

Konfiguration IP-Adressen-Änderung



Administrationsanleitung für Systembetreiber

19.11.2020

Originalanleitung

Produktlinie neo, Version 6.x

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

EVOIPneo

EVOLUTIONneo / XXL / eco

INSPIRATIONneo

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	IP-Adressen-Änderung im Betriebssystem	6
4	IP-Adressen-Änderung in der Aufzeichnungssoftware	8
5	HTTPS-Zertifikat aktualisieren	11
5.1	Von ASC erzeugtes selbst generiertes SSL/TLS-Zertifikat aktualisieren	11
5.2	Kundenspezifisches HTTPS-Zertifikat importieren	13
5.2.1	X.509/Private key importieren	13
5.2.2	PKCS12 importieren	15
	Abbildungsverzeichnis	17
	Tabellenverzeichnis	18
	Glossar	19

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

2 Einleitung

Während der Installation der ASC-Software wird die IP-Adresse des Aufzeichnungsservers automatisch ausgelesen. Diese Anleitung beschreibt die Schritte, die bei einer nachträglichen Änderung der IP-Adresse erforderlich sind.



Dieses Kapitel bezieht sich ausschließlich auf die englische Sprachvariante, da ASC nur das englische Betriebssystem unterstützt.

1. Drücken Sie die Windows-Taste.
2. Öffnen Sie das Fenster *Network and Sharing Center* (Netzwerkverbindung) über *Control Panel > Network and Internet > Network and Sharing Center*.
3. Klicken Sie auf der linken Seite auf *Change adapter settings*.

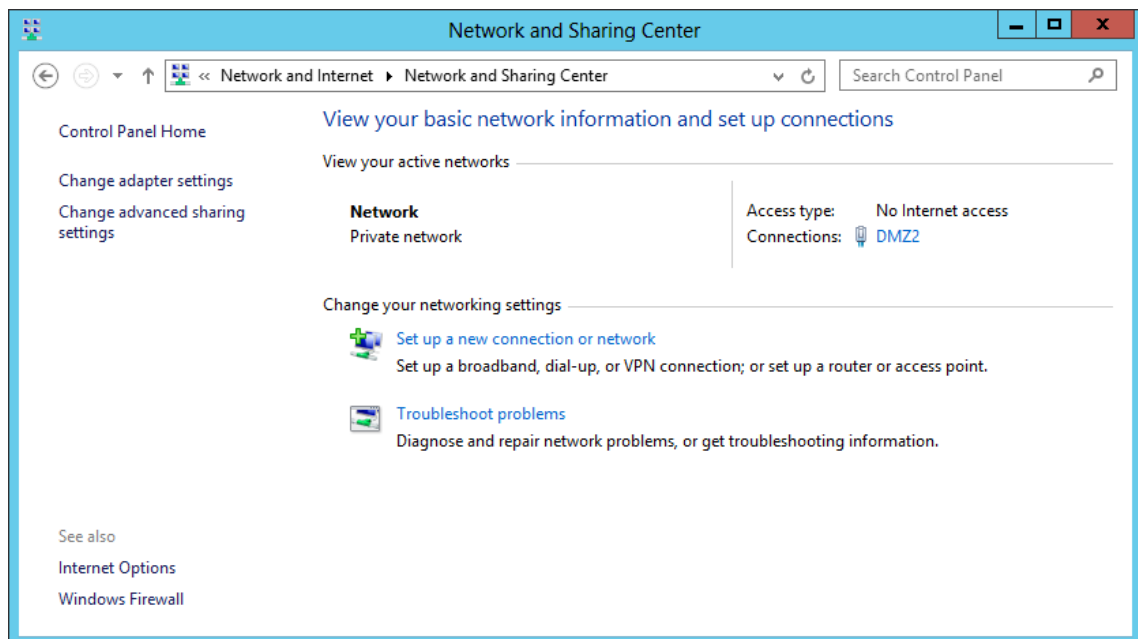


Abb. 1: Netzwerk- und Freigabe-Center

4. Klicken Sie auf die eingesetzte Karte.
5. Öffnen Sie mit der rechten Maustaste das Kontextmenü.
6. Wählen Sie den Menüpunkt *Properties*.

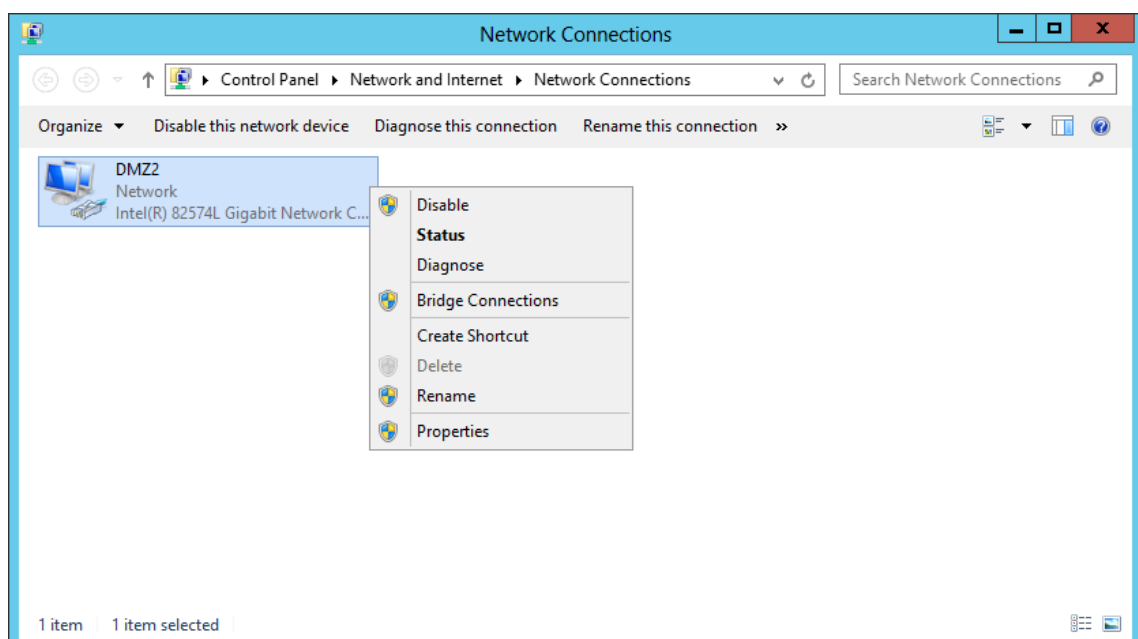


Abb. 2: Netzwerkverbindungen

7. Klicken Sie im Fenster der Eigenschaften auf die Schaltfläche *Properties*.

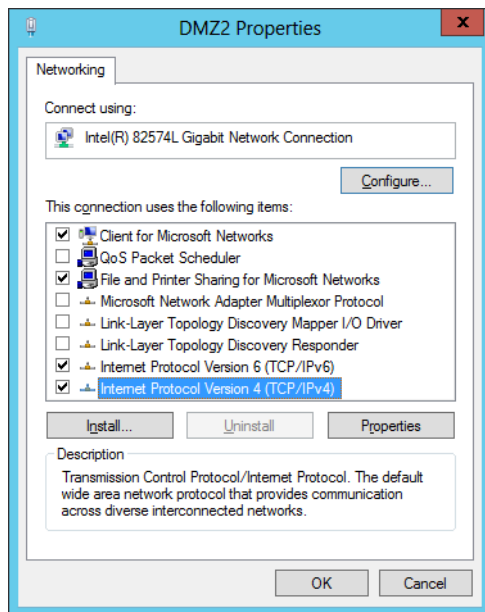


Abb. 3: Netzwerkverbindung Eigenschaften

8. Für die ASC-Software muss eine statische IP-Adresse vergeben werden. Wählen Sie die Option *Use the following IP address*.

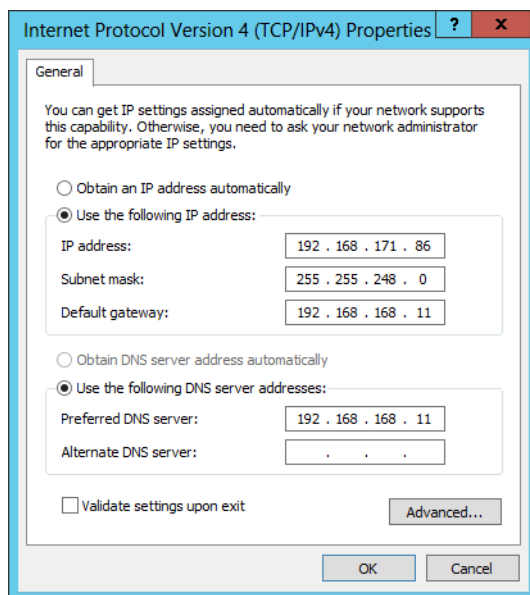


Abb. 4: IP-Adresse konfigurieren

9. Geben Sie die IP-Adresse, die Subnetzmaske und das Standard-Gateway ein.
10. Klicken Sie auf die Schaltfläche *OK*, um die Einstellungen zu speichern und das Fenster zu schließen.

IP-Adressen-Änderung in der Aufzeichnungssoftware

Nach einer Änderung der IP-Adresse auf Betriebssystem-Ebene muss die IP-Adresse auch in der Aufzeichnungssoftware übernommen werden.

Dazu müssen Sie auf jeden Fall auf den entsprechenden Servern den Service *ASC ServiceMan* neu starten.

1. Öffnen Sie das Fenster *Services* über *Start > Administrative Tools > Services*.
2. Starten Sie den Service *ASC ServiceMan* neu.
3. Prüfen Sie in der Applikation System Configuration, dass im Server-Modul die entsprechende IP-Adresse für die Kommunikation ausgewählt ist.
4. Falls Sie die IP-Adresse im Server-Modul umkonfigurieren müssen, wechseln Sie in das Integrationen-Modul und deaktivieren Sie die verwendete Integration.
5. Wechseln Sie in das Aufzeichnungsarchitekturen-Modul und deaktivieren Sie die Aufzeichnungsarchitektur.
6. Dann wird im Server-Modul die Option zur Konfiguration der entsprechenden IP-Adresse aktiv.
7. Konfigurieren Sie die entsprechende IP-Adresse.
8. Aktivieren Sie dann zuerst im Aufzeichnungsarchitekturen-Modul die Aufzeichnungsarchitektur wieder.
9. Aktivieren Sie dann im Integrationen-Modul die Integration wieder.
10. Prüfen Sie anschließend, ob die Aufzeichnung korrekt erfolgt.

Zusätzliche Schritte bei Multi-Server-Systemen

Falls Sie bei Multi-Server-Systemen die IP-Adresse eines oder mehrerer [App-Server](#) geändert haben, müssen Sie allen Servern ohne [App-Server](#)-Komponenten die neuen IP-Adressen bekannt geben.

Die Änderung müssen Sie manuell über den Windows-Explorer in der Konfigurationsdatei *setup.xml* vornehmen.

1. Öffnen Sie den Windows-Explorer, um auf die Konfigurationsdatei *setup.xml* zuzugreifen.
2. Wechseln Sie in das Verzeichnis *C:\Program Files (x86)\ASC\ASC Product Suite\Updater\config*.

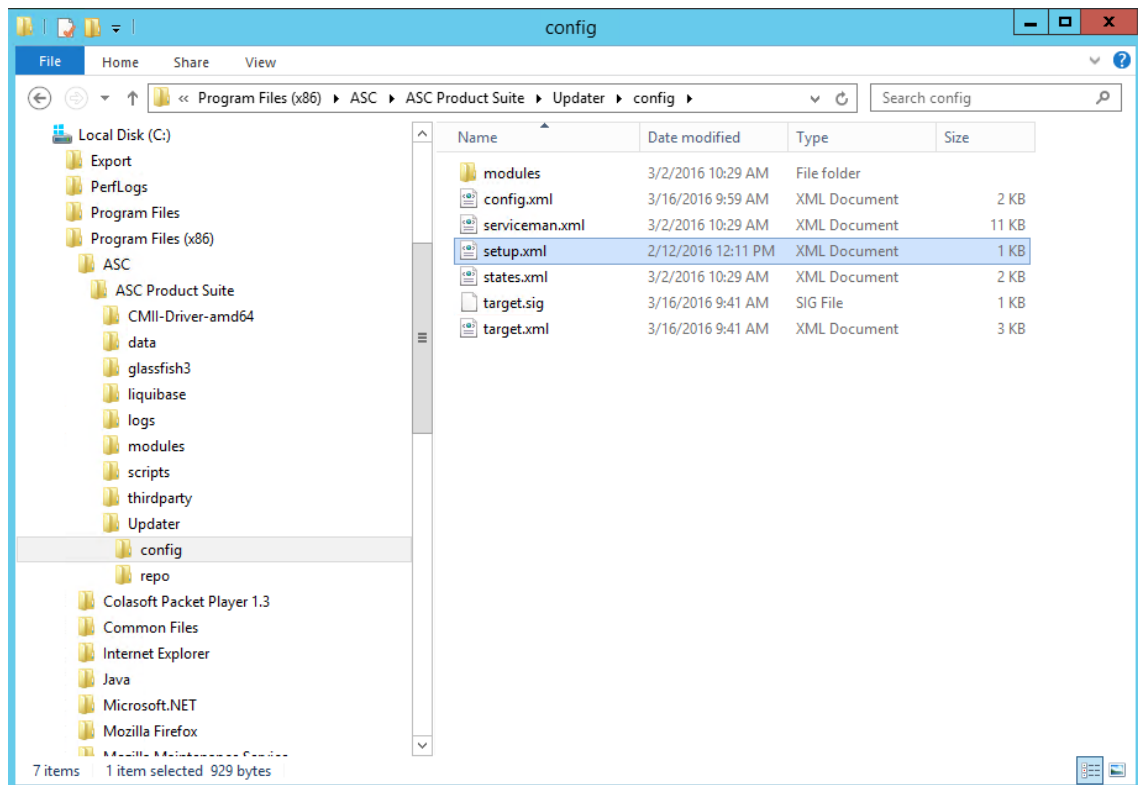


Abb. 5: Pfad zur Datei Setup.xml

3. Öffnen Sie die Datei *setup.xml* zum Bearbeiten im Editor, z. B. Notepad.

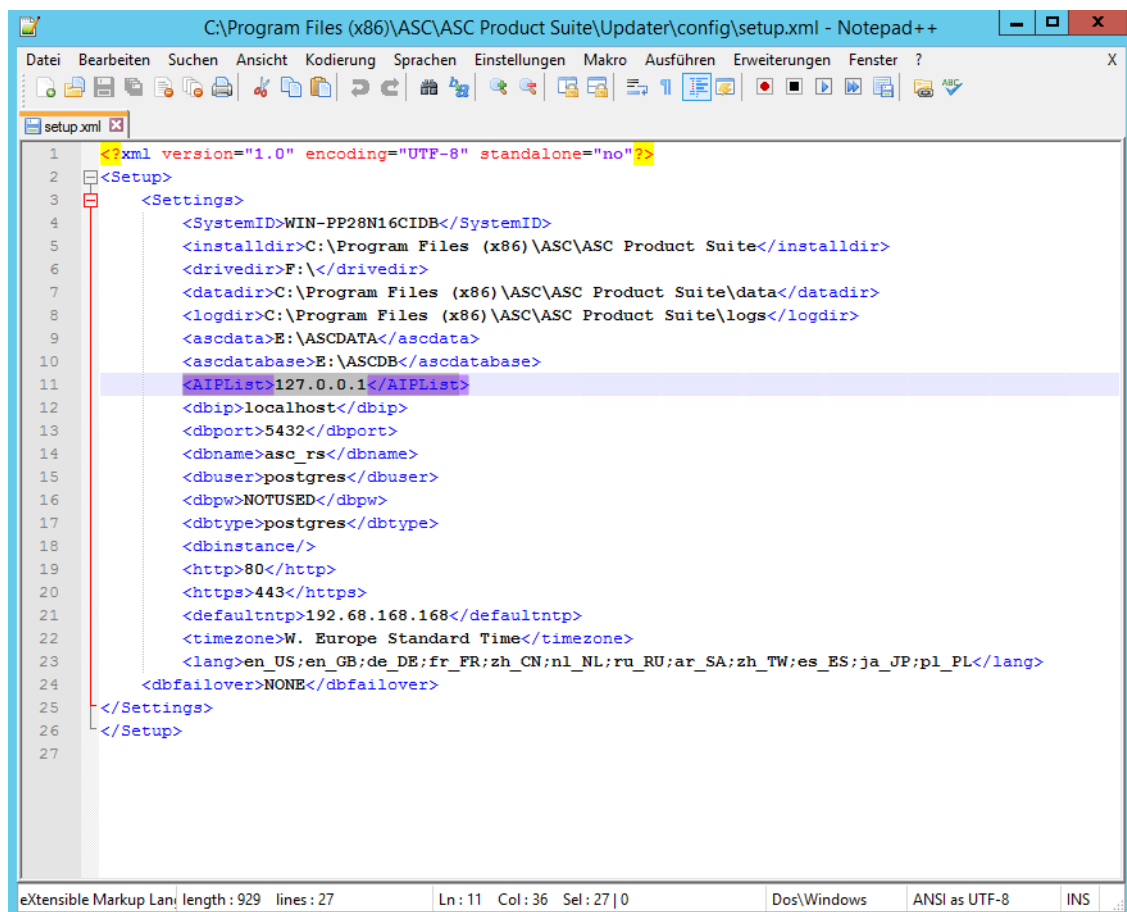


Abb. 6: IP-Adressen in Setup.xml ändern

4. Geben Sie in der Zeile `<AIPList>127.0.0.1</AIPList>` die neue IP-Adresse des Application Servers ein.
Falls Sie mehrere Server verwenden, geben Sie die entsprechenden IP-Adressen durch Semikolon getrennt ein.
5. Speichern Sie die Datei *setup.xml* ab.
6. Um die Änderungen zu übernehmen, müssen Sie alle ASC-Services neu starten.
7. Öffnen Sie das Fenster *Services* über *Start > Administrative Tools > Services*.
8. Starten Sie alle ASC-Services neu. Alternativ dazu können Sie auch den Server neu starten.

5

HTTPS-Zertifikat aktualisieren

5.1

Von ASC erzeugtes selbst generiertes SSL/TLS-Zertifikat aktualisieren

ASC liefert ein Zertifikat mit aus, das bei der Änderung der IP-Adresse aktualisiert werden muss. Die Aktualisierung können Sie über das Certificate Import Tool durchführen.

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. Wählen Sie aus dem Kontextmenü der Datei *certimporter.exe* den Menüpunkt *Als Administrator ausführen* aus.
- ⇒ Das Fenster Certificate Import Tool erscheint.



Abb. 7: Certificate Import Tool

4. Klicken Sie auf die Schaltfläche *Reset all with self signed*, um ein Zertifikat mit der aktuellen IP-Adresse oder dem Hostnamen zu erzeugen und das automatisch generierte Zertifikat zu importieren.

⇒ Die folgende Meldung erscheint:

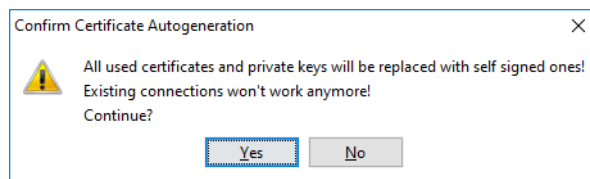


Abb. 8: Sicherheitsabfrage

5. Klicken Sie auf die Schaltfläche *Yes*, um die aktuell verwendeten Zertifikate und privaten Schlüssel zu ersetzen.

⇒ Es erscheint eine weitere Sicherheitsabfrage, um die Aktion gegebenenfalls abbrechen, da die bestehenden Verbindungen danach nicht mehr funktionieren.

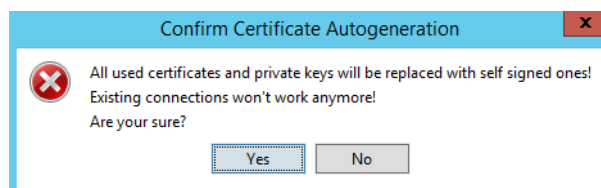


Abb. 9: Sicherheitsabfrage

6. Klicken Sie auf die Schaltfläche *Yes*, um die aktuell verwendeten Zertifikate und privaten Schlüssel zu überschreiben.
Klicken Sie auf die Schaltfläche *No*, um die verwendeten Zertifikate und Schlüssel zu behalten.

⇒ Falls Sie die Sicherheitsabfrage bestätigt haben, erscheint folgendes Fenster:

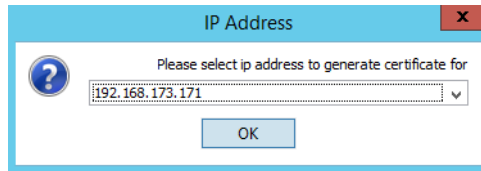


Abb. 10: IP-Adresse auswählen.

7. Wählen Sie aus der Dropdown-Liste entweder die IP-Adresse oder den Hostnamen aus, wofür das automatisch generierte Zertifikat erstellt werden soll.
8. Klicken Sie auf die Schaltfläche *OK*.

⇒ Das folgende Fenster erscheint, um die Gültigkeit des Zertifikats zu konfigurieren.

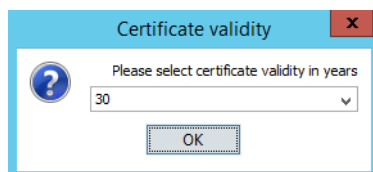


Abb. 11: Gültigkeitsdauer des Zertifikats auswählen

9. Wählen Sie aus der Dropdown-Liste die Anzahl der Jahre, wie lange das Zertifikat gültig sein soll.
10. Klicken Sie auf die Schaltfläche *OK*.

⇒ Die Erfolgsmeldung des Zertifikatsimports erscheint.

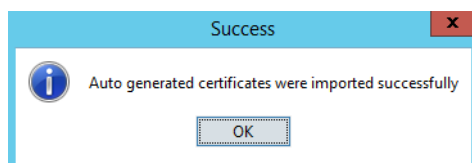


Abb. 12: Erfolgsmeldung über den Zertifikatsimport

11. Klicken Sie auf die Schaltfläche *OK*, um das Fenster zu schließen.
12. Starten Sie den Glassfish-Server neu, damit das Zertifikat übernommen wird.
13. In der Registerkarte *Current Certificate* können Sie das aktuell gültige Zertifikat überprüfen.

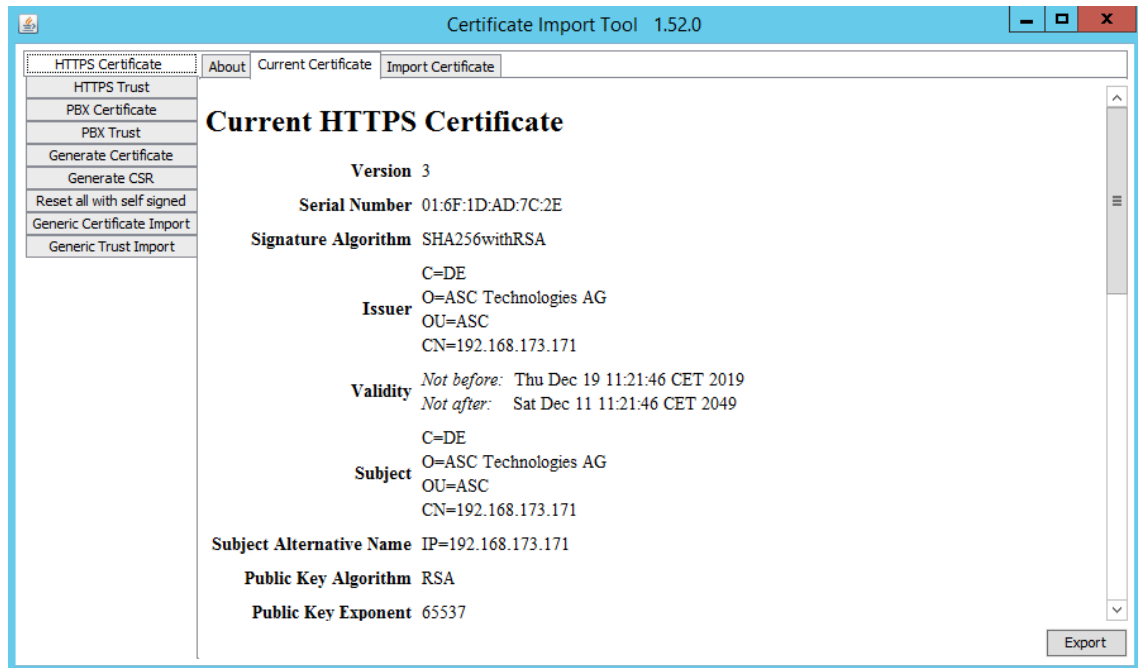


Abb. 13: Aktuell gültiges Zertifikat überprüfen

5.2

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. 14: Certificate Import Tool

Folgende Formate werden unterstützt:

- PKCS12
- X.509/Private key

5.2.1

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.

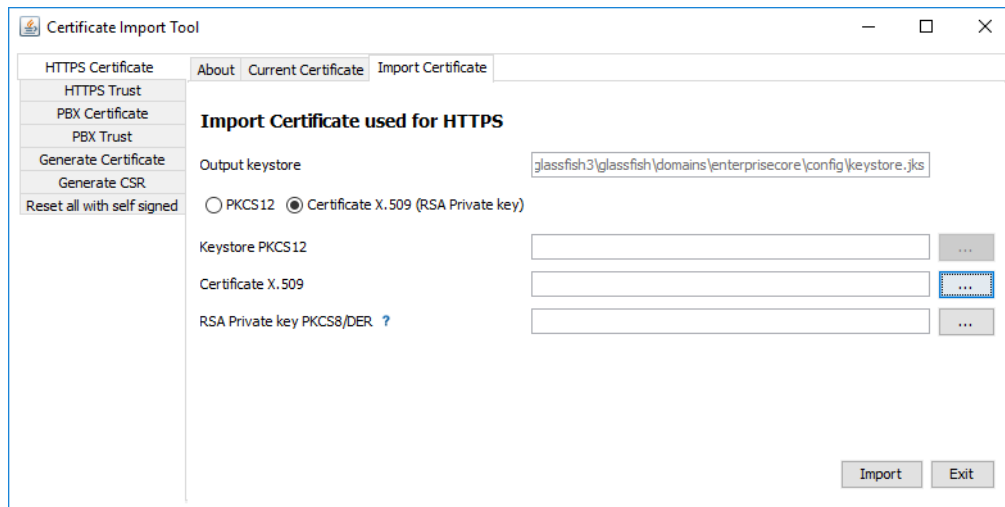


Abb. 15: X.509importieren

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

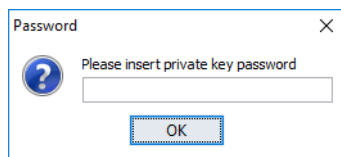


Abb. 16: Passwort für den Private Key eingeben

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.

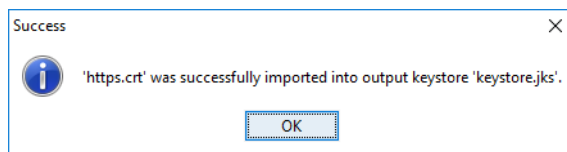


Abb. 17: Meldung - Erfolgreicher Import

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.

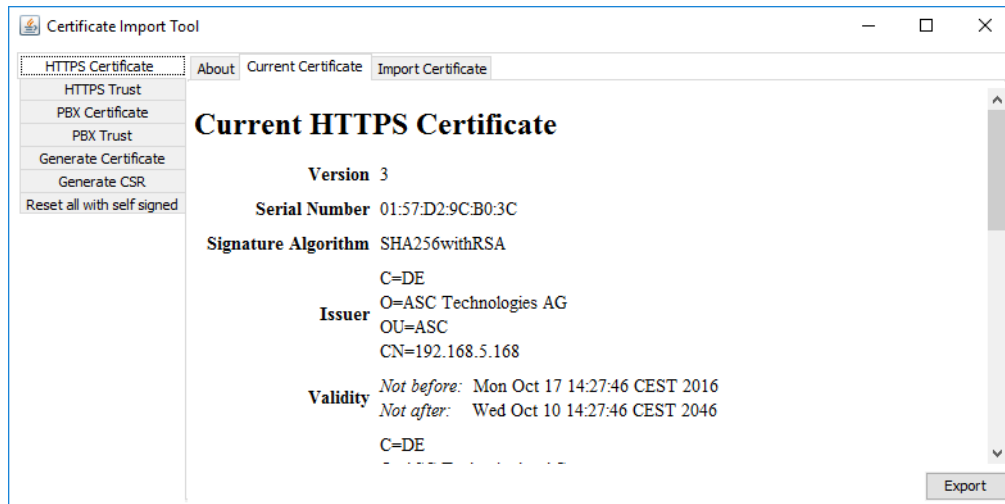


Abb. 18: Aktuell gültiges HTTPS-Zertifikat überprüfen

5.2.2 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.

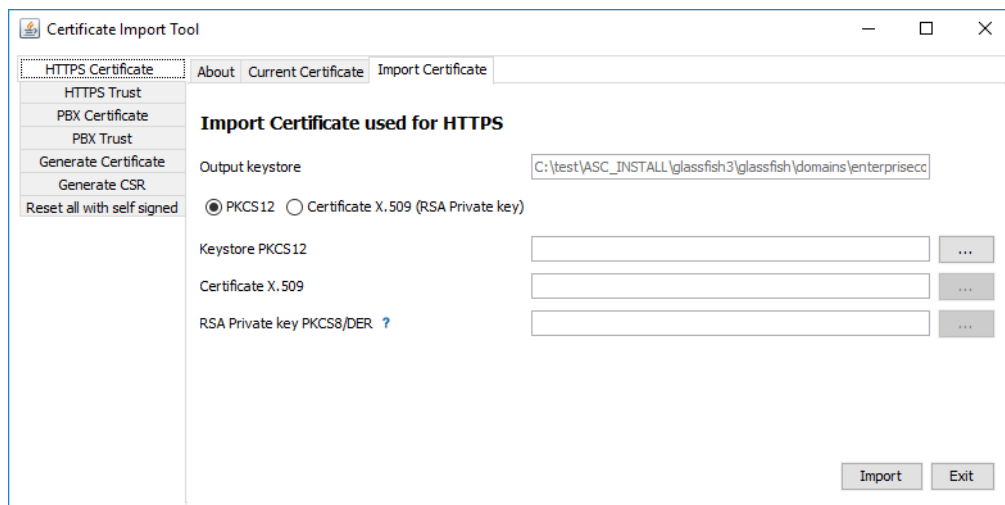


Abb. 19: PKCS12 Keystore importieren

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

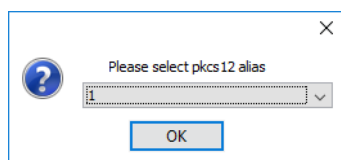


Abb. 20: Alias bestätigen

6. Klicken Sie auf die Schaltfläche *OK*, um den Alias zu bestätigen.
⇒ Das Fenster zur Eingabe des Passworts erscheint.

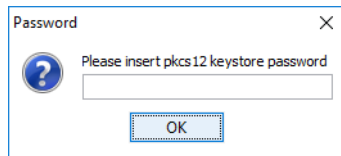


Abb. 21: Passwort für PKCS12 Keystore eingeben

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.

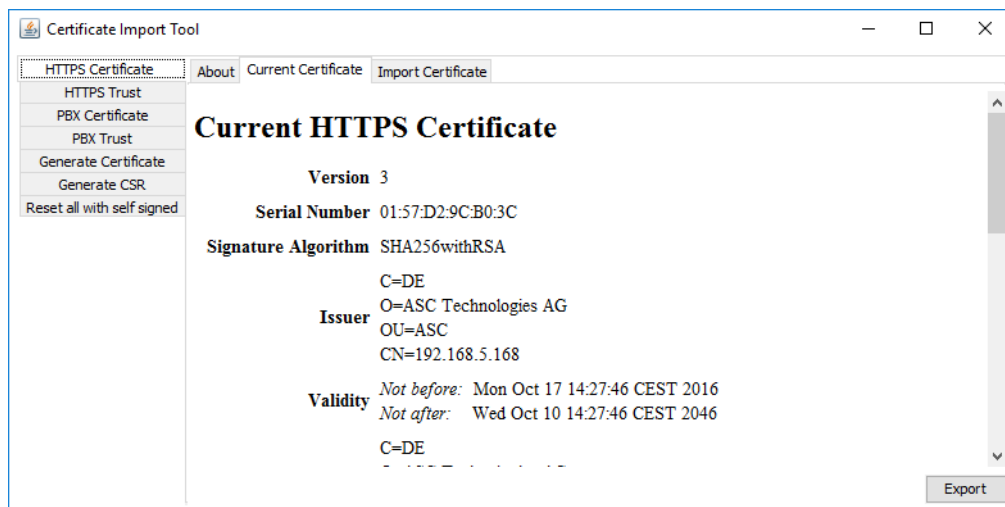


Abb. 22: Aktuell gültiges HTTPS-Zertifikat überprüfen

Abbildungsverzeichnis

Abb. 1	Netzwerk- und Freigabe-Center	6
Abb. 2	Netzwerkverbindungen	6
Abb. 3	Netzwerkverbindung Eigenschaften.....	7
Abb. 4	IP-Adresse konfigurieren.....	7
Abb. 5	Pfad zur Datei Setup.xml	9
Abb. 6	IP-Adressen in Setup.xml ändern	9
Abb. 7	Certificate Import Tool.....	11
Abb. 8	Sicherheitsabfrage	11
Abb. 9	Sicherheitsabfrage	11
Abb. 10	IP-Adresse auswählen.	12
Abb. 11	Gültigkeitsdauer des Zertifikats auswählen.....	12
Abb. 12	Erfolgsmeldung über den Zertifikatsimport	12
Abb. 13	Aktuell gültiges Zertifikat überprüfen.....	13
Abb. 14	Certificate Import Tool.....	13
Abb. 15	X.509importieren.....	14
Abb. 16	Passwort für den Private Key eingeben	14
Abb. 17	Meldung - Erfolgreicher Import.....	14
Abb. 18	Aktuell gültiges HTTPS-Zertifikat überprüfen.....	15
Abb. 19	PKCS12 Keystore importieren	15
Abb. 20	Alias bestätigen.....	15
Abb. 21	Passwort für PKCS12 Keystore eingeben	16
Abb. 22	Aktuell gültiges HTTPS-Zertifikat überprüfen.....	16

Tabellenverzeichnis

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.