ENDPOINT PROTECTOR APPLIANCE

Benutzerhandbuch Version 4.0.0.4

Benutzerhandbuch A20 / A50 / A100 / A250 / A500 / A1000 / A2000 / A4000

COSOSYS

Inhaltsverzeichnis

1. Endpoint Protector Appliance Setup

1.1. Endpoint Protector Appliance Lieferumfang

Beim Empfang der Endpoint Protector Appliance enthält das Paket:

- Endpoint Protector Appliance
- Netzkabel
- Gekreuztes Netzwerkkabel für das Appliance Setup (gelbe Markierung) (nicht bei A20 enthalten da nicht erforderlich)
- Netzwerkkabel für die Verbindung der Appliance mit Ihrem Netzwerk
- Schrauben für Rack Einbau
  (nicht bei A20 enthalten da nicht erforderlich)
- Ausziehbare Rack Montageschienen (nur bei A250, A500, A1000, A4000 Modellen inklusive)
- Externes Netzteil für A20 Appliance (bei A20 inklusive und erforderlich)

1.2. Verbinden der Appliance für erstes Setup

Schließen Sie das Netzkabel an die Appliance und eine Steckdose an.

Bei der A20 Appliance verbinden Sie bitte das externe Netzteil mit der Appliance und einer Steckdose. Danach, verbinden Sie das blaue Kabel zu dem Netzwerkport und danach zu dem Netzwerk.

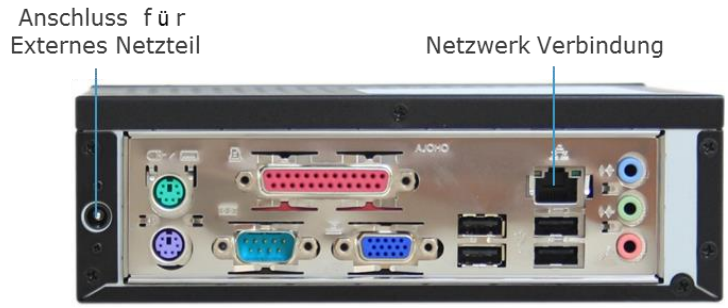
Ihre Hardware-Appliance (Modelle von A50 bis A4000) besitzt auf der Rückseite zwei Netzwerk-Ports diese sind gelb markiert für CONFIG (Konfigurations-Verbindung) und blau für NET (Netzwerk Verbindung) markiert. Die A20 Appliance hat einen Netzwerk-Port welcher für die Inbetriebnahme der A20 ausreicht.

Schließen Sie das gekreuztes Netzwerkkabel (gelbe Markierung), an den Konfiguration Netzwerk-Port CONFIG (gelb markiert) auf der Rückseite des Gerätes und verbinden Sie es DIREKT mit einem PC (Laptop, PC, Netbook).

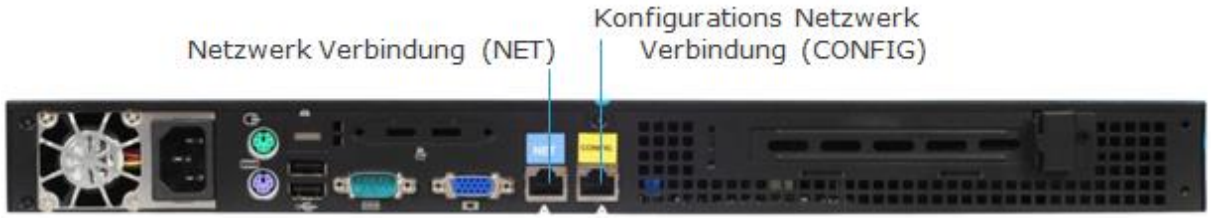
Starten Sie die Appliance, indem Sie den An-Schalter drücken.

1.3. Hardware Appliance Rückseite / Vorderseite

1.3.1. A20 Appliance Rückseite



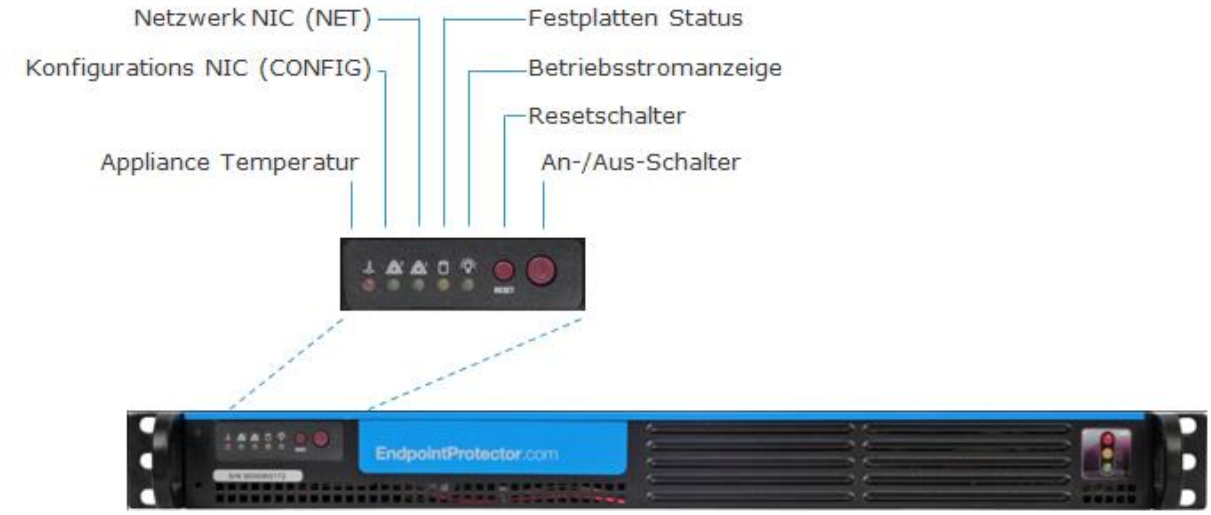
1.3.2. A50 und A100 Appliance Rückseite



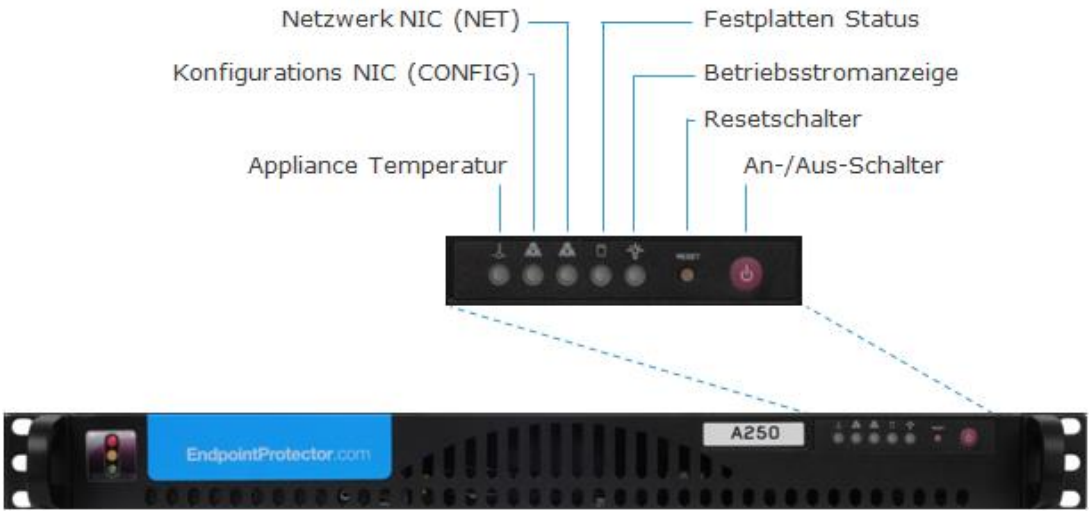
Die Rückseite der Modelle A250 bis A4000 verfügen ebenfalls über blau und gelb markierte Netzwerk-Ports wie die oben dargestellte A50 und A100 Appliance.

1.3.3. A20 Appliance Vorderseite

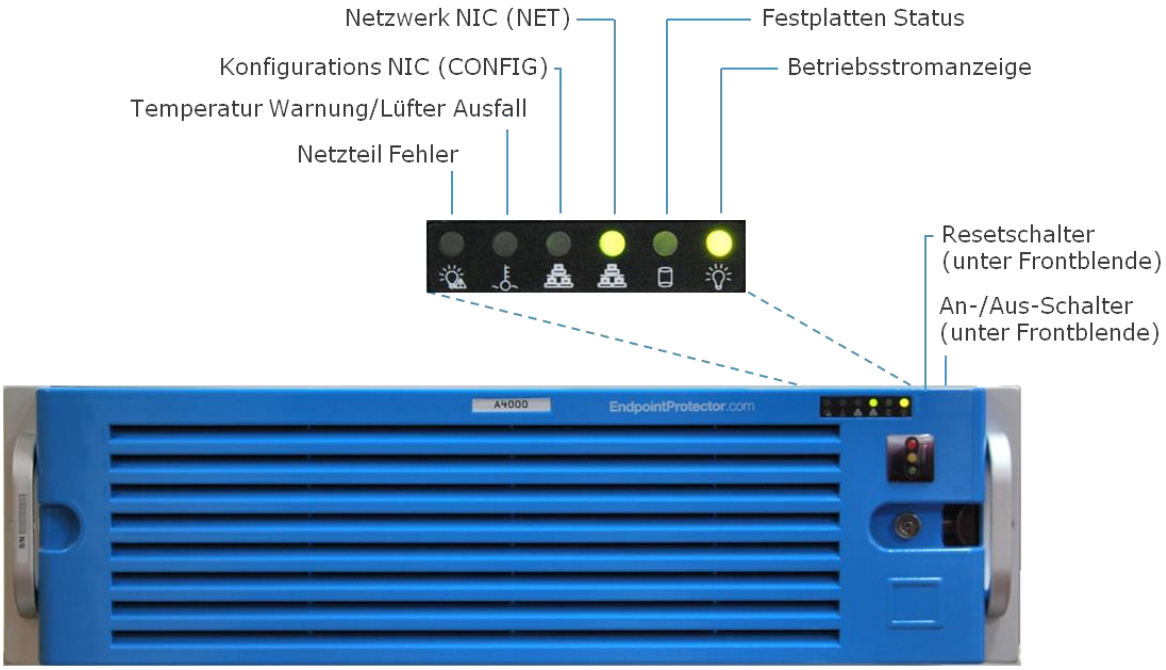
1.3.4. A50 und A100 Appliance Vorderseite



1.3.5. A250, A500 und A1000 Appliance Vorderseite

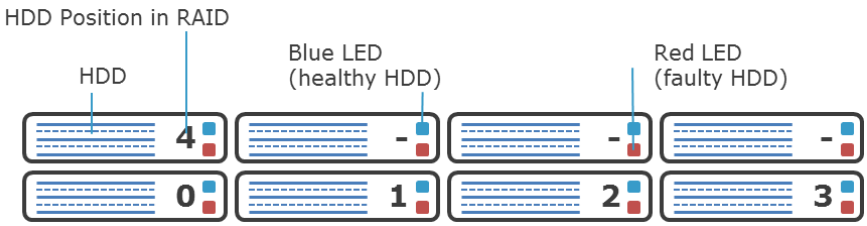


1.3.6. A2000 - A4000 Appliance Vorderseite



1.4. A2000 / A4000 Appliance HDD Konfiguration

1.4.1. A2000 Appliance HDD Konfiguration

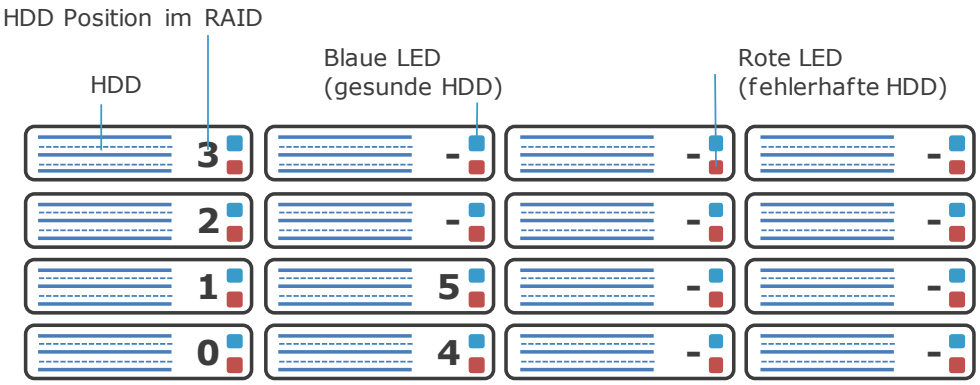


Die A2000 Appliance verfügt über 4 Festplatten in RAID 5 Konfiguration. Die Festplatten sind in der von 0-3 nummerierten Reihenfolge installiert.

Im Falle eines Festplattenversagens, kann eine Festplatte durch ein baugleiches Model ausgetauscht werden.

Jeder Festplatteneinschub verfügt über eine blaue und rote LED zur Anzeige des Festplattenstatus. Eine blaue Anzeige symbolisiert eine gesunde Festplatte, eine rote Anzeige eine fehlerhafte Festplatte. Eine fehlerhafte Festplatte sollte umgehend durch ein baugleiches Model ausgetauscht werden.

1.4.2. A4000 Appliance HDD Konfiguration



Die A4000 Appliance verfügt über 6 Festplatten in RAID 5 Konfiguration. Die Festplatten sind in der von 0-5 nummerierten Reihenfolge installiert.

Im Falle eines Festplattenversagens, kann eine Festplatte durch ein baugleiches Model ausgetauscht werden.

Jeder Festplatteneinschub verfügt über eine blaue und rote LED zur Anzeige des Festplattenstatus. Eine blaue Anzeige symbolisiert eine gesunde Festplatte, eine rote Anzeige eine fehlerhafte Festplatte. Eine fehlerhafte Festplatte sollte umgehend durch ein baugleiches Model ausgetauscht werden.

1.4.3. A2000 - A4000 Appliance HDD RAID 3ware® 3DM® Zusatz-Software

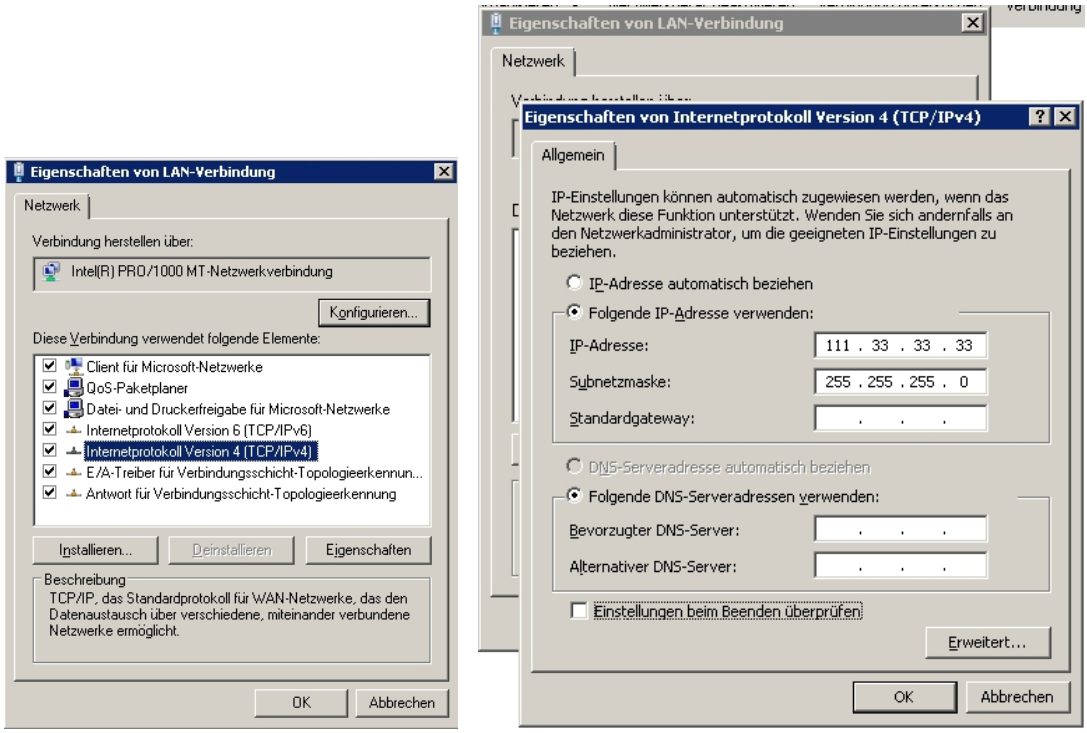
Die A2000 und A4000 Appliance verfügen über einen zusätzlich konfigurierbare Software von 3Ware® mit der Sie als Administrator über mögliche Fehler an einer der Festplatten per E-Mail gewarnt/informiert werden können. Weiter Informationen zur Konfiguration dieser Zusatzsoftware finden Sie in unserem Benutzerhandbuch Anhang „3ware® 3DM® 2 Zusatz-Software Benutzerhandbuch“.

1.5. Zugriff auf Appliance Setup-Assistent mit normalem Netzwerkkabel (nur für A20)

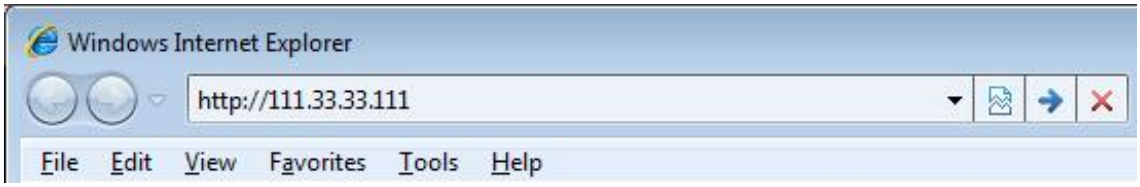
Verbinden Sie den blauen Kabel zu den A20 Netzwerkport und danach zu dem Netzwerk. Die Netzwerkeinstellungen auf Ihrem Computer sollten für TCP/IPv4 folgende sein:

IP Adresse 111.33.33.33

Subnetzmaske 255.255.255.0 (Subnet Mask)



Dann können Sie über einen Internet-Browser über die folgende IP Adresse zugreifen. Geben Sie diese einfach http://111.33.33.111 in die URL Leiste ein.

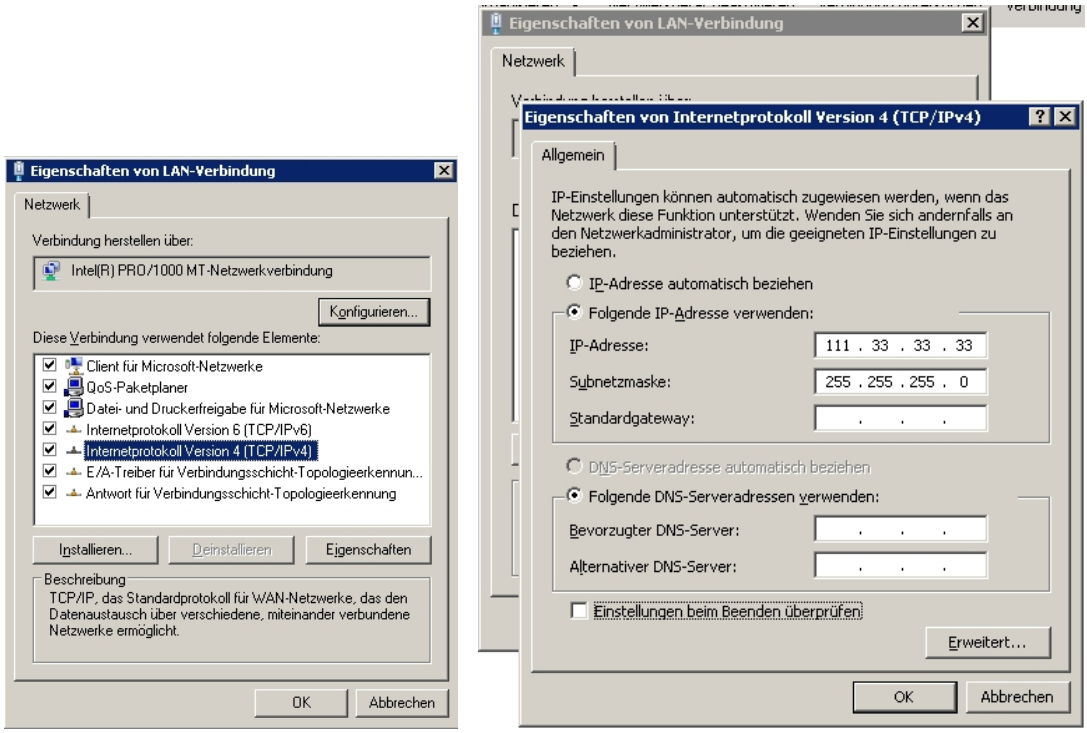


1.6. Zugriff auf Appliance Setup-Assistent mit gekreuztem Netzwerkkabel (für A50 und größere Modelle)

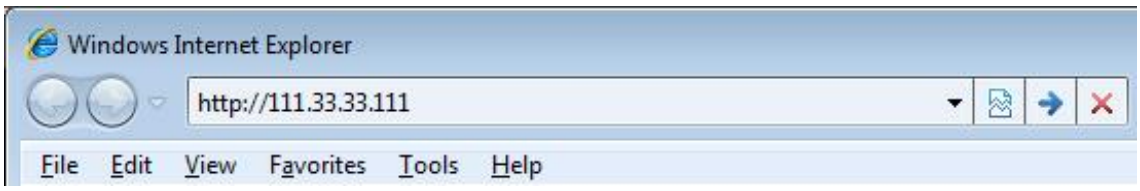
Mit Ihrem Computer verbinden Sie sich nun über das gekreuzte Kabel. Die Netzwerkeinstellungen auf Ihrem Computer sollten für TCP/IPv4 folgende sein:

IP Adresse 111.33.33.33

Subnetzmaske 255.255.255.0 (Subnet Mask)

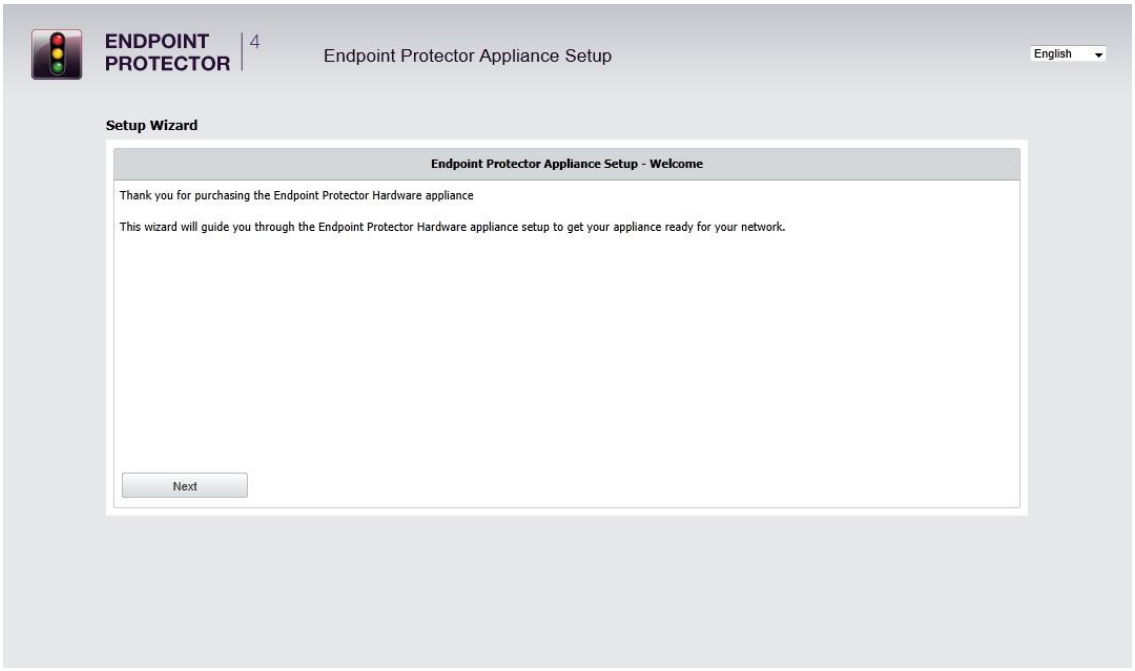


Dann können Sie über einen Internet-Browser über die folgende IP Adresse zugreifen. Geben Sie diese einfach http://111.33.33.111 in die URL Leiste ein.

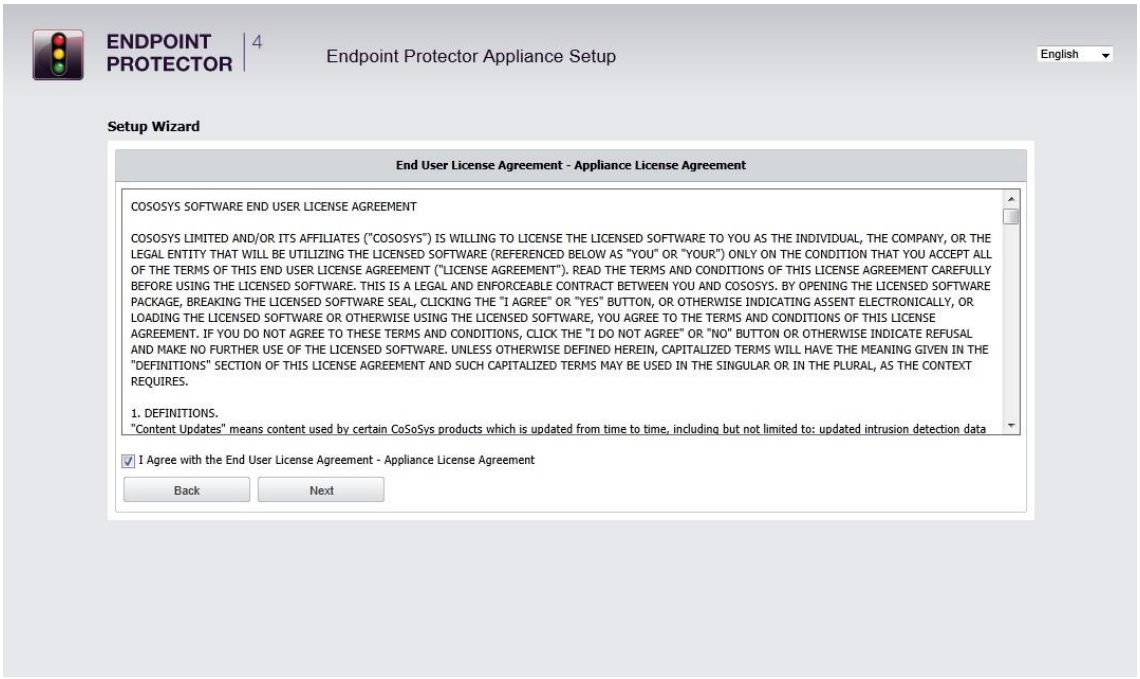


1.7. Appliance Setup-Assistent

Dieser Assistent wird Sie durch das Setup der Endpoint Protector Hardware Appliance führen um es für Ihr Netzwerk betriebsbereit einzurichten.

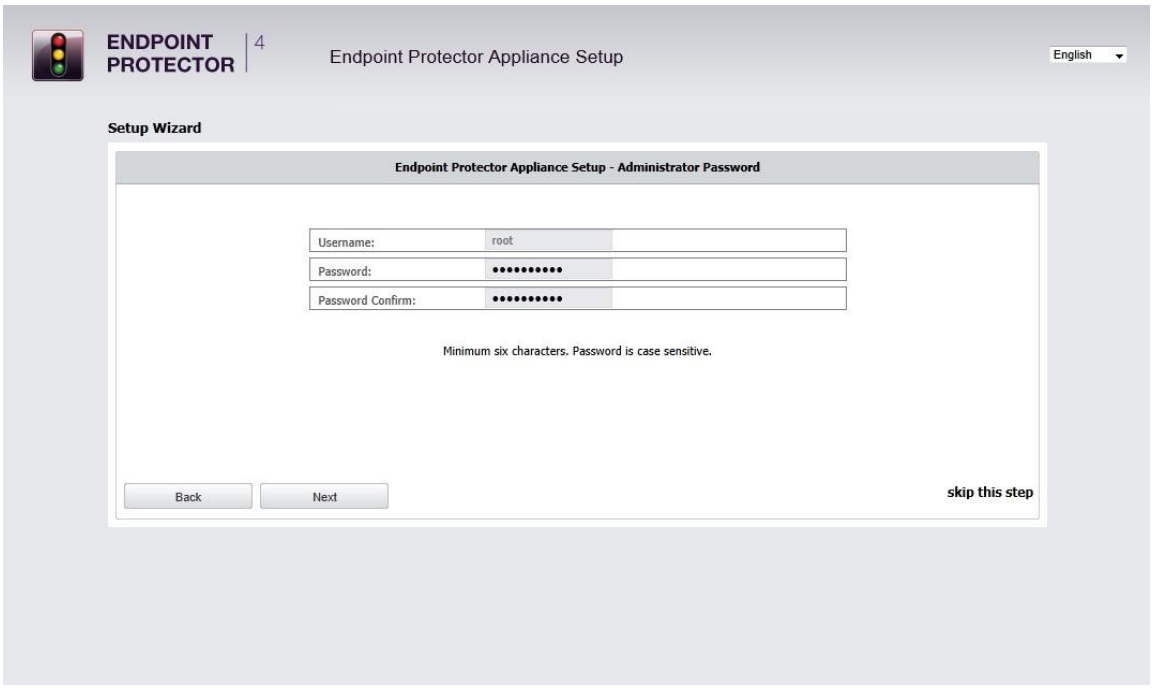


1.7.1. End User Lizenzvertrag - Appliance Lizenzvertrag



Um mit dem Setup-Prozess fortzufahren, stimmen Sie bitte den End User Lizenzvertrag - Appliance Lizenzvertrag zu.

1.7.2. Definieren Sie Ihr Appliance Administrator-Passwort



Geben Sie bitte Ihr Administrator-Kennwort ein und bestätigen Sie dieses.

Die Mindestlänge beträgt 6 Zeichen und die Klein- und Großschreibung ist zu beachten.

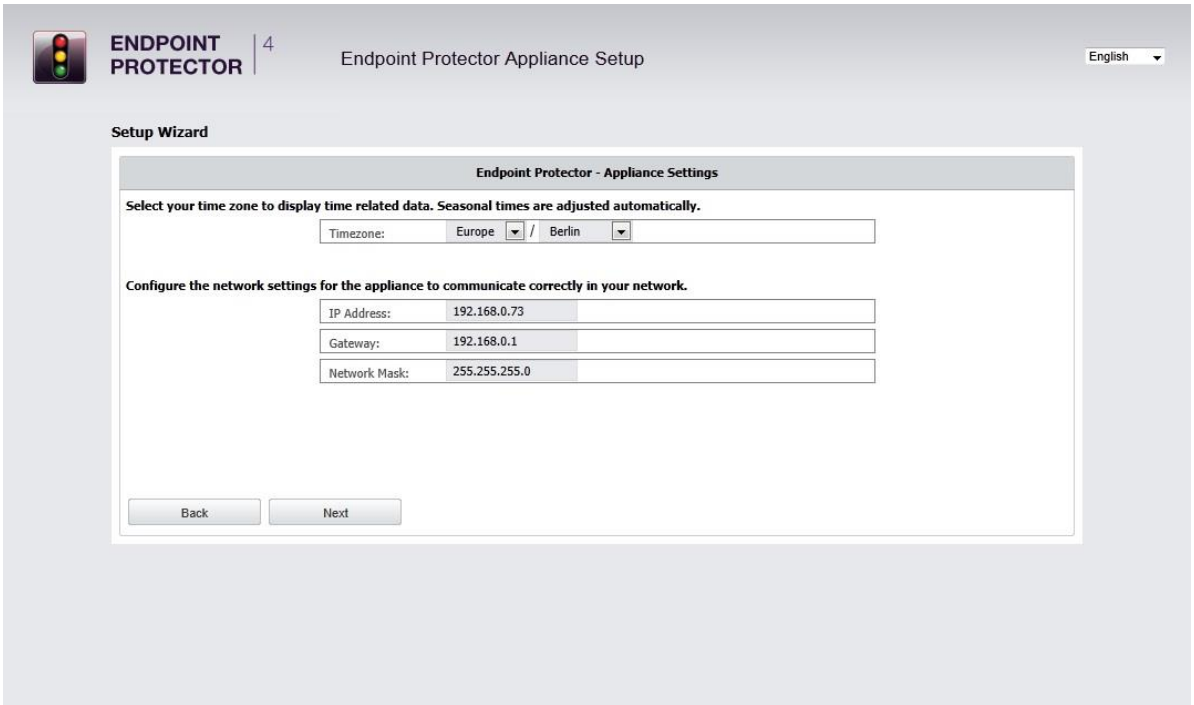
Die standardmäßigen Logindaten für das Endpoint Protector Administrations und Reporting Cockpit sind:

BENUTZERNAME: root

KENNWORT: epp2011

Nach Eingabe und Bestätigung des Administrator-Passworts klicken Sie auf Weiter, um fortzufahren.

Zeitzone Festlegen

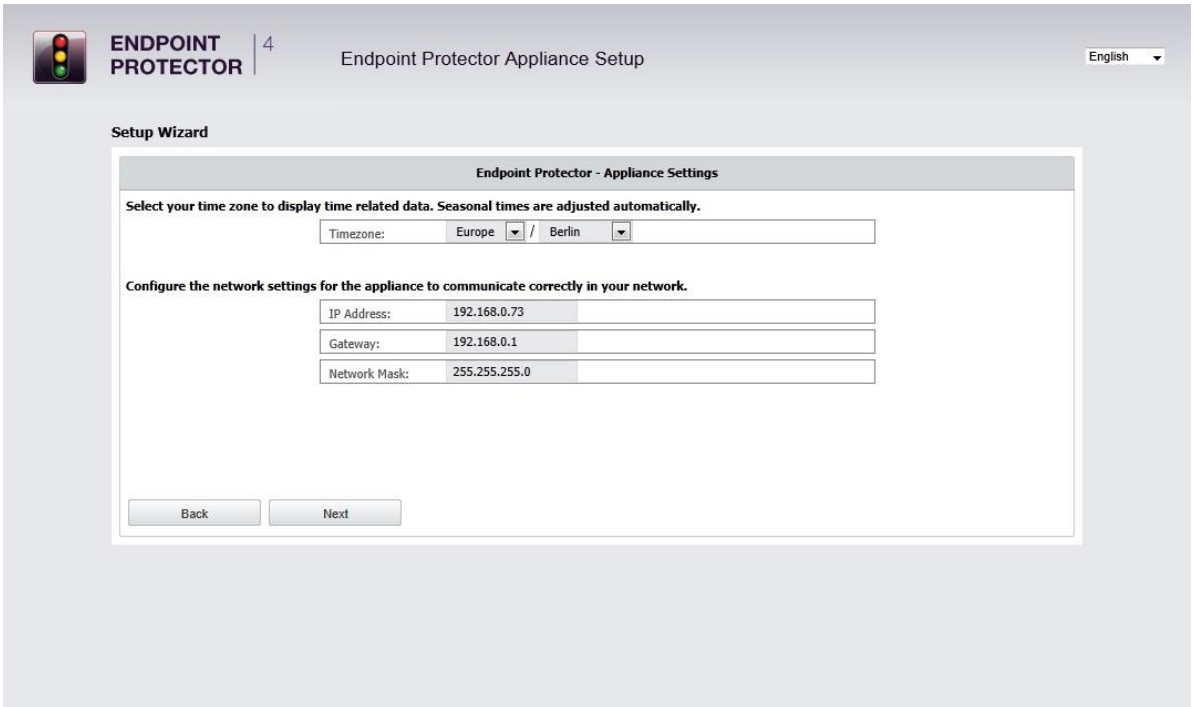


Wählen Sie bitte Ihre Zeitzone aus, damit zeitbezogene Daten korrekt angezeigt werden.

Saisonale Zeit Änderungen werden automatisch angepasst.

Sie können diese Einstellung auch später unter dem Menüpunkt, Appliance - System Pflege ändern.

1.7.3. Netzwerk IP Adresse der Appliance Festlegen



Geben Sie eine IP-Adresse für Ihr Appliance ein. Unter diese IP-Adresse wird die Appliance in Ihrem Netzwerk erreichbar sein. Für den Fall dass Ihr Netzwerk Ips von 192.169.0.0 Typ benutzt, hat die IP Adresse dass zu die Endpoint Protector Applikation zugeordnet die Nummer 192.168.0.201. Wenn diese IP Adresse nicht zum Ihren Netzwerk zugeordnet ist, braucht dann diese Einstellung keine Veränderung.

NOTE!

Die Netzwerk Konfiguration muss an Ihre Netzwerk Topologie zusammenpassen. Zum Beispiel, wenn Ihr Netzwerk eine Klasse A IP benutzt (z.B. 10.10.5.10) und keine Unternetzwerke definiert sind, dann müssen die folgende Information eingegeben werden:

IP Adresse: 10.10.5.10

Gateway: 10.10.5.1

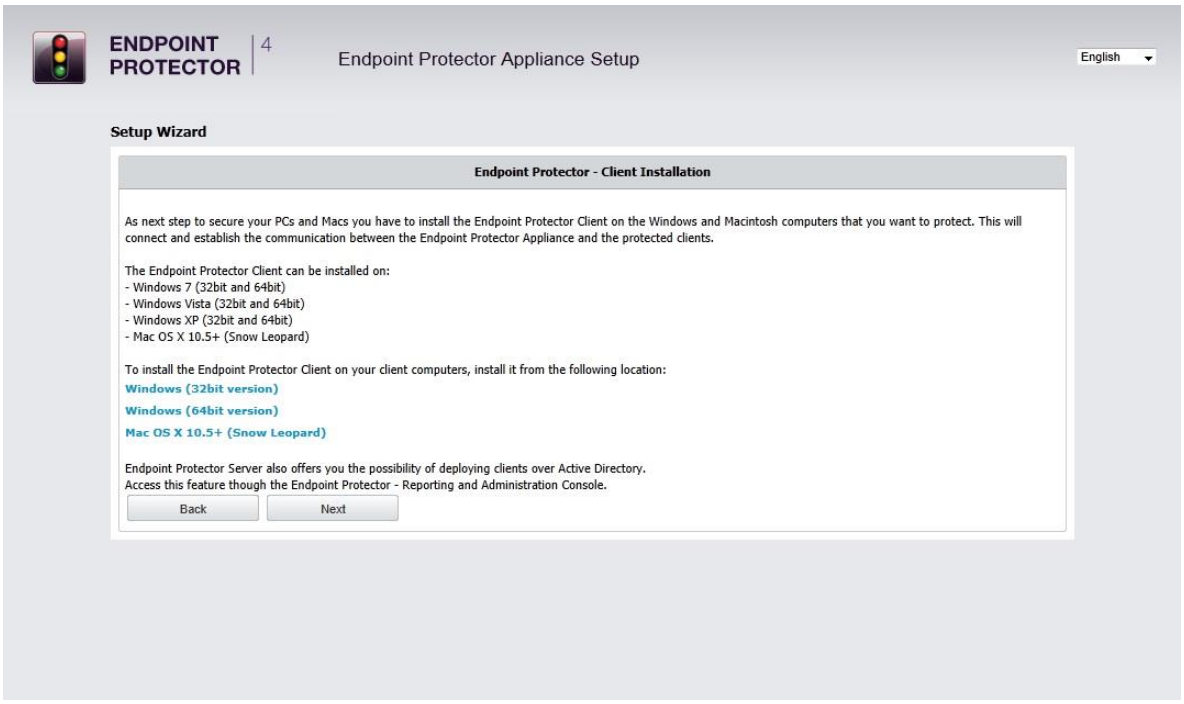
Netzwerk Maske: 255.255.255.0

Eine statische IP ist für die Endpoint Protector Appliance erforderlich, damit eine stabile und dauerhafte Kommunikation zwischen Appliance und Client Computer hergestellt werden kann.

Daher ist DHCP für die Appliance nicht möglich. Bitte geben Sie auch Gateway, Network Mask, Broadcast-und Netzwerk-Einstellungen an, sollte eine Änderung der Standardwerte (Default Einstellungen) erforderlich sein.

Sie können diese Einstellung auch später unter dem Menüpunkt, Appliance - System Pflege ändern.

1.7.4. Endpoint Protector Client – Automatische MSI Anpassung



Nach der Festelegung der statischen IP-Adresse der Appliance, wird die MSI Installationsdatei für den Endpoint Protector Client automatisch angepasst. Die Appliance IP-Adresse wurde der MSI Installationsdatei hinzugefügt.

Für die Macintosh-Installationsdatei muss die Appliance IP-Adresse manuell während dem Installationsprozess des Endpoint Protector Clients auf Mac OS X Computer eingegeben werden.

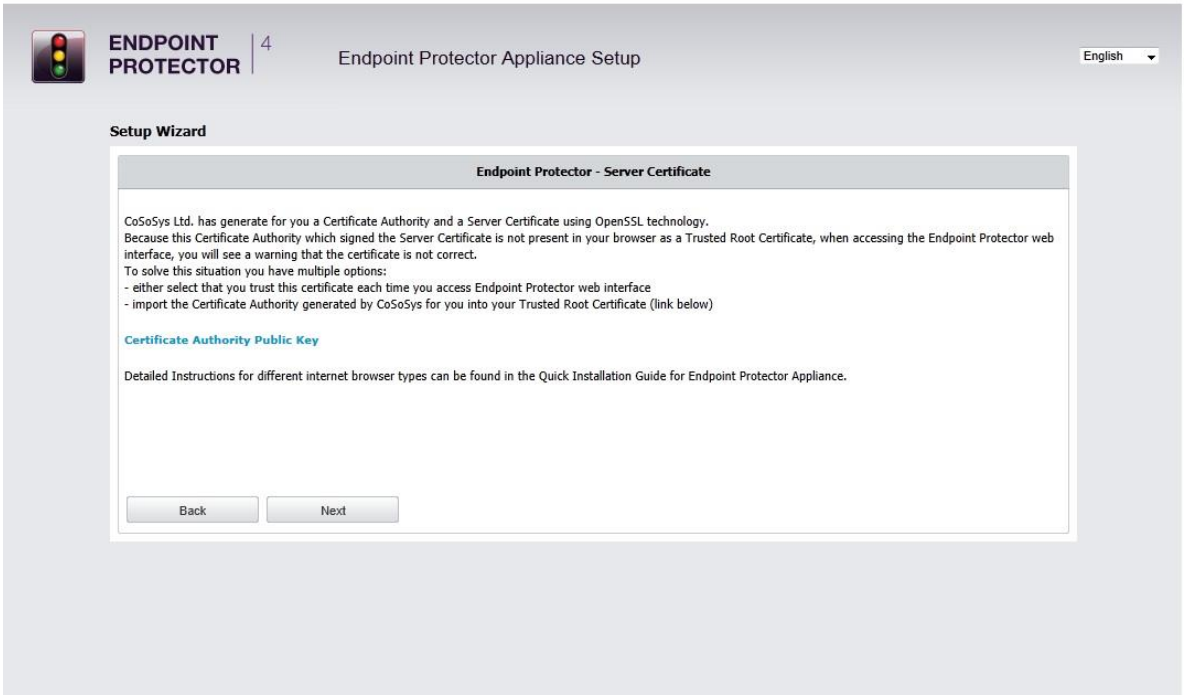
1.7.5. Appliance Server Zertifikat

Nachdem Eingabe der statischen IP -Adresse der Appliance wurde mit OpenSSL Technologie eine Certificate Authority auf der Appliance eingerichtet. Dies ermöglicht es, eine sichere Verbindung über Ihr Netzwerk mit der Web-basierte Administrationsoberfläche der Appliance und eine sichere und verschlüsselte Kommunikation zwischen der Appliance und den geschützten Client-Computern herzustellen.

Wir empfehlen Ihnen das Root-Zertifikat der Endpoint Protector Appliance den vertrauenswürdigen Stammzertifikate Ihres Internet Browsers hinzuzufügen.

Sollten Sie das Zertifikat nicht den vertrauenswürdigen Stammzertifikate Ihres Internet Browsers hinzuzufügen, dann akzeptieren Sie bitte die Fehlermeldung für ungültige Zertifikate in Ihrem Internet Browser.

Eine detaillierte Anleitungen wie Sie Root-Zertifikat für verschiedene Internet-Browser Typen hinzufügen finden Sie in Kapitel 4. "Zertifikat als Root-Zertifikat einem Internet Browser hinzufügen".

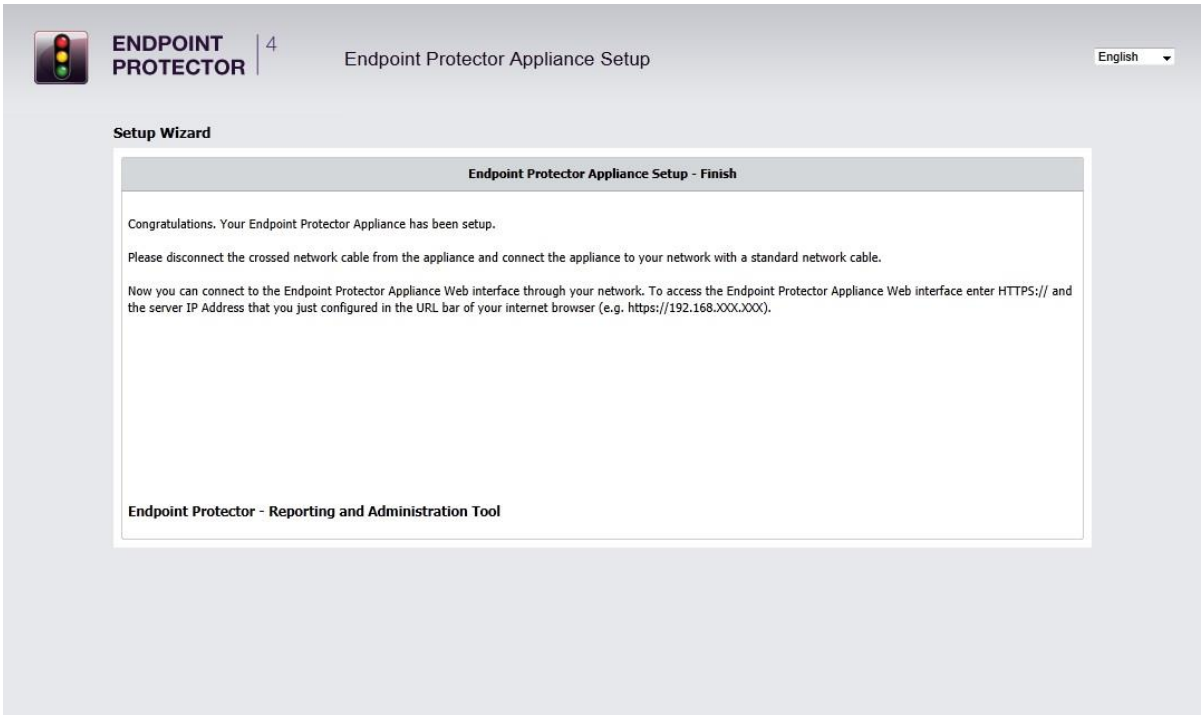


Bei Verwendung von Internet Explorer mit der Option „Verstärkten Sicherheitskonfiguration", müssen Sie die Webseite des Endpoint Protector Administrations-Cockpits den vertrauenswürdigen Seiten im Internet Explorer hinzufügen. Dazu gehen Sie im Internet Explorer in das Menü Extras – Internetoptionen – Sicherheit – Vertrauenswürdige Sites – Sites – Hinzufügen.

1.7.6. Beenden des Endpoint Protector Appliance Setup

Ihre Endpoint Protector Appliance wurde nun erfolgreich eingerichtet.

Entfernen Sie nun bitte das gekreuzte Netzwerkkabel von der Appliance und Ihrem PC. Fahren Sie dann mit den nachstehenden Schritten zum Verbinden der Appliance mit Ihrem Netzwerk fort.



NOTE!

Bitte dieses Schritt für die A20 Modele überspringen!

Bitte beachten Sie dass das blaue Kabel angeschlossen ist.

2. Endpoint Protector Appliance Konfiguration

2.1. Verbindung zwischen Appliance und Netzwerk

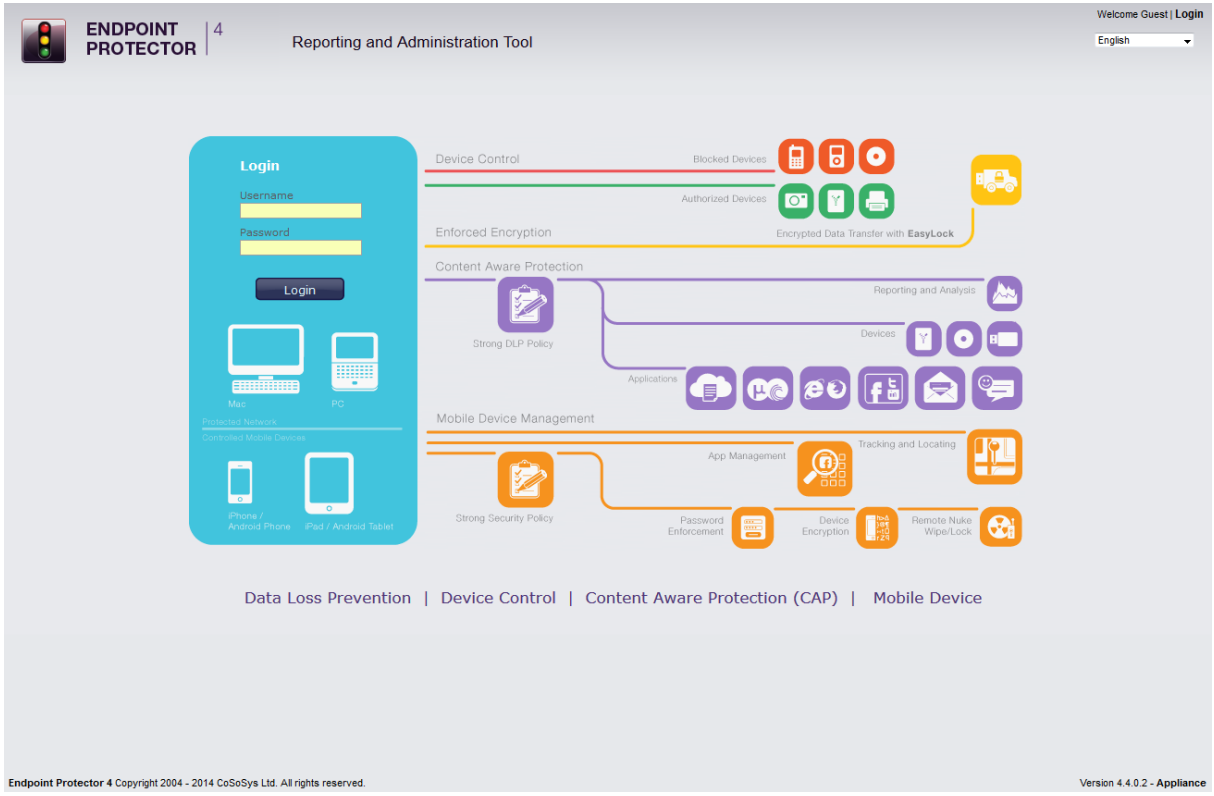
Schließen Sie das Gerät mit einem Standard-Netzwerkkabel durch den Netzwerkanschluss auf der Rückseite der Appliance, die mit NET (blau markiert ist) an Ihr Netzwerk.

2.2. Appliance Web-Interface über Netzwerk öffnen

Jetzt können Sie über Ihr Netzwerk das Endpoint Protector Appliance Web-Interface öffnen. Dazu geben Sie einfach die zuvor zugewiesene statische IP-Adresse mit http**s** ein. Die Standard IP-Adresse (Default IP Adresse) ist z.B. https://192.168.0.201.

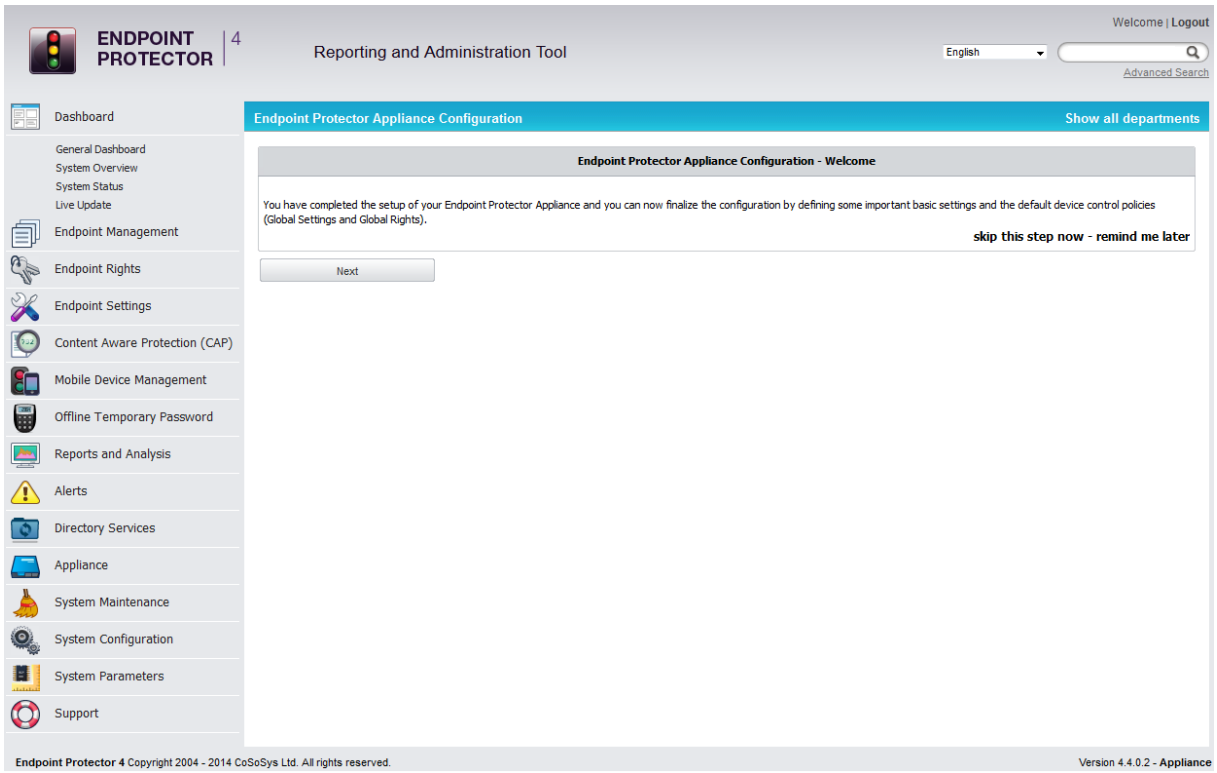
2.3. Anmeldung am Appliance Web-Interface

Bitte geben Sie Ihren Benutzernamen und das Passwort, das Sie zuvor im Setup definiert haben ein. Der Benutzername ist in der Standard Einstellung root.



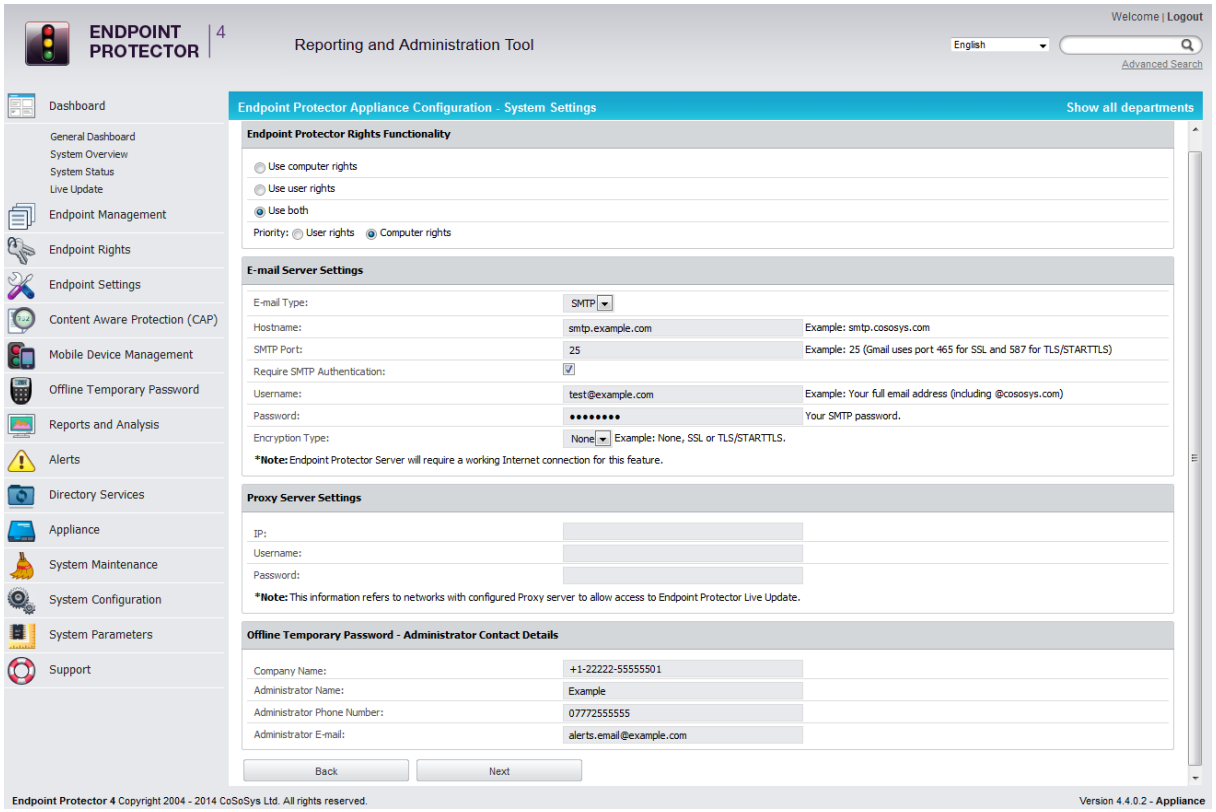
2.4. Appliance Konfigurations-Assistent

Jetzt können Sie im Konfigurations-Assistenten wichtige Grundeinstellungen der Appliance abschließend vornehmen. Unter anderem auch die Standard Geräterichtlinien (Globale Einstellungen) indem sie den nächsten Schritten im Konfigurations-Assistenten folgen.



2.5. Appliance Grundeinstellungen

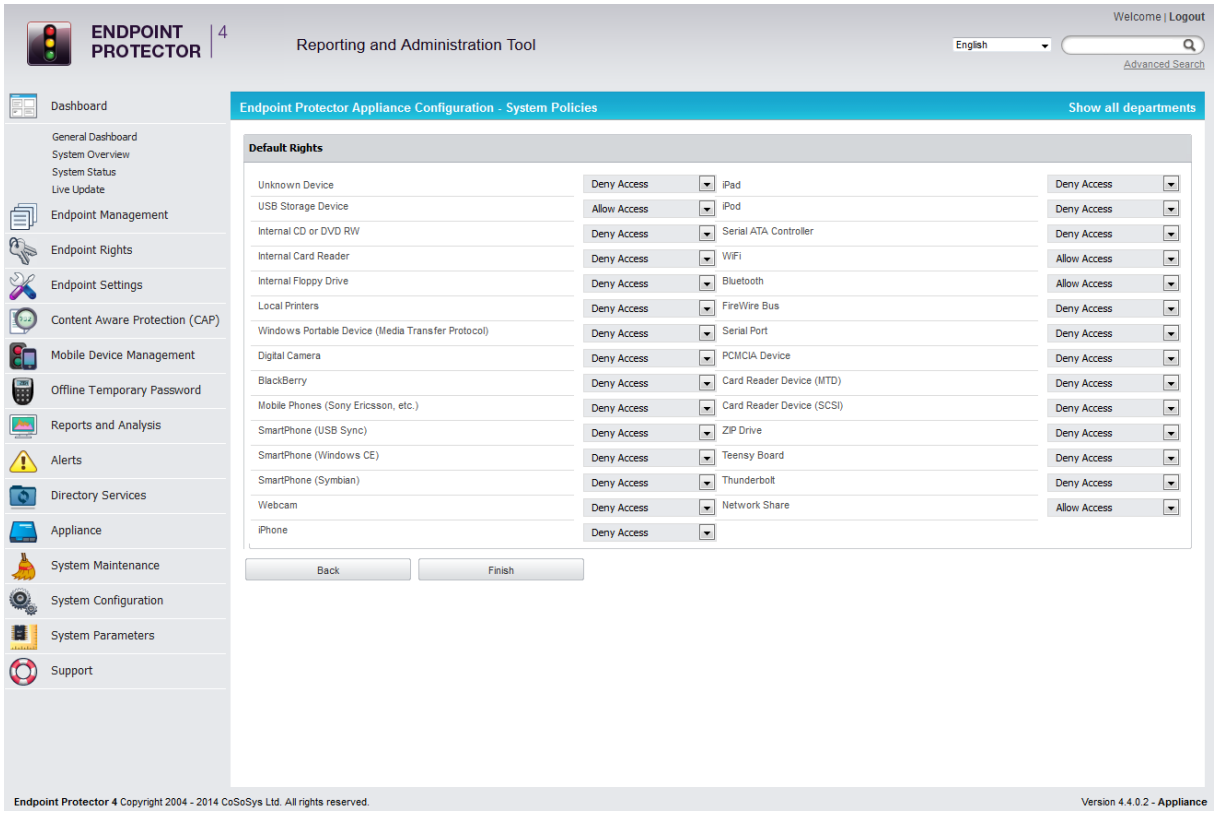
Bitte wählen Sie in diesem Schritt alle notwendigen Einstellungen aus. Wählen Sie, welche später definierten Rechte (Computer oder Benutzer) Vorrang haben werden. Legen Sie die E-Mail-Adresse unter der Sie System Benachrichtigungen empfangen wollen. Und legen Sie die Administrator Kontaktdaten fest, die den Benutzern im Offline Temporary Passwort System-Tray angezeigt werden sollen.



2.6. Standard Geräterichtlinie (Globale Einstellungen)

In diesem Schritt werden die Standard Geräterichtlinie festgelegt die als Grundeinstellung an die geschützten Computer kommuniziert werden.

Diese Standard Geräterichtlinie (Global Settings) kann später jederzeit wieder geändert werden.



2.7. Appliance Konfigurations-Assistent Beenden

Sie haben nun das Appliance Setup erfolgreich beendet.

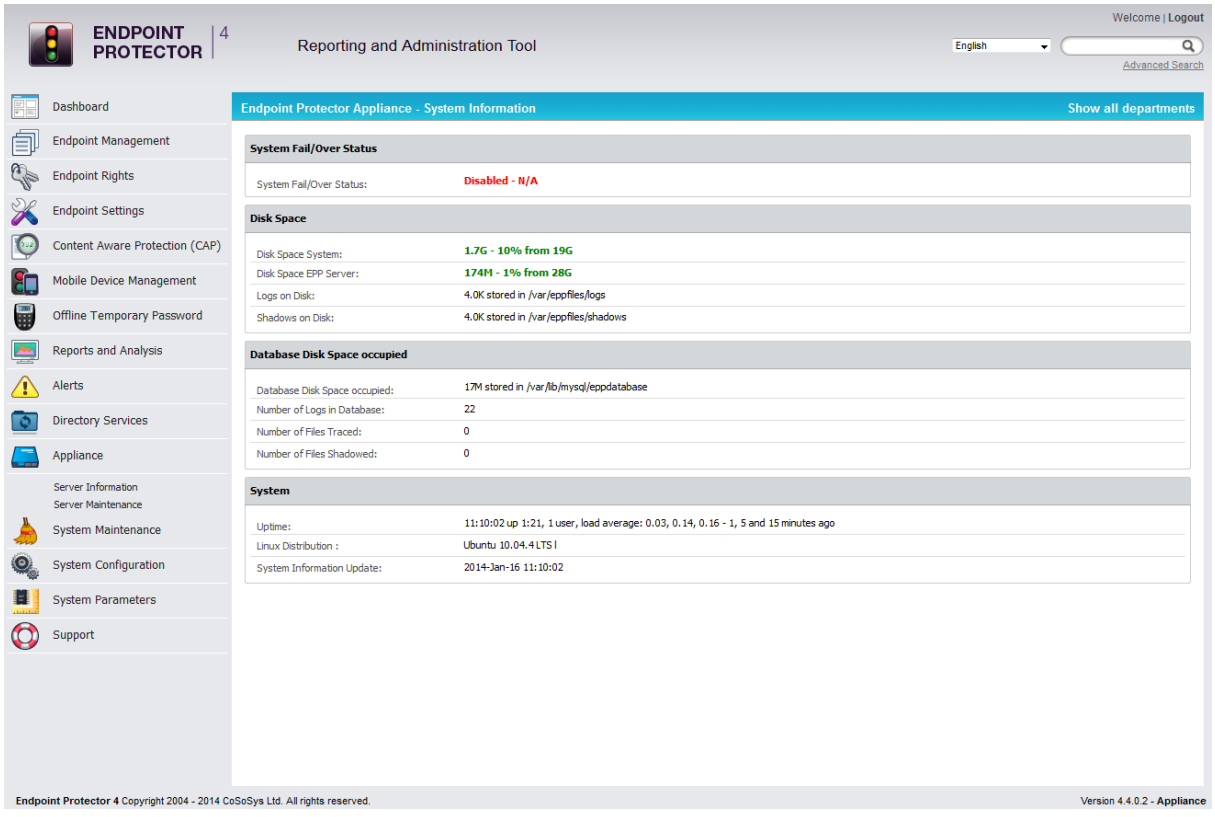
Nun empfehlen wir Ihnen zum Schutz Ihrer Windows und Macintosh Computer den Endpoint Protector Client auf diesen wie nachfolgenden in Kapitel 3.3 beschrieben zu installieren.

3. Appliance-Einstellungen und System Pflege

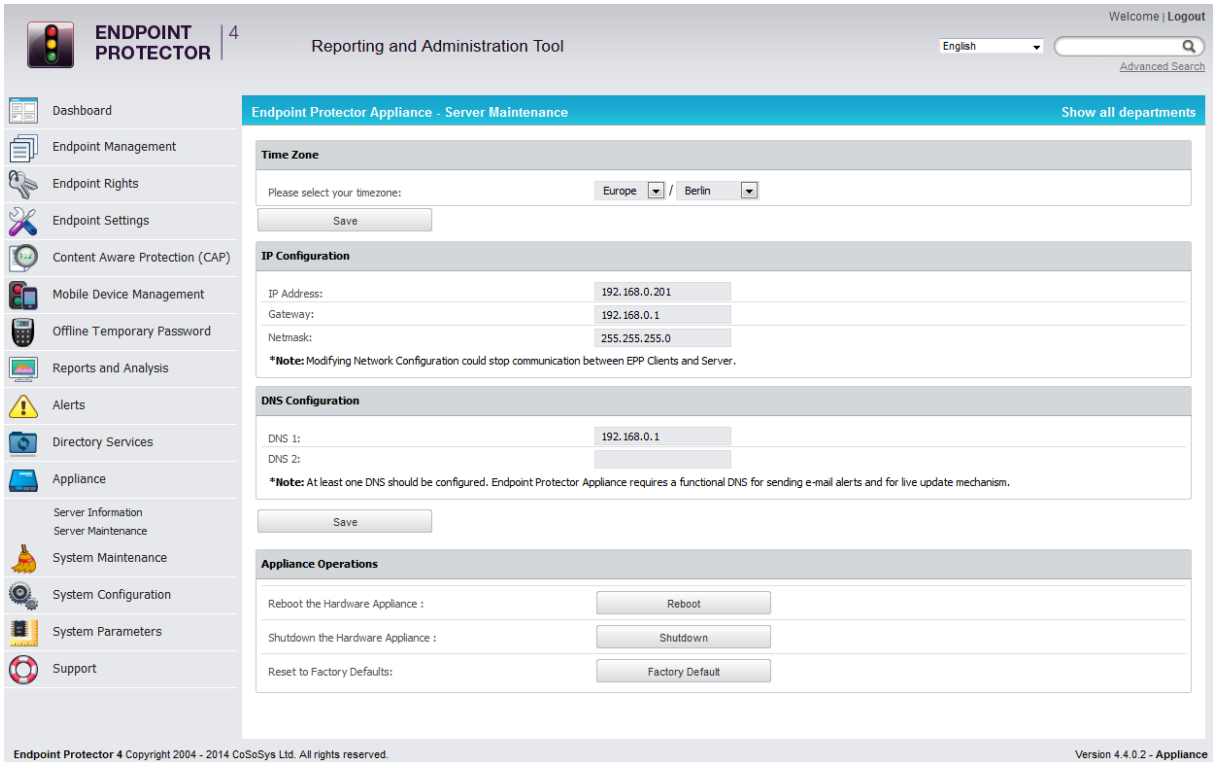
Auf die Endpoint Protector Appliance Einstellungen und System Pflege kann über das Administrations- und Reporting Cockpit unter dem Menüpunkt Appliance zugegriffen werden.

3.1. Server Informationen

Hier erhalten Sie auf einen Blick Informationen über den aktuellen Systemzustand der Appliance.



3.2. Server Pflege



3.2.1. Netzwerk Einstellungen

Unter diesem Menüpunkt kann die IP-Adresse der Endpoint Protector Appliance geändert werden sollte diese erforderlich sein.

3.2.2. Neustart / Reboot

Durch klicken der Taste Neustart / Reboot, wird die Appliance neu gestartet.

3.2.3. Werkseinstellungen / Factory Default

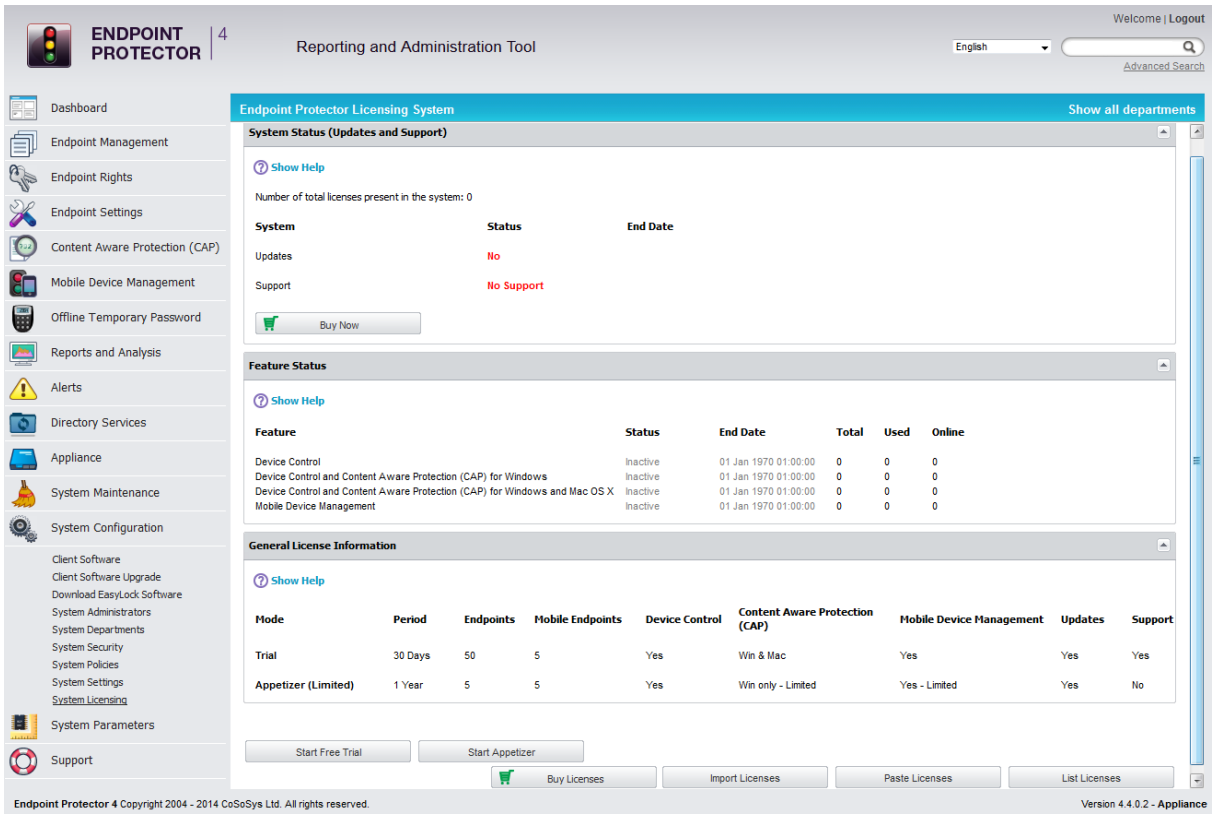
Wenn Sie Option auf Werkseinstellungen zurücksetzen ausführen, werden alle Einstellungen und die Kommunikation zwischen Appliance und Endpoint Protector Clients unterbrochen.

Eine komplette Neuinstallation aller Endpoint Protector Clients und eine neue Konfiguration der Appliance wird als Folge erforderlich sein.

3.3. Endpoint Protector Client Installation für Appliance

NOTE!

Bitte beachten Sie die Endpoint Protector Lizenzierung zu aktivieren, bevor Sie den EPP Client installieren. Die Lizenz kann unter Sistem Konfiguration -> Sistem Lizenz konfiguriert werden.



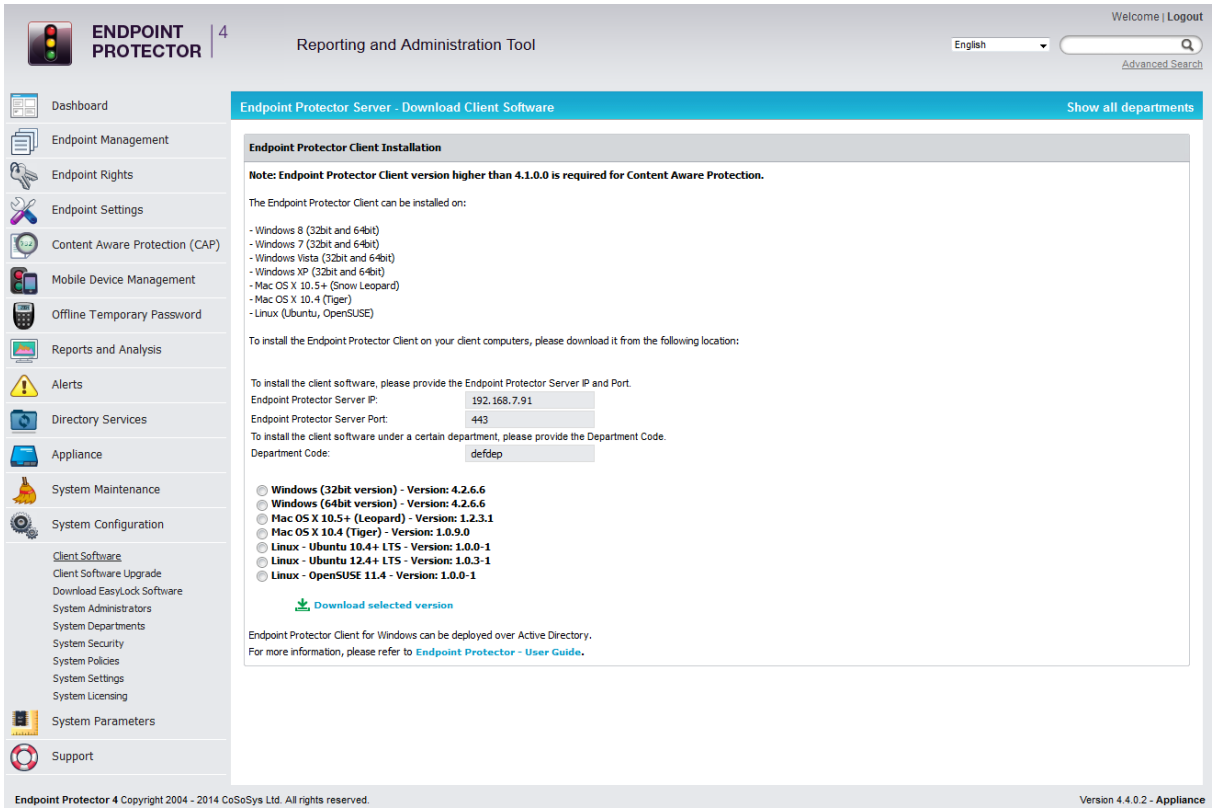
Als nächsten Schritt zur Absicherung Ihrer Computer, müssen Sie den Endpoint Protector Client auf den Windows- und Macintosh-Computern installieren, die Sie schützten wollen. Dadurch wird eine Verbindung und die Kommunikation zwischen der Endpoint Protector Appliance und Client Computer hergestellt.

Zur Installation der Endpoint Protector Clients auf Ihren Client-Computern, greifen Sie auf die Appliance über einen Internet Browser zu. Geben Sie dazu einfach die IP-Adresse in einen Browser ein (z.B. http://192.168.0.201) und eine Liste der Verfügbaren Endpoint Protector Clients wird Ihnen angezeigt.

Hinweis: Der Zugang ist über HTTP und nicht HTTPS um die Client Software anzuzeigen.

Bitte wählen Sie den passenden Client für das jeweilige Client-Computer Betriebssystem aus.

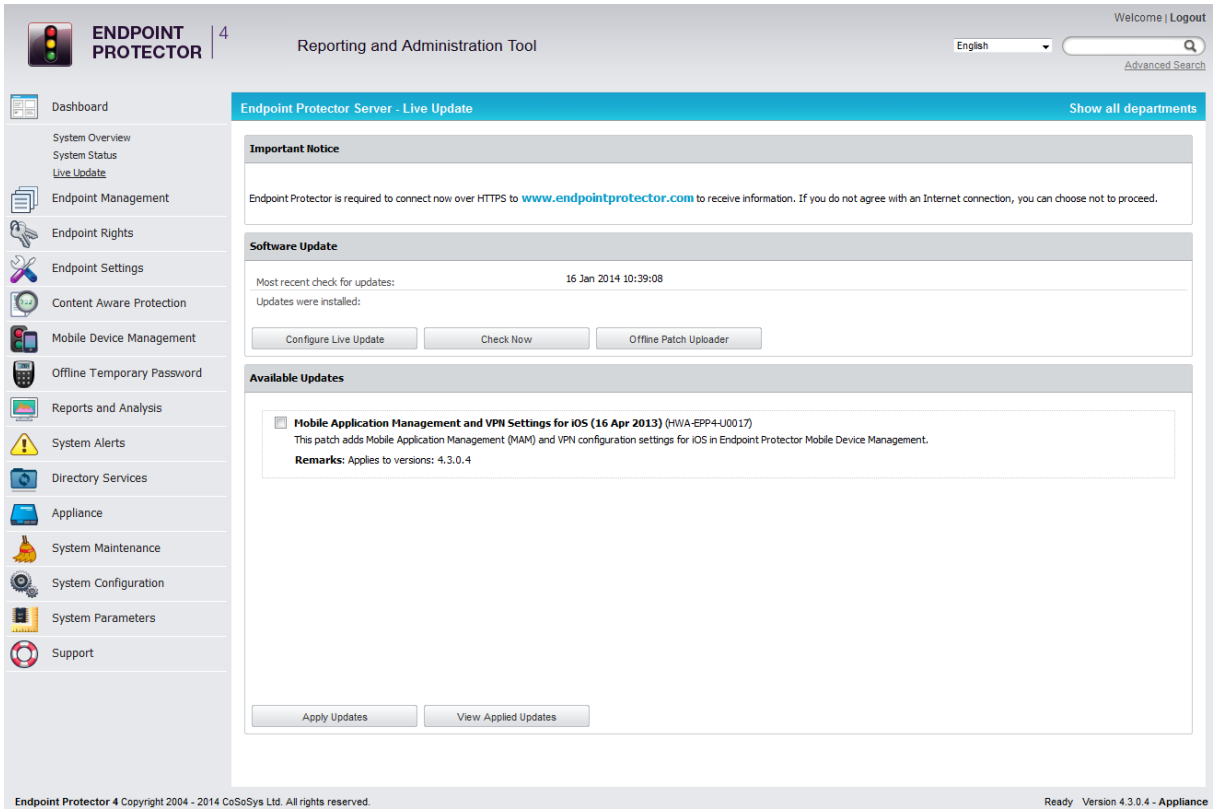
Active Directory kann zur Verteilung der Endpoint Protector Clients auch verwendet werden, und ist unter dem Endpoint Protector Menüpunkt System Konfiguration – Active Directory zu finden.



3.4. Appliance Online Live Update

Die Live-Update-Funktion prüft, ob Online-Updates für die Appliance und Endpoint Protector Client-Software verfügbar sind.

Sie haben die Wahl ob die Appliance automatisch nach Updates oder manuell die Verfügbarkeit von Updates überprüft. Updates werden nur installiert, wenn der Administrator „Update Ausführen" klickt.


ENDPOINT PROTECTOR 4
Reporting and Administration Tool
Welcome | Logout
English
Advanced Search
Dashboard
System Overview
System Status
Live Update
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection
Mobile Device Management
Offline Temporary Password
Reports and Analysis
System Alerts
Directory Services
Appliance
System Maintenance
System Configuration
System Parameters
Support
Endpoint Protector Server - Live Update
Show all departments
Important Notice
Endpoint Protector is required to connect now over HTTPS to www.endpointprotector.com to receive information. If you do not agree with an Internet connection, you can choose not to proceed.
Software Update
Most recent check for updates:
16 Jan 2014 10:39:08
Updates were installed:
Configure Live Update
Check Now
Offline Patch Uploader
Available Updates
Mobile Application Management and VPN Settings for iOS (16 Apr 2013) (HWA-EPP4-U0017)
This patch adds Mobile Application Management (MAM) and VPN configuration settings for iOS in Endpoint Protector Mobile Device Management.
Remarks: Applies to versions: 4.3.0.4
Apply Updates
View Applied Updates
Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.
Ready Version 4.3.0.4 - Appliance

4. Zertifikat als Root-Zertifikat einem Internet Browser hinzufügen

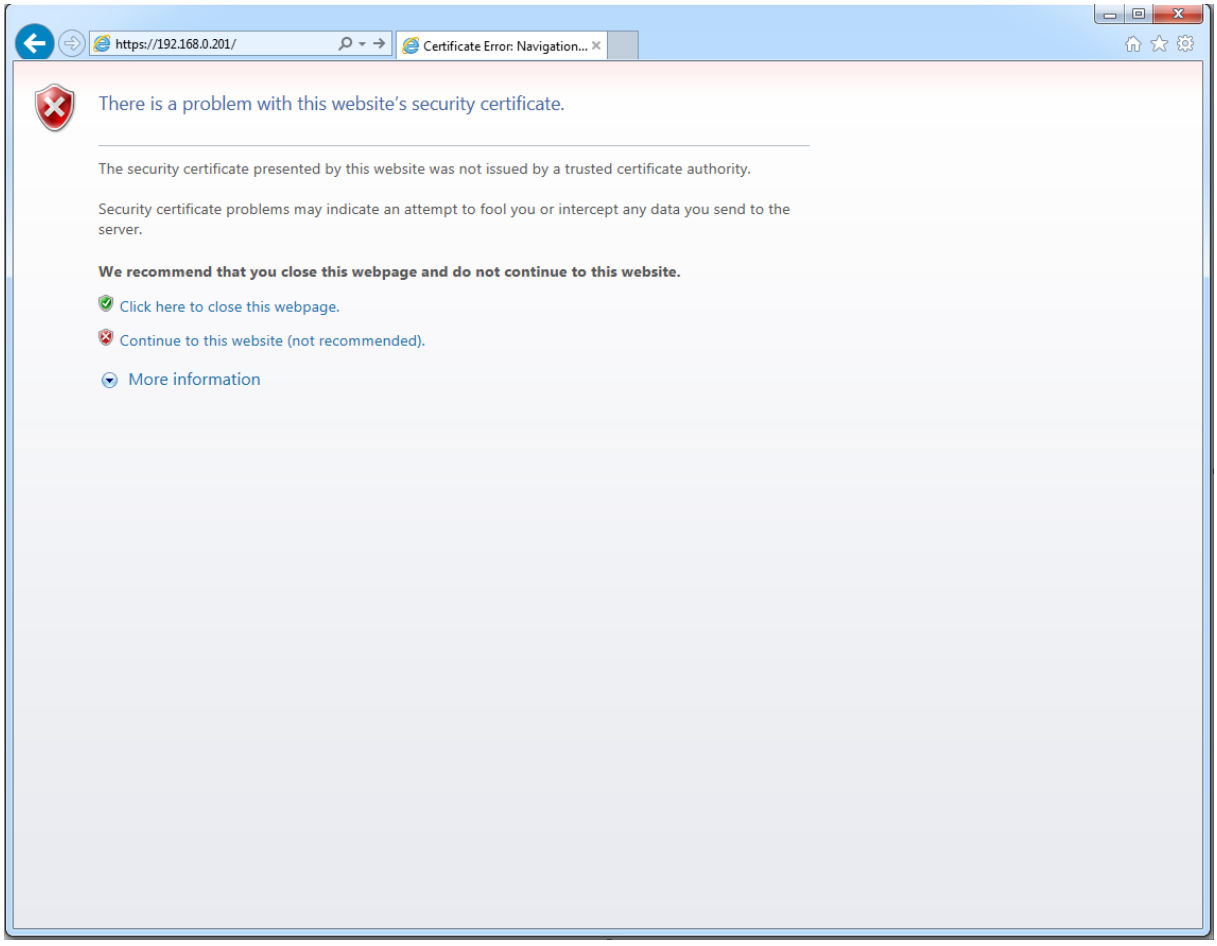
Wir empfehlen Ihnen das Root-Zertifikat der Endpoint Protector Appliance den vertrauenswürdigen Stammzertifikate Ihres Internet Browsers hinzuzufügen.

Sollten Sie das Zertifikat nicht den vertrauenswürdigen Stammzertifikate Ihres Internet Browsers hinzuzufügen, dann akzeptieren Sie bitte die Fehlermeldung für ungültige Zertifikate in Ihrem Internet Browser.

4.1. Für Microsoft Internet Explorer

Öffnen Sie das Endpoint Protector Administrations-Cockpit unter der IP-Adresse im Browser (z.B. http://192.168.0.201).

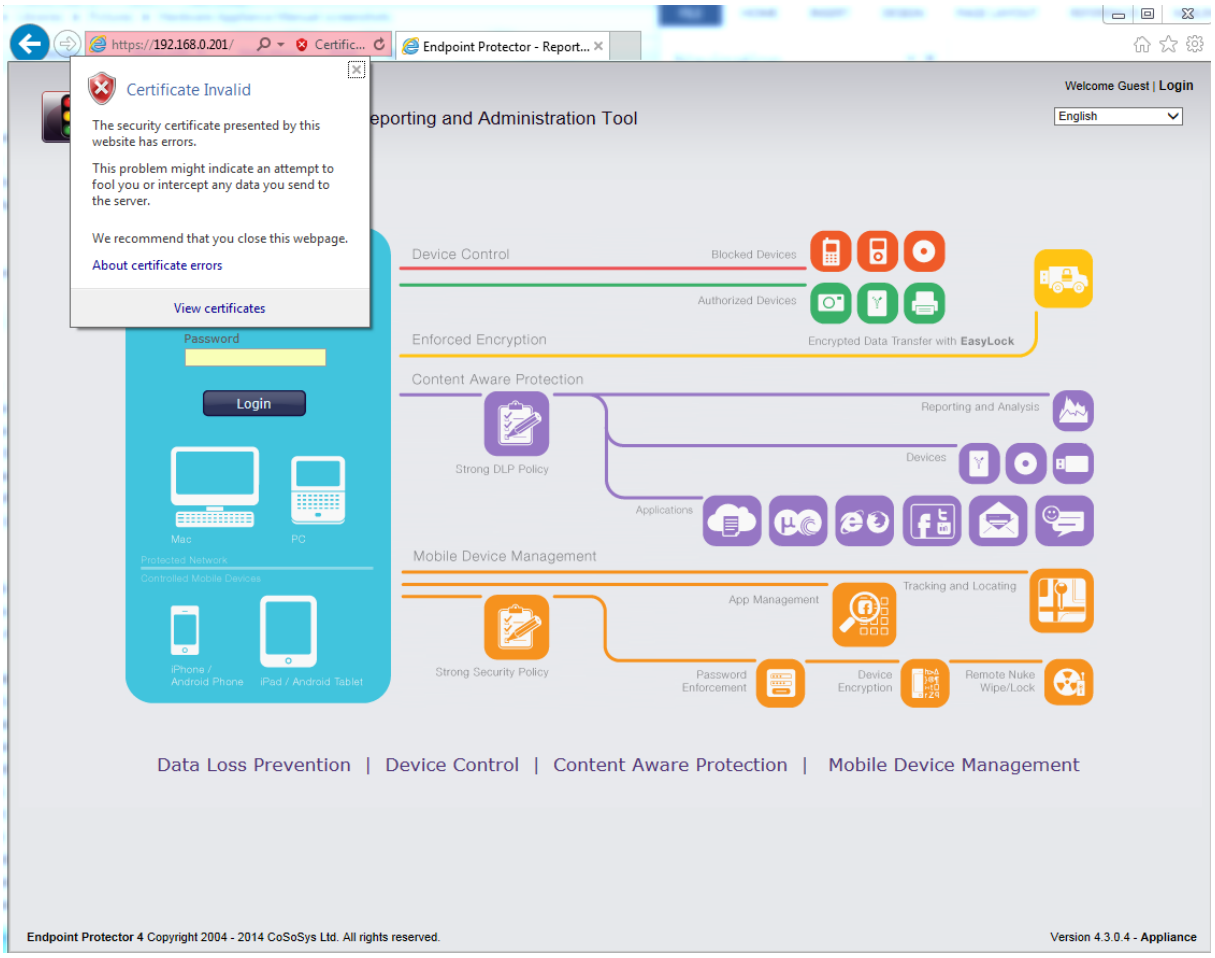
Wichtig ist für die nachfolgenden Schritte das die IP-Adresse dem Internet Explorer bereits zuvor wie in Schritt 1.7.5 beschrieben den Vertrauenswürdigen Sites hinzugefügt wurde.



Wurde das Zertifikat nicht bereits installiert, sehen Sie nachfolgende Zertifikat Fehlermeldung.

Bitte fahren Sie fort, indem Sie auf die Option  "Laden dieser Webseite fortsetzen (nicht empfohlen)" klicken.

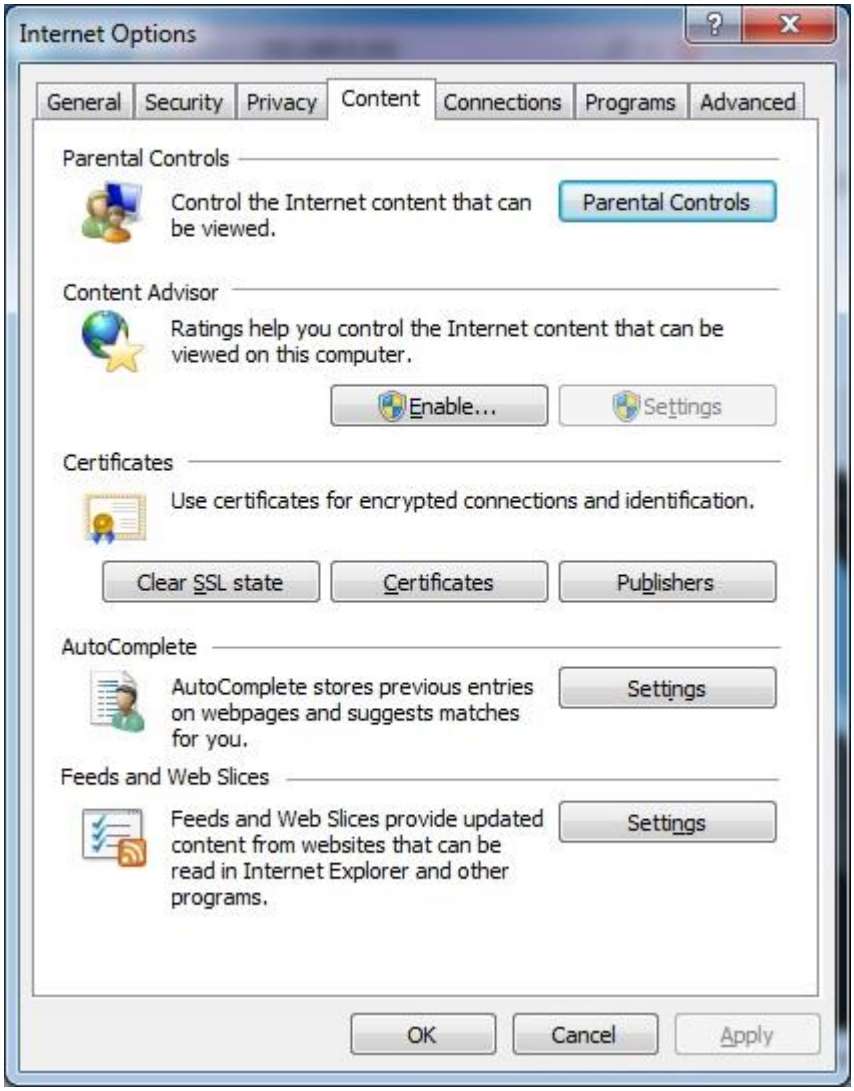
Klicken Sie auf die Schaltfläche „Zertifikatfehler" gleich neben der Internet Explorer URL Adressleiste. Durch Anklicken der Taste " Zertifikatfehler", erscheint ein Pop-up Fenster.



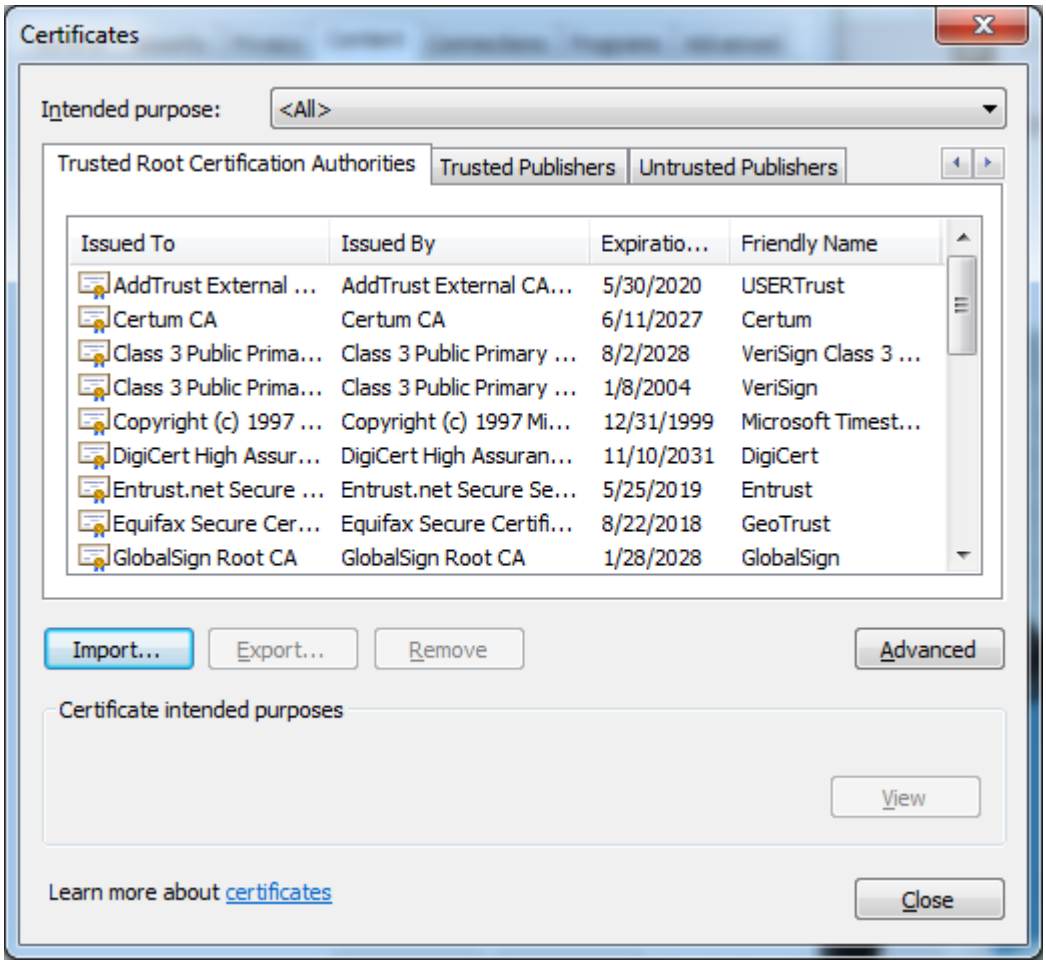
Klicken Sie jetzt auf Schaltfläche "Zertifikate anzeigen" in diesem Pop-up-Fenster.

Ein weiteres Pop-up-Fenster öffnet sich dadurch, welches drei Registerkarten anzeigt. Unter der ersten Registerkarte „Allgemein" klicken Sie bitte auf „Zertifikat installieren".

Sollten Sie die Schaltfläche "Zertifikat installieren" nicht angezeigt bekommen, wurde die IP-Adresse wie in Schritt 1.4.6 beschrieben noch nicht den Vertrauenswürdigen Sites hinzugefügt.

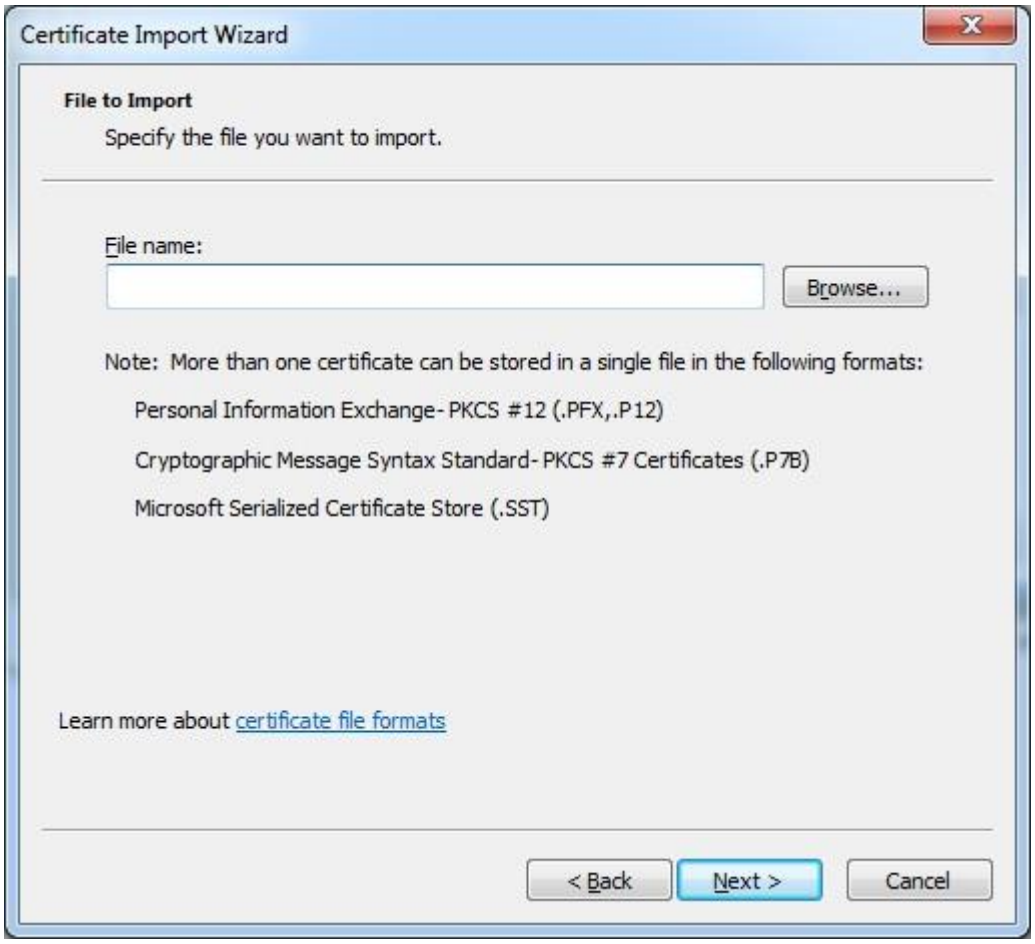


Aus der Liste waehlen Sie bitte “Vertrauenswürdige Zertifizierungsstellen” aus und klicken “Import”.

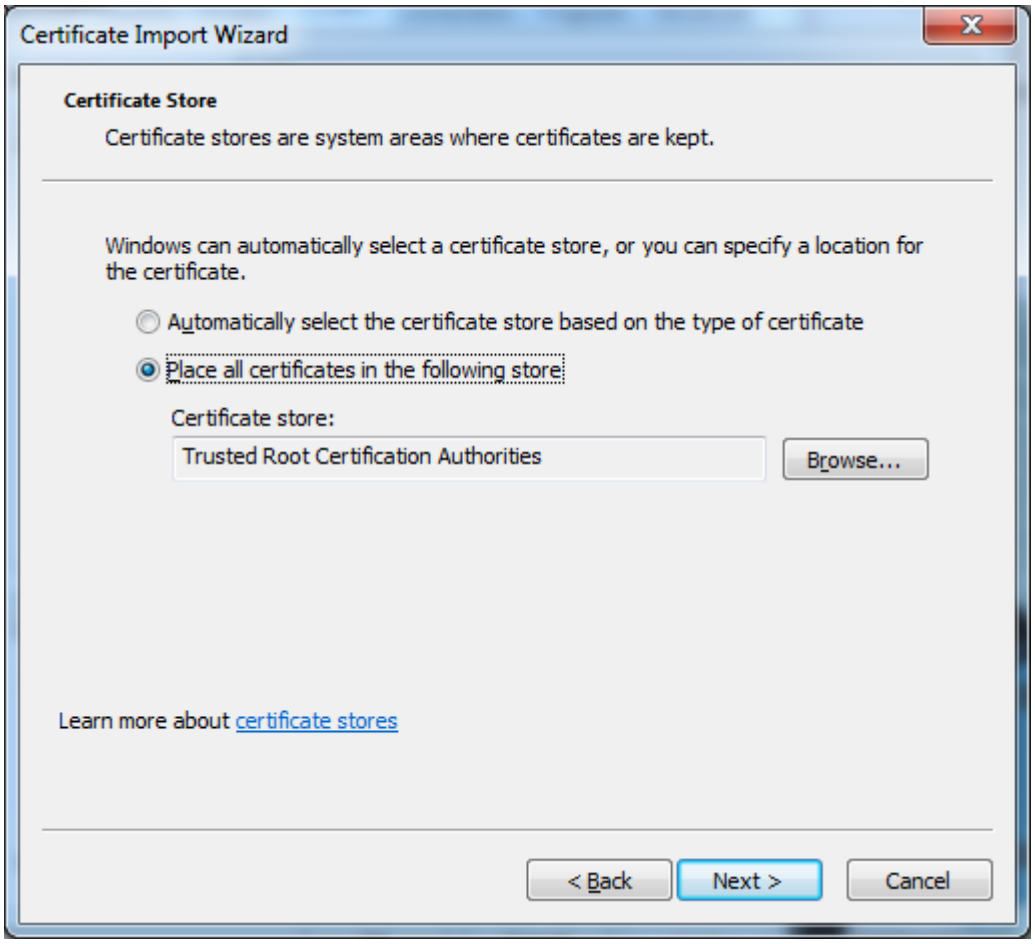


Ein Zertifikatimport-Assistent öffnet sich. Klicken Sie auf die Schaltfläche Weiter.

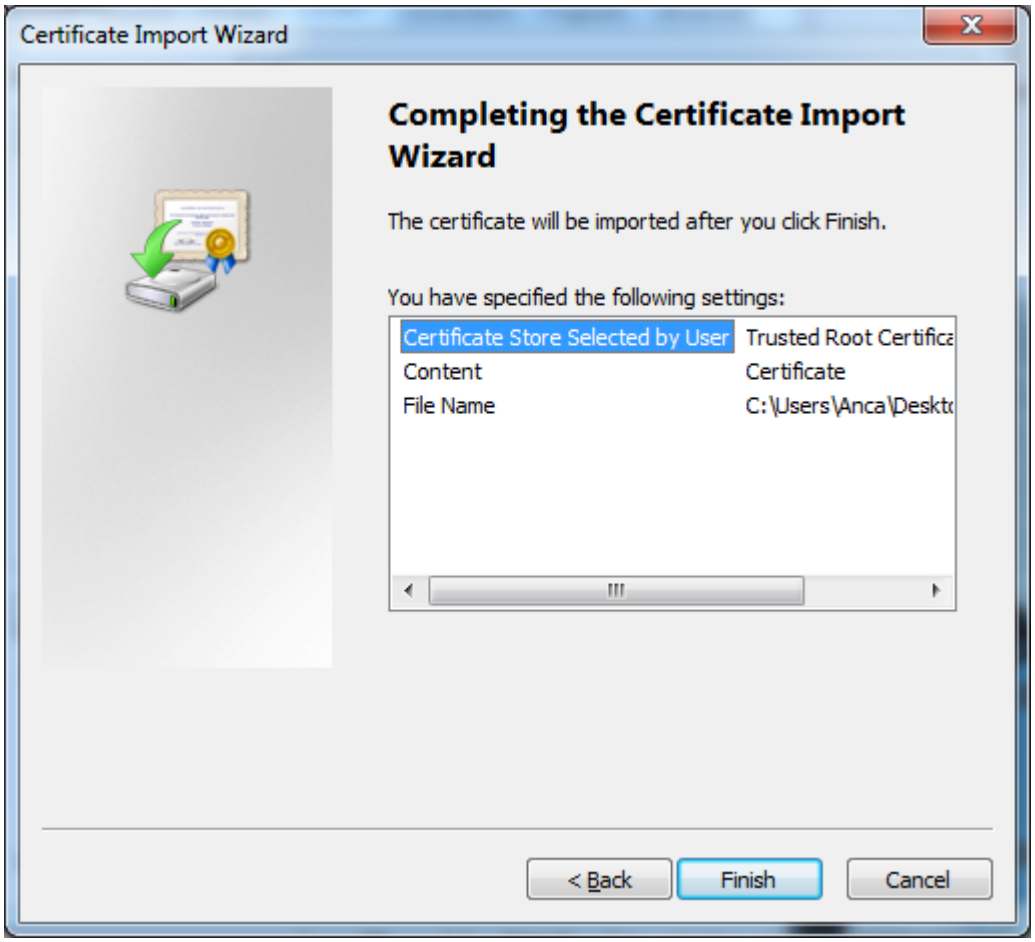
Klicken Sie auf "Durchsuchen"**.**



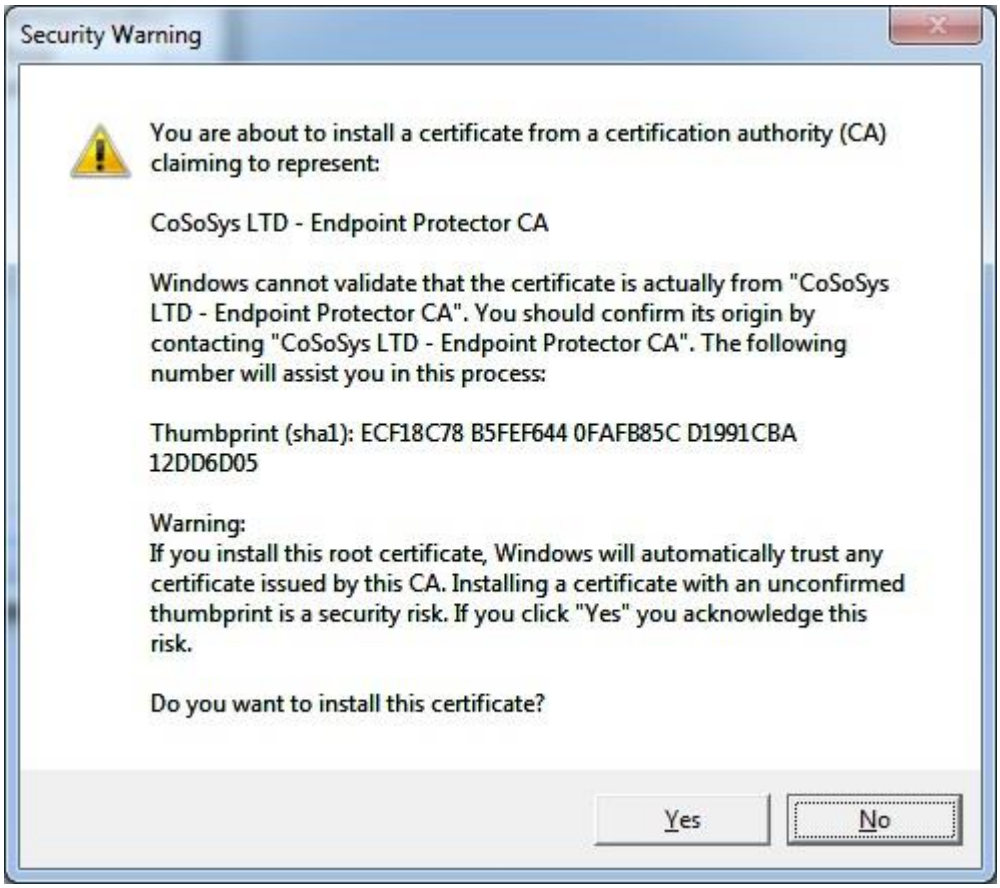
Im Zertifikatimport-Assistent wählen Sie bitte die zweite Option "Alle Zertifikate in folgendem Speicher speichern".



Klicken Sie auf „Weiter„ um fortzufahren.

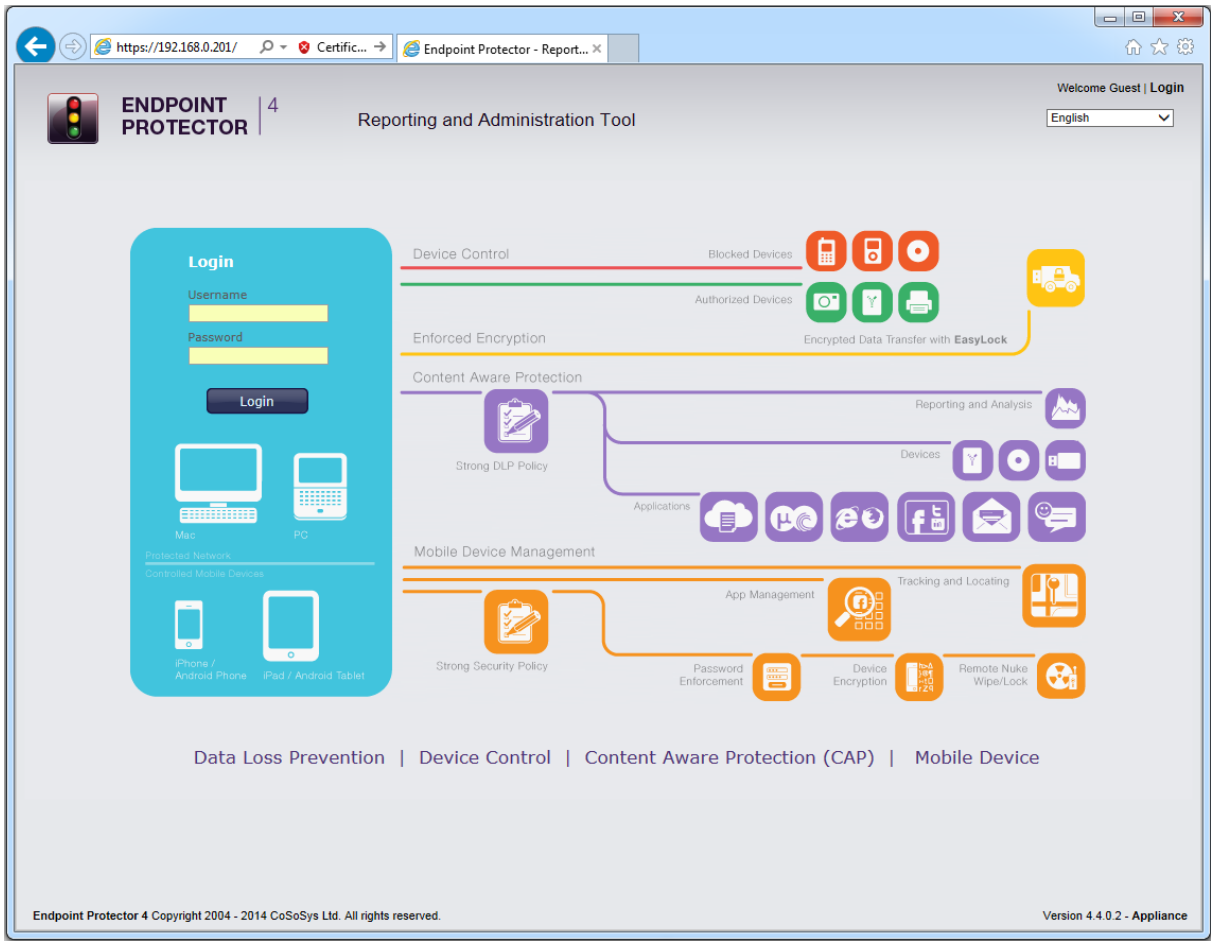


Klicken Sie auf „Fertig stellen“ um fortzufahren.



Eine „Sicherheitswarnung" erscheint. Klicken Sie bitte auf "Ja".

Sie haben nun erfolgreich das Zertifikat installiert.



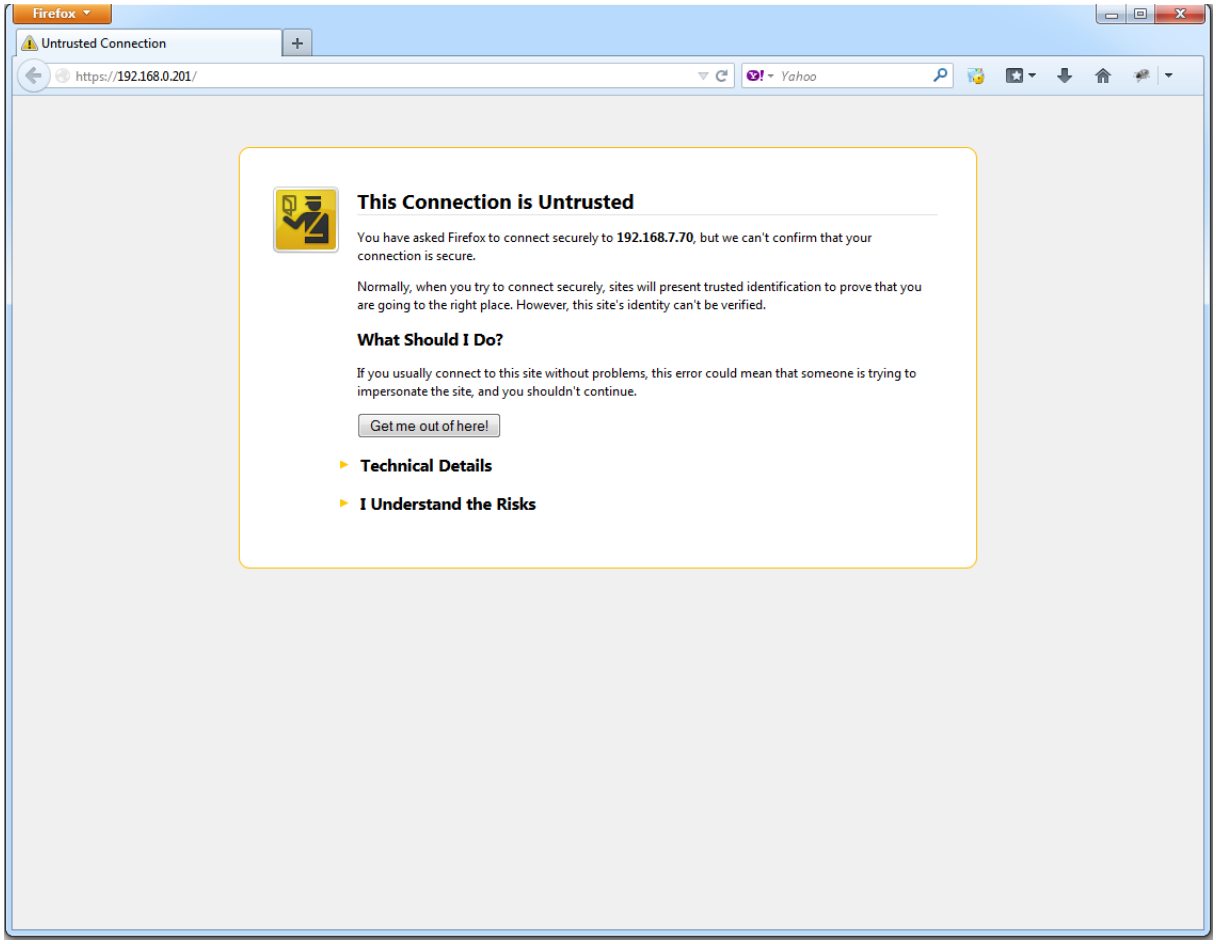
Schließen Sie jetzt bitte Internet Explorer und öffnen erneut das Endpoint Protector Administrations-Cockpit unter der IP-Adresse im Browser.

4.2. Für Mozilla Firefox

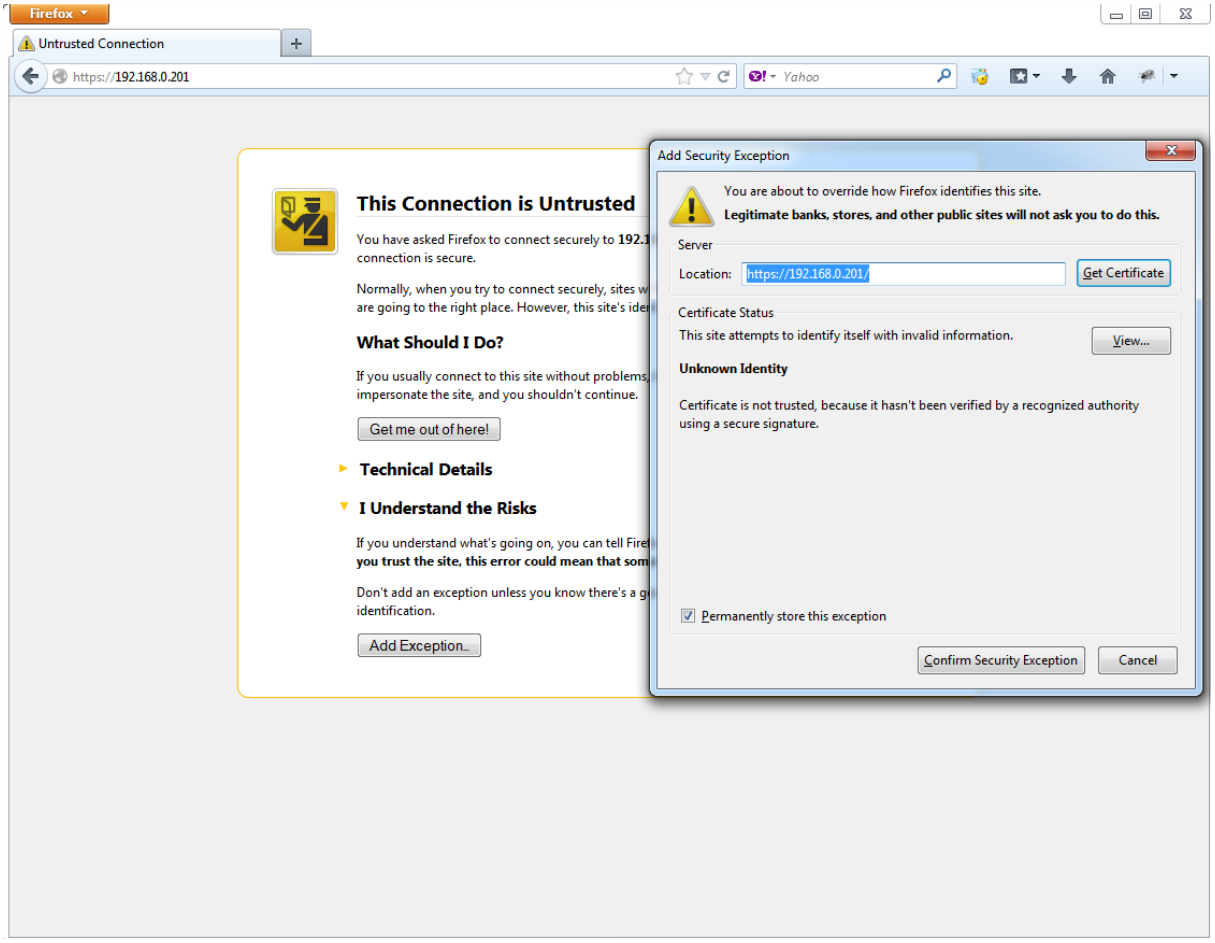
Starten sie Mozilla Firefox.

Öffnen Sie das Endpoint Protector Administrations-Cockpit unter der IP-Adresse im Browser (z.B. http://192.168.0.201).

Der Mozilla Firefox Browser zeigt an „Dieser Verbindung wird nicht vertraut". Klicken Sie auf „Ich kenne das Risiko" um fortzufahren.

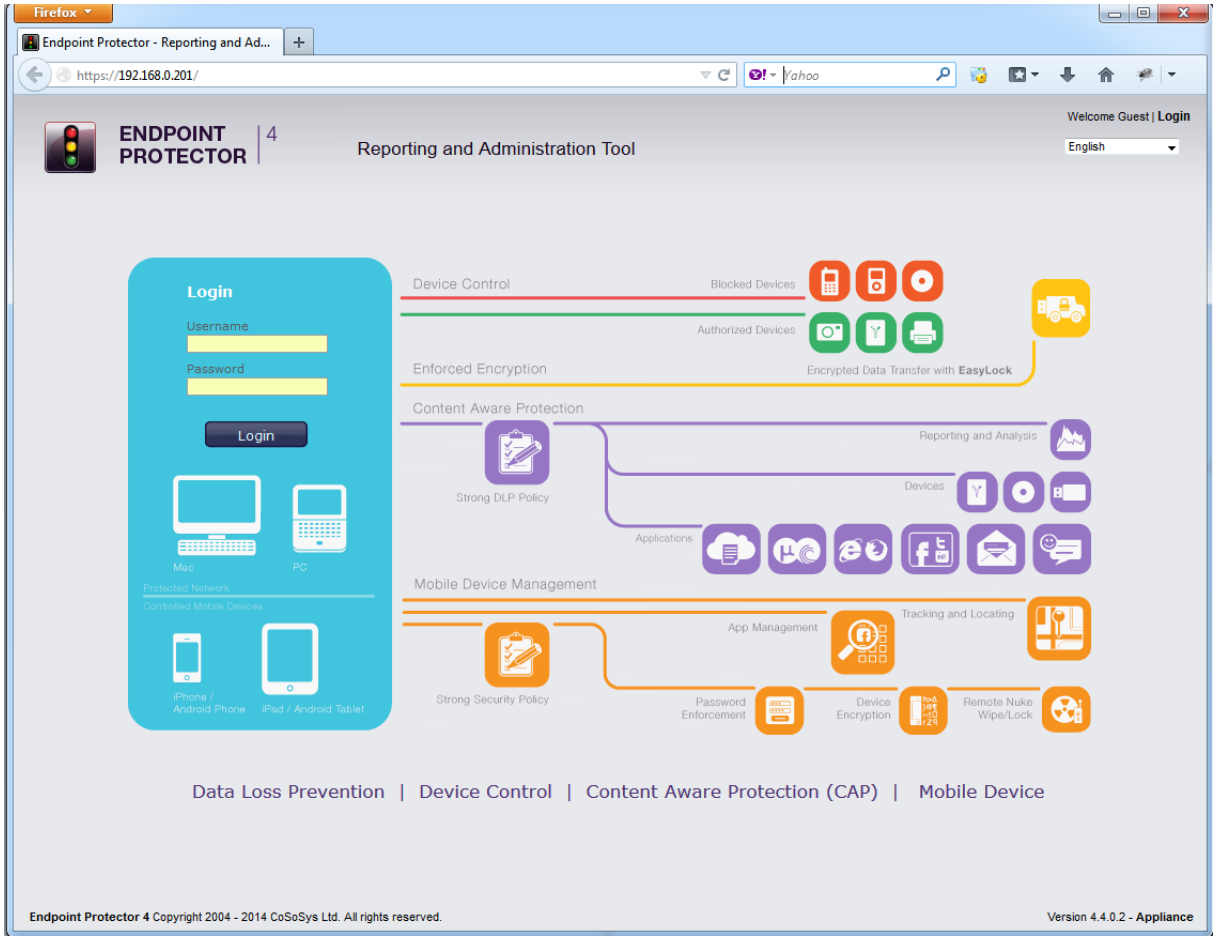


Klicken Sie auf „Ausnahme hinzufügen“. Ein Fester “Sicherheits-Ausnahmeregel hinzufügen” öffnet sich.



Klicken Sie auf „Zertifikat herunterladen“ und danach auf „Sicherheits-Ausnahmeregel bestätigen“.

Schließen Sie jetzt bitte Mozilla Firefox und öffnen erneut das Endpoint Protector Administrations-Cockpit unter der IP-Adresse im Browser.



5. Support / Hilfe

Brauchen Sie weitere Hilfe, wie FAQs oder E-Mail-Support, besuchen Sie bitte unsere Support-Website unter http://www.cososys.com/help.html.