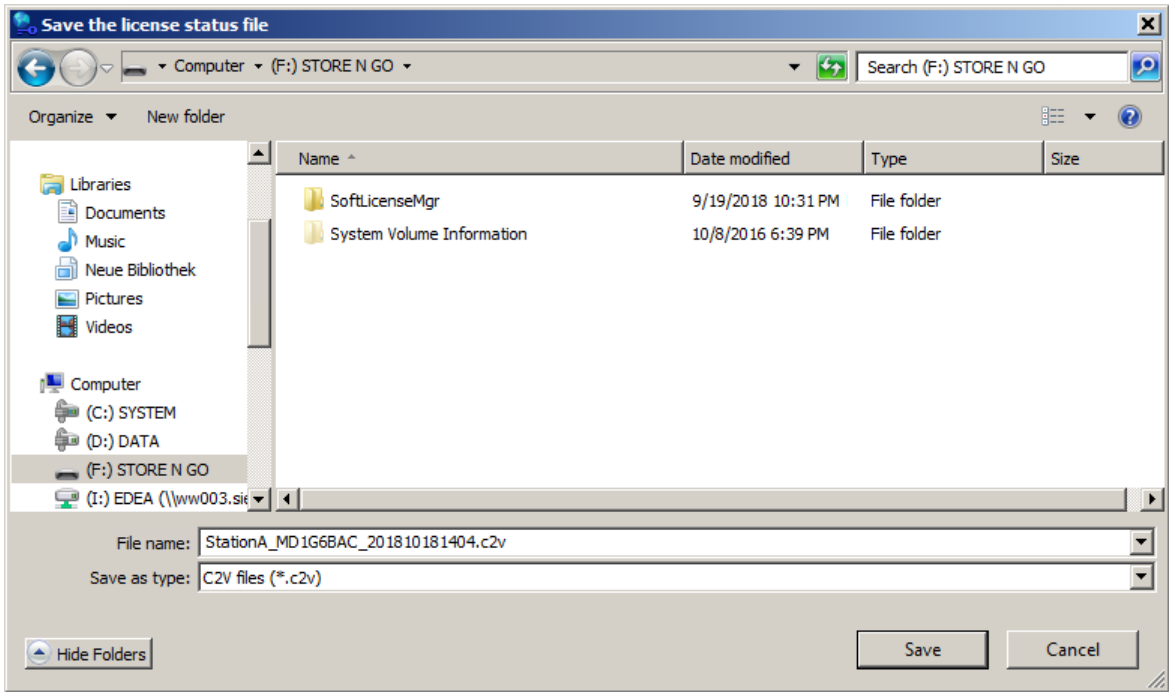


Figure A-29 Generating the License Status File

✧ Select **Create license status file...** from the **Tool** menu.

The **Save the license status file** dialog opens as soon as the license status file has been generated.



[sc_save_C2V, 2, en_US]

Figure A-30 Saving the License Status File

✧ Save the C2V license status file with a unique name.

NOTE

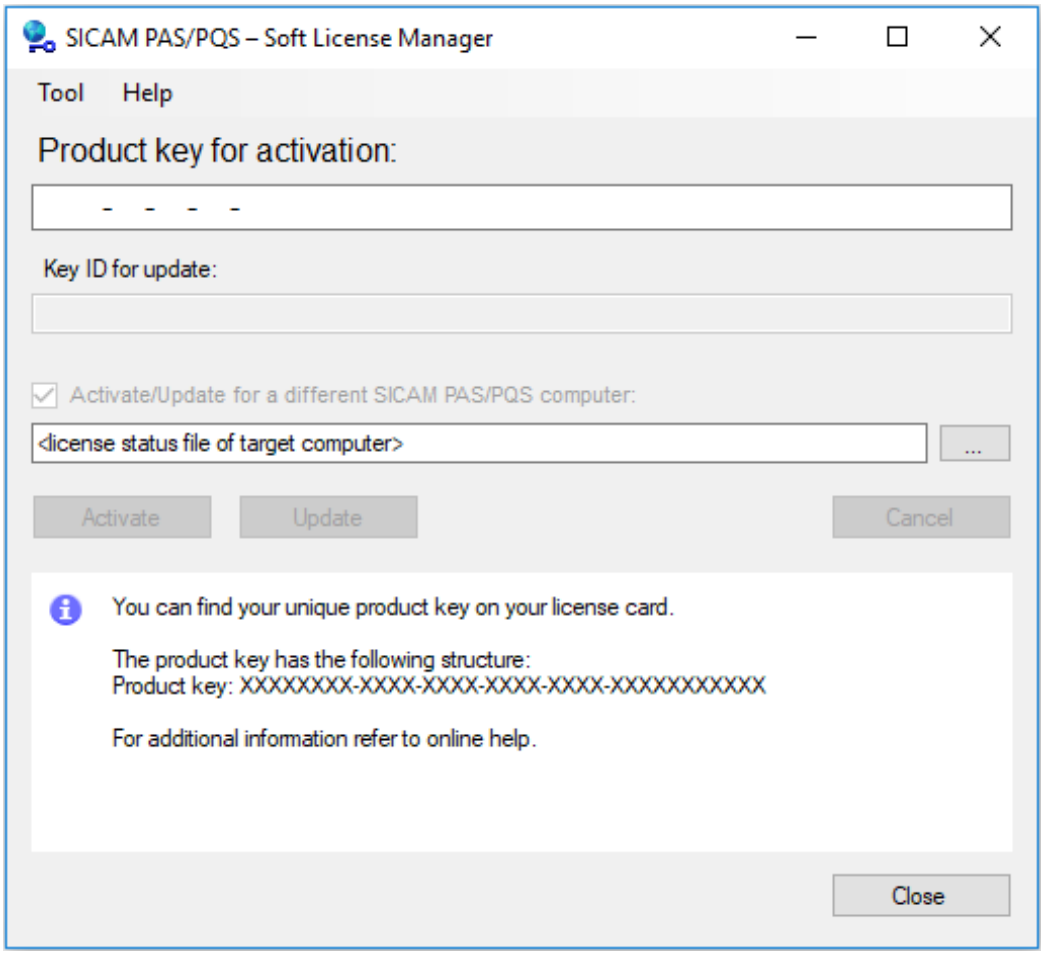
The C2V license status file is required in order to extend the Soft License on the computer with Internet access.

Activating the Product Key

✧ Change to a computer with Internet access.

✧ Transfer the C2V license status file.

✧ Start the Soft License Manager.



[sc_SLM_PAS_not_installed, 1, --_--]

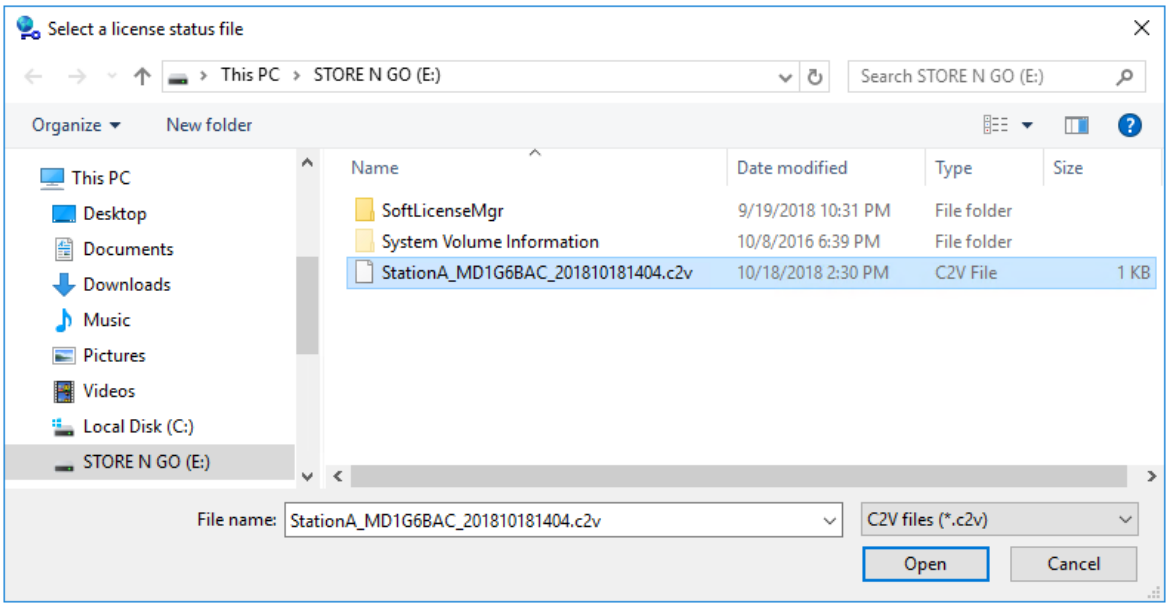
Figure A-31 Soft License Manager – SICAM PAS/PQS not Installed

✧ Enter the product key for the destination system.

NOTE

If SICAM PAS/PQS is installed on the computer on which you perform the activation, activate the **Activate SICAM PAS/PQS for a different machine** checkbox.

✧ Click **...** to go to the C2V license status file on the destination system.



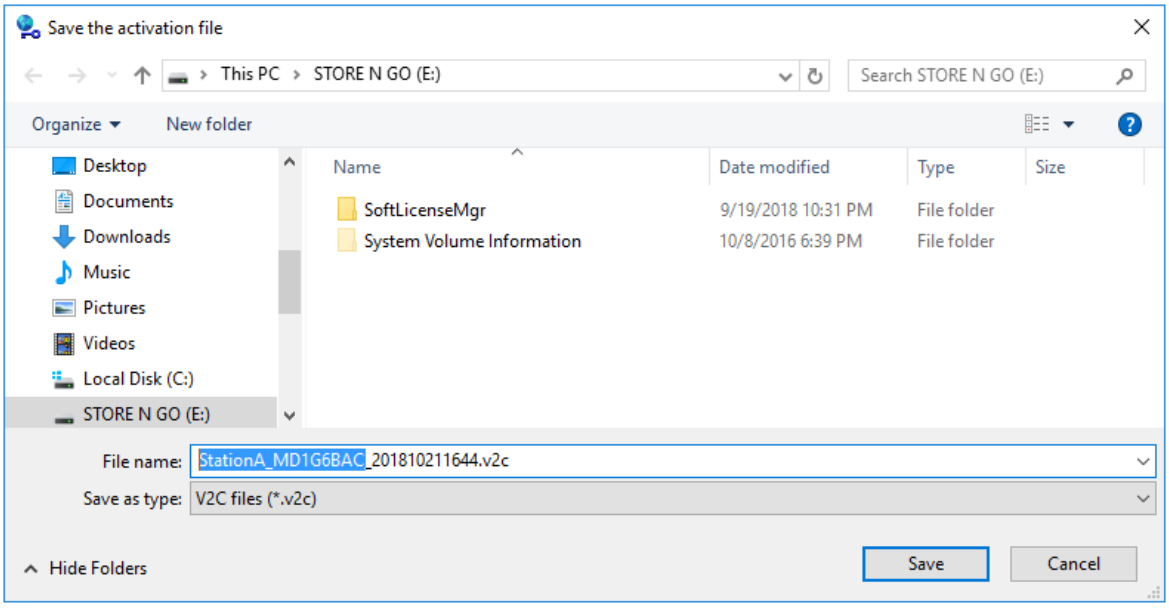
[sc_select_C2V, 2, en_US]

Figure A-32 Selecting the Licence Status File

The **Activate** button is enabled once the product key has been entered completely and the C2V license status file has been selected.

✧ Click **Activate**.

The **Save the activation file** dialog opens after the activation.

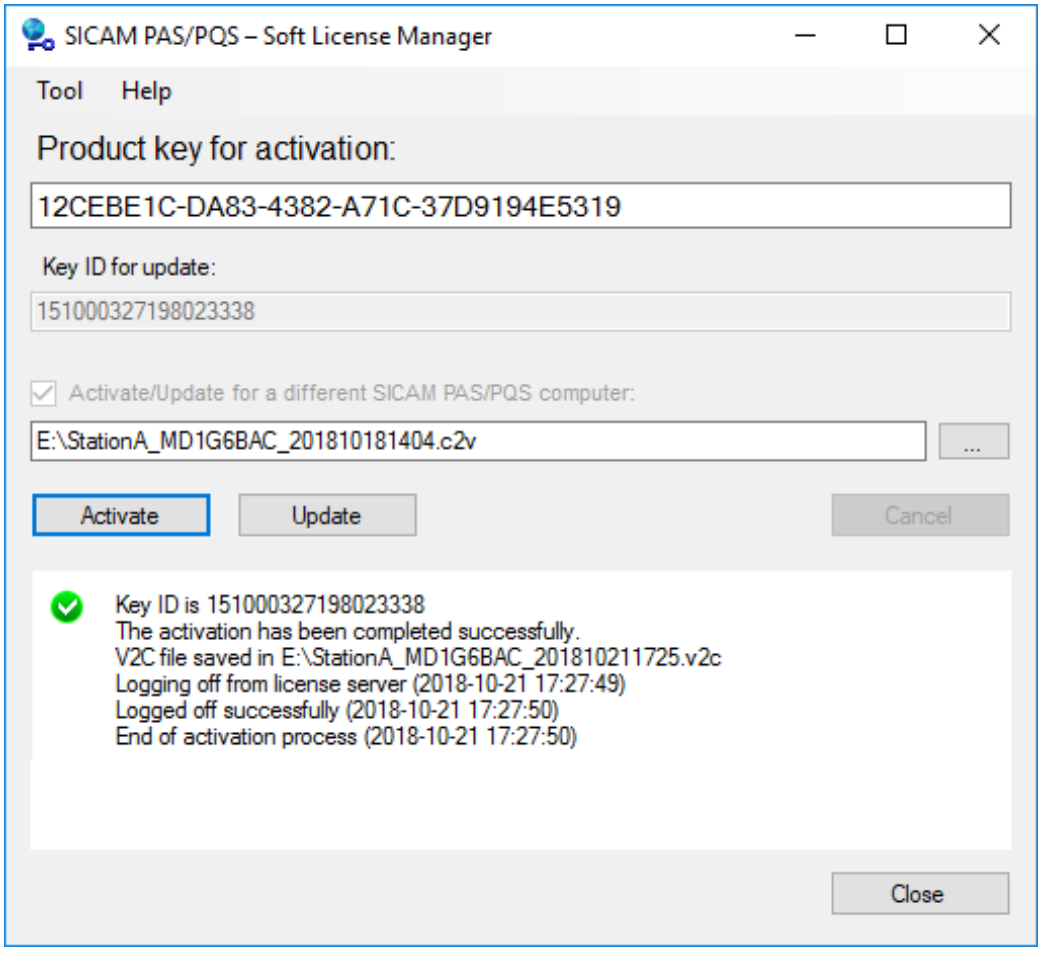


[sc_save_V2C_offline, 2, en_US]

Figure A-33 Saving the License File

✧ Save the V2C license file with a unique name.

A message informs you that the activation has been successful.



[sc_system_activated_offline, 2, --, --]

Figure A-34 Activation Completed

NOTE

The V2C license file is required on the target computer in order to enable the features in the Feature Enabler.

Enabling the Features

- ✧ Change to the destination system.
- ✧ Transfer the V2C license file to the destination system.
- ✧ Enable the features in the Feature Enabler, see *A.18 Importing the License File*.

A.15 Extending a System with Internet Access

The following steps must be performed in order to extend your already existing Soft License for your system **with** Internet access:

- Updating the Soft License
- Enabling the features

Updating the Soft License

✧ Start the Soft License Manager.

✧ Click **Update**.

The **Save the activation file** dialog opens after the Soft License has been updated.

✧ Save the V2C license file with a unique name.

A message informs you that the Soft License has been successfully updated.

Enabling the Features

✧ Enable the features in the Feature Enabler, see *A.18 Importing the License File*.

A.16 Extending a System without Internet Access

The following steps must be performed in order to extend an existing Soft License for your system **without** Internet access:

- Creating a license status file for the system to be extended (destination system)
- Updating the Soft License for the destination system on a computer **with** Internet access
- Enabling the features on the destination system using the Feature Enabler

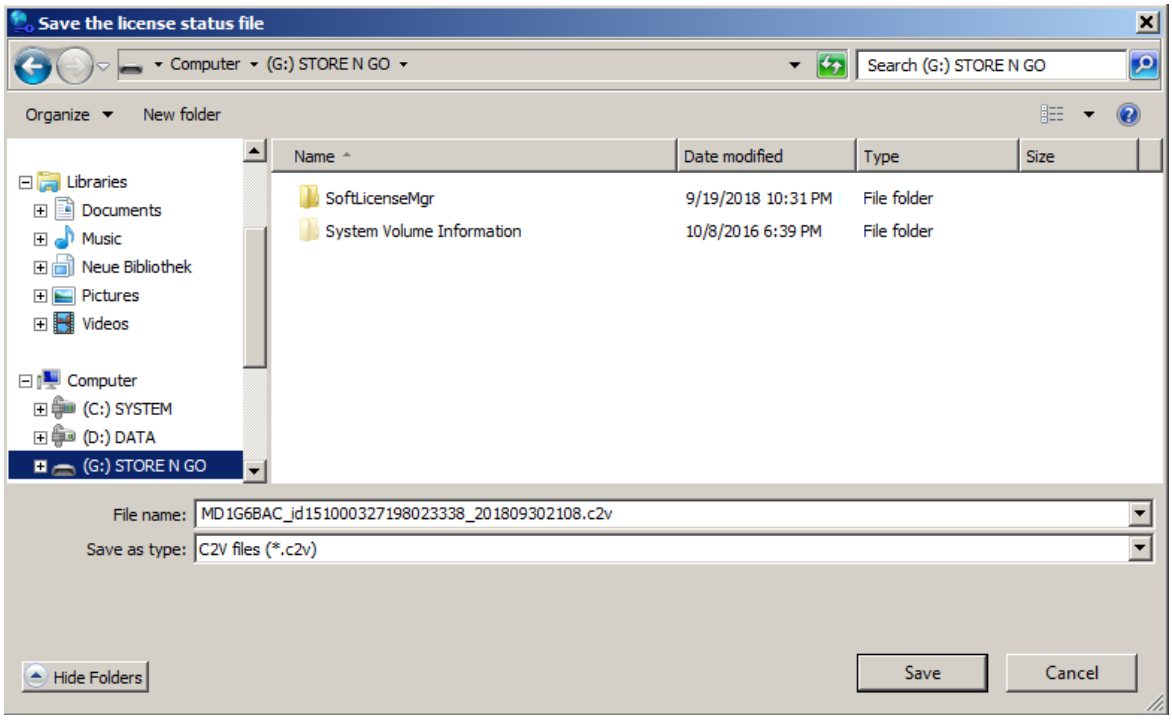
Creating a License Status File

To create a license status file for the destination system on which SICAM PAS/PQS is installed:

✧ Start the Soft License Manager on the destination system.

✧ Select **Create license status file...** in the **Tool** menu.

Once the license status file has been generated, the **Save the license status file** dialog opens.



[sc_Update_save_C2V, 1, en_US]

Figure A-35 Saving the License Status File

✧ Save the C2V license status file with a unique name.

NOTE

The C2V license status file is required in order to extend the Soft License on the computer with Internet access.

Updating the Soft License

✧ Change to a computer with Internet access.

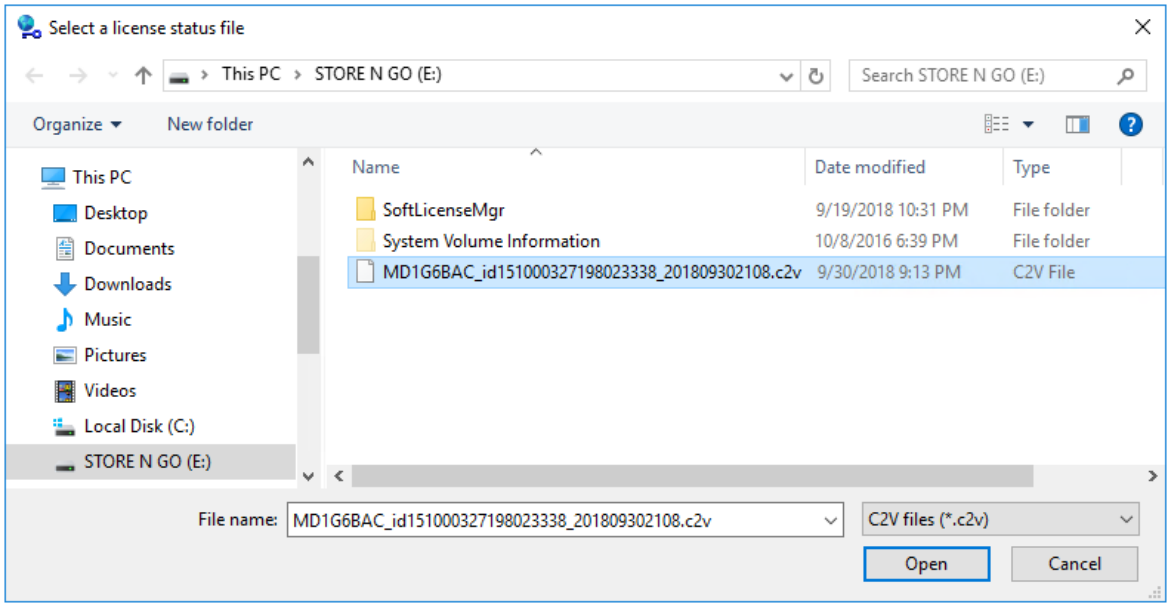
✧ Transfer the C2V license status file.

✧ Start the Soft License Manager.

NOTE

If SICAM PAS/PQS is installed on the computer on which you perform the activation, activate the **Activate SICAM PAS/PQS for a different machine** checkbox.

✧ Click **...** to go to the C2V license status file of the destination system.

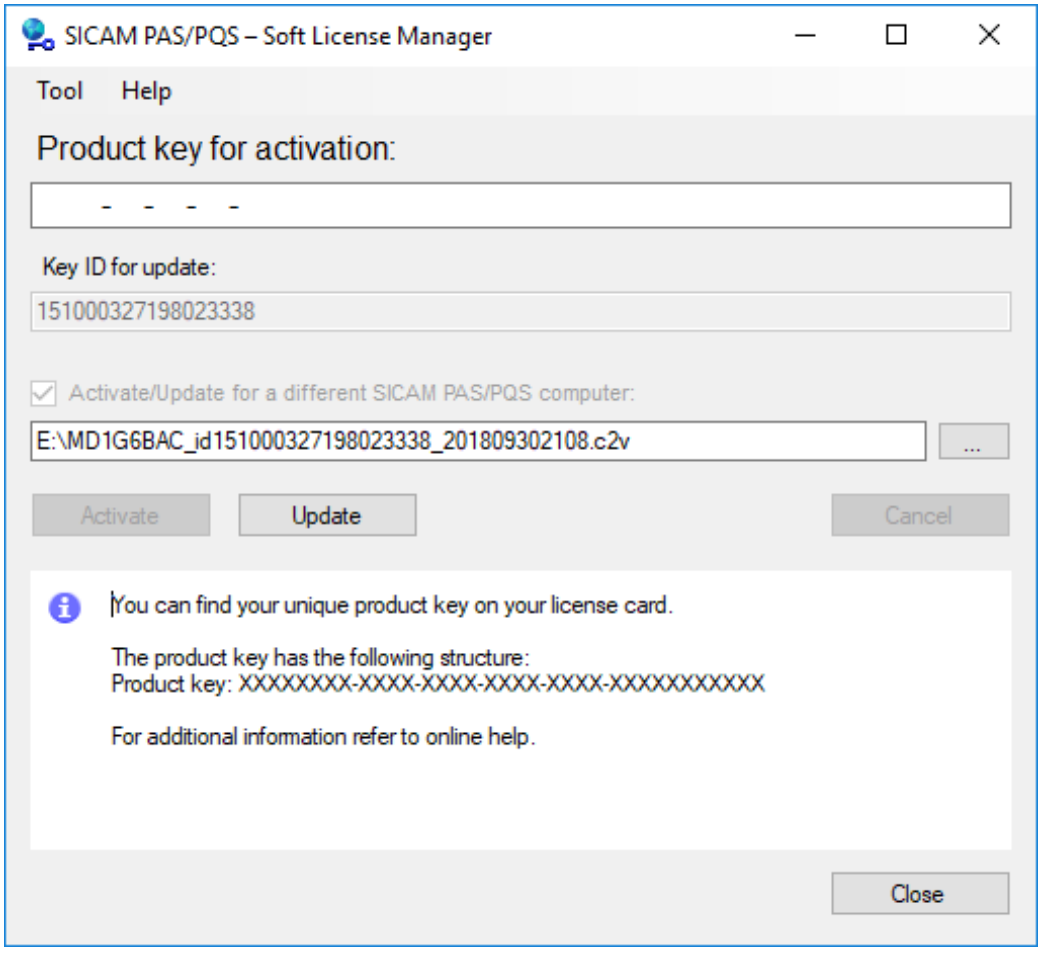


[sc_Update_select_C2V.tif, 1, en_US]

Figure A-36 Selecting the Licence Status File

✧ Click **Open**.

The Key ID of your system is displayed.



[sc_Update_C2V_selected_KEY_ID_displayed, 1, --_--]

Figure A-37 Updating, License Status File Selected and Key ID Displayed

✧ Click **Update**.

Once the Soft License has been updated, the **Save the activation file** dialog opens.

✧ Save the V2C license file with a unique name.

A message informs you that the Soft License has been successfully updated.

NOTE

The V2C license file is required on the target computer in order to enable the features in the Feature Enabler.

Enabling the Features

✧ Change to the destination system.

✧ Transfer the V2C license file to the destination system.

✧ Enable the features in the Feature Enabler, see *A.18 Importing the License File*.

A.17 Extending a Dongle via Internet

A system licensed with a dongle for SICAM PAS/PQS V8.02 and later can be extended using the Soft License Manager.

- ✧ Plug the dongle into the computer on which SICAM PAS/PQS is installed.
- ✧ Open the Soft License Manager.

System with Internet Access

- ✧ Click **Update**.

A message informs you that the Soft License has been successfully updated.

- ✧ Save the V2C license file with a unique name.

System without Internet Access

- ✧ Create a C2V license status file.
- ✧ Transfer the C2V license status file to a computer with Internet access.
- ✧ Open the Soft License Manager and select the C2V license status file.
- ✧ Click **Update**.

A message informs you that the Soft License has been successfully updated.

- ✧ Save the V2C license file with a unique name.

Enabling the Features

- ✧ Enable the features in the Feature Enabler, see *A.18 Importing the License File*.

A.18 Importing the License File

To import additional licenses:

- ✧ Start the **Feature Enabler**.

The installed features are displayed.

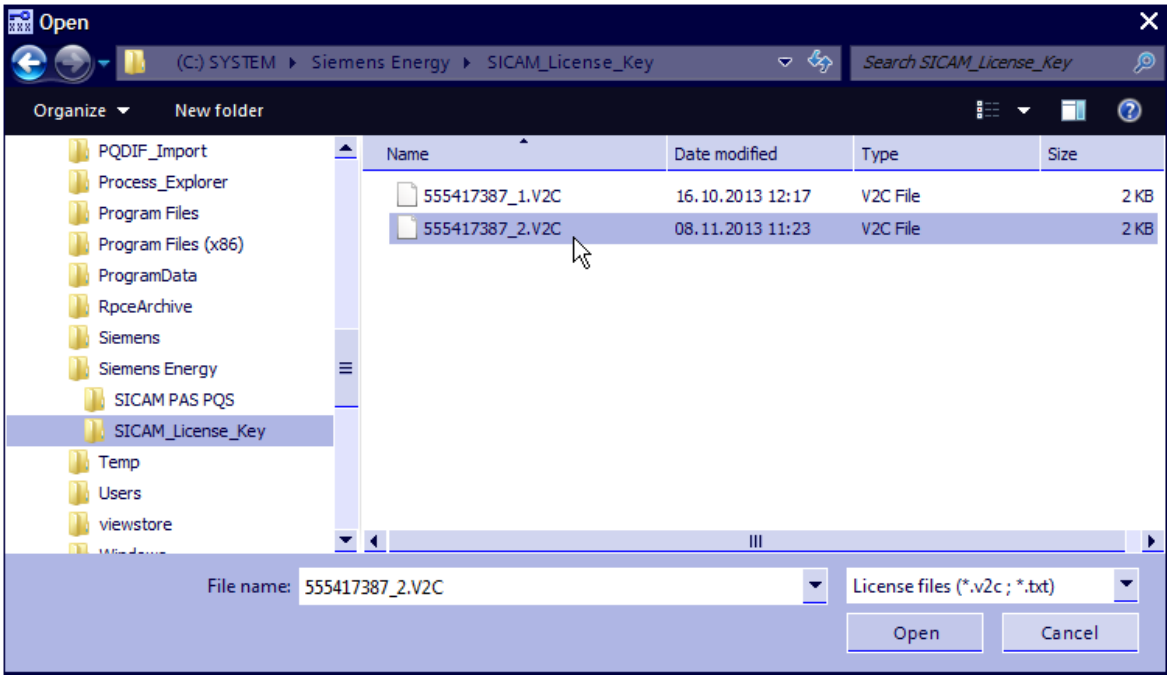
[sc_FeatureEnabler_Installed_Licenses, 2, en_US]

Figure A-38 Installed Licenses with Key ID

✧ Click **Import...** .

✧ Navigate to the directory in which the V2C license file is stored.

✧ Select the V2C license file.



[sc_Select_License_File, 1, en_US]

Figure A-39 Selecting the License File

✧ Click **Open** to confirm.

The features are now enabled.

A.19 Using a Dongle to License a SICAM PAS/PQS System, V8.01 and Earlier

When performing an upgrade or extending an existing installation by new features, the dongle acquired for SICAM PAS/PQS V8.01 and earlier versions remains valid.

NOTE

Since version V8.07, the **Runtime – Large** feature is limited to the use of 180 devices. The **Runtime – Extra Large** feature must be used for a system configured for more than 180 devices.

To run a large system, enable the **Runtime – Extra Large** feature by entering the **Runtime – Large** license key from the license card or from the exported license key file.

Extending the System

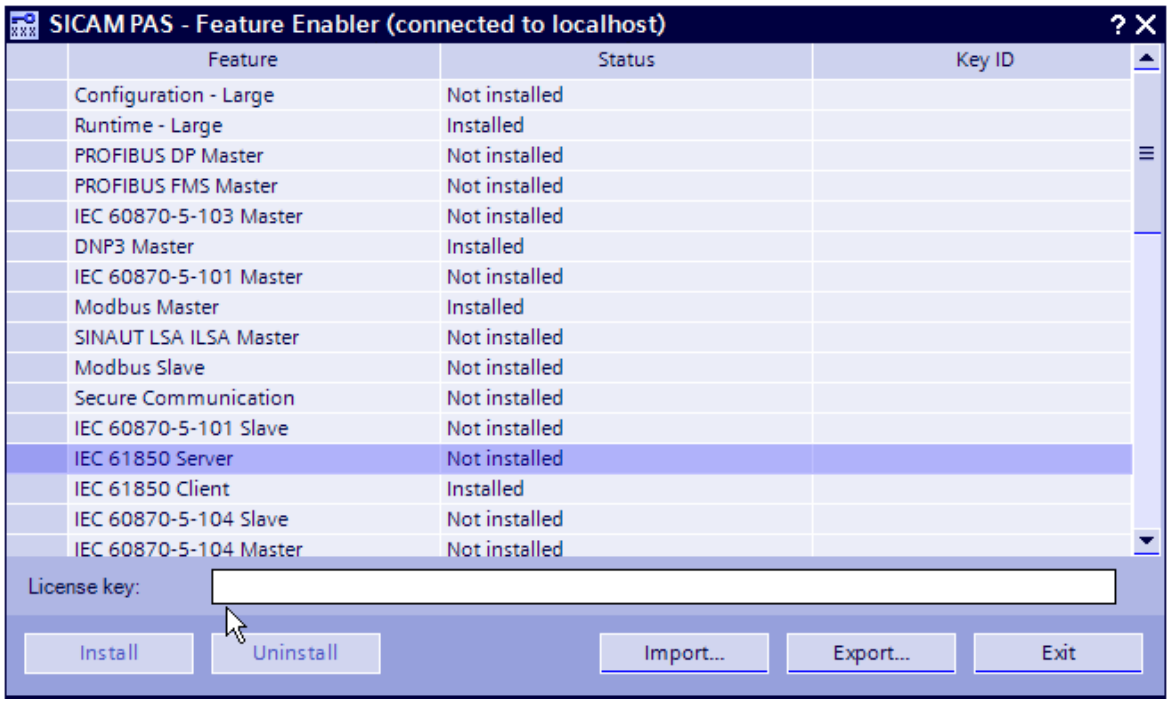
To enable additional features, the corresponding license key must be entered in the Feature Enabler. Keep this license key in a safe place.

To enable the individual SICAM PAS/PQS features:

✧ Make sure that the dongle has been plugged.

✧ Start the **Feature Enabler**.

✧ Select the feature which you want to enable.



[sc_FeatureEnabler_Select_Features, 2, en_US]

Figure A-40 Selecting Features Using the Feature Enabler

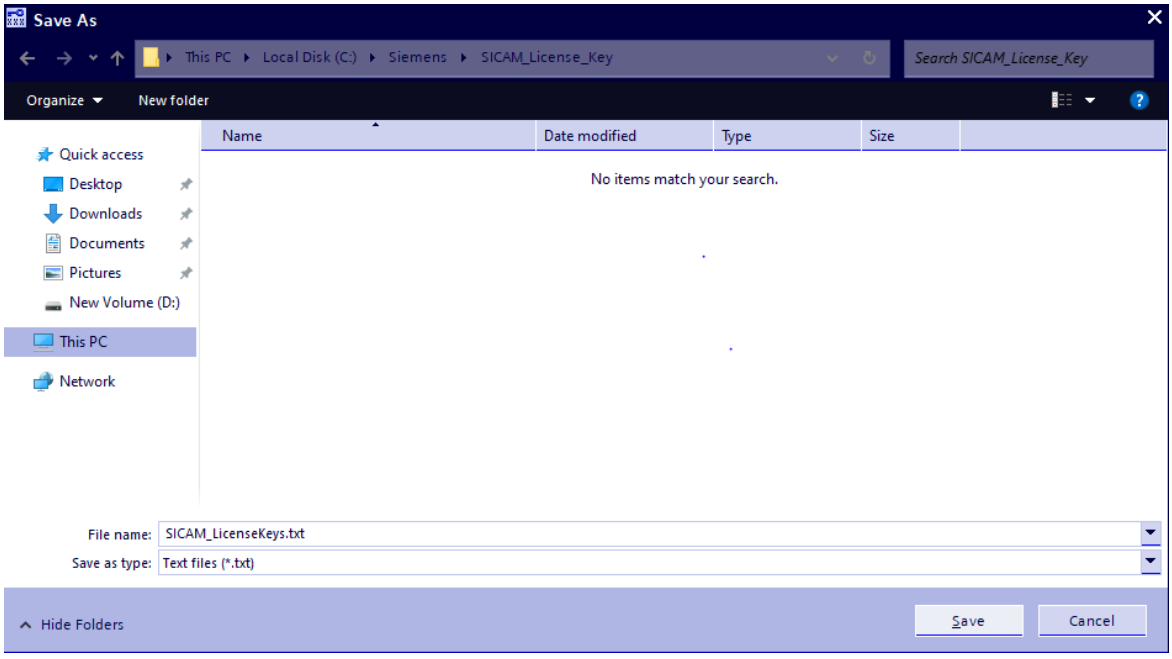
- ✧ Under **License key** enter the license key which you have received for the selected feature. Next, click **Install**.
- ✧ Repeat these two steps for all the features which you want to enable.
- ✧ As soon as you have enabled all desired features click **Exit** to exit the Feature Enabler.

Saving the License Key

You can export the license keys entered for this dongle and import them during a system reinstallation.

To export all the license keys installed in your system:

- ✧ Make sure that the dongle has been plugged.
- ✧ Start the **Feature Enabler**.
- ✧ Click **Export...** .
- ✧ Navigate to the directory in which you want to save the TXT license key file and enter a name for the license key file.



{sc_Export_License_Key, 2, en_US}

Figure A-41 Exporting the License Keys

✧ Click **Save**.

The export of the license keys is logged in the **Export license keys** dialog.

✧ Click **OK** to confirm the export.

✧ Exit the **Feature Enabler**.

All license keys are stored in the license key file in the specified directory and can be imported for the same dongle.

Importing the License Keys

After the reinstallation of SICAM PAS/PQS no features are enabled by the **Feature Enabler**.

To import the license keys for the system:

✧ Make sure that the dongle has been plugged.

✧ Start the **Feature Enabler**.

✧ Click **Import...** .

✧ Navigate to the directory of the license key file.

✧ Select the TXT license key file assigned to the dongle and click **Open**.

The import of the license keys is logged in the **Import license keys** dialog.

NOTE

The license key for an unlimited number of devices (**Runtime – Extra Large**) cannot be imported and must be entered separately.

✧ Click **OK** to confirm the import.

The installed license keys are shown in the Feature Enabler.

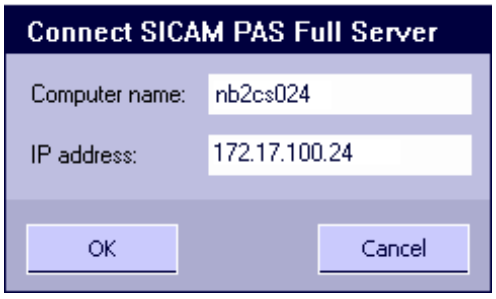
✧ Exit the **Feature Enabler**.

A.20 Connecting the DIP to the Full Server

In a distributed system you must connect a DIP to the Full Server. As a prerequisite, a network connection must have been set up to the Full Server and the Full Server must run.

To connect the DIP to the Full Server:

✧ Start the **Feature Enabler** on the DIP.



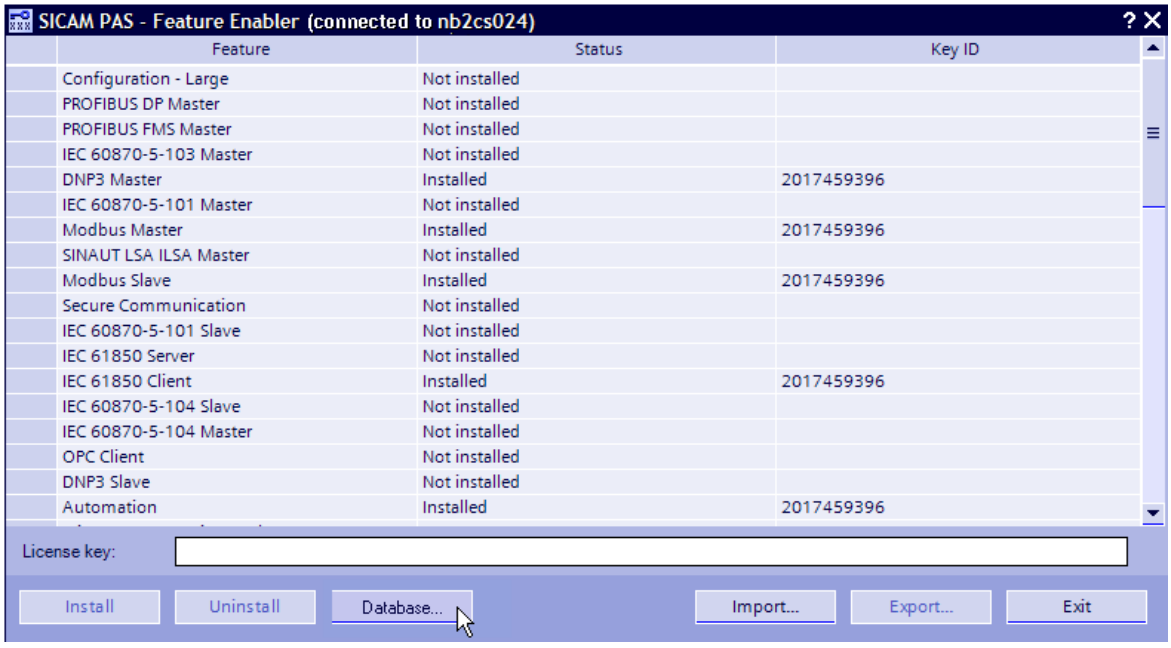
[sc_SICAMPAS_Server_Connection, 2, en_US]

Figure A-42 Entering the IP address

✧ Enter the **Computer name** and the **IP address** of the computer on which the Full Server to be connected to the DIP is running.

✧ Click **OK**.

The **Feature Enabler** opens and displays the features enabled on the DIP.



[sc_FeatureEnabler, 2, en_US]

Figure A-43 Feature Enabler

✧ If you want to connect the DIP to another Full Server, click **Database...** .

NOTE

Be aware of the following in order to ensure that all the SICAM PAS/PQS computers within a system can access the current configuration data:

- The user who performs the system update must have a user account on each SICAM PAS/PQS computer.
- This user must have read and write rights for the **C:\Siemens\SySrv\Data** directory.

Literature

/1/ SICAM PAS, Overview
E50417-X8976-C431-C7

/2/ SICAM PQS, Overview
E50417-X8976-C464-C5

/3/ SICAM PAS/PQS, Installation
E50417-M8976-C432-C7

/4/ SICAM PAS/PQS, Configuration and Operation
E50417-P8976-C433-C8

/5/ SICAM SCC, Human Machine Interface SICAM SCC
E50417-H8976-C501-B7

/6/ SICAM Valpro, Measured/Metered Value Processing Utility SICAM Valpro
E50417-H8976-C479-A5

/7/ SICAM PAS, Automation Blocks
E50417-H8976-C436-B4

/8/ SICAM PAS/PQS, Security
E50417-H8976-C438-B9

/9/ SICAM PAS, Redundancy
E50417-H8976-C441-C1

/10/ SICAM PAS, Device Description
E50417-T8976-C437-B3

/11/ SICAM Station Unit V2.40
E50417-H8976-C381-A6

/12/ SICAM PQS, Fault Locator
E50417-H8976-C421-B1

/13/ SICAM PQ Analyzer
E50417-H8976-C397-C7

/14/ SICAM PQ Analyzer, Incident Explorer
E50417-H8976-C465-C5

/15/ SICAM PAS, CFE Test and Diagnosis
E50417-H8976-C425-A5

/16/ SIMEAS R PAR, Parameterization Tool
E50417-H1076-C439-B1

/17/ SIMEAS R, Manual Digital Fault and Power Quality Recorder
E50417-B1076-C209-A6

/18/ SIMEAS R-PMU, Manual Digital Fault Recorder
E50417-H1076-C360-A4

/19/ SIMEAS R-PMU, Maintenance Manual
E50417-H1076-C364-A3

/20/ SICAM P850/P855 7KG85xx V2.60, Power Monitoring Device and Power Quality Recorder, Device Manual
E50417-C1076-C482-A8

/21/ SICAM Q100 7KG95xx V2.10, Power Monitoring Device and Class A Power Quality Recorder, Device Manual
E50417-H1076-C522-A7

/22/ SICAM Q200 7KG97 V2.40, Multifunctional Recorder, Device Manual
E50417-H1040-C606-A7

/23/ SIPROTEC 5 7KE85 V7.80 and later, Fault Recorder, Manual
C53000-G5040-C018-6

/24/ SICAM GridPass V1.30, Manual
E50417-H8940-C598-A5

/25/ SIMATIC HMI WinCC V7.5, WinCC Information System, System Manual
Printout of the online help, 09/2018, A5E46376856-AA

/26/ SICAM Q80 Power Quality Recorder, System Manual
E50417-H1076-C420-A2

Index

T

U

V