Installation of the recording software of ASC

Installation manual

for system providers

9/10/2021

Product line *neo*, version 6.x

The described functions can be used with the following ASC products:

EVOIP*neo*

INSPIRATION*neo*

EVOLUTION*neo* / XXL / eco

Please note that you can always find the most up-to-date technical documentation and product updates in the partner area on our website at http://www.asctechnologies.com.

ASC Technologies AG - Seibelstr. 2-4 - 63768 Hösbach - Germany

Contents

1 General information

In the context of this document ASC represents ASC Technologies AG, its subsidiaries, branch offices, and distributors. An up-to-date overview of the aforementioned entities can be found at https://www.asctechnologies.com

ASC assumes no guarantee for the actuality, correctness, integrity or quality of the information provided in the manuals.

ASC regularly checks the content of the released manuals for consistency with the described hardware and software. Nevertheless, deviations cannot be excluded. Necessary revisions are included in subsequent editions.

Some aspects of the ASC technology are described in general terms to protect the ownership and the confidential information or trade secrets of ASC.

Representative, if not defined otherwise, is the technical status at the time of the delivery of the software, the devices and the manuals of ASC. Technical changes without specified announcements are reserved. Previous manuals lose their validity.

The general conditions of sales and delivery of ASC in their latest version apply.

2 Introduction

This document describes the installation of the *neo* software.

Make sure that you have all administrator rights for the installation.

When installing and/or updating the *neo* software, on-access scanning must have been disabled.

Before the installation of the *neo* software make sure that the installation and configuration of Microsoft Windows have been carried out according to our demands.

For information about the installation and configuration of Microsoft Windows refer to the respective installation manual for system providers *Configuration Windows Server 2012 R2*, *Configuration Windows Server 2016* or *Configuration Windows Server 2019*.

For new installations, OpenJDK is installed by default. If Oracle JDK is supposed to be used, the setup.exe must be called up with the parameter *oraclejdk_mode* with Windows command line (*setup.exe oraclejdk_mode*).

A later update from Oracle JDK to OpenJDK is possible anytime. For further information refer to the installation manual for system provider *Software updates*.

The *neo* software contains different applications. With the basic installation the following applications are released:

- Portal
- System Configuration
- System Monitoring
- POWER*play* Web

All additional applications are subject to licensing.

Individual recording solutions and functions depend on license and are only available if the corresponding license has been installed.

For further information about the license administration refer to the administration manual *License administration*.

Every *neo* system is initially installed as a 1-tenant system with one predefined tenant, the 1st-tenant. The system provider is set up as tenant, too. However, the system provider is not another tenant in the true sense of the word.

For the respective administrators of the system provider and of the predefined tenant, an account with the following login data is created during the installation of the system by default:

Login data for the administrator of the system provider:

User name:	*system-admin*
neo version < 6.3	
Default password:	*1* If the default password *1* has never been changed before a software update to a *neo* version ≥ 6.3, the password must be changed upon the next login or by entering it again. If the default password has already been changed before a software update to a *neo* version ≥ 6.3, the changed password remains.
neo version ≥ 6.3	

Default password:	*A$c123*

Tab. 1: Login data - system provider

Login data for the administrator of the 1st tenant:

User name:	*1st-tenant-admin*
neo version < 6.3	
Default password:	*1* If the default password *1* has never been changed before a software update to a *neo* version ≥ 6.3, the password must be changed upon the next login or by entering it again. If the default password has already been changed before a software update to a *neo* version ≥ 6.3, the changed password remains.
neo version ≥ 6.3	
Default password:	*A$c123*

Tab. 2: Login data - 1st tenant

Depending on the licensing, the *neo* recording system is operated as a 1-tenant system or as a multi-tenant system. In a 1-tenant system, there is only the predefined tenant; no other tenants can be created. In a multi-tenant system, the system provider can create as many additional tenants as there are tenant licenses in the system.

3 System requirements

For basic information about the necessary hardware and software components refer to the installation manual *Installation requirements.*

Firewall

The service *Windows Firewall* must have started **before** the installation of the *neo* software so that the *neo* installation routine can open the corresponding communication ports in the Windows firewall automatically. If the Windows firewall starts at a later moment, the recording system will not work properly.

The *neo* installation routine makes changes only to the Windows firewall. Other firewall solutions must be configured manually according to the communication matrix. See installation manual *Installation requirements*.

Load Balancer

To operate a multi-core architecture, a Layer 4 Load Balancer is required. The load balancer has to be provided by the system provider.

ASC software

4 Installation requirements

4.1 Licenses

The *neo* recording system can be installed and configured without licenses. The system runs for a grace period of 30 days without any licenses. Within this period you have to request a valid license. Without a license, all functions will be deactivated after these 30 days.

Contact your distribution partner of ASC to find out which licenses are necessary in your case.

4.2 Virus protection

The installation of an antivirus software on a *neo* recording system lies within the responsibility of the customer.

The installation of an antivirus software does affect neither warranty nor maintenance contracts; however ASC does not assume any liability for consequential damages that may occur due to the use of the antivirus software.

Running an antivirus software may slow down the execution of the *neo* software during periods of high system utilization. Running an antivirus software has an impact on the execution of functions, too, which involve increased data exchange at the I/O interfaces (e. g. creating diagnostic data, statistics or updating configuration data) and may thus cause functional impairment.

For this reason, ASC recommends defining time intervals for scanning the entire system for viruses when system utilization and data transfer rates are low.

Antivirus programs tested by ASC and supported:

- Windows Defender (virus protection integrated into Windows operating systems)

Required settings of an antivirus software:

- On-access scanning must have been activated
- The following directories are mandatory to be excluded from the virus scan:
  - All directories on the database partition (ASCDB, replication, …)
  - Directory *ASCDATA*
  - Directory *ASC Product Suite*
- The following file is mandatory to be excluded from the virus scan:
  - File *C:\Program Files\PostgreSQL\9.5\bin\postgres.exe* or *C:\Program Files\PostgreSQL\12\bin\postgres.exe* (the path depends on the deployed PostgreSQL version.)

When installing and/or updating the *neo* software, on-access scanning must have been disabled.

Troubleshooting

If the antivirus software should cause errors in the *neo* software, proceed as follows:

1. Uninstall or deactivate the antivirus software to restore the flawless operation of the *neo* software.
2. Contact your local ASC support or +49 700 27278776 to coordinate the further course of action.

5 Redundancy options

The recording system offers the following options to secure full functionality in the event of a failure:

Redundant setup of the application server (multi-core system)

To secure the recording in the event of a failure of the application server, you can set up several application servers (app server) in a cluster. In this cluster, the system load is distributed automatically among the different application servers. If an application server fails, the other application servers share all tasks among each other.

During the installation of the *neo* software, you configure which servers are supposed to be available as application servers in your recording system and are to be deployed in the cluster, see chapter "Install recording software", p. 13.

To operate a multi-core architecture, a Layer 4 Load Balancer is required. The load balancer has to be provided by the system provider.

Redundant setup of the database

To secure the access to the recordings in case of a failure of the database, you can set up a failover capability with another database.

If you use an MSSQL database, configure the failover operation of the databases according to the manual of the respective manufacturer.

If you use the PostgreSQL database refer to the installation manual *Failover operation for PostgreSQL databases* for information about the configuration of the failover concept. This manual includes a description of the steps you have to take to reset the failover operation once the primary database is available again.

Redundant setup of the recording server

To secure the recording in the event of a failure of the recording server or of a recording component, you can set up different failover recording architectures.

For information about the configuration of failover architectures refer to the installation manual *Configuration servers and recording architectures*.

6 Internal database

The recording system is delivered with an integrated PostgreSQL database. The target directory for the database is defined during the installation routine (default setting: *ASCDB/* on a separate partition).

During the installation of the provided PostgreSQL database of the *neo* recording software, a backup job is created for the PostgreSQL database which covers the last 5 days (default value).

By default, you find the files in the following directory:

- `%ASCDATA%\DatabaseBackup\`

The period for the backup job of the PostgreSQL database (default value: 5 days) can be changed by means of the administration tool for the database, if required.

To optimize the capacity of the database, the recording system carries out a defragmentation and reindexation once a week.

All processes are logged. The log files are stored in *\logs\Postgres*.

7 External databases

The external database has to be installed before installing the *neo* software. If you would like to use an external database, you have to open the port which allows the *neo* software to access the database.

Information about the backup and restoration of a Microsoft SQL database can be found at http://msdn.microsoft.com/en-us/library/ms187510.aspx.

8 Download and deployment

1. On our website http://www.asctechnologies.com in the partner area on ASC XCHANGE, you will find the released software packages to download.
2. In the area *Software Download*, open the required directory, e. g. *neo Suite* > *_Hotfixes*.
3. Download the ISO image or the ZIP file.
4. In the download area in the directory *Software Download* >*Tools*, you will find the script `checksumcheck.ps1` to check the integrity of the downloaded file. By means of this script, you can compare the checksum of the ISO image with the value in the md5 file and thus check it for completeness and functionality.
5. Download the script, too, and save it in the folder where the ISO image and the md5 file have been saved.
   NOTICE! There must be no other files in the directory.
6. Right-click on the file `checksumcheck.ps1` and select the function *Execute with Powershell* in the context menu.
   ⇨ Powershell will subsequently display the check result. If the check fails, download the ISO image again.
   ⇨ If the result is correct, you can start the installation.

ⓘ Use one of the following methods to provide the ISO image:
- Mount the ISO image as drive (context menu > menu item *Mount*).
- Burn a DVD with the ISO image.

9 Install recording software

During the installation of multi-server systems, the server on which the database is supposed to run has to be installed first.

When using failover databases, the server on which the primary database is supposed to run has to be installed first.

The time zone must be set **before** starting the setup.

1. Insert the installation medium for the *neo* software.
2. Change to the directory of the *neo* software.
3. From the context menu of the file *setup.exe*, select the menu item *Run as Administrator*.
4. Execute the installation routine as administrator and follow the instructions of the installation wizard.
   ⇨ If Microsoft Visual C++ Redistributable has not yet been installed, the following window appears:

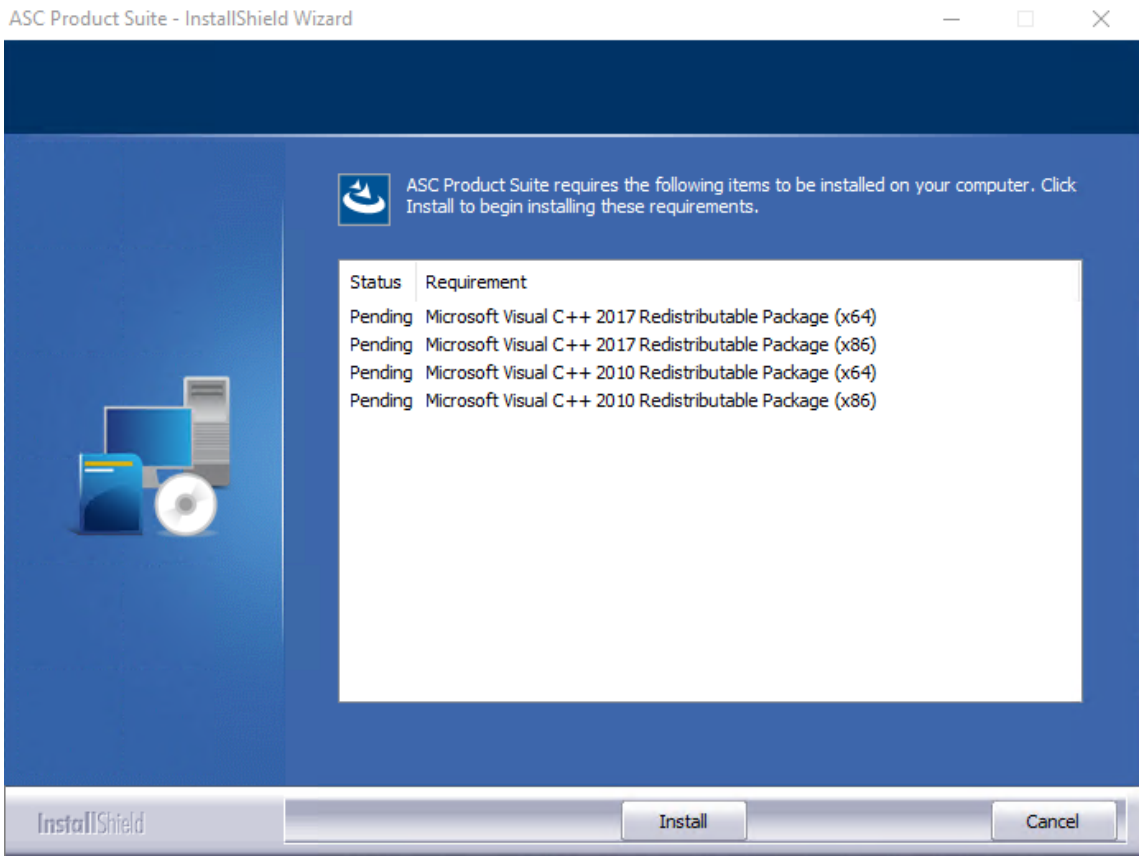

Fig. 1: Install Microsoft Visual C++

5. Start the installation of Microsoft Visual C++ by clicking on the button *Install*.
6. If SNMP was not installed during the installation of the operating system, you have to confirm the following note:

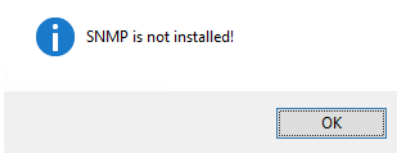

Fig. 2: Note that SNMP is not installed

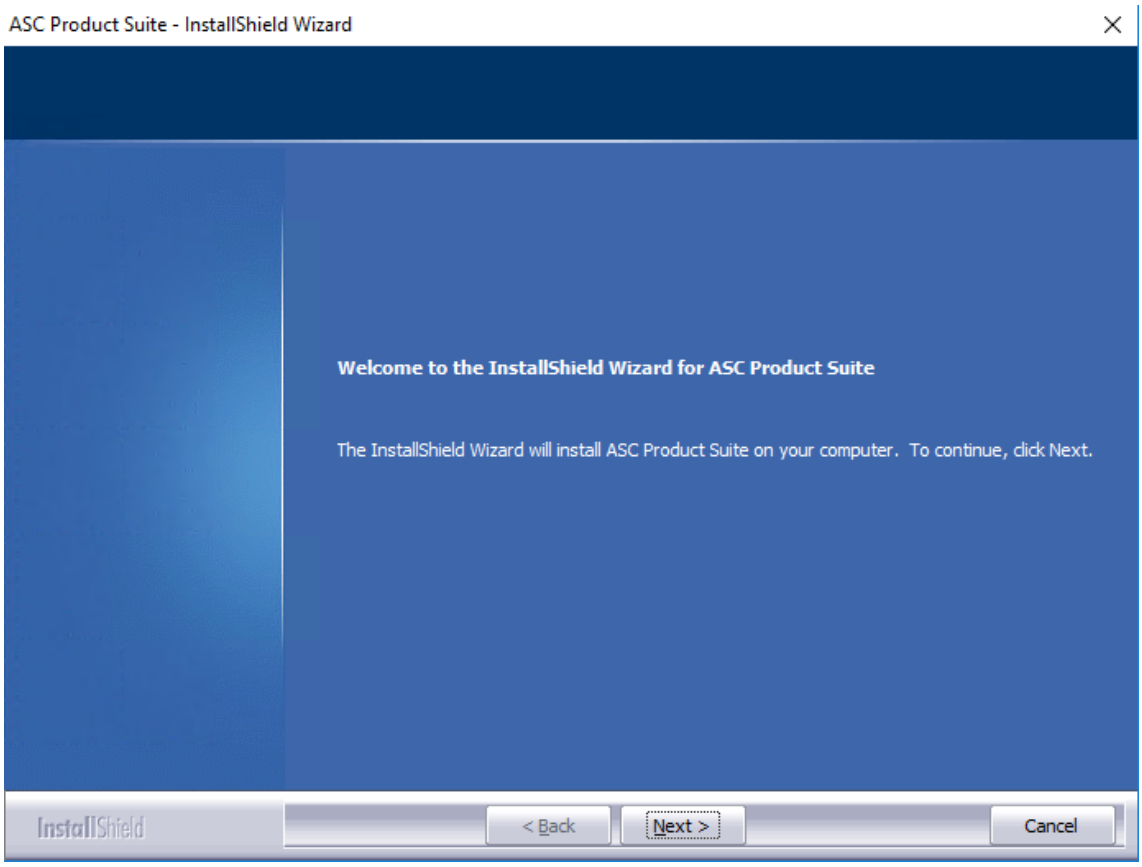

Fig. 3: Start installation routine

7. Start the installation routine for the *neo* software by clicking on the button *Next*.
   ⇨ The window containing the license agreement appears.

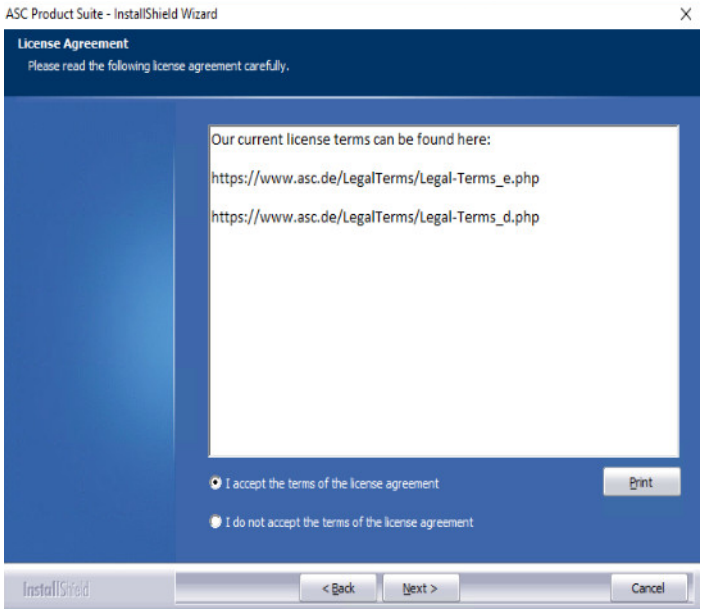

Fig. 4: License agreement

8. Select the option *I accept the terms of the license agreement* and click on the button *Next*.
   ⇨ The window to select the installation directory appears.

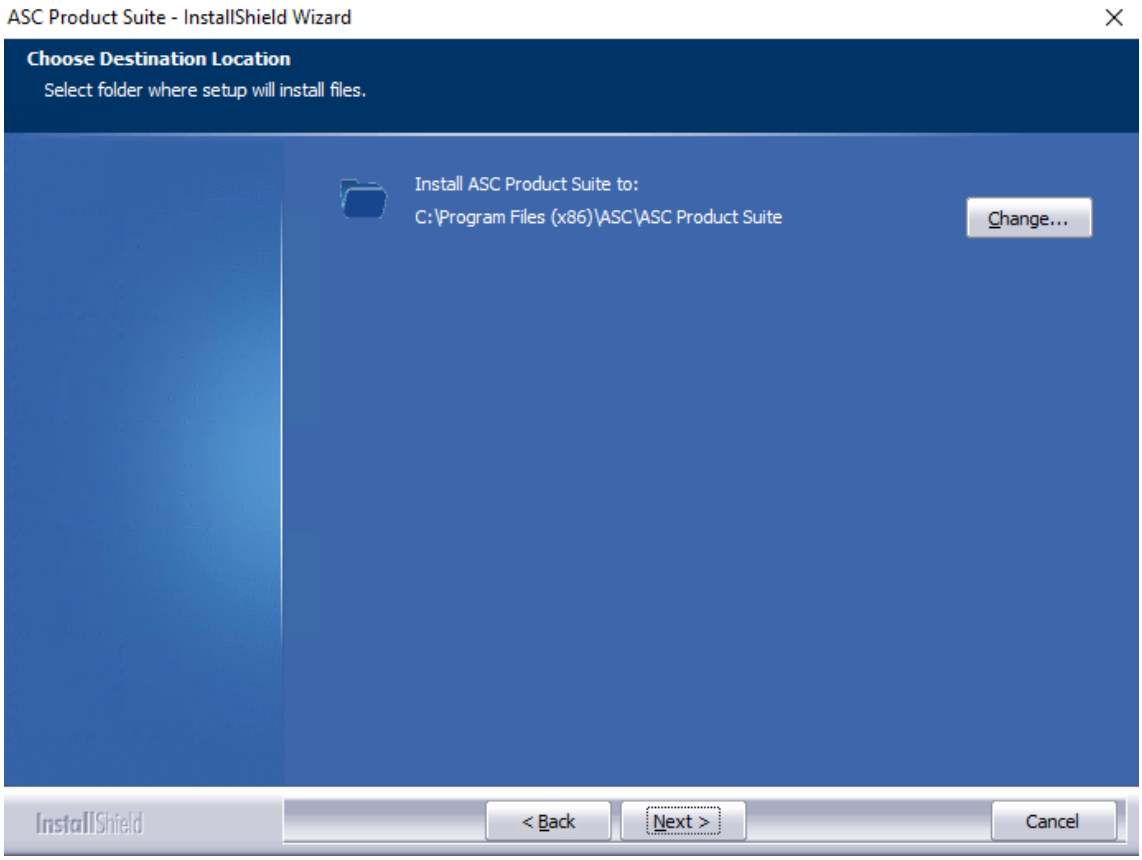

Fig. 5: Confirm the target directory for the installation

9. Select the target directory for the installation by clicking on the button *Change*.
   NOTICE! Third-party software components such as e. g. .NET, Java, PostgreSQL or WinPCap are installed in the predefined default installation paths and cannot be changed.

10. Click on the button *Next* to confirm the target directory.
    ⇨ The window appears to select the data partition on which the conversations are supposed to be stored.

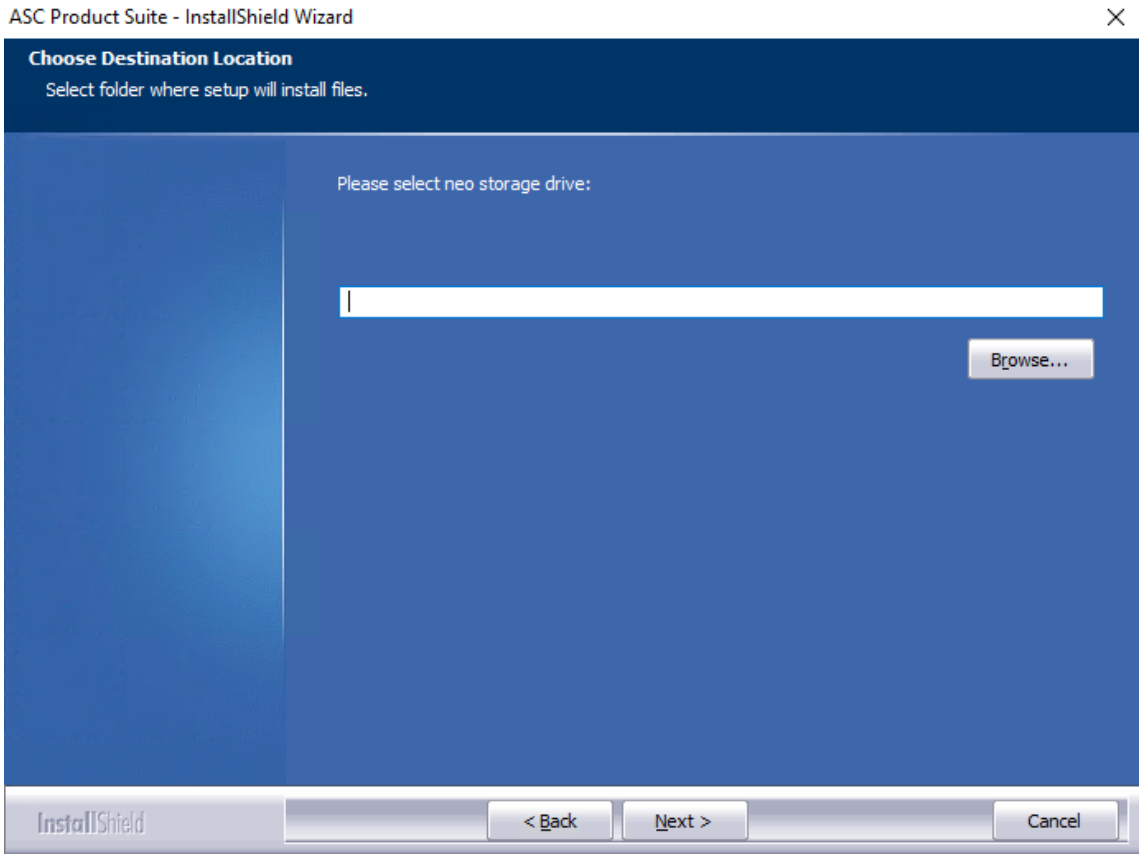

Fig. 6: Confirm data partition

11. Click on the button *Browse* to select the partition on which the recording data is supposed to be stored.
    This must not be the same partition where the *neo* software has been installed in order not to compromise its functionality.
    ⇨ The directory *ASCDATA* is created.

The letters of the drive can be selected freely during the installation.

However, changing the letters of the drive subsequently will cause access issues and thus severe interferences with internal processes.

12. Click on the button *Next* to confirm the entries.
    ⇨ 2 windows appear to select the languages. After the installation the selected languages appear in the language selection as available languages in which the user interface of the applications of the *neo* Suite can be displayed.

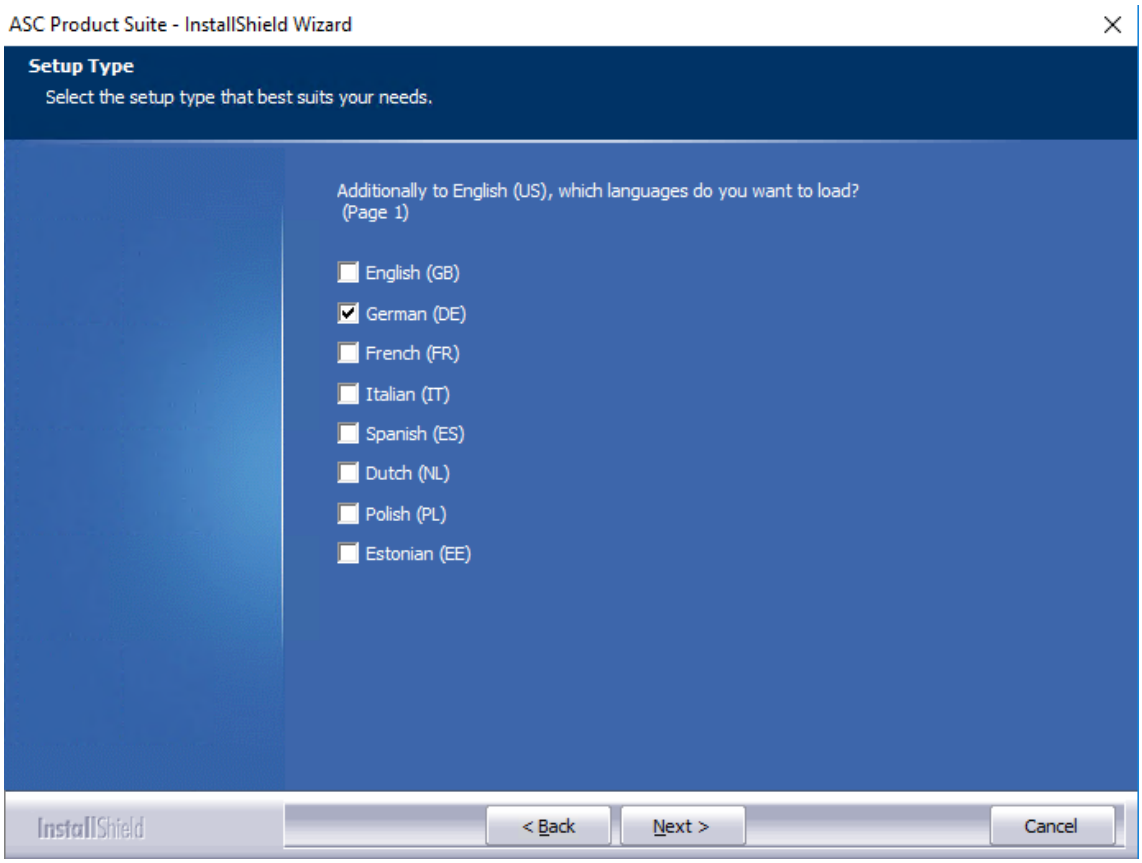

Fig. 7: Select languages for the graphical user interface

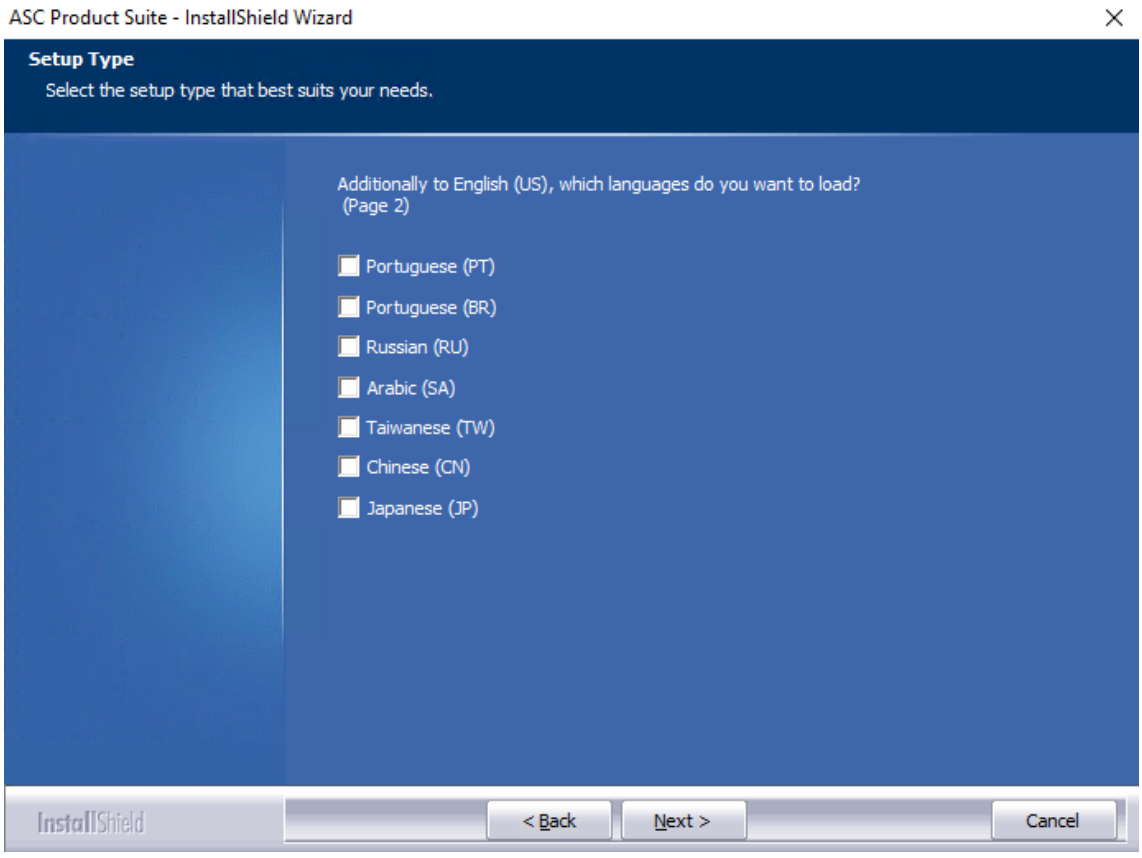

Fig. 8: Select languages for the graphical user interface

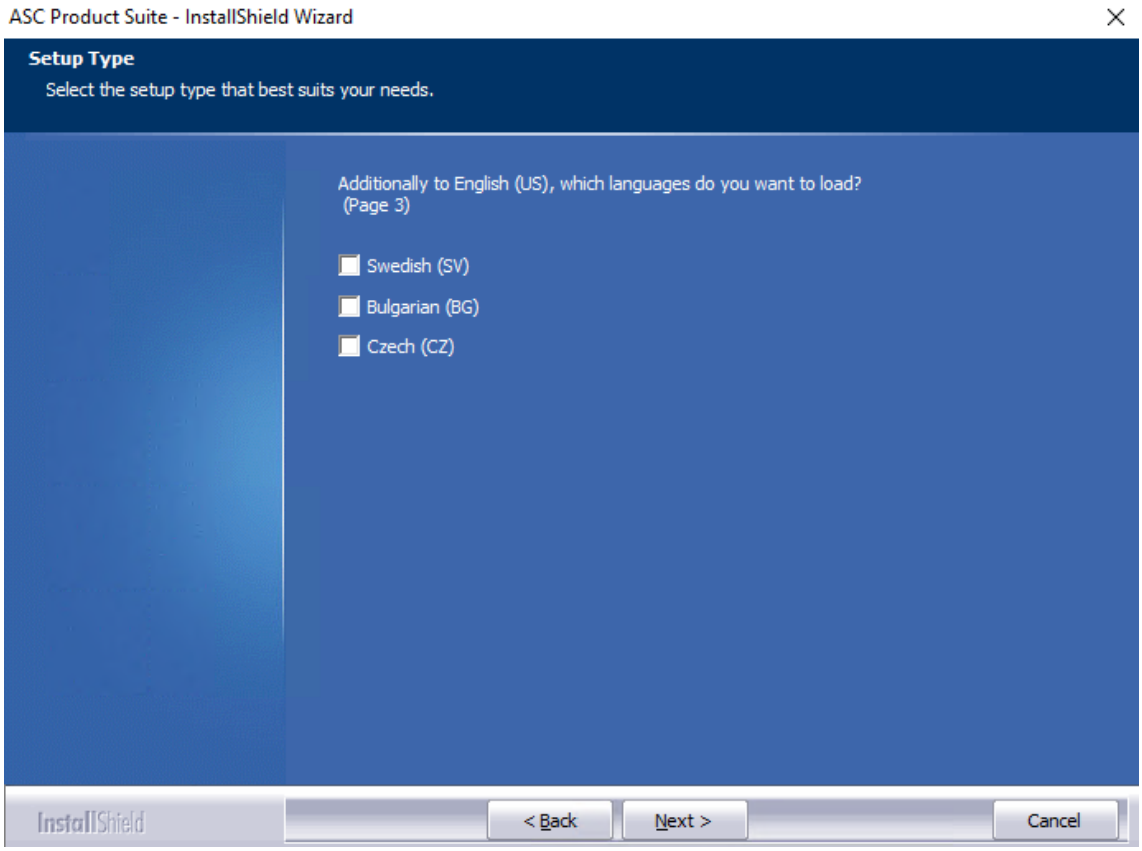

Fig. 9: Select languages for the graphical user interface

13. Select the respective languages which are supposed to be available after the installation has been completed. Multiple selections are possible.
14. Click on the button *Next* to confirm the entry.
    ⇨ The window for entering the ASC cluster ID appears.

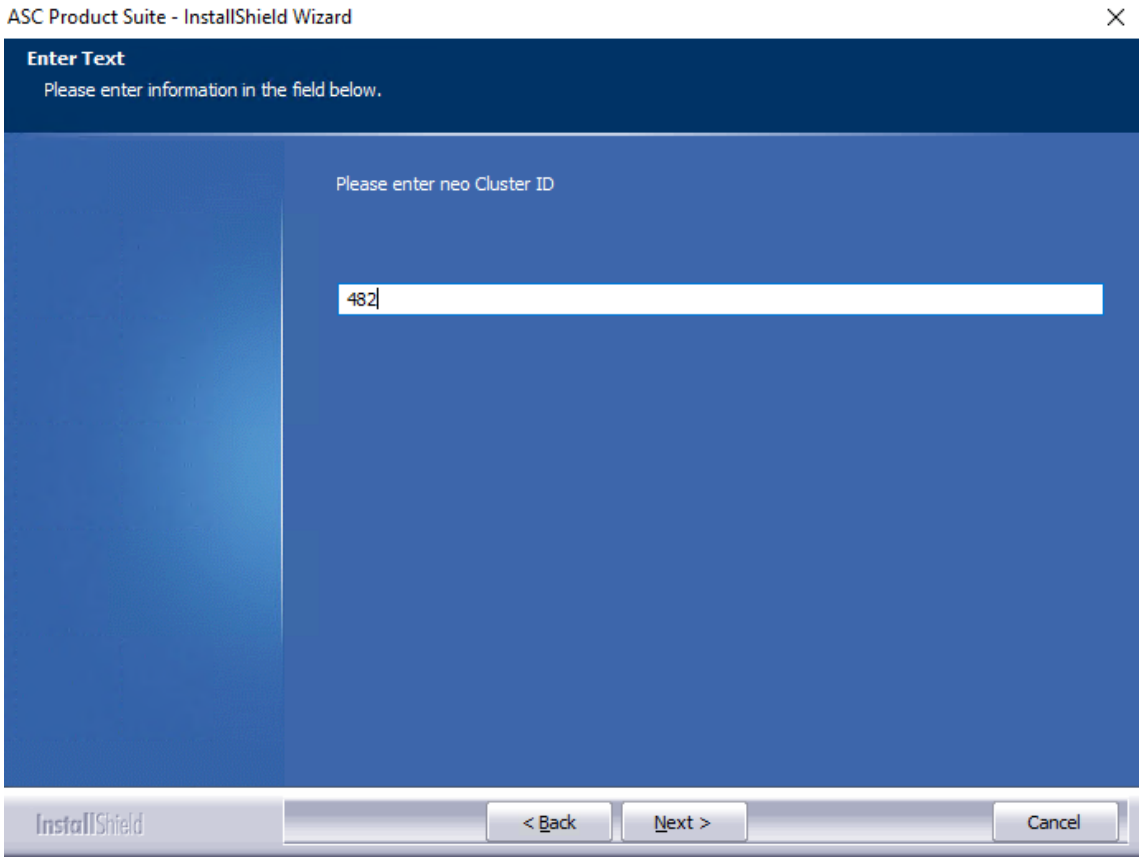

Fig. 10: Enter cluster ID

15. Enter the cluster ID.
    The server name is entered here automatically as default ID. For single-server systems, you can apply this ID.
    When setting up a multi-server system with several application servers, you have to replace the default ID with another, freely selectable cluster ID which is identical for all application servers.
16. Click on the button *Next* to confirm the entry.
    ⇨ The window for entering the IP addresses for the application servers (app server) appears.

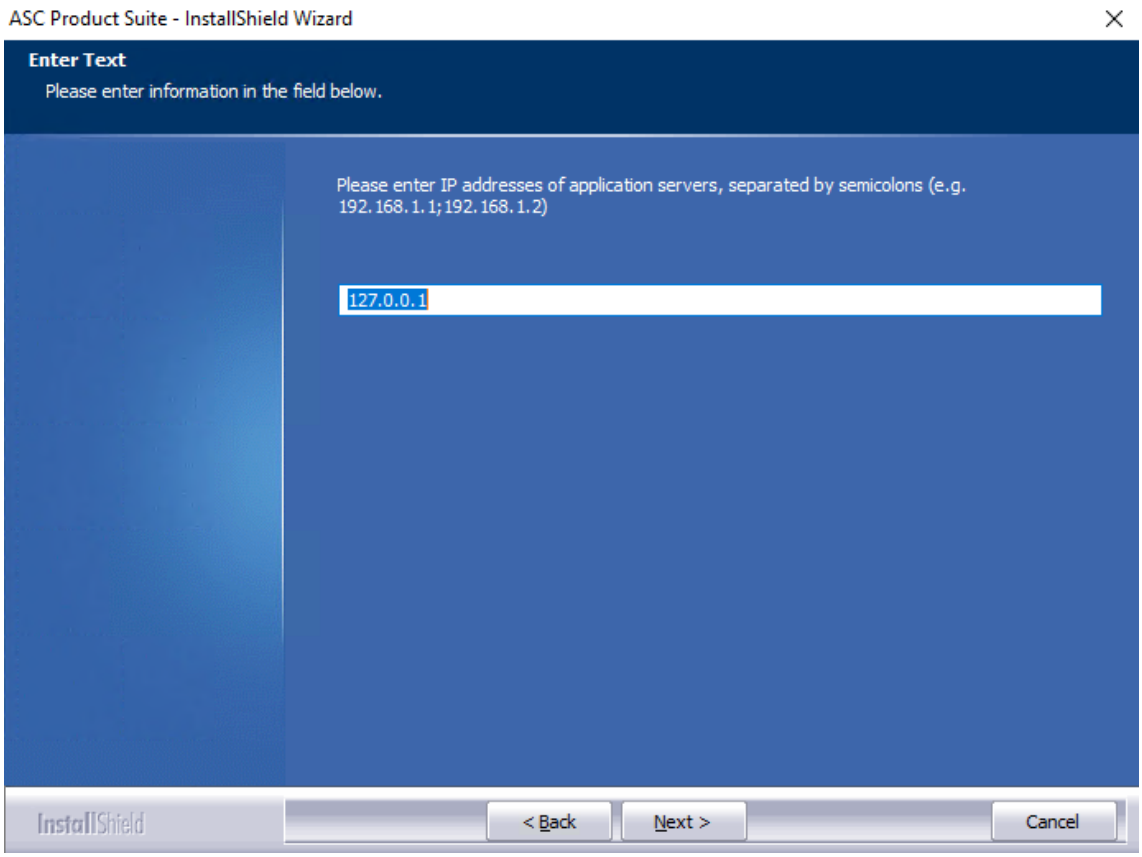

Fig. 11: Install multi-server systems

17. To use multi-server systems, enter the IP addresses of all application servers (app servers), separated by a semicolon.

    Additionally, a priority of the transmission can be set in the app server list. The app servers with the highest priority (highest number) are preferred. Several app servers can have the same priority for the purpose of distributed load sharing. In the event that all app servers of the same priority have failed, then the app server with a lower priority is used.

    To do so, enter the following syntax:

    Example 1:
    trm://172.16.203.30/?priority=2;trm://173.14.200.23/?priority=2

    In this configuration, both app servers have the same priority. The load is distributed among both app servers equally.

    Example 2:
    trm://172.16.203.30/?priority=2;trm://173.14.200.23/?priority=1

    In this configuration, app server 1 with the IP address 172.16.203.30 receives all messages. App server 2 with the IP address 173.14.200.23 only receives messages when app server 1 is not available.

    Example 2:
    trm://172.16.203.30/?priority=2;trm://173.14.200.23/?priority=1; trm://172.16.203.35/?priority=2

    In this configuration, all notifications are sent to app server 1 with the IP address

172.16.203.30 and to app server 3 with the IP address 172.16.203.35 alternately. Usually, no notifications are sent to app server 2 with the IP address 173.14.200.23. App server 2 only receives notifications when app server 1 and **app server** 3 are not available.

18. When installing a single-server system, leave the default entry on *127.0.0.1*.
19. Click on the button *Next* to confirm the entry.
    ⇨ The window for entering the IP address for the NTP server appears.

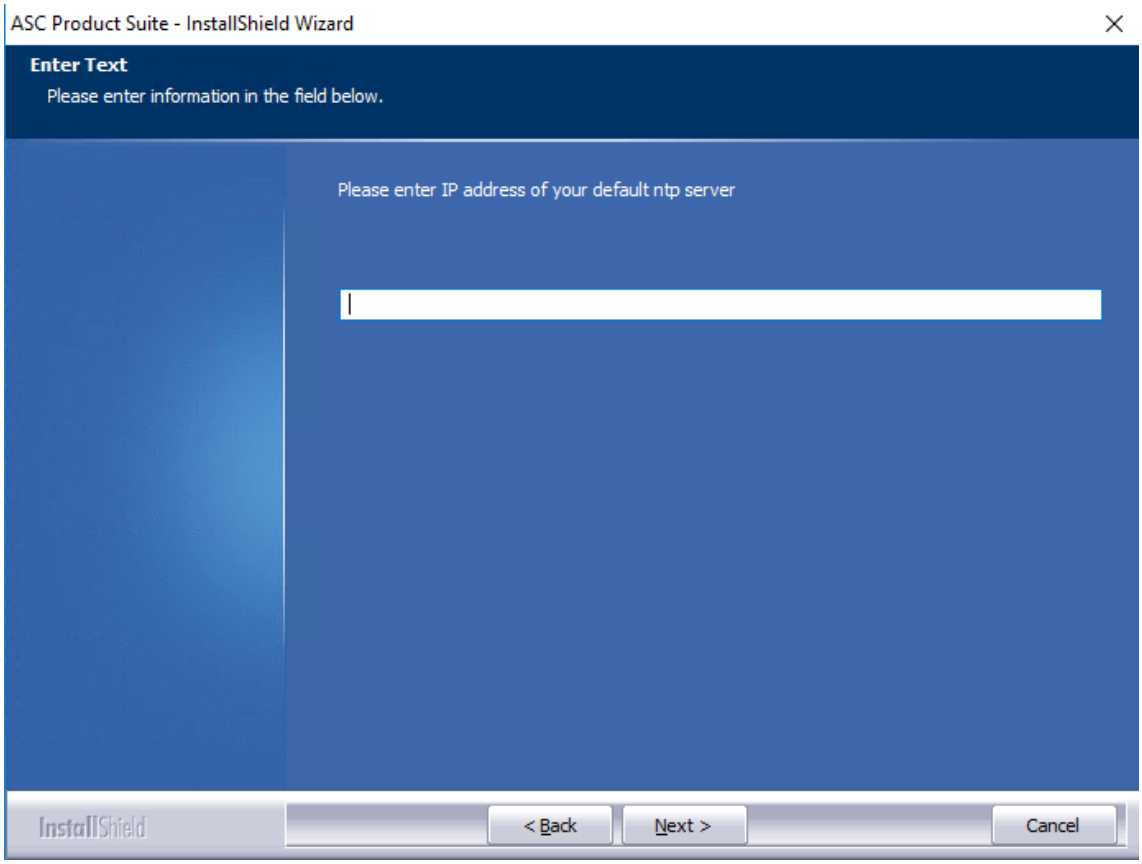

Fig. 12: Enter the address of the NTP server.

20. Enter the IP address of the NTP server.
    NOTICE!
    If the NTP times differ for more than 10 minutes, correct the time manually in the Windows control panel before.
21. Click on the button *Next* to confirm the entry.
    ⇨ The window to select the features appears.
22. If you install a multi-server system, deactivate the following features for the servers on which the features are not used.
    NOTICE!
    In multi-server systems, the components of the application server (app server) and the database are necessary on one server only. You can use these features in parallel on several servers, too, though.

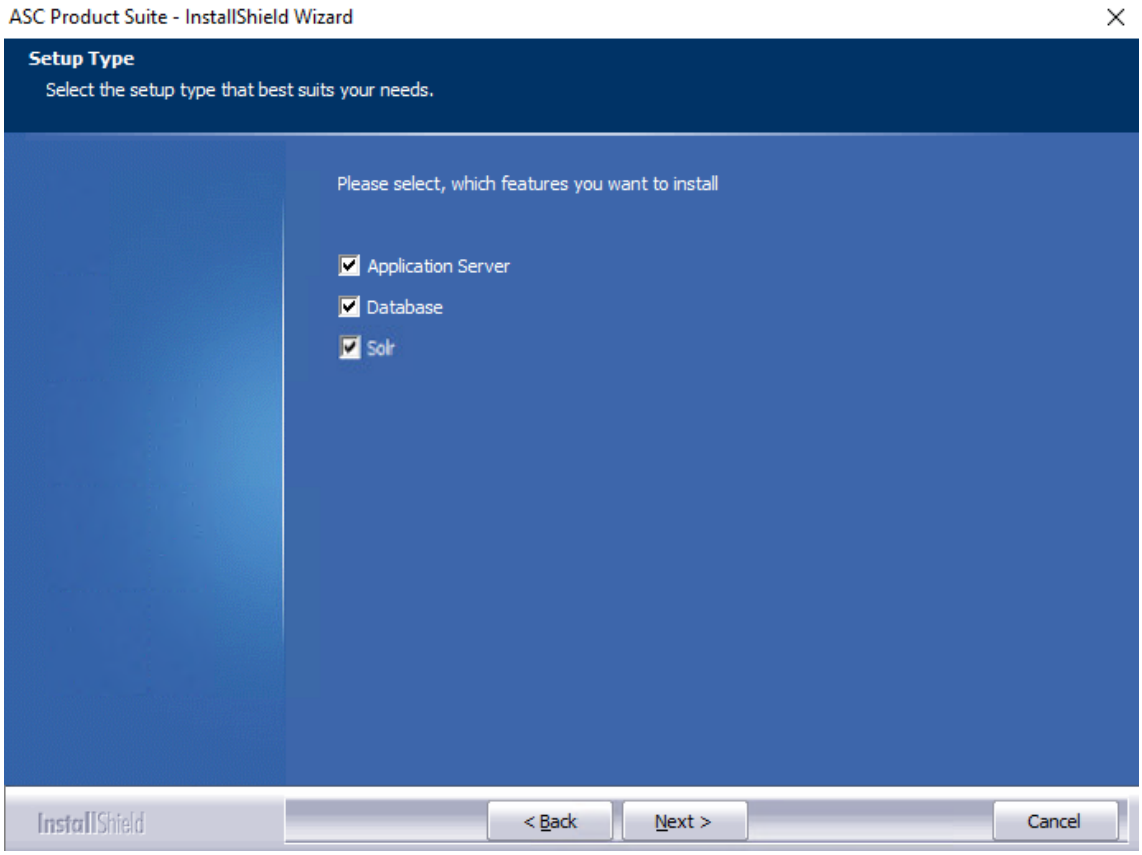

Fig. 13: Select features for the installation

Single-server systems

Select the following options to install a single-server system:

◉	Application server	The selection includes all relevant services for the web applications, i. e. also the function of an app server. Activate this option if the Enterprise Core is supposed to run on this server.
◉	Database	Activate this option to install the provided PostgreSQL database on the same server.

Multi-server systems

For multi-server systems, the following installations options are available:

Server with Enterprise Core, PostgreSQL database, and recording components

◉	*Application server*	Activate this option if the Enterprise Core is supposed to run on this server.
◉	*Database*	Activate this option if the database is supposed to be installed on this server.
○	*Database*	Deactivate this option, if you want to install the database on a separate server.

Exclusively PostgreSQL server

◉	*Database*	Activate this option if only a PostgreSQL database is supposed to be installed on this server.

Exclusively recording server

○	*Application server*	Deactivate this option, if this server is used for recording only.
○	*Database*	Deactivate this option, if this server is used for recording only.

Solr

Select the function *Solr* if you would like to use full-text search in INSPIRATION*neo*.

1. Click on the button *Next* to confirm the entry.
2. When installing the database on the same server, continue with the following chapter: chapter "Install internal database", p. 23
3. When you have installed the database externally, continue with the following chapter: chapter "Install external database", p. 24

ⓘ After a software update of *neo* version 6.5 or higher and the subsequent installation of Solr for full-text search, each previously created analysis engine or previously created project must be saved again without changes to ensure proper language mapping in the *neo* database.

9.1 Install internal database

When installing the database on the same server, a query appears concerning the drive where the database is supposed to be installed

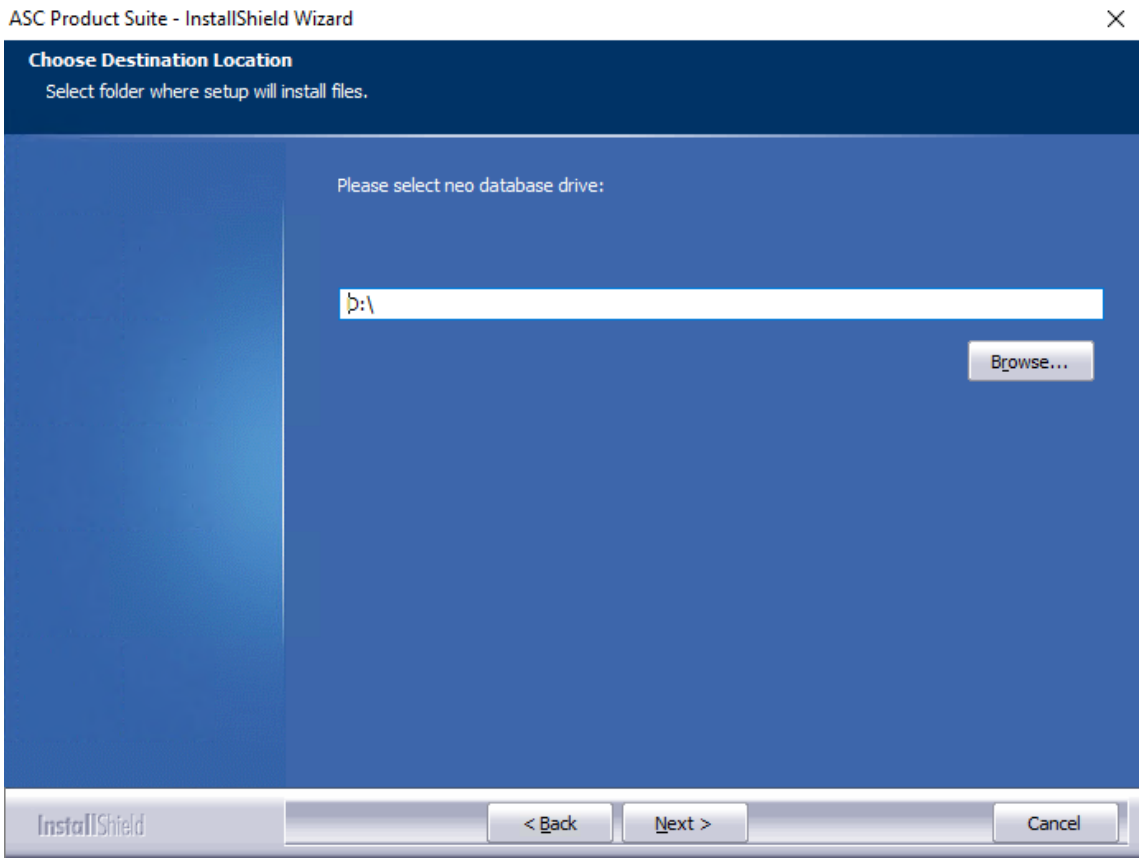

Fig. 14: Select target drive for the internal database

1. Click on the button *Browse* to select the drive where the database is supposed to be saved.
   ⇨ The directory *ASCDB* is created.
2. Click on the button *Next*.
   ⇨ If you have installed several network cards, carry out the installation routine to select the IP address for certificate creation.
   See chapter "Select the IP address for the SSL/TLS certificate", p. 30.

- ⇨ If you have installed only one network card, the certificate is issued for the configured IP address automatically. The installation routine then guides you directly to the WinPcap installation. See chapter "Install WinPcap", p. 32
- ⇨ If you would like to install a server server without recording, you can skip the installation of WinPcap by clicking on the button Cancel. The installation routine then guides you directly to the ASC Updater. See chapter "Start updater", p. 34.

9.2 Install external database

When you have installed the database externally, the following queries to configure the connection data appear.

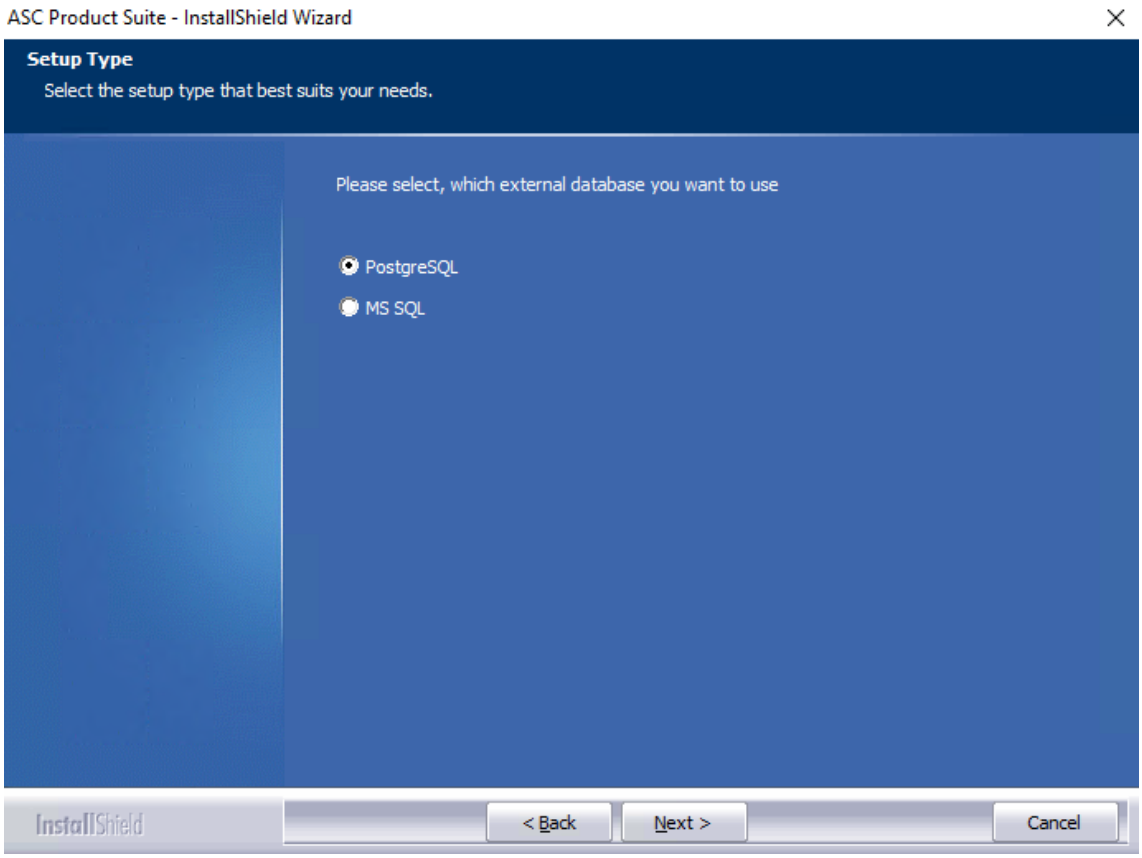

Fig. 15: Select the type of the external database

1. Select the type of the external database which has already been installed.
2. Click on the button *Next* to confirm the entry.
   - ⇨ The window appears for entering the IP address of the external database

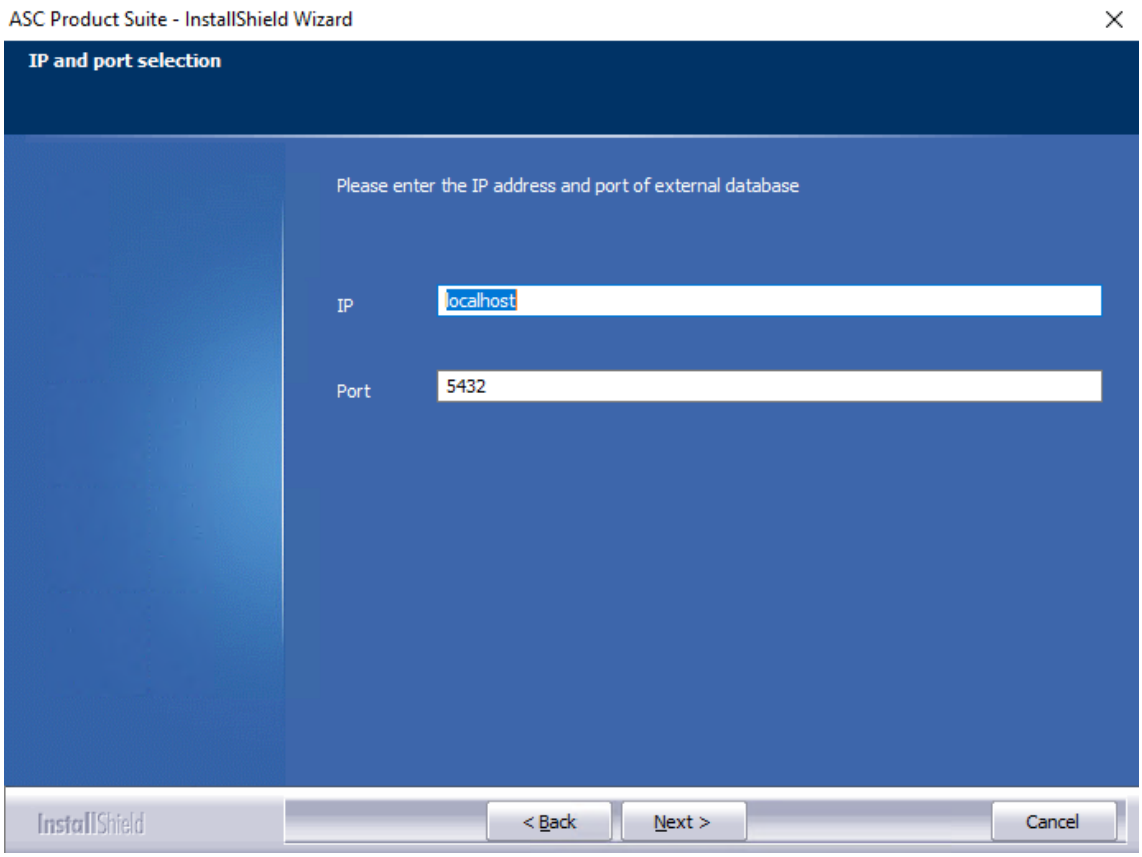

Fig. 16: Create shortcut to the external database

3. To create a shortcut to the external database, enter the IP address of the server on which the database has been installed as well as the configured port.
4. Click on the button *Next* to save the entries.
   ⇨ When installing an MSSQL database, the following window appears:

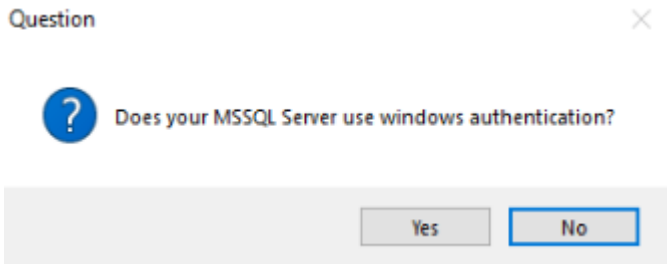

Fig. 17: Prompt for the MSSQL authentication

5. Click on the button *Yes* to activate Windows authentication.
   ⇨ MSSQL authentication is deactivated.
6. Click on the button *No* to activate MSSQL authentication.
   ⇨ Windows authentication is deactivated.
   ⇨ If an additional server is installed in multi-server systems for which the option *Solr* has not been activated, the following window appears:

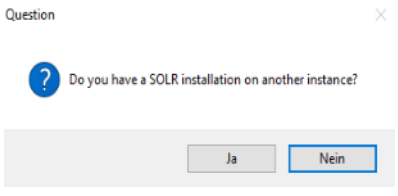

Fig. 18: Prompt for Solr server instance

7. Click on the button *No* if you have not installed the function *Solr* on any server.
8. Click on the button *Yes* if you have installed the function *Solr* on a different server.
   ⇨ The window to enter the IP address appears:

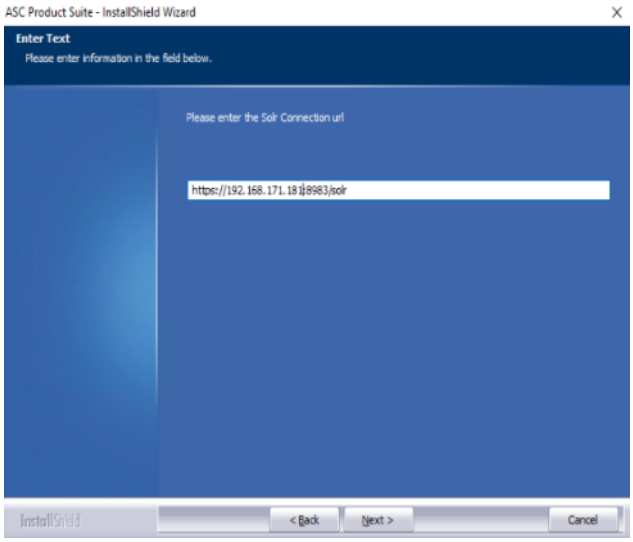

Fig. 19: Enter IP address of server instance for Solr

9. Enter the IP address of the server where you have installed the function *Solr*.
   Example: *https://192.168.171.181:8983/solr*.
10. Click on the button *Next* to save the entries.
    ⇨ The window appears for entering the login data for the external database.

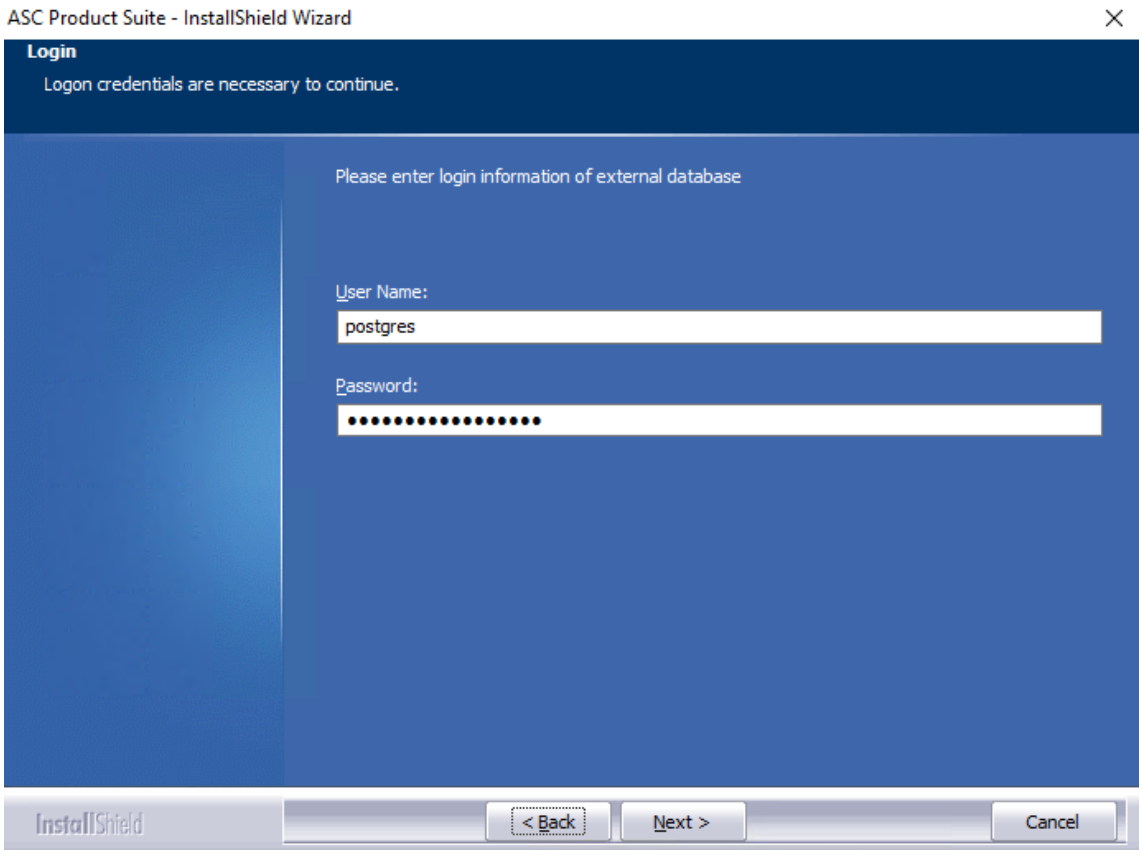

Fig. 20: Configure users for the database

11. Enter the login data for the user of the external database.
    Make sure that the user has all rights to be able to create databases.

12. Click on the button *Next* to save the entries.
    ⇨ When installing an MSSQL database, the following window appears:

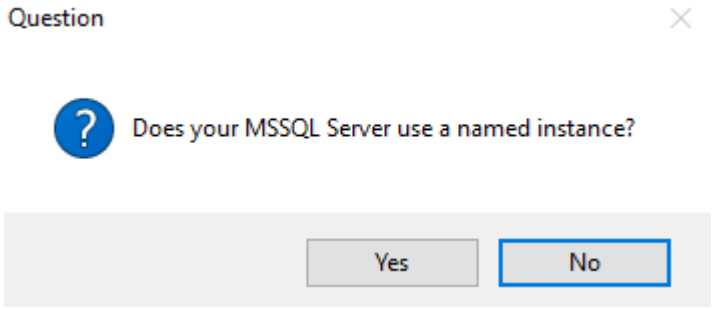

Fig. 21: Prompt for the MSSQL server instance

13. Click on the button *No* if you do not want to use any specific MSSQL instance.
14. Click on the button *Yes* to enter a name for the MSSQL instance.
    ⇨ The window for entering the name of the MSSQL instance appears.

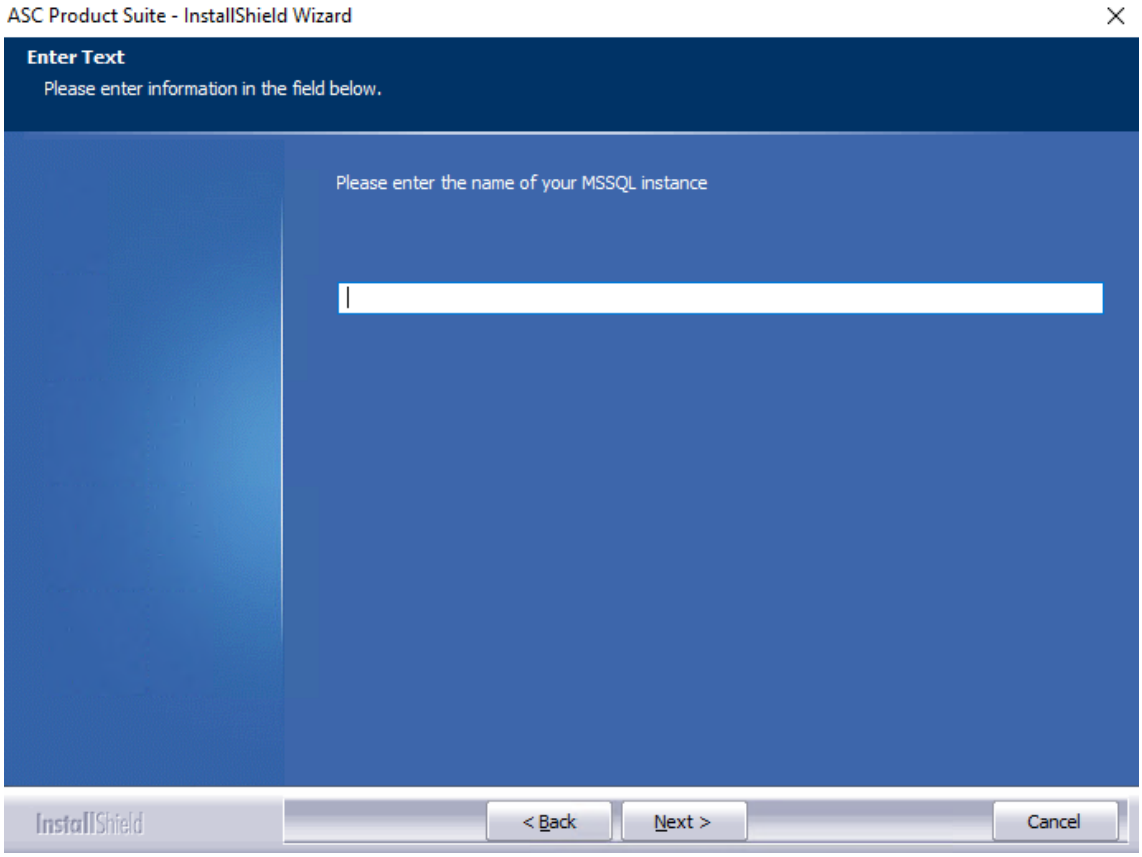

Fig. 22: Enter name of MSSQL instance

Please note that the MSSQL instance must already exist on the SQL database.

15. Click on the button *Next* to save the entries.
    ⇨ The window for starting the installation process appears.

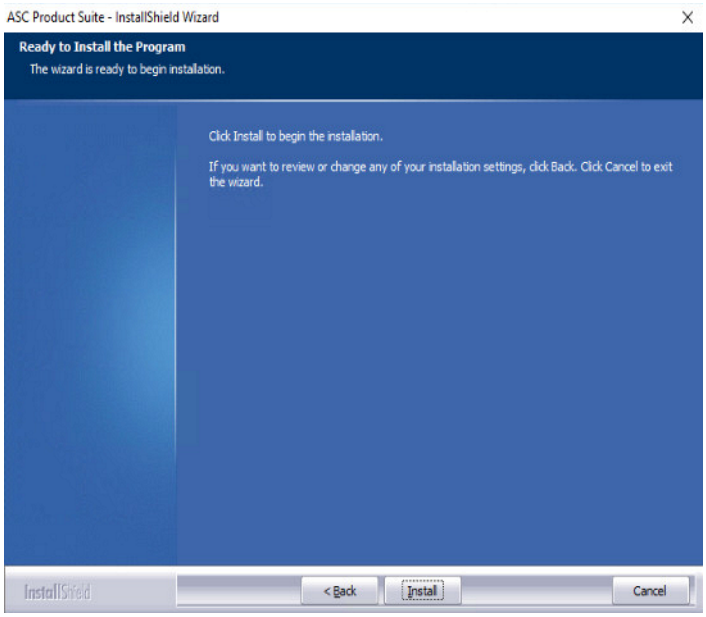

Fig. 23: Start installation process

16. Click on the button *Install* to start the installation.
    ⇨ The installation progress is displayed.

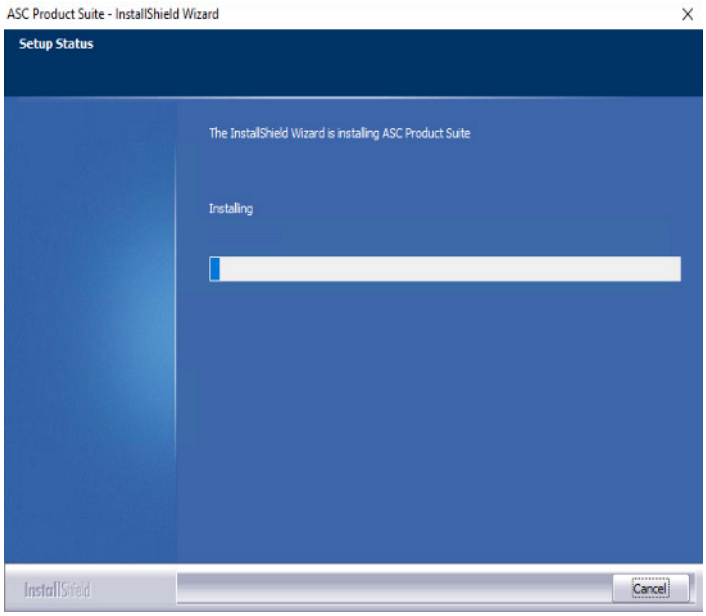

Fig. 24: Information about the installation progress

The installation can take a certain time.

17. Now you can check the HTTP or the HTTPS ports and change them if necessary.
    ⇨ The following window appears:

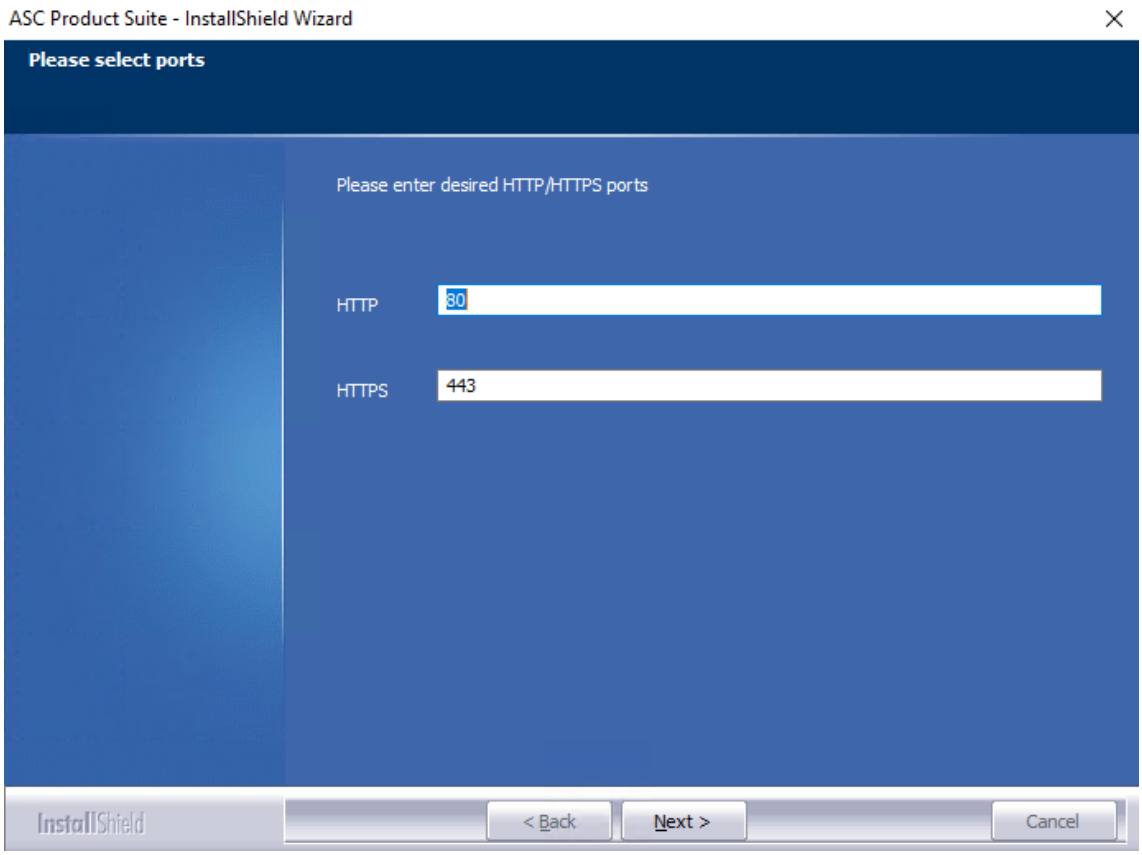

Fig. 25: Configure web server ports

18. Enter the ports for HTTP and HTTPS to connect to the web server.
19. Click on the button *Next*.
    - ⇨ If you have installed several network cards, carry out the installation routine to select the IP address for certificate creation.
      See chapter "Select the IP address for the SSL/TLS certificate", p. 30
    - ⇨ If you have installed only one network card, the certificate is issued for the configured IP address automatically. The installation routine then guides you directly to the WinPcap installation. See chapter "Install WinPcap", p. 32
    - ⇨ If you would like to install a server without recording, you can skip the installation of WinPcap by clicking on the button Cancel. The installation routine then guides you directly to the ASC Updater. See chapter "Start updater", p. 34.

9.3 Select IP protocol

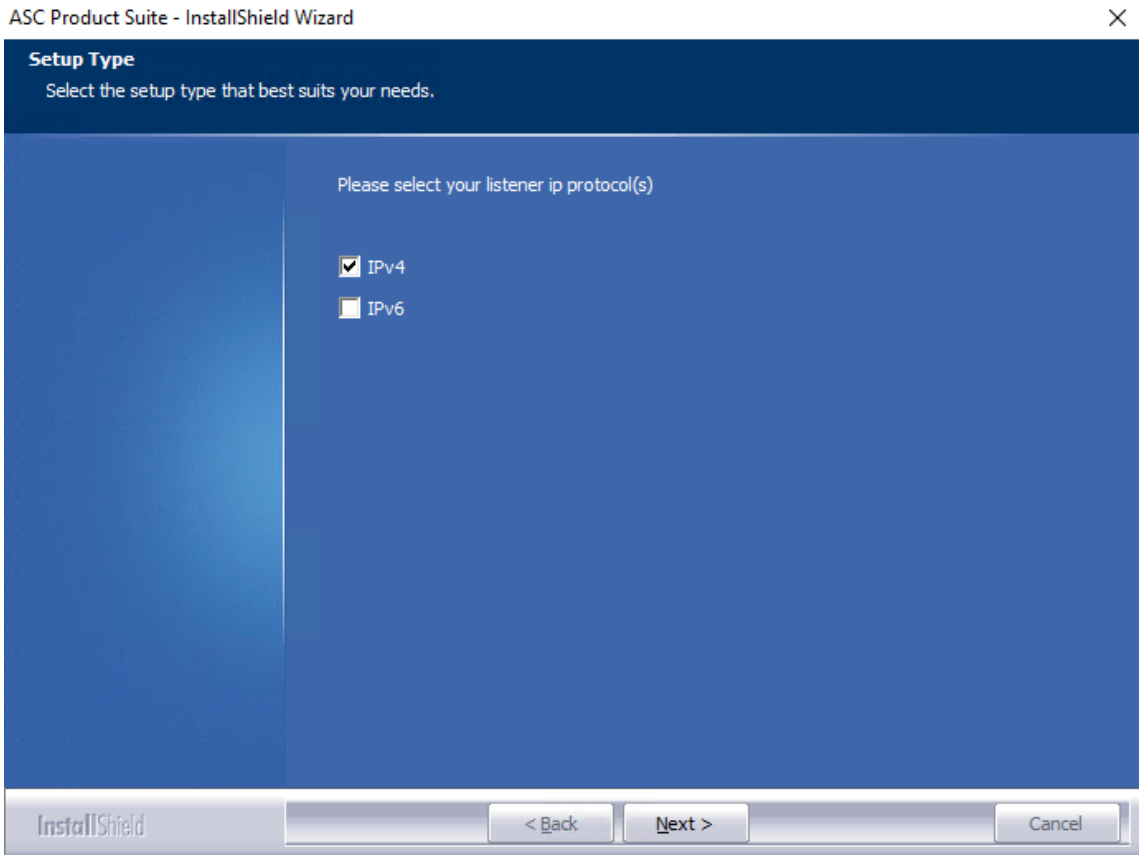

Fig. 26: Select IP protocol

1. Select the IPv4 protocol if you would like to use the default addresses. Select the IPv6 protocol if you would like to use an extended number of addresses.
2. Click on the button *Next*.
   ⇨ The window for starting the installation process appears.

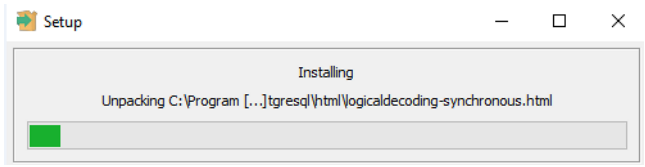

Fig. 27: Installing the IP protocol

9.4 Select the IP address for the SSL/TLS certificate

NOTICE! If several network cards have been installed and configured, a window appears in which you can select for which card the SSL/TLS certificate is supposed to be created.

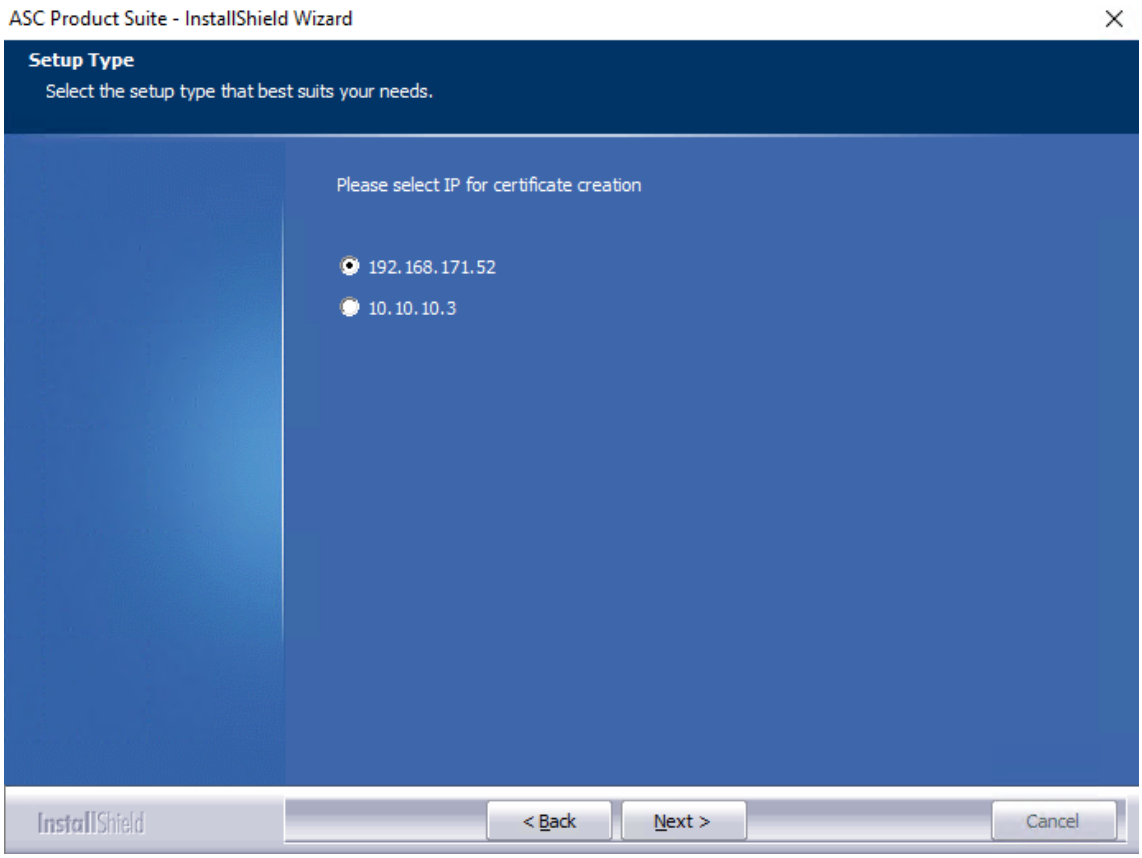

Fig. 28: Select IP address of the network card (example Ipv4)

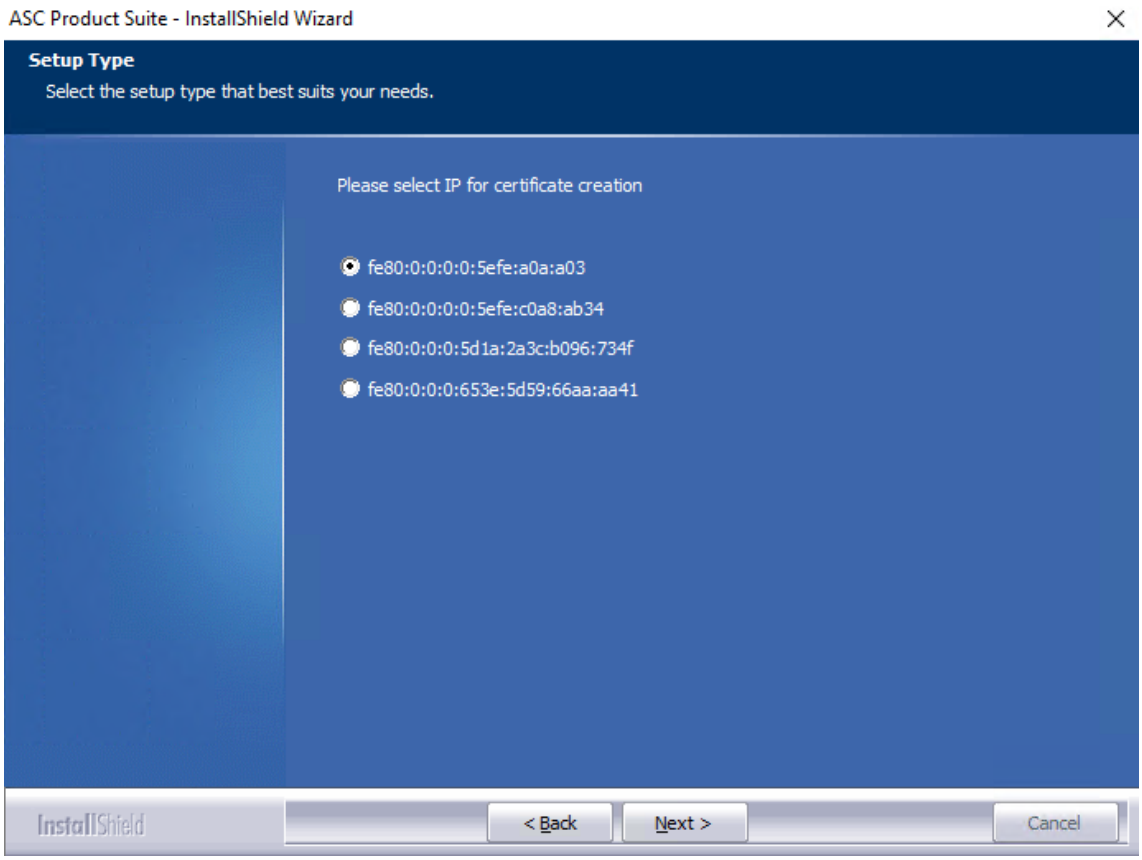

Fig. 29: Select IP address of the network card (example Ipv6)

1. Select the IP address of the network card for which the certificate is supposed to be created.

2. Click on the button *Next*.
   ⇨ The installation routine to install WinPcap starts.

If you would like to install a server without recording, you can skip the installation of WinPcap. Continue with chapter "Start updater", p. 34.

9.5 Install WinPcap

An installation of WinPcap is only required on servers on which a recording is running. During the installation of servers without recording components, you can cancel the following routine by clicking on the button *Cancel*.

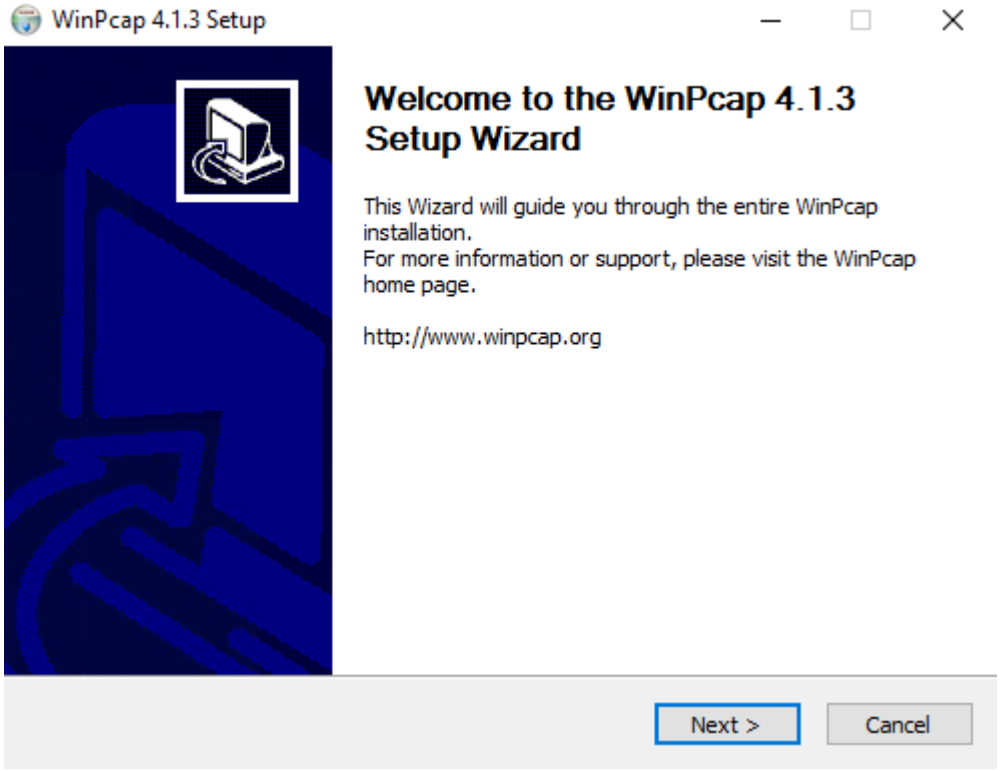

Fig. 30: Installation Wizard welcome screen

1. Click on the button *Next*.
2. Click on the button *Next*.
   ⇨ The window with the license agreement appears.

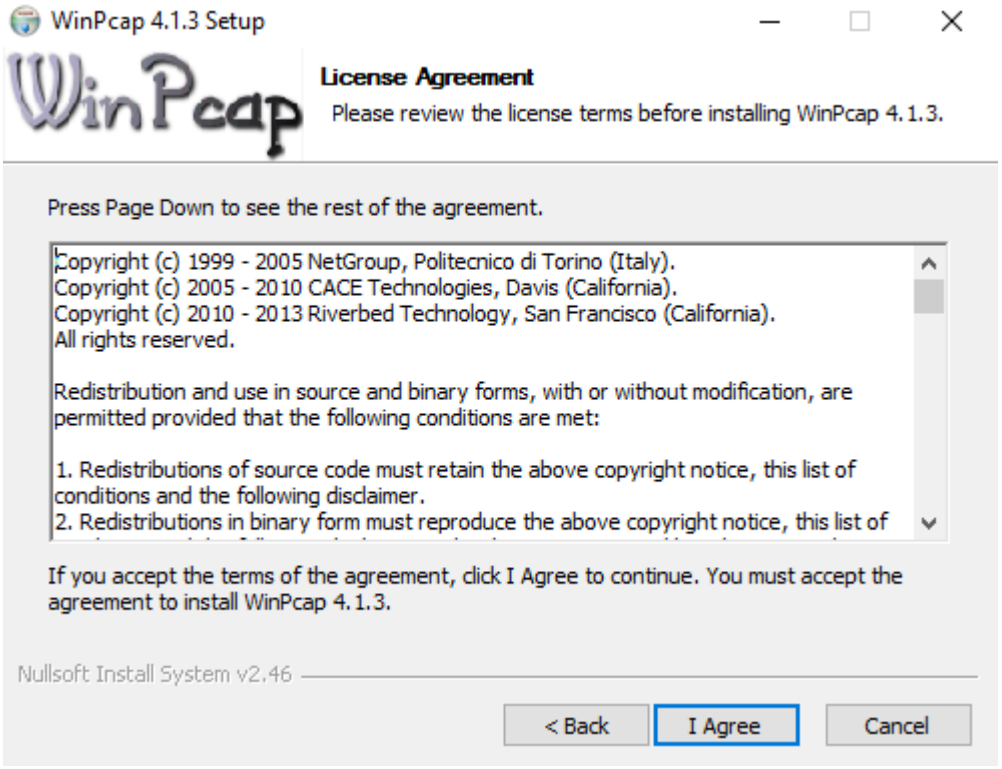

Fig. 31: License Agreement

3. Click on the button *I Agree* to accept the license agreement.
   ⇨ The following window appears:

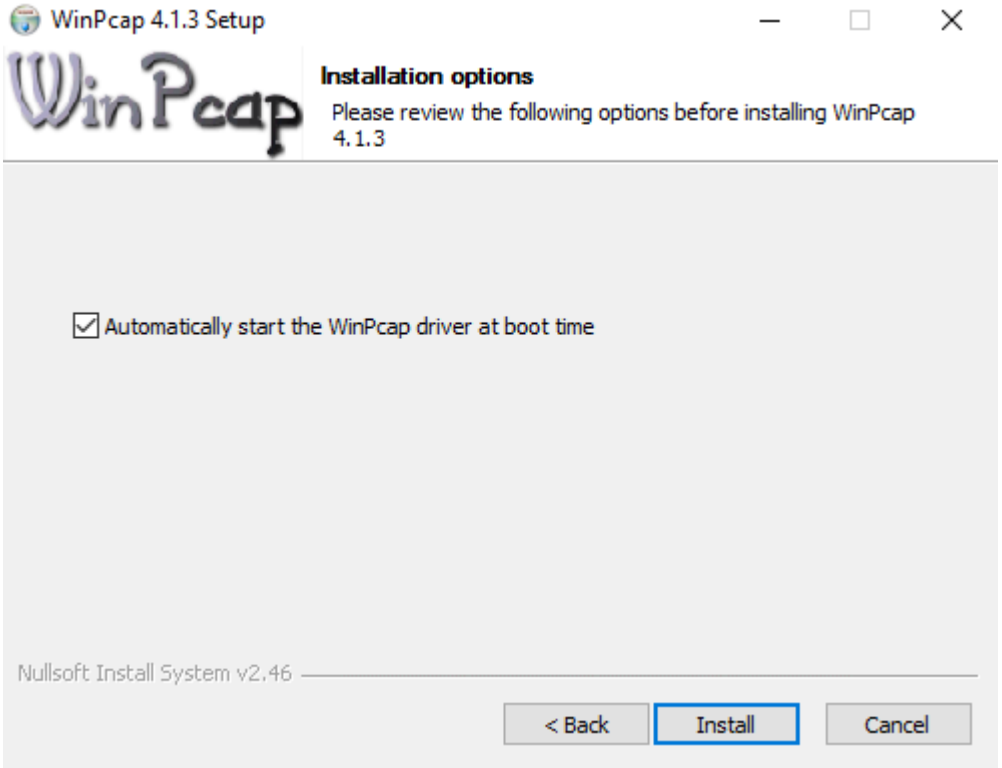

Fig. 32: Start installation of the WinPcap software

4. Start the installation process by clicking on the button *Install*.

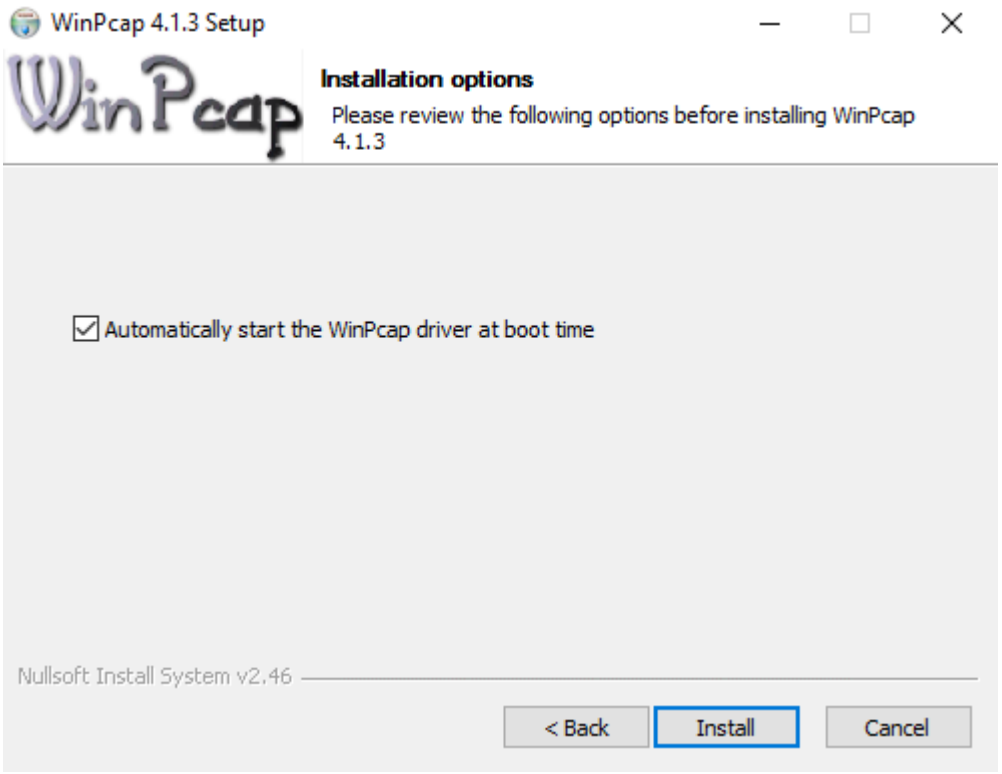

Fig. 33: Finish installation of the WinPcap software

5. To complete the installation of the *WinPcap* software, click on the button *Finish*.

9.6 Start updater

The installation routine directs you to the *ASC Updater*.

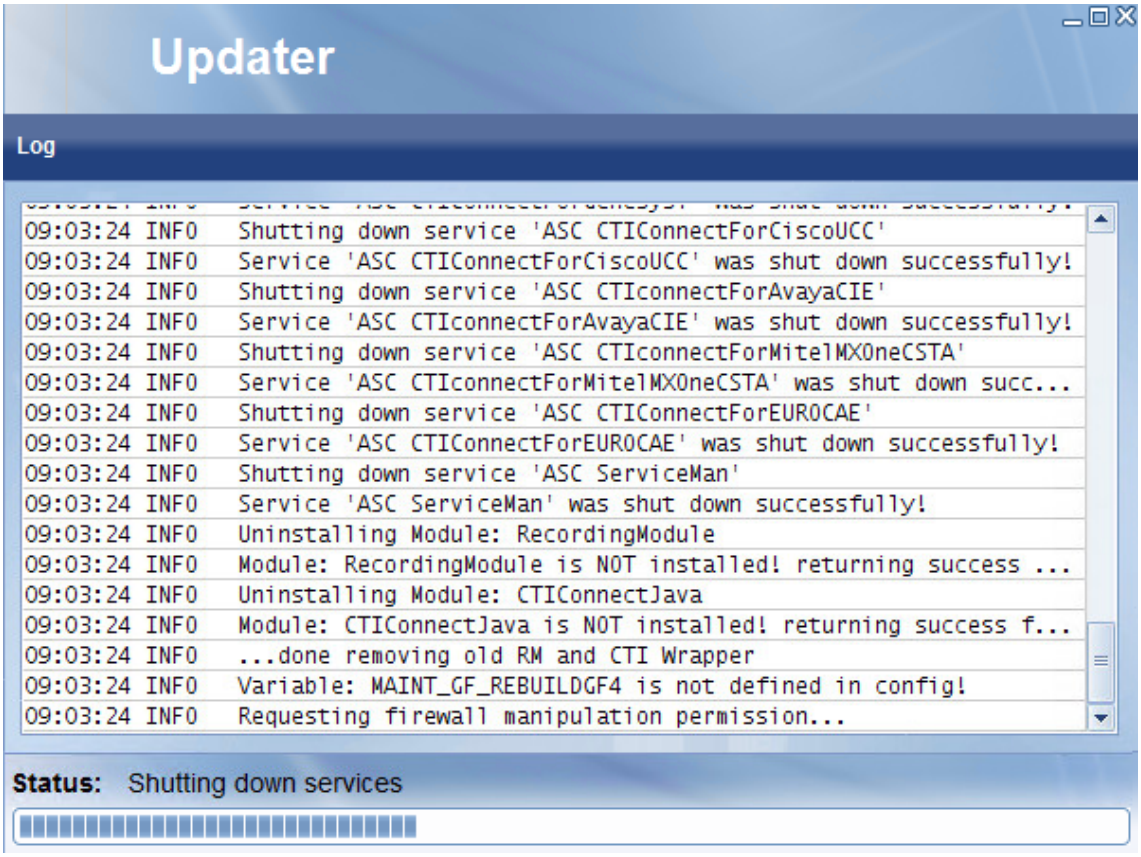

Fig. 34: ASC Updater - Services are shut down

The security prompt to open the firewall ports for the software update appears.

Fig. 35: ASC Updater - Security prompt for firewall

1. Confirm the prompt with *Yes* so that the Updater can continue running.
   ⇨ The prompt to install the device software for recording cards appears.

Fig. 36: Install device driver for recording cards

This prompt only appears when installing the *neo* software on a hardware system.

2. In this dialog window you must select an option for the Updater to continue running.
3. If you would like to use VOIP recording and have not installed recording cards, click on the button *Don't install*.
   If you would like to use TDM recording with recording cards, you must install the device driver for the recording cards. To do so, click on the button *Install*.
   ⇨ The window with the installation report opens.

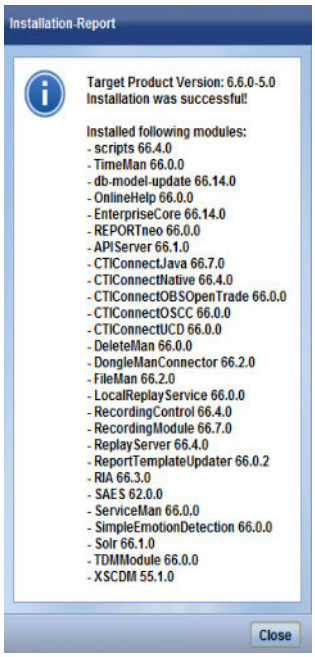

Fig. 37: ASC Updater - Installation report

4. Click on the button *Close* to finish the Updater.
   ⇨ The *InstallShield Wizard* appears again.

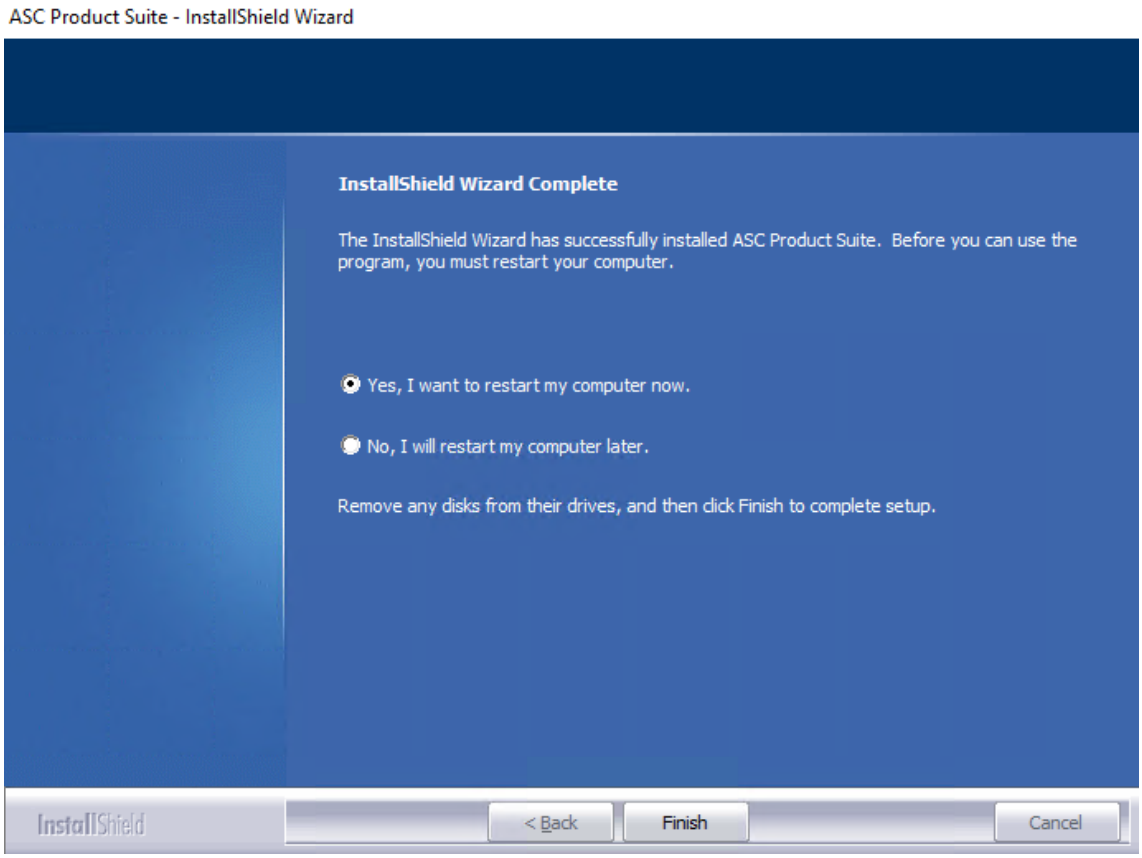

Fig. 38: Finish installation and reboot server

5. Select the option *Yes, I want to restart my computer now*.
6. Finish the installation of the *neo* software by clicking on the button *Finish*.

10 Import HTTPS certificate

10.1 Request certificate via CSR

If you would like to request a certificate at an authorized authentication authority, you can create a request with your company-specific data by means of the Certificate Import Tool.

1. Open the Windows Explorer to call up the tool.
2. Change to the folder *C:\Program Files (x86)\ASC\ASC Product Suite\scripts*.
3. Double-click on the file *certimporter.exe*.
   ⇨ The window Certificate Import Tool appears.

Fig. 39: Certificate Import Tool

4. Select the menu item *Generate CSR* in the navigation bar to create a Certificate Signing Request.
   ⇨ The window to select the certificate type appears.
5. From the drop-down list, select the type of the certificate that you would like to create.
   ⇨ A window CSR appears where you can enter company-specific data.

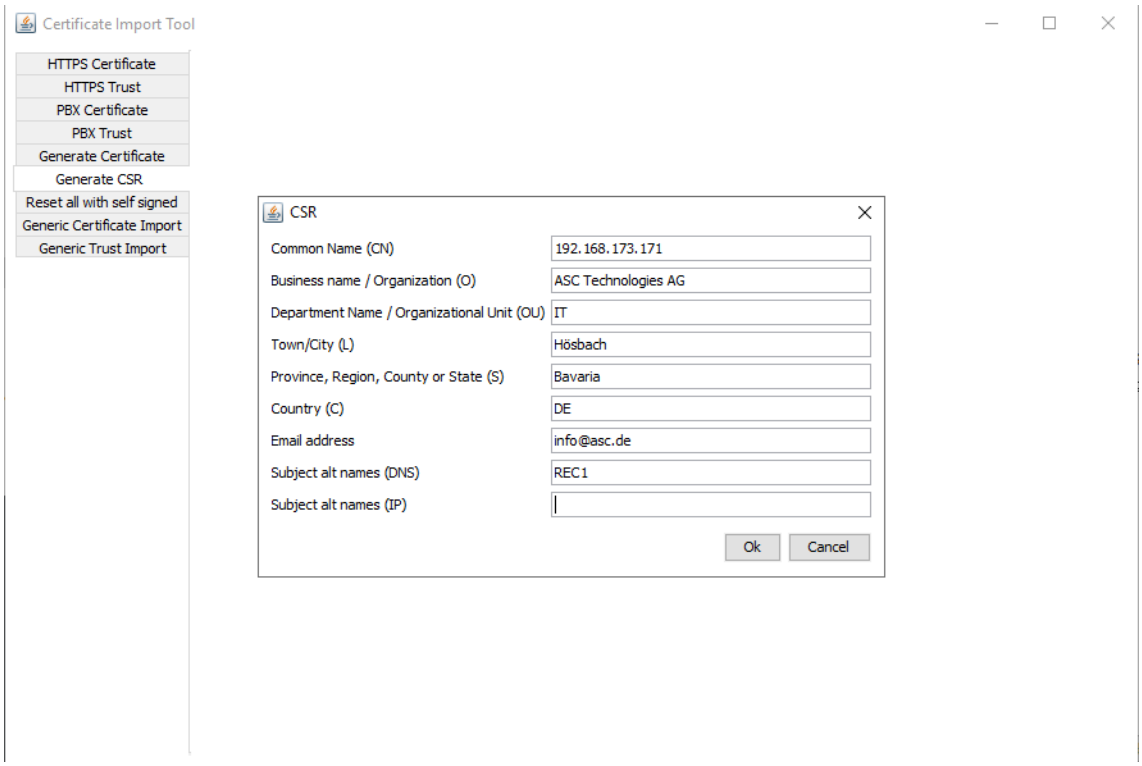

Fig. 40: Enter company-specific parameters for authentication

6. Enter the company data.
7. Click on the button *OK*.
   ⇨ The Explorer window appears where you can select the storage directory.
8. Select the directory in which you would like to save the request for the certificate.
9. Click on the button *Open*.
   ⇨ The following success message appears:

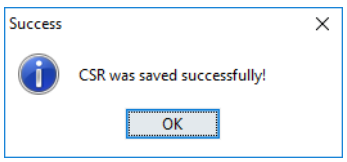

Fig. 41: Success message

10. Click on the button *OK*.
11. You can send the file to a certification authority to request a certificate.

When importing certificates without a private key or with an inadequate private key, it may be possible that the system will not boot again. There is a chance that this happens, too, when the certificate has not been create via a CSR.

12. You can import the new certificate via the option *X.509/Private key*. See chapter "Import X.509/Private key", p. 39.

10.2 Import customer-specific HTTPS certificate

If you would like to use a customer-specific certificate, you can import it with the program *certimporter.exe*.

1. Change to the folder *C:\Program Files (x86)\ASC\ASC Product Suite\scripts*.
2. Open the file *certimporter.exe*.
   ⇨ The window Certificate Import Tool appears.

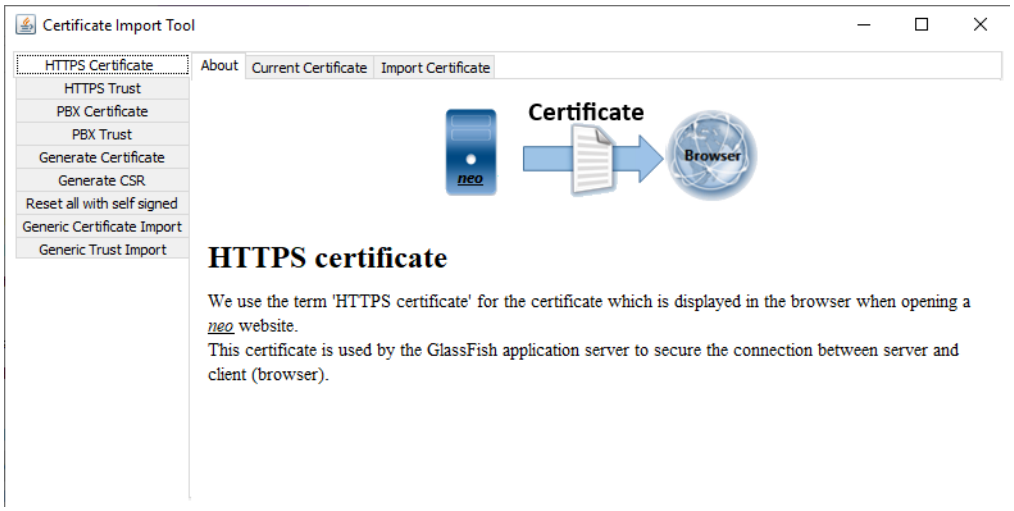

Fig. 42: Certificate Import Tool

The following formats are supported:

- *PKCS12*
- *X.509/Private key*

10.2.1 Import X.509/Private key

1. Select the menu item *HTTPS Certificate* in the navigation bar.
2. Click on the tab *Import Certificate*.
3. If you certificate is a X.509/Private, select the option *Certificate X.509 (RSA Private key)*.
4. Click on the button next to the field *Certificate X.509* to select your certificate.

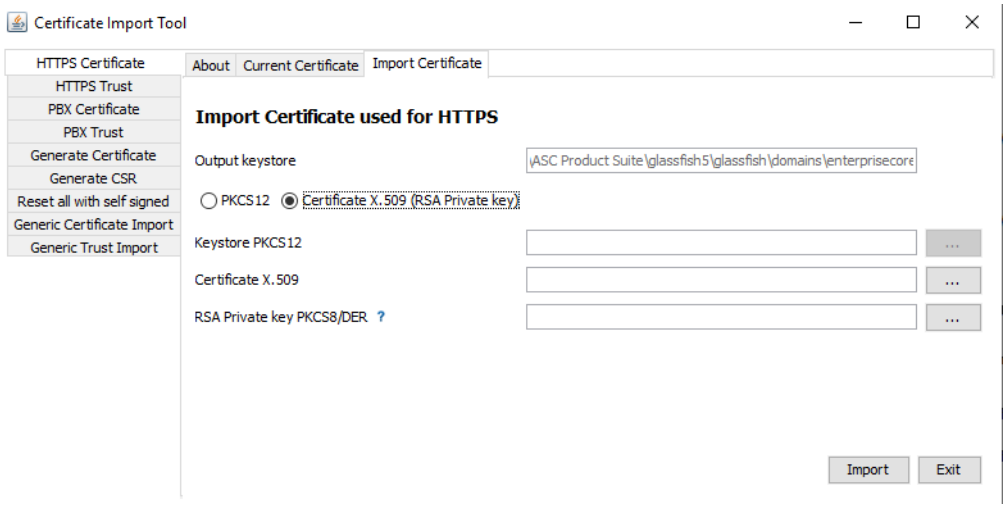

Fig. 43: Import X.509

5. Click on the button *Import*.
   ⇨ The window to enter the password for the private key appears.

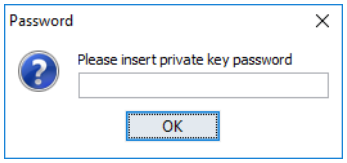

Fig. 44: Enter password for the private key

6. Enter the password for your private key.
   If you do not use a password, leave this field empty.

7. Click on the button *OK* to confirm the password.
   ⇨ A message will inform you about the successful import.

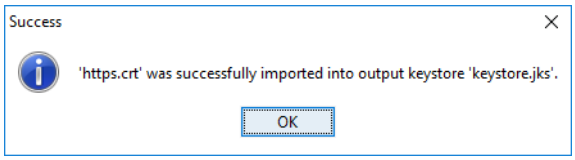

Fig. 45: Message - Successful import

8. Click on the button *OK* to confirm the success message.
9. Click on the button *Exit* to exit the program.
10. Restart the Glassfish server so that the certificate will be applied.
11. In the tab *Current Certificate*, you can check the currently valid certificate.

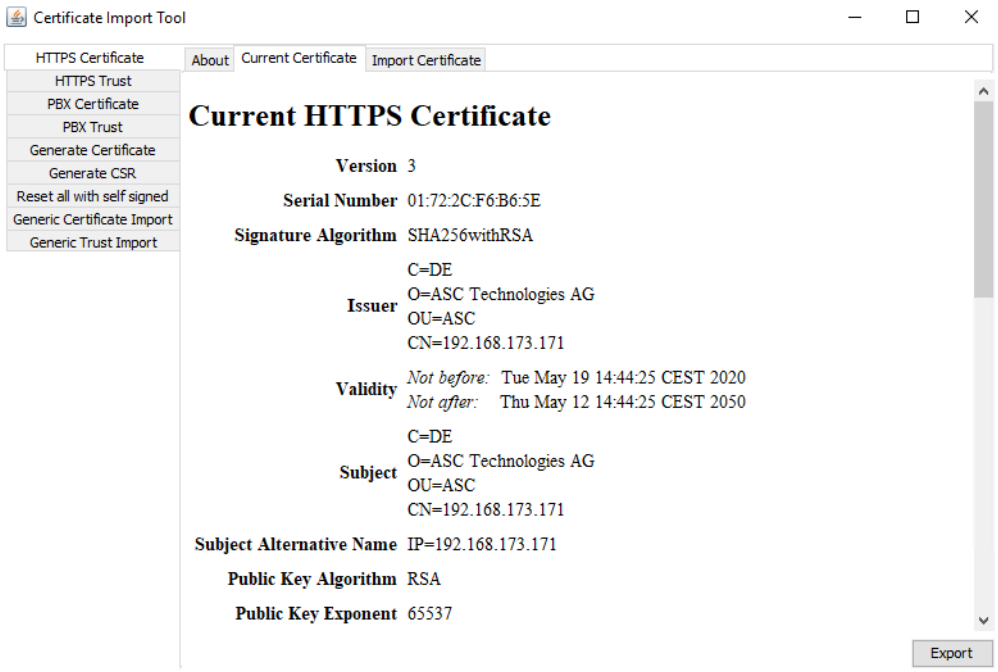

Fig. 46: Check currently valid HTTPS certificate

10.2.2 Import PKCS12

1. Select the menu item *HTTPS Certificate* in the navigation bar.
2. Click on the tab *Import Certificate*.
3. If you certificate is a PKCS12 Keystore, select the option *PKCS12*.
4. Click on the button next to the field *Keystore PKCS12* to select your PKCS12 Keystore.

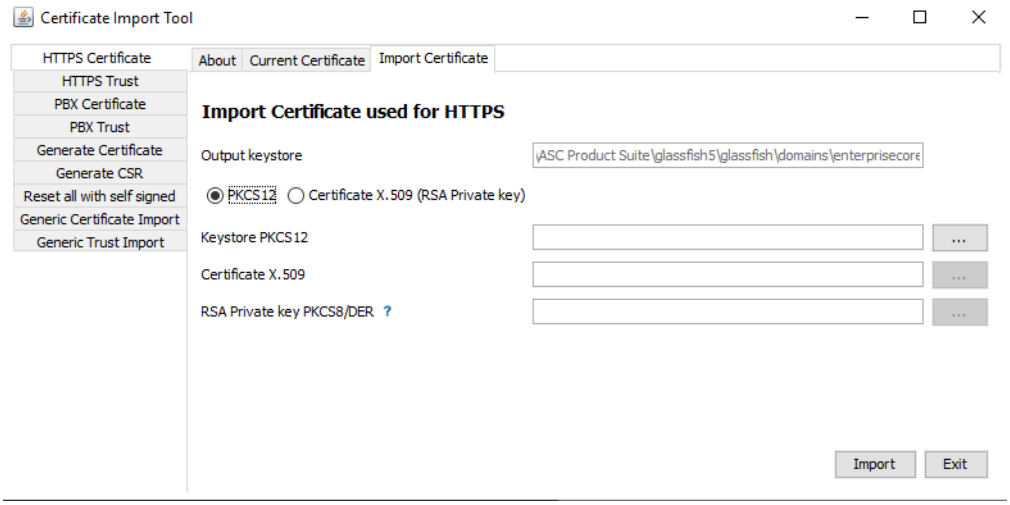

Fig. 47: Import PKCS12 Keystore

5. Click on the button *Import*.
   ⇨ The window to enter the alias for the PKCS12 Keystore appears.

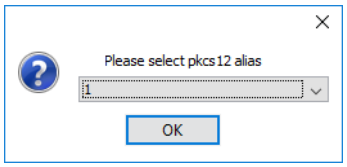

Fig. 48: Confirm alias

6. Click on the button *OK* to confirm the alias.
   ⇨ The window to enter the password appears.

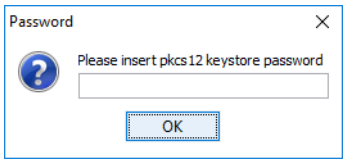

Fig. 49: Enter password for PKCS12 Keystore

7. Enter the password for your PKCS12 Keystore.
   If you do not use a password, leave this field empty.
8. Click on the button *OK* to confirm the password.
9. Click on the button *Exit* to exit the program.
10. Restart the Glassfish server so that the certificate will be applied.
11. In the tab *Current Certificate*, you can view the currently valid certificate.

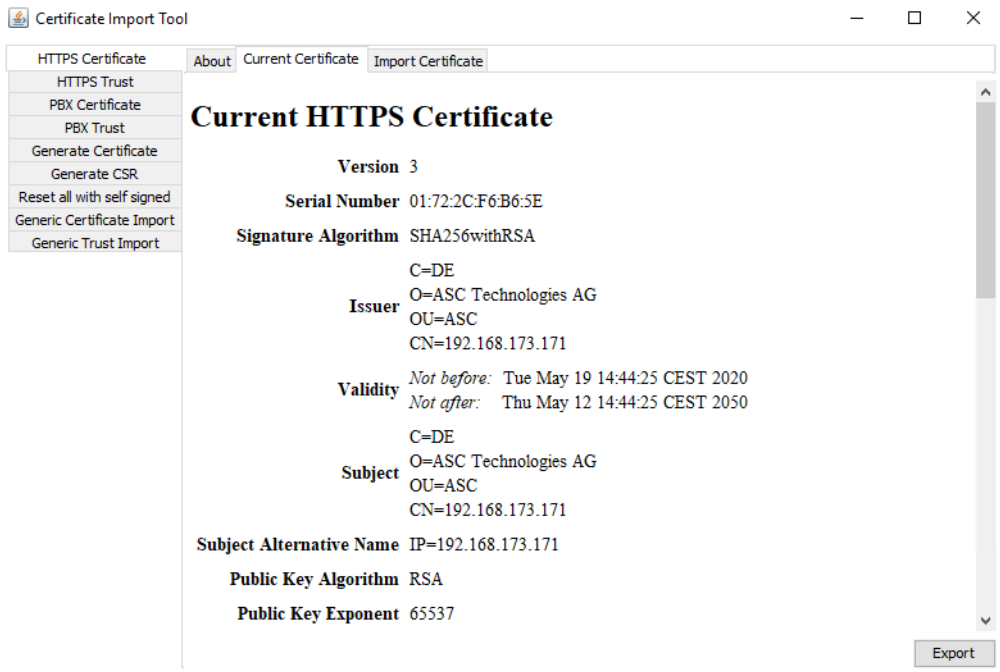

Fig. 50: Check currently valid HTTPS certificate

10.3 Import HTTPS certificate in silent mode installation

If the *neo* software has been installed in silent mode (*/asc silent_mode*), the HTTPS certificate must always be imported manually with the program certimporter.exe, see chapter "Import customer-specific HTTPS certificate", p. 38.

For more information about the installation and update of certificates refer to the administration manual for system providers *Certificate Import Tool*.

List of figures

List of figures

List of tables

Glossary

Glossary

App server

Application server or web server. In the system architectures: the server on which the Enterprise Core and the GlassFish software have been installed.

CSR

Certificate Signing Request

Multi-server system

Recording system in which the individual components (Enterprise Core, recording components, database) are installed on different servers.

NTP

Network Time Protocol NTP is a standard for the synchronization of clocks in computer systems via packet-based communication networks. NTP uses the connectionless transport protocol UDP. It has been developed with the objective to guarantee reliable time verification across networks with variable packet runtime. (Source: Wikipedia 12th June 2018)

Single-server system

Recording system in which all components (Enterprise Core, recording components, database) are installed on the same server.

SNMP

Simple Network Management Protocol is a network protocol and serves to monitor and manage network components. The protocol does not depend on the IP network protocol for the transport. It sends notifications (traps) about the activities on the network components on its own accord.

VoIP

Voice over IP