

Installation der Aufzeichnungssoftware von ASC



Installationsanleitung für Systembetreiber

06.05.2020

Originalanleitung

Produktlinie neo, Version 6.x

Die beschriebenen Funktionen können mit folgenden ASC-Produkten verwendet werden:

EVOIPneo

INSPIRATIONneo

EVOLUTIONneo / XXL / eco

Im Partnerbereich unserer Webseite <http://www.asctechnologies.com> finden Sie immer die aktuellsten technischen Dokumente und Produktaktualisierungen.

Copyright © 2019 ASC Technologies AG. Alle Rechte vorbehalten.

Windows ist ein eingetragenes Markenzeichen der Microsoft Corporation. VMware® ist ein eingetragenes Markenzeichen von VMware, Inc. Alle anderen hier erwähnten Marken und Produktnamen sind das Eigentum ihrer jeweiligen Inhaber.

Inhaltsverzeichnis

1	Allgemeine Hinweise	4
2	Einleitung	5
3	Systemvoraussetzungen	7
4	Installationsvoraussetzungen	8
4.1	Lizenzen	8
5	Redundanzoptionen	9
6	Interne Datenbank	10
7	Externe Datenbanken	11
8	Aufzeichnungssoftware installieren	12
8.1	Interne Datenbank installieren	21
8.2	Externe Datenbank installieren	22
8.3	IP-Protokoll auswählen	27
8.4	IP-Adresse für das SSL/TLS-Zertifikat auswählen	27
8.5	WinPcap installieren	29
8.6	Updater starten	31
9	HTTPS-Zertifikat importieren	35
9.1	Zertifikat über CSR anfordern	35
9.2	Kundenspezifisches HTTPS-Zertifikat importieren	36
9.2.1	X.509/Private key importieren	36
9.2.2	PKCS12 importieren	38
	Abbildungsverzeichnis	40
	Tabellenverzeichnis	42
	Glossar	43

Allgemeine Hinweise

ASC steht im Kontext dieses Dokuments für die ASC Technologies AG, deren Tochtergesellschaften, Niederlassungen und Vertriebsbüros. Deren aktuelle Übersicht kann auf der Webseite unter <https://www.asctechnologies.com> eingesehen werden.

ASC übernimmt keinerlei Gewähr für die Aktualität, Korrektheit, Vollständigkeit oder Qualität der in den Anleitungen bereitgestellten Informationen.

ASC kontrolliert regelmäßig den Inhalt der veröffentlichten Anleitungen auf Übereinstimmung mit der beschriebenen Hard- und Software. Dennoch können Abweichungen nicht ausgeschlossen werden. Notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Einige Aspekte der ASC-Technologie werden in allgemeiner Form beschrieben, um das Eigentum und die vertraulichen Informationen und/oder Geschäftsgeheimnisse von ASC zu schützen.

Die Softwareprogramme und Anleitungen von ASC sind urheberrechtlich geschützt. Alle Rechte an den Anleitungen sind vorbehalten, auch die der Reproduktion und/oder Vervielfältigung in jeglicher Form, sei es fotomechanisch, drucktechnisch oder auf digitalen Datenträgern. Dies gilt auch für Übersetzungen. Nachdruck der Anleitungen, vollständig oder auszugsweise, ist nur mit schriftlicher Genehmigung von ASC gestattet.

Maßgebend ist, soweit nicht anders angegeben, der technische Stand zum Zeitpunkt der Auslieferung von Software, Geräten und Anleitungen durch ASC. Technische Änderungen ohne gesonderte Ankündigung bleiben vorbehalten. Bisherige Anleitungen verlieren ihre Gültigkeit.

Es gelten die Allgemeinen Verkaufs- und Lieferbedingungen von ASC in ihrer jeweils gültigen Fassung.

2 Einleitung

Dieses Dokument beschreibt die Installation der neo-Software.



Stellen Sie sicher, dass Sie für die Installation die vollen Administratorrechte besitzen.



Während der Installation und während einer Aktualisierung der neo-Software muss On-access Scanning deaktiviert sein.



Bitte stellen Sie **vor** der Installation der neo-Software sicher, dass die Installation und Konfiguration von Microsoft Windows gemäß unseren Vorgaben durchgeführt wurde.



Informationen zur Installation und Konfiguration von Microsoft Windows finden Sie in der jeweiligen Installationsanleitung für Systembetreiber *Konfiguration Windows Server 2012 R2*, *Konfiguration Windows Server 2016* oder *Konfiguration Windows Server 2019*.

Die neo-Software beinhaltet verschiedene Applikationen. Mit der Grundinstallation sind folgende Applikationen freigeschaltet:

- Portal
- System Configuration
- System Monitoring
- POWERplay Web

Alle weiteren Applikationen sind lizenzpflichtig.

Individuelle Aufzeichnungslösungen und Funktionen sind lizenzabhängig und erst verfügbar, wenn die entsprechende Lizenz eingespielt wurde.

Weitere Informationen zur Lizenzverwaltung finden Sie in der Administrationsanleitung *Lizenzverwaltung*.

Jedes neo-System wird initial als 1-Mandanten-System mit einem vordefinierten Mandanten, dem 1st-Tenant, installiert. Auch der Systembetreiber wird automatisch als Mandant angelegt. Er ist aber nicht als Mandant im eigentlichen Sinne zu betrachten.

Für den jeweiligen Administrator des Systembetreibers und des vordefinierten Mandanten wird bei der Installation des Systems standardmäßig ein Account mit folgenden Login-Daten angelegt:

Login-Daten für den Administrator des Systembetreibers:

Benutzername:	<i>system-admin</i>
<u>neo</u> -Version < 6.3	
Standard-Passwort:	1
	Wenn vor einer Softwareaktualisierung auf eine <u>neo</u> -Version ≥ 6.3 das Standard-Passwort 1 noch nie geändert wurde, muss beim nächsten Login das Passwort geändert oder durch erneute Eingabe bestätigt werden.
	Wenn vor einer Softwareaktualisierung auf eine <u>neo</u> -Version ≥ 6.3 das Standard-Passwort schon einmal geändert wurde, wird das geänderte Passwort beibehalten.
<u>neo</u> -Version ≥ 6.3	
Standard-Passwort:	A\$c123

Tab. 1: Login-Daten - Systembetreiber

Login-Daten für den Administrator des 1. Mandanten:

Benutzername:	<i>1st-tenant-admin</i>
<u>neo</u> -Version < 6.3	
Standard-Passwort:	<i>1</i>
	Wenn vor einer Softwareaktualisierung auf eine <u>neo</u> -Version ≥ 6.3 das Standard-Passwort <i>1</i> noch nie geändert wurde, muss beim nächsten Login das Passwort geändert oder durch erneute Eingabe bestätigt werden.
	Wenn vor einer Softwareaktualisierung auf eine <u>neo</u> -Version ≥ 6.3 das Standard-Passwort schon einmal geändert wurde, wird das geänderte Passwort beibehalten.
<u>neo</u> -Version ≥ 6.3	
Standard-Passwort:	<i>A\$c123</i>

Tab. 2: Login-Daten - 1. Mandant

Je nach Lizenzierung wird das neo-System als 1-Mandanten-System oder als Multi-Mandanten-System betrieben. In einem 1-Mandanten-System gibt es nur den vordefinierten Mandanten, es können keine weiteren Mandanten angelegt werden. In einem Multi-Mandanten-System kann der Systembetreiber so viele zusätzliche Mandanten anlegen wie Mandanten-Lizenzen im System vorhanden sind.

3 Systemvoraussetzungen



Grundlegende Informationen zu den benötigten Hard- und Softwarekomponenten finden Sie in der Installationsanleitung *Installationsvoraussetzungen*.

Firewall

Der Dienst *Windows Firewall* muss **vor** Installation der Aufzeichnungssoftware gestartet sein, damit die *neo*-Installationsroutine die entsprechenden Kommunikationsports in der Windows Firewall automatisch freischalten kann. Ein späterer Start der Windows Firewall führt dazu, dass das Aufzeichnungssystem nicht ordnungsgemäß funktionieren wird.



Die *neo*-Installationsroutine nimmt nur Änderungen an der Windows Firewall vor. Andere Firewall-Lösungen müssen manuell nach der Communication Matrix konfiguriert werden. Siehe Installationsanleitung *Installationsvoraussetzungen*.

Load Balancer

Für den Betrieb einer Multi-Core-Architektur ist ein Layer 4 Load Balancer erforderlich. Der Load Balancer muss vom Systembetreiber zur Verfügung gestellt werden.

4 Installationsvoraussetzungen

4 Installationsvoraussetzungen

4.1 Lizenzen



Das *neo*-Aufzeichnungssystem kann ohne Lizenzen installiert und konfiguriert werden. Das System läuft über einen Testzeitraum von 30 Tagen ohne Lizenzen. Innerhalb dieses Zeitraums müssen Sie eine gültige Lizenz anfordern. Ohne Lizenz werden nach diesen 30 Tagen alle Funktionen inaktiv geschaltet.

Welche Lizenzen für Ihre Anforderungen erforderlich sind, können Sie mit Ihrem Vertriebspartner von ASC klären.

Redundanzoptionen

Das Aufzeichnungssystem bietet folgende Optionen zur Absicherung der vollen Funktionalität im Fehlerfall:

Redundante Auslegung des Applikationsservers (Multi-Core-System)

Zur Absicherung der Aufzeichnung beim Ausfall eines Applikationsservers können Sie mehrere Applikationsserver ([App-Server](#)) in einem Cluster einrichten. In diesem Cluster wird die Systemlast automatisch auf die verschiedenen Applikationsserver verteilt. Fällt ein Applikationsserver aus, übernehmen die übrigen Applikationsserver alle Aufgaben.

Welche Server in Ihrem Aufzeichnungssystem als Applikationsserver zur Verfügung stehen und im Cluster verwendet werden sollen, stellen Sie während der Installation der Aufzeichnungssoftware ein, siehe [Kapitel "Aufzeichnungssoftware installieren"](#), S. 12.

Für den Betrieb einer Multi-Core-Architektur ist ein Layer 4 Load Balancer erforderlich. Der Load Balancer muss vom Systembetreiber zur Verfügung gestellt werden.

Redundante Auslegung der Datenbank

Zur Absicherung des Zugriffs auf die Aufzeichnungen bei einem Ausfall der Datenbank können Sie eine Failover-Funktion mit einer weiteren Datenbank einrichten.

Falls Sie eine MSSQL-Datenbank nutzen, konfigurieren Sie den Failover-Betrieb der Datenbanken gemäß der Anleitung des jeweiligen Herstellers.



Falls Sie die PostgreSQL-Datenbank nutzen, finden Sie Informationen zur Konfiguration des Failover-Konzepts in der Installationsanleitung *Failover-Betrieb für PostgreSQL-Datenbanken*. In dieser Anleitung finden Sie auch eine Beschreibung der Schritte, die Sie durchführen müssen, um den Failover-Betrieb wieder zurückzusetzen, wenn die Primär-Datenbank wieder zur Verfügung steht.

Redundante Auslegung des Aufzeichnungsservers

Zur Absicherung der Aufzeichnung beim Ausfall eines Aufzeichnungsservers oder einer Aufzeichnungskomponente können Sie verschiedene Failover-Aufzeichnungsarchitekturen einrichten.



Informationen zur Konfiguration von Failover-Aufzeichnungsarchitekturen finden Sie in der Installationsanleitung *Konfiguration Server und Aufzeichnungsarchitekturen*.

Das Aufzeichnungssystem wird mit einer integrierten PostgreSQL-Datenbank ausgeliefert. Das Zielverzeichnis für die Datenbank wird während des Installationsvorgangs definiert (Default-Einstellung: *ASCDB/* auf einer eigenen Partition).



Die in der folgenden Beschreibung genannten Zeiträume entsprechen den Default-Werten, die bei der Installation automatisch eingestellt werden. Bei Bedarf können Sie die Zeiträume über das Administrations-Tool für die Datenbank verändern.

Mit der Installation der mitgelieferten PostgreSQL-Datenbank der *neo*-Aufzeichnungssoftware wird ein Backup-Job für die PostgreSQL-Datenbank eingerichtet, der die letzten 5 Tage vorhält.

Sie finden die Dateien standardmäßig in folgendem Verzeichnis:

- %ASCDATA%\DatabaseBackup\



Informationen zur Wiederherstellung der PostgreSQL-Datenbank finden Sie unter <http://www.pgadmin.org/docs/dev/restore.html>.

Zur Optimierung der Datenbankgröße führt das Aufzeichnungssystem einmal wöchentlich eine Defragmentierung und Reindexierung durch.

Alle Vorgänge werden protokolliert. Die Logdateien werden im Installationsverzeichnis unter *\logs\Postgres* abgelegt.

7 Externe Datenbanken



Die Installation der externen Datenbank muss vor der Installation der neo-Software durchgeführt werden. Falls Sie eine externe Datenbank nutzen möchten, muss der Port geöffnet werden, über den der Zugriff von der neo-Software erfolgen soll.



Informationen zum Backup und zur Wiederherstellung einer PostgreSQL-Datenbank finden Sie unter

<http://www.pgadmin.org/docs/dev/backup.html> bzw. unter
<http://www.pgadmin.org/docs/dev/restore.html>.



Informationen zum Backup und zur Wiederherstellung einer Microsoft SQL-Datenbank finden Sie unter

<http://msdn.microsoft.com/de-de/library/ms187510.aspx>.



Bei der Installation von Multi-Server-Systemen muss der Server, auf dem die Datenbank laufen soll, zuerst installiert werden.

Bei Verwendung von Failover-Datenbanken muss der Server, auf dem die Primär-Datenbank laufen soll, zuerst installiert werden.

1. Legen Sie das Installationsmedium für die Aufzeichnungssoftware ein.
2. Wechseln Sie in das Verzeichnis der Aufzeichnungssoftware.
3. Wählen Sie aus dem Kontextmenü der Datei *setup.exe* den Menüpunkt *Run as administrator*.
4. Führen Sie die Installationsroutine als Administrator aus und folgen Sie den Anweisungen des Installationsassistenten.
 - ⇒ Falls Microsoft Visual C++ Redistributable noch nicht installiert ist, erscheint das folgende Fenster:

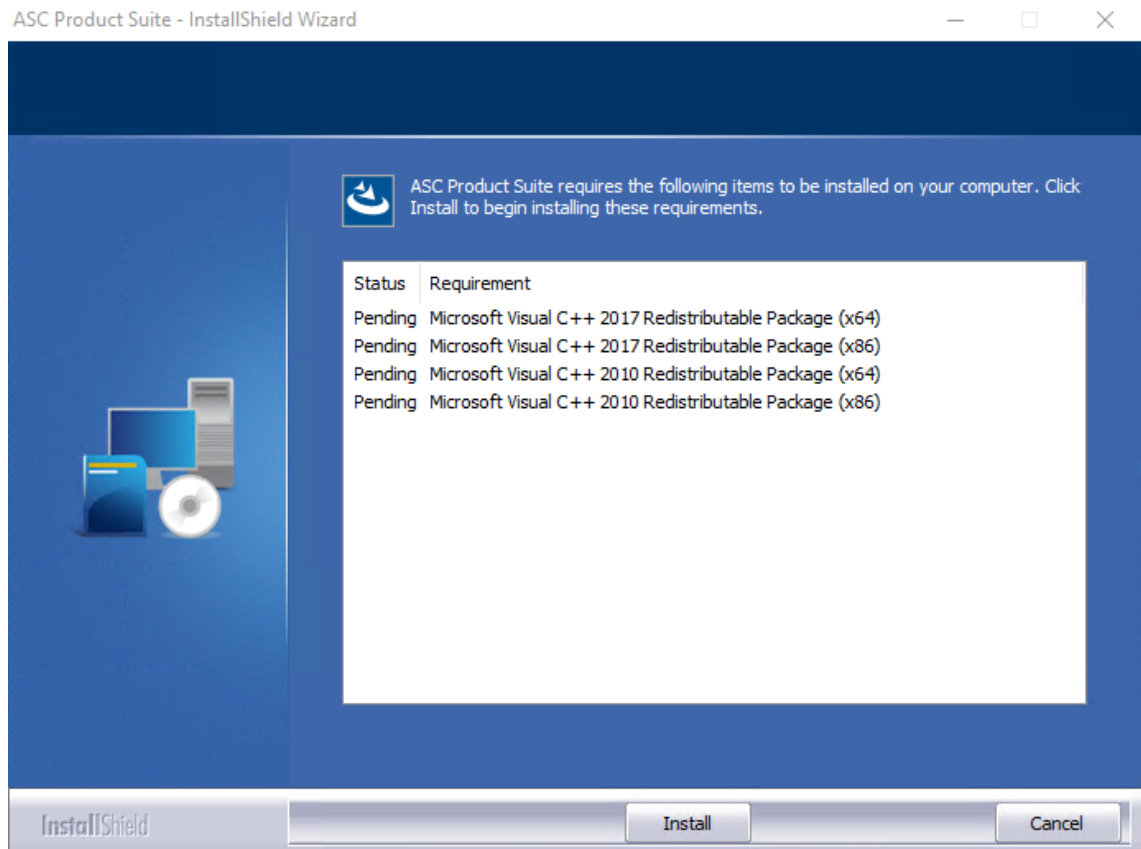


Abb. 1: Microsoft Visual C++ installieren

5. Starten Sie die Installation von Microsoft Visual C++, indem Sie auf die Schaltfläche *Install* klicken.
6. Falls bei der Betriebssystem-Installation **SNMP** nicht installiert wurde, müssen Sie folgenden Hinweis bestätigen:

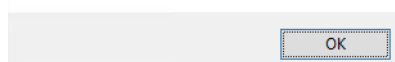
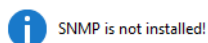


Abb. 2: Hinweis, dass SNMP nicht installiert ist

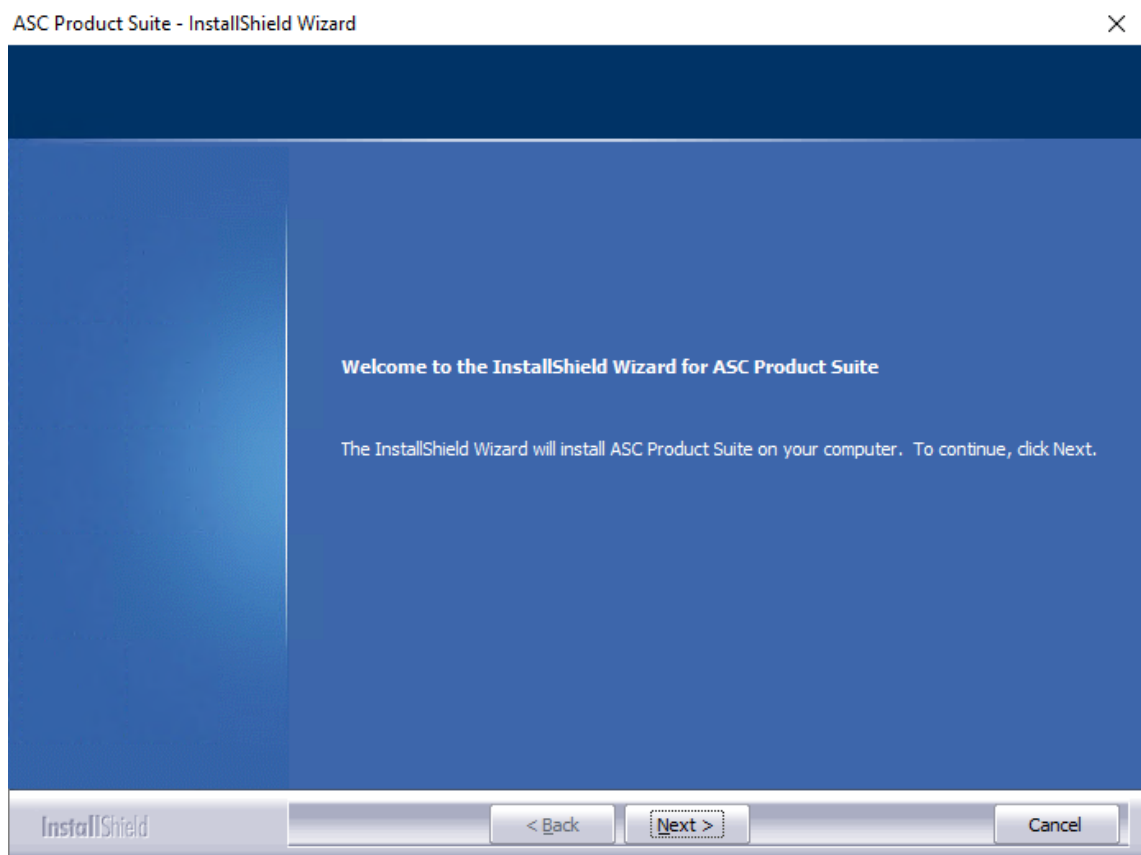


Abb. 3: Installationsroutine starten

7. Starten Sie die Installationsroutine für die Aufzeichnungssoftware, indem Sie auf die Schaltfläche *Next* klicken.
 - ⇒ Das Fenster zur Auswahl des Installationsverzeichnis erscheint.

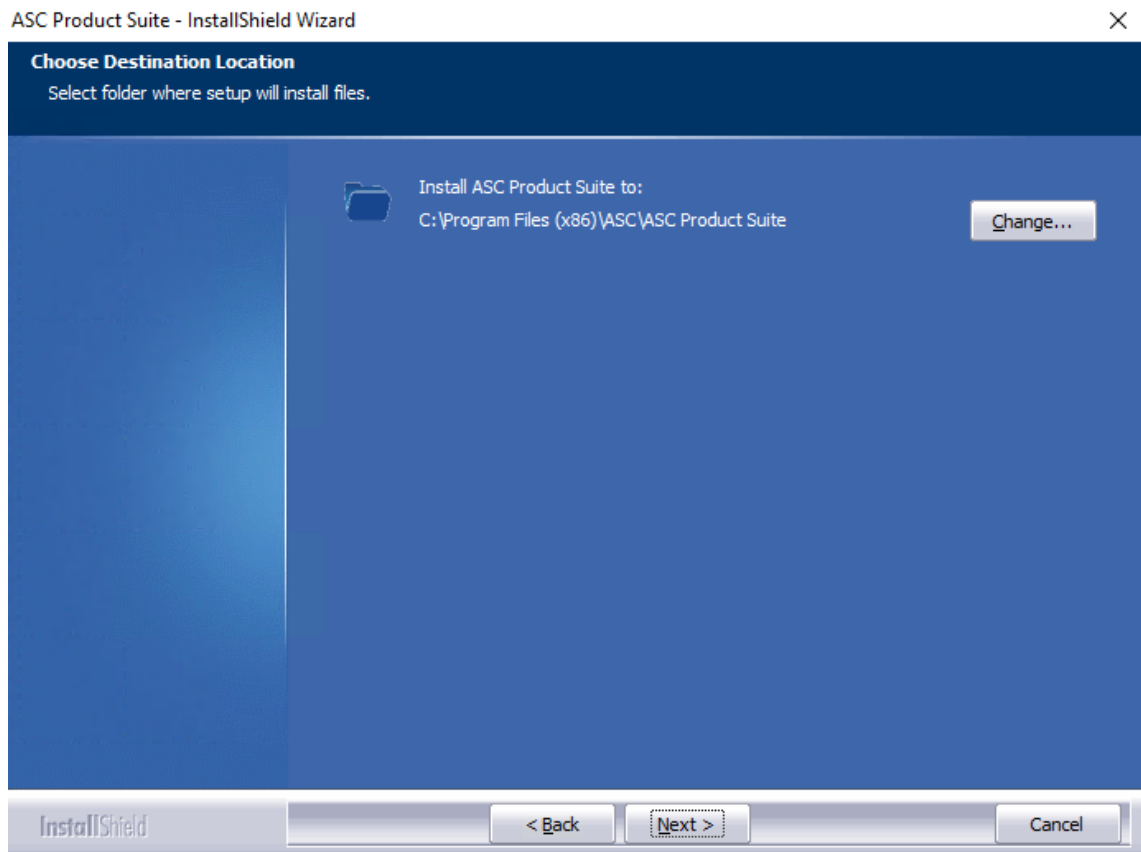


Abb. 4: Zielverzeichnis für die Installation bestätigen

8. Wählen Sie das Zielverzeichnis für die Installation, indem Sie auf die Schaltfläche *Change* klicken.
HINWEIS! Third-Party-Software-Komponenten wie z. B. .NET, Java, PostgreSQL oder WinPCap werden in die vordefinierten Standard-Installationspfade installiert und können nicht geändert werden.
9. Klicken Sie auf die Schaltfläche *Next*, um das Zielverzeichnis zu bestätigen.
 - ⇒ Das Fenster zur Auswahl der Datenpartition erscheint, auf der die Konversationen abgelegt werden.

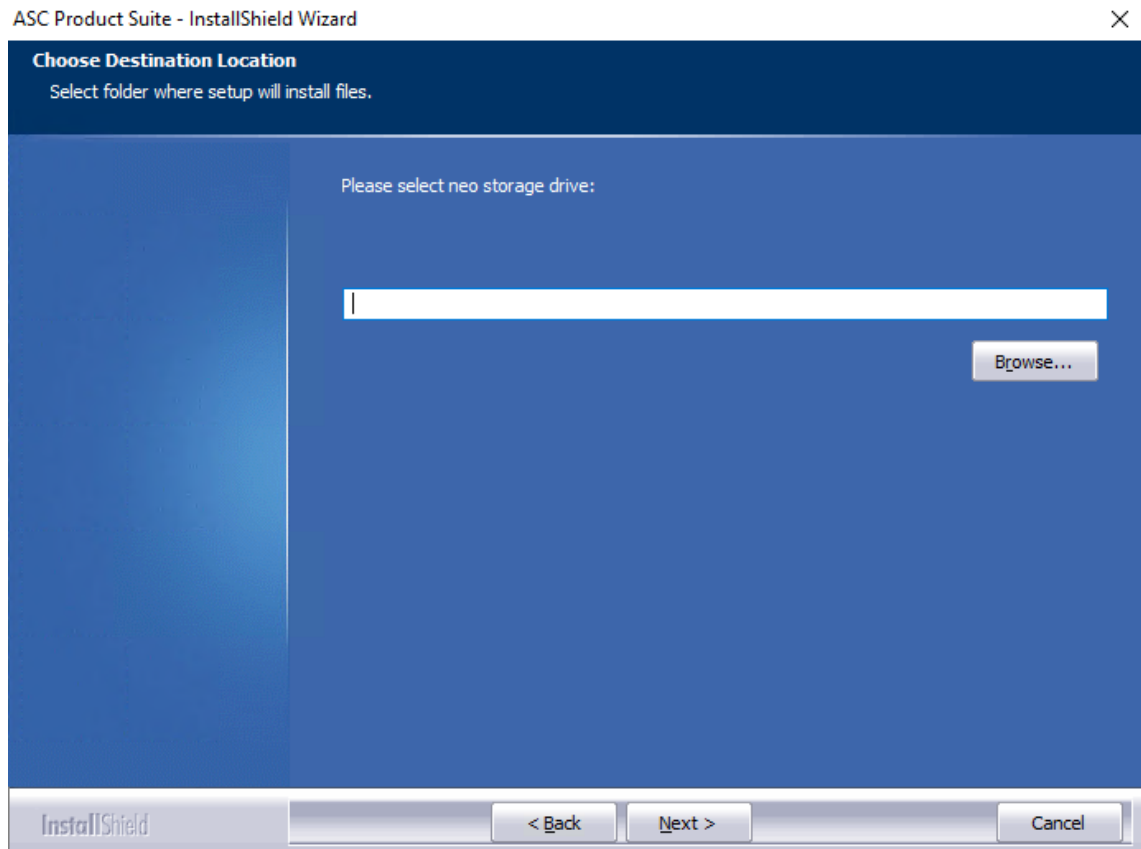


Abb. 5: Datenpartition bestätigen

10. Klicken Sie auf die Schaltfläche *Browse*, um die Partition auszuwählen, auf der die Aufzeichnungsdaten gespeichert werden sollen.
Dies darf nicht die gleiche Partition sein, auf der die Aufzeichnungssoftware installiert ist, damit die Funktionalität nicht gefährdet ist.
⇒ Das Verzeichnis *ASCDATA* wird angelegt.



Die Laufwerksbuchstaben sind bei der Installation frei wählbar.

Eine nachträgliche Änderung der Laufwerksbuchstaben führt jedoch zu Zugriffsproblemen und damit zu schwerwiegenden Störungen der internen Prozesse.

11. Klicken Sie auf die Schaltfläche *Next*, um die Eingaben zu bestätigen.
⇒ Es erscheinen 2 Fenster zur Sprachauswahl. Die ausgewählten Sprachen erscheinen nach der Installation in der Sprachauswahl für die Benutzeroberfläche der Anwendungen der *neo* Suite.

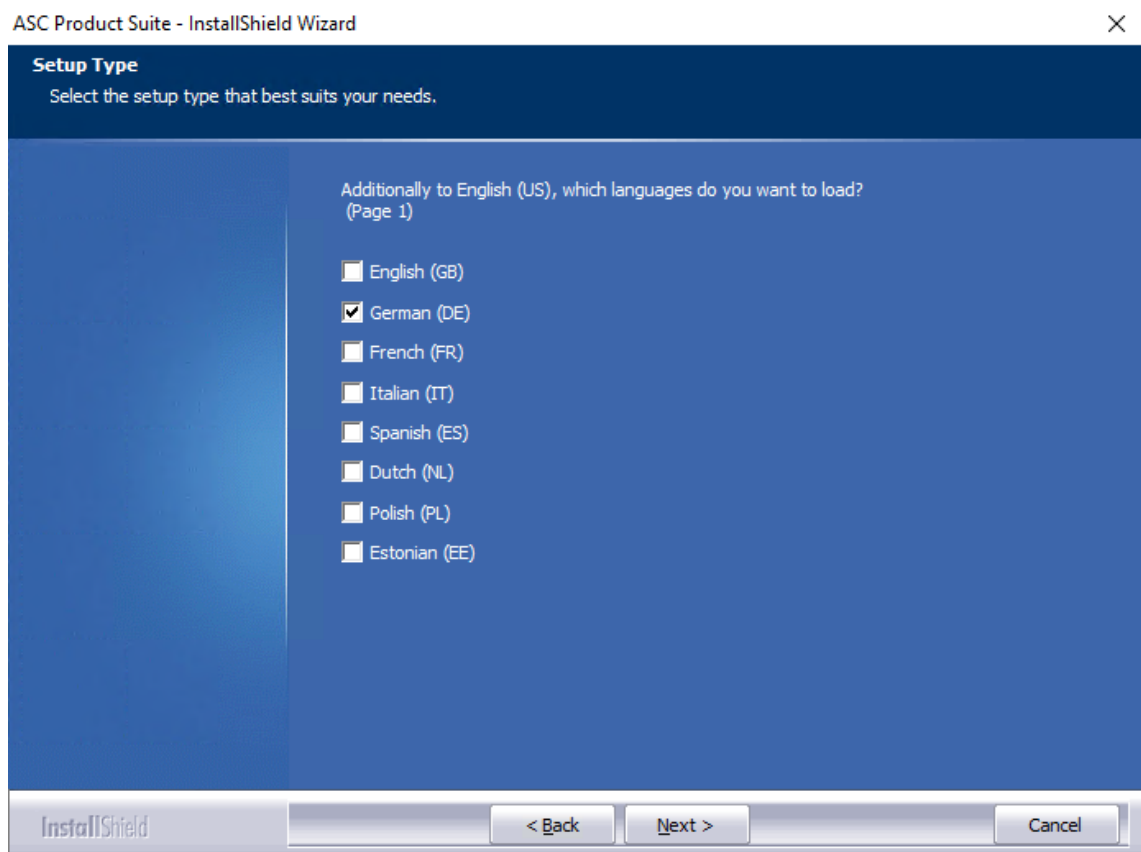


Abb. 6: Sprachen für die grafische Benutzeroberfläche auswählen

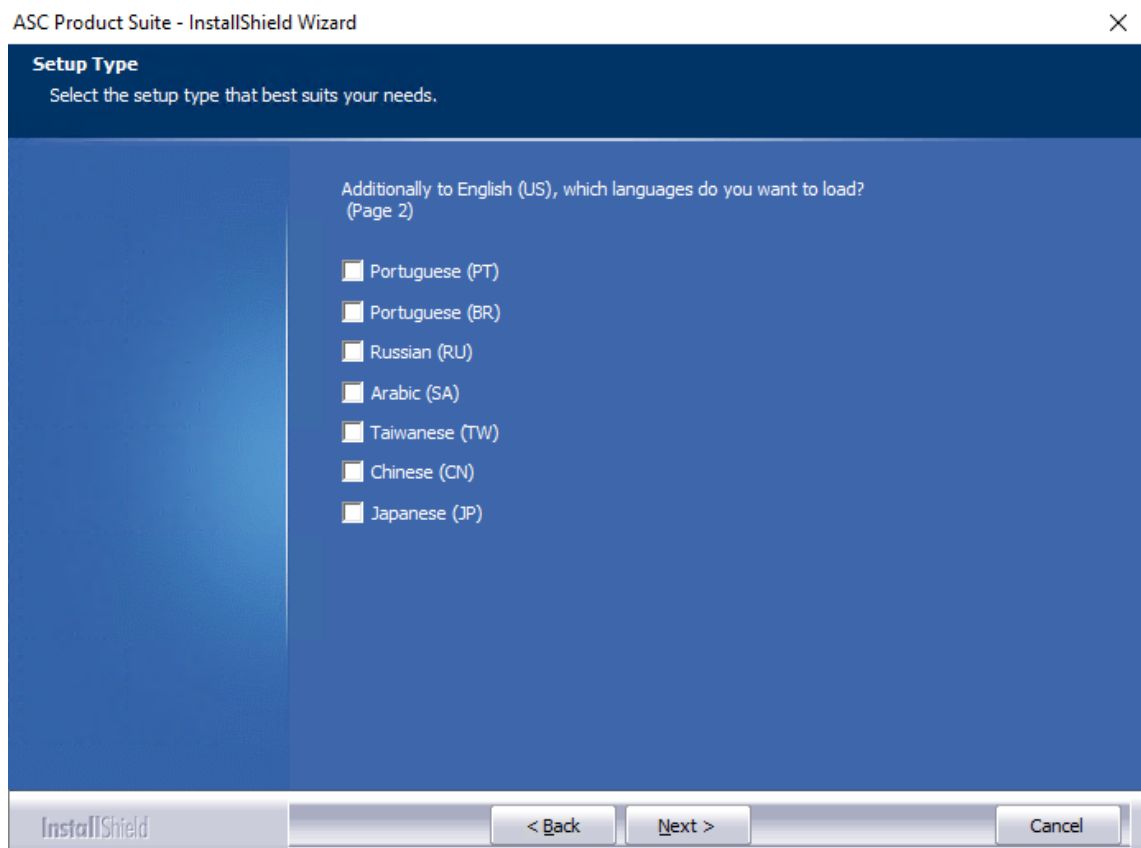


Abb. 7: Sprachen für die grafische Benutzeroberfläche auswählen

12. Wählen Sie die entsprechenden Sprachen aus, die nach der Installation zur Verfügung stehen sollen. Mehrfachmarkierungen sind möglich.

13. Klicken Sie auf die Schaltfläche *Next*, um die Eingabe zu bestätigen.
⇒ Das Fenster zur Eingabe der ASC-Cluster-ID erscheint.

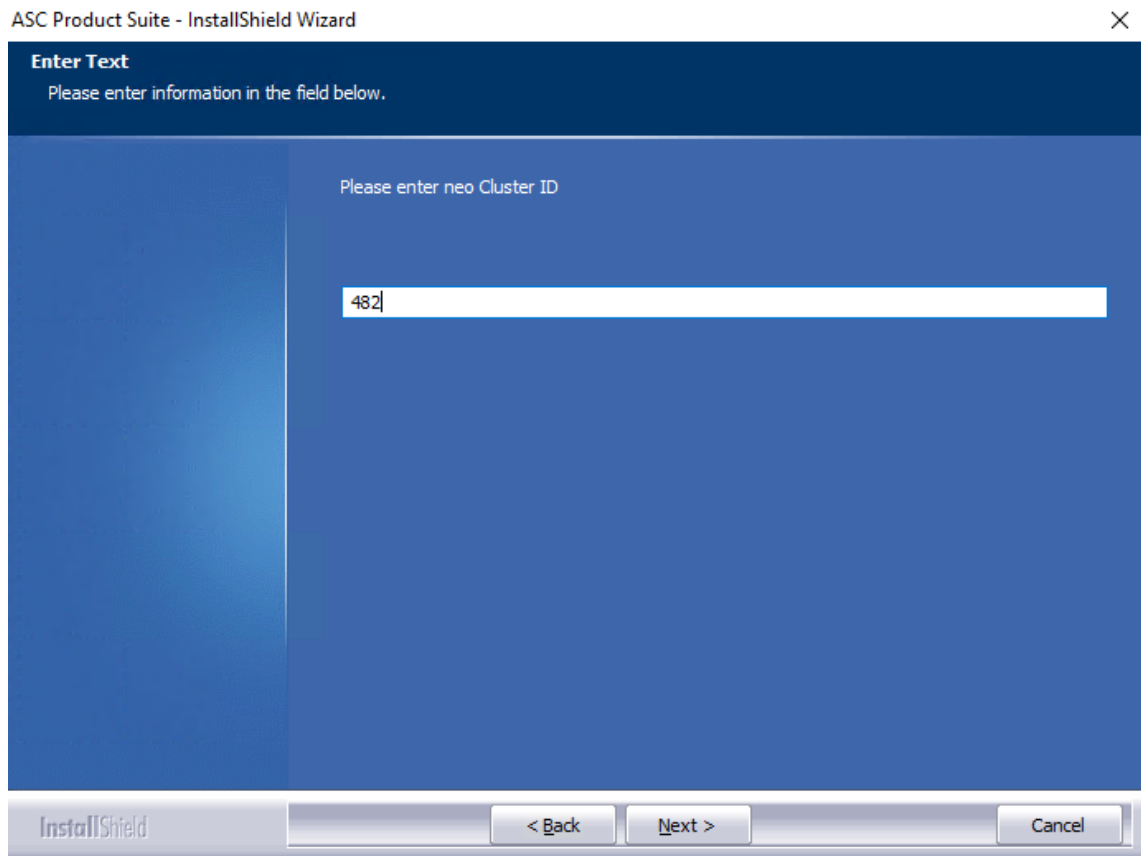


Abb. 8: Cluster-ID eingeben

14. Geben Sie die Cluster-ID ein.
Als Default-ID wird hier automatisch der Servername eingetragen. Für Single-Server-Systeme können Sie diese ID übernehmen.
Wenn Sie ein Multi-Server-System mit mehreren Applikationsservern einrichten, müssen Sie für alle Applikationsserver die Default-ID durch eine andere, frei wählbare und für alle Applikationsserver identische Cluster-ID ersetzen.
15. Klicken Sie auf die Schaltfläche *Next*, um die Eingabe zu bestätigen.
⇒ Das Fenster zur Eingabe der IP-Adressen für die Applikationsserver ([App-Server](#)) erscheint.

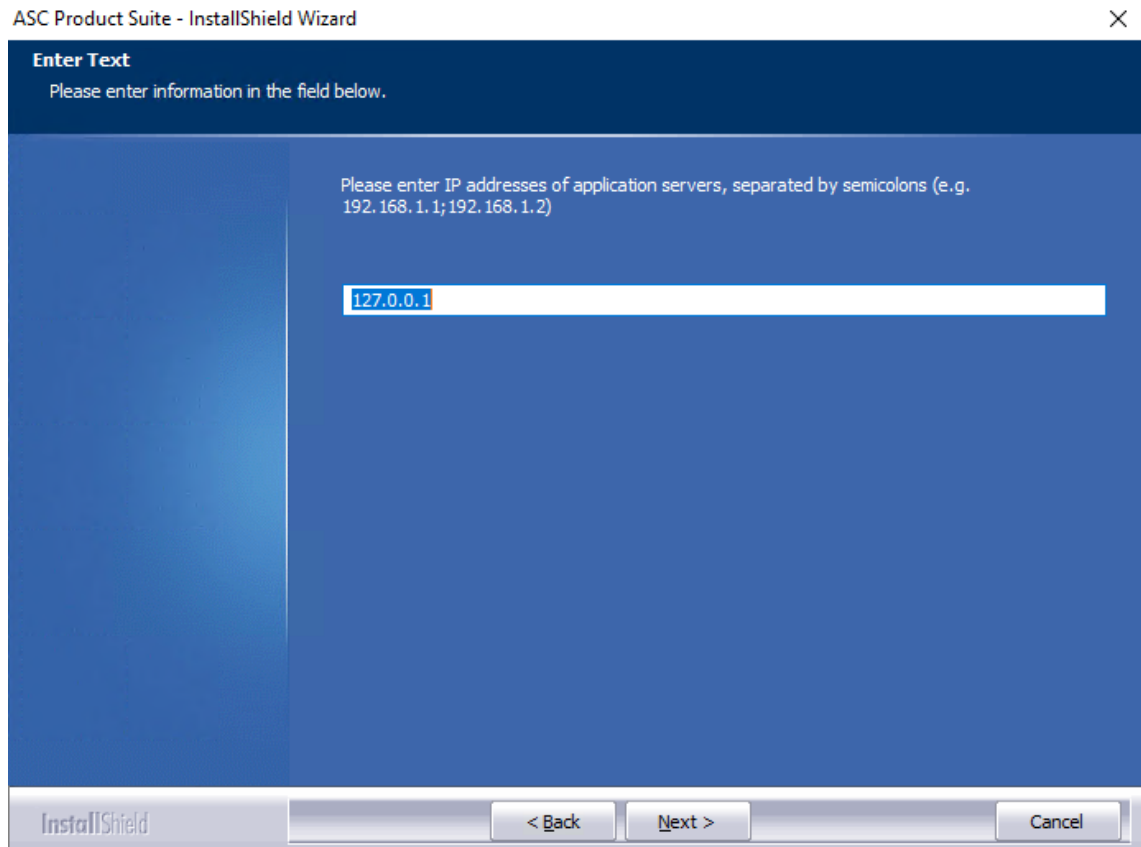


Abb. 9: Multi-Server-Systeme installieren

16. Zur Nutzung von [Multi-Server-Systemen](#) geben Sie die IP-Adressen aller Applikationsserver ([App-Server](#)), getrennt durch ein Semikolon, ein.

In der [App-Server](#)-Liste kann man zusätzlich eine Priorität der Transmission setzen. Die [App-Server](#) mit der höchsten Priorität (höchste Zahl) werden bevorzugt verwendet. Mehrere [App-Server](#) können zur Lastverteilung auch die gleiche Priorität haben. Für den Fall, dass alle [App-Server](#) einer Priorität ausgefallen sind, wird der [App-Server](#) mit einer niedrigeren Priorität verwendet.

Geben Sie dazu folgenden Syntax an:

Beispiel 1:

`trm://172.16.203.30/?priority=2;trm://173.14.200.23/?priority=2`

Bei dieser Konfiguration haben beide [App-Server](#) die gleiche Priorität. Die Last wird auf beide [App-Server](#) gleichmäßig verteilt.

Beispiel 2:

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

Bei dieser Konfiguration erhält der [App-Server](#) 1 mit der IP-Adresse 172.16.203.30 alle Nachrichten. Der [App-Server](#) 2 mit der IP-Adresse 173.14.200.23 erhält nur Nachrichten, wenn der [App-Server](#) 1 nicht verfügbar ist.

Beispiel 2:

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

Bei dieser Konfiguration werden alle Nachrichten abwechselnd an den [App-Server](#) 1 mit

der IP-Adresse 172.16.203.30 und den **App-Server** 3 mit der IP-Adresse 172.16.203.35 geschickt. Normalerweise werden keine Nachrichten an den **App-Server** 2 mit der IP-Adresse 173.14.200.23 geschickt. Der **App-Server** 2 erhält nur Nachrichten, wenn der **App-Server** 1 und der **App-Server** 3 nicht verfügbar sind.

17. Bei der Installation eines **Single-Server**-Systems belassen Sie die Standardeingabe 127.0.0.1.
18. Klicken Sie auf die Schaltfläche *Next*, um die Eingabe zu bestätigen.
⇒ Das Fenster zur Eingabe der IP-Adresse für den **NTP**-Server erscheint.

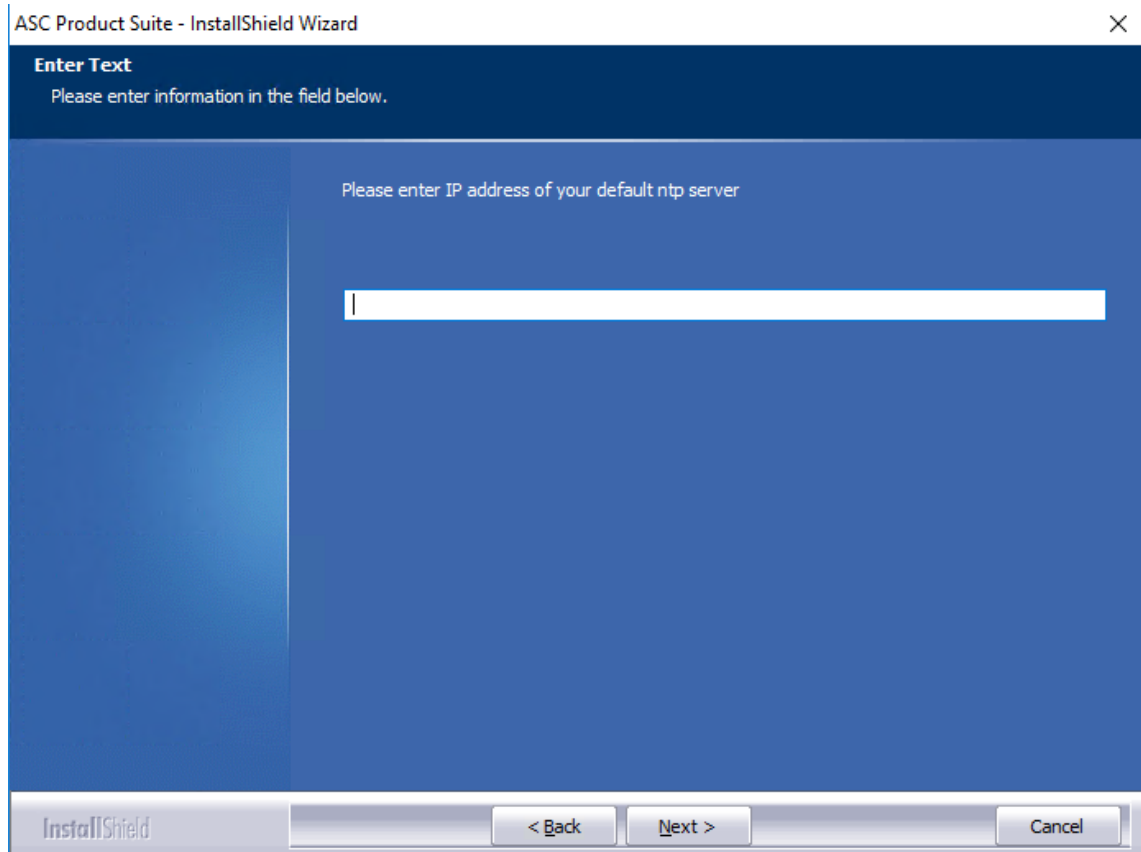


Abb. 10: Adresse des NTP-Servers eingeben

19. Geben Sie die IP-Adresse des NTP-Servers ein.
HINWEIS!
Wenn sich NTP-Zeiten mehr als 10 Minuten abweichend verändern, korrigieren Sie vorher die Zeit manuell in der Systemsteuerung von Windows.
20. Klicken Sie auf die Schaltfläche *Next*, um die Eingabe zu bestätigen.
⇒ Das Fenster zur Auswahl der Features erscheint.
21. Falls Sie ein Multi-Server-System installieren, deaktivieren Sie die folgenden Features für die Server, auf denen die Features nicht genutzt werden.
HINWEIS!
In Multi-Server-Systemen werden die Komponenten des Applikationsservers (**App-Server**) und die Datenbank nur auf einem Server benötigt. Sie können diese Features aber auch parallel auf mehreren Servern nutzen.

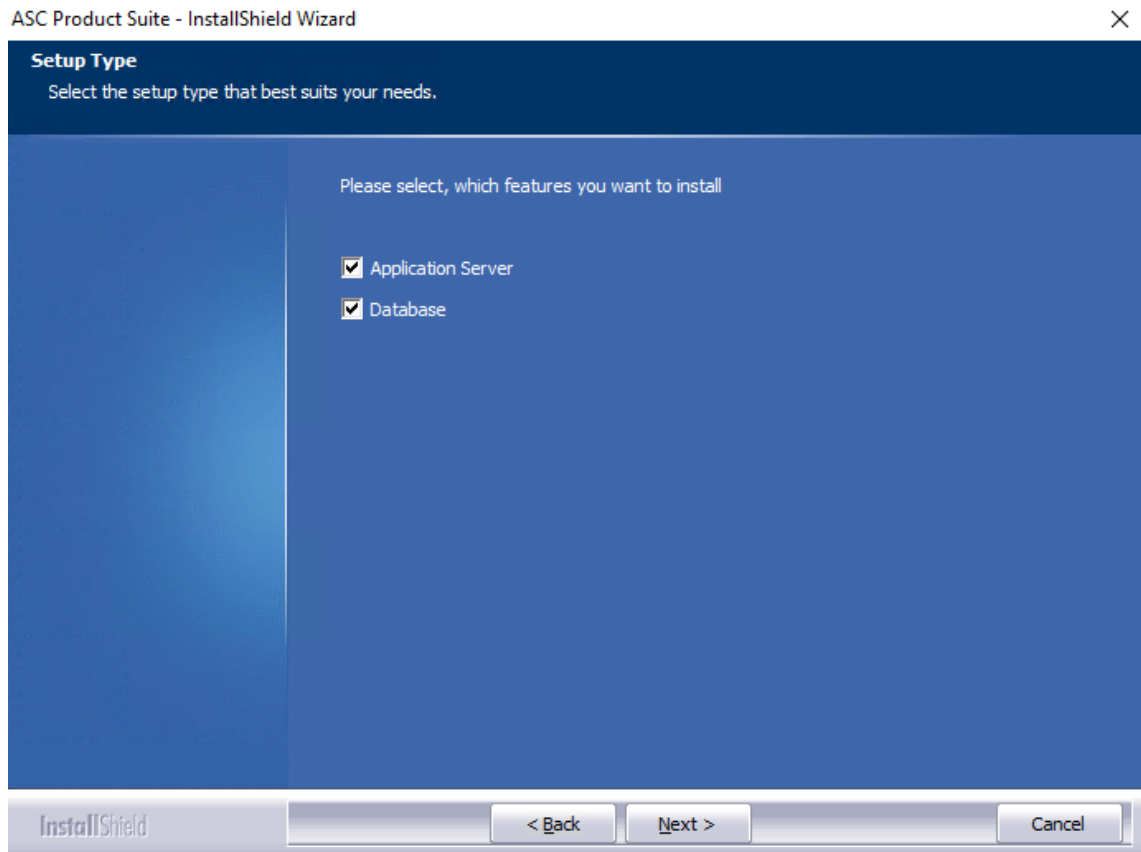


Abb. 11: Features zur Installation auswählen

Single-Server-Systeme

Wählen Sie folgende Optionen, um ein Single-Server-System zu installieren:

<input checked="" type="radio"/>	Application Server	Die Auswahl beinhaltet alle relevanten Dienste für die Web-Applikationen, also für die Funktion eines App-Servers . Aktivieren Sie diese Option, wenn auf diesem Server der Enterprise Core laufen soll.
<input checked="" type="radio"/>	Database	Aktivieren Sie diese Option, um die mitgelieferten PostgreSQL-Datenbank auf dem gleichen Server zu installieren.

Multi-Server-Systeme

Für Multi-Server-Systeme stehen Ihnen folgende Installationsvarianten zur Verfügung:

Server mit Enterprise Core, PostgreSQL-Datenbank und Aufzeichnungskomponenten

<input checked="" type="radio"/>	Application Server	Aktivieren Sie diese Option, wenn auf diesem Server der Enterprise Core laufen soll.
<input checked="" type="radio"/>	Database	Aktivieren Sie diese Option, wenn auf diesem Server ebenfalls die Datenbank installiert werden soll.
<input type="radio"/>	Database	Deaktivieren Sie diese Option, wenn Sie die Datenbank auf einem separaten Server installieren möchten.

Reiner PostgreSQL-Server

<input checked="" type="radio"/>	Database	Aktivieren Sie diese Option, wenn auf diesem Server nur eine PostgreSQL-Datenbank installiert werden soll.
----------------------------------	----------	--

Reiner Aufzeichnungsserver

<input type="radio"/>	<i>Application Server</i>	Deaktivieren Sie diese Option, wenn dieser Server nur zur Aufzeichnung dienen soll.
<input type="radio"/>	<i>Database</i>	Deaktivieren Sie diese Option, wenn dieser Server nur zur Aufzeichnung dienen soll.

1. Klicken Sie auf die Schaltfläche *Next*, um die Eingabe zu bestätigen.
2. Wenn Sie die Datenbank auf dem gleichen Server installieren, fahren Sie mit folgendem Kapitel fort:
[Kapitel "Interne Datenbank installieren", S. 21.](#)
3. Wenn Sie die Datenbank extern installiert haben, fahren Sie mit folgendem Kapitel fort:
[Kapitel "Externe Datenbank installieren", S. 22](#)

8.1 Interne Datenbank installieren

Wenn Sie die Datenbank auf dem gleichen Server installieren, erscheint die Abfrage nach dem Laufwerk, auf dem die Datenbank installiert werden soll.

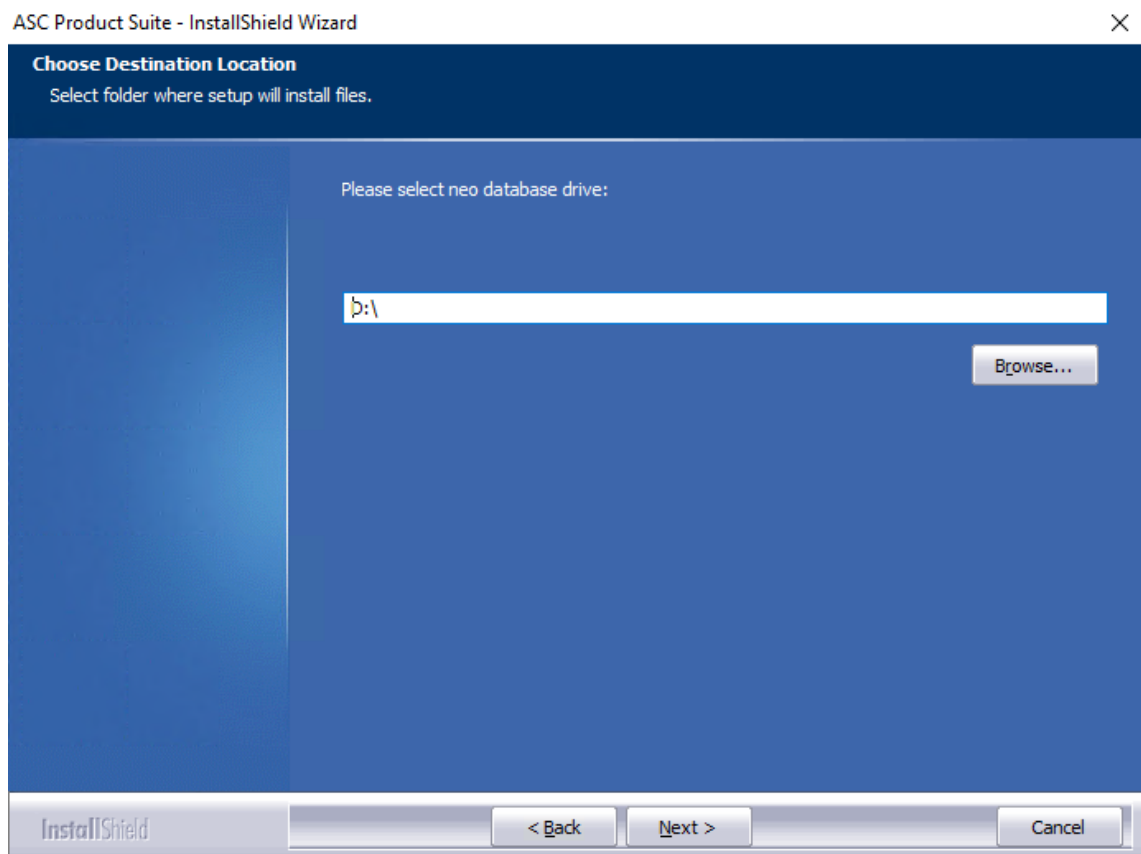


Abb. 12: Ziellaufwerk für die interne Datenbank wählen

1. Klicken Sie auf die Schaltfläche *Browse*, um das Laufwerk auszuwählen, auf dem die Datenbank gespeichert werden soll.
 - ⇒ Das Verzeichnis *ASCDB* wird angelegt.
2. Klicken Sie auf die Schaltfläche *Next*.
 - ⇒ Falls Sie mehrere Netzwerkkarten installiert haben, führt Sie die Installations-Routine zur Auswahl der IP-Adresse für die Zertifikatserstellung.
Siehe [Kapitel "IP-Adresse für das SSL/TLS-Zertifikat auswählen", S. 27.](#)
 - ⇒ Falls Sie nur eine Netzwerkkarte installiert haben, wird das Zertifikat automatisch auf die konfigurierte IP-Adresse ausgestellt. Die Installations-Routine führt Sie dann direkt zur Installation von WinPcap. Siehe [Kapitel "WinPcap installieren", S. 29.](#)

- ⇒ Falls Sie einen Server ohne Aufzeichnung installieren möchten, können Sie die Installation von WinPcap überspringen, indem Sie auf die Schaltfläche Cancel klicken. Die Installations-Routine führt Sie dann direkt zum ASC Updater. Siehe [Kapitel "Updater starten", S. 31](#).

8.2 Externe Datenbank installieren

Wenn Sie die Datenbank extern installiert haben, erscheinen folgende Abfragen zur Konfiguration der Verbindungsdaten.

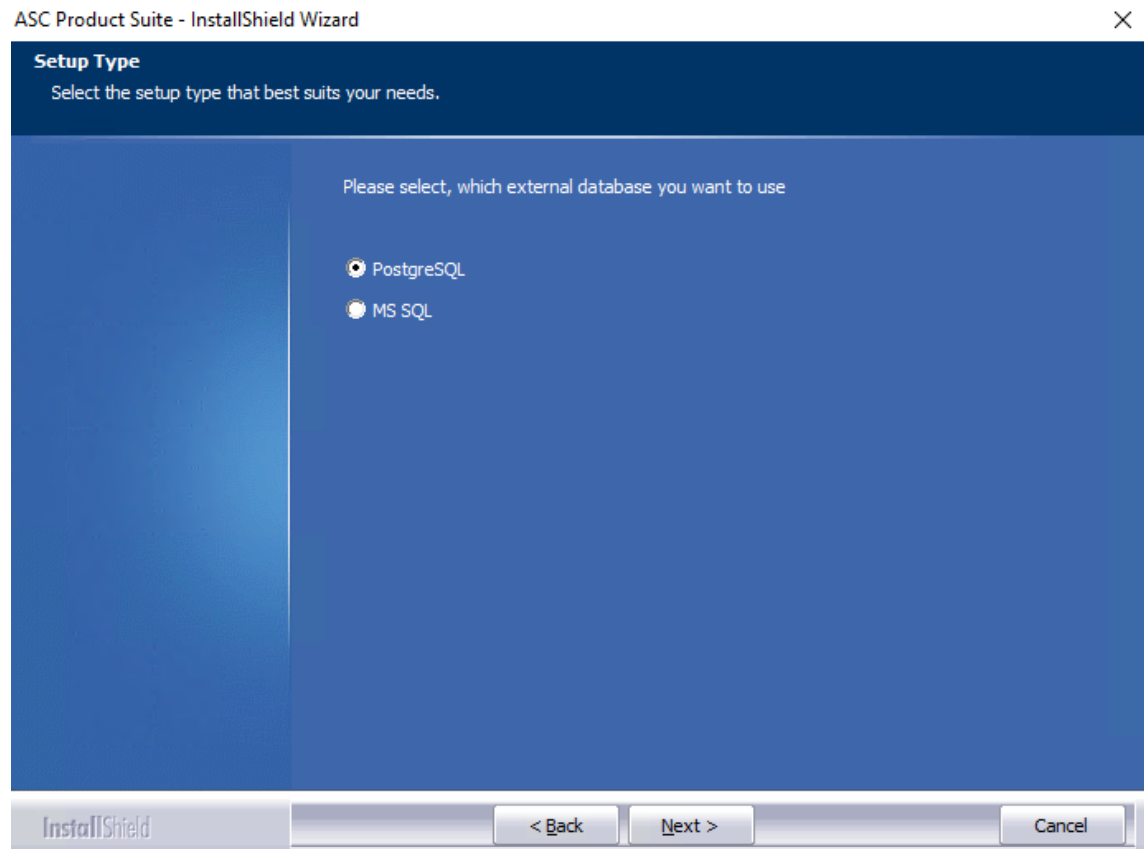


Abb. 13: Typ der externen Datenbank auswählen

1. Wählen Sie den Typ der externen schon installierten Datenbank aus.
2. Klicken Sie auf die Schaltfläche *Next*, um die Eingabe zu bestätigen.
 - ⇒ Das Fenster zur Eingabe der IP-Adresse für die externe Datenbank erscheint.

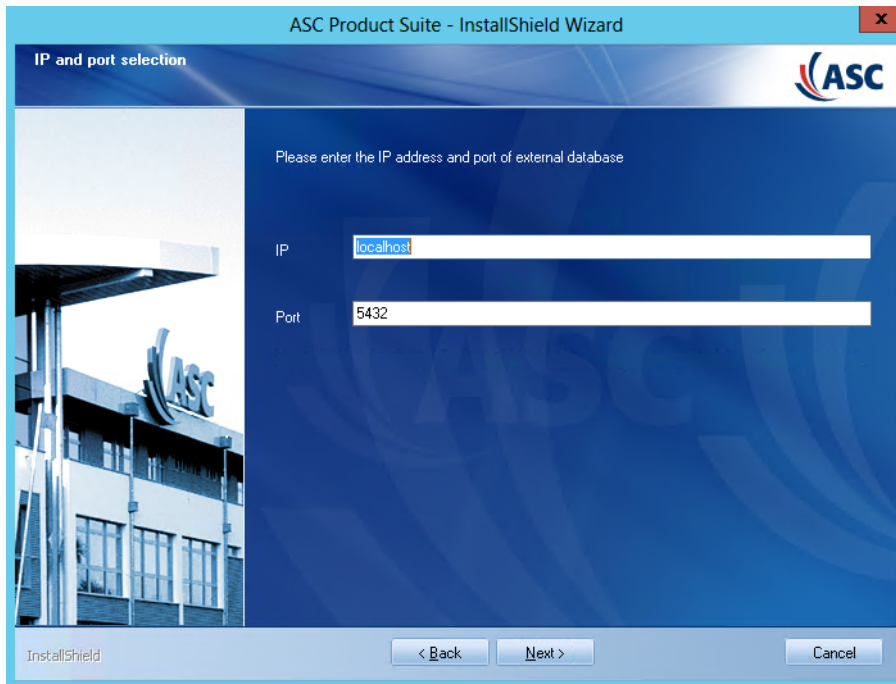


Abb. 14: Verknüpfung zur externen Datenbank erstellen

3. Um die Verknüpfung zu der externen Datenbank zu erstellen, geben Sie die IP-Adresse des Servers ein, auf dem die Datenbank installiert ist, sowie den konfigurierten Port.
4. Klicken Sie auf die Schaltfläche *Next*, um die Eingaben zu speichern.
 - ⇒ Das Fenster zur Eingabe der Login-Daten für die externe Datenbank erscheint.

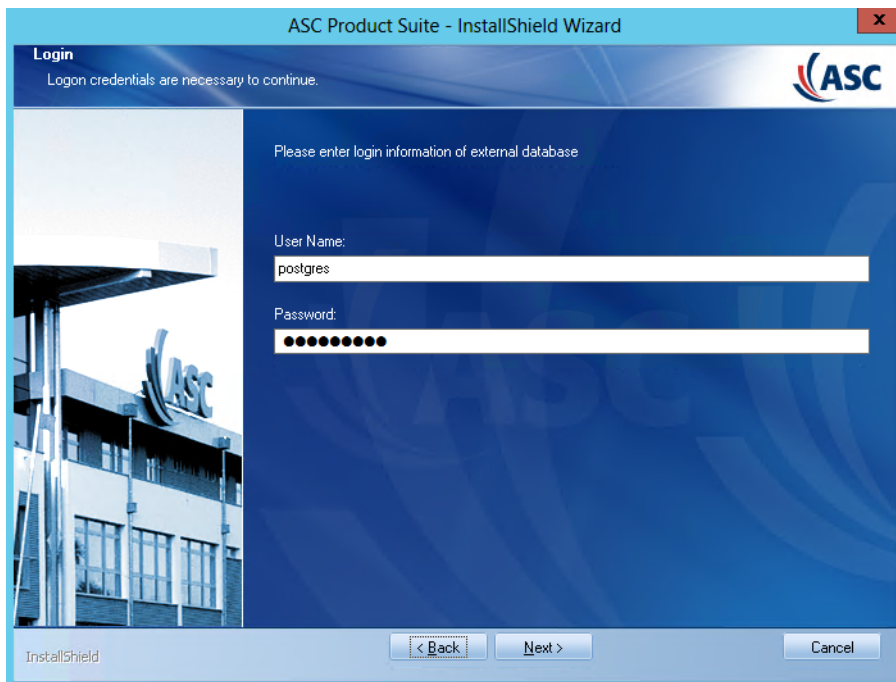


Abb. 15: Benutzer für die Datenbank konfigurieren

5. Geben Sie die Login-Daten für den Benutzer der externen Datenbank ein. Stellen Sie sicher, dass diesem Benutzer die Rechte zum Erstellen von Datenbanken zugewiesen sind.
6. Klicken Sie auf die Schaltfläche *Next*, um die Eingaben zu speichern.
 - ⇒ Bei der Installation einer MSSQL-Datenbank erscheint das folgende Fenster:

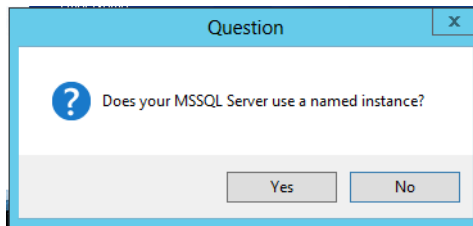


Abb. 16: Abfrage zur MSSQL-Serverinstanz

7. Klicken Sie auf die Schaltfläche *No*, wenn Sie keine spezielle MSSQL-Instanz verwenden möchten.
8. Klicken Sie auf die Schaltfläche *Yes*, um einen Namen für die MSSQL-Instanz einzugeben.
⇒ Das Fenster zur Eingabe des Namens für die MSSQL-Instanz erscheint.

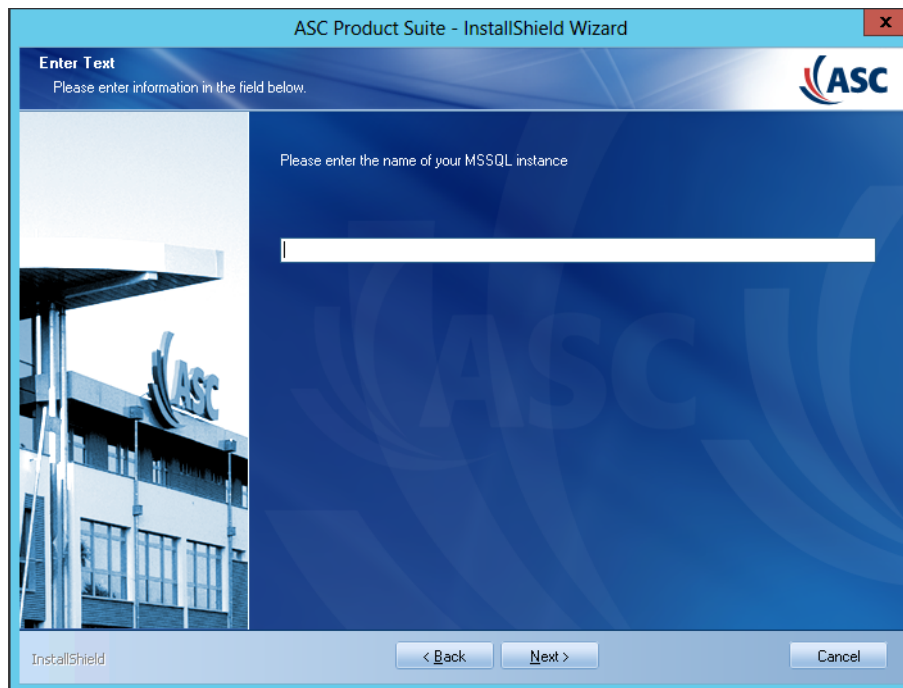


Abb. 17: Namen der MSSQL-Instanz eingeben

9. Klicken Sie auf die Schaltfläche *Next*, um die Eingaben zu speichern.
⇒ Das Fenster zum Starten des Installationsvorgangs erscheint.

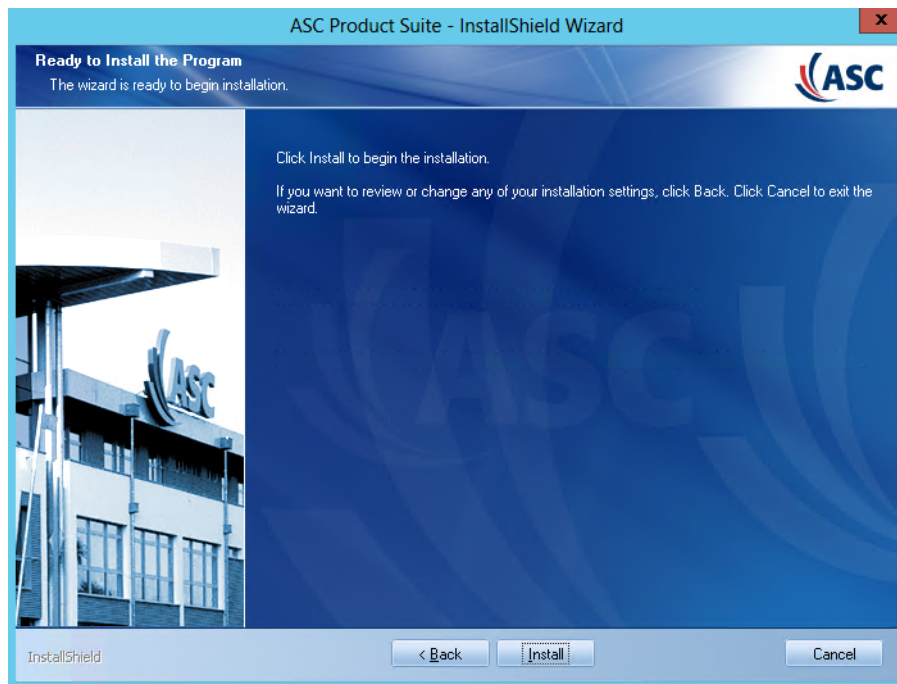


Abb. 18: Installationsvorgang starten

10. Klicken Sie auf die Schaltfläche *Install*, um die Installation zu starten.
⇒ Der Installationsfortschritt wird angezeigt.

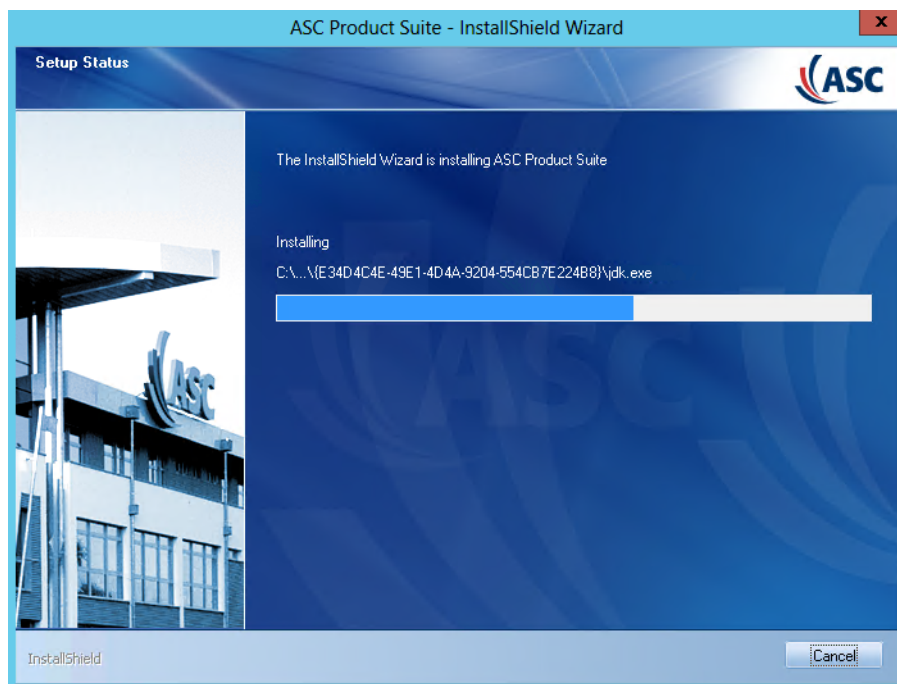


Abb. 19: Information zum Installationsfortschritt



Die Installation kann einige Zeit in Anspruch nehmen.

11. Jetzt können die HTTP- bzw. HTTPS-Ports kontrolliert und ggf. geändert werden.
⇒ Das folgende Fenster erscheint:

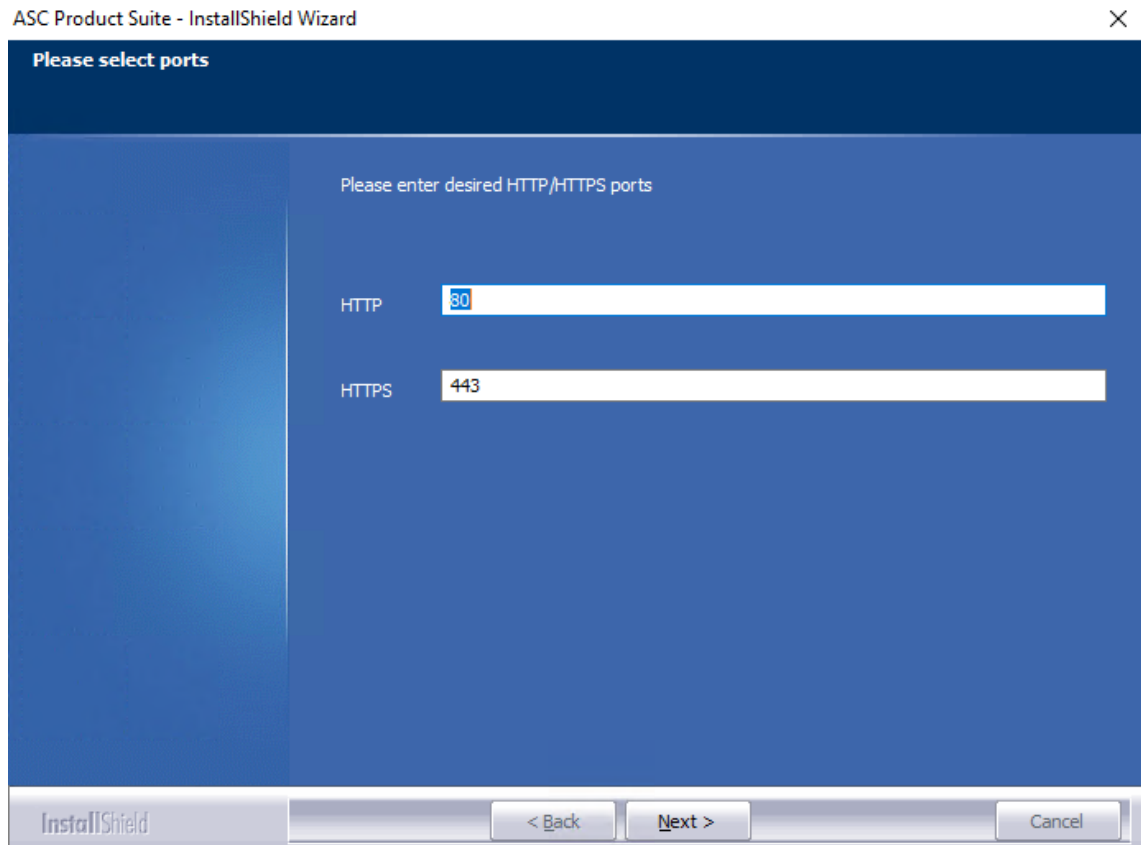


Abb. 20: Webserver Ports konfigurieren

12. Geben Sie die Ports für HTTP und HTTPS an, über die der Webserver erreichbar sein soll.

13. Klicken Sie auf die Schaltfläche *Next*.

- ⇒ Falls Sie mehrere Netzwerkkarten installiert haben, führt Sie die Installations-Routine zur Auswahl der IP-Adresse für die Zertifikatserstellung.
Siehe [Kapitel "IP-Adresse für das SSL/TLS-Zertifikat auswählen"](#), S. 27.
- ⇒ Falls Sie nur eine Netzwerkkarte installiert haben, wird das Zertifikat automatisch auf die konfigurierte IP-Adresse ausgestellt. Die Installations-Routine führt Sie dann direkt zur Installation von WinPcap. Siehe [Kapitel "WinPcap installieren"](#), S. 29.
- ⇒ Falls Sie einen Server ohne Aufzeichnung installieren möchten, können Sie die Installation von WinPcap überspringen, indem Sie auf die Schaltfläche Cancel klicken. Die Installations-Routine führt Sie dann direkt zum ASC Updater. Siehe [Kapitel "Updater starten"](#), S. 31.

8.3 IP-Protokoll auswählen

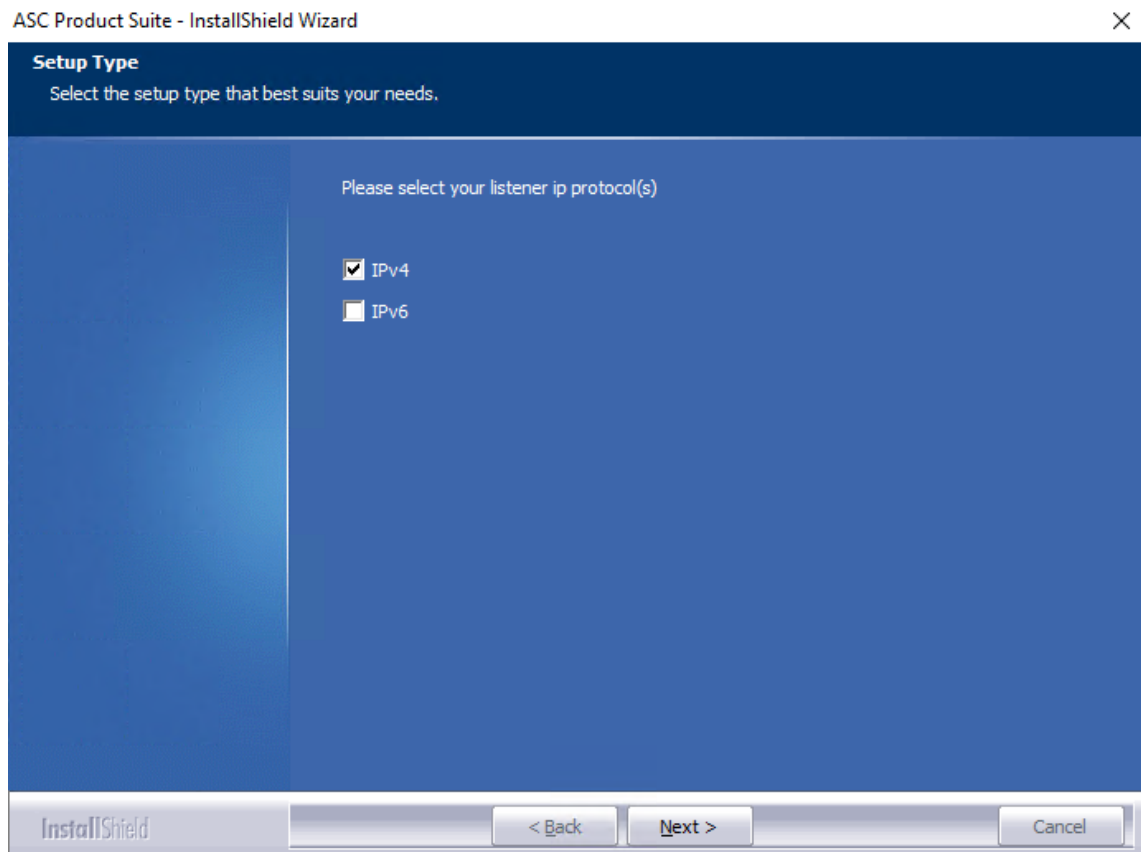


Abb. 21: IP-Protokoll auswählen

1. Wählen Sie das IPv4-Protokoll aus, wenn Sie den normalen Adressenkreis verwenden möchten. Wählen Sie das IPv6-Protokoll aus, wenn Sie einen erweiterten Adressenkreis verwenden möchten.
2. Klicken Sie auf die Schaltfläche *Next*.
⇒ Das Fenster zum Installationsvorgang erscheint.

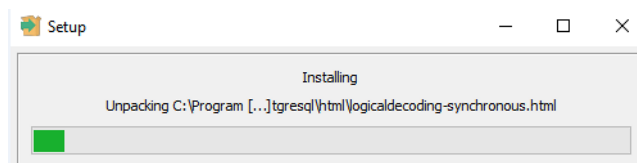


Abb. 22: Durchführung der IP-Protokoll-Installation

8.4 IP-Adresse für das SSL/TLS-Zertifikat auswählen

HINWEIS! Falls mehrere Netzwerkkarten installiert und konfiguriert sind, erscheint das Auswahlfenster, für die das SSL/TLS-Zertifikat erstellt werden soll.

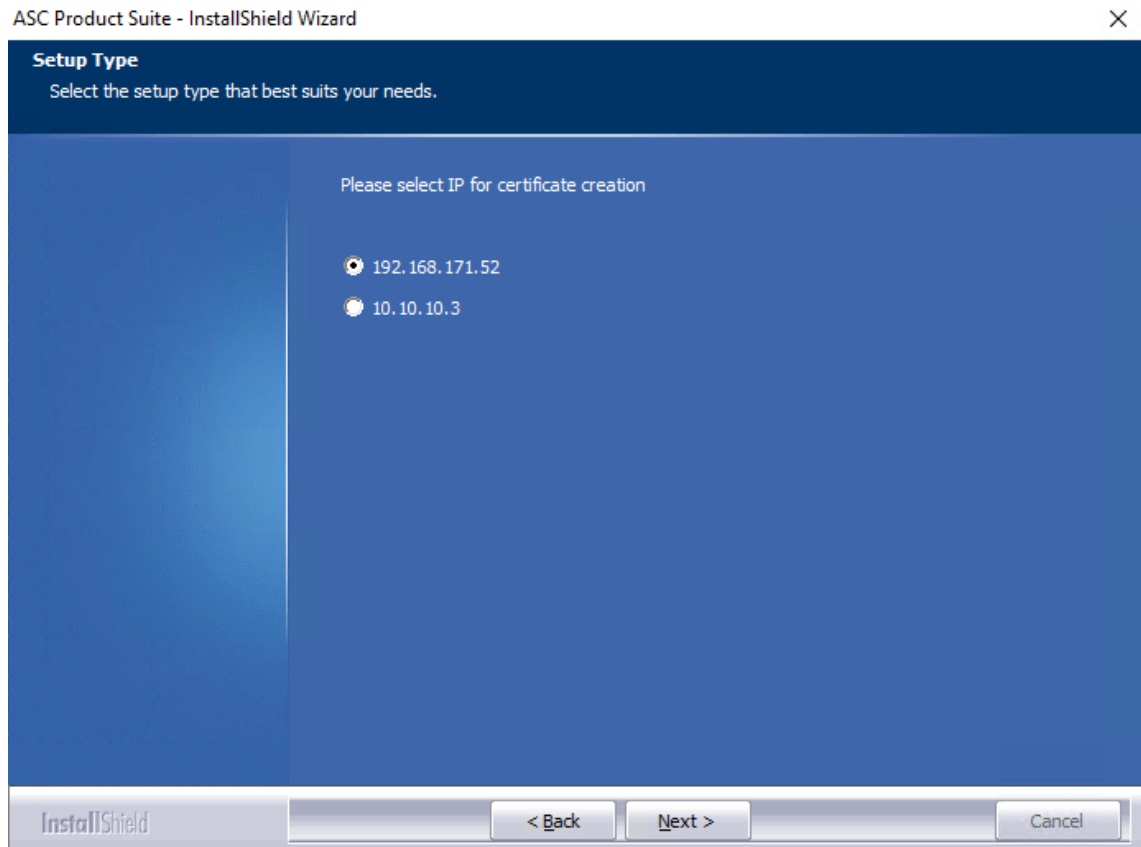


Abb. 23: IP-Adresse der Netzwerkkarte auswählen (Beispiel IPv4)

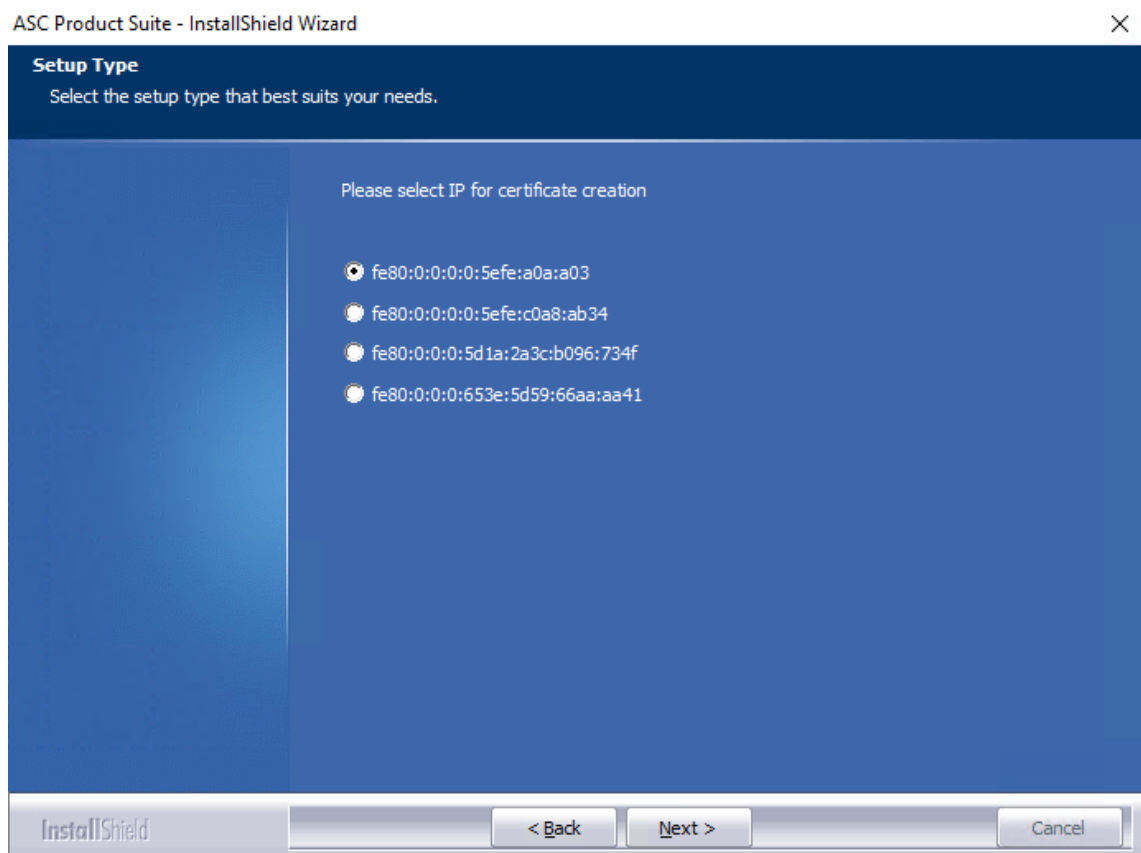


Abb. 24: IP-Adresse der Netzwerkkarte auswählen (Beispiel IPv6)

1. Wählen Sie die IP-Adresse der Netzwerkkarte aus, für die das Zertifikat erzeugt werden soll.

2. Klicken Sie auf die Schaltfläche *Next*.

⇒ Die Installations-Routine zur Installation von WinPcap startet.



Falls Sie einen Server ohne Aufzeichnung installieren möchten, können Sie die Installation des WinPcap überspringen. Fahren Sie dann fort mit [Kapitel "Updater starten"](#), S. 31.

8.5

WinPcap installieren



Die Installation von WinPcap ist nur auf Servern erforderlich, auf denen auch eine Aufzeichnung läuft. Für Installationen von Servern ohne Aufzeichnungs-komponenten können Sie die folgende Routine abbrechen, indem Sie auf die Schaltfläche *Cancel* klicken.

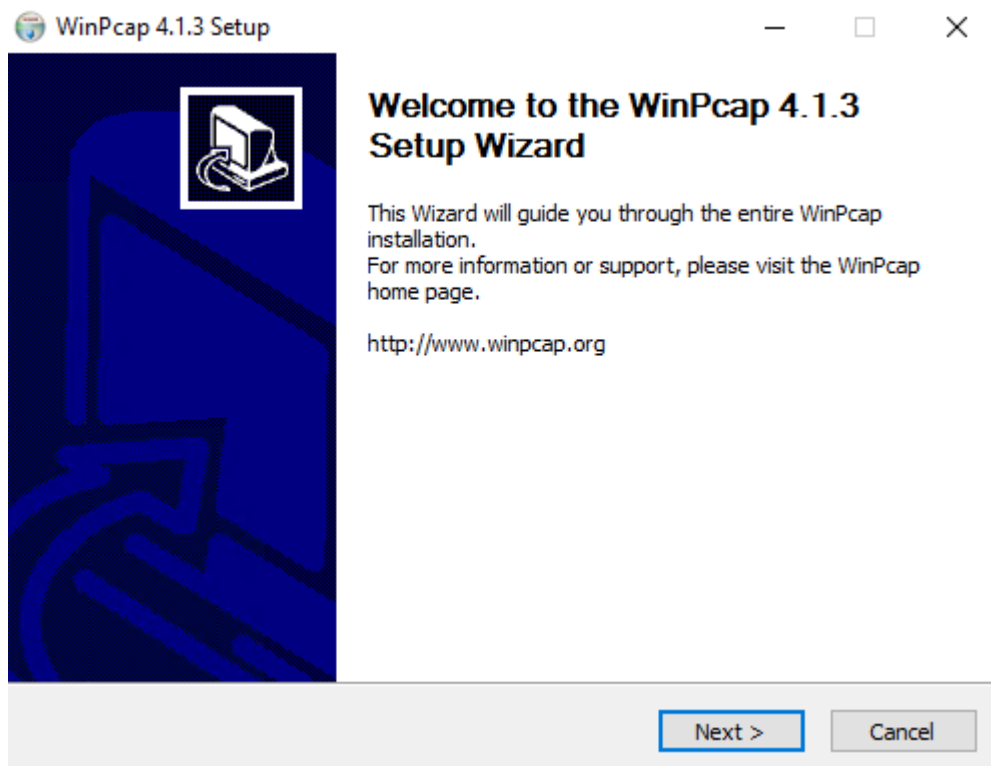


Abb. 25: Installationsassistent Startbildschirm

1. Klicken Sie auf die Schaltfläche *Next*.

2. Klicken Sie auf die Schaltfläche *Next*.

⇒ Das Fenster mit der Lizenzabfrage erscheint.

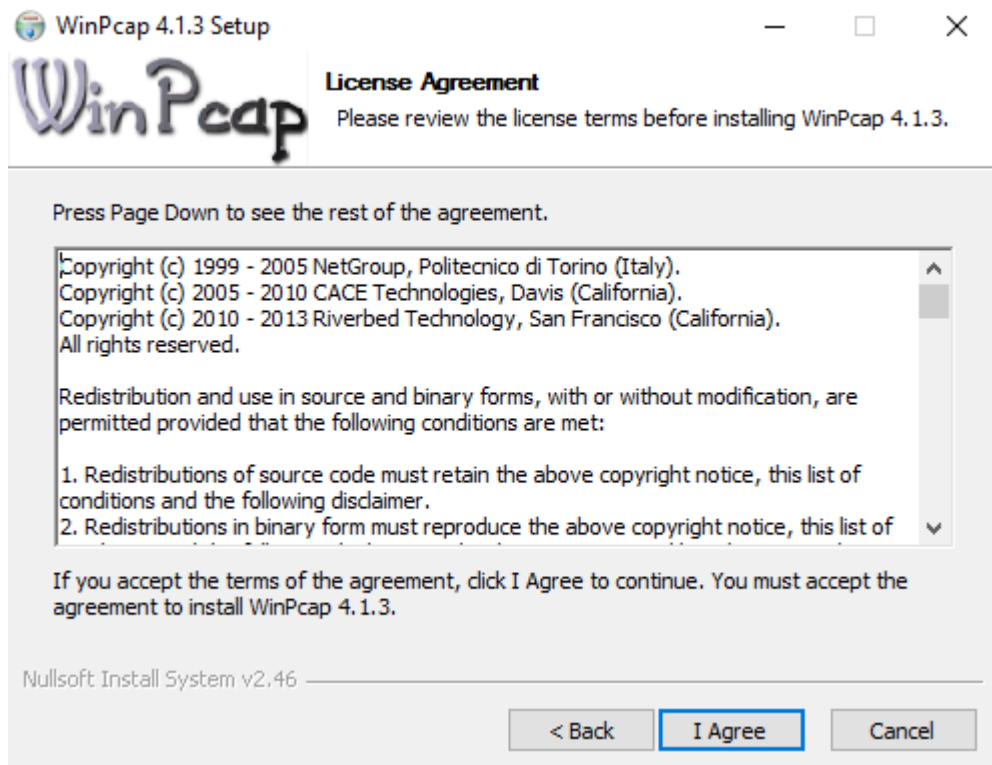


Abb. 26: Lizenzabfrage

3. Klicken Sie auf die Schaltfläche *I Agree*, um die Lizenzvereinbarung zu akzeptieren.
⇒ Das folgende Fenster erscheint:

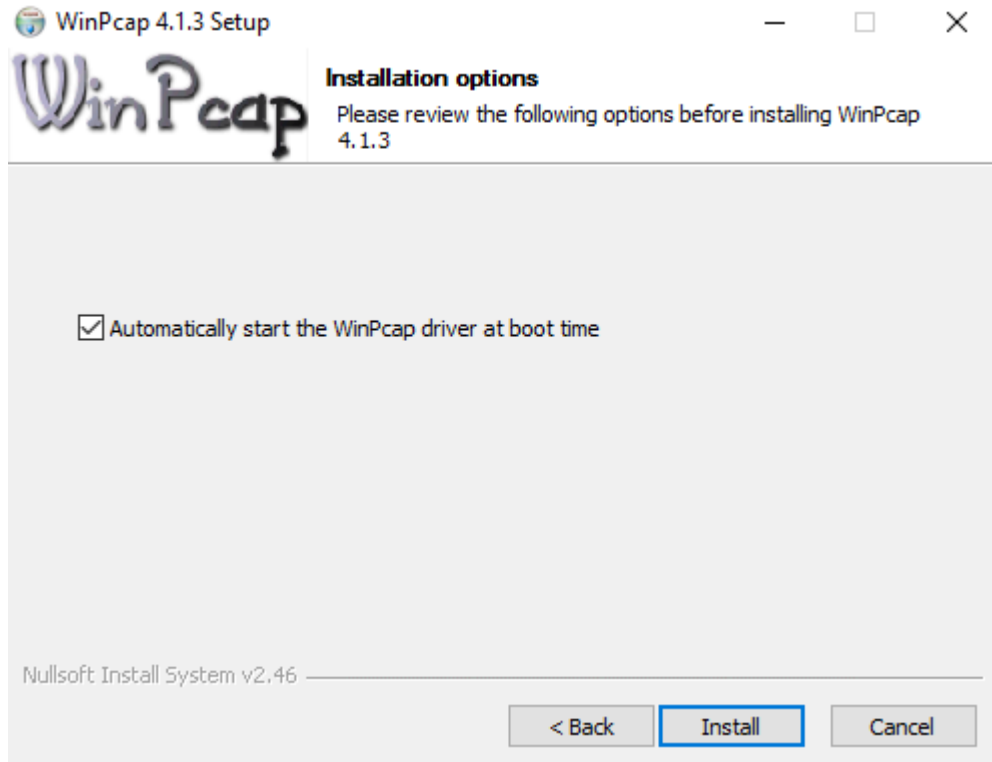


Abb. 27: Installation der Software WinPcap starten

4. Starten Sie die Installation, indem Sie auf die Schaltfläche *Install* klicken.

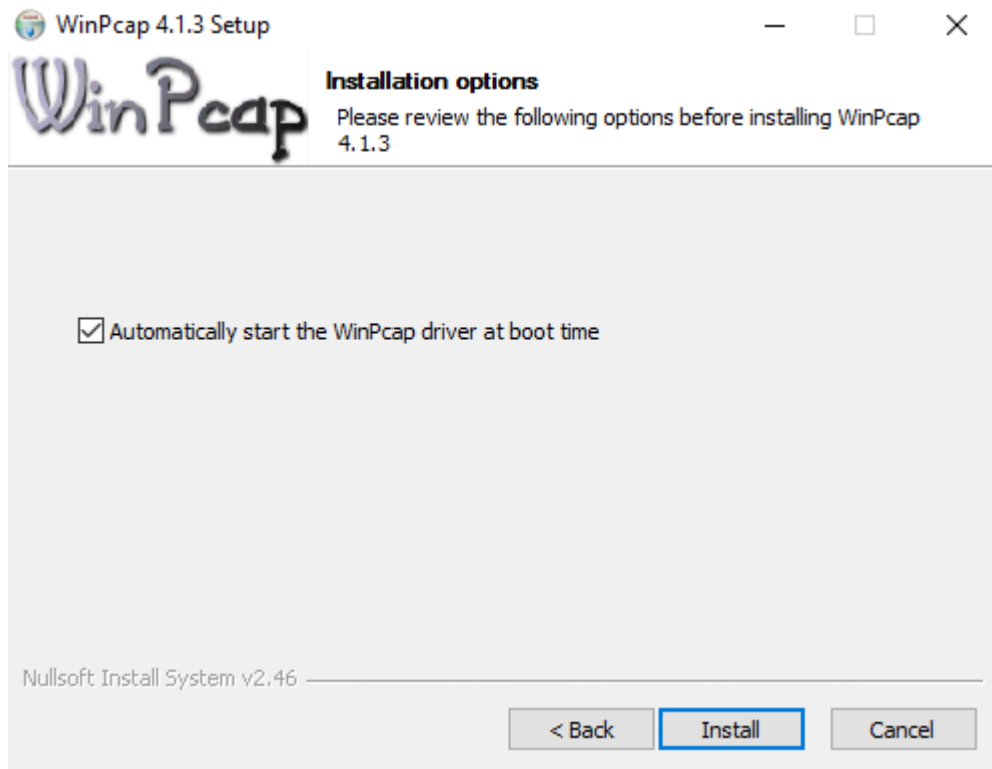


Abb. 28: Installation der Software WinPcap beenden

5. Beenden Sie die Installation der Software *WinPcap*, indem Sie auf die Schaltfläche *Finish* klicken.

8.6

Updater starten

Die Installations-Routine führt Sie zum *ASC Updater*.

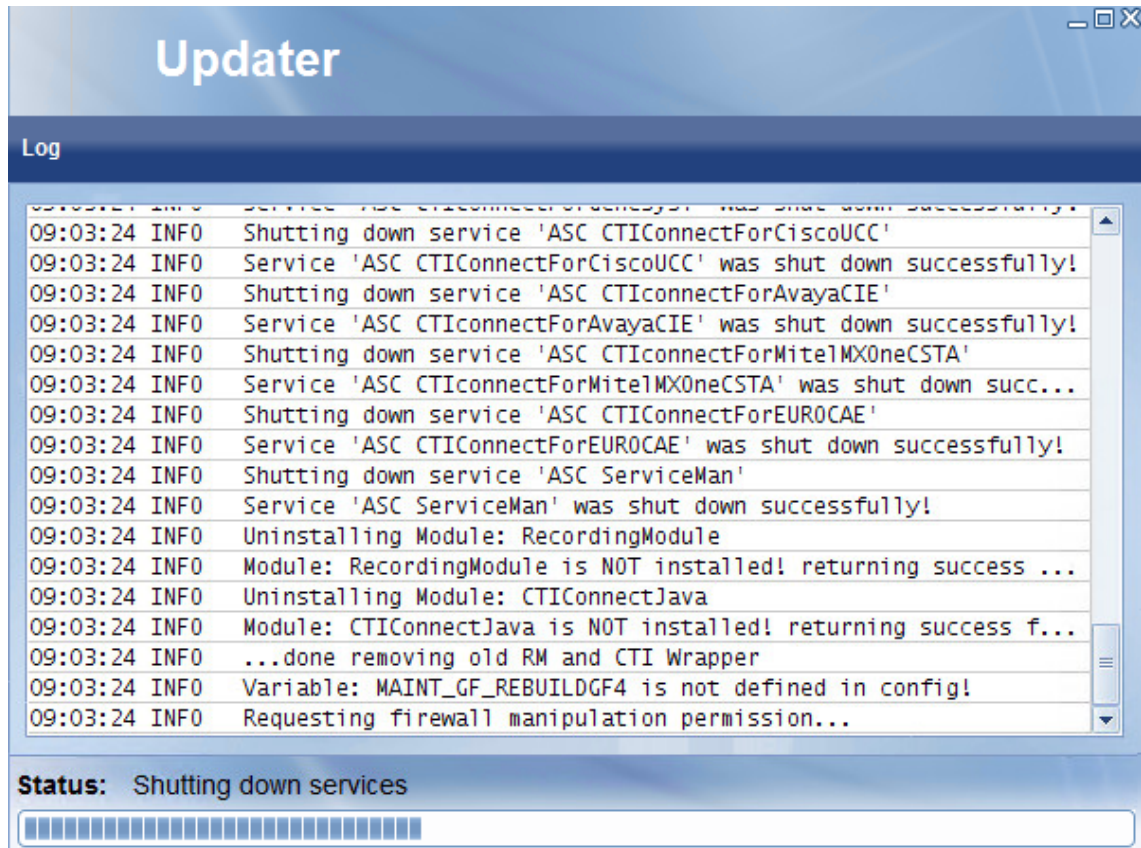


Abb. 29: ASC Updater - Services werden herunterfahren

Die Sicherheitsabfrage zum Öffnen der Firewall-Ports für das Software-Update erscheint.



Abb. 30: ASC Updater - Sicherheitsabfrage für Firewall

- Bestätigen Sie die Abfrage mit Yes, damit der Updater weiterlaufen kann.
⇒ Die Abfrage zum Installieren der Gerätesoftware für die Aufzeichnungskarten erscheint.

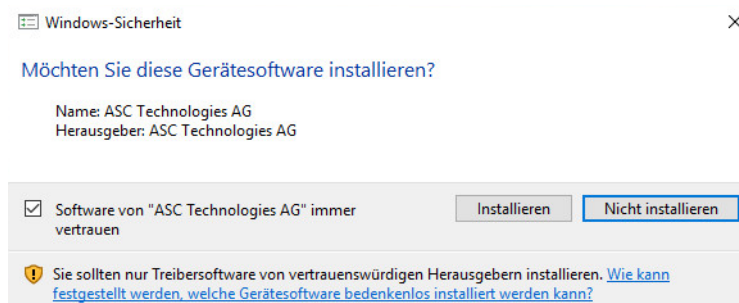


Abb. 31: Gerätetreiber für die Aufzeichnungskarten installieren

- In diesem Dialogfenster müssen Sie eine Auswahl treffen, damit der Updater weiterlaufen kann.

3. Wenn Sie eine **VOIP**-Aufzeichnung verwenden möchten und keine Aufzeichnungskarten installiert sind, klicken Sie auf die Schaltfläche *Nicht installieren*.
Wenn Sie eine TDM-Aufzeichnung mit Aufzeichnungskarten verwenden möchten, müssen Sie den Gerätetreiber für die Aufzeichnungskarten installieren, klicken Sie dazu auf die Schaltfläche *Installieren*.

⇒ Das Fenster mit dem Installationsreport öffnet sich.

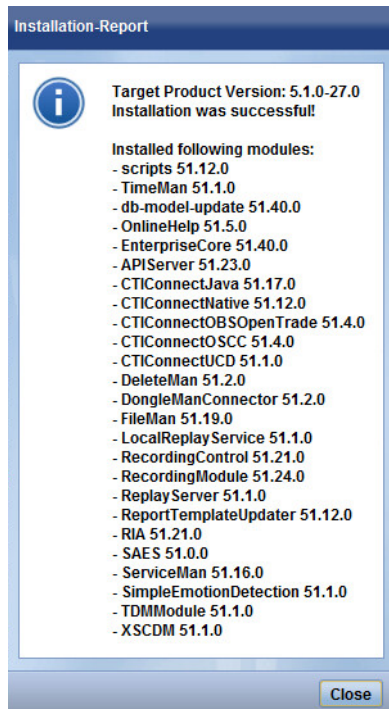


Abb. 32: ASC Updater - Installation Report

4. Klicken Sie auf die Schaltfläche *Close*, um den Updater zu beenden.

⇒ Der *InstallShield Wizard* erscheint wieder.

ASC Product Suite - InstallShield Wizard

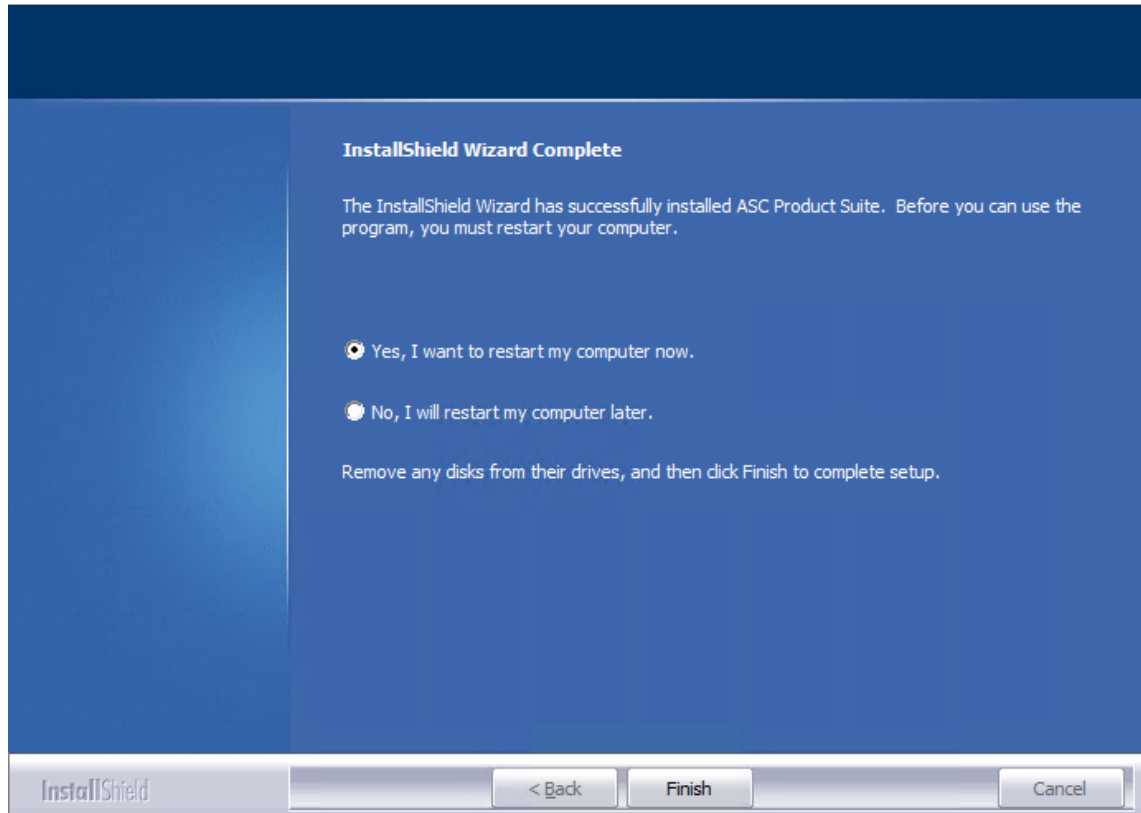


Abb. 33: Installation beenden und Server durchstarten

5. Wählen Sie die Option *Yes, I want to restart my computer now.*
6. Beenden Sie die Installation der Aufzeichnungssoftware, indem Sie auf die Schaltfläche *Finish* klicken.

9

HTTPS-Zertifikat importieren

9.1

Zertifikat über CSR anfordern

Falls Sie ein Zertifikat bei einer autorisierten Zertifizierungsstelle anfordern möchten, können Sie mit dem Certificate Import Tool eine Anforderung mit Ihren firmenspezifischen Daten erstellen.

1. Öffnen Sie den Windows Explorer, um das Tool aufzurufen.
2. Wechseln Sie in den Ordner *C:\Program Files (x86)\ASC\ASC Product Suite\scripts*.
3. Doppelklicken Sie auf die Datei *certimporter.exe*.
⇒ Das Fenster Certificate Import Tool erscheint.

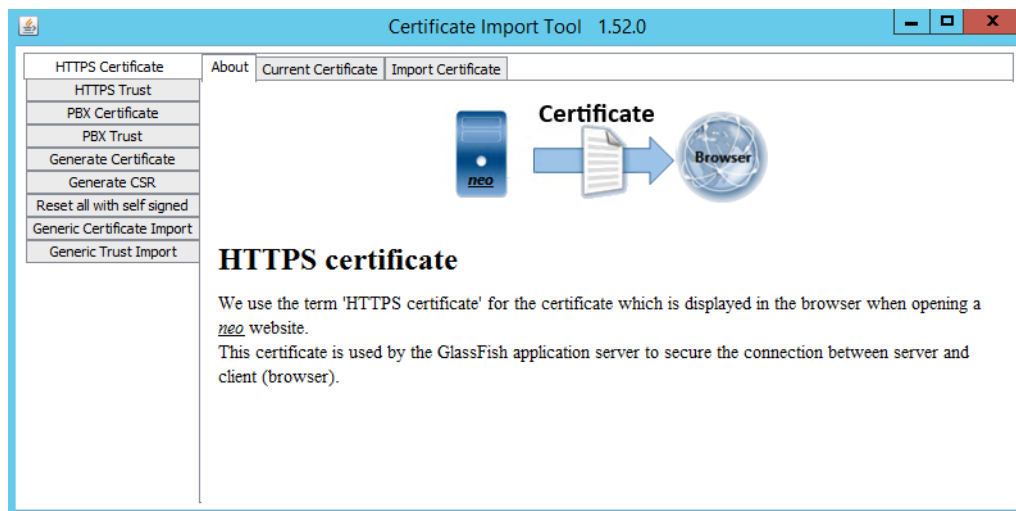


Abb. 34: Certificate Import Tool

4. Wählen Sie in der Navigationsleiste den Menüpunkt *Generate CSR*, um einen Certificate Signing Request zu erstellen.
⇒ Das Fenster **CSR** erscheint, zur Eingabe der firmenspezifischen Daten.

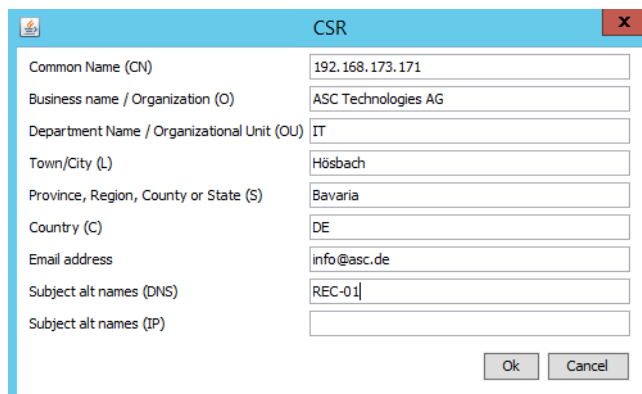


Abb. 35: Firmenspezifische Parameter zur Authentifizierung angeben

5. Geben Sie die Firmendaten ein.
6. Klicken Sie auf die Schaltfläche *Ok*.
⇒ Das Explorerfenster erscheint, zur Auswahl des Ablageverzeichnisses.
7. Wählen Sie das Verzeichnis, in dem Sie die Anfrage für das Zertifikat speichern möchten.
8. Klicken Sie auf die Schaltfläche *Open*.
⇒ Die folgende Erfolgsmeldung erscheint:

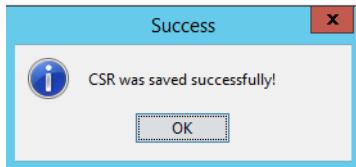


Abb. 36: Erfolgsmeldung

9. Klicken Sie auf die Schaltfläche **OK**.
10. Die gespeicherte Datei können Sie zu einer Zertifizierungsstelle schicken, um ein Zertifikat anzufordern.



Wenn Sie Zertifikate ohne privaten Key oder mit einem unpassenden privaten Key importieren, kann es dazu führen, dass das System nicht mehr hochfährt. Das Risiko besteht auch, wenn das Zertifikat nicht über einen [CSR](#) erstellt wurde.

11. Das neue Zertifikat können Sie über die Option *X.509/Private key* importieren. Siehe [Kapitel "X.509/Private key importieren"](#), S. 36.

9.2

Kundenspezifisches HTTPS-Zertifikat importieren

Falls Sie ein kundenspezifisches Zertifikat verwenden möchten, können Sie dieses mit dem Programm *certimporter.exe* importieren.

1. Wechseln Sie in den Ordner *C:\Program Files (x86)\ASC\ASC Product Suite\scripts*.
2. Öffnen Sie die Datei *certimporter.exe*.
⇒ Das Fenster Certificate Import Tool erscheint.

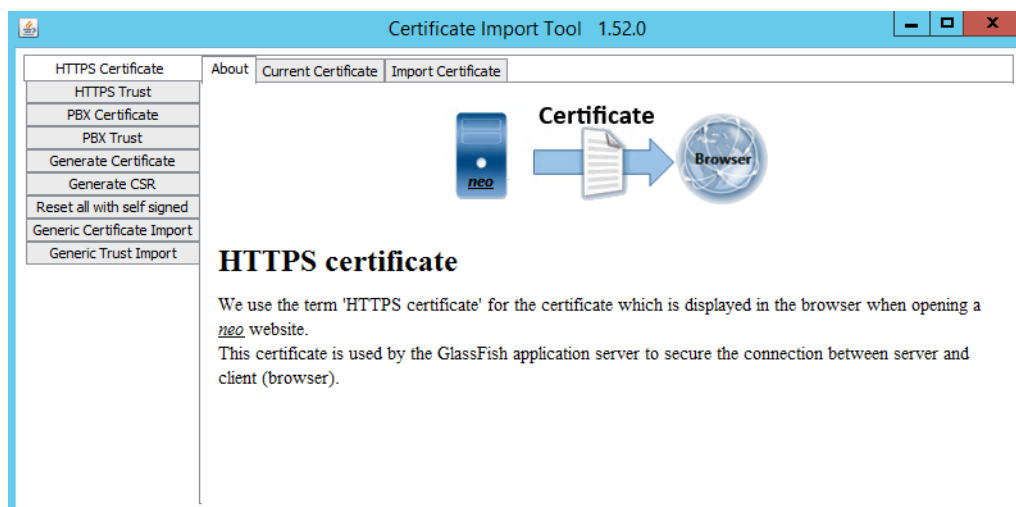


Abb. 37: Certificate Import Tool

Folgende Formate werden unterstützt:

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

9.2.1

X.509/Private key importieren

1. Wählen Sie in der Navigationsleiste den Menüpunkt *HTTPS Certificate*.
2. Klicken Sie auf die Registerkarte *Import Certificate*.
3. Liegt ihr Zertifikat als *X.509/Private key* vor, wählen Sie die Option *Certificate X.509 (RSA Private key)*.
4. Klicken Sie neben dem Feld *Certificate X.509* auf die Schaltfläche , um Ihr Zertifikat auszuwählen.

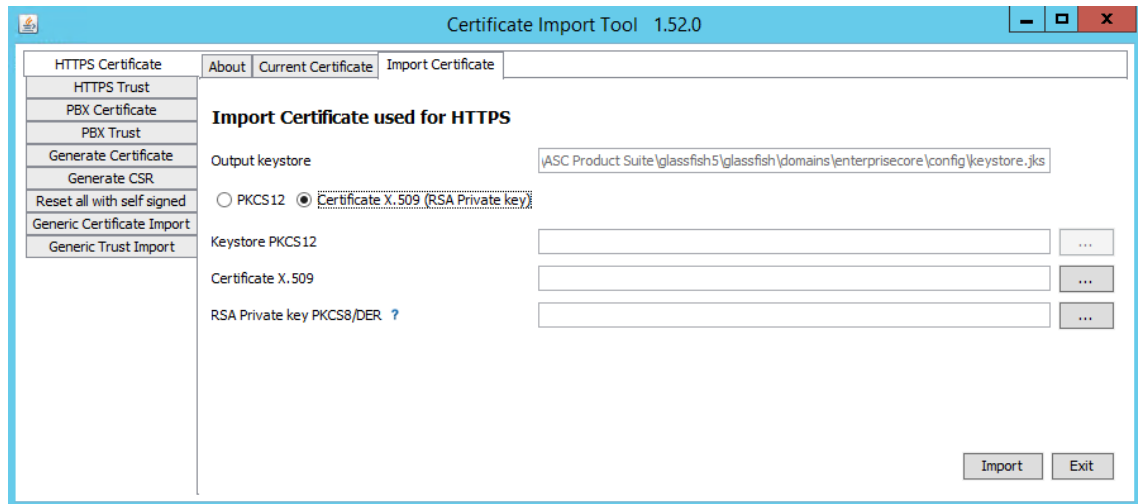


Abb. 38: X.509 importieren

5. Klicken Sie auf die Schaltfläche *Import*.
 ⇒ Das Fenster zur Eingabe des Passworts für den Private Key erscheint.

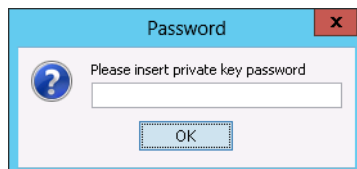


Abb. 39: Passwort für den Private Key eingeben

6. Geben Sie das Passwort für Ihren Private Key ein.
Sollten Sie kein Passwort verwenden, können Sie das Feld leer lassen.
7. Klicken Sie auf die Schaltfläche *OK*, um das Passwort zu bestätigen.
 ⇒ Die Meldung über den erfolgreichen Import erscheint.

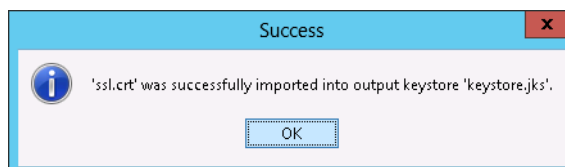


Abb. 40: Meldung - Erfolgreicher Import

8. Klicken Sie auf die Schaltfläche *OK*, um die Erfolgsmeldung zu bestätigen.
9. Klicken Sie auf die Schaltfläche *Exit*, um das Programm zu verlassen.
10. Starten Sie den Glassfish-Server neu, damit das Zertifikat übernommen wird.
11. In der Registerkarte *Current Certificate* können Sie das aktuell gültige Zertifikat überprüfen.

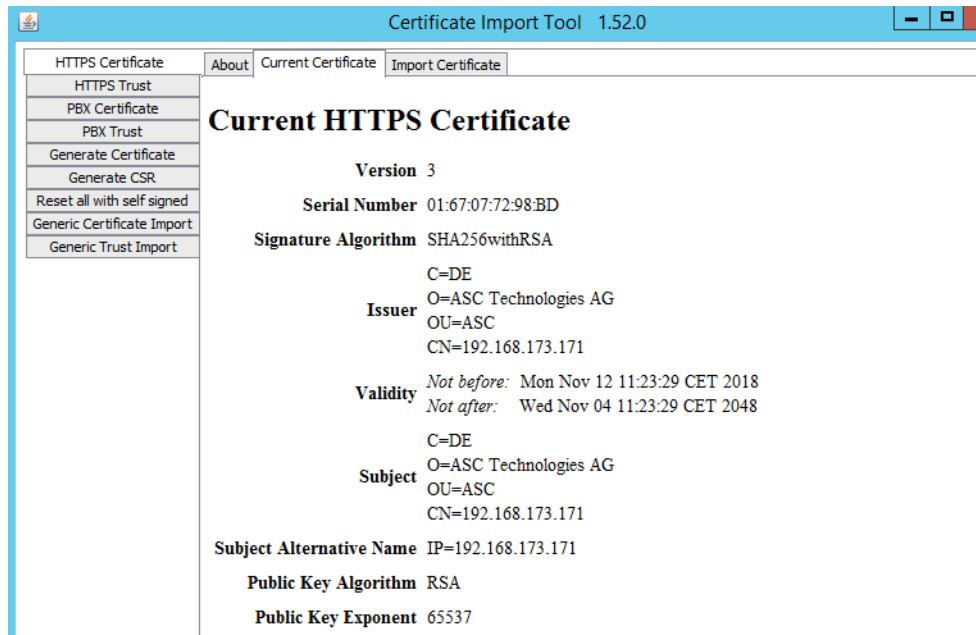


Abb. 41: Aktuell gültiges HTTPS-Zertifikat überprüfen

9.2.2

PKCS12 importieren

1. Wählen Sie in der Navigationsleiste den Menüpunkt *HTTPS Certificate*.
2. Klicken Sie auf die Registerkarte *Import Certificate*.
3. Liegt ihr Zertifikat als PKCS12 Keystore vor, wählen Sie die Option *PKCS12*.
4. Klicken Sie auf die Schaltfläche neben dem Feld *Keystore PKCS12*, um Ihren PKCS12 Keystore auszuwählen.

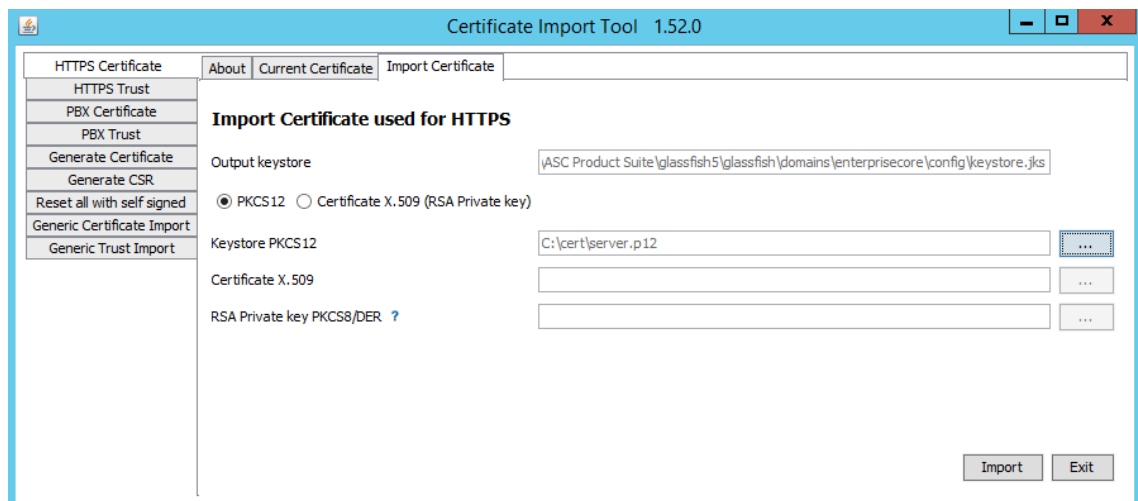


Abb. 42: PKCS12 Keystore importieren

5. Klicken Sie auf die Schaltfläche *Import*.
⇒ Das Fenster zur Eingabe des Alias für PKCS12 Keystore erscheint.

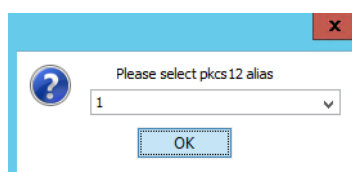


Abb. 43: Alias bestätigen

6. Klicken Sie auf die Schaltfläche *OK*, um den Alias zu bestätigen.

⇒ Das Fenster zur Eingabe des Passworts erscheint.

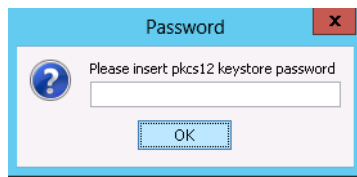


Abb. 44: Passwort für PKCS12 Keystore eingeben

7. Geben Sie das Passwort für Ihren PKCS12 Keystore ein.
Sollten Sie kein Passwort verwenden, können Sie das Feld leer lassen.
8. Klicken Sie auf die Schaltfläche *OK*, um das Passwort zu bestätigen.
9. Klicken Sie auf die Schaltfläche *Exit*, um das Programm zu verlassen.
10. Starten Sie den Glassfish-Server neu, damit das Zertifikat übernommen wird.
11. In der Registerkarte *Current Certificate* können Sie das aktuell gültige Zertifikat überprüfen.

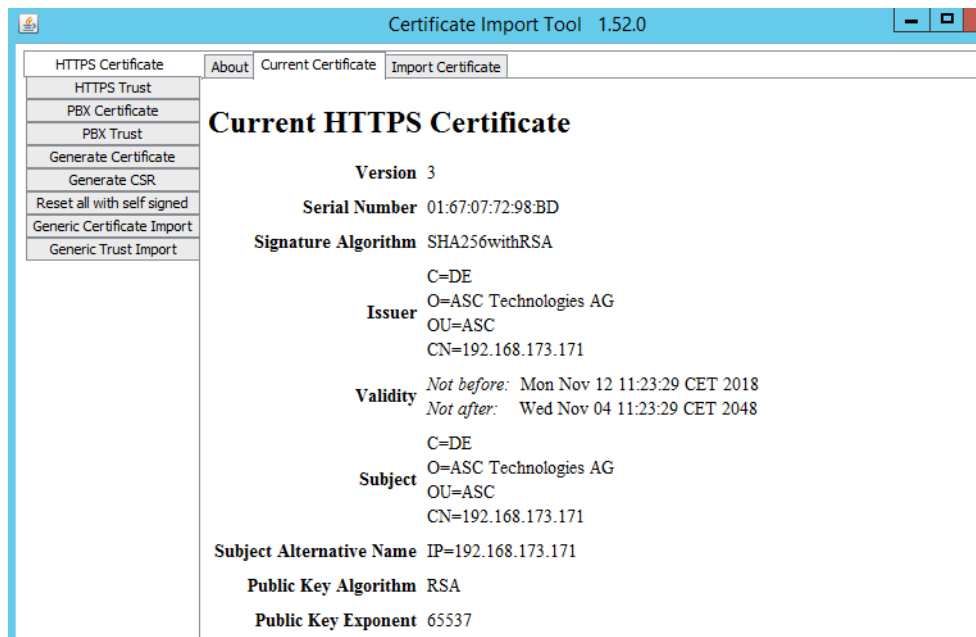


Abb. 45: Aktuell gültiges HTTPS-Zertifikat überprüfen

Abbildungsverzeichnis

Abb. 1	Microsoft Visual C++ installieren	12
Abb. 2	Hinweis, dass SNMP nicht installiert ist	12
Abb. 3	Installationsroutine starten	13
Abb. 4	Zielverzeichnis für die Installation bestätigen.....	14
Abb. 5	Datenpartition bestätigen	15
Abb. 6	Sprachen für die grafische Benutzeroberfläche auswählen.....	16
Abb. 7	Sprachen für die grafische Benutzeroberfläche auswählen.....	16
Abb. 8	Cluster-ID eingeben	17
Abb. 9	Multi-Server-Systeme installieren	18
Abb. 10	Adresse des NTP-Servers eingeben.....	19
Abb. 11	Features zur Installation auswählen.....	20
Abb. 12	Ziellaufwerk für die interne Datenbank wählen	21
Abb. 13	Typ der externen Datenbank auswählen	22
Abb. 14	Verknüpfung zur externen Datenbank erstellen.....	23
Abb. 15	Benutzer für die Datenbank konfigurieren.....	23
Abb. 16	Abfrage zur MSSQL-Serverinstanz.....	24
Abb. 17	Namen der MSSQL-Instanz eingeben	24
Abb. 18	Installationsvorgang starten	25
Abb. 19	Information zum Installationsfortschritt.....	25
Abb. 20	Webserver Ports konfigurieren.....	26
Abb. 21	IP-Protokoll auswählen	27
Abb. 22	Durchführung der IP-Protokoll-Installation	27
Abb. 23	IP-Adresse der Netzwerkkarte auswählen (Beispiel IPv4).....	28
Abb. 24	IP-Adresse der Netzwerkkarte auswählen (Beispiel IPv6).....	28
Abb. 25	Installationsassistent Startbildschirm	29
Abb. 26	Lizenzabfrage.....	30
Abb. 27	Installation der Software WinPcap starten	30
Abb. 28	Installation der Software WinPcap beenden	31
Abb. 29	ASC Updater - Services werden herunterfahren.....	32
Abb. 30	ASC Updater - Sicherheitsabfrage für Firewall	32
Abb. 31	Gerätetreiber für die Aufzeichnungskarten installieren	32
Abb. 32	ASC Updater - Installation Report.....	33
Abb. 33	Installation beenden und Server durchstarten	34
Abb. 34	Certificate Import Tool.....	35
Abb. 35	Firmenspezifische Parameter zur Authentifizierung angeben.....	35
Abb. 36	Erfolgsmeldung	36
Abb. 37	Certificate Import Tool.....	36
Abb. 38	X.509importieren.....	37
Abb. 39	Passwort für den Private Key eingeben	37
Abb. 40	Meldung - Erfolgreicher Import.....	37
Abb. 41	Aktuell gültiges HTTPS-Zertifikat überprüfen.....	38

Abb. 42	PKCS12 Keystore importieren	38
Abb. 43	Alias bestätigen	38
Abb. 44	Passwort für PKCS12 Keystore eingeben	39
Abb. 45	Aktuell gültiges HTTPS-Zertifikat überprüfen	39

Tabellenverzeichnis

Tab. 1	Login-Daten - Systembetreiber	5
Tab. 2	Login-Daten - 1. Mandant	6

Glossar

App-Server

Applikationsserver bzw. Web-Server. In den Systemarchitekturen ist das der Server, auf dem der Enterprise Core und die GlassFish-Software installiert sind.

CSR

Certificate Signing Request

Multi-Server-System

Aufzeichnungssystem, in dem die einzelnen Komponenten (Enterprise Core, Aufzeichnungskomponenten, Datenbank) auf verschiedenen Servern installiert sind.

NTP

Network Time Protocol NTP ist ein Standard zur Synchronisierung von Uhren in Computersystemen über paketbasierte Kommunikationsnetze. NTP verwendet das verbindungslose Transportprotokoll UDP. Es wurde speziell entwickelt, um eine zuverlässige Zeitangabe über Netzwerke mit variabler Paketlaufzeit zu ermöglichen. (Quelle: Wikipedia 12.06.2018)

Single-Server-System

Aufzeichnungssystem, in dem alle Komponenten (Enterprise Core, Aufzeichnungskomponenten, Datenbank) auf einem einzigen Server installiert sind.

SNMP

Simple Network Management Procol ist ein Netzwerkprotokoll und dient zur Überwachung und Steuerung von Netzwerkkomponenten. Das Protokoll ist beim Transport nicht auf das IP-Netzwerkprotokoll angewiesen. Es versendet unaufgefordert Nachrichten (Traps) von Aktivitäten auf den Netzwerkelementen.

VoIP

Voice over IP