

Configuration IP address change



Administration manual for system providers

11/19/2020

Product line neo, version 6.x

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

EVOIPneo

EVOLUTIONneo / XXL / eco

INSPIRATIONneo

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>.

Copyright © 2019 ASC Technologies AG. All rights reserved.

Windows is a registered trademark of Microsoft Corporation. VMware® is a registered trademark of VMware, Inc. All other marks and names mentioned herein may be trademarks of their respective companies.

Contents

| | | |
|----------|---------------------------------------------------------------|-----------|
| 1 | General information | 4 |
| 2 | Introduction | 5 |
| 3 | IP address change in the operating system | 6 |
| 4 | IP address change in the recording software | 8 |
| 5 | Update HTTPS certificate | 10 |
| 5.1 | Update SSL/TLS certificate created and generated by ASC | 10 |
| 5.2 | Import customer-specific HTTPS certificate | 12 |
| 5.2.1 | Import X.509/Private key | 12 |
| 5.2.2 | Import PKCS12 | 13 |
| | List of figures | 16 |
| | List of tables | 17 |
| | Glossary | 18 |

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.

The software programs and the manuals of ASC are protected by copyright law. All rights on the manuals are reserved including the rights of reproduction and multiplication of any kind, be it photo mechanical, typographical or on digital data media. This also applies to translations. Copying the manuals, completely or in parts, is only allowed with written authorization 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

2 Introduction

During the installation of the ASC software, the IP address of the recording server is read automatically. This manual describes the steps which have to be taken when the IP address is supposed to be changed subsequently.



This chapter exclusively refers to the English-language version since ASC only supports the English-language operating system.

1. Press the Windows key.
2. Open the window *Network and Sharing Center* (network connection) via *Control Panel > Network and Internet > Network and Sharing Center*.
3. Click on *Change adapter settings* on the left side.

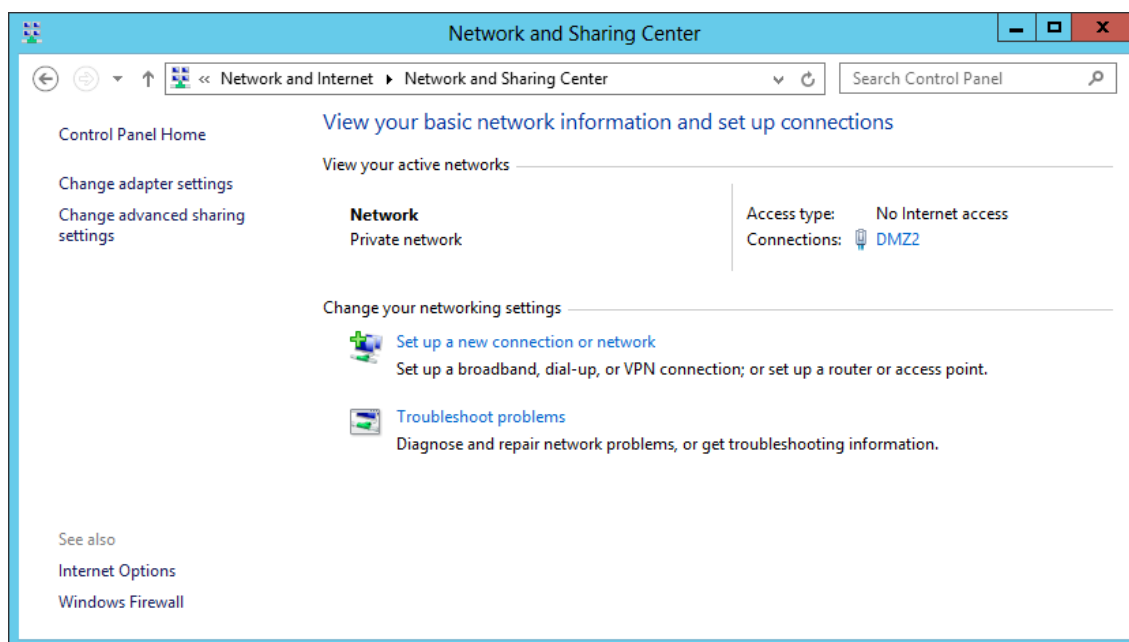


Fig. 1: Network and Sharing Center

4. Click on the inserted card.
5. Open the context menu with a right-click.
6. Select the menu item *Properties*.

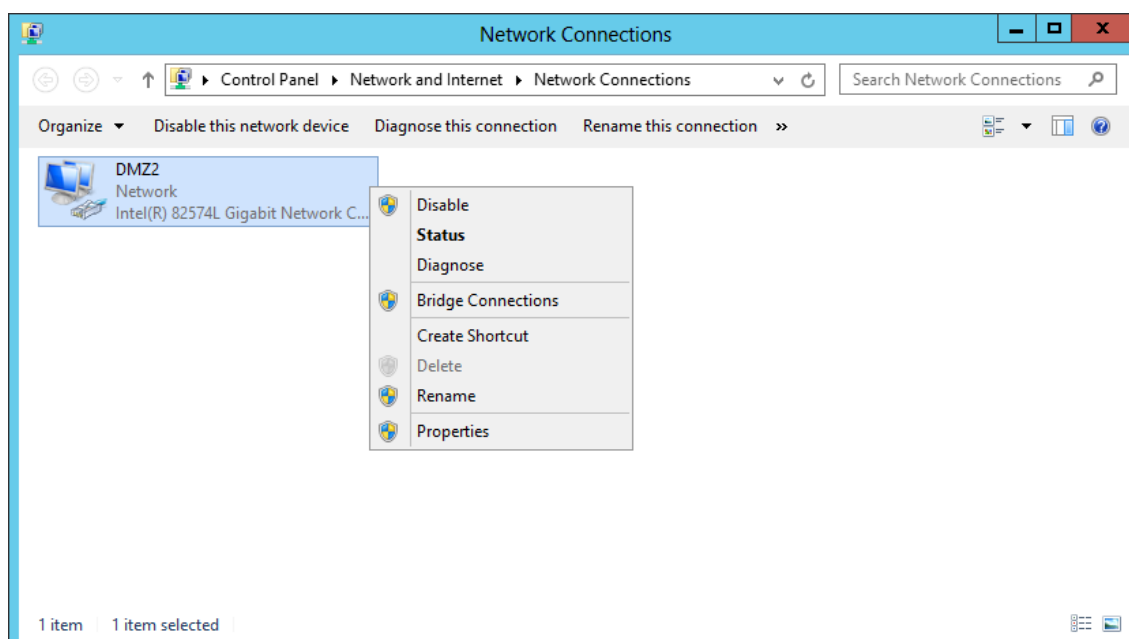


Fig. 2: Network Connections

7. Click on the button *Properties* in the window of the properties.

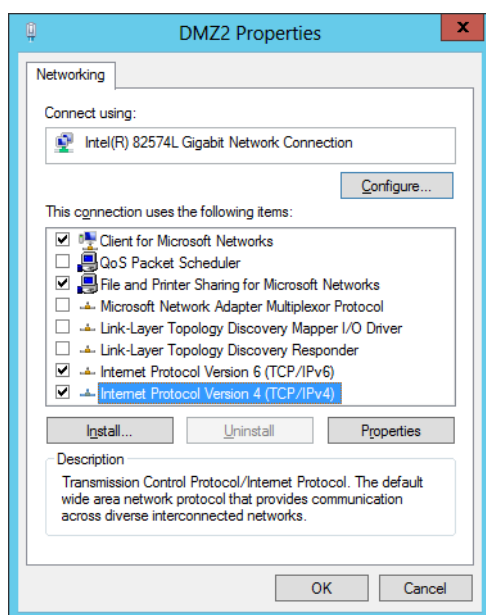


Fig. 3: Network connection properties

8. You have to assign a static IP address for the ASC software. Select the option *Use the following IP address*.

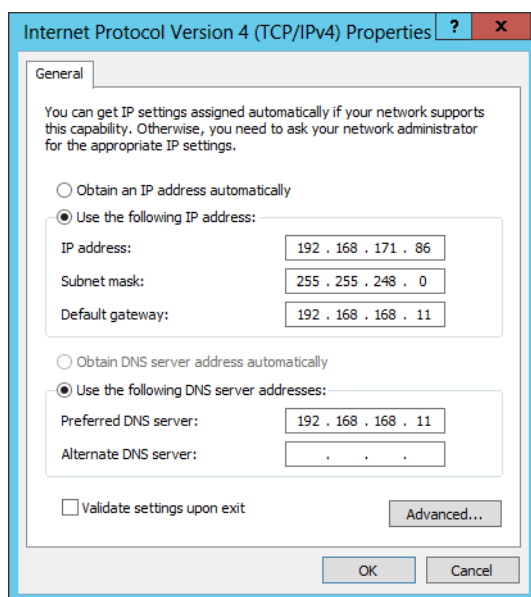


Fig. 4: Configure IP address

9. Enter the IP address, the subnet mask, and the default gateway.
10. Click on the button *OK* to save the settings and to close the window.

4

IP address change in the recording software

Once the IP address has been changed in the operating system, it has to be changed in the recording software, too.

To do so, you have to restart the service *ASC ServiceMan* on the respective servers.

1. Open the window *Services* via *Start > Administrative Tools > Services*.
2. Restart the service *ASC ServiceMan*.
3. Go to the application System Configuration to verify that the respective IP address for the communication has been selected in the Servers module.
4. If you have to re-configure the IP address in the Servers module, change to the Integrations module and deactivate the integration which is used.
5. Change to the Recording Architectures module and deactivate the recording architecture.
6. The option to configure the respective IP address becomes active in the Servers module.
7. Configure the respective IP address.
8. Activate the recording architecture in the Recording Architectures module again.
9. Activate the integration in the Integrations module again.
10. Subsequently verify that the recording works properly.

Additional steps for multi-server systems

If you have changed the IP address of one or of several [app servers](#) in a multi-server system, you have to inform all servers without [app server](#) components about the new IP addresses.

You have to make this change manually via the Windows Explorer in the configuration file *setup.xml*.

1. Open the Windows Explorer to access the configuration file *setup.xml*.
2. Change to the directory *C:\Program Files (x86)\ASC\ASC Product Suite\Updater\config*.

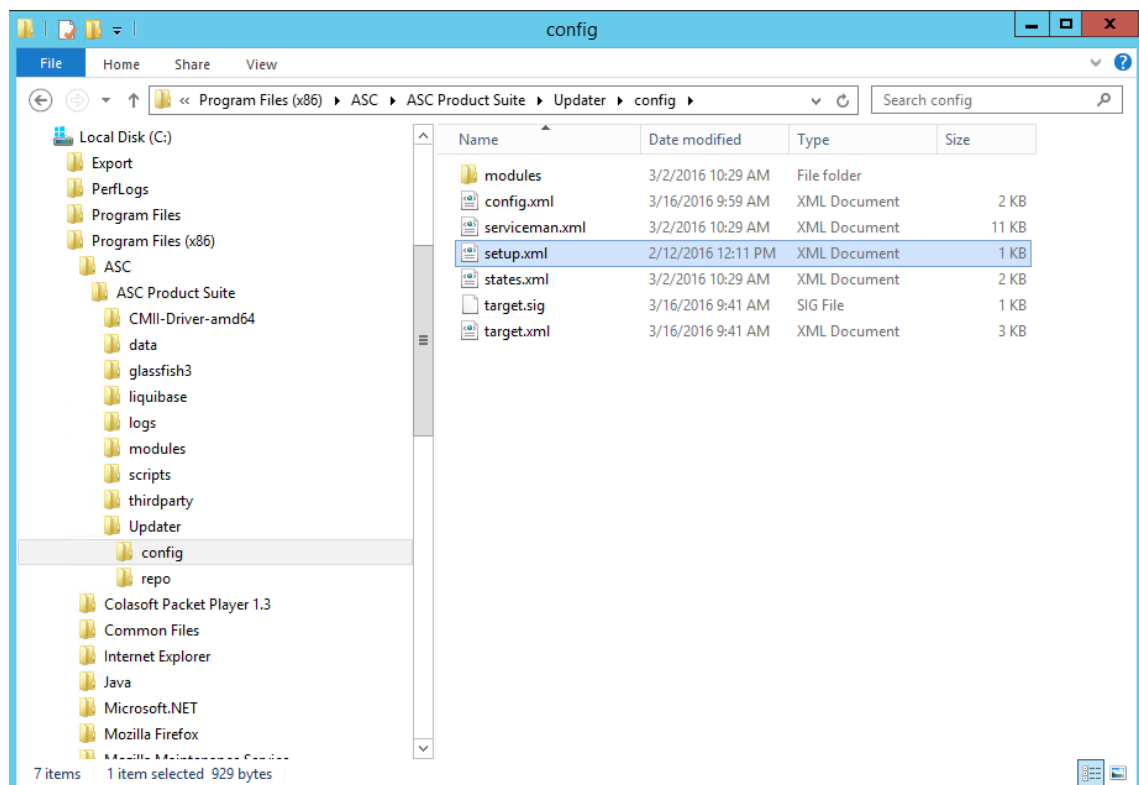
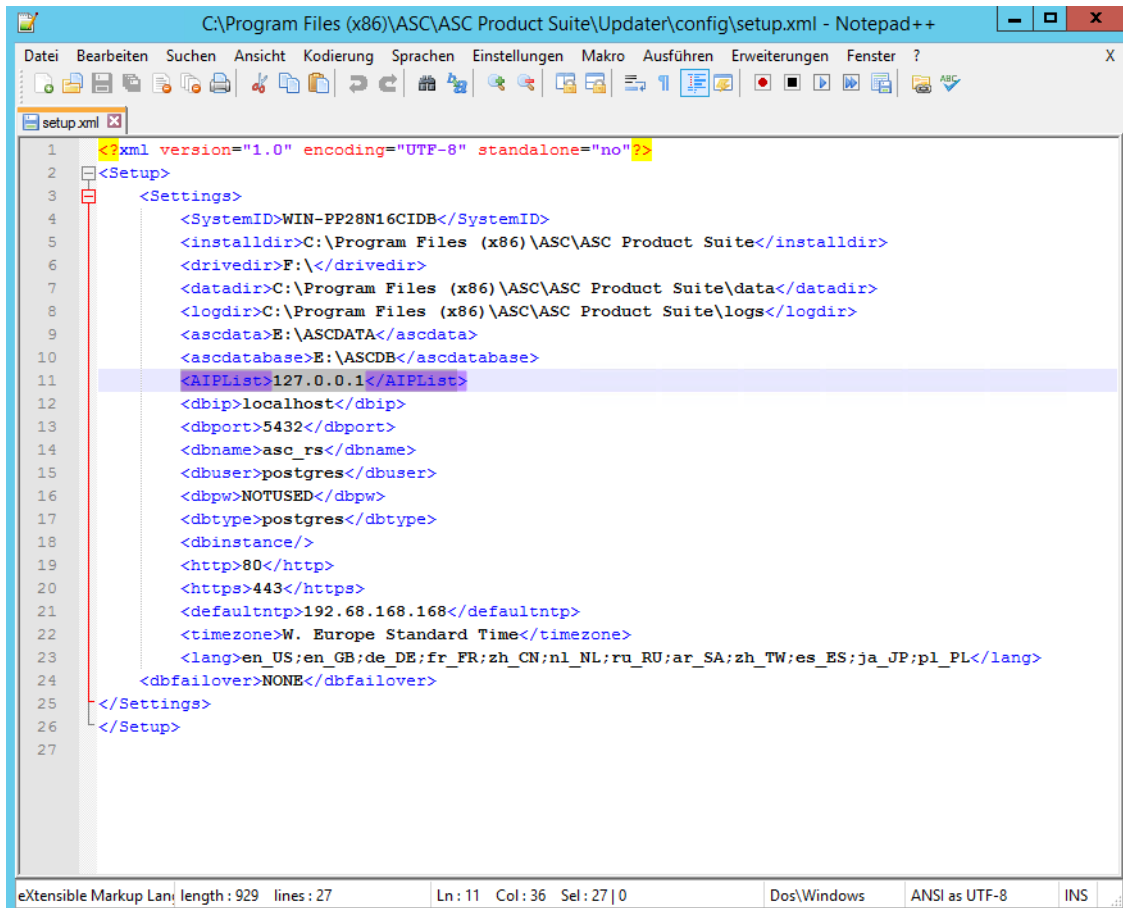


Fig. 5: Path to the file Setup.xml

3. Open the file *setup.xml* in an editor such as Notepad to edit it.



```

1  <?xml version="1.0" encoding="UTF-8" standalone="no"?>
2  <Setup>
3    <Settings>
4      <SystemID>WIN-PP28N16CIBD</SystemID>
5      <installdir>C:\Program Files (x86)\ASC\ASC Product Suite</installdir>
6      <drivedir>F:\</drivedir>
7      <datadir>C:\Program Files (x86)\ASC\ASC Product Suite\data</datadir>
8      <logdir>C:\Program Files (x86)\ASC\ASC Product Suite\logs</logdir>
9      <ascdata>E:\ASCDATA</ascdata>
10     <ascdatabase>E:\ASCDDB</ascdatabase>
11     <AIPList>127.0.0.1</AIPList>
12     <dbip>localhost</dbip>
13     <dbport>5432</dbport>
14     <dbname>asc_rs</dbname>
15     <dbuser>postgres</dbuser>
16     <dbpw>NOTUSED</dbpw>
17     <dbtype>postgres</dbtype>
18     <dbinstance/>
19     <http>80</http>
20     <https>443</https>
21     <defaultntp>192.68.168.168</defaultntp>
22     <timezone>W. Europe Standard Time</timezone>
23     <lang>en_US;en_GB;de_DE;fr_FR;zh_CN;nl_NL;ru_RU;ar_SA;zh_TW;es_ES;ja_JP;pl_PL</lang>
24     <dbfailover>NONE</dbfailover>
25   </Settings>
26 </Setup>
27

```

Fig. 6: Change IP addresses in Setup.xml

4. Enter the new IP address of the application server in the line `<AIPList>127.0.0.1</AIPList>`. If you use several servers, enter the respective IP addresses separated by semicolons.
5. Save the file `setup.xml`.
6. To apply the changes, you have to restart all ASC services.
7. Open the window *Services* via *Start > Administrative Tools > Services*.
8. Restart all ASC services. Alternatively, you can restart the server.

5 Update HTTPS certificate

5.1 Update SSL/TLS certificate created and generated by ASC

ASC provides a certificate which has to be updated when the IP address changes. You can carry out the update via 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. From the context menu of the file *certimporter.exe*, select the menu item *Run as Administrator*.
⇒ The window Certificate Import Tool appears.



Fig. 7: Certificate Import Tool

4. Click on the button *Reset all with self signed* to create a certificate with the current IP address or the host name and to import the automatically generated certificate.
⇒ The following notification appears:

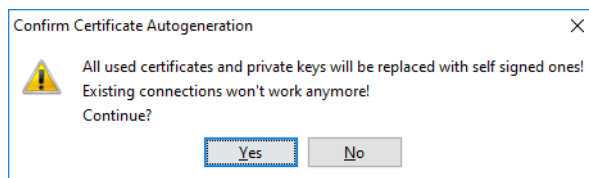


Fig. 8: Security Prompt

5. Click on the button *Yes* to replace the currently used certificates and private keys.
⇒ Another security prompt appears to cancel the action if required since the existing connection will not e working afterwards.

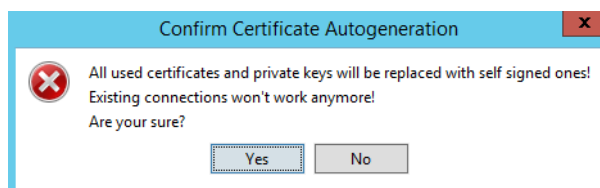


Fig. 9: Security Prompt

6. Click on the button *Yes* to overwrite the currently used certificates and private keys. Click on the button *No* to keep the currently used certificates and private keys.
⇒ If you have confirmed the security prompt, the following window appears:

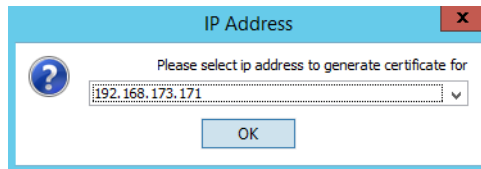


Fig. 10: Select IP address.

7. From the drop-down list, either select the IP address or the host name for which the automatically generated certificate is supposed to be created.
8. Click on the button OK.
 - ⇒ The following window to configure the validity of the certificate appears.



Fig. 11: Select validity of the certificate

9. From the drop-down list, select the number of years that the certificate is supposed to be valid.
10. Click on the button OK.
 - ⇒ A message informing you that the certificate has been imported successfully appears.

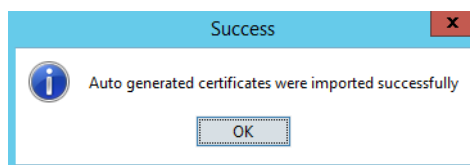


Fig. 12: Message about the successful import of the certificate

11. Click on the button OK to close the window.
12. Restart the Glassfish server so that the certificate will be applied.
13. In the tab *Current Certificate*, you can view the currently valid certificate.

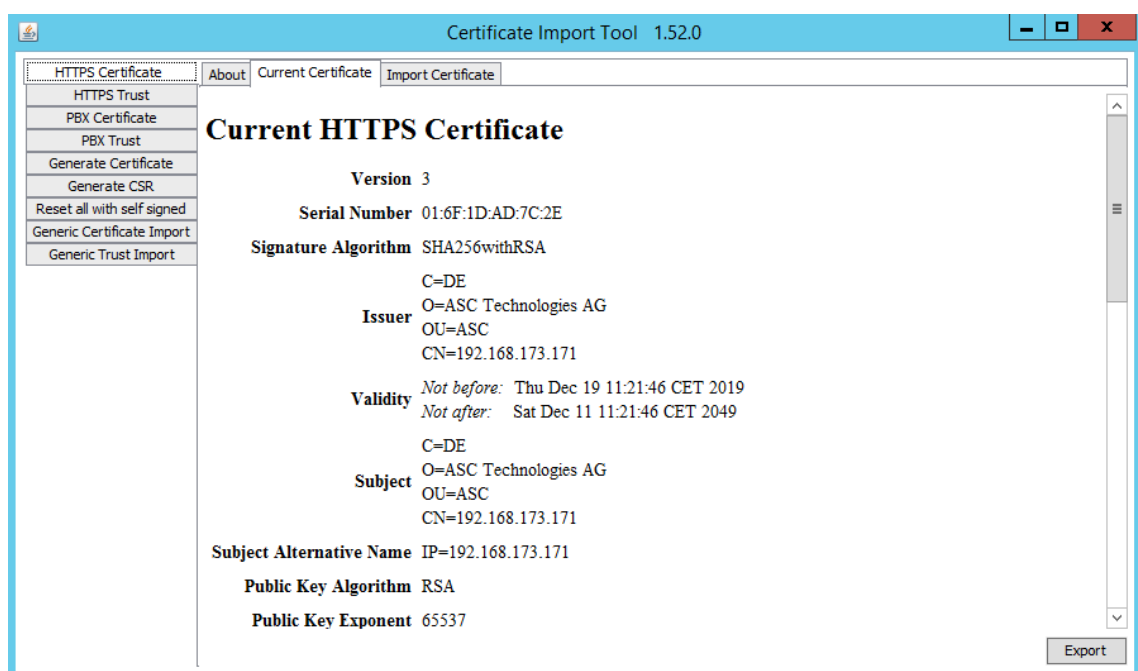


Fig. 13: Check currently valid certificate

5.2 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.

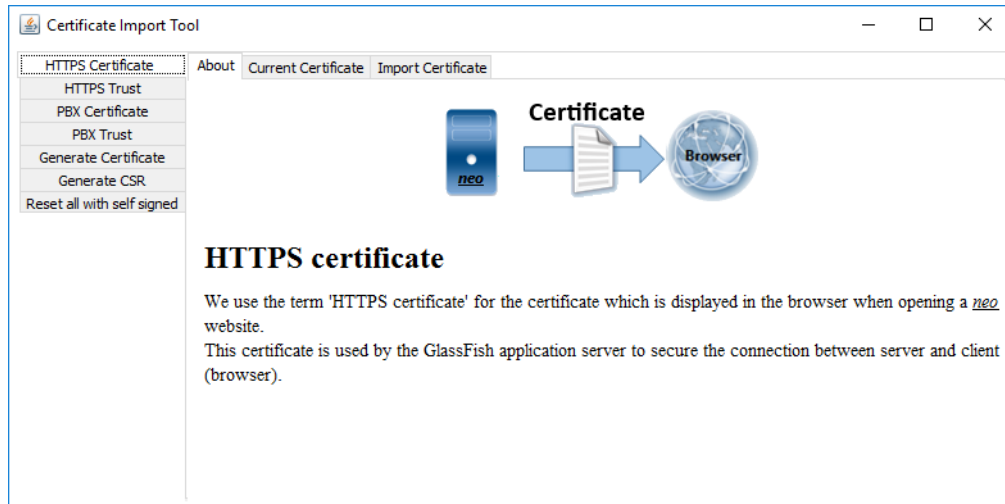


Fig. 14: Certificate Import Tool

The following formats are supported:

- PKCS12
- X.509/Private key

5.2.1 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.

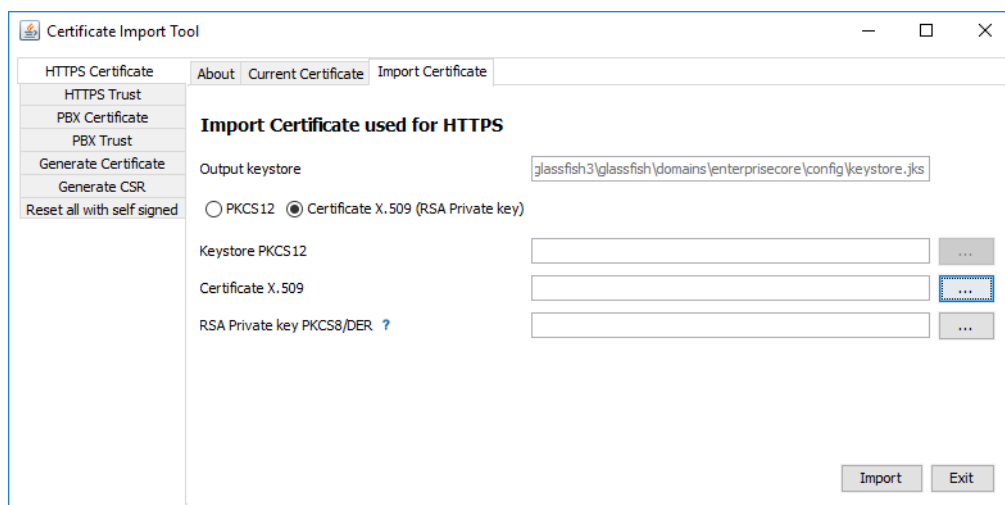


Fig. 15: Import X.509

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

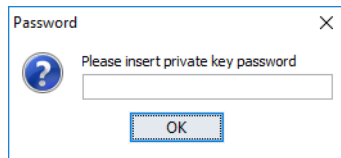


Fig. 16: Enter password for the private key

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.

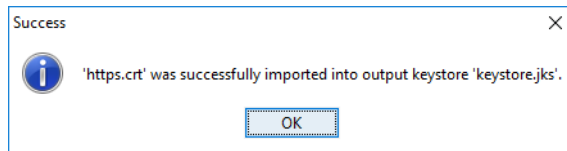


Fig. 17: Message - Successful import

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.

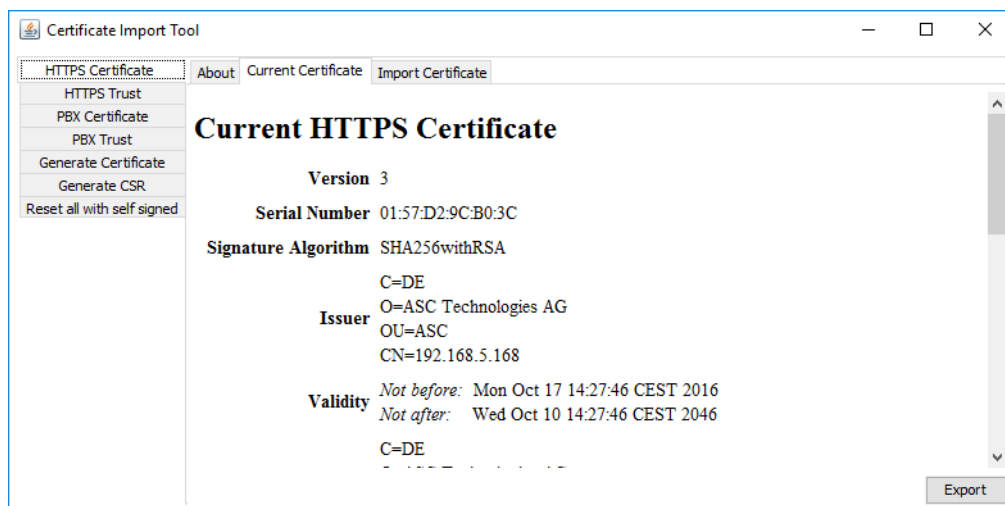


Fig. 18: Check currently valid HTTPS certificate

5.2.2 Import PKCS12

1. Select the menu item *HTTPS Certificate* in the navigation bar.
2. Click on the tab *Import Certificate*.
3. If your 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.

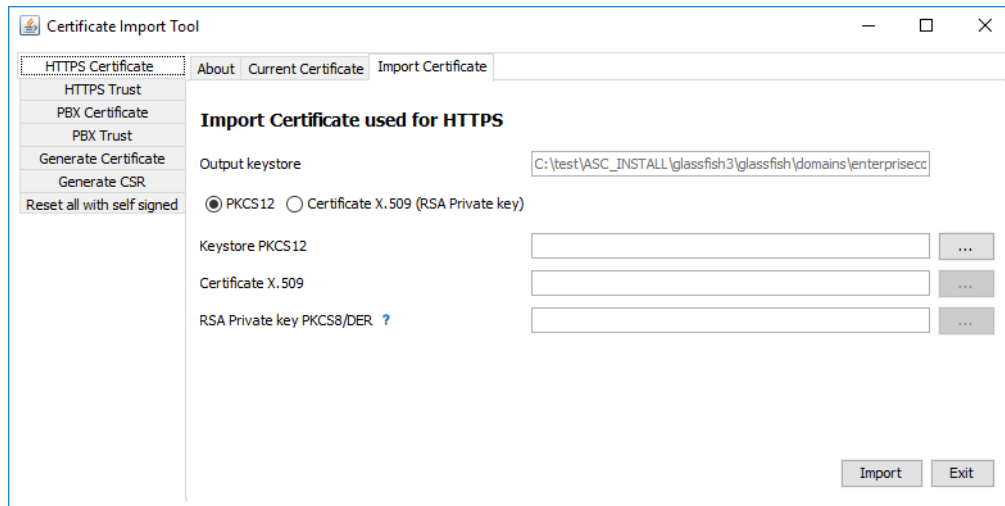


Fig. 19: Import PKCS12 Keystore

5. Click on the button *Import*.

⇒ The window to enter the alias for the PKCS12 Keystore appears.

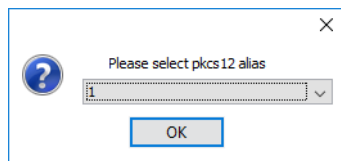


Fig. 20: Confirm alias

6. Click on the button *OK* to confirm the alias.

⇒ The window to enter the password appears.

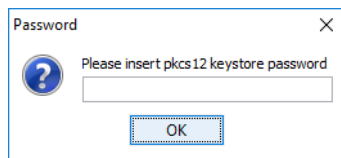


Fig. 21: Enter password for PKCS12 Keystore

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.

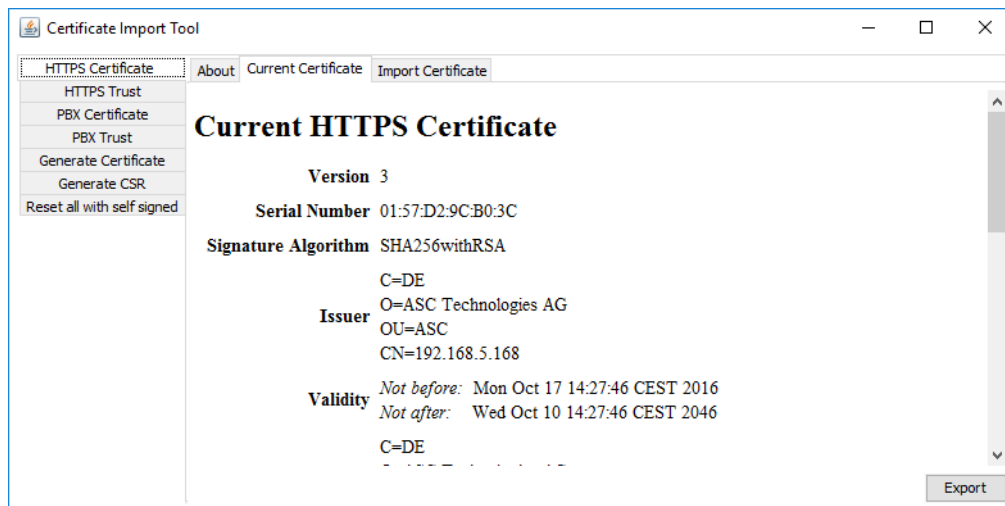


Fig. 22: Check currently valid HTTPS certificate

List of figures

| | | |
|---------|--------------------------------------------------------------|----|
| Fig. 1 | Network and Sharing Center | 6 |
| Fig. 2 | Network Connections | 6 |
| Fig. 3 | Network connection properties | 7 |
| Fig. 4 | Configure IP address | 7 |
| Fig. 5 | Path to the file Setup.xml | 8 |
| Fig. 6 | Change IP addresses in Setup.xml | 9 |
| Fig. 7 | Certificate Import Tool | 10 |
| Fig. 8 | Security Prompt | 10 |
| Fig. 9 | Security Prompt | 10 |
| Fig. 10 | Select IP address. | 11 |
| Fig. 11 | Select validity of the certificate | 11 |
| Fig. 12 | Message about the successful import of the certificate | 11 |
| Fig. 13 | Check currently valid certificate | 11 |
| Fig. 14 | Certificate Import Tool | 12 |
| Fig. 15 | Import X.509 | 12 |
| Fig. 16 | Enter password for the private key | 13 |
| Fig. 17 | Message - Successful import | 13 |
| Fig. 18 | Check currently valid HTTPS certificate | 13 |
| Fig. 19 | Import PKCS12 Keystore | 14 |
| Fig. 20 | Confirm alias | 14 |
| Fig. 21 | Enter password for PKCS12 Keystore | 14 |
| Fig. 22 | Check currently valid HTTPS certificate | 15 |

List of tables

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.