

# Konfiguration Browser



## Installationsanleitung für Systembetreiber und Mandanten

19.08.2020

*Originalanleitung*

### Produktlinie neo, Version 6.x

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

EVOIPneo

EVOLUTIONneo / XXL / eco

EVOflex (länderspezifisch)

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

<b>1</b>	<b>Allgemeine Hinweise .....</b>	<b>4</b>
<b>2</b>	<b>Einleitung .....</b>	<b>5</b>
<b>3</b>	<b>Konfiguration Internet Explorer Version 11.....</b>	<b>6</b>
3.1	Pop-up-Blocker konfigurieren.....	6
3.2	Sicherheitsausnahme hinzufügen .....	7
3.3	Sicherheitsausnahme für POWERplay Web konfigurieren .....	9
3.4	Single Sign On konfigurieren .....	12
3.5	Kompatibilitätsansicht konfigurieren.....	14
3.5.1	Internet Explorer Version 11 .....	14
<b>4</b>	<b>Konfiguration Microsoft Edge.....</b>	<b>16</b>
4.1	Zertifikat installieren .....	16
4.2	Sicherheitsausnahme für POWERplay Web konfigurieren .....	19
<b>5</b>	<b>Konfiguration Mozilla Firefox.....</b>	<b>21</b>
5.1	Sicherheitsausnahme für POWERplay Web konfigurieren .....	21
5.2	Single Sign On konfigurieren .....	22
5.3	Mozilla Firefox Standard .....	23
5.3.1	Pop-up-Blocker konfigurieren.....	23
5.3.2	Sicherheitsausnahme hinzufügen .....	25
5.4	Mozilla Firefox ESR.....	26
5.4.1	Pop-up-Blocker konfigurieren.....	26
5.4.2	Sicherheitsausnahme hinzufügen .....	28
<b>6</b>	<b>Konfiguration Google Chrome.....</b>	<b>30</b>
<b>7</b>	<b>Quick Guide .....</b>	<b>31</b>
7.1	Konfiguration Internet Explorer Version 11 .....	31
7.2	Konfiguration Microsoft Edge .....	31
7.3	Konfiguration Mozilla Firefox.....	32
	<b>Glossar.....</b>	<b>36</b>

**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 Konfiguration der Browser für die ASC-Software.



---

Stellen Sie sicher, dass JavaScript aktiviert ist.

---



---

Stellen Sie sicher, dass Cookies erlaubt sind.

---


## 3

## Konfiguration Internet Explorer Version 11

1. Starten Sie den Browser, um alle im Folgenden beschriebenen Konfigurationen vorzunehmen.

## 3.1

## Pop-up-Blocker konfigurieren

1. Klicken Sie auf das Symbol  (*Extras*).
2. Klicken Sie auf den Menüpunkt *Internetoptionen*.
3. Klicken Sie auf die Registerkarte *Datenschutz*.

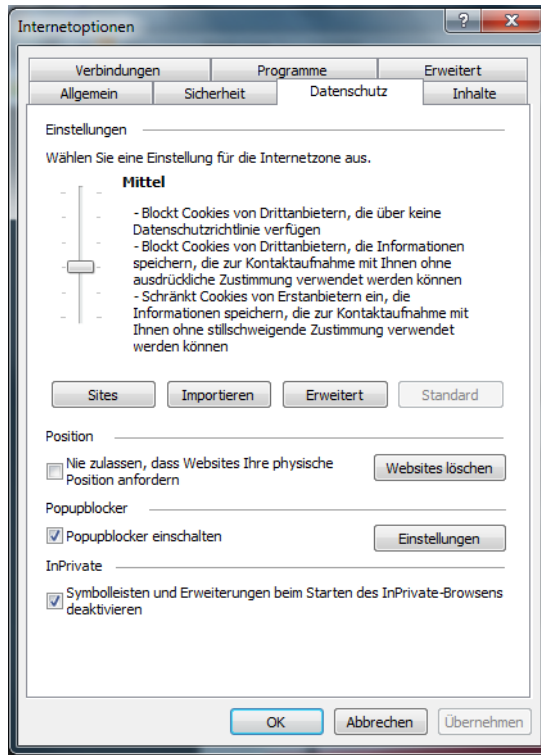


Abb. 1: Registerkarte Datenschutz

4. Klicken Sie auf die Schaltfläche *Einstellungen*.
5. Geben Sie im Eingabefeld *Adresse der Website, die zugelassen werden soll* die [URL](#) des [APP-Servers](#) ein.

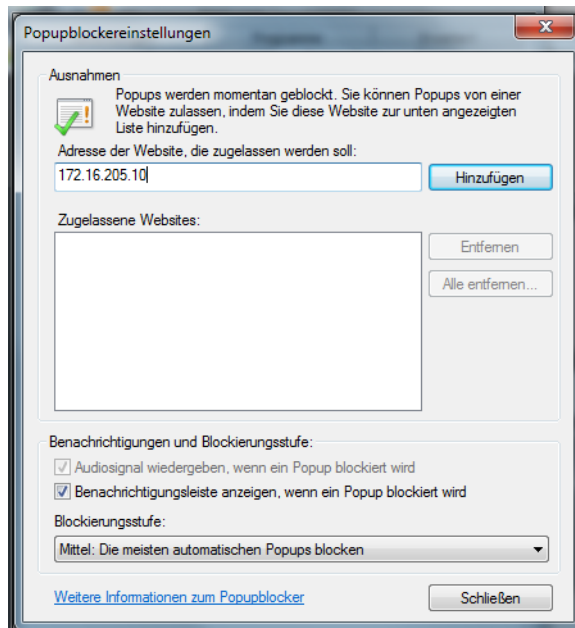


Abb. 2: Pop-upblockereinstellungen (Beispiel)

6. Klicken Sie auf die Schaltfläche *Hinzufügen*.  
⇒ Die Webseite wird im Feld *Zugelassene Websites* hinzugefügt.
7. Klicken Sie auf die Schaltfläche *Schließen*.
8. Klicken Sie auf die Schaltfläche *OK*.

### 3.2 Sicherheitsausnahme hinzufügen

Die folgenden Schritte sind nur notwendig, wenn das neo-Serverzertifikat noch nicht als vertrauenswürdig eingestuft wurde.

1. Geben Sie die **URL** des **APP-Servers** in die Adressleiste ein.
2. Klicken Sie auf *Laden dieser Website fortsetzen (nicht empfohlen)*.

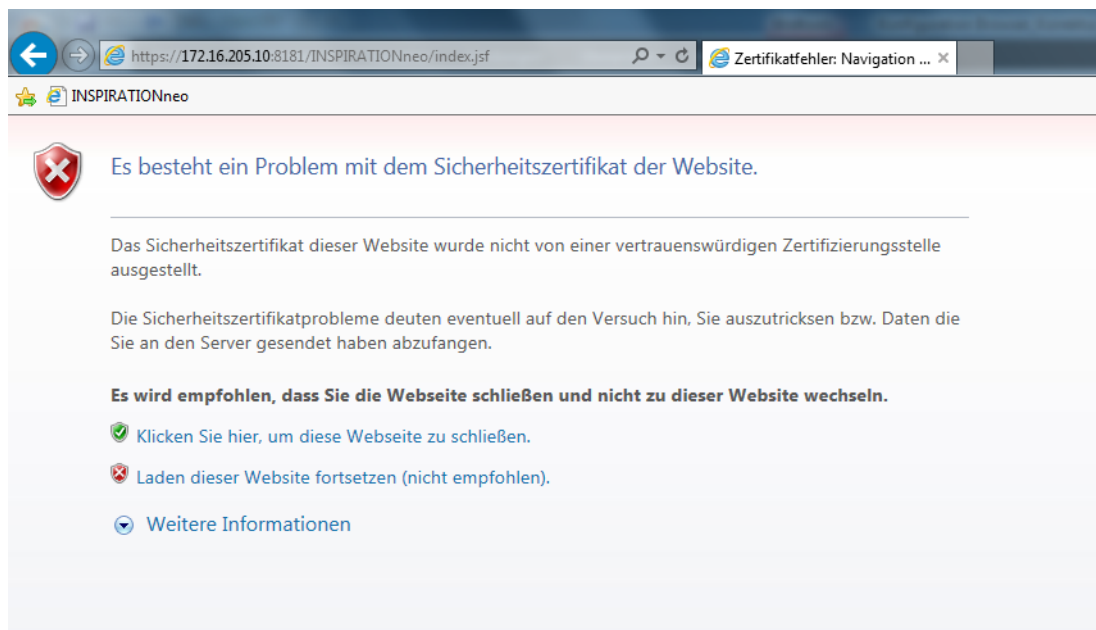


Abb. 3: Laden dieser Website fortsetzen

3. Falls ein Zertifikatsfehler angezeigt wird, klicken Sie auf das rote Feld *Zertifikatsfehler* in der Kopfzeile und fahren Sie mit den folgenden Schritten fort.

4. Klicken Sie auf *Zertifikate anzeigen*.  
⇒ Das folgende Fenster erscheint:

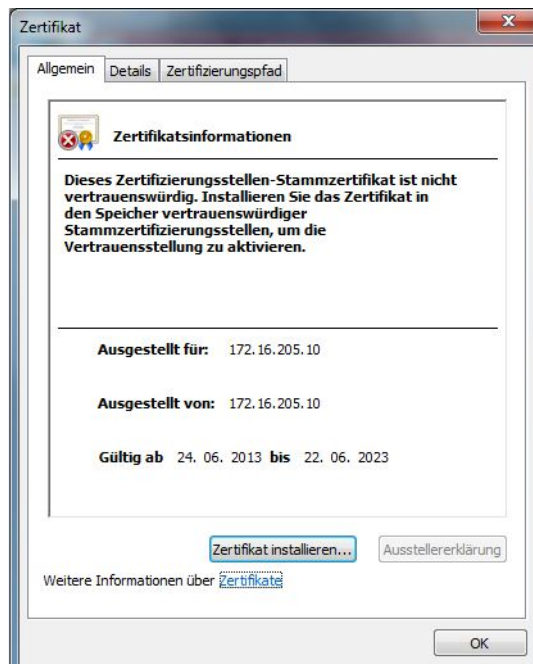


Abb. 4: Zertifikat

5. Klicken Sie auf die Registerkarte *Allgemein*.
6. Klicken Sie auf die Schaltfläche *Zertifikat installieren*.
7. Klicken Sie auf die Schaltfläche *Weiter*, um den Zertifikatimport-Assistenten zu starten.

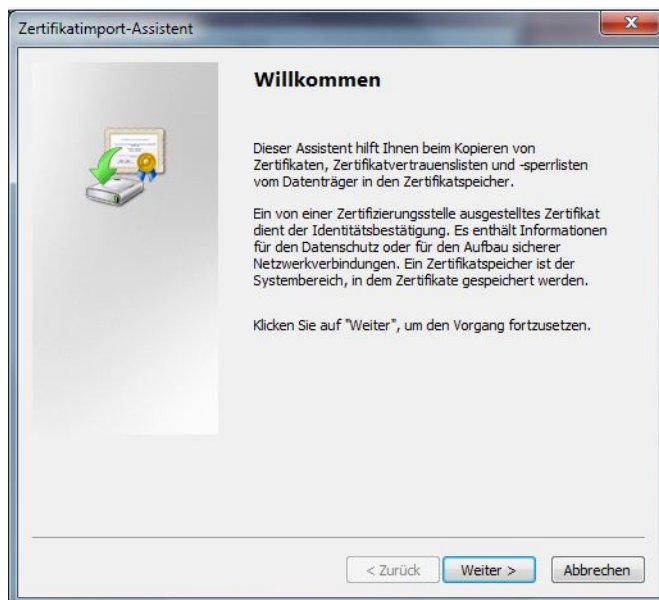


Abb. 5: Zertifikatimport-Assistent

8. Wenn das Zertifikat nur für den aktuellen Benutzer des Client-PCs gültig sein soll, wählen Sie als Speicherort die Option *Aktueller Benutzer*.  
Wenn das Zertifikat für alle Benutzer des Client-PCs gültig sein soll, wählen Sie als Speicherort die Option *Lokaler Computer*.
9. Klicken Sie auf die Schaltfläche *Weiter*.
10. Aktivieren Sie die Option *Alle Zertifikate in folgendem Speicher speichern*.
11. Klicken Sie auf die Schaltfläche *Durchsuchen*.



12. Klicken Sie auf das Verzeichnis *Vertrauenswürdige Stammzertifizierungsstellen*.

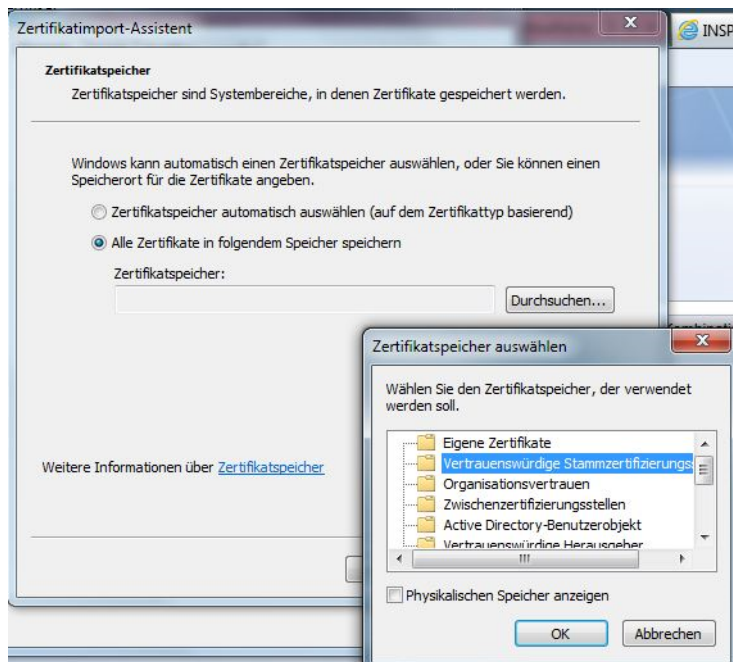


Abb. 6: Zertifikatspeicher auswählen

13. Klicken Sie auf die Schaltfläche *OK*.

14. Klicken Sie auf die Schaltfläche *Weiter*.

15. Klicken Sie auf die Schaltfläche *Fertig stellen*.

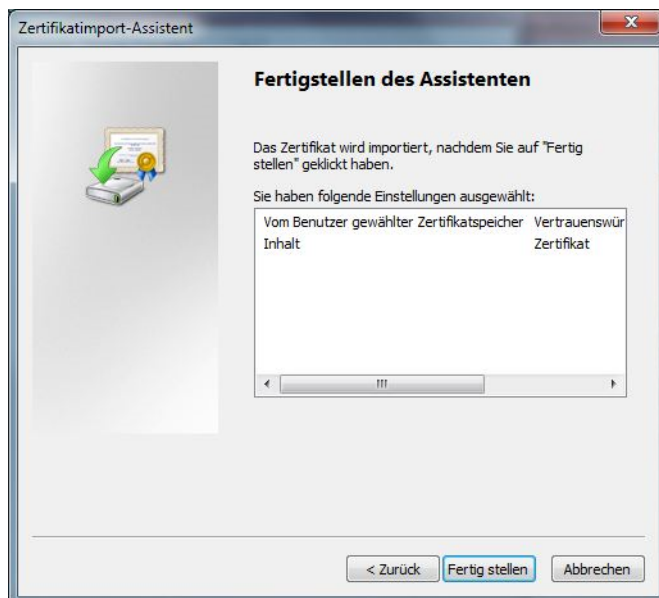


Abb. 7: Zertifikatsimport-Assistent

16. Bestätigen Sie die Sicherheitsabfrage.

### 3.3

#### Sicherheitsausnahme für POWERplay Web konfigurieren

1. Geben Sie die folgende URL in die Adresszeile ein:  
`https://<System-IP>/POWERplayWeb/`
2. Ersetzen Sie in der URL den Parameter <System-IP> durch die IP-Adresse des APP-Servers.
3. Drücken Sie die [Enter]-Taste.

- ⇒ Der Anmeldebildschirm erscheint.
- 4. Melden Sie sich mit Ihrem Benutzernamen und dem Passwort an der Applikation an.
  - ⇒ Die Applikation wird geöffnet.
- Das folgende Fenster erscheint:

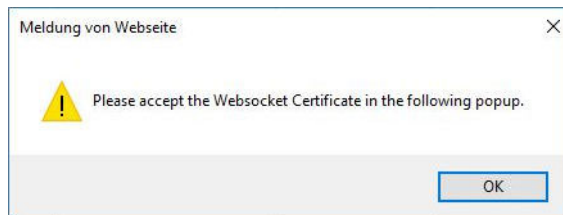


Abb. 8: Websocket-Zertifikat akzeptieren

- 5. Klicken Sie auf die Schaltfläche **OK**.
- 6. Klicken Sie auf *Laden dieser Website fortsetzen (nicht empfohlen)*.

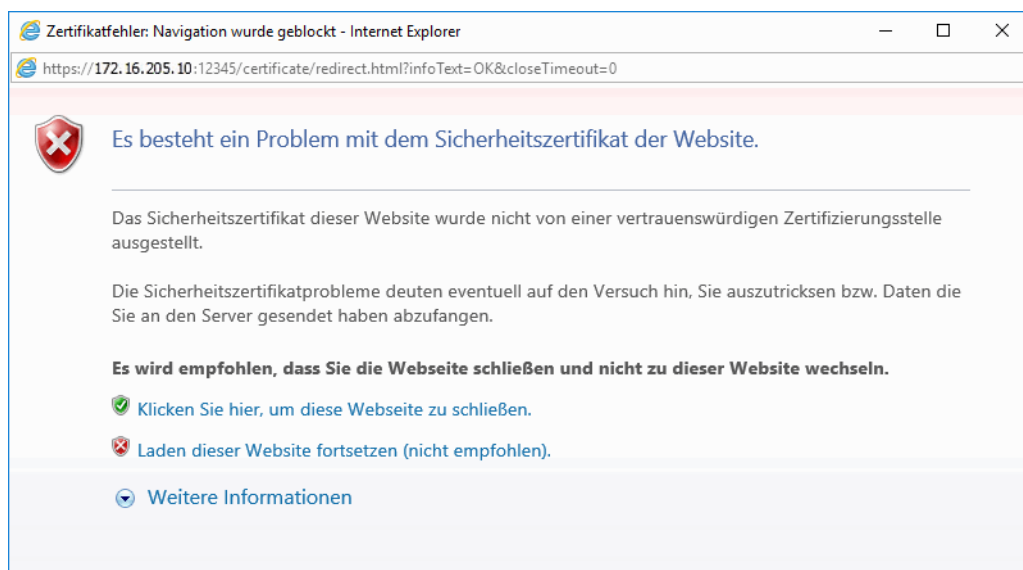


Abb. 9: Laden dieser Website fortsetzen

- 7. Falls ein Zertifikatsfehler angezeigt wird, klicken Sie auf das rote Feld *Zertifikatsfehler* in der Kopfzeile und fahren Sie mit den folgenden Schritten fort.
- 8. Klicken Sie auf *Zertifikate anzeigen*.
  - ⇒ Das folgende Fenster erscheint:

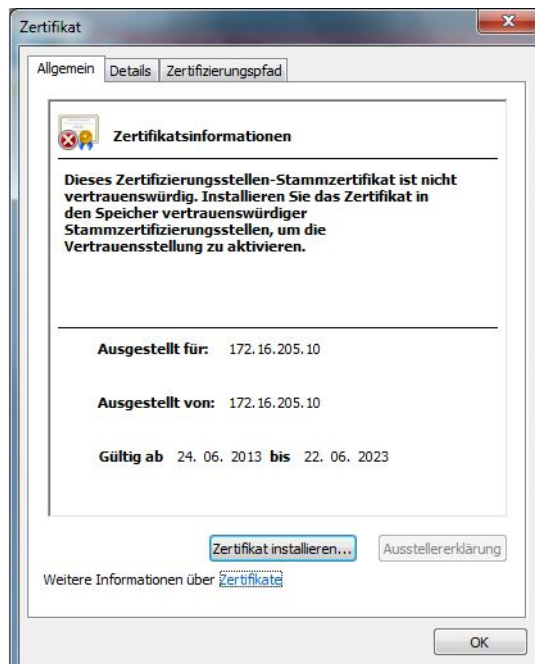


Abb. 10: Zertifikat

9. Klicken Sie auf die Registerkarte *Allgemein*.
10. Klicken Sie auf die Schaltfläche *Zertifikat installieren*.
11. Klicken Sie auf die Schaltfläche *Weiter*, um den Zertifikatimport-Assistenten zu starten.

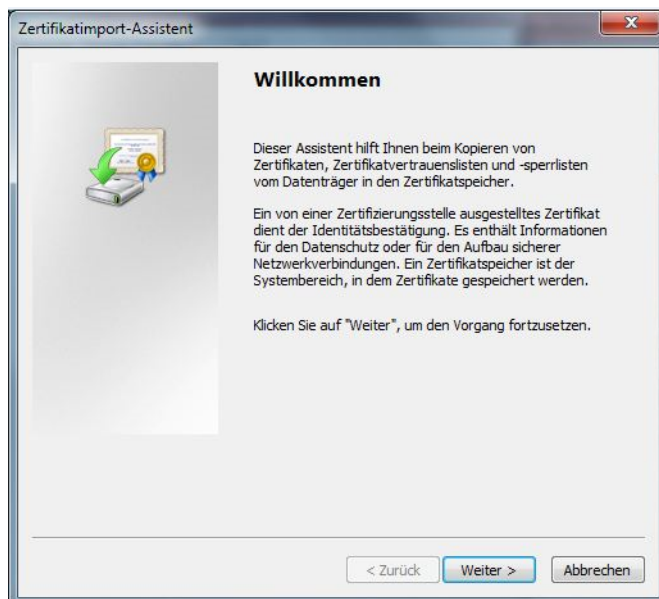


Abb. 11: Zertifikatimport-Assistent

12. Wenn das Zertifikat nur für den aktuellen Benutzer des Client-PCs gültig sein soll, wählen Sie als Speicherort die Option *Aktueller Benutzer*. Wenn das Zertifikat für alle Benutzer des Client-PCs gültig sein soll, wählen Sie als Speicherort die Option *Lokaler Computer*.
13. Klicken Sie auf die Schaltfläche *Weiter*.
14. Aktivieren Sie die Option *Alle Zertifikate in folgendem Speicher speichern*.
15. Klicken Sie auf die Schaltfläche *Durchsuchen*.
16. Klicken Sie auf das Verzeichnis *Vertrauenswürdige Stammzertifizierungsstellen*.

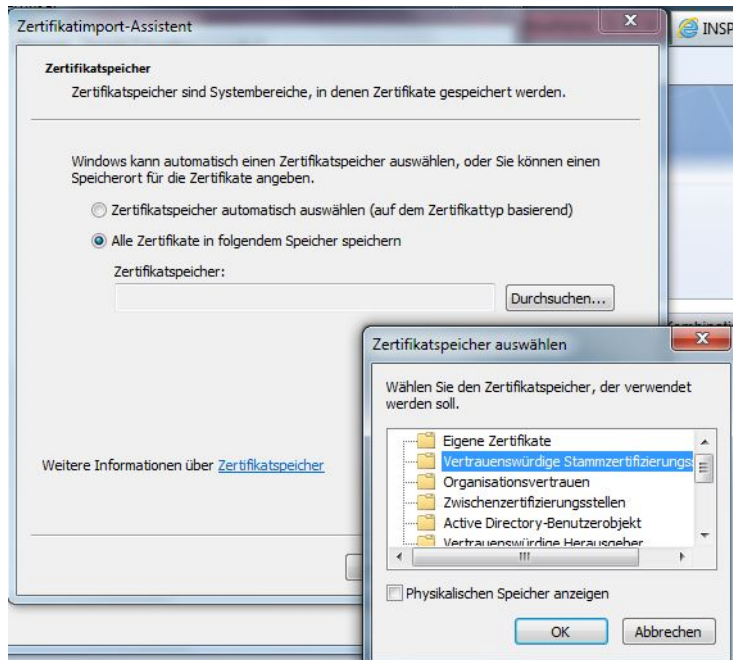


Abb. 12: Zertifikatspeicher auswählen

17. Klicken Sie auf die Schaltfläche **OK**.
18. Klicken Sie auf die Schaltfläche **Weiter**.
19. Klicken Sie auf die Schaltfläche **Fertig stellen**.

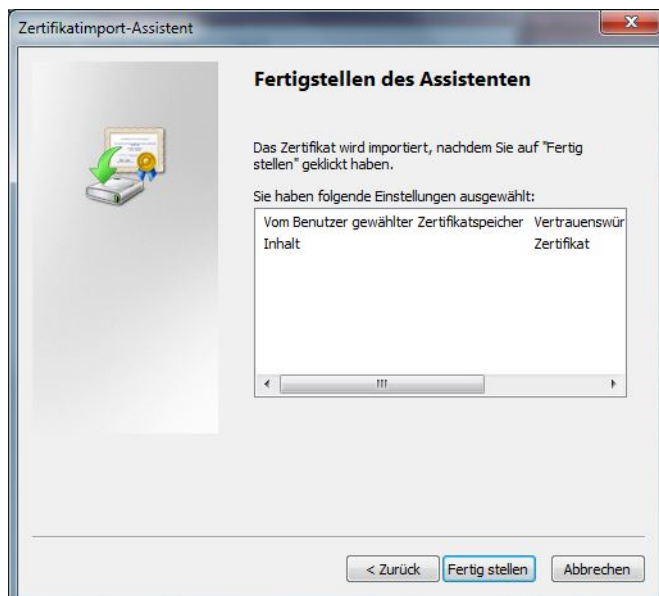


Abb. 13: Zertifikatimport-Assistent


20. Bestätigen Sie die Sicherheitsabfrage.
21. Klicken Sie in der Applikation auf das Symbol  (*Logoff*), um die Applikation zu schließen.

### 3.4 Single Sign On konfigurieren



Stellen Sie sicher, dass die **URL** des **APP-Servers** bei den vertrauenswürdigen Seiten hinzugefügt wurde (siehe Vertrauenswürdige Seite einrichten).

Single Sign On (**SSO**) funktioniert für alle Webapplikationen nur in einer Domäne. Deshalb müssen alle Rechner in eine entsprechende Windows-Domäne aufgenommen werden.

1. Klicken Sie auf das Symbol  (*Extras*).
2. Klicken Sie auf den Menüpunkt *Internetoptionen*.
3. Klicken Sie auf die Registerkarte *Erweitert*.

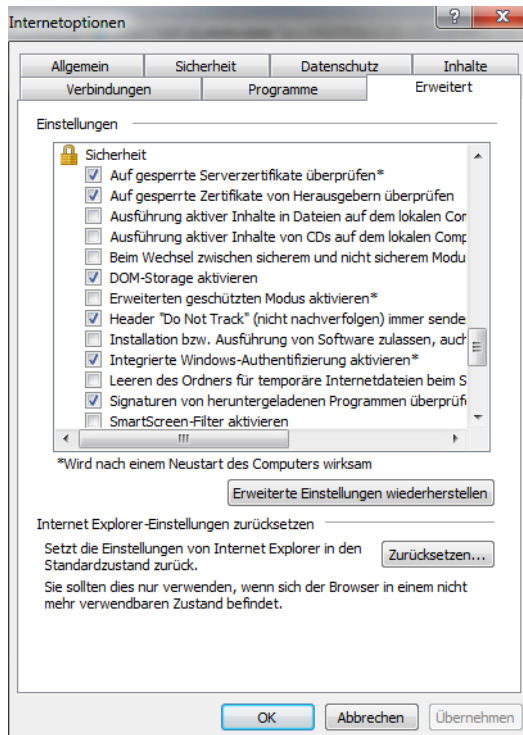


Abb. 14: Registerkarte Erweitert

4. Aktivieren Sie unter *Sicherheit* die Option *Integrierte Windows-Authentifizierung aktivieren*\*.  
☒ = Option ist aktiviert.  
☐ = Option ist deaktiviert.
5. Klicken Sie auf die Registerkarte *Sicherheit*.

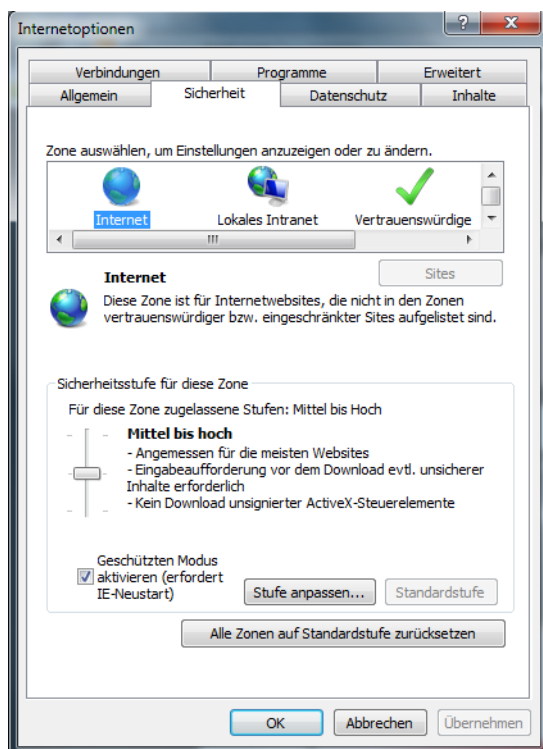


Abb. 15: Registerkarte Sicherheit

6. Klicken Sie auf das Symbol *Internet*.
7. Klicken Sie auf die Schaltfläche *Stufe anpassen*.
8. Wählen Sie unter *Benutzerauthentifizierung* > *Anmeldung* die Option *Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort*.

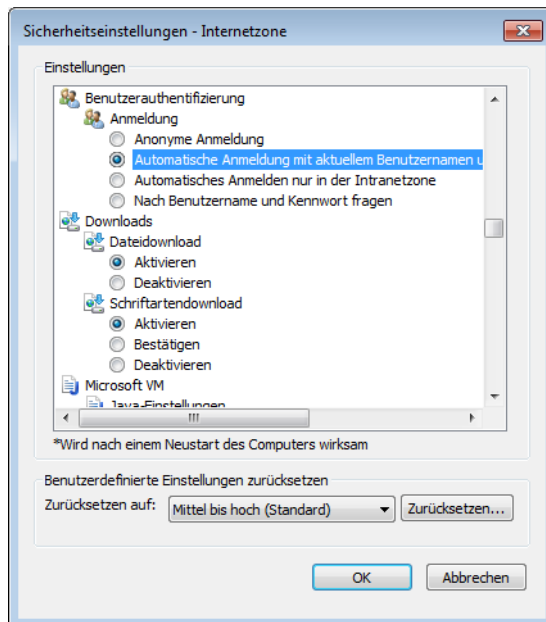



Abb. 16: Sicherheitseinstellungen - Internetzone

9. Klicken Sie auf die Schaltfläche *OK*.
10. Klicken Sie auf die Schaltfläche *OK*.

### 3.5 Kompatibilitätsansicht konfigurieren

Um auf den Web-Seiten der ASC-Software die Funktionen zu gewährleisten, muss beim Internet Explorer der Kompatibilitätsmodus deaktiviert sein.

#### 3.5.1 Internet Explorer Version 11

1. Klicken Sie auf das Symbol  (*Extras*).
2. Klicken Sie auf den Menüpunkt *Einstellungen der Kompatibilitätsansicht*.

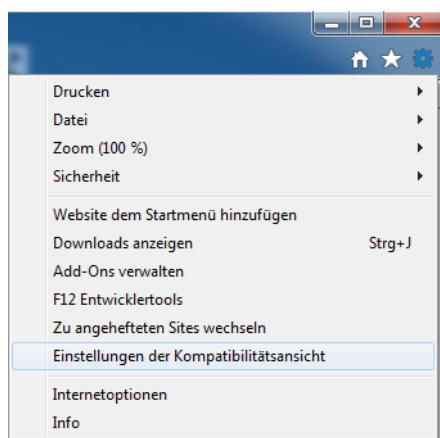


Abb. 17: Internet Explorer > Einstellungen der Kompatibilitätsansicht

3. Stellen Sie sicher, dass der Kompatibilitätsmodus für den **APP-Server** deaktiviert ist. Im Feld *Zur Kompatibilitätsansicht hinzugefügte Websites* darf die **URL** des **APP-Servers** nicht aufgelistet sein.

4. Falls im Feld *Zur Kompatibilitätsansicht hinzugefügte Websites* die URL des APP-Servers aufgeführt ist, klicken Sie auf die URL des APP-Servers. Klicken Sie auf die Schaltfläche *Entfernen*.
5. Deaktivieren Sie die Option *Intranetsites in Kompatibilitätsansicht anzeigen*.
6. Deaktivieren Sie die Option *Kompatibilitätslisten von Microsoft verwenden*.

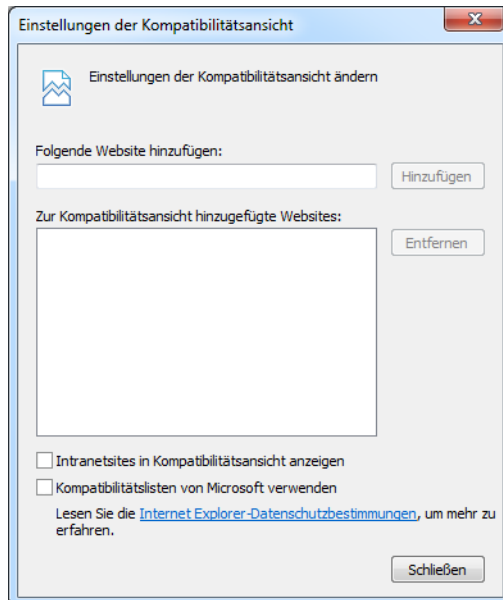


Abb. 18: Einstellungen der Kompatibilitätsansicht (Beispiel)

7. Klicken Sie auf die Schaltfläche *Schließen*.



## 4 Konfiguration Microsoft Edge

## 4.1 Zertifikat installieren

Der Browser Microsoft Edge bietet keine Möglichkeit, ein Zertifikat zu installieren. Um trotzdem ein Zertifikat für den Client-Rechner zu installieren, führen Sie eine der 2 Möglichkeiten durch:

- Zertifikat mit dem Browser Internet Explorer installieren
- Zertifikat vom [APP-Server](#) auf den Client-Rechner kopieren und installieren

**Zertifikat mit dem Browser Internet Explorer installieren**

1. Starten Sie den Browser Internet Explorer.
2. Installieren Sie das Zertifikat. Siehe Kapitel [Kapitel "Sicherheitsausnahme hinzufügen"](#), S. 7.

**Zertifikat vom [APP-Server](#) auf den Client-Rechner kopieren und installieren**

1. Kopieren Sie auf dem [APP-Server](#) die Datei (das Zertifikat) `C:\Program Files (x86)\ASC\ASC Product Suite\data\crypto\https.crt` auf den Desktop des Client-Rechners.
2. Klicken Sie auf dem Desktop des Client-Rechners mit der rechten Maustaste auf das Icon der Datei `https.crt`.

⇒ Das folgende Kontextmenü erscheint:

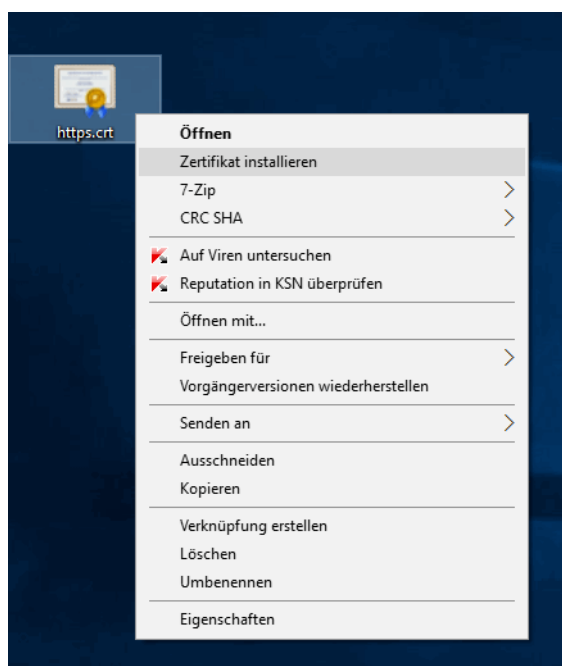


Abb. 19: Zertifikat installieren

3. Klicken Sie im Kontextmenü auf den Menüpunkt *Zertifikat installieren*.
4. Klicken Sie auf die Schaltfläche *Weiter*.



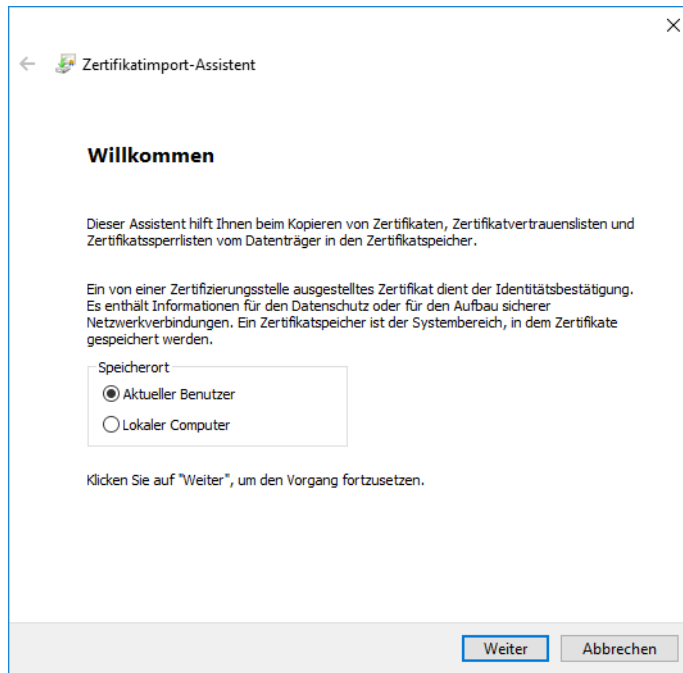


Abb. 20: Zertifikatimport-Assistent

5. Wenn das Zertifikat nur für den aktuellen Benutzer des Client-PCs gültig sein soll, wählen Sie als Speicherort die Option *Aktueller Benutzer*.  
Wenn das Zertifikat für alle Benutzer des Client-PCs gültig sein soll, wählen Sie als Speicherort die Option *Lokaler Computer*.
6. Klicken Sie auf die Schaltfläche *Weiter*.
7. Aktivieren Sie die Option *Alle Zertifikate in folgendem Speicher speichern*.
8. Klicken Sie auf die Schaltfläche *Durchsuchen*.
9. Klicken Sie auf das Verzeichnis *Vertrauenswürdige Stammzertifizierungsstellen*.

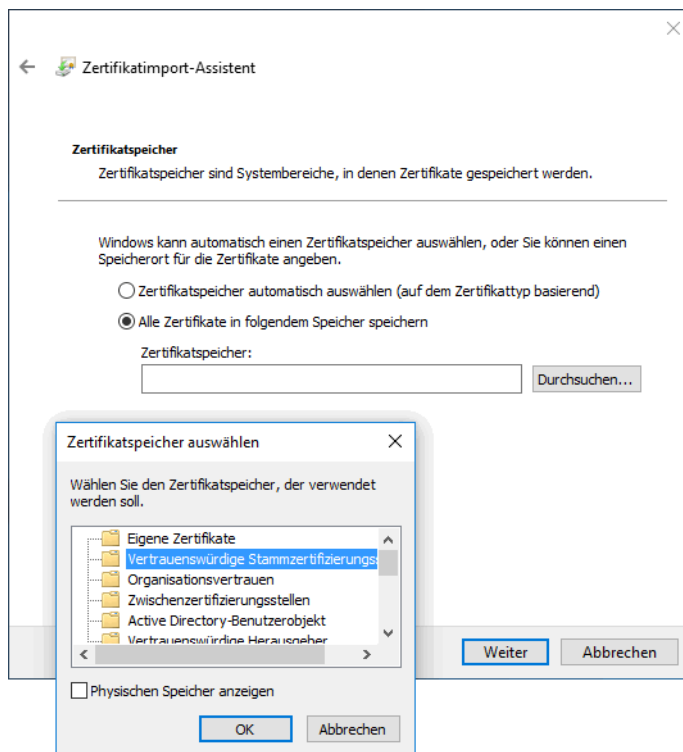


Abb. 21: Zertifikatspeicher auswählen

10. Klicken Sie auf die Schaltfläche *OK*.

11. Klicken Sie auf die Schaltfläche *Weiter*.
12. Klicken Sie auf die Schaltfläche *Fertig stellen*.

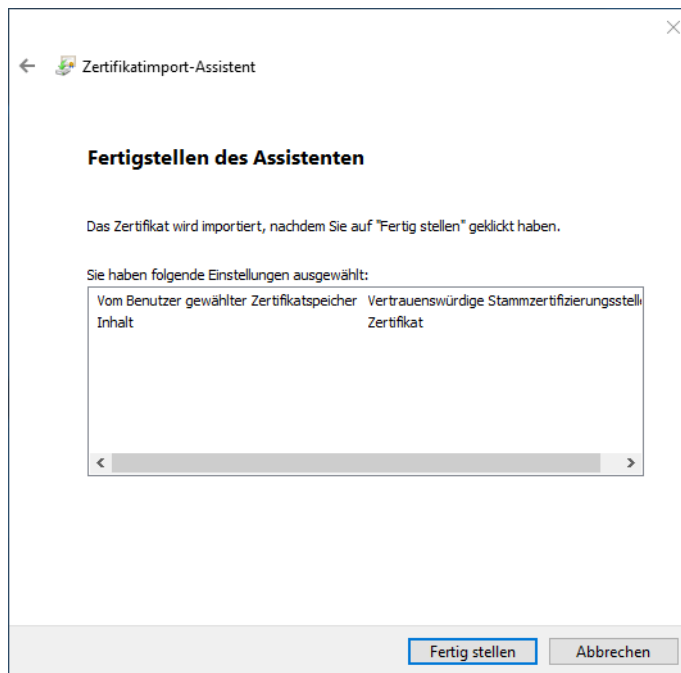


Abb. 22: Zertifikatimport-Assistent

13. Klicken Sie auf die Schaltfläche *Ja*.

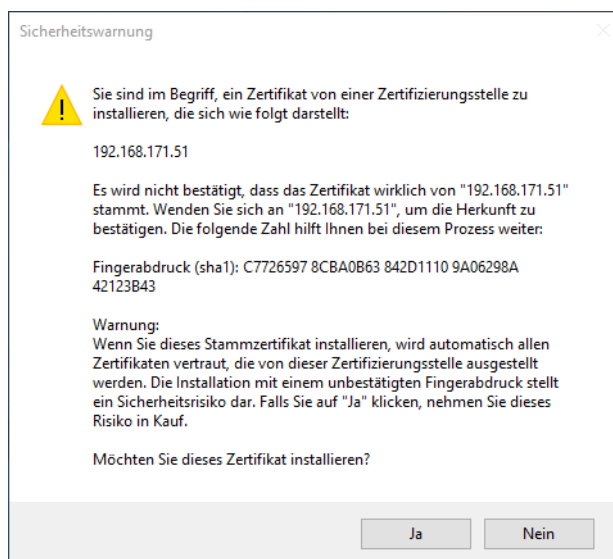


Abb. 23: Sicherheitswarnung

14. Klicken Sie auf die Schaltfläche *OK*.

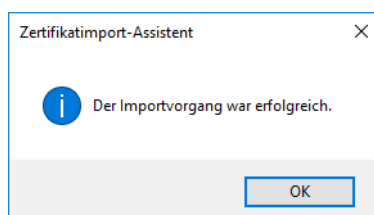


Abb. 24: Zertifikatimport-Assistent

## 4.2

**Sicherheitsausnahme für POWERplay Web konfigurieren**

1. Starten Sie den Browser.
2. Geben Sie die folgende URL in die Adresszeile ein:  
*https://<System-IP>/POWERplayWeb/*
3. Ersetzen Sie in der URL den Parameter <System-IP> durch die IP-Adresse des APP-Servers.
4. Drücken Sie die [Enter]-Taste.  
⇒ Der Anmeldebildschirm erscheint.
5. Melden Sie sich mit Ihrem Benutzernamen und dem Passwort an der Applikation an.  
⇒ Die Applikation wird geöffnet.  
Das folgende Fenster erscheint:

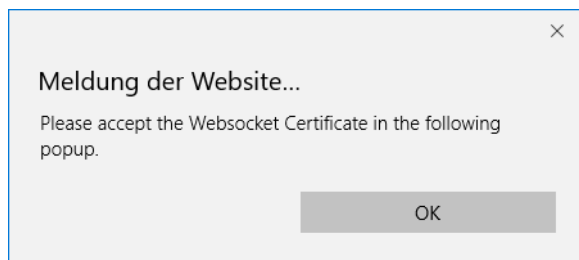


Abb. 25: Websocket-Zertifikat akzeptieren

6. Klicken Sie auf die Schaltfläche OK.  
⇒ Der Startbildschirm der Applikation erscheint.

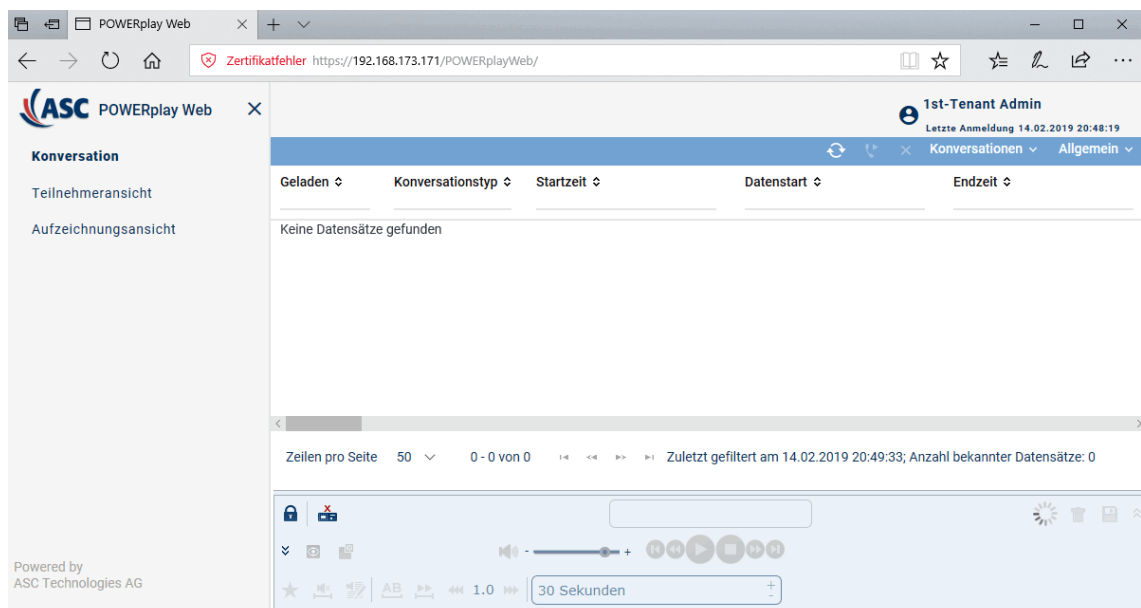


Abb. 26: Startbildschirm

7. Klicken Sie im Hauptbildschirm unten, im Popup-Fenster *Microsoft Edge hat ein Popup ... blockiert* auf die Schaltfläche *Immer zulassen*.
8. Klicken Sie auf *Details*.

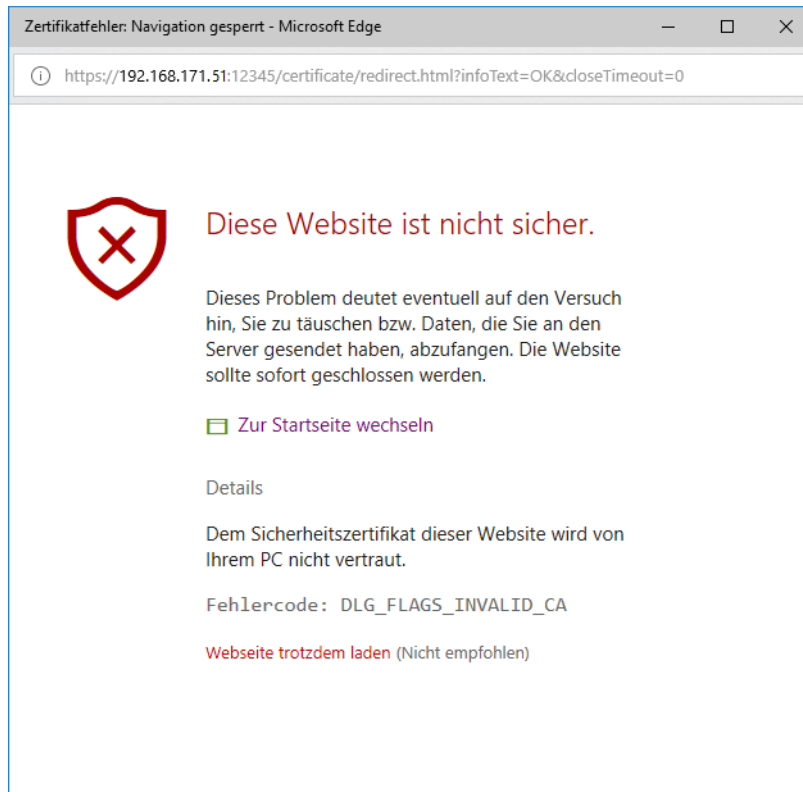



Abb. 27: Mit dieser Webseite fortfahren

9. Klicken Sie auf *Webseite trotzdem laden (Nicht empfohlen)*.
10. Die Serververbindung wird automatisch nach wenigen Sekunden aktualisiert. Sobald die Serververbindung aufgebaut ist, wird im Replay-Modul das Symbol  angezeigt.

## 5 Konfiguration Mozilla Firefox



ASC empfiehlt den Browser Mozilla Firefox ESR zu nutzen.

1. Starten Sie den Browser, um alle im Folgenden beschriebenen Konfigurationen vorzunehmen.

## 5.1 Sicherheitsausnahme für POWERplay Web konfigurieren

1. Geben Sie die folgende URL in die Adresszeile ein:  
`https://<System-IP>/POWERplayWeb/`
2. Ersetzen Sie in der URL den Parameter `<System-IP>` durch die IP-Adresse des APP-Servers.
3. Drücken Sie die [Enter]-Taste.  
⇒ Der Anmeldebildschirm erscheint.
4. Melden Sie sich mit Ihrem Benutzernamen und dem Passwort an der Applikation an.  
⇒ Die Applikation wird geöffnet.  
Das folgende Fenster erscheint:



Abb. 28: Websocket-Zertifikat akzeptieren

5. Klicken Sie auf die Schaltfläche *OK*.
6. Klicken Sie auf die Schaltfläche *Erweitert*.

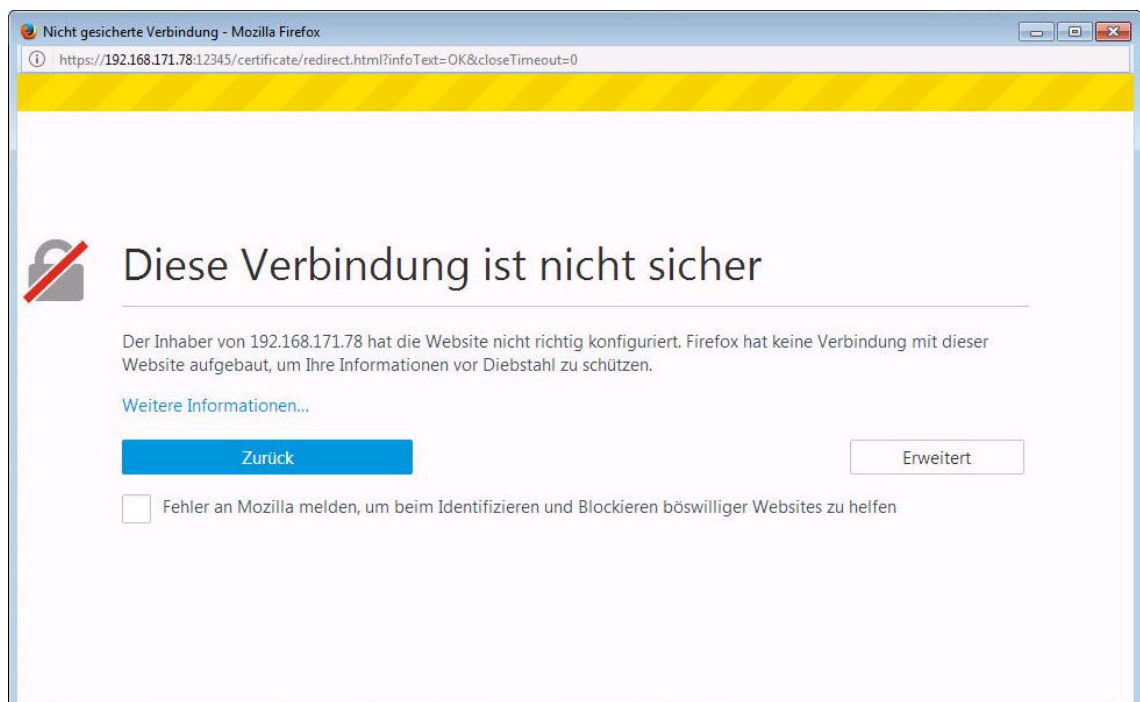


Abb. 29: Nicht gesicherte Verbindung

7. Klicken Sie auf die Schaltfläche *Ausnahme hinzufügen*.

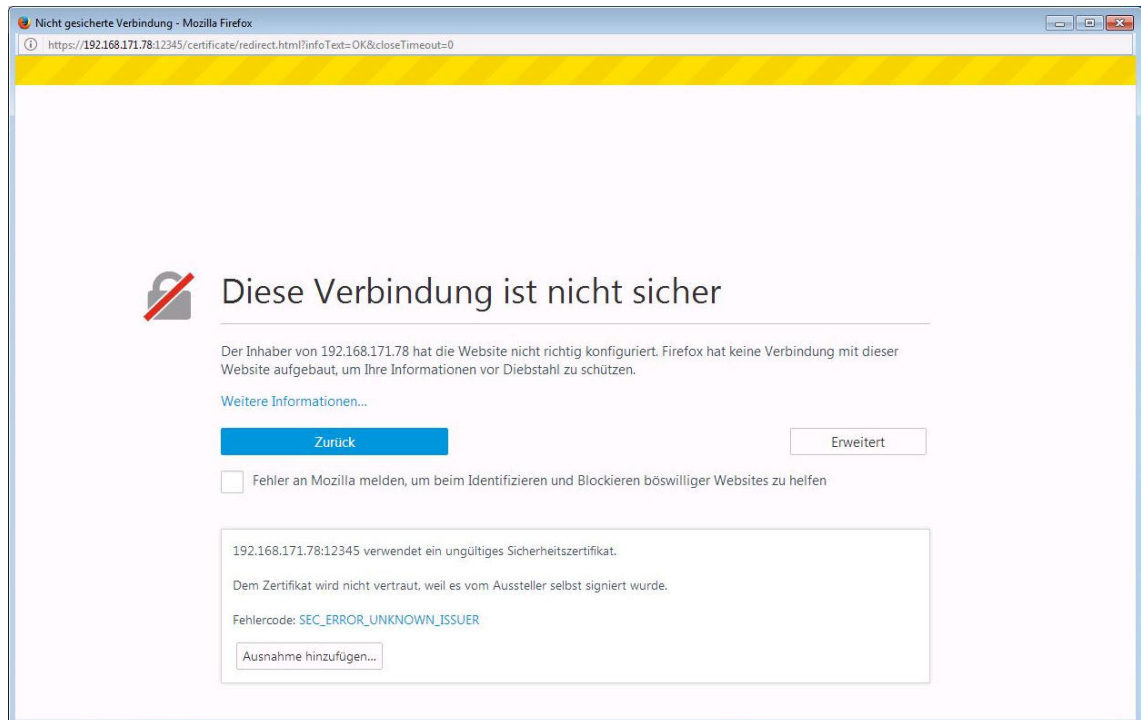


Abb. 30: Nicht gesicherte Verbindung

8. Klicken Sie auf die Schaltfläche *Sicherheits-Ausnahmeregel bestätigen*.

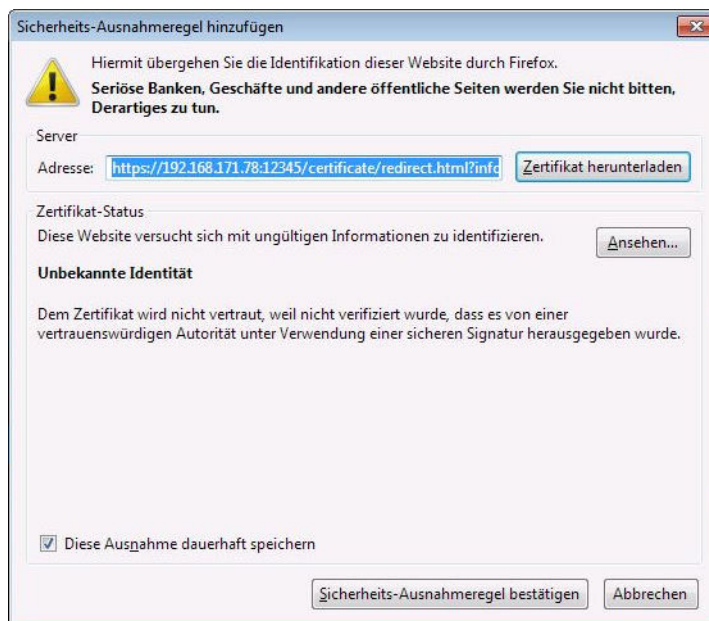



Abb. 31: Sicherheits-Ausnahmeregel bestätigen

9. Klicken Sie in der Applikation auf das Symbol  (Logoff), um die Applikation zu schließen.

## 5.2 Single Sign On konfigurieren

Single Sign On (SSO) funktioniert für alle Webapplikationen nur in einer Domäne. Deshalb müssen alle Rechner in eine entsprechende Windows-Domäne aufgenommen werden.

1. Geben Sie die URL `about:config` ein und betätigen Sie die Enter-Taste.
2. Bestätigen Sie die Sicherheitsabfrage.
3. Geben Sie im Eingabefeld *Suchen* den Wert `network.negotiate-auth.trusted-uris` ein.

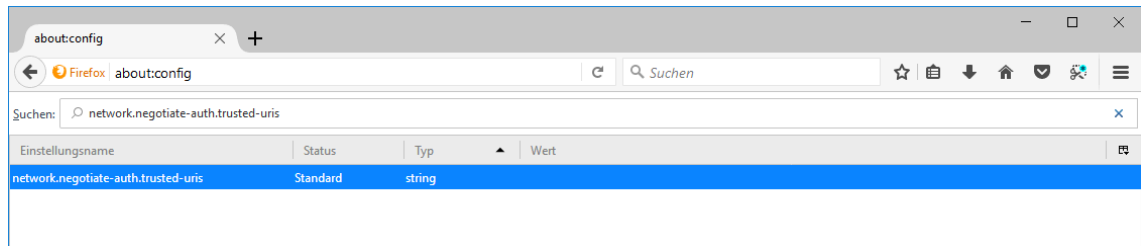


Abb. 32: about:config > network.negotiate-auth.trusted-uris

4. Doppelklicken Sie auf den Einstellungsnamen *network.negotiate-auth.trusted-uris*.
5. Geben Sie im Eingabefeld *network.negotiate-auth.trusted-uris* die URL des APP-Servers ein.

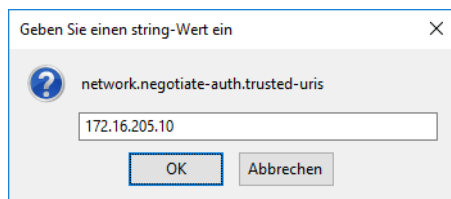



Abb. 33: IP-Adresse eingeben (Beispiel)

6. Klicken Sie auf die Schaltfläche *OK*.

### 5.3 Mozilla Firefox Standard

#### 5.3.1 Pop-up-Blocker konfigurieren

1. Klicken Sie in der rechten oberen Ecke des Fensters auf das Symbol  (*Menü öffnen*).
2. Klicken Sie auf den Menüpunkt *Einstellungen*.

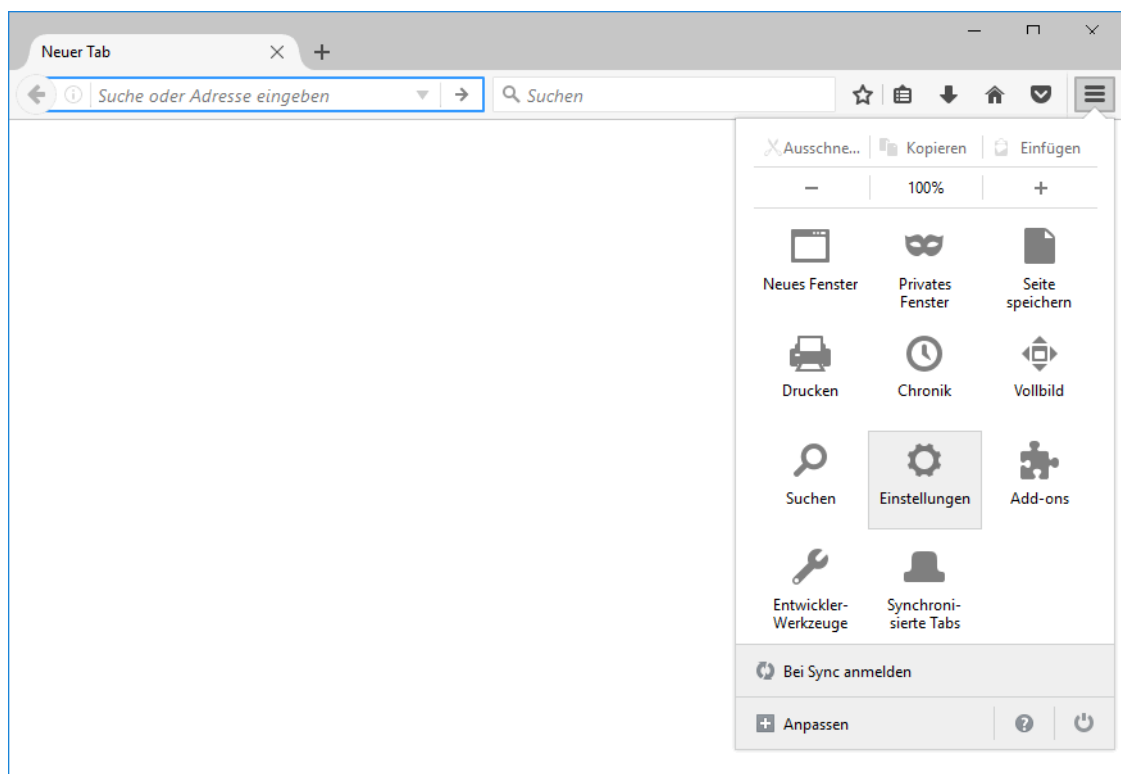


Abb. 34: Firefox > Einstellungen

3. Klicken Sie auf den Menüpunkt *Datenschutz & Sicherheit*.

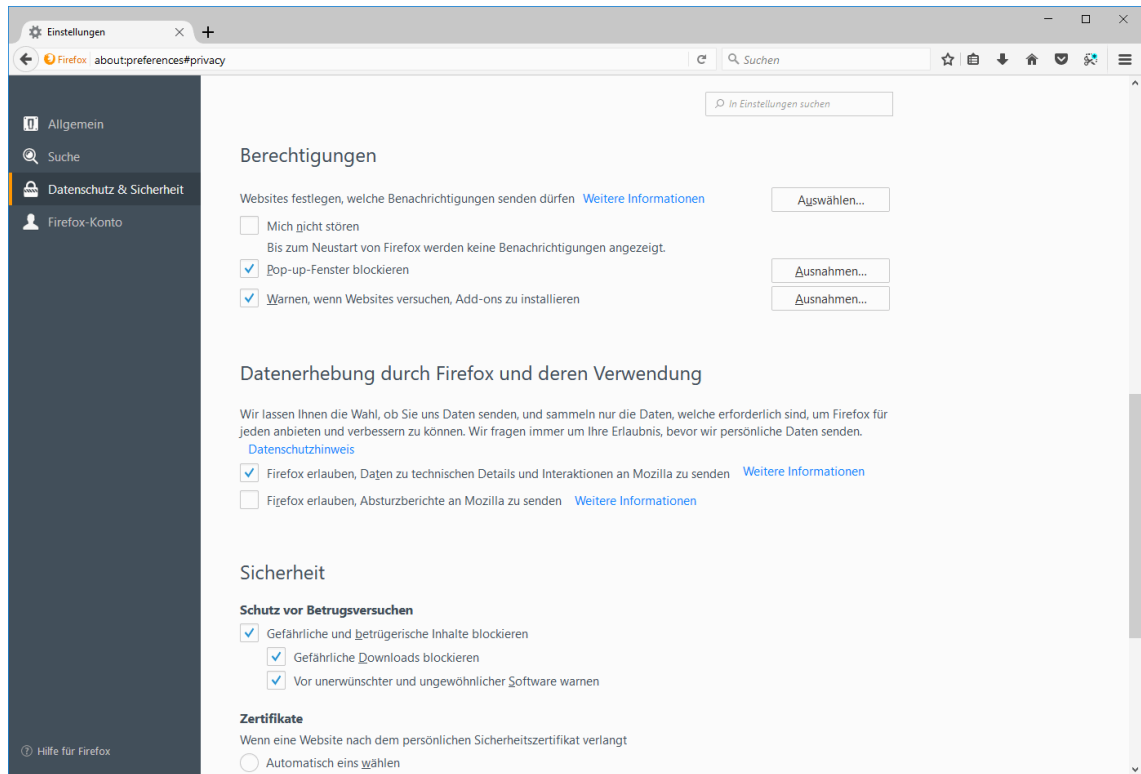


Abb. 35: Registerkarte Inhalt

4. Aktivieren Sie die Option *Pop-up-Fenster blockieren*.  
☒ = Option ist aktiviert.  
☐ = Option ist deaktiviert.
5. Klicken Sie bei *Pop-up-Fenster blockieren* auf die Schaltfläche *Ausnahmen*.
6. Geben Sie im Eingabefeld *Adresse der Website* die URL des APP-Servers ein.

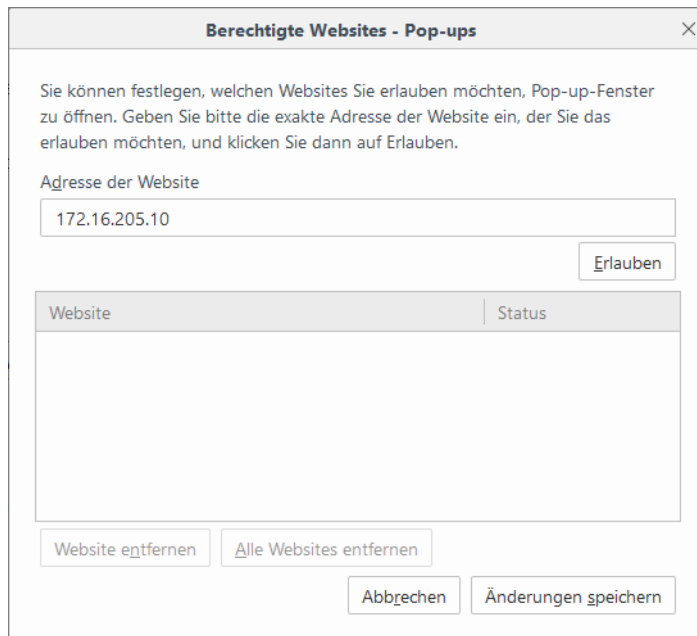



Abb. 36: Berechtigte Websites - Pop-ups (Beispiel)

7. Klicken Sie auf die Schaltfläche *Erlauben*.
8. Klicken Sie auf die Schaltfläche *Änderungen speichern*.



## 5.3.2

## Sicherheitsausnahme hinzufügen

1. Klicken Sie in der rechten oberen Ecke des Fensters auf das Symbol  (Menü öffnen).
2. Klicken Sie auf den Menüpunkt *Einstellungen*.
3. Klicken Sie auf den Menüpunkt *Datenschutz & Sicherheit*.

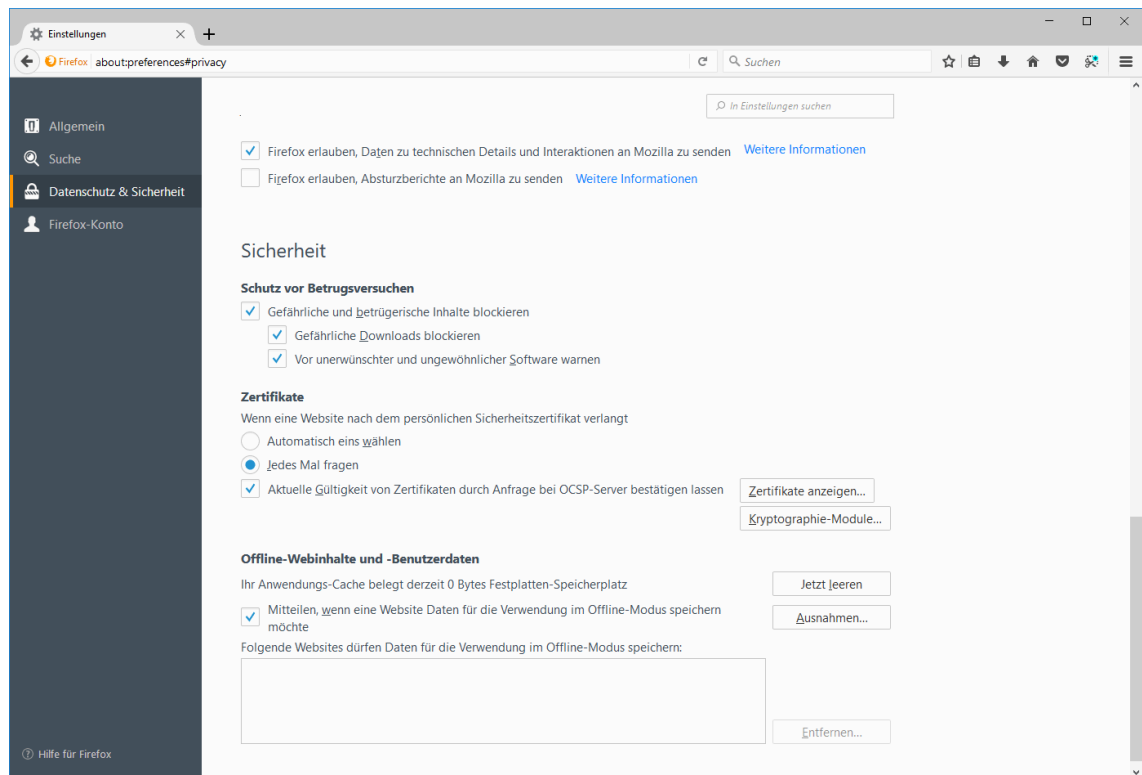


Abb. 37: Verschlüsselung

4. Klicken Sie auf die Schaltfläche *Zertifikate anzeigen*.
5. Klicken Sie auf die Registerkarte *Server*.

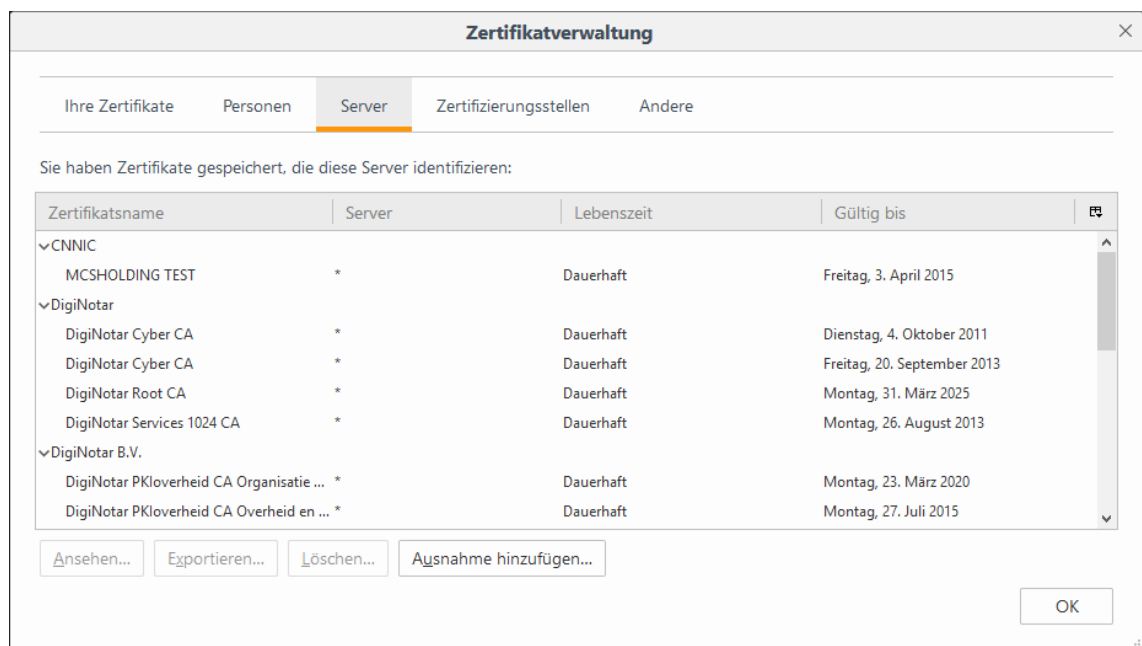



Abb. 38: Zertifikat-Manager

6. Klicken Sie auf die Schaltfläche *Ausnahme hinzufügen*.
7. Geben Sie im Eingabefeld *Adresse* die URL des APP-Servers ein.

8. Klicken Sie auf die Schaltfläche *Zertifikat herunterladen*.
9. Klicken Sie auf die Schaltfläche *Sicherheits-Ausnahmenregel bestätigen*.
10. Klicken Sie auf die Schaltfläche *OK*.

## 5.4 Mozilla Firefox ESR

### 5.4.1 Pop-up-Blocker konfigurieren

1. Klicken Sie in der rechten oberen Ecke des Fensters auf das Symbol  (*Menü öffnen*).
2. Klicken Sie auf den Menüpunkt *Einstellungen*.

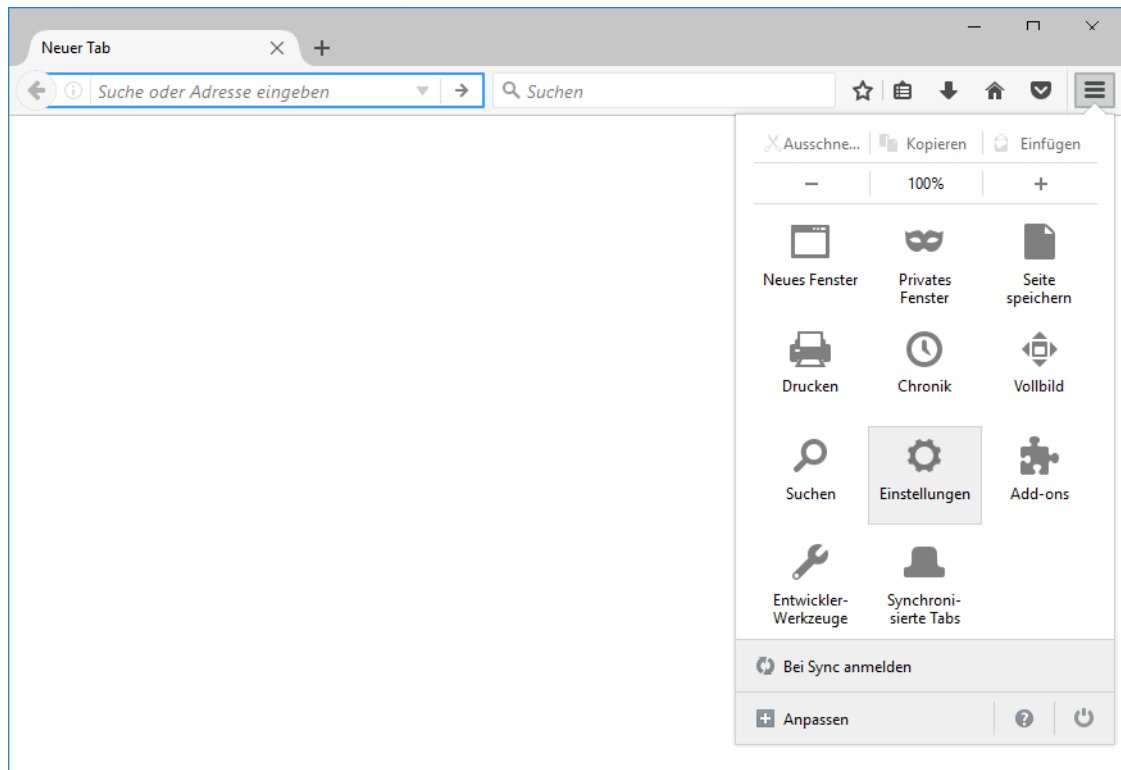


Abb. 39: Firefox > Einstellungen

3. Klicken Sie auf den Menüpunkt *Inhalt*.

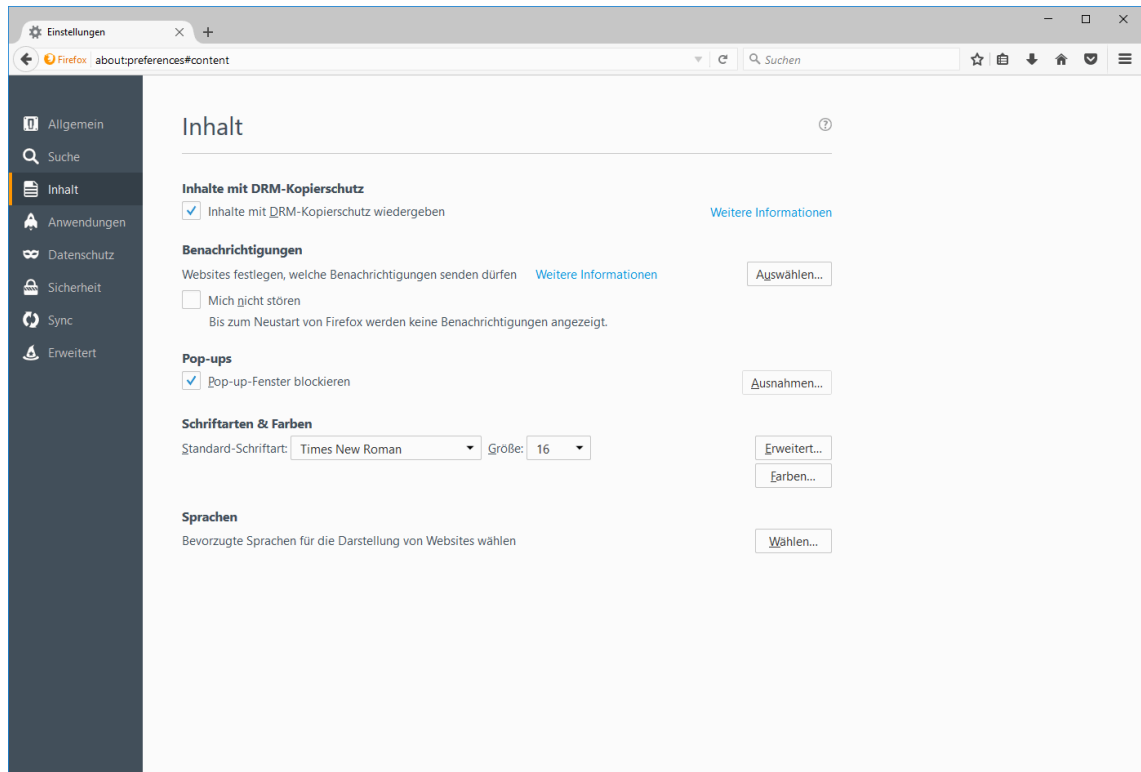


Abb. 40: Inhalt

4. Aktivieren Sie die Option *Pop-up-Fenster blockieren*.  
☒ = Option ist aktiviert.  
☐ = Option ist deaktiviert.
5. Klicken Sie bei *Pop-up-Fenster blockieren* auf die Schaltfläche *Ausnahmen*.
6. Geben Sie im Eingabefeld *Adresse der Website* die URL des APP-Servers ein.

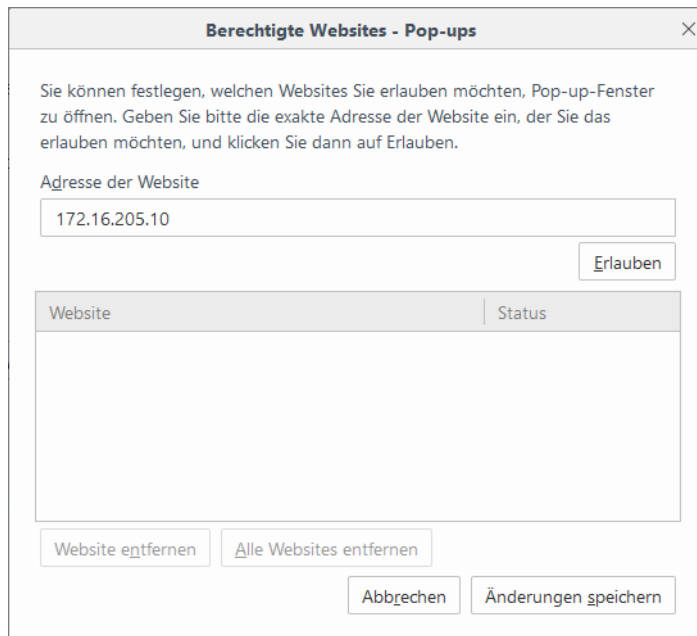



Abb. 41: Berechtigte Websites - Pop-ups (Beispiel)

7. Klicken Sie auf die Schaltfläche *Erlauben*.
8. Klicken Sie auf die Schaltfläche *Änderungen speichern*.

### 5.4.2 Sicherheitsausnahme hinzufügen

1. Klicken Sie in der rechten oberen Ecke des Fensters auf das Symbol  (Menü öffnen).
2. Klicken Sie auf den Menüpunkt *Einstellungen*.
3. Klicken Sie auf den Menüpunkt *Erweitert*.

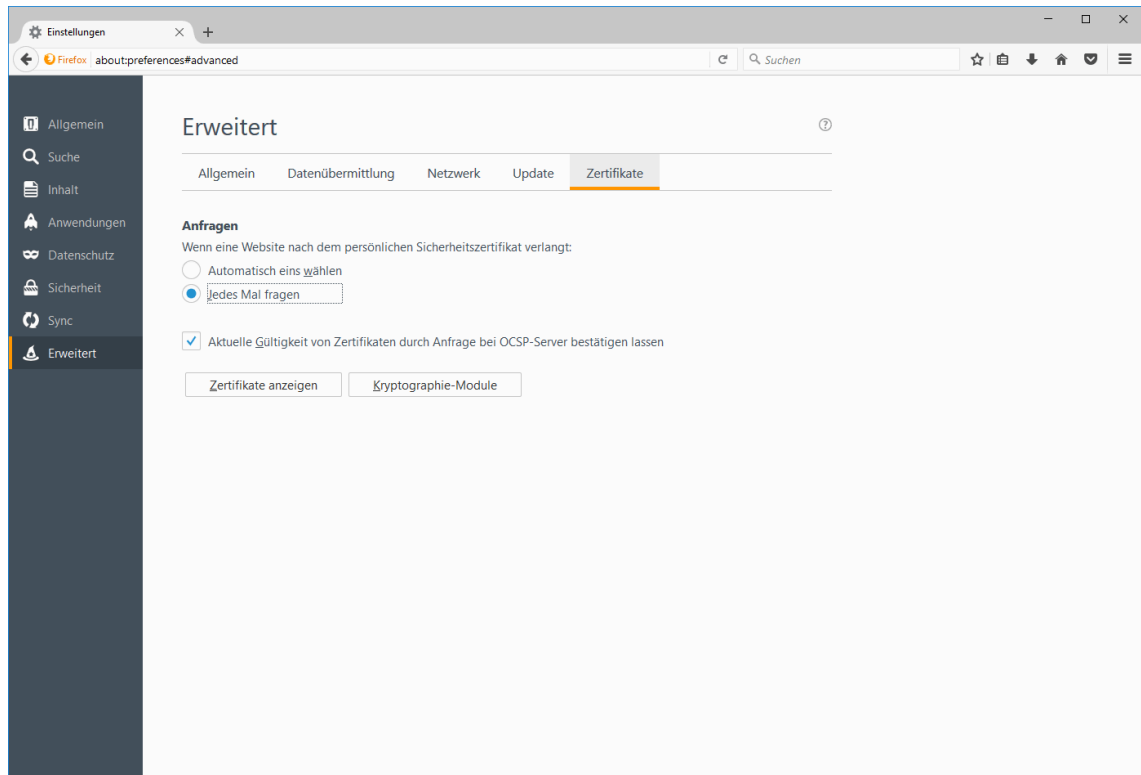


Abb. 42: Zertifikate

4. Klicken Sie auf die Registerkarte *Zertifikate*.
5. Klicken Sie auf die Schaltfläche *Zertifikate anzeigen*.
6. Klicken Sie auf die Registerkarte *Server*.

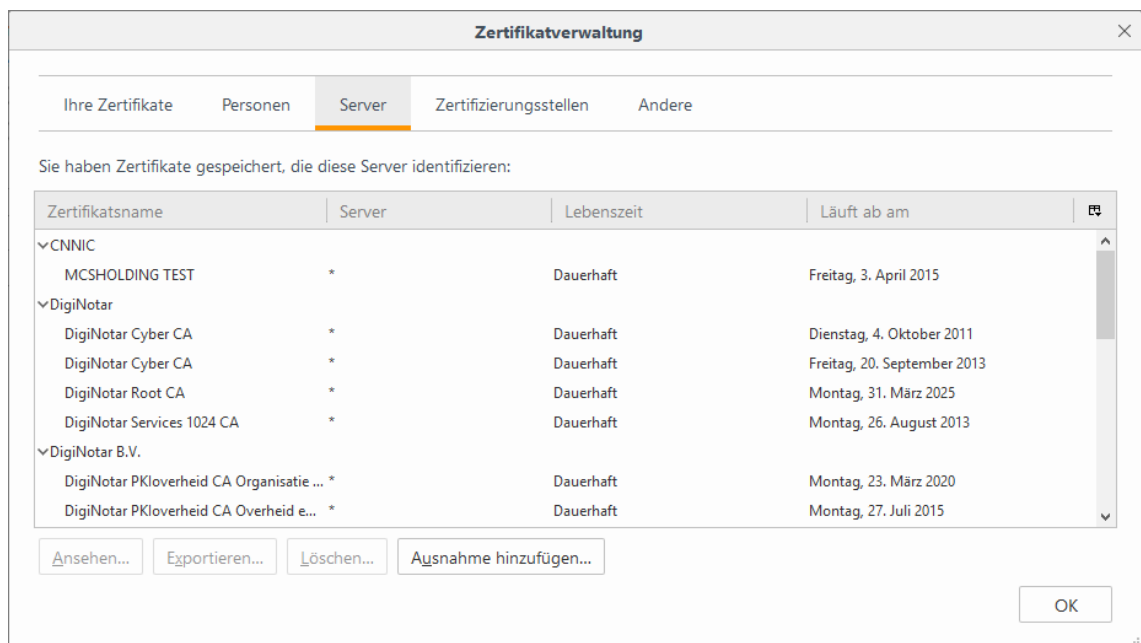


Abb. 43: Zertifikatverwaltung

7. Klicken Sie auf die Schaltfläche *Ausnahme hinzufügen*.

8. Geben Sie im Eingabefeld *Adresse* die [URL](#) des [APP-Servers](#) ein.
9. Klicken Sie auf die Schaltfläche *Zertifikat herunterladen*.
10. Klicken Sie auf die Schaltfläche *Sicherheits-Ausnahmenregel bestätigen*.

## 6 Konfiguration Google Chrome

---

### 6 Konfiguration Google Chrome

Für die Nutzung der ASC-Software mit Google Chrome ist keine spezielle Konfiguration notwendig.


## 7

## Quick Guide

## 7.1

## Konfiguration Internet Explorer Version 11


- Pop-up-Blocker konfigurieren:

 (Extras) > **Internetoptionen** > **Datenschutz** > **Einstellungen** > **Adresse der Website, die zugelassen werden soll:** URL des APP-Servers eingeben > **Hinzufügen** > **Schließen** > **OK**


- Sicherheitsausnahme hinzufügen:

URL des APP-Servers in der Adressleiste eingeben > **Laden dieser Website fortsetzen (nicht empfohlen)** > **Zertifikatsfehler** > **Zertifikate anzeigen** > **Allgemein** > **Zertifikat installieren** > **Weiter** > **Aktueller Benutzer** (Zertifikat nur für den aktuellen Benutzer des Client-PCs) bzw. **Lokaler Computer** (Zertifikat für alle Benutzer des Client-PCs) > **Weiter** > **Alle Zertifikate in folgendem Speicher speichern:** aktivieren > **Durchsuchen** > **Vertrauenswürdige Stammzertifizierungsstellen** > **OK** > **Weiter** > **Fertig stellen** > Sicherheitsabfrage bestätigen.

- Sicherheitsausnahme für POWERplay Web konfigurieren:


URL https://<System-IP>/POWERplayWeb/ eingeben; in der URL den Parameter <System-IP> durch die URL des APP-Servers ersetzen > **Enter-Taste** > An der Applikation anmelden > **OK** > **Laden dieser Website fortsetzen (nicht empfohlen)** > **Zertifikatsfehler** > **Zertifikate anzeigen** > **Allgemein** > **Zertifikat installieren** > **Weiter** > **Aktueller Benutzer** (Zertifikat nur für den aktuellen Benutzer des Client-PCs) bzw. **Lokaler Computer** (Zertifikat für alle Benutzer des Client-PCs) > **Weiter** > **Alle Zertifikate in folgendem Speicher speichern:** aktivieren > **Durchsuchen** > **Vertrauenswürdige Stammzertifizierungsstellen** > **OK** > **Weiter** > **Fertig stellen** > Sicherheitsabfrage bestätigen >  (Logoff).

- Single Sign On konfigurieren:

 (Extras) > **Internetoptionen** > **Erweitert** > **Sicherheit** > **Integrierte WindowsAuthentifizierung aktivieren\***: aktivieren > **Sicherheit** > **Internet** > **Stufe anpassen** > **Benutzerauthentifizierung** > **Anmeldung** > **Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort** > **OK** > **OK**.

- Kompatibilitätsansicht konfigurieren:

Internet Explorer Version 11:

 (Extras) > **Einstellungen der Kompatibilitätsansicht** > sicher stellen, dass der Kompatibilitätsmodus für den APP-Server deaktiviert ist; URL des APP-Servers darf nicht aufgelistet sein > **Intranetsites in Kompatibilitätsansicht anzeigen:** deaktivieren > **Kompatibilitätslisten von Microsoft verwenden:** deaktivieren > **Schließen**.

## 7.2

## Konfiguration Microsoft Edge

- Zertifikat installieren:

Zertifikat mit dem Browser Internet Explorer installieren:

Browser Internet Explorer starten > URL des APP-Servers in der Adressleiste eingeben > **Laden dieser Website fortsetzen (nicht empfohlen)** > **Zertifikatsfehler** > **Zertifikate anzeigen** > **Allgemein** > **Zertifikat installieren** > **Weiter** > **Aktueller Benutzer** (Zertifikat nur für den aktuellen Benutzer des Client-PCs) bzw. **Lokaler Computer** (Zertifikat für alle Benutzer des Client-PCs) > **Weiter** > **Alle Zertifikate in folgendem Speicher speichern:** aktivieren > **Durchsuchen** > **Vertrauenswürdige Stammzertifizierungsstellen** > **OK** > **Weiter** > **Fertig stellen** > Sicherheitsabfrage bestätigen.

oder

Zertifikat vom APP-Server auf den Client-Rechner kopieren und installieren:

Vom APP-Server die Datei C:\Program Files (x86)\ASC\ASC Product Suite\data\crypto\https.crt auf den Desktop des Client-Rechners kopieren > auf dem Desktop

des Client-Rechners mit rechter Maustaste auf Icon der Datei **https.crt** klicken > **Zertifikat installieren** > **Weiter** > **Aktueller Benutzer** (Zertifikat nur für den aktuellen Benutzer des Client-PCs) bzw. **Lokaler Computer** (Zertifikat für alle Benutzer des Client-PCs) > **Weiter** > **Alle Zertifikate in folgendem Speicher speichern: aktivieren** > **Durchsuchen** > **Vertrauenswürdige Stammzertifizierungsstellen** > **OK** > **Weiter** > **Fertig stellen** > **Ja** > **OK**.


- Sicherheitsausnahme für POWERplay Web konfigurieren:

Browser Microsoft Edge starten > **URL** <https://<System-IP>/POWERplayWeb/> eingeben; in der **URL** den Parameter <System-IP> durch die **URL** des **APP-Servers** ersetzen > **Enter-Taste** > An der Applikation anmelden > **OK** > **Immer zulassen** > **Details** > **Webseite trotzdem laden (Nicht empfohlen)**.

### 7.3

#### Konfiguration Mozilla Firefox

- Sicherheitsausnahme für POWERplay Web konfigurieren:


**URL** <https://<System-IP>/POWERplayWeb/> eingeben; in der **URL** den Parameter <System-IP> durch die **URL** des **APP-Servers** ersetzen > **Enter-Taste** > An der Applikation anmelden > **OK** > **Erweitert** > **Ausnahme hinzufügen** > **Sicherheits-Ausnahmeregel bestätigen** >  (*Logoff*).

- Single Sign On konfigurieren:


**URL** <about:config> eingeben > **Enter-Taste** > Sicherheitsabfrage bestätigen > **Suchen:** [network.negotiate-auth.trusted-uris](#) eingeben > Doppelklick auf den Einstellungsnamen **network.negotiate-auth.trusted-uris** > **URL** des **APP-Servers** eingeben > **OK**.

#### Mozilla Firefox Standard

- Pop-up-Blocker konfigurieren:


 (*Menü öffnen*) > **Einstellungen** > **Datenschutz & Sicherheit** > **Pop-up-Fenster blockieren: aktivieren** > **Ausnahmen** > **URL** des **APP-Servers** eingeben > **Erlauben** > **Änderungen speichern**.

- Sicherheitsausnahme hinzufügen:

 (*Menü öffnen*) > **Einstellungen** > **Datenschutz & Sicherheit** > **Zertifikate anzeigen** > **Server** > **Ausnahme hinzufügen** > **URL** des **APP-Servers** eingeben > **Zertifikat herunterladen** > **Sicherheits-Ausnahmenregel bestätigen** > **OK**.

#### Mozilla Firefox ESR

- Pop-up-Blocker konfigurieren:

 (*Menü öffnen*) > **Einstellungen** > **Inhalt** > **Pop-up-Fenster blockieren: aktivieren** > **Ausnahmen** > **URL** des **APP-Servers** eingeben > **Erlauben** > **Änderungen speichern**.

- Sicherheitsausnahme hinzufügen:

 (*Menü öffnen*) > **Einstellungen** > **Erweitert** > **Zertifikate** > **Zertifikate anzeigen** > **Server** > **Ausnahme hinzufügen** > **URL** des **APP-Servers** eingeben > **Zertifikat herunterladen** > **Sicherheits-Ausnahmenregel bestätigen**.



## Abbildungsverzeichnis

Abb. 1	Registerkarte Datenschutz .....	6
Abb. 2	Popupblockereinstellungen (Beispiel) .....	7
Abb. 3	Laden dieser Website fortsetzen .....	7
Abb. 4	Zertifikat .....	8
Abb. 5	Zertifikatimport-Assistent .....	8
Abb. 6	Zertifikatspeicher auswählen .....	9
Abb. 7	Zertifikatimport-Assistent .....	9
Abb. 8	Websocket-Zertifikat akzeptieren .....	10
Abb. 9	Laden dieser Website fortsetzen .....	10
Abb. 10	Zertifikat .....	11
Abb. 11	Zertifikatimport-Assistent .....	11
Abb. 12	Zertifikatspeicher auswählen .....	12
Abb. 13	Zertifikatimport-Assistent .....	12
Abb. 14	Registerkarte Erweitert .....	13
Abb. 15	Registerkarte Sicherheit .....	13
Abb. 16	Sicherheitseinstellungen - Internetzone .....	14
Abb. 17	Internet Explorer > Einstellungen der Kompatibilitätsansicht .....	14
Abb. 18	Einstellungen der Kompatibilitätsansicht (Beispiel) .....	15
Abb. 19	Zertifikat installieren .....	16
Abb. 20	Zertifikatimport-Assistent .....	17
Abb. 21	Zertifikatspeicher auswählen .....	17
Abb. 22	Zertifikatimport-Assistent .....	18
Abb. 23	Sicherheitswarnung .....	18
Abb. 24	Zertifikatimport-Assistent .....	18
Abb. 25	Websocket-Zertifikat akzeptieren .....	19
Abb. 26	Startbildschirm .....	19
Abb. 27	Mit dieser Webseite fortfahren .....	20
Abb. 28	Websocket-Zertifikat akzeptieren .....	21
Abb. 29	Nicht gesicherte Verbindung .....	21
Abb. 30	Nicht gesicherte Verbindung .....	22
Abb. 31	Sicherheits-Ausnahmeregel bestätigen .....	22
Abb. 32	about:config > network.negotiate-auth.trusted-uris .....	23
Abb. 33	IP-Adresse eingeben (Beispiel) .....	23
Abb. 34	Firefox > Einstellungen .....	23
Abb. 35	Registerkarte Inhalt .....	24
Abb. 36	Berechtigte Websites - Pop-ups (Beispiel) .....	24
Abb. 37	Verschlüsselung .....	25
Abb. 38	Zertifikat-Manager .....	25
Abb. 39	Firefox > Einstellungen .....	26
Abb. 40	Inhalt .....	27
Abb. 41	Berechtigte Websites - Pop-ups (Beispiel) .....	27

---

Abb. 42	Zertifikate .....	28
Abb. 43	Zertifikatverwaltung .....	28

---

### 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.

### **SSO**

---

Single Sign On; Vereinfachtes Login-Verfahren. Nach einer einmaligen Authentifizierung an einem Arbeitsplatz kann der Benutzer an diesem Arbeitsplatz alle Dienste und Applikationen nutzen, für die er autorisiert ist. Er muss sich an den einzelnen Applikationen nicht erneut authentifizieren.

### **URL**

---

Uniform Resource Locator. Identifiziert und lokalisiert eine Ressource (z. B. eine Website) über die zu verwendende Zugriffsmethode (z. B. das verwendete Netzwerkprotokoll wie HTTP oder FTP) und den Ort der Ressource in Computernetzwerken. (Quelle: Wikipedia 20.11.2013)