

Configuration browser



Installation manual for system providers and tenants

11/13/2019

Product line neo, version 6.x

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

EVOIPneo

EVOLUTIONneo / XXL / eco

EVOflex (country-specific)

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	Configuration Internet Explorer version 11	6
3.1	Configure pop-up blocker	6
3.2	Add security exception	7
3.3	Configure security exception for POWERplay Web	9
3.4	Configure Single Sign On.....	13
3.5	Configure compatibility view.....	14
3.5.1	Internet Explorer version 11	15
4	Configuration Microsoft Edge.....	16
4.1	Install certificate	16
4.2	Configure security exception for POWERplay Web	18
5	Configuration Mozilla Firefox.....	21
5.1	Configure security exception for POWERplay Web	21
5.2	Configure Single Sign On.....	23
5.3	Mozilla Firefox default	23
5.3.1	Configure pop-up blocker	23
5.3.2	Add security exception	25
5.4	Mozilla Firefox ESR.....	26
5.4.1	Configure pop-up blocker	26
5.4.2	Add security exception	28
6	Configuration Google Chrome.....	30
7	Quick guide.....	31
7.1	Configuration Internet Explorer version 11.....	31
7.2	Configuration Microsoft Edge.....	31
7.3	Configuration Mozilla Firefox.....	32
	Glossary	36

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

This document describes the configuration of the browsers for the ASC software.



Make sure that JavaScript has been activated.



Make sure that cookies have been allowed.


3

Configuration Internet Explorer version 11

1. Start the browser to carry out the configurations described below.

3.1

Configure pop-up blocker

1. Click on the icon  (*Extras*).
2. Click on the menu item *Internet options*.
3. Click on the tab *Privacy*.

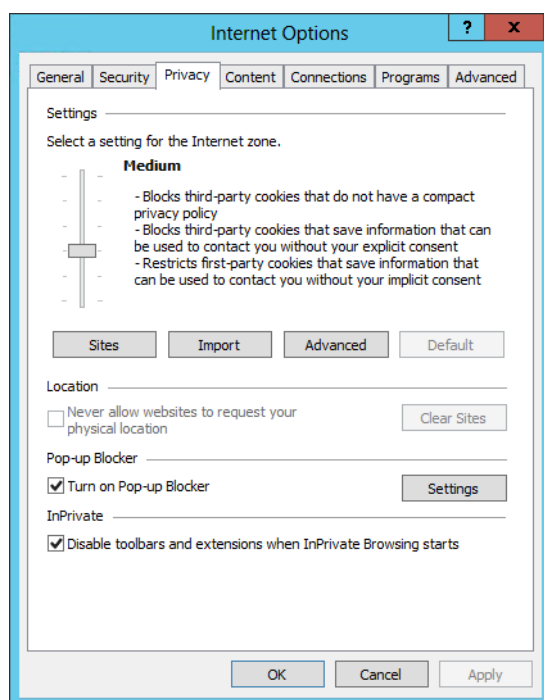


Fig. 1: Tab Privacy

4. Click on the button *Settings*.
5. In the entry field *Address of website to allow*, enter the [URL](#) of the [APP Server](#).

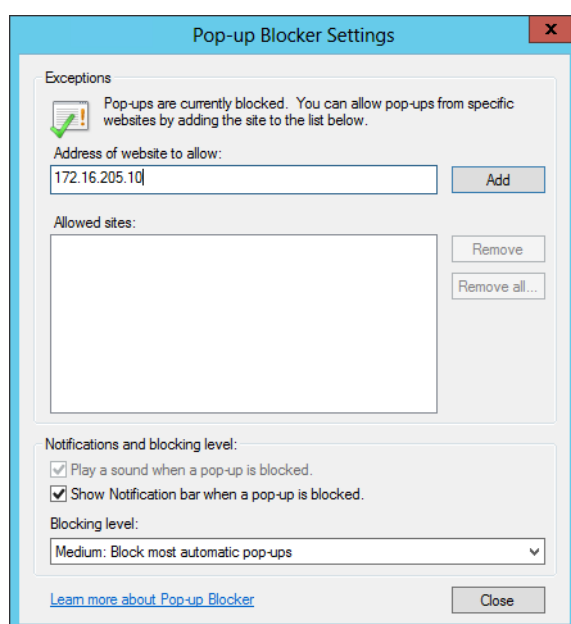


Fig. 2: Pop-up Blocker Settings (example)

6. Click on the button *Add*.

⇒ The website is added in the field *Allowed sites*.

7. Click on the button *Close*.
8. Click on the button *OK*.

3.2 Add security exception

The following steps are only required if the *neo* server certificate has not been classified as trusted yet.

1. Enter the [URL](#) of the [app server](#) in the address bar.
2. Click on *Continue to this website (not recommended)*

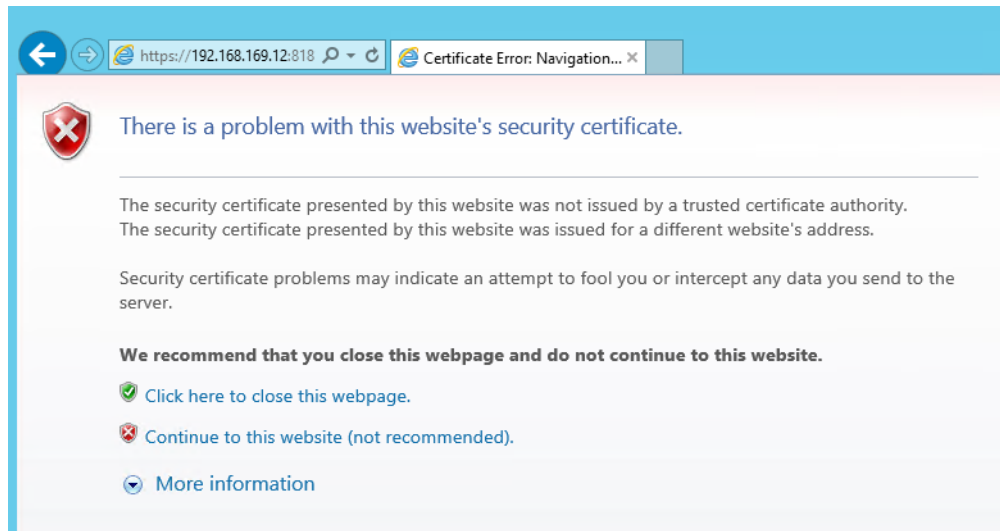


Fig. 3: Continue to this website

3. If a certificate error is displayed, click on the red field *Certificate Error* in the header and proceed with the following steps.
 4. Click on *View certificates*.
- ⇒ The following window appears:

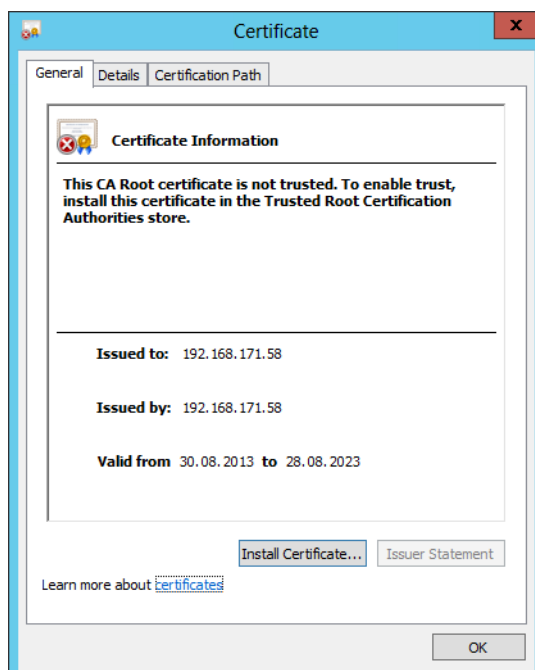


Fig. 4: Certificate

5. Click on the tab *General*.
6. Click on the button *Install Certificate*.
7. Click on the button *Next* to start the Certificate Import Wizard.

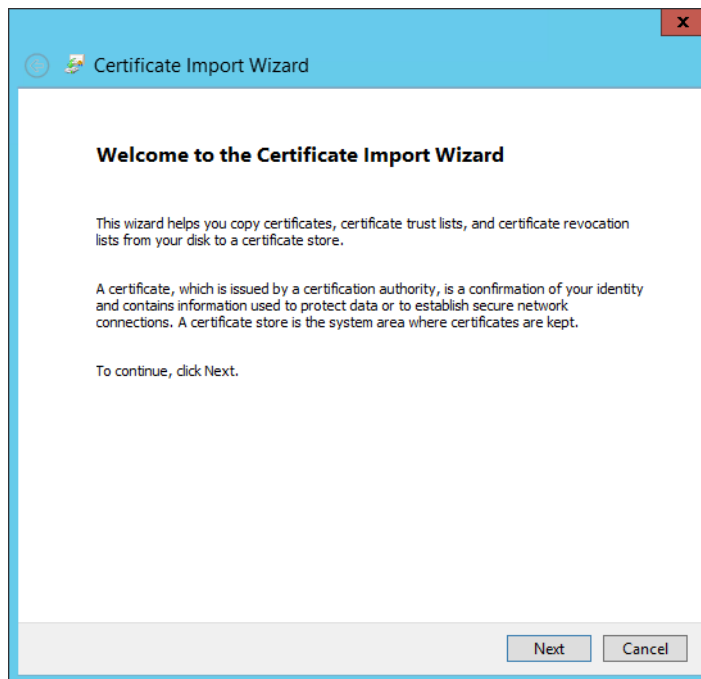


Fig. 5: Certificate Import Wizard

8. If the certificate is supposed to be valid only for the current user of the client computer, select the option *Current user* as storage location.
If the certificate is supposed to be valid for all users of the client computer, select the option *Local computer* as storage location.
9. Click on the button *Next*.
10. Activate the option *Place all certificates in the following store*.
11. Click on the button *Browse*.
12. Click on the directory *Trusted Root Certification Authorities*.

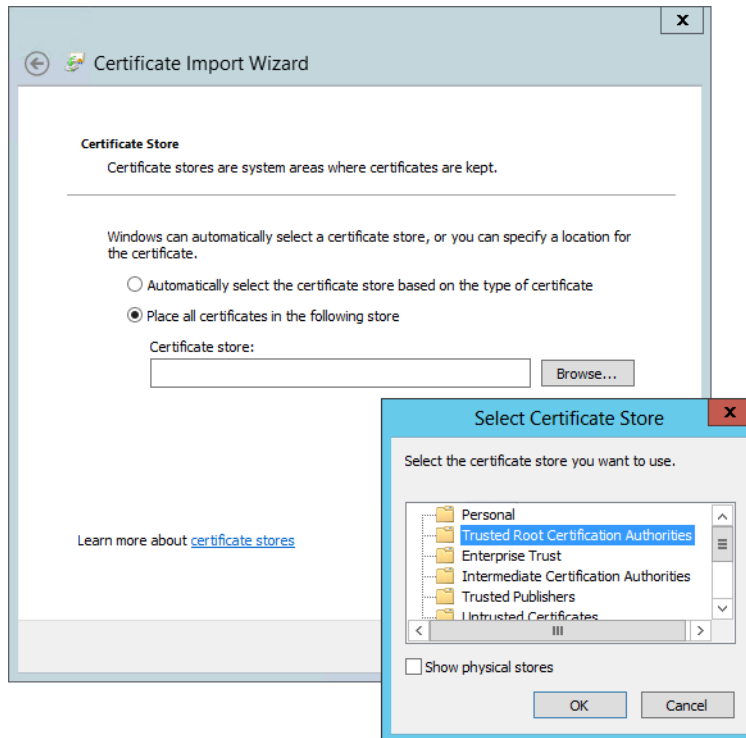


Fig. 6: Select certificate store

13. Click on the button *OK*.
14. Click on the button *Next*.
15. Click on the button *Finish*.

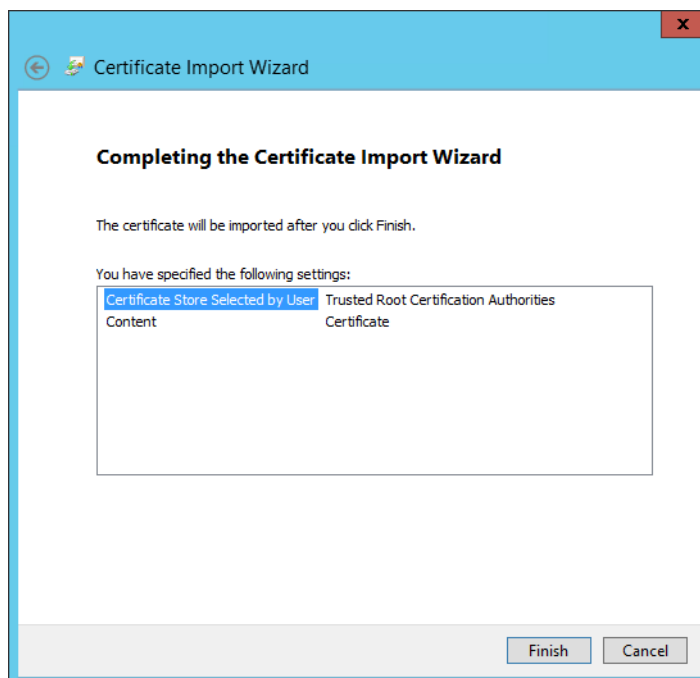


Fig. 7: Certificate Import Wizard

16. Confirm the security prompt.

3.3 Configure security exception for POWERplay Web

1. Enter the following URL into the address bar:
`https://<System-IP>/POWERplayWeb/`
2. In the [URL](#), replace the parameter <System-IP> with the IP address of the [app server](#).

3. Press the [Enter] key.
⇒ The login screen appears.
4. Log in to the application with your user name and password.
⇒ The application opens.
The following window appears:

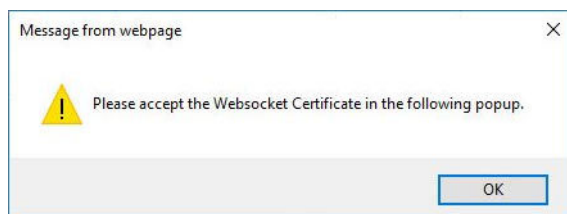


Fig. 8: Accept Websocket certificate

5. Click on the button **OK**.
6. Click on *Continue to this website (not recommended)*

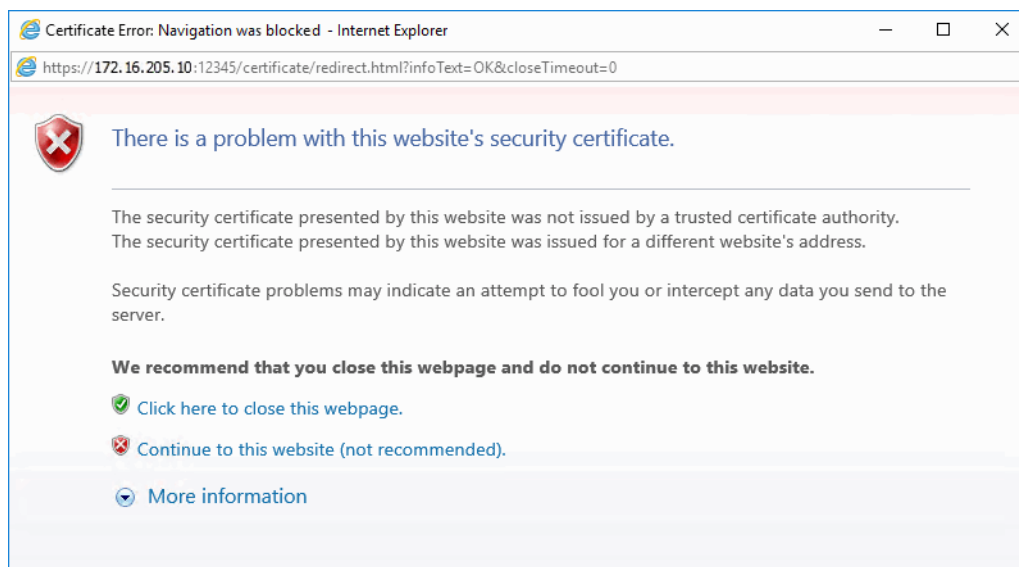


Fig. 9: Continue to this website

7. If a certificate error is displayed, click on the red field *Certificate Error* in the header and proceed with the following steps.
8. Click on *View certificates*.
⇒ The following window appears:

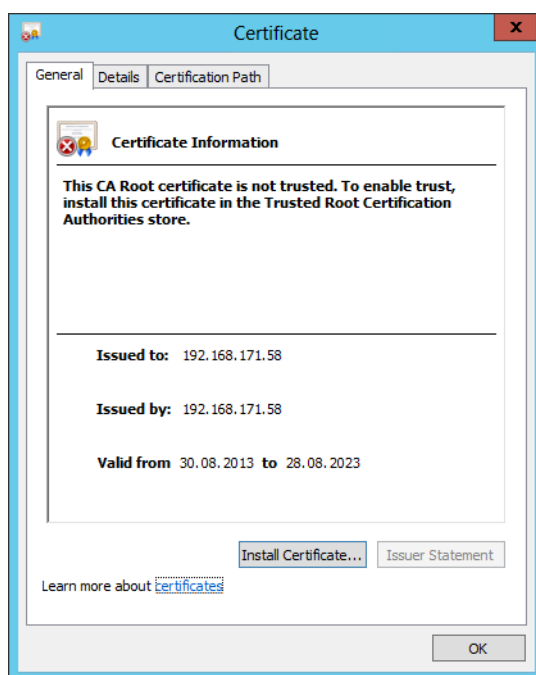


Fig. 10: Certificate

9. Click on the tab *General*.
10. Click on the button *Install Certificate*.
11. Click on the button *Next* to start the Certificate Import Wizard.

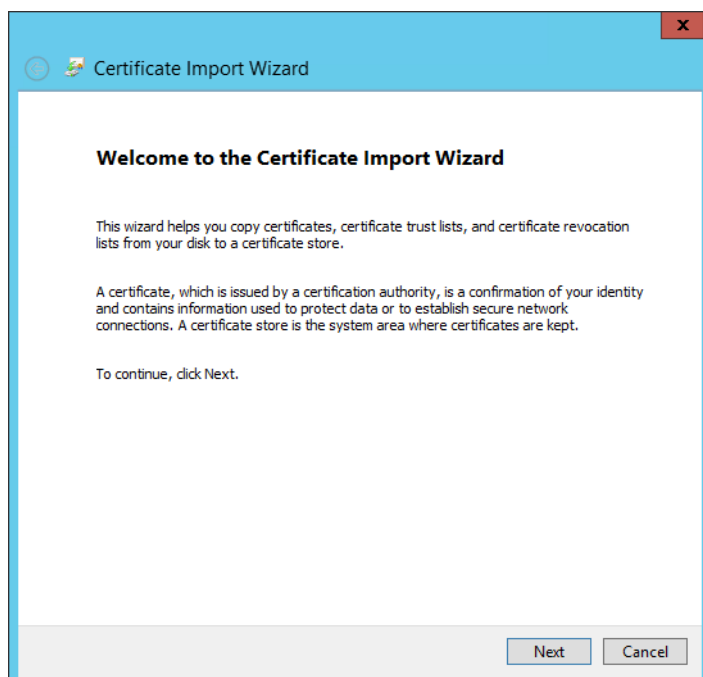


Fig. 11: Certificate Import Wizard

12. If the certificate is supposed to be valid only for the current user of the client computer, select the option *Current user* as storage location.
If the certificate is supposed to be valid for all users of the client computer, select the option *Local computer* as storage location.
13. Click on the button *Next*.
14. Activate the option *Place all certificates in the following store*.
15. Click on the button *Browse*.

16. Click on the directory *Trusted Root Certification Authorities*.

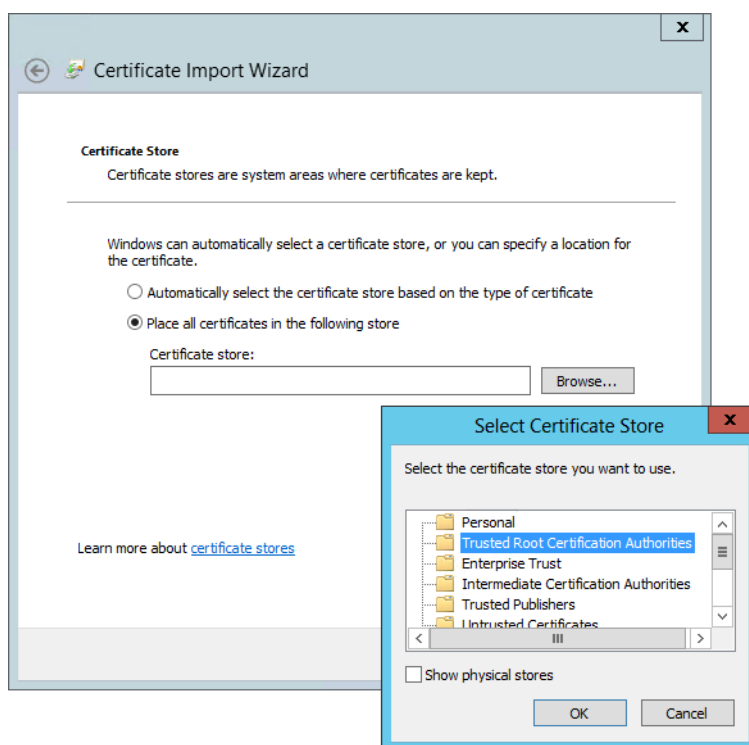


Fig. 12: Select certificate store

17. Click on the button *OK*.
18. Click on the button *Next*.
19. Click on the button *Finish*.

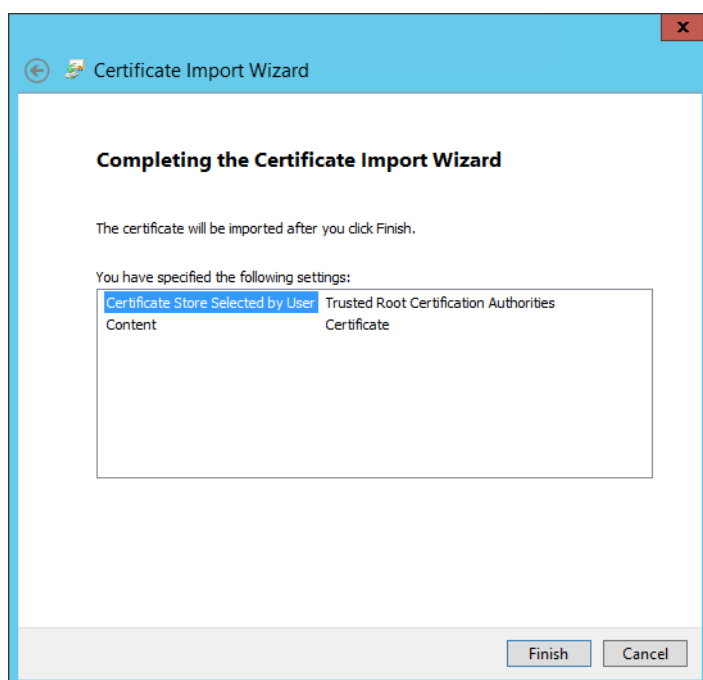



Fig. 13: Certificate Import Wizard


20. Confirm the security prompt.
21. Click on the icon  (*Logoff*) to close the application.

3.4 Configure Single Sign On



Make sure that the **URL** of the **app server** has been added to the trusted sites (see Set up a trusted site).

Single Sign On (**SSO**) only works in one domain for all web applications. For this reason, all computers have to be included in one corresponding Windows domain.

1. Click on the icon  (*Extras*).
2. Click on the menu item *Internet options*.
3. Click on the tab *Advanced*.

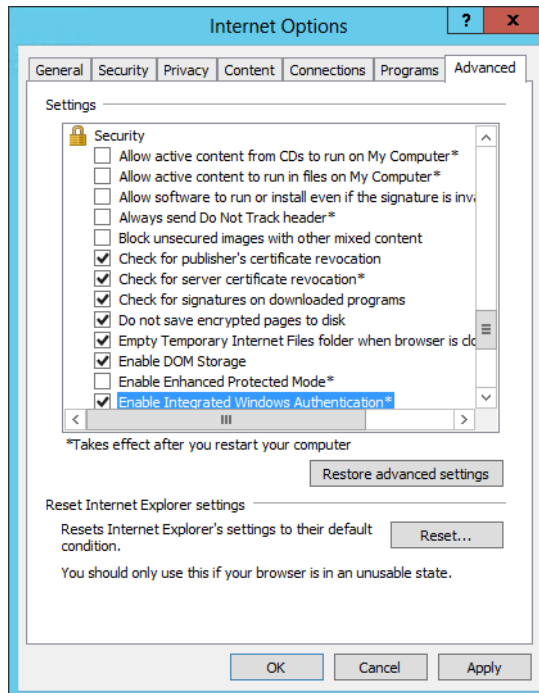


Fig. 14: Tab Advanced

4. Activate the option *Enable Integrated Windows Authentication** under Security.
 - ☒ = Option has been activated.
 - ☐ = Option has been deactivated.
5. Click on the tab *Security*.

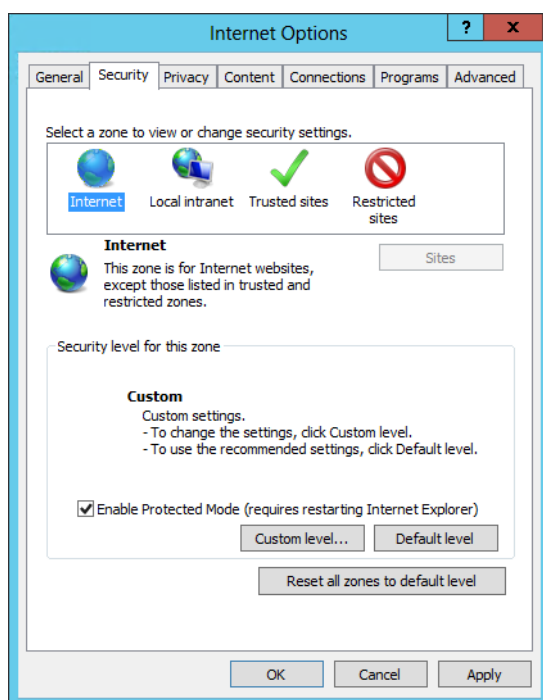


Fig. 15: Tab Security

6. Click on the icon *Internet*.
7. Click on the button *Custom level*.
8. Under *User Authentication > Logon*, select the options *Automatic logon with current user name and password*.

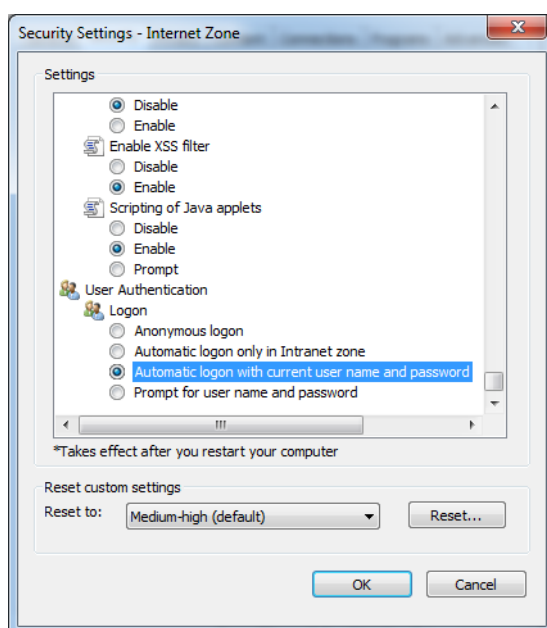



Fig. 16: Security Settings - Internet Zone

9. Click on the button *OK*.
10. Click on the button *OK*.

3.5 Configure compatibility view

To guarantee the functions on the websites of the ASC software, the compatibility mode in the Internet Explorer must be deactivated.

3.5.1 Internet Explorer version 11

1. Click on the icon  (*Extras*).
2. Click on the menu item *Compatibility View settings*.

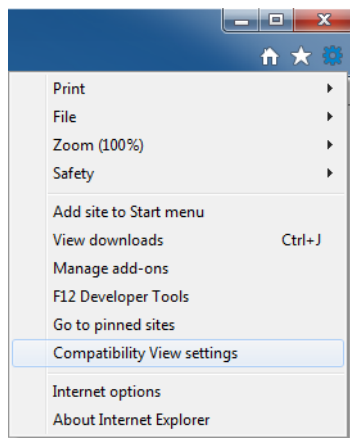


Fig. 17: Internet Explorer > Compatibility View Settings

3. Make sure that the compatibility mode for the [app server](#) has been deactivated.
In the field *Websites you've added to Compatibility View*, the [URL](#) of the [app server](#) may not be listed.
4. If the [URL](#) of the [app server](#) is included in the field *Websites you've added to Compatibility View*, click on the [URL](#) of the [app server](#).
Click on the button *Remove*.
5. Deactivate the option *Display intranet sites in Compatibility View*.
6. Deactivate the option *Use Microsoft Compatibility Lists*.

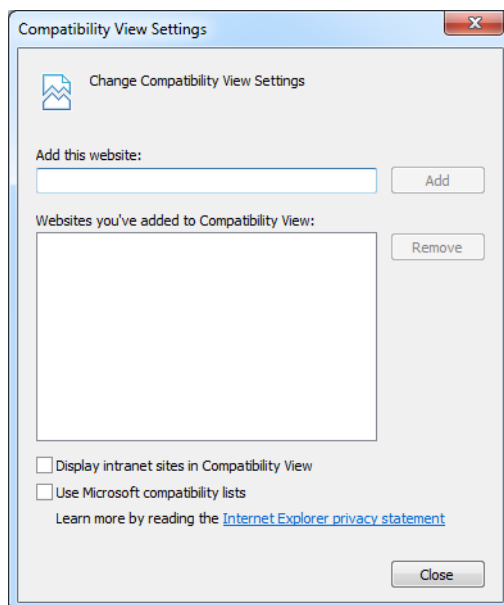


Fig. 18: Compatibility View settings (example)

7. Click on the button *Close*.

4 Configuration Microsoft Edge

4.1 Install certificate

The Browser Microsoft Edge does not offer any possibility to install a certificate. To install a certificate for the client computer nonetheless, use one of the following 2 options:

- Install certificate with the browser Internet Explorer
- Copy certificate to the client computer from the [app server](#) and install it

Install certificate with the browser Internet Explorer

1. Start the browser Internet Explorer.
2. Install the certificate. See chapter [chapter "Add security exception"](#), p. 7.

Copy certificate to the client computer from the [app server](#) and install it

1. Copy the file `C:\Program Files (x86)\ASC\ASC Product Suite\data\crypto\https.crt` from the [app server](#) to the desktop of the client computer.
2. On the desktop of the client computer, right-click on the file `https.crt`.
⇒ The following context menu appears:

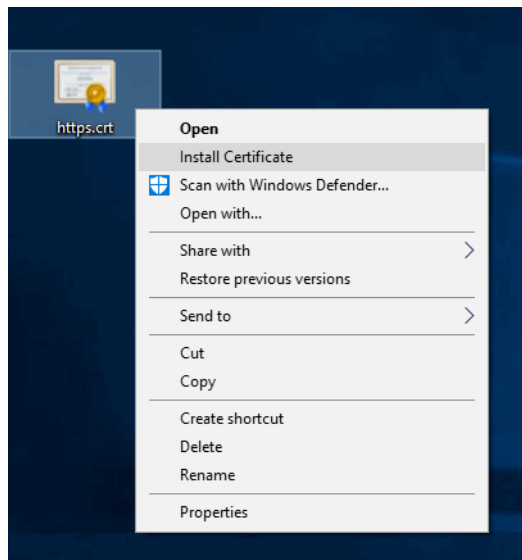


Fig. 19: Install certificate

3. In the context menu, click on the menu item *Install Certificate*.
4. Click on the button *Next*.

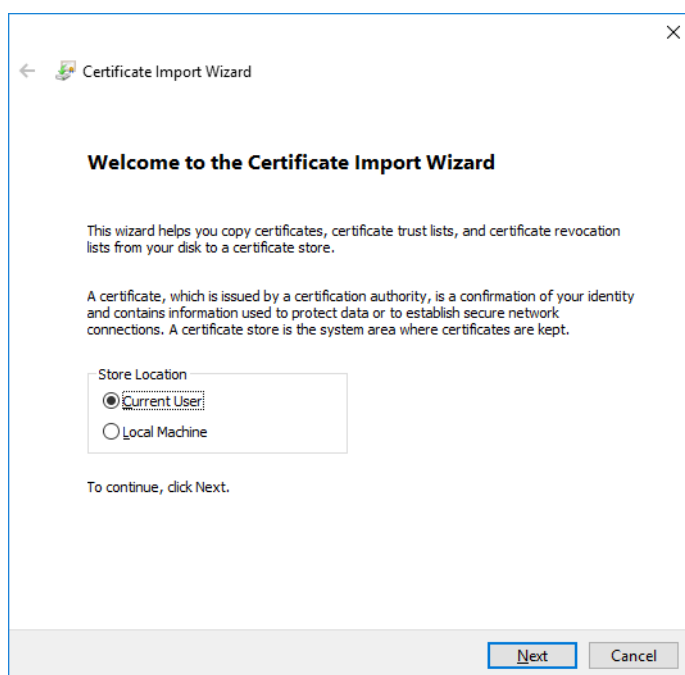


Fig. 20: Certificate Import Wizard

5. If the certificate is supposed to be valid only for the current user of the client computer, select the option *Current user* as storage location.
If the certificate is supposed to be valid for all users of the client computer, select the option *Local computer* as storage location.
6. Click on the button *Next*.
7. Activate the option *Place all certificates in the following store*.
8. Click on the button *Browse*.
9. Click on the directory *Trusted Root Certification Authorities*.

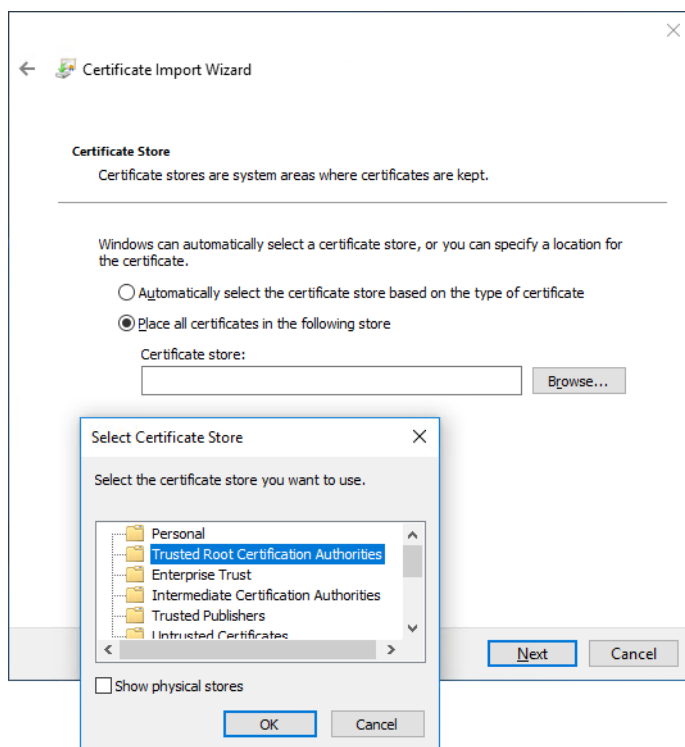


Fig. 21: Select certificate store

10. Click on the button *OK*.

11. Click on the button *Next*.
12. Click on the button *Finish*.

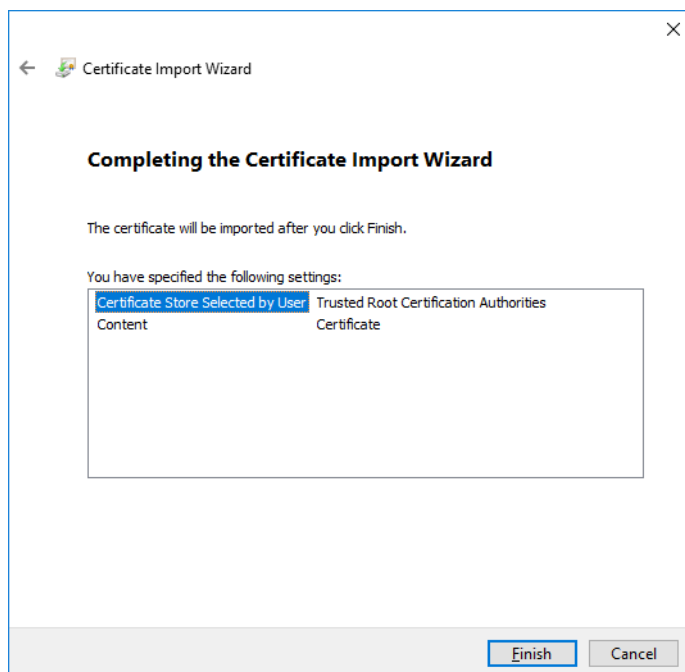


Fig. 22: Certificate Import Wizard

13. Click on the button *Yes*.

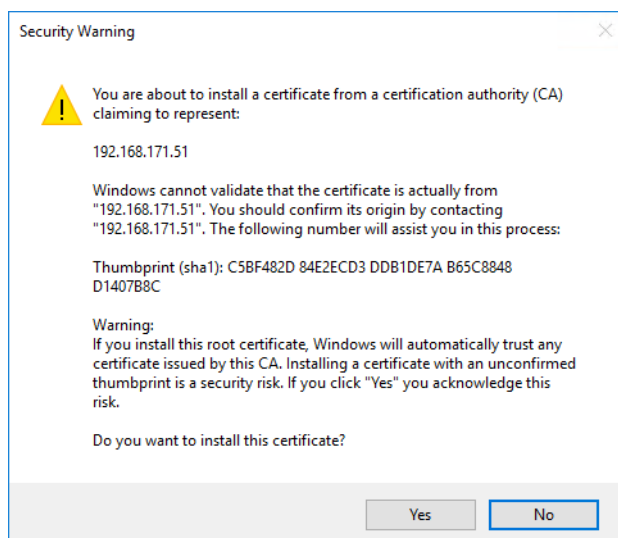


Fig. 23: Security warning

14. Click on the button *OK*.

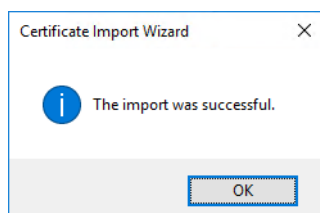


Fig. 24: Certificate Import Wizard

4.2 Configure security exception for POWERplay Web

1. Start the browser.

2. Enter the following URL into the address bar:
`https://<System-IP>/POWERplayWeb/`
3. In the URL, replace the parameter <System-IP> with the IP address of the [app server](#).
4. Press the [Enter] key.
 - ⇒ The login screen appears.
5. Log in to the application with your user name and password.
 - ⇒ The application opens.
 The following window appears:

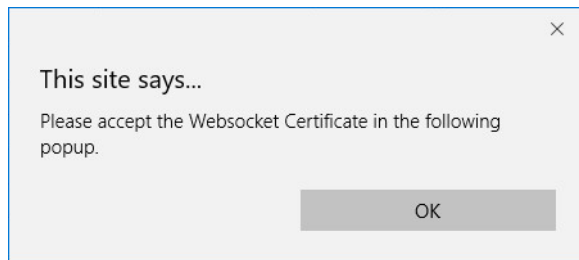


Fig. 25: Accept Websocket certificate

6. Click on the button **OK**.
 - ⇒ The welcome screen of the application appears.

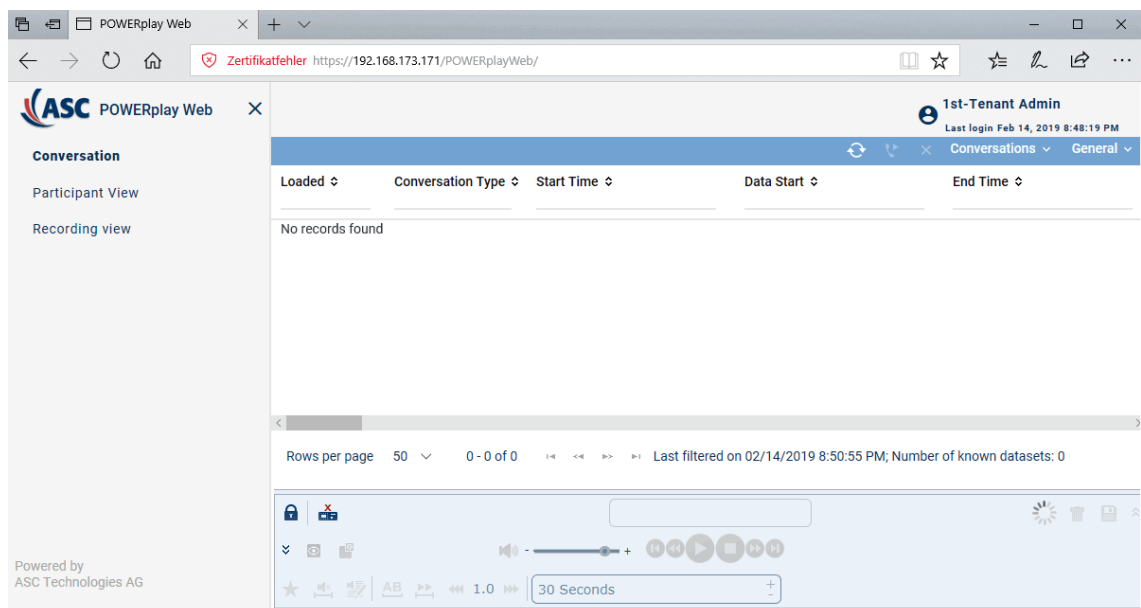


Fig. 26: Welcome screen

7. In the pop-up window *Microsoft Edge blocked a pop-up from ...* at the bottom of the main view, click on the button *Always allow*.
8. Click on *Details*.

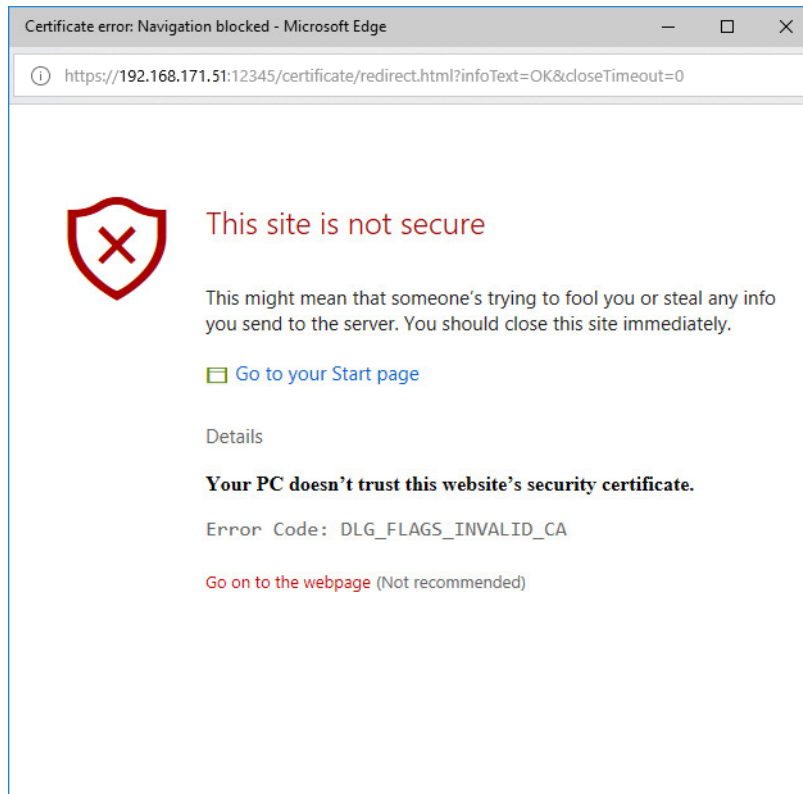



Fig. 27: Continue to this website

9. Click on *Go on to webpage (Not recommended)*.
10. The server connection is refreshed automatically after a few seconds. Once the server connection has been established, the icon  is displayed in the Replay module.

5

Configuration Mozilla Firefox



ASC recommends using the browser Mozilla Firefox ESR.

1. Start the browser to carry out the configurations described below.

5.1

Configure security exception for POWERplay Web

1. Enter the following URL into the address bar:
`https://<System-IP>/POWERplayWeb/`
2. In the [URL](#), replace the parameter `<System-IP>` with the IP address of the [app server](#).
3. Press the [Enter] key.
⇒ The login screen appears.
4. Log in to the application with your user name and password.
⇒ The application opens.
The following window appears:



Fig. 28: Accept Websocket certificate

5. Click on the button *OK*.
6. Click on the button *Advanced*.

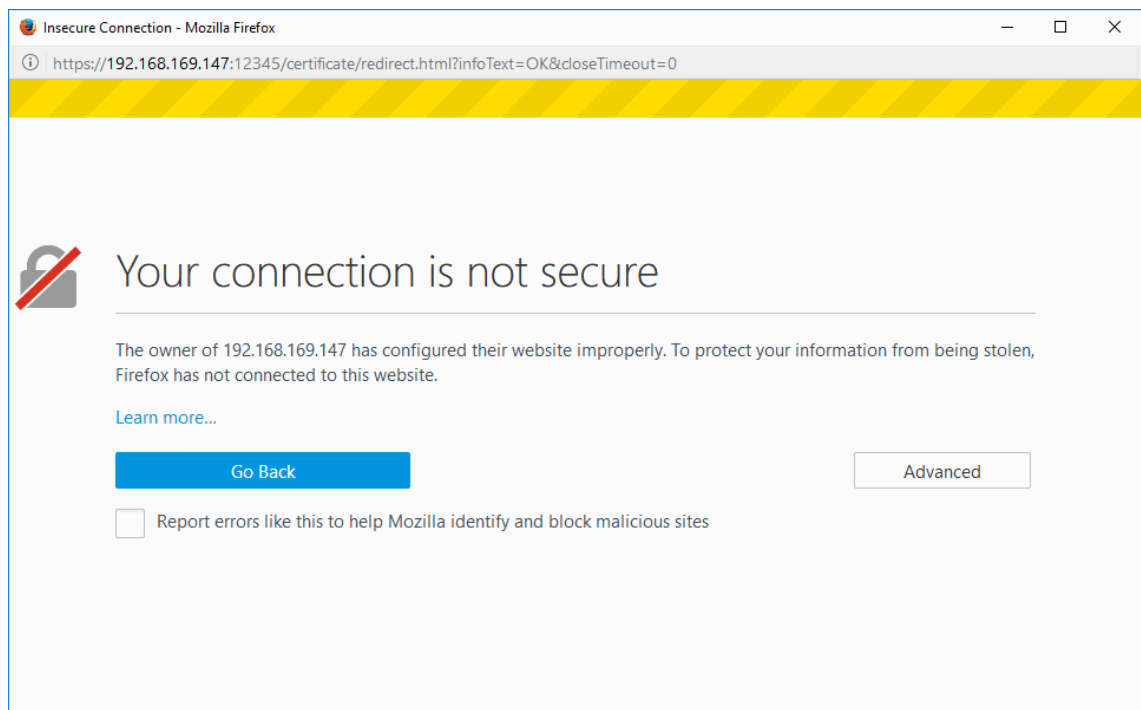


Fig. 29: No secure connection

7. Click on the button *Add Exception*.

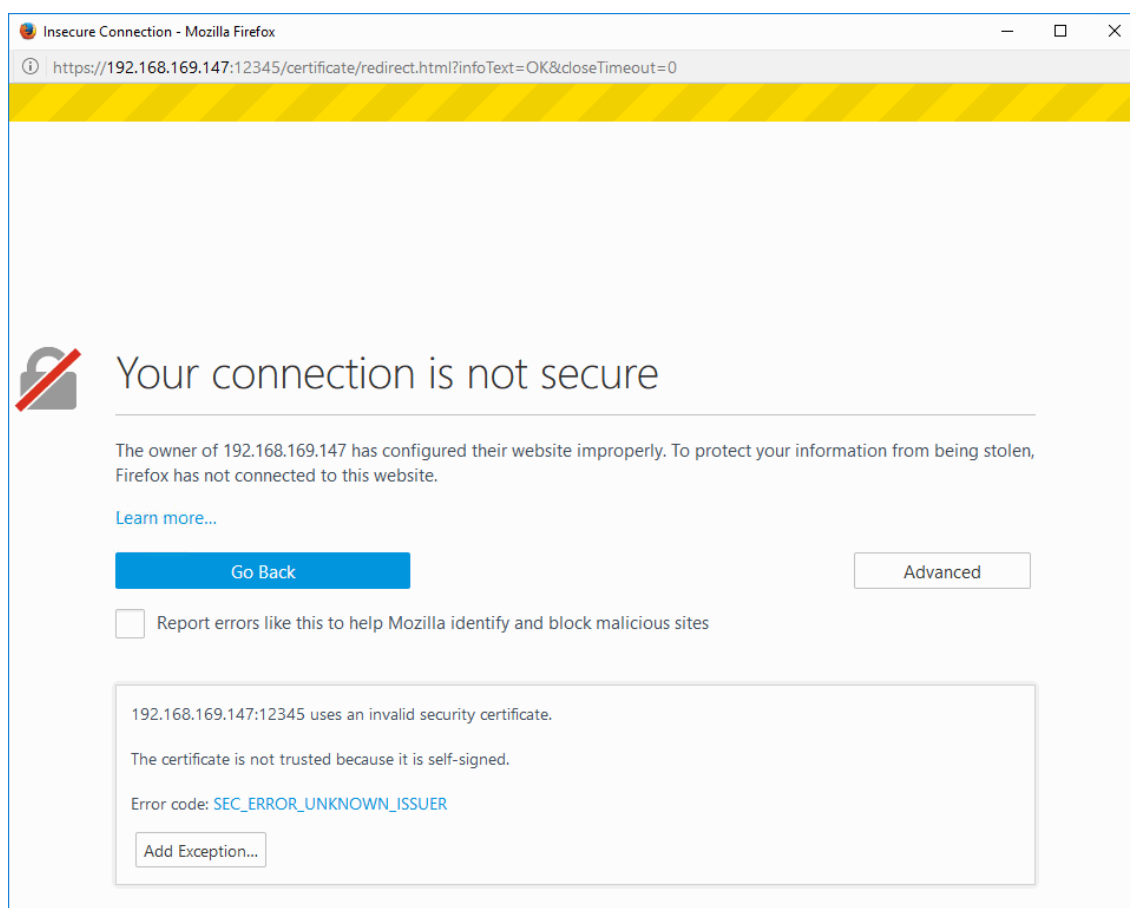


Fig. 30: No secure connection

8. Click on the button *Confirm Security Exception*.

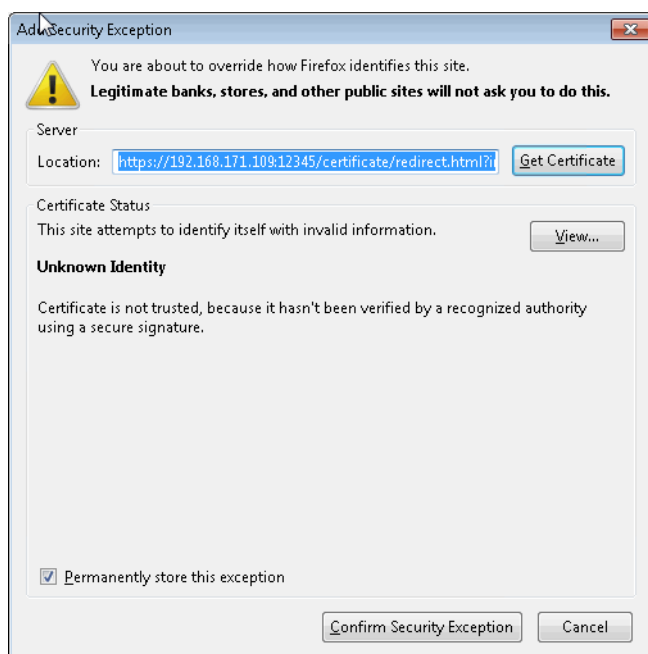


Fig. 31: Confirm security exception

9. Click on the icon  (*Logoff*) to close the application.

5.2 Configure Single Sign On

Single Sign On ([SSO](#)) only works in one domain for all web applications. For this reason, all computers have to be included in one corresponding Windows domain.

1. Enter the [URL](#) *about:config* and confirm it by pressing the [Enter] key.
2. Confirm the security prompt.
3. In the entry field *Search*, enter the value *network.negotiate-auth.trusted-uris*.

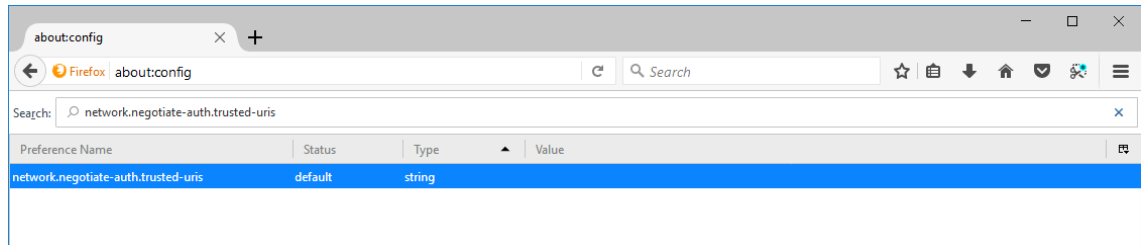


Fig. 32: about:config > network.negotiate-auth.trusted-uris

4. Double-click on the entry *network.negotiate-auth.trusted-uris*.
5. In the entry field *network.negotiate-auth.trusted-uris*, enter the [URL](#) of the [APP Server](#).

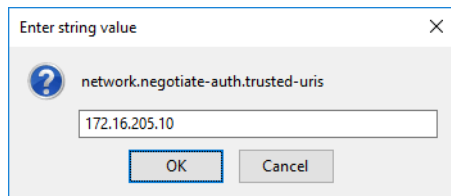



Fig. 33: Enter IP address (example)

6. Click on the button *OK*.

5.3 Mozilla Firefox default

5.3.1 Configure pop-up blocker

1. Click on the icon  (*Open menu*) in the top right corner of the window.
2. Click on the menu item *Options*.

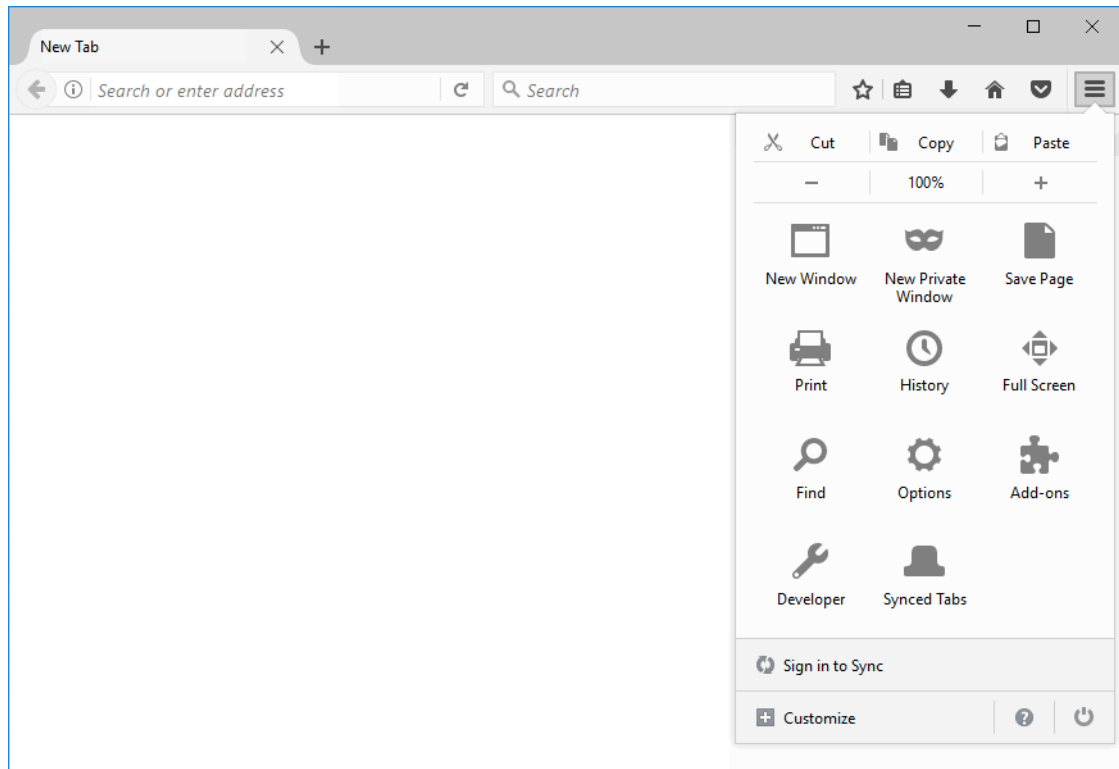


Fig. 34: Firefox > Options

- Click on the menu item *Privacy & Security*.

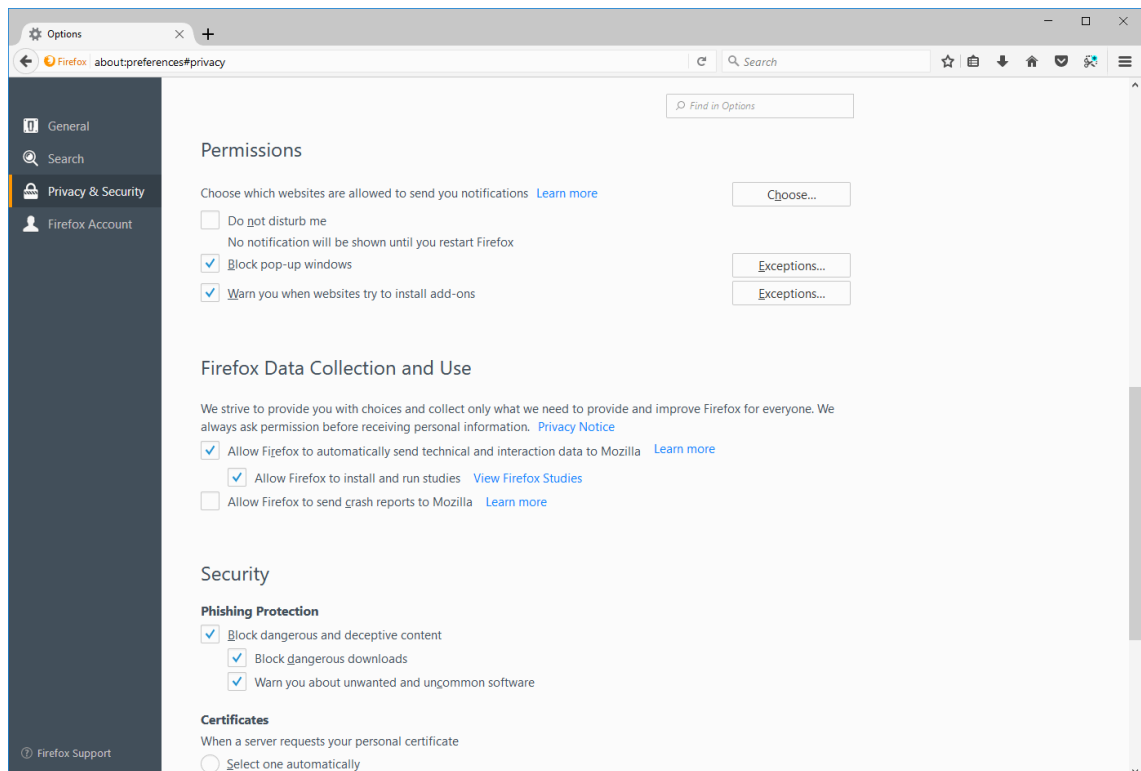


Fig. 35: Tab Content

- Activate the option *Block pop-up windows*.
☒ = Option has been activated.
☐ = Option has been deactivated.
- Click on the button *Exceptions* under *Block pop-up window*.
- In the entry field *Address of website*, enter the [URL](#) of the [APP Server](#).

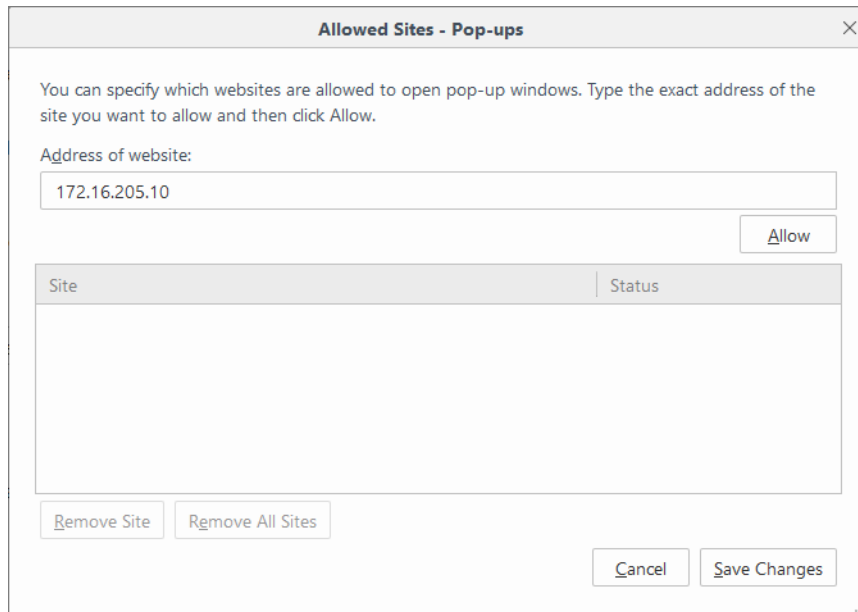



Fig. 36: Allowed Sites - Pop-ups (example)

7. Click on the button *Allow*.
8. Click on the button *Save Changes*.

5.3.2 Add security exception

1. Click on the icon  (*Open menu*) in the top right corner of the window.
2. Click on the menu item *Options*.
3. Click on the menu item *Privacy & Security*.

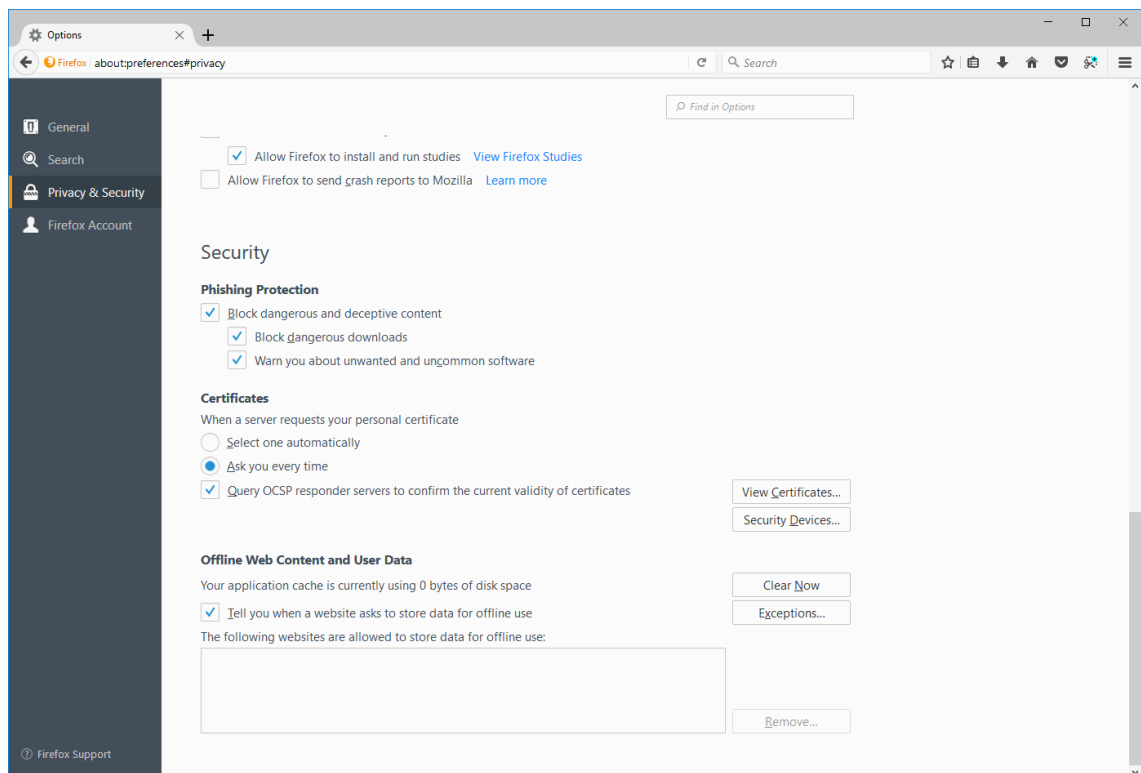


Fig. 37: Encryption

4. Click on the button *View Certificates*.
5. Click on the tab *Servers*.

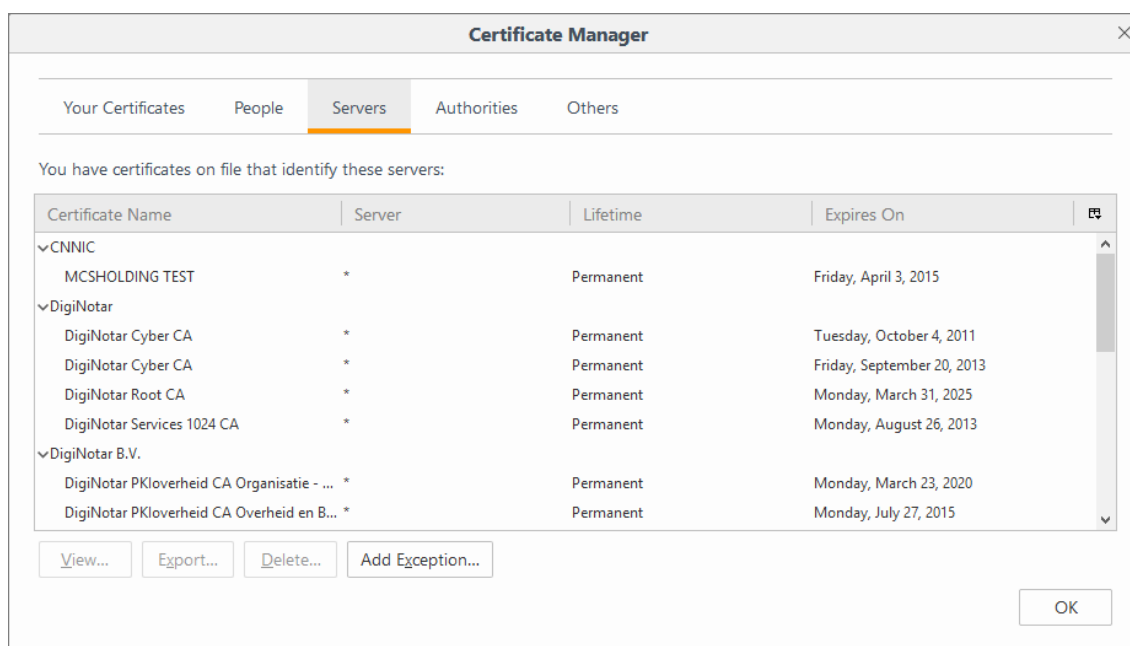



Fig. 38: Certificate Manager

6. Click on the button *Add Exception*.
7. In the entry field *Address*, enter the [URL](#) of the [APP Server](#).
8. Click on the button *Download Certificate*.
9. Click on the button *Confirm Security Exception*.
10. Click on the button *OK*.

5.4 Mozilla Firefox ESR

5.4.1 Configure pop-up blocker

1. Click on the icon  (*Open menu*) in the top right corner of the window.
2. Click on the menu item *Options*.

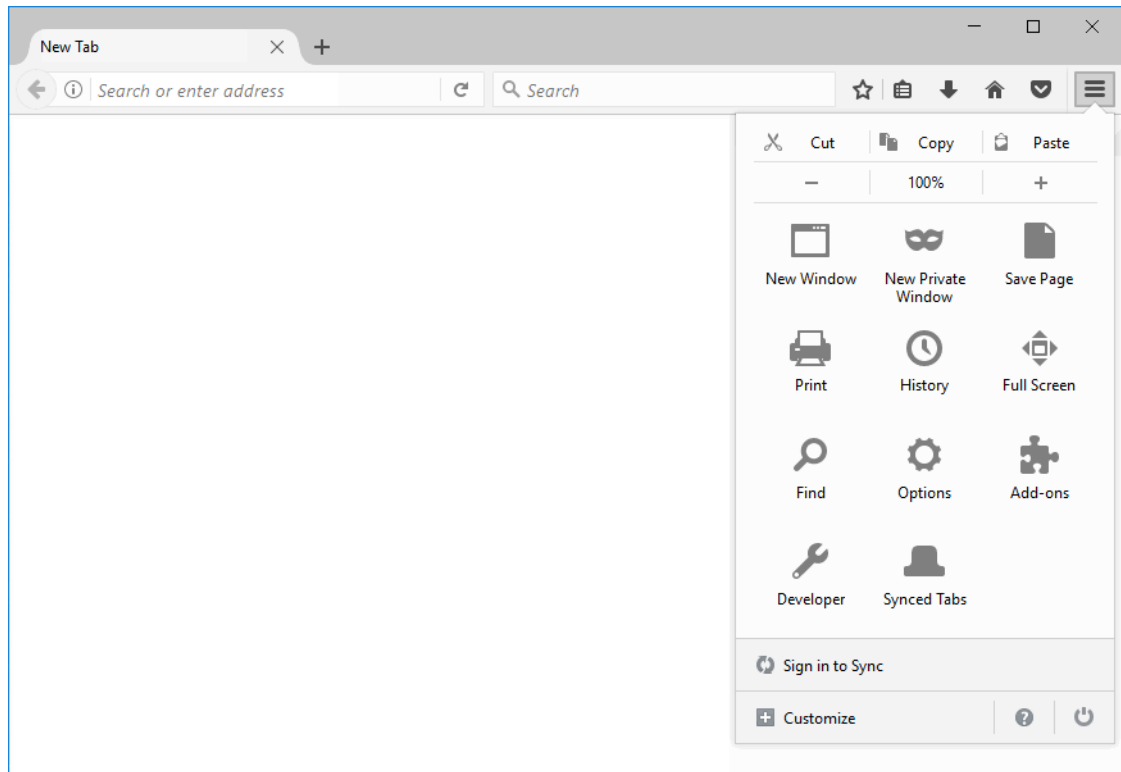


Fig. 39: Firefox > Options

3. Click on the menu item *Content*.

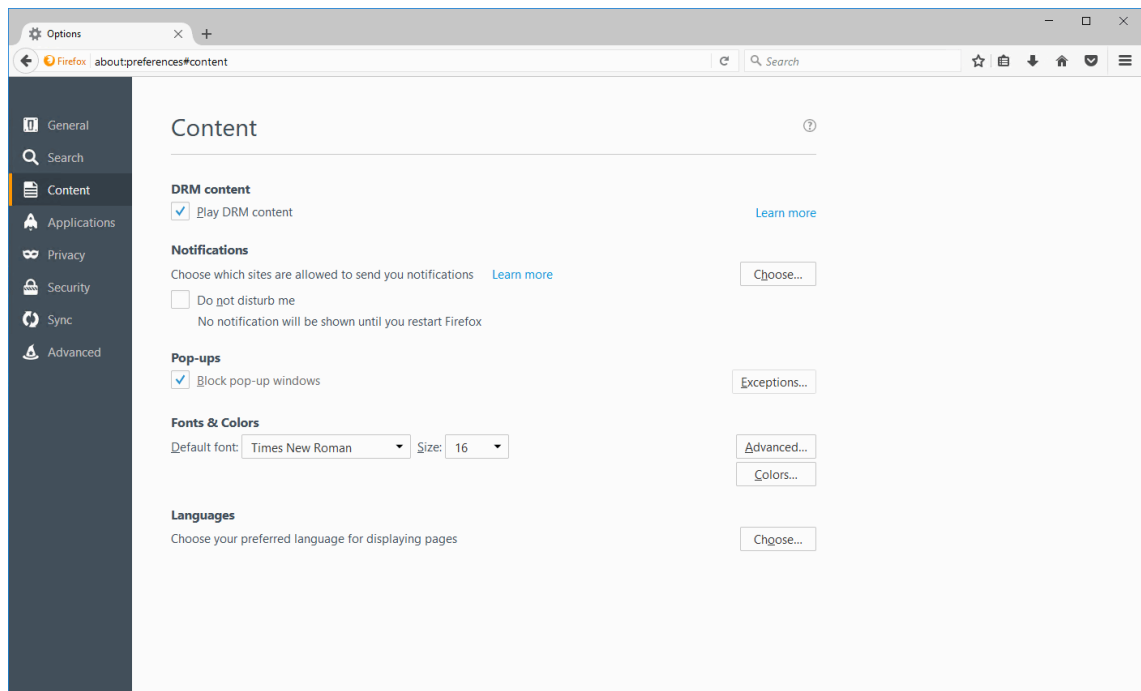


Fig. 40: Content

4. Activate the option *Block pop-up windows*.
☒ = Option has been activated.
☐ = Option has been deactivated.
5. Click on the button *Exceptions* under *Block pop-up window*.
6. In the entry field *Address of website*, enter the [URL](#) of the [APP Server](#).

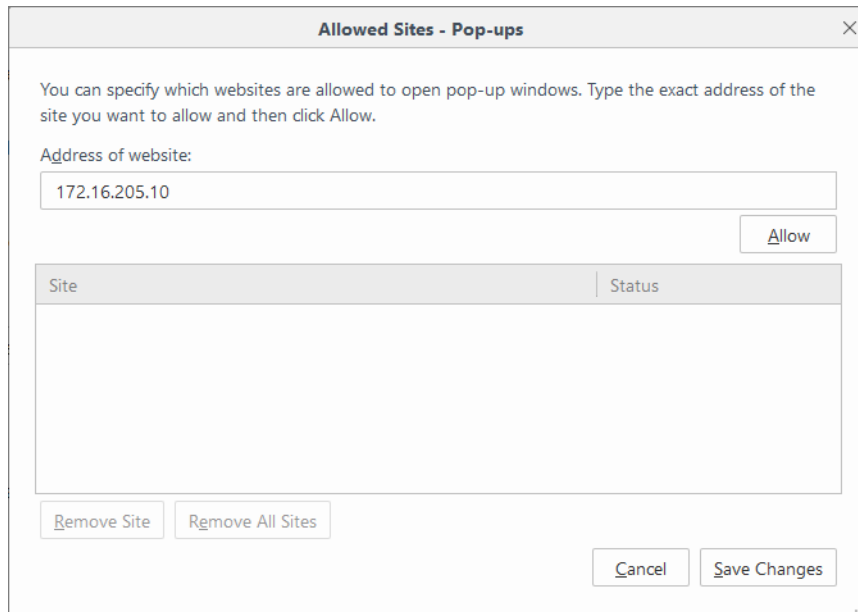



Fig. 41: Allowed Sites - Pop-ups (example)

7. Click on the button *Allow*.
8. Click on the button *Save Changes*.

5.4.2 Add security exception

1. Click on the icon  (*Open menu*) in the top right corner of the window.
2. Click on the menu item *Options*.
3. Click on the menu item *Advanced*.

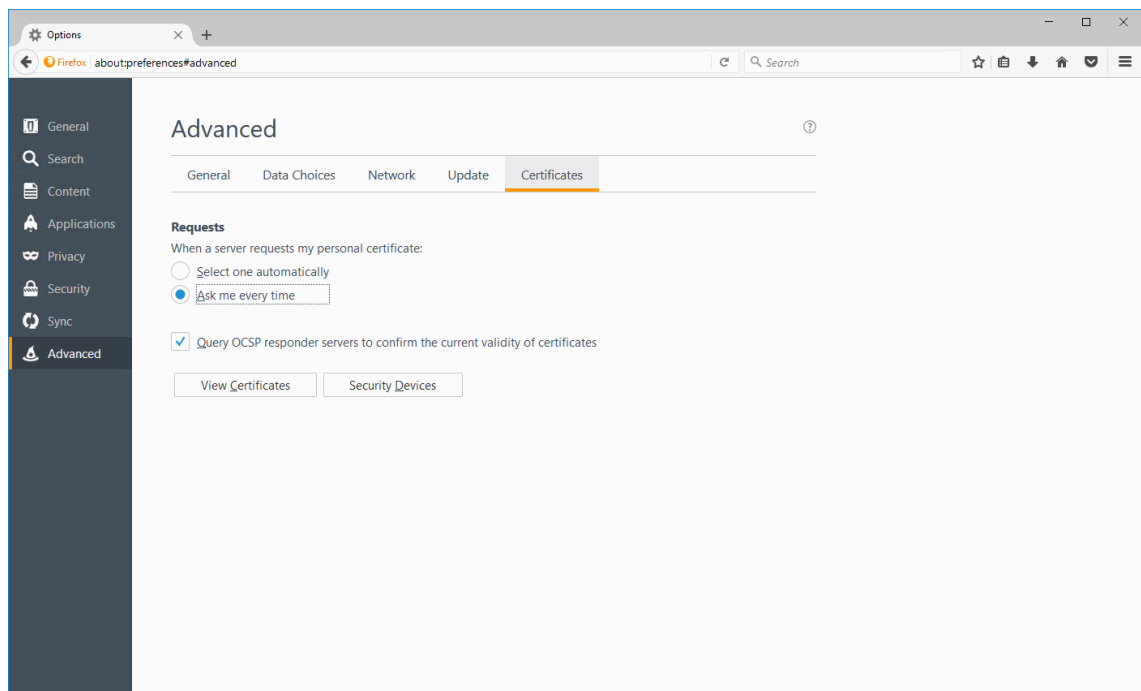


Fig. 42: Certificates

4. Click on the tab *Certificates*.
5. Click on the button *View Certificates*.
6. Click on the tab *Servers*.

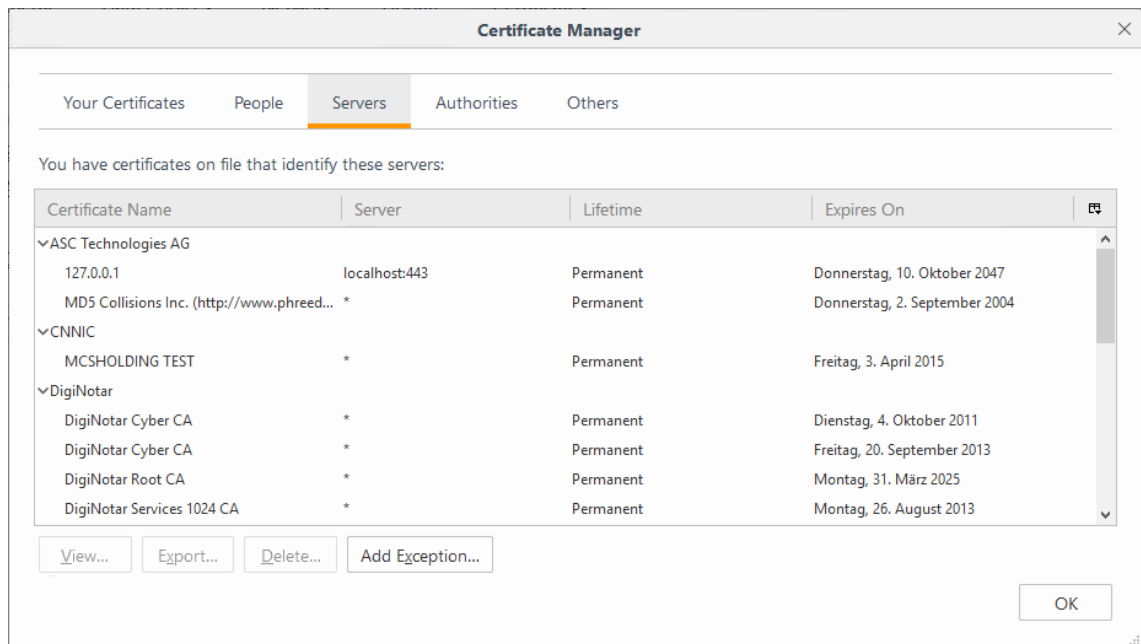


Fig. 43: Certificate Manager

7. Click on the button *Add Exception*.
8. In the entry field *Address*, enter the [URL](#) of the [APP Server](#).
9. Click on the button *Download Certificate*.
10. Click on the button *Confirm Security Exception*.

6 Configuration Google Chrome

6 Configuration Google Chrome

Using the ASC software with Google Chrome does not require any special configuration.

7

Quick guide

7.1 Configuration Internet Explorer version 11


- Configure pop-up blocker:

 (Extras) > **Internet options** > **Privacy** > **Settings** > **Address of website to allow:** enter [URL](#) of the [app server](#) > **Add** > **Close** > **OK**.

- Add security exception:

Enter [URL](#) of the [app server](#) into the address bar, activate > **Continue to this website (not recommended)** > **Certificate Error** > **View Certificates** > **General** > **Install Certificate** > **Next** > **Current user** (certificate only for the current user of the client PC) or **Local computer** (certificate for all users of the client PC) > **Next** > **Place all certificates in the following store:** > **Browse** > **Trusted Root Certification Authorities** > **OK** > **Next** > **Finish** > confirm security prompt.

- Configure security exception for POWERplay Web:


Enter [URL](#) <https://<System-IP>/POWERplayWeb/>; in the [URL](#), replace the parameter <System-IP> with the [URL](#) of the [app server](#) > **Enter key** > log in to the application > **OK** > **Continue to this website (not recommended)** > **Certificate Error** > **View Certificates** > **General** > **Install Certificate** > **Next** > **Current user** (certificate for the current user of the client PC) or **Local computer** (certificate for all users of the client PC) > **Next** > **Place all certificates in the following store:** > **Browse** > **Trusted Root Certification Authorities** > **OK** > **Next** > **Finish** > confirm security prompt >  (Logoff).

- Configure Single Sign On:

 (Extras) activate > **Internet options** > **Advanced** > **Security** > **Enable Integrated Windows Authentication***: **Security** > **Internet** > **Custom level** > **User Authentication** > **Logon** > **Automatic logon with current user name and password** > **OK** > **OK**.

- Configure compatibility view:

Internet Explorer version 11:

 (Extras) > **Compatibility View Settings** > ensure that the compatibility mode for the [app server](#) has been deactivated; [URL](#) of the [app server](#) must not be listed; deactivate > **Display intranet sites in Compatibility View**; deactivate > **Use Microsoft Compatibility Lists** > **Close**.

7.2 Configuration Microsoft Edge

- Install certificate:

Install certificate with the browser Internet Explorer:

Start the browser Internet Explorer > enter [URL](#) of the [app server](#) into the address bar, activate > **Continue to this website (not recommended)** > **Certificate Error** > **View Certificates** > **General** > **Install Certificate** > **Next** > **Current user** (certificate only for the current user of the client PC) or **Local computer** (certificate for all users of the client PC) > **Next** > **Place all certificates in the following store:** > **Browse** > **Trusted Root Certification Authorities** > **OK** > **Next** > **Finish** > confirm security prompt.

or


Copy certificate to the client computer from the [app server](#) and install it:

Copy the file C:\Program Files (x86)\ASC\ASC Product Suite\data\crypto\https.crt from the [app server](#) to the desktop of the client computer > on the desktop of the client computer, right-click on the icon of the file **https.crt** activate > **Install Certificate** > **Next** > **Current user** (certificate only for the current user of the client PC) or **Local computer** (certificate for all users of the client PC) > **Next** > **Place all certificates in the following store:** > **Browse** > **Trusted Root Certification Authorities** > **OK** > **Next** > **Finish** > **Yes** > **OK**.



- Configure security exception for POWERplay Web:
Start browser Microsoft Edge > enter **URL** <https://<System-IP>/POWERplayWeb/>; in the **URL**, replace the parameter <System-IP> with the **URL** of the **app server** > **Enter key** > log in to the application > **OK** > **Always allow** > **Details** > **Go on to webpage (Not recommended)**.

7.3



Configuration Mozilla Firefox

- Configure security exception for POWERplay Web:
Enter **URL** <https://<System-IP>/POWERplayWeb/>; in the **URL**, replace the parameter <System-IP> with the **URL** of the **app server** > **Enter key** > log in to the application > **OK** > **Advanced** > **Add exception** > **Confirm security exception** >  (*Logoff*).
- Configure Single Sign On:
Enter **URL** <about:config> > **[Enter] key** > confirm security prompt > **Search:** enter `network.negotiate-auth.trusted-uris` > double-click on the entry **network.negotiate-auth.trusted-uris** > enter **URL** of the **app server** > **OK**.

Mozilla Firefox default

- Configure pop-up blocker:
 (*Open menu*) activate > **Settings** > **Privacy & Security** > **Block pop-up window** > **Exceptions** > enter **URL** of the **app server** > **Allow** > **Save Changes**.
- Add security exception:
 (*Open menu*) > **Settings** > **Privacy & Security** > **View Certificates** > **Servers** > **Add Exception** > enter **URL** of the **app server** > **Download Certificate** > **Confirm Security Exception Rule** > **OK**.

Mozilla Firefox ESR

- Configure pop-up blocker:
 (*Open menu*) activate > **Settings** > **Content** > **Block pop-up window** > **Exceptions** > enter **URL** of the **app server** > **Allow** > **Save Changes**.
- Add security exception:
 (*Open menu*) > **Settings** > **Advanced** > **Certificates** > **View Certificates** > **Servers** > **Add Exception** > enter **URL** of the **app server** > **Download Certificate** > **Confirm Security Exception Rule**.

List of figures

Fig. 1	Tab Privacy	6
Fig. 2	Pop-up Blocker Settings (example).....	6
Fig. 3	Continue to this website	7
Fig. 4	Certificate	7
Fig. 5	Certificate Import Wizard.....	8
Fig. 6	Select certificate store	9
Fig. 7	Certificate Import Wizard.....	9
Fig. 8	Accept Websocket certificate	10
Fig. 9	Continue to this website	10
Fig. 10	Certificate	11
Fig. 11	Certificate Import Wizard.....	11
Fig. 12	Select certificate store	12
Fig. 13	Certificate Import Wizard.....	12
Fig. 14	Tab Advanced	13
Fig. 15	Tab Security	14
Fig. 16	Security Settings - Internet Zone.....	14
Fig. 17	Internet Explorer > Compatibility View Settings	15
Fig. 18	Compatibility View settings (example)	15
Fig. 19	Install certificate	16
Fig. 20	Certificate Import Wizard.....	17
Fig. 21	Select certificate store	17
Fig. 22	Certificate Import Wizard.....	18
Fig. 23	Security warning.....	18
Fig. 24	Certificate Import Wizard.....	18
Fig. 25	Accept Websocket certificate	19
Fig. 26	Welcome screen	19
Fig. 27	Continue to this website	20
Fig. 28	Accept Websocket certificate	21
Fig. 29	No secure connection	21
Fig. 30	No secure connection	22
Fig. 31	Confirm security exception.....	22
Fig. 32	about:config > network.negotiate-auth.trusted-uris	23
Fig. 33	Enter IP address (example)	23
Fig. 34	Firefox > Options.....	24
Fig. 35	Tab Content	24
Fig. 36	Allowed Sites - Pop-ups (example).....	25
Fig. 37	Encryption	25
Fig. 38	Certificate Manager.....	26
Fig. 39	Firefox > Options.....	27
Fig. 40	Content.....	27
Fig. 41	Allowed Sites - Pop-ups (example).....	28



Fig. 42	Certificates	28
Fig. 43	Certificate Manager	29

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.

SSO

Single Sign On; Simplified login mode. After a one-off authentication at one workplace users will be able to use all services and applications that they have been authorized for from this workplace. They do not have to authenticate for the individual applications again.

URL

Uniform resource locator. Identifies and locates a resource (e. g. a website) about the used access method (e. g. the used network protocol as HTTP or FTP) and the location of the resource in the computer network. (Source: Wikipedia 20th November 2013)