

IT- und Medienzentrum

Stand: 04.06.2018

WEBVPN UND SSL NETWORK EXTENDER

Anleitung für Studierende

INHALT

Allgemeines.....	3
Voraussetzungen	3
Anmeldung Mobiler Webzugang.....	3
Mobiler Webzugang – Bereich Web	4
SSL Network Extender	7
Installation im Internet Explorer.....	8
Hinweis zu Windows Browser Edge.....	10
Installation im Mozilla Firefox	12
Installation im Safari unter Mac OS X	16
Verbindungsaufbau.....	23
Häufige Fragen - FAQ:	24
Kontakt.....	24
Abbildungsverzeichnis:.....	25

Allgemeines

Das Webportal der Hochschule RheinMain eröffnet einen einfachen Zugang zu Daten im Internet, die ausschließlich aus dem Hochschulnetz erreichbar sind. So können beispielsweise E-Books oder elektronische Datenbanken über das Portal abgerufen werden.

Das neue WebVPN steht ab sofort allen Studierenden der Hochschule zur Verfügung und kann mit allen gängigen Browsern, mit Ausnahme von Microsoft Edge, genutzt werden.

Voraussetzung: Die Installation von Java 8 in der 32-bit Version!

Voraussetzungen

1. Aktive Internetverbindung
2. HDS-Account aktiviert
3. Verwenden sie nicht das Masterpasswort, sondern das selbst vergebene Passwort
4. Ihr Passwort sollte keine Sonderzeichen, wie z.B. !,? und dergleichen enthalten

Anmeldung Mobiler Webzugang

Sie erreichen die Seite des WebVPN der Hochschule RheinMain unter

<https://webvpn.hs-rm.de>



Abbildung 1:Anmeldung

Auf dieser Seite melden sich Studierende mit ihrem HDS-Account an.

Mobiler Webzugang – Bereich Web

Nach dem Login stehen Ihnen dort u.a. Links zu den Online-Angeboten der HLB zur Verfügung.



Abbildung 2:Webzugriff

Weitere Webseiten können durch Eingabe der URL in das entsprechende Textfeld auf dieser Seite im Feld „Adresse“ geladen und angezeigt werden.

Eine zusätzliche VPN-Verbindung ist damit nicht mehr erforderlich.

Über die Option „Favoriten“ können Sie sich beliebige Links auf Internetseiten setzen, die Sie dann zukünftig automatisch in der Liste angezeigt bekommen.

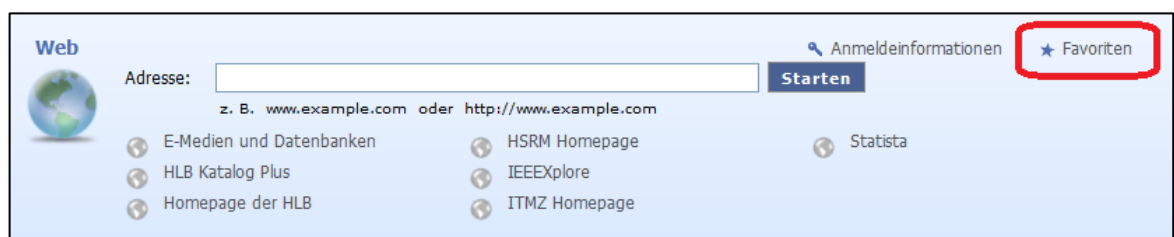


Abbildung 3:Favoriten

Hierzu klicken Sie auf die Schaltfläche „Hinzufügen“.



Abbildung 4:Webfavoriten

In der folgenden Eingabemaske tragen Sie die URL und die Bezeichnung ein. Optional auch den Tooltip, der erscheinen soll, wenn der Mauszeiger über dem Eintrag steht.



The screenshot shows the 'Webfavoriten hinzufügen' form. It has three input fields: 'Bezeichnung' with the value 'Eigener Link', 'URL' with the value 'http://www.beispiel.de' and a note 'z. B. www.example.com oder http://www.example.com', and 'Tooltip' with the value 'Selbst erstellter Link'. There are 'OK' and 'Abbrechen' buttons at the bottom.

Abbildung 5:Webfavoriten hinzufügen

Nach der Bestätigung mit „OK“ sehen Sie den neuen Link in der Liste der Webfavoriten.



Abbildung 6:Webfavoriten hinzufügen

Wenn Sie jetzt wieder zur Startseite zurückgehen, befindet sich der neue Link in der Liste unterhalb des Feldes „Adresse“.

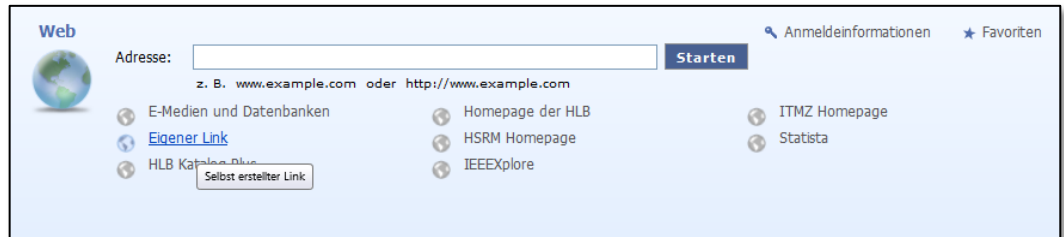


Abbildung 7: Eigene Webfavoriten

Um einen einmal angelegten Link wieder zu entfernen, gehen Sie wieder in die Seite der Webfavoriten, markieren Sie den zu entfernenden Link und klicken Sie auf „Entfernen“

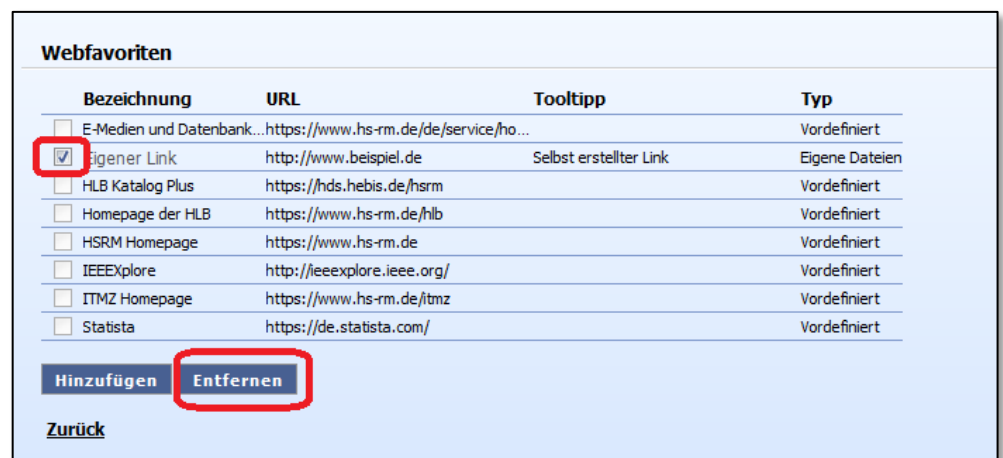


Abbildung 8: Webfavoriten entfernen

Sie können nur selbst erstellte Links löschen.

SSL Network Extender

Um im Hochschulnetz arbeiten zu können, d.h. auf Laufwerke oder auf Datenbank-Systeme wie <https://de.statista.com>, <https://www.wiso-net.de> oder <https://ieeexplore.ieee.org> zu zugreifen, benötigen Sie eine SSL Verbindung ins Hochschulnetz.

Hierzu müssen Sie über die Schaltfläche „Verbindung aufnehmen“ den SSL Network Extender starten.



Abbildung 9: Verbindung starten

Je nach verwendetem Browser muss bei der ersten Verbindung Software (Web-VPN - SSL Network Extender (SNX)) installiert werden. Die einzelnen Schritte entnehmen Sie bitte den folgenden Kapiteln.

Da die Installation in allen Betriebssystemen grundlegend gleich verlaufen und nur abhängig vom eingesetzten Browser sind, werden im Folgenden die Schritte unter Windows 10 bzw. MAC OS X pro Browser erläutert.

PROBLEM BEIM AUFRUFEN VON ONLINEMEDIEN UND DATENBANK-SEITEN

Bei Problemen die folgenden Seiten direkt über das WebVPN-Portal aufzurufen gibt es eine einfache Lösung. Für den Zugriff auf Datenbank-Systeme wie <https://de.statista.com>, <https://www.wiso-net.de> oder <https://ieeexplore.ieee.org> benötigen Sie unbedingt eine SSL (🔒) Verbindung ins Hochschulnetz.

Starten Sie die „SSL-Verbindung“ über „🔒 Verbindung aufnehmen“.

Bitte verwenden Sie nun **nicht** das vorhandene Web-Adressfeld, sondern öffnen Sie hierfür bitte ein neues, separates Browser-Fenster in dem gleichen Webbrowser, in dem auch die WebVPN & SSL-Network Extender Verbindung geöffnet ist, geben Sie dort in der Adresszeile nun den gewünschten Link ein!

Installation im Internet Explorer

Die SNX Installation über den Internet Explorer erfolgt mittels Active-X. Nach dem Starten des Verbindungsprozesses über die Schaltfläche „Verbindung aufnehmen“ folgt ein Hinweis auf die Installation eines Add-On.

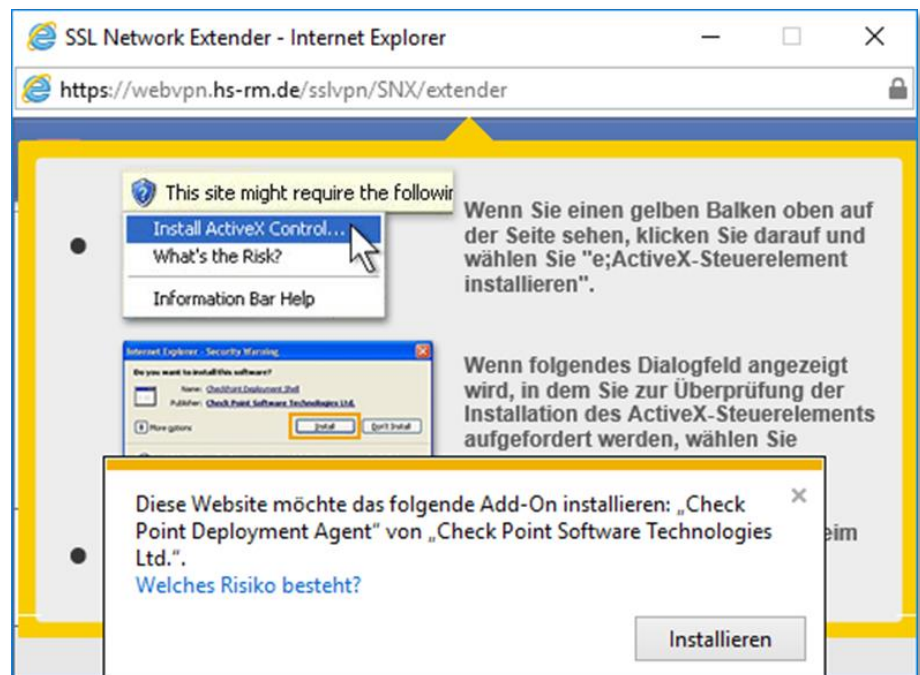


Abbildung 10: Add-On installieren

Bitte installieren Sie das Add-On „Check Point Deployment Agent“. Sollte die Installation nicht angeboten werden, so müssen Sie zunächst ActiveX aktivieren. Wie dies geschieht, ist ebenfalls in dem Popup beschrieben.

Ein weiteres Popup Fenster öffnet sich, welches Sie mit „Trust Server“ bestätigen müssen

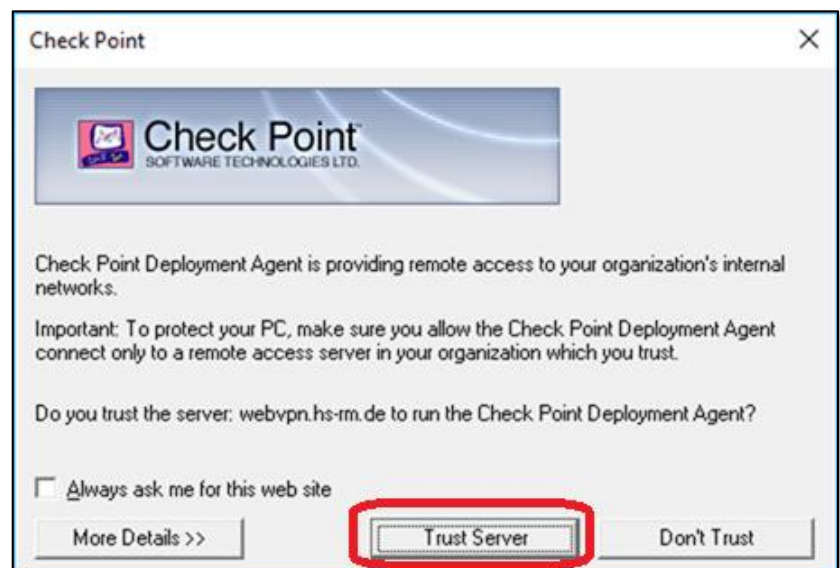


Abbildung 11: Check Point Abfrage

Die Installation müssen Sie ggf. mit dem Button „Zulassen“ bestätigen.

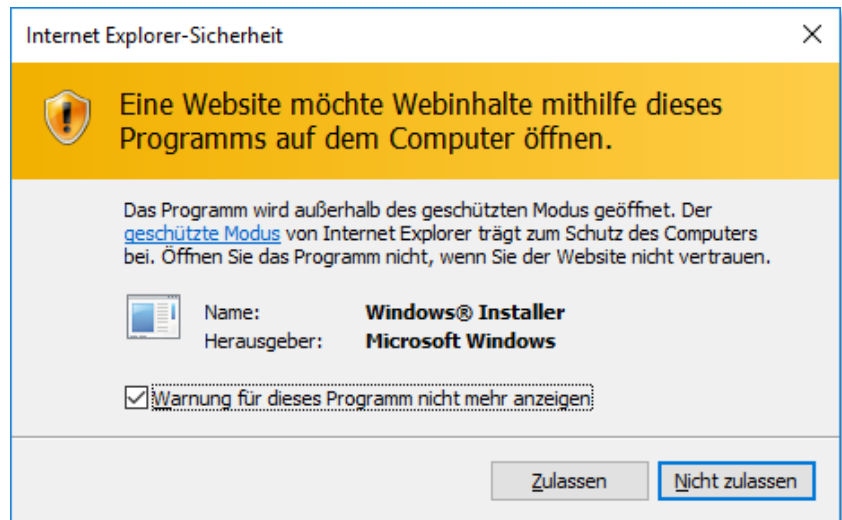


Abbildung 12: Sicherheitsabfrage

Daraufhin wird die Installation ausgeführt.

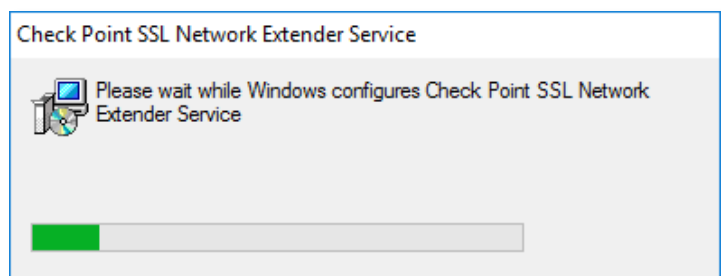


Abbildung 13: Installationsfortschritt

Nach der Installation müssen Sie ggf. die Windows Firewall freigeben, so dass die Verbindung gestartet werden kann.

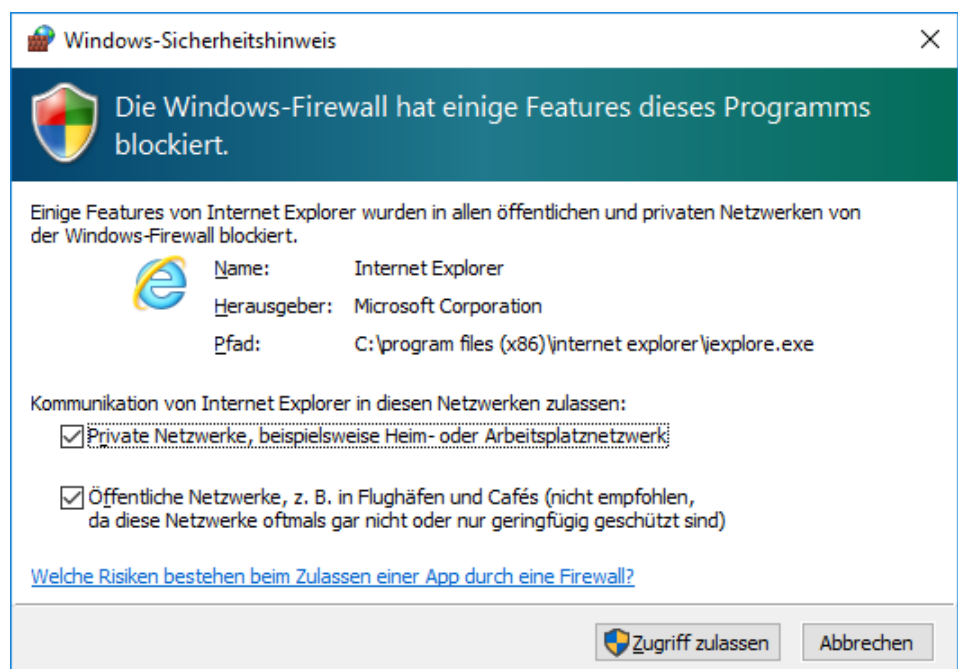


Abbildung 14: Windows Firewall

Nach der erfolgreichen Installation wird die Verbindung automatisch gestartet.

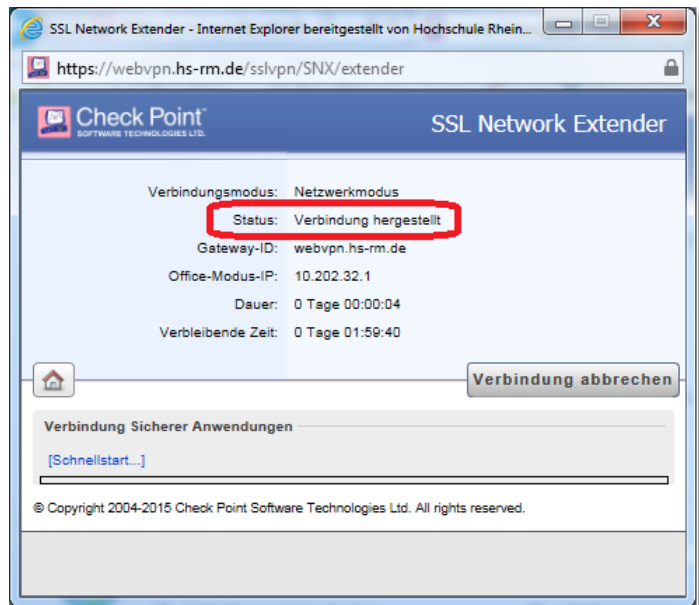


Abbildung 15: Automatischer Verbindungsaufbau

HINWEIS ZU WINDOWS BROWSER EDGE

Sollte die Verbindung unter Windows Edge nicht zustande kommen, melden Sie sich ab. Wenn Sie die Anmeldeseite von WebVPN sehen gehen Sie wie folgt vor: Klicken Sie hierzu zunächst auf das Symbol oben rechts in ihrem Edge Browser wie in Abbildung 16 zu sehen.

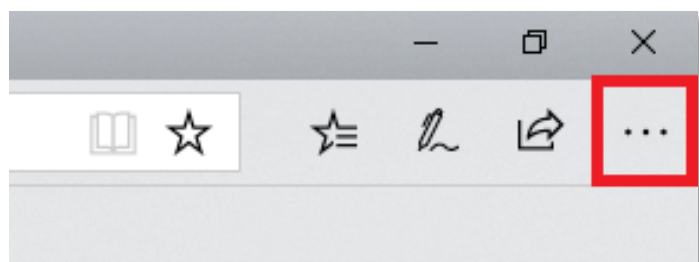


Abbildung 16: In Edge den Internet Explorer aufrufen

Klicken Sie auf „Mit Internet Explorer öffnen“. Die Anmeldeseite des WebVPN öffnet sich nun im Internet Explorer.

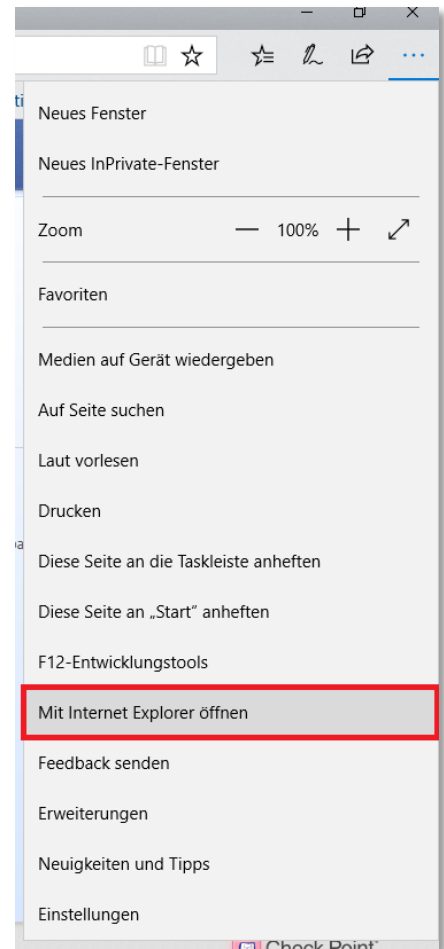


Abbildung 17: Seite mit Internet Explorer öffnen

Folgen Sie den Schritten wie in „Installation im Internet Explorer“ beschrieben fort.

Installation im Mozilla Firefox

Für die Benutzung des SSL Network Extenders mit Mozilla Firefox wird Oracle Java benötigt. Gehen Sie hierzu auf www.java.com und laden sich das aktuelle Java Runtime Environment in der 32 Bit Version für Windows herunter.

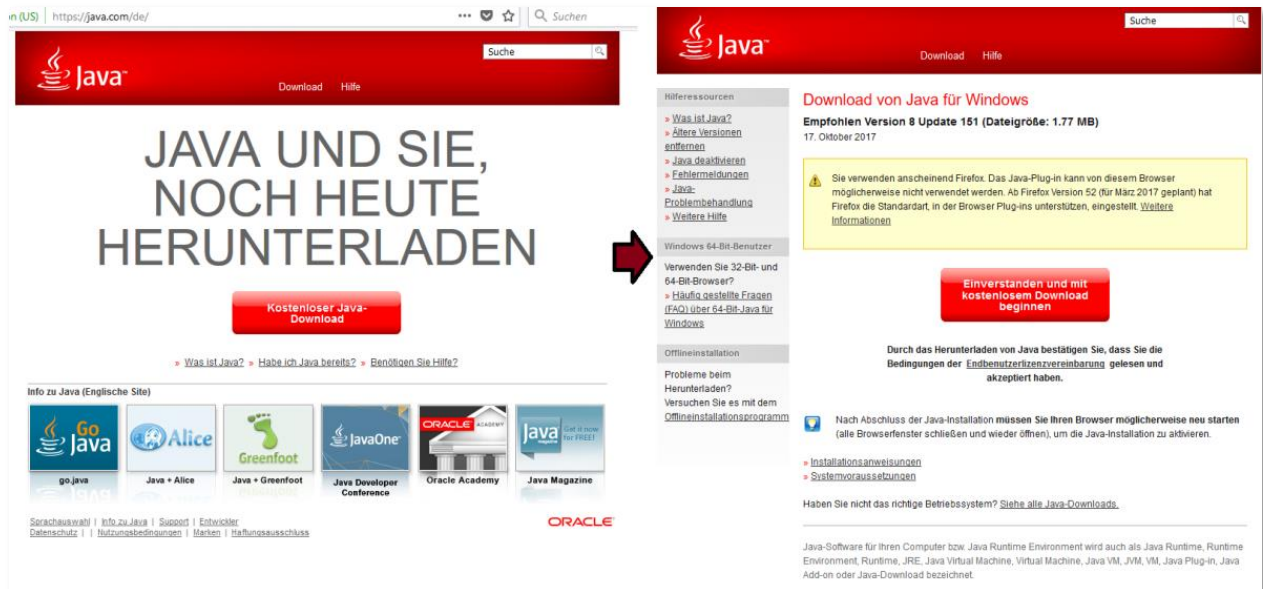


Abbildung 18: Java Download

Installieren Sie das heruntergeladene Paket mit der Installationsroutine. Achten Sie darauf nur Java zu installieren. Wählen Sie Bloatware jeglicher Art ab, sofern Sie es nicht explizit installieren möchten.



Abbildung 19: Java Installation

Bitte starten Sie Ihren Browser nach erfolgreicher Installation neu!

Nach erfolgreicher Java-Installation müssen Sie die Erstkonfiguration ausführen. Hierfür melden Sie sich mit Ihrer Nutzerkennung auf der Startseite des mobilen Webzugangs der Hochschule RheinMain an.

<https://webvpn.hs-rm.de>



Abbildung 20: Anmeldung zur Erstkonfiguration

Nach der Anmeldung starten Sie per „Verbindung aufnehmen“ den Verbindungsprozess, sofern sich nicht automatisch ein Popup Fenster geöffnet hat.



Abbildung 21: Verbindungsprozess

Im nächsten Schritt kann der SSL Network Extender heruntergeladen und installiert werden.



Abbildung 22: Installation Check Point Deployment-Agent

Gehen Sie auf den Link um die CckeckPointMobileAgent.msi herunterzuladen und führen dann, nach erfolgtem herunterladen, Sie die Installationsdatei aus. Hier werden Sie gefragt, ob Sie die Installationsdatei wirklich ausführen wollen, was einfach mit „OK“ bestätigt werden kann, um zum nächsten Schritt zu kommen.

Nun kommt eine Sicherheitswarnung, die Sie mit „Ja“ bestätigen, dass Zertifikat dieser Zertifizierungsstelle dient der Absicherung der Kommunikation der Komponenten des SSL Network Extender, der darin enthaltene Fingerabdruck wird bei jeder Installation neu generiert.

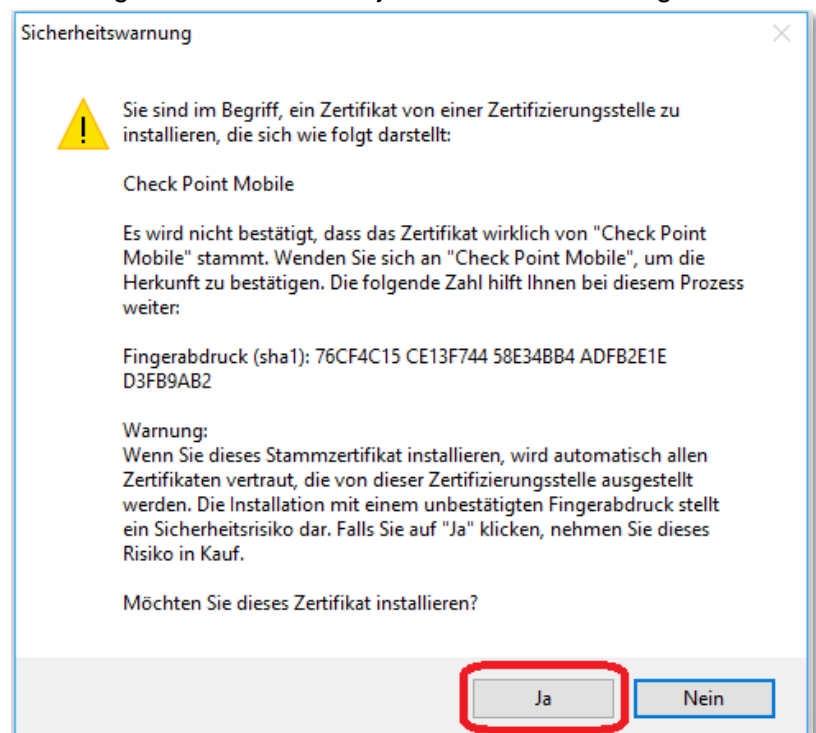


Abbildung 23: Sicherheitswarnung

Mit „Trust Server“ schließen Sie die Konfiguration ab.

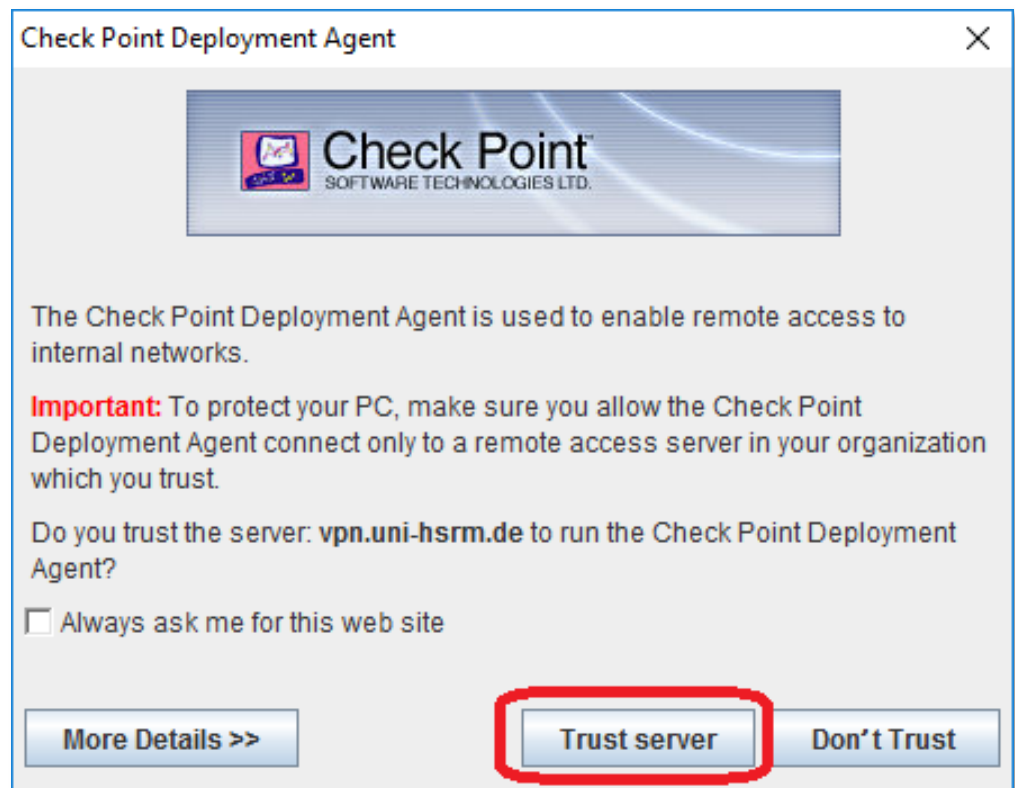


Abbildung 24: Trust Server Abfrage

Nach der Installation wird die Verbindung automatisch gestartet.

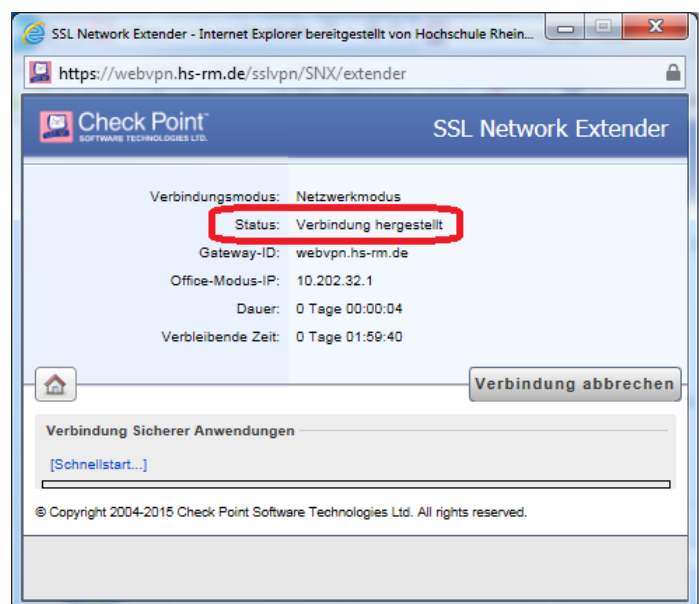


Abbildung 25: Verbindungsaufbau

Installation im Safari unter Mac OS X

Die Web-VPN - SSL Network Extender (SNX) - Installation wird im Browser Safari unter MAC OS X folgendermaßen vorgenommen.

Für die Benutzung des SSL Network Extenders wird Oracle Java benötigt. Gehen Sie hierzu auf www.java.com und laden sich das aktuelle Java Runtime Environment für MAC OS herunter.

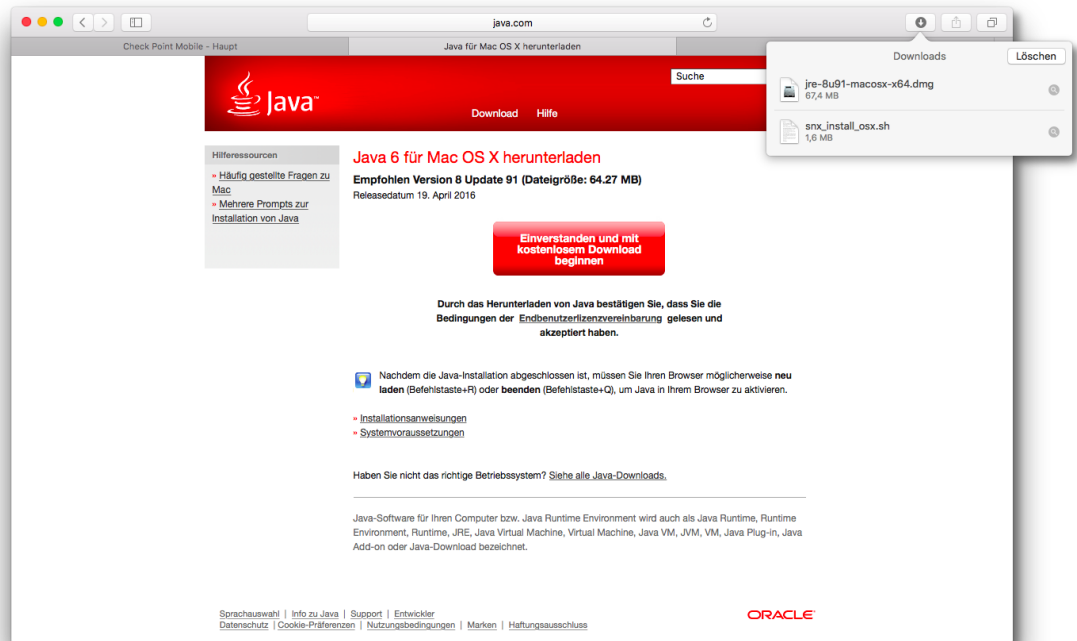


Abbildung 26:Java für Mac OS X

Öffnen Sie die heruntergeladene DMG-Datei und starten die Installation mit einem Doppelklick.



Abbildung 27:Installation Java für Mac OS X

Bestätigen Sie im nächsten Schritt das Ausführen der Installation. Gegebenenfalls müssen Sie im nächsten Schritt Ihre lokalen Zugangsdaten angeben.

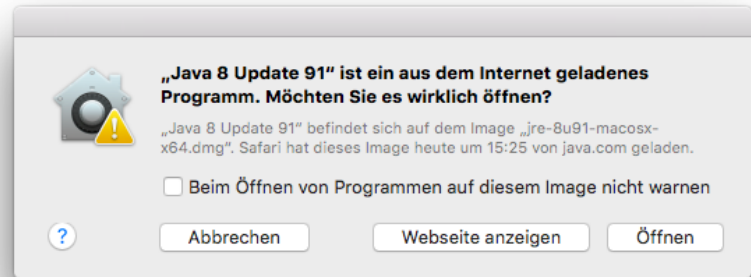


Abbildung 28:Java für Mac OS X

Nach erfolgreicher Java-Installation müssen Sie die Erstkonfiguration ausführen. Hierfür melden Sie sich mit Ihrer Nutzerkennung auf der Startseite des mobilen Webzugangs der Hochschule RheinMain an.

<https://webvpn.hs-rm.de>

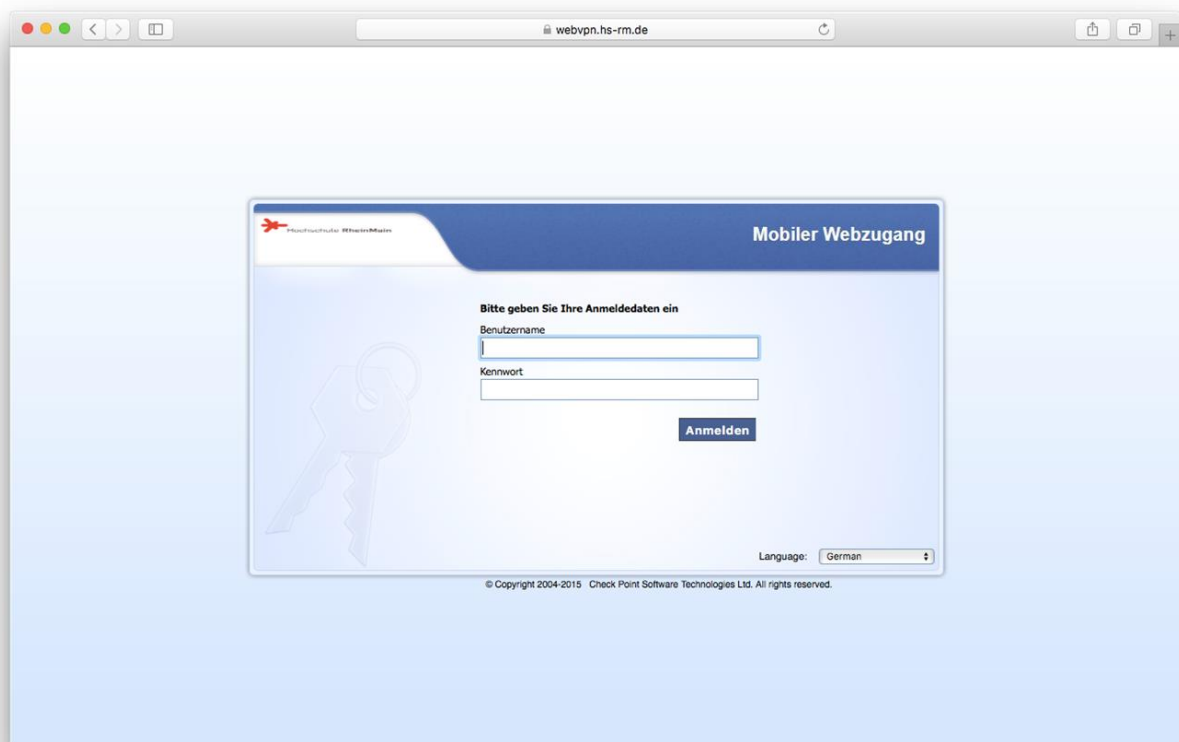


Abbildung 29: Anmeldung zur Erstkonfiguration

Nach der Anmeldung öffnen Sie die Einstellungen unter dem Safari Browser (Menüleiste - Safari - Einstellungen) und öffnen den Reiter Sicherheit.

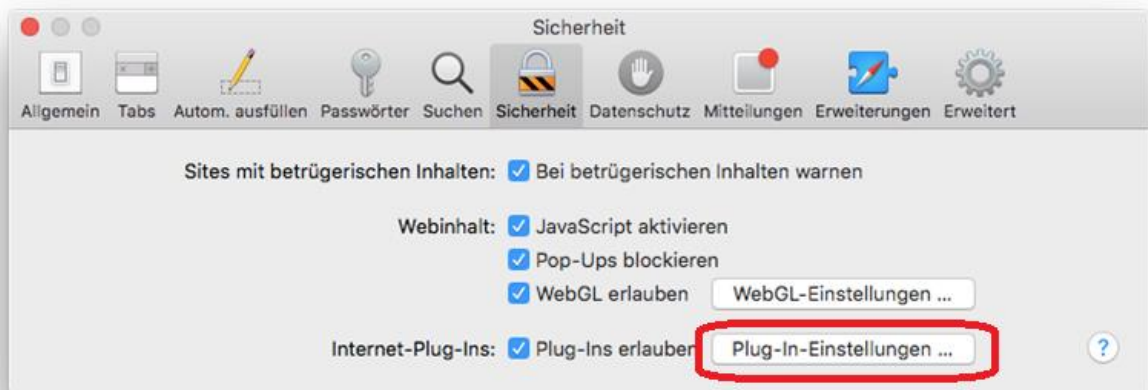


Abbildung 30: Einstellungen Safari 10.XX

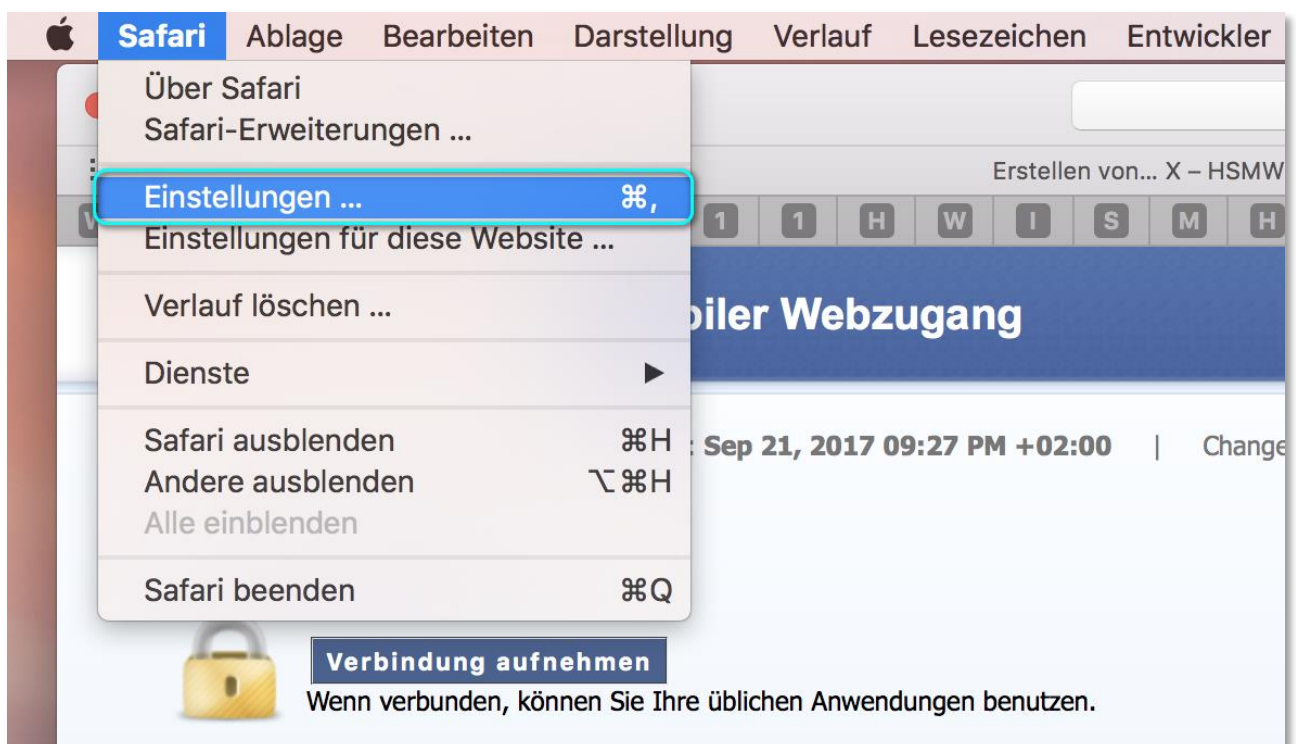


Abbildung 31: Einstellungen Safari 11.XX

Stellen Sie sicher, dass der Haken bei „JavaScript aktivieren“ aktiviert ist und öffnen anschließend das Menü „Plug-In Einstellungen“.

Aktivieren Sie das Plug-In Java und erlauben Sie dem Plug-In den Punkt „im unsicheren Modus ausführen“ für die Portalseite der Hochschule RheinMain.

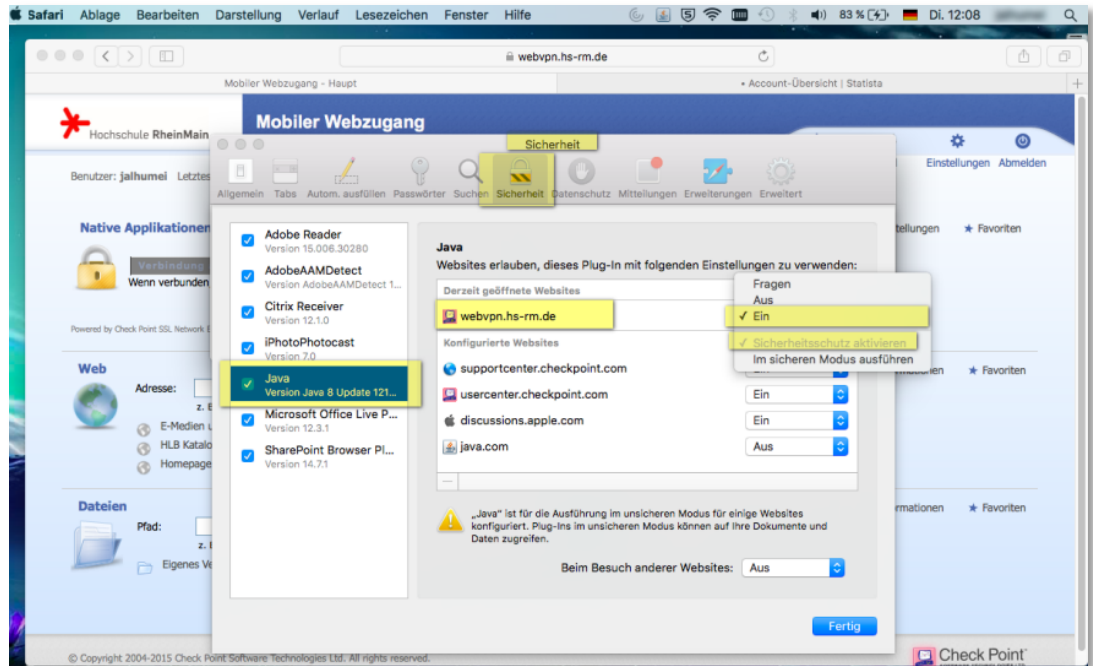


Abbildung 32: Einstellungen Plug-In Safari 10.XX

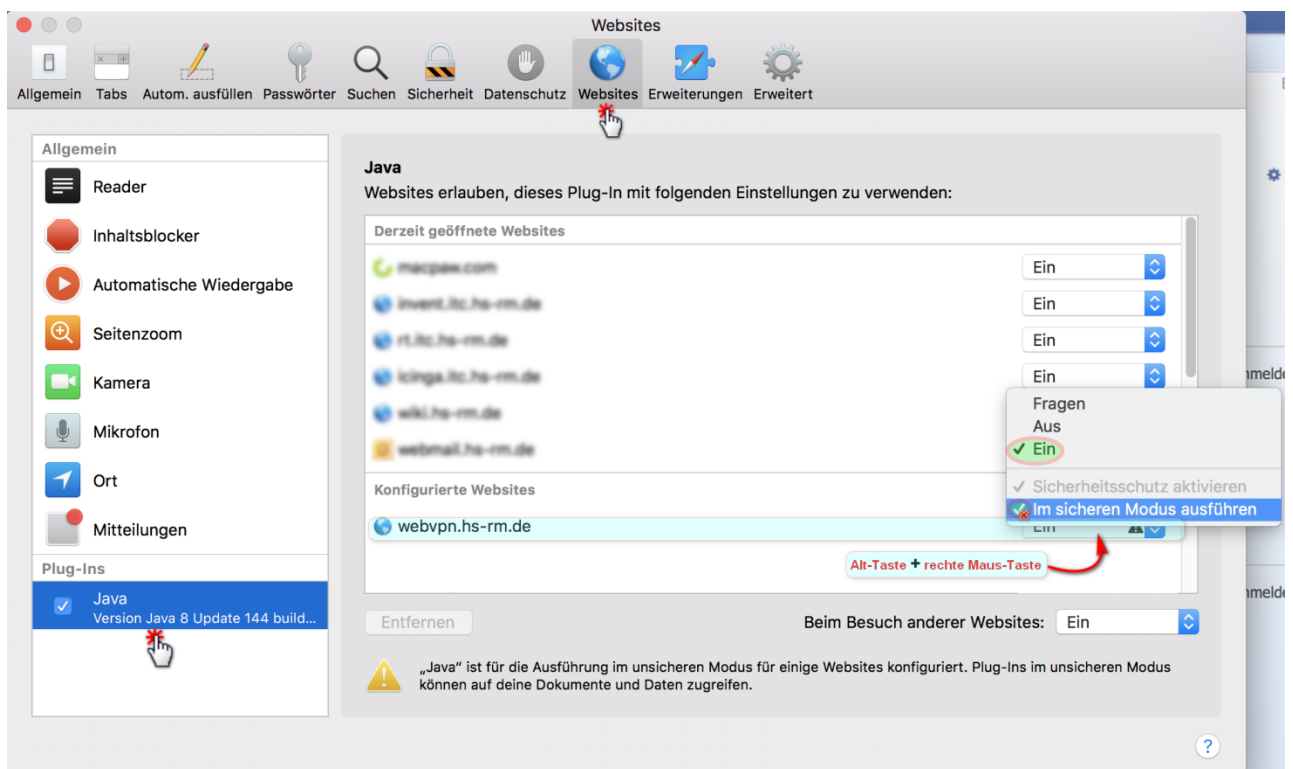


Abbildung 33: Einstellungen Plug-In Safari 11.XX

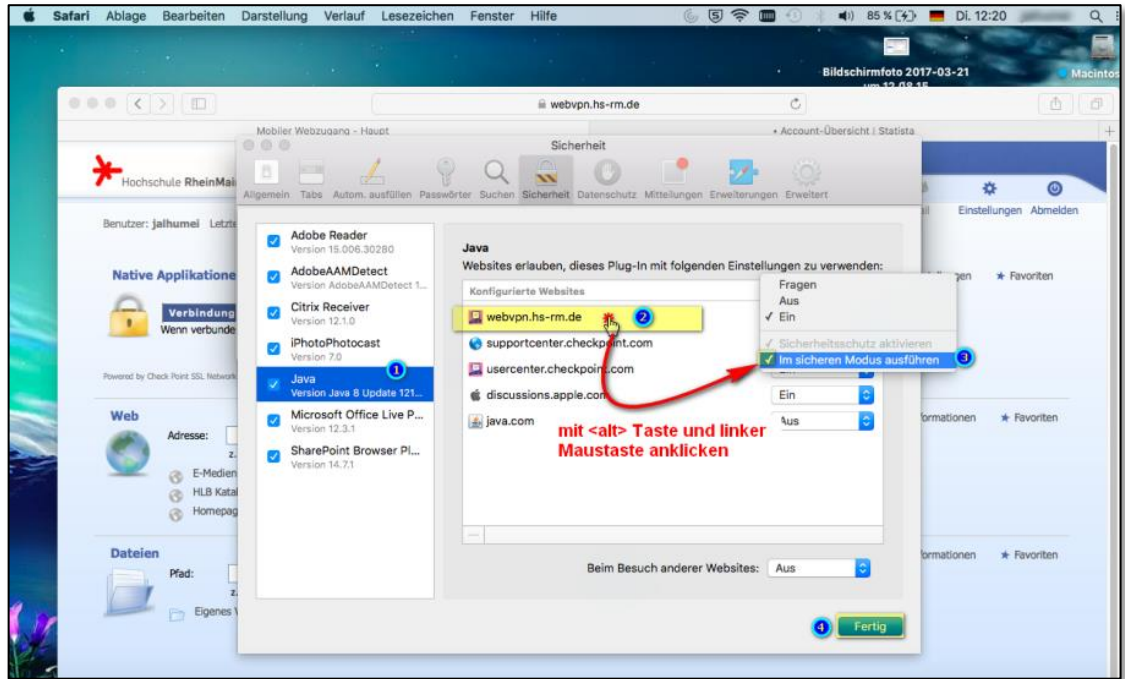


Abbildung 34: Einstellungen Plug-In – unsicherer Modus Safari 10.XX

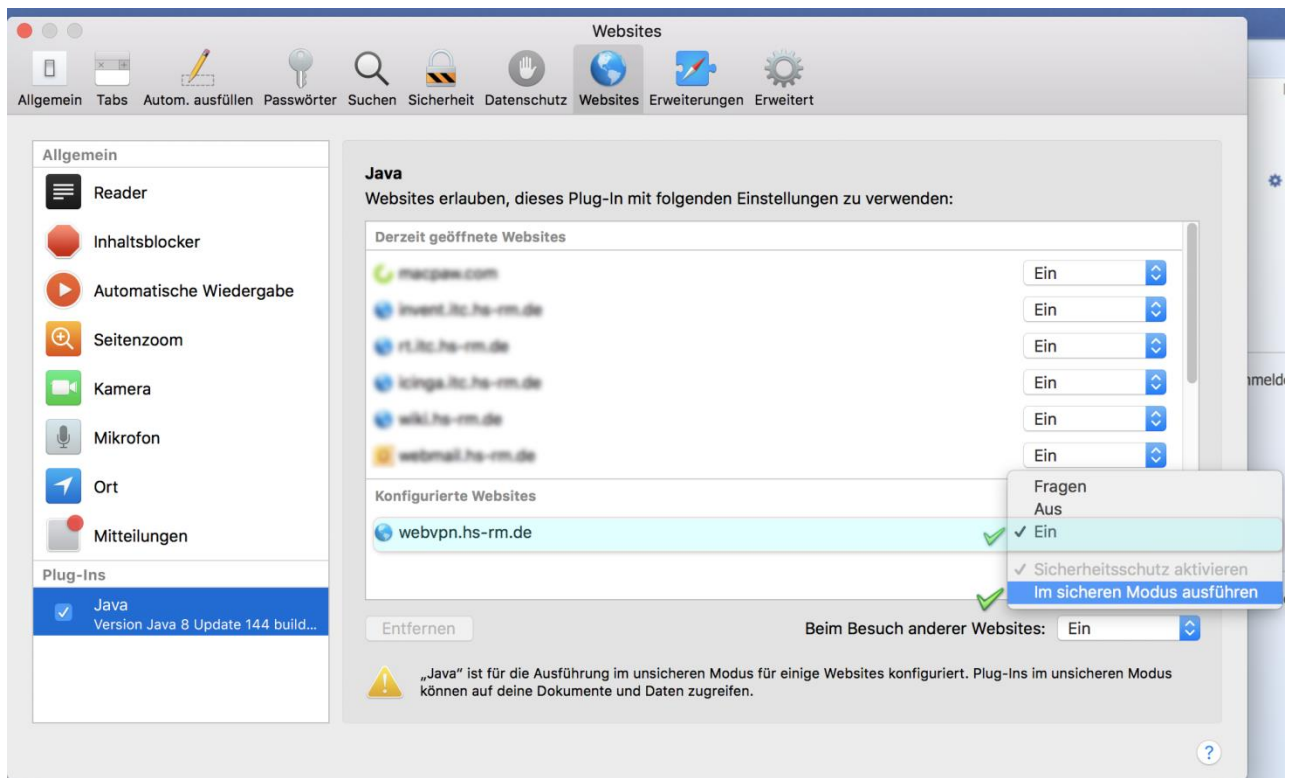


Abbildung 35: Einstellungen Plug-In – unsicherer Modus Safari 11.XX

Im nächsten Schritt müssen Sie der Änderung zustimmen. Klicken Sie hierfür auf den Button „Vertrauen“.

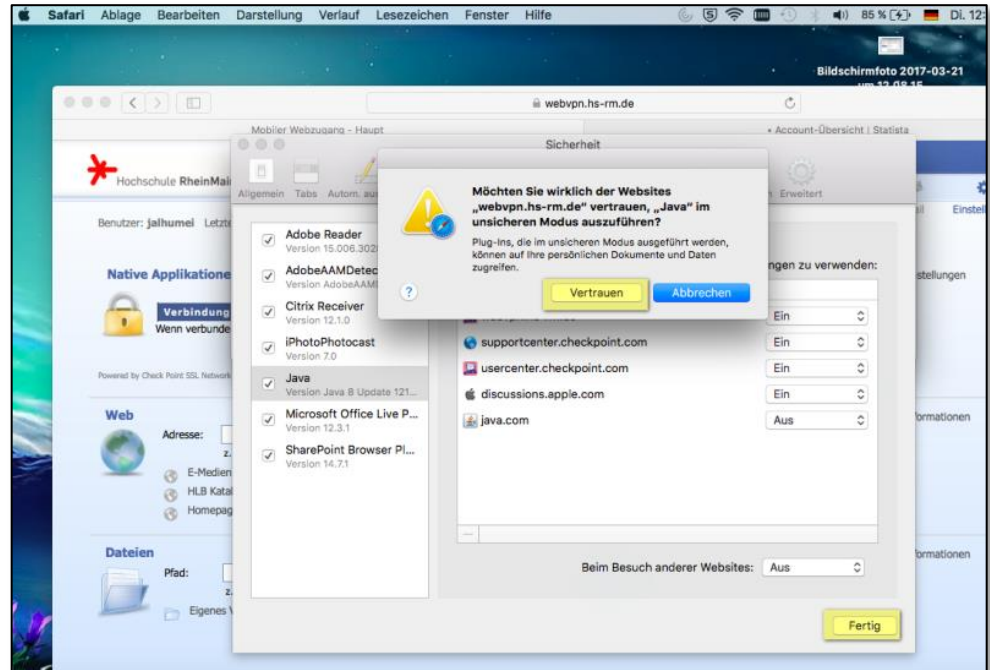


Abbildung 36: Vertrauensabfrage

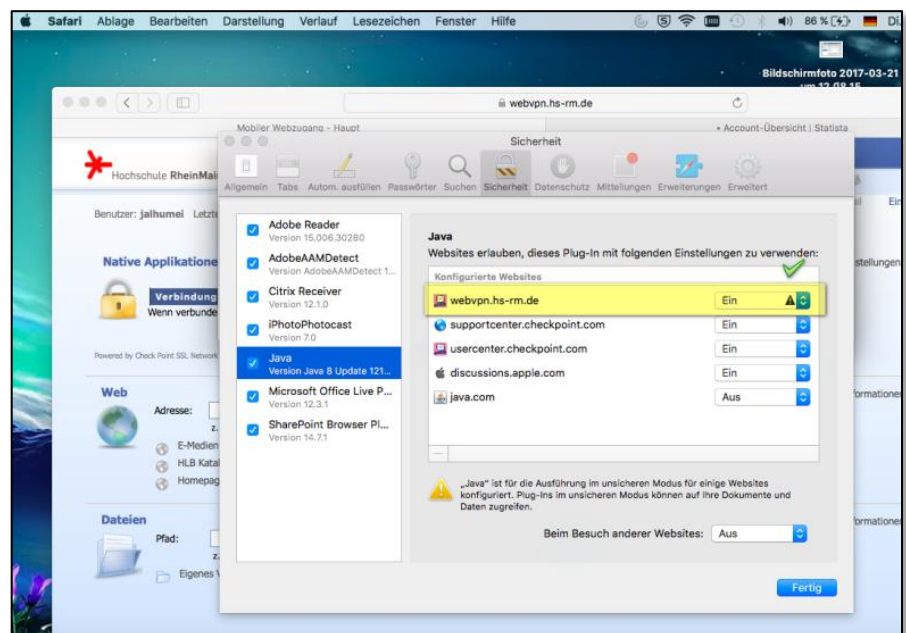


Abbildung 37: Verwendung Java Plug-In Safari 10.XX

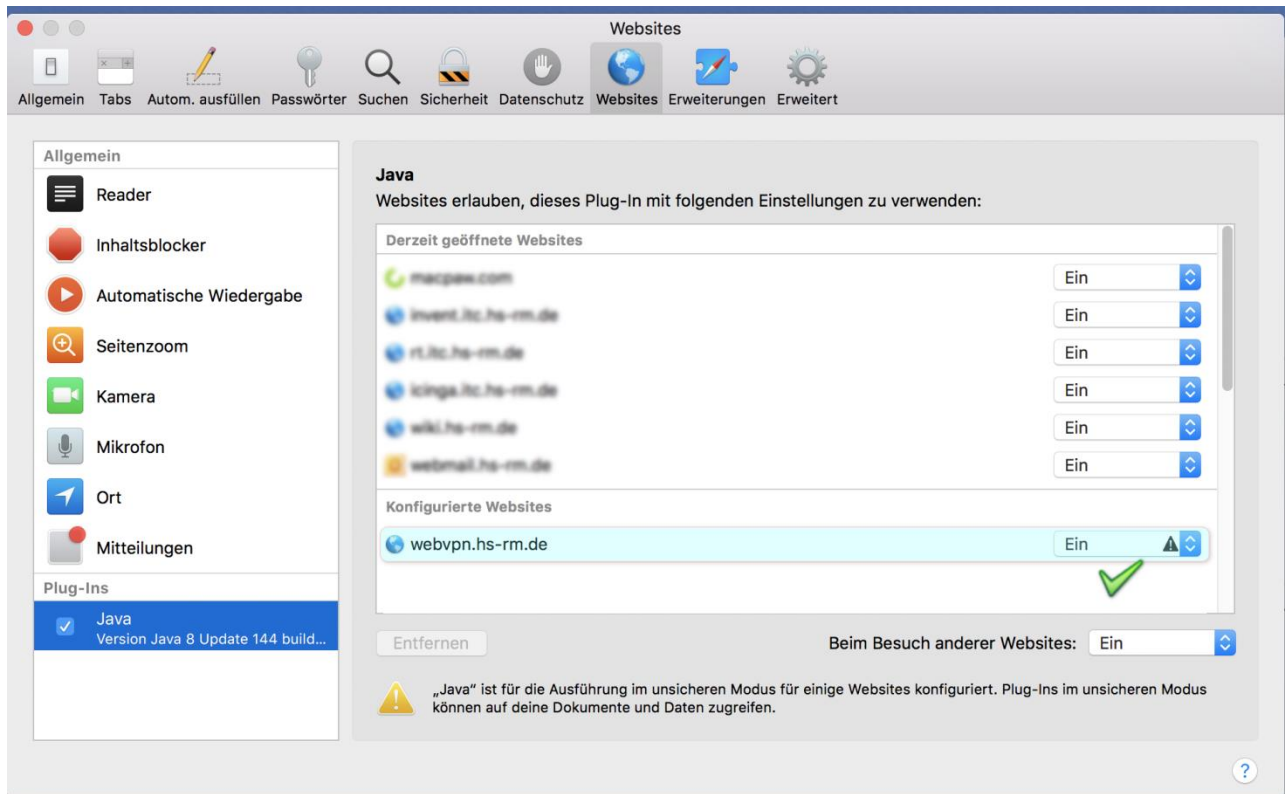


Abbildung 38: Verwendung Java Plug-In Safari 11.XX

Im Anschluss schließen Sie die zuvor geöffneten Fenster mit den Buttons „Fertig“ und dem roten ‚x‘ in der oberen linken Ecke.

Beim ersten Aufbau der Verbindung müssen Sie dem Plug-In für die Seite nochmals zustimmen: Zum Aufbau der Verbindung können Sie, nach Anmeldung auf der Portalseite der Hochschule RheinMain, den Button „Verbindung aufnehmen“ benutzen, sofern dies nicht bereits automatisch geschehen ist.

In einem Popup öffnet sich der Network SSL Extender. Bitte stellen Sie sicher, dass das Java-Plug-In sämtliche Zugriffe gewährt bekommt, die es benötigt.

Klicken Sie hierzu auf „Vertrauen“.

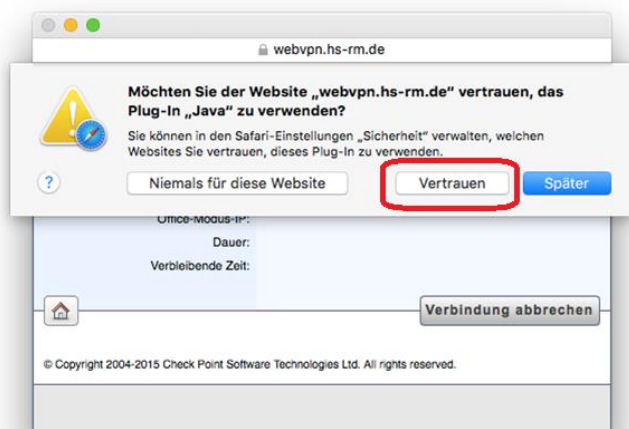


Abbildung 39: Website vertrauen

Verbindungsaufbau

Hierzu müssen Sie nach der Anmeldung über die Schaltfläche „Verbindung aufnehmen“ den SSL Connector starten.



Abbildung 40:Verbindung starten

Der Aufbau der Verbindung wird im Browser angezeigt

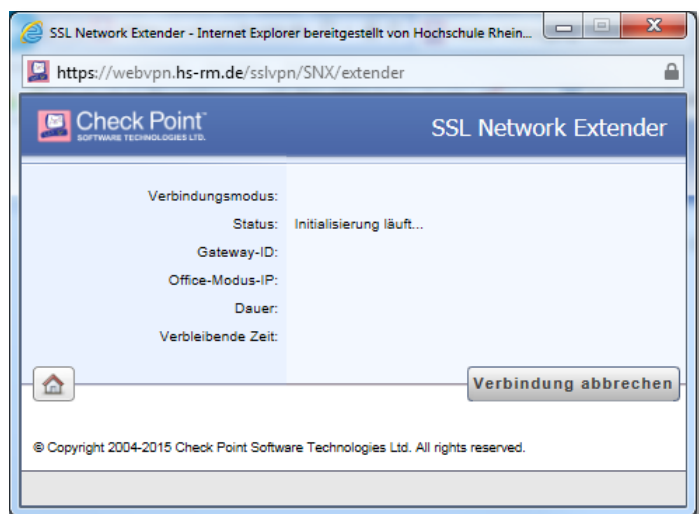


Abbildung 41:Initialisierung

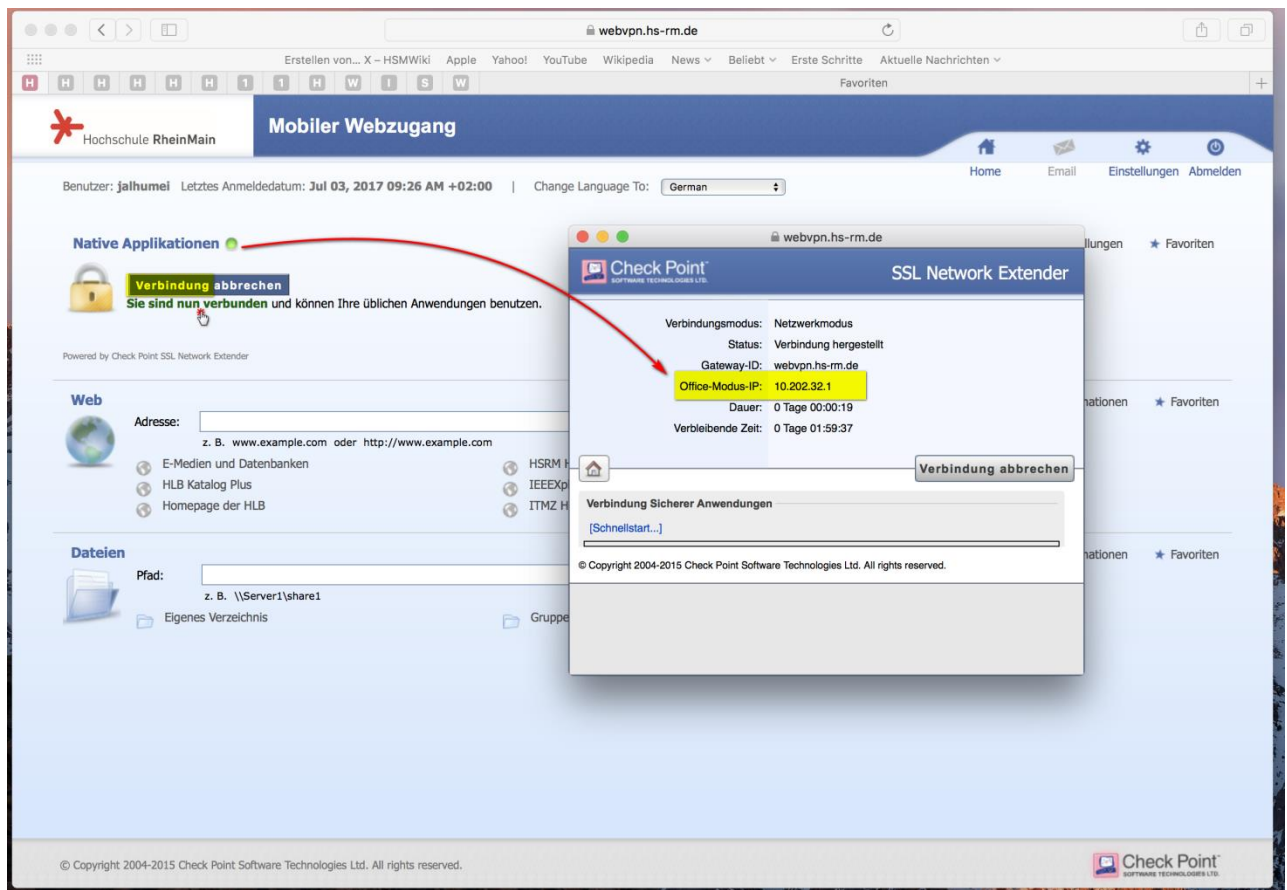


Abbildung 42: SSL Verbindung

Häufige Fragen - FAQ:

Beachten Sie bitte, dass auf unserer Homepage unter www.hs-rm.de/ITMZ/FAQ_VPN_Studierende FAQ verfügbar sind, die regelmäßig aktualisiert werden.

Kontakt

IT- und Medienzentrum
Kurt-Schumacher-Ring 18
Gebäude A Raum 223b
65197 Wiesbaden

Tel. +49 (0)611 9495-1700
Fax +49 (0)611 9495-1701
service-itmz@hs-rm.de

Sprechzeiten: Mo - Fr
08.00 – 12.00 Uhr und
13.00 – 16.00 Uhr

Abbildungsverzeichnis:

Abbildung 1:Anmeldung	3
Abbildung 2:Webzugriff	4
Abbildung 3:Favoriten	4
Abbildung 4:Webfavoriten	5
Abbildung 5:Webfavoriten hinzufügen	5
Abbildung 6:Webfavoriten hinzufügen	5
Abbildung 7:Eigene Webfavoriten	6
Abbildung 8:Webfavoriten entfernen.....	6
Abbildung 9: Verbindung starten	7
Abbildung 10: Add-On installieren	8
Abbildung 11: Check Point Abfrage	8
Abbildung 12: Sicherheitsabfrage	9
Abbildung 13: Installationsfortschritt	9
Abbildung 14: Windows Firewall	9
Abbildung 15: Automatischer Verbindungsaufbau	10
Abbildung 16: In Edge den Internet Explorer aufrufen	10
Abbildung 17: Seite mit Internet Explorer öffnen.....	11
Abbildung 18: Java Download	12
Abbildung 19: Java Installation	12
Abbildung 20: Anmeldung zur Erstkonfiguration	13
Abbildung 21:Verbindungsprozess	13
Abbildung 22: Installation Check Point Deployment-Agent	14
Abbildung 23: Sicherheitswarnung	14
Abbildung 24: Trust Server Abfrage.....	15
Abbildung 25: Verbindungsaufbau.....	15
Abbildung 26:Java für Mac OS X.....	16
Abbildung 27:Installation Java für Mac OS X.....	16
Abbildung 28:Java für Mac OS X.....	17
Abbildung 29: Anmeldung zur Erstkonfiguration	17
Abbildung 30: Einstellungen Safari 10.XX	18
Abbildung 31: Einstellungen Safari 11.XX	18
Abbildung 32: Einstellungen Plug-In Safari 10.XX	19
Abbildung 33: Einstellungen Plug-In Safari 11.XX	19
Abbildung 34: Einstellungen Plug-In – unsicherer Modus Safari 10.XX	20
Abbildung 35: Einstellungen Plug-In – unsicherer Modus Safari 11.XX	20
Abbildung 36: Vertrauensabfrage	21
Abbildung 37: Verwendung Java Plug-In Safari 10.XX	21
Abbildung 38: Verwendung Java Plug-In Safari 11.XX	22
Abbildung 39: Website vertrauen.....	22
Abbildung 40:Verbindung starten	23
Abbildung 41:Initialisierung.....	23
Abbildung 42: SSL Verbindung.....	24