



ENDPOINT PROTECTOR APPLIANCE

Benutzerhandbuch Version 4.0.0.4

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



Inhaltsverzeichnis

1.Endpoint Protector Appliance Setup	1
1.1. Endpoint Protector Appliance Lieferumfang.....	1
1.2. Verbinden der Appliance für erstes Setup.....	2
1.3. Hardware Appliance Rückseite / Vorderseite	3
1.3.1. A20 Appliance Rückseite	3
1.3.2. A50 und A100 Appliance Rückseite.....	3
1.3.3. A20 Appliance Vorderseite.....	3
1.3.4. A50 und A100 Appliance Vorderseite	4
1.3.5. A250, A500 und A1000 Appliance Vorderseite	4
1.3.6. A2000 - A4000 Appliance Vorderseite	5
1.4. A2000 / A4000 Appliance HDD Konfiguration.....	5
1.4.1. A2000 Appliance HDD Konfiguration	5
1.4.2. A4000 Appliance HDD Konfiguration	6
1.4.3. A2000 - A4000 Appliance HDD RAID 3ware® 3DM® Zusatz-Software.....	6
1.5. Zugriff auf Appliance Setup-Assistent mit normalem Netzkabel (nur für A20)	7
1.6. Zugriff auf Appliance Setup-Assistent mit gekreuztem Netzkabel (für A50 und größere Modelle)	8
1.7. Appliance Setup-Assistent.....	9
1.7.1. End User Lizenzvertrag - Appliance Lizenzvertrag.....	9
1.7.2. Definieren Sie Ihr Appliance Administrator-Passwort.....	10
1.7.3. Netzwerk IP Adresse der Appliance Festlegen	12
1.7.4. Endpoint Protector Client – Automatische MSI Anpassung ..	14
1.7.5. Appliance Server Zertifikat	15
1.7.6. Beenden des Endpoint Protector Appliance Setup	16
2.Endpoint Protector Appliance Konfiguration	17
2.1. Verbindung zwischen Appliance und Netzwerk	17
2.2. Appliance Web-Interface über Netzwerk öffnen.....	17
2.3. Anmeldung am Appliance Web-Interface.....	18
2.4. Appliance Konfigurations-Assistent.....	19
2.5. Appliance Grundeinstellungen.....	20

2.6. Standard Geräterichtlinie (Globale Einstellungen).....	21
2.7. Appliance Konfigurations-Assistent Beenden.....	21
3.Appliance-Einstellungen und System Pflege	22
3.1. Server Informationen	22
3.2. Server Pflege.....	23
3.2.1. Netzwerk Einstellungen.....	23
3.2.2. Neustart / Reboot	23
3.2.3. Werkseinstellungen / Factory Default.....	23
3.3. Endpoint Protector Client Installation für Appliance	24
3.4. Appliance Online Live Update.....	25
4.Zertifikat als Root-Zertifikat einem Internet Browser hinzufügen	27
4.1. Für Microsoft Internet Explorer	28
4.2. Für Mozilla Firefox	38
5.Support / Hilfe	41

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 Netzkabel für das Appliance Setup (gelbe Markierung) (nicht bei A20 enthalten da nicht erforderlich)
- Netzkabel 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.

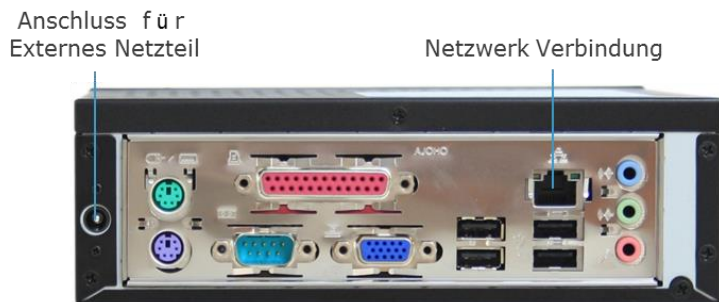
Ihre Hardware-Appliance (Modelle von A50 bis A4000) besitzt auf der Rückseite zwei Netzwerk-Ports diese sind gelb markiert für CONFIG (Konfigurations-Verbindung) und blau für NET (Netzwerk Verbindung) markiert. Die A20 Appliance hat einen Netzwerk-Port welcher für die Inbetriebnahme der A20 ausreicht.

Schließen Sie das gekreuztes Netzworkkabel (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).

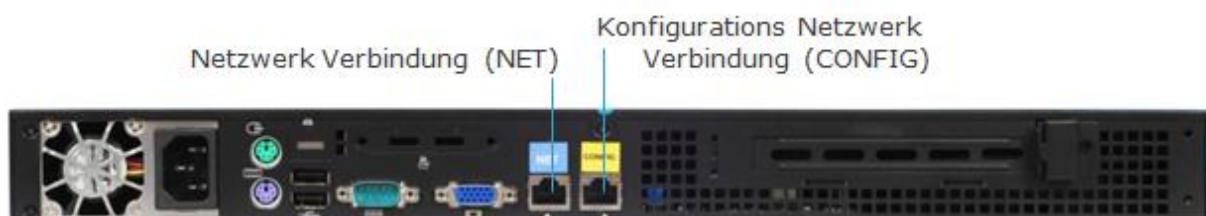
Starten Sie die Appliance, indem Sie den An-Schalter drücken.

1.3. Hardware Appliance Rückseite / Vorderseite

1.3.1. A20 Appliance Rückseite



1.3.2. A50 und A100 Appliance Rückseite

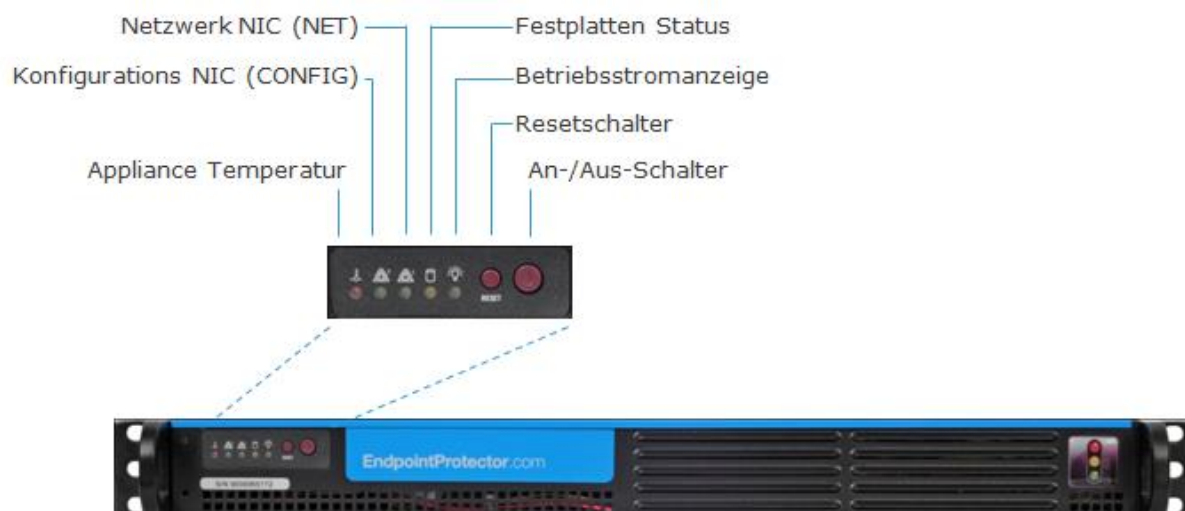


Die Rückseite der Modelle A250 bis A4000 verfügen ebenfalls über blau und gelb markierte Netzwerk-Ports wie die oben dargestellte A50 und A100 Appliance.

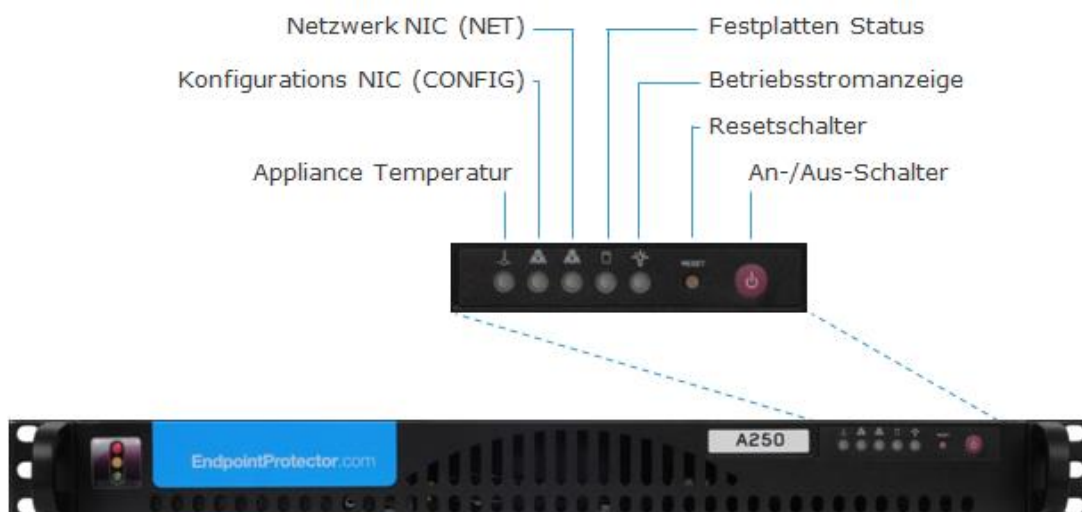
1.3.3. A20 Appliance Vorderseite



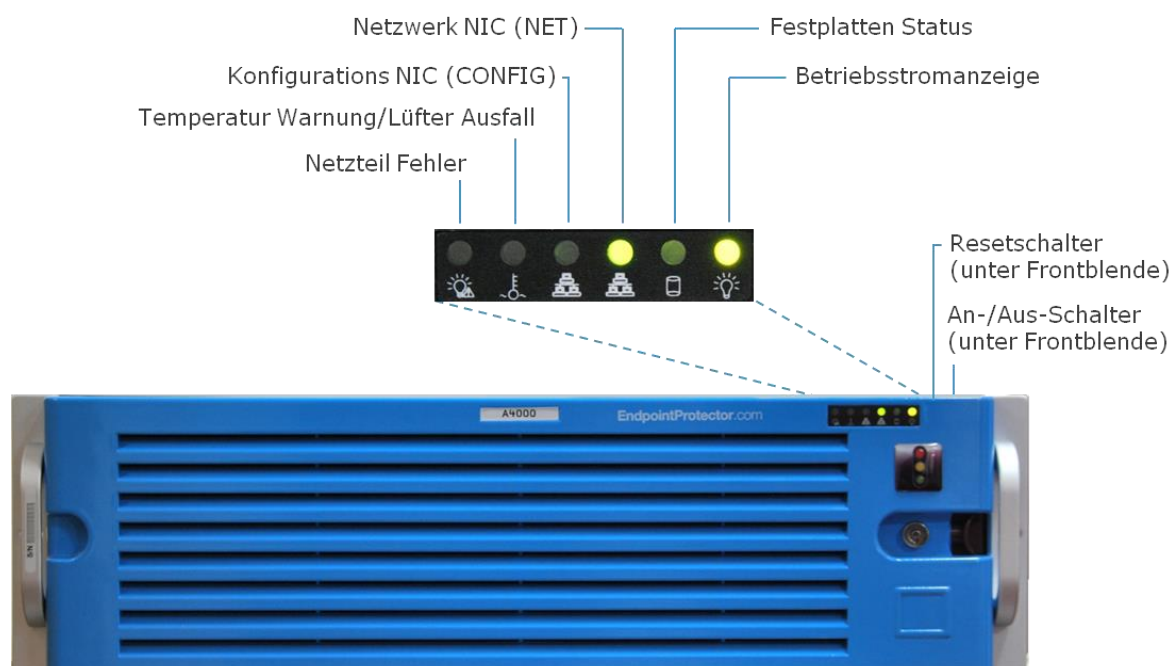
1.3.4. A50 und A100 Appliance Vorderseite



1.3.5. A250, A500 und A1000 Appliance Vorderseite

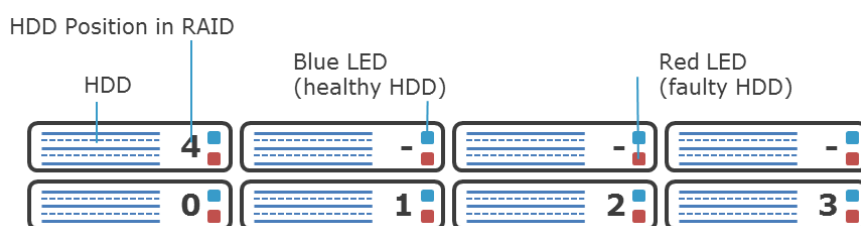


1.3.6. A2000 - A4000 Appliance Vorderseite



1.4. A2000 / A4000 Appliance HDD Konfiguration

1.4.1. A2000 Appliance HDD Konfiguration

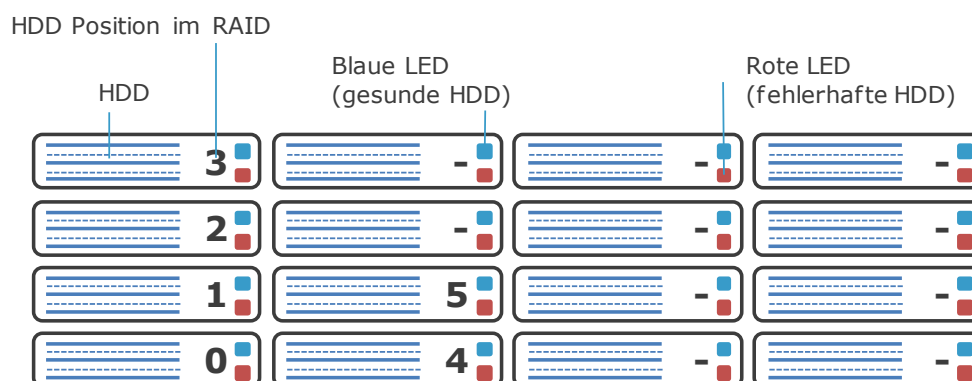


Die A2000 Appliance verfügt über 4 Festplatten in RAID 5 Konfiguration. Die Festplatten sind in der von 0-3 nummerierten Reihenfolge installiert.

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

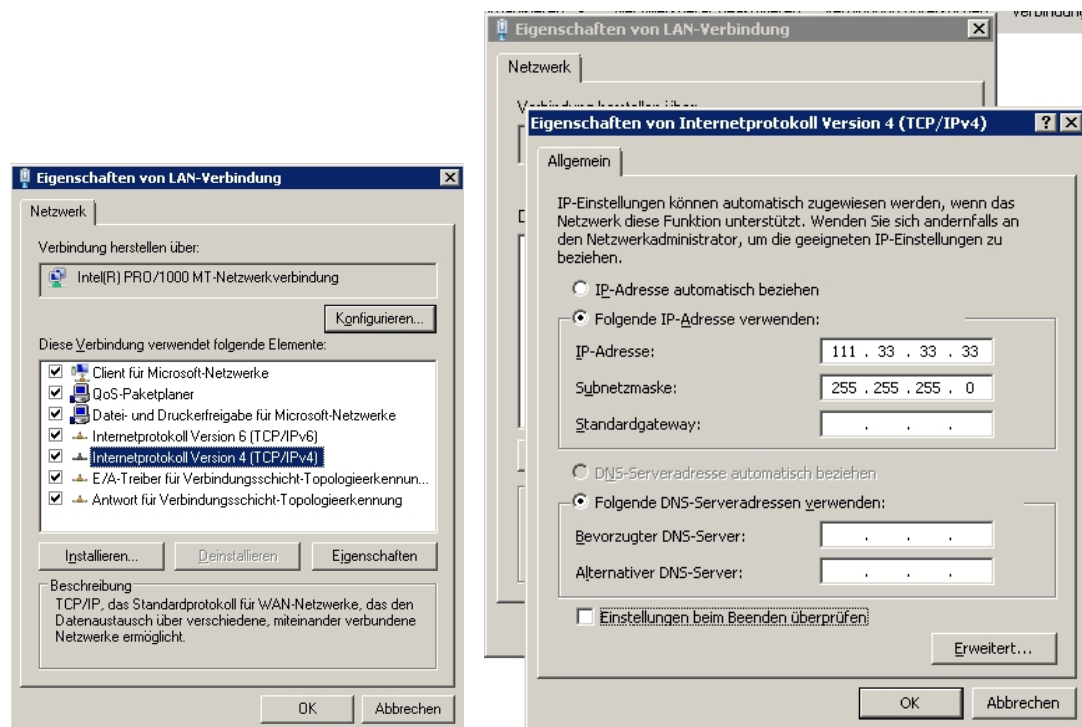
Die A2000 und A4000 Appliance verfügen über einen zusätzlich konfigurierbare Software von 3Ware® mit der Sie als Administrator über mögliche Fehler an einer der Festplatten per E-Mail gewarnt/informiert werden können. Weiter Informationen zur Konfiguration dieser Zusatzsoftware finden Sie in unserem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

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

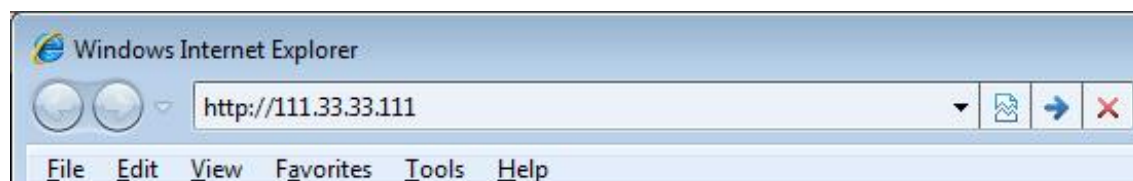
Verbinden Sie den blauen Kabel zu den A20 Netzwerkport und danach zu dem Netzwerk. Die Netzwerkeinstellungen auf Ihrem Computer sollten für TCP/IPv4 folgende sein:

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.

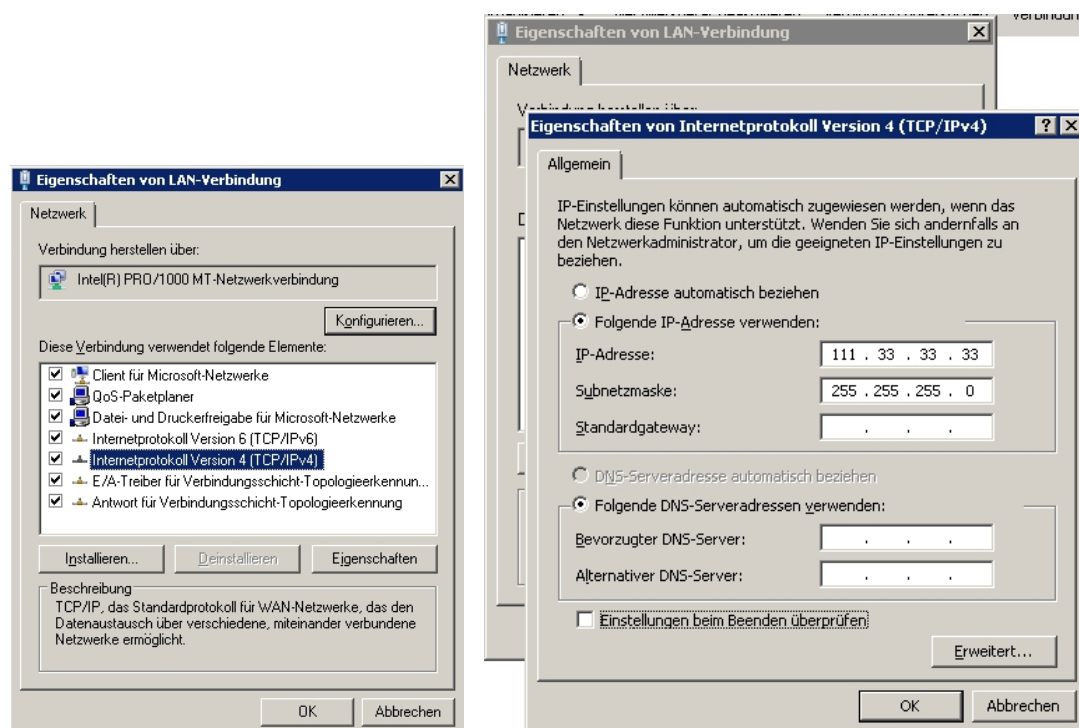


1.6. Zugriff auf Appliance Setup-Assistent mit gekreuztem Netzkabel (für A50 und größere Modelle)

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)

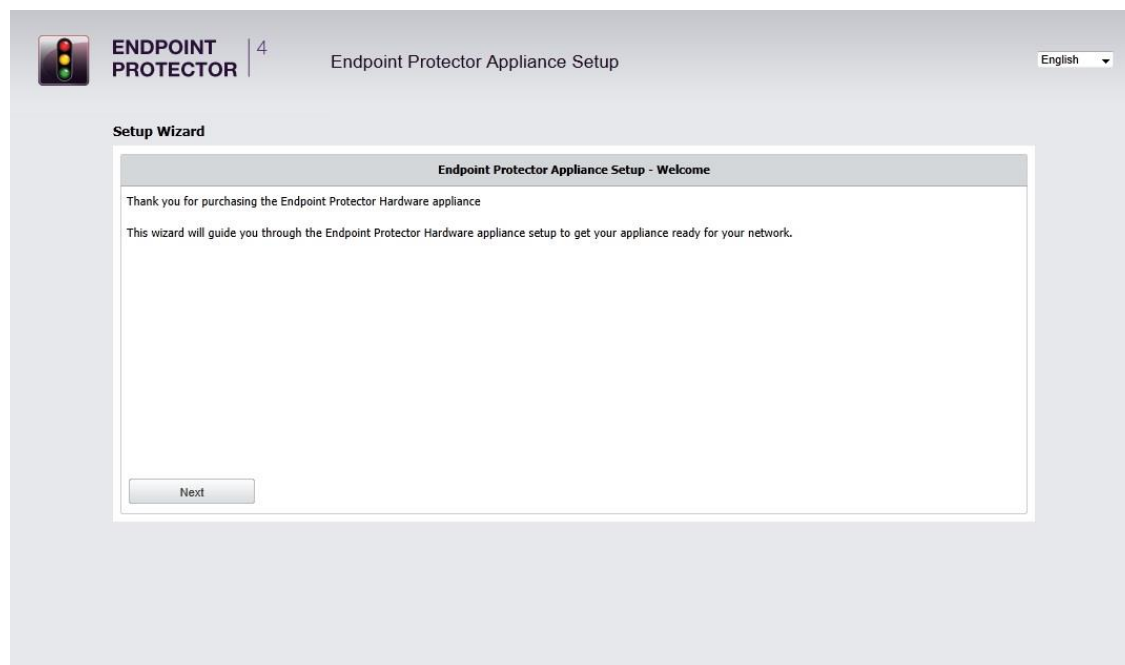


Dann können Sie über einen Internet-Browser über die folgende IP Adresse zugreifen. Geben Sie diese einfach <http://111.33.33.111> in die URL Leiste ein.

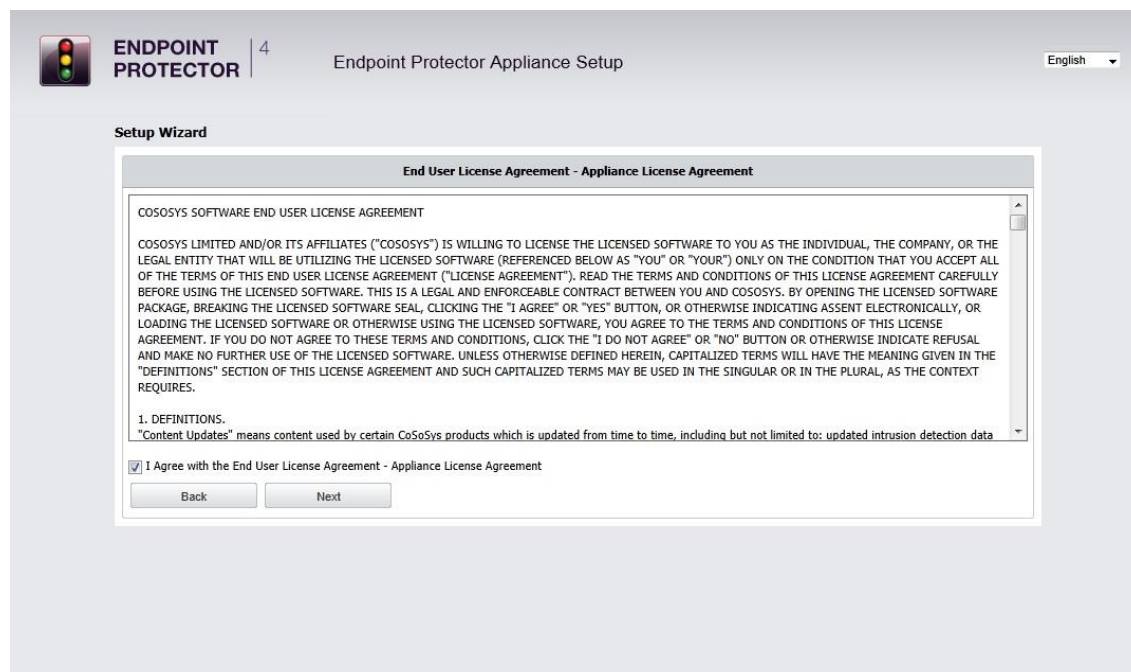


1.7. Appliance Setup-Assistent

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

Endpoint Protector Appliance Setup - Administrator Password

Username: root

Password: ••••••••

Password Confirm: ••••••••

Minimum six characters. Password is case sensitive.

Back Next skip this step

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

Endpoint Protector | 4 | Endpoint Protector Appliance Setup | English

Setup Wizard

Endpoint Protector - Appliance Settings

Select your time zone to display time related data. Seasonal times are adjusted automatically.

Timezone: Europe / Berlin

Configure the network settings for the appliance to communicate correctly in your network.

IP Address: 192.168.0.73

Gateway: 192.168.0.1

Network Mask: 255.255.255.0

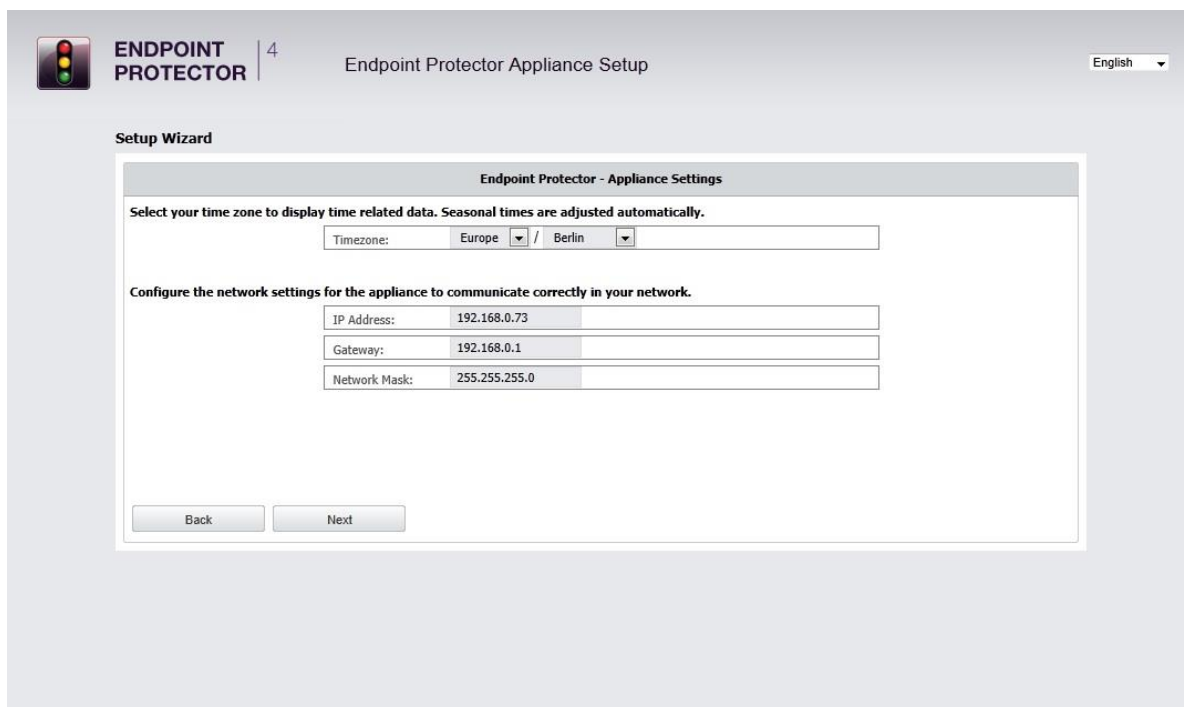
Back Next

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

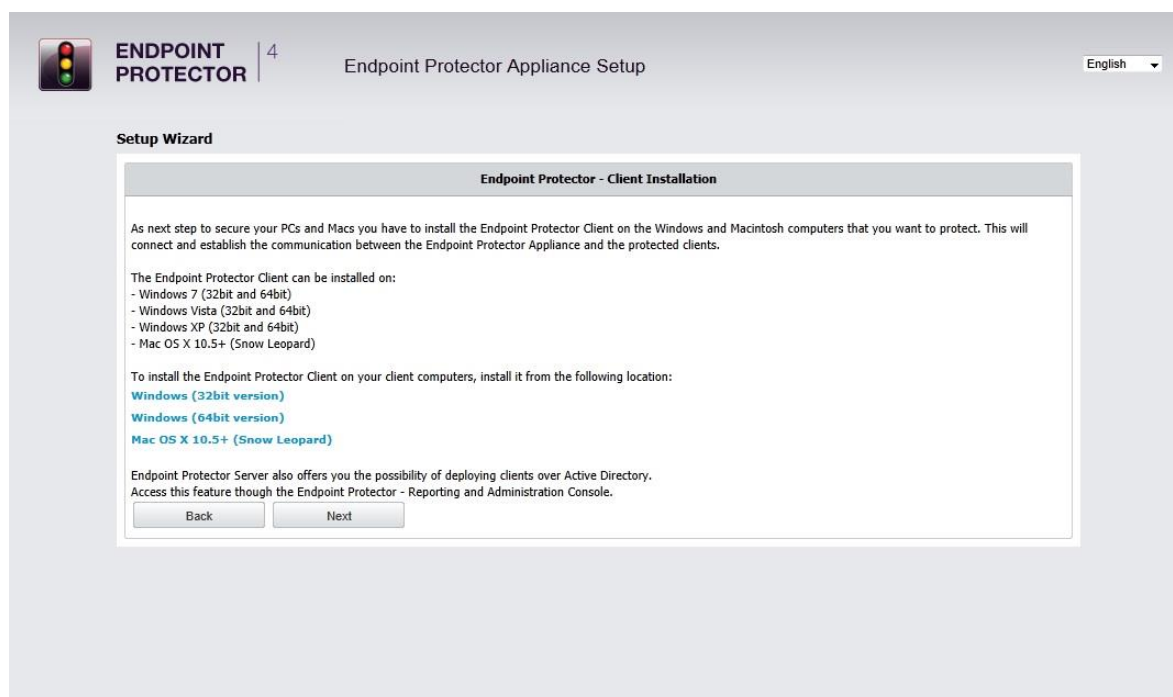
Netzwerk Maske: 255.255.255.0

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 Festlegung 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.

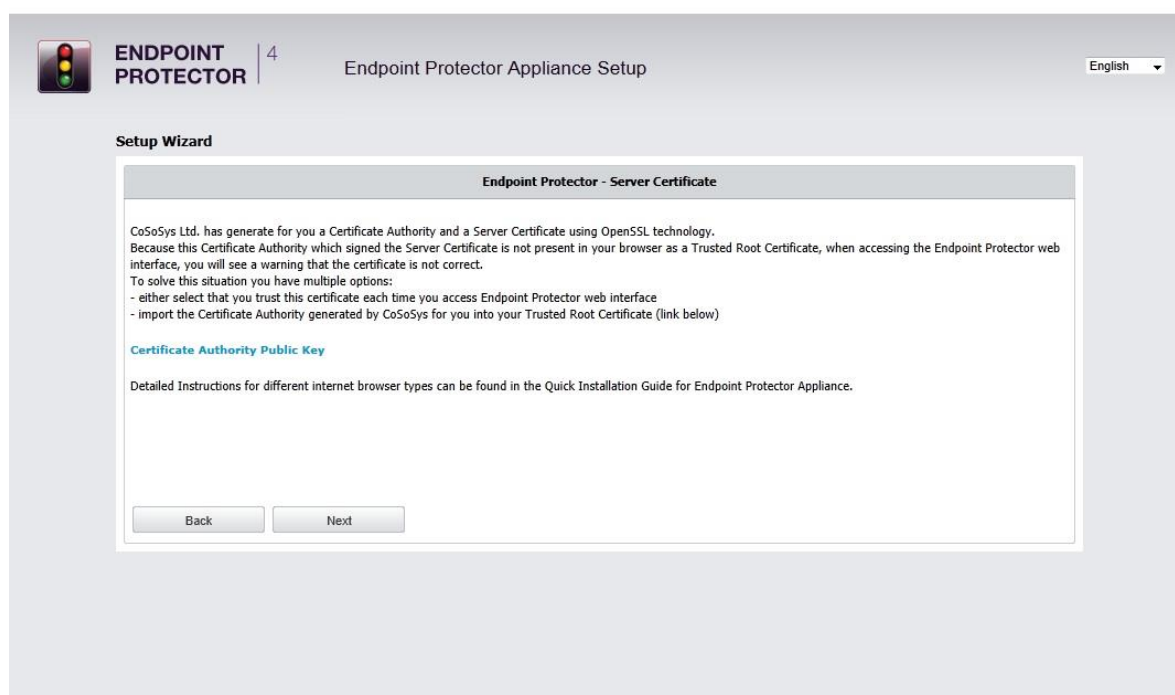
1.7.5. Appliance Server Zertifikat

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".

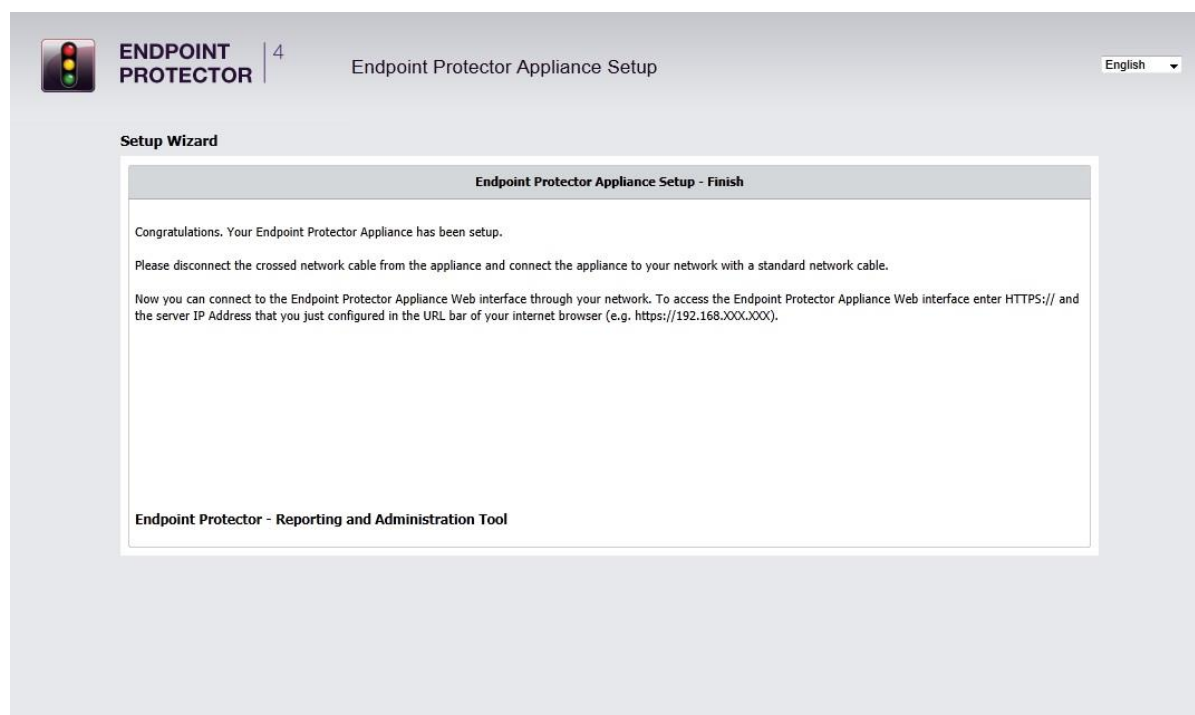


Bei Verwendung von Internet Explorer mit der Option „Verstärkten Sicherheitskonfiguration“, müssen Sie die Webseite des Endpoint Protector Administrations-Cockpits den vertrauenswürdigen Seiten im Internet Explorer hinzufügen. Dazu gehen Sie im Internet Explorer in das Menü Extras – Internetoptionen – 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 Netzkabel 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 Modelle überspringen!

Bitte beachten Sie dass das blaue Kabel angeschlossen ist.

2. Endpoint Protector Appliance Konfiguration

2.1. Verbindung zwischen Appliance und Netzwerk

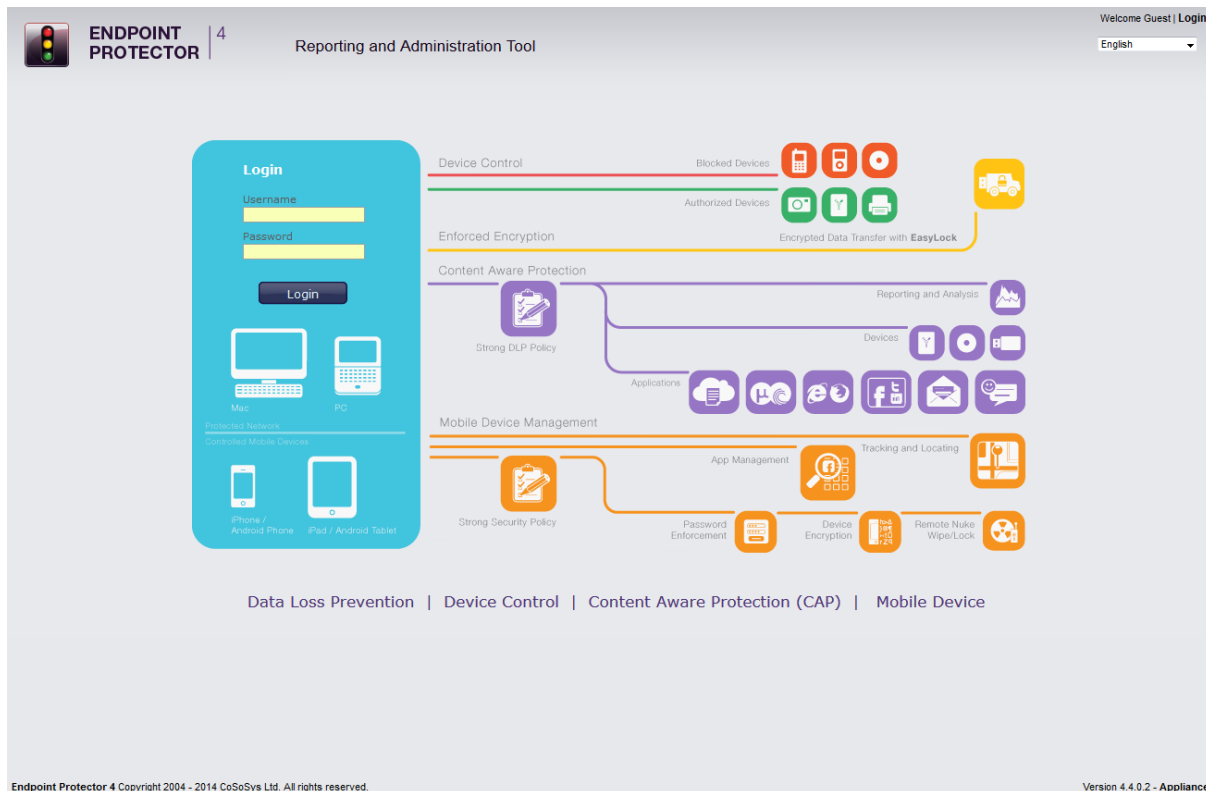
Schließen Sie das Gerät mit einem Standard-Netzkabel durch den Netzwerkanschluss auf der Rückseite der Appliance, die mit NET (blau markiert ist) an Ihr Netzwerk.

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 **https** ein. Die Standard IP-Adresse (Default IP Adresse) ist z.B. <https://192.168.0.201>.

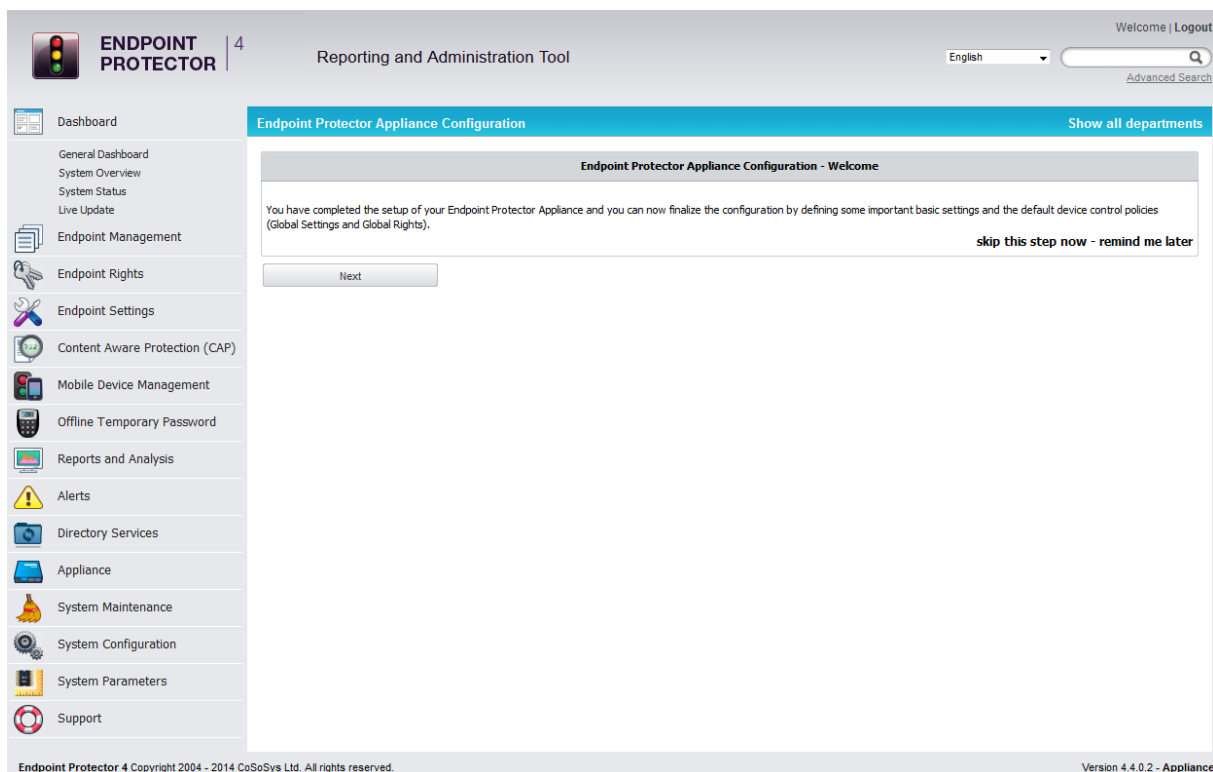
2.3. Anmeldung am Appliance Web-Interface

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.

The screenshot displays the 'Endpoint Protector 4' Reporting and Administration Tool interface. The left sidebar contains a navigation menu with options: Dashboard, General Dashboard, System Overview, System Status, Live Update, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main content area is titled 'Endpoint Protector Appliance Configuration - System Settings' and includes a 'Show all departments' link. The settings are organized into four sections:

- Endpoint Protector Rights Functionality:**
 - Use computer rights
 - Use user rights
 - Use both** (selected)
 - Priority: ☐ User rights ☒ Computer rights
- E-mail Server Settings:**
 - E-mail Type: SMTP
 - Hostname: smtp.example.com (Example: smtp.cososys.com)
 - SMTP Port: 25 (Example: 25 (Gmail uses port 465 for SSL and 587 for TLS/STARTTLS))
 - Require SMTP Authentication: ☒
 - Username: test@example.com (Example: Your full email address (including @cososys.com))
 - Password: ***** (Your SMTP password)
 - Encryption Type: None (Example: None, SSL or TLS/STARTTLS)
 - *Note:** Endpoint Protector Server will require a working Internet connection for this feature.
- Proxy Server Settings:**
 - IP:
 - Username:
 - Password:
 - *Note:** This information refers to networks with configured Proxy server to allow access to Endpoint Protector Live Update.
- Offline Temporary Password - Administrator Contact Details:**
 - Company Name: +1-22222-5555501
 - Administrator Name: Example
 - Administrator Phone Number: 07772555555
 - Administrator E-mail: alerts_email@example.com

At the bottom of the settings area are 'Back' and 'Next' buttons. The footer of the interface shows 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and 'Version 4.4.0.2 - Appliance'.

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.

The screenshot shows the 'Endpoint Protector Reporting and Administration Tool' interface. The left sidebar contains a navigation menu with options: Dashboard, General Dashboard, System Overview, System Status, Live Update, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main content area is titled 'Endpoint Protector Appliance Configuration - System Policies' and 'Show all departments'. It displays a table of 'Default Rights' with columns for device type, access level, and device name. The table lists various devices and their default access levels, with 'Deny Access' being the default for most. At the bottom of the table are 'Back' and 'Finish' buttons. The footer of the interface shows 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and 'Version 4.4.0.2 - Appliance'.

Device Type	Access Level	Device Name	Access Level
Unknown Device	Deny Access	iPad	Deny Access
USB Storage Device	Allow Access	iPod	Deny Access
Internal CD or DVD RW	Deny Access	Serial ATA Controller	Deny Access
Internal Card Reader	Deny Access	WiFi	Allow Access
Internal Floppy Drive	Deny Access	Bluetooth	Allow Access
Local Printers	Deny Access	FireWire Bus	Deny Access
Windows Portable Device (Media Transfer Protocol)	Deny Access	Serial Port	Deny Access
Digital Camera	Deny Access	PCMCIA Device	Deny Access
BlackBerry	Deny Access	Card Reader Device (MTD)	Deny Access
Mobile Phones (Sony Ericsson, etc.)	Deny Access	Card Reader Device (SCSI)	Deny Access
SmartPhone (USB Sync)	Deny Access	ZIP Drive	Deny Access
SmartPhone (Windows CE)	Deny Access	Teensy Board	Deny Access
SmartPhone (Symbian)	Deny Access	Thunderbolt	Deny Access
Webcam	Deny Access	Network Share	Allow Access
iPhone	Deny Access		

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.

The screenshot displays the 'Endpoint Protector Reporting and Administration Tool' interface. The left sidebar contains a navigation menu with items: Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, Server Information, Server Maintenance, System Maintenance, System Configuration, System Parameters, and Support. The main content area is titled 'Endpoint Protector Appliance - System Information' and includes a 'Show all departments' link. It contains three sections: 'System Fail/Over Status' (System Fail/Over Status: Disabled - N/A), 'Disk Space' (Disk Space System: 1.7G - 10% from 19G, Disk Space EPP Server: 174M - 1% from 28G, Logs on Disk: 4.0K stored in /var/eppfiles/logs, Shadows on Disk: 4.0K stored in /var/eppfiles/shadows), and 'Database Disk Space occupied' (Database Disk Space occupied: 17M stored in /var/lib/mysql/eppdatabase, Number of Logs in Database: 22, Number of Files Traced: 0, Number of Files Shadowed: 0). A 'System' section at the bottom shows: Uptime: 11:10:02 up 1:21, 1 user, load average: 0.03, 0.14, 0.16 - 1, 5 and 15 minutes ago; Linux Distribution: Ubuntu 10.04.4 LTS; System Information Update: 2014-Jan-16 11:10:02. The footer indicates 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and 'Version 4.4.0.2 - Appliance'.

Endpoint Protector Appliance - System Information	
System Fail/Over Status	
System Fail/Over Status:	Disabled - N/A
Disk Space	
Disk Space System:	1.7G - 10% from 19G
Disk Space EPP Server:	174M - 1% from 28G
Logs on Disk:	4.0K stored in /var/eppfiles/logs
Shadows on Disk:	4.0K stored in /var/eppfiles/shadows
Database Disk Space occupied	
Database Disk Space occupied:	17M stored in /var/lib/mysql/eppdatabase
Number of Logs in Database:	22
Number of Files Traced:	0
Number of Files Shadowed:	0
System	
Uptime:	11:10:02 up 1:21, 1 user, load average: 0.03, 0.14, 0.16 - 1, 5 and 15 minutes ago
Linux Distribution:	Ubuntu 10.04.4 LTS
System Information Update:	2014-Jan-16 11:10:02

3.2. Server Pflege

The screenshot displays the 'Endpoint Protector Appliance - Server Maintenance' web interface. The left sidebar contains a navigation menu with items: Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, Server Information, Server Maintenance, System Maintenance, System Configuration, System Parameters, and Support. The main content area is titled 'Endpoint Protector Appliance - Server Maintenance' and includes a 'Show all departments' link. The interface is divided into several configuration sections:

- Time Zone:** A section with a 'Please select your timezone:' label and two dropdown menus set to 'Europe' and 'Berlin'. A 'Save' button is below.
- IP Configuration:** A section with three input fields: 'IP Address' (192.168.0.201), 'Gateway' (192.168.0.1), and 'Netmask' (255.255.255.0). A note states: '*Note: Modifying Network Configuration could stop communication between EPP Clients and Server.' A 'Save' button is at the bottom.
- DNS Configuration:** A section with two input fields: 'DNS 1' (192.168.0.1) and 'DNS 2'. A note states: '*Note: At least one DNS should be configured. Endpoint Protector Appliance requires a functional DNS for sending e-mail alerts and for live update mechanism.' A 'Save' button is at the bottom.
- Appliance Operations:** A section with three rows, each containing a label and a button: 'Reboot the Hardware Appliance : Reboot', 'Shutdown the Hardware Appliance : Shutdown', and 'Reset to Factory Defaults: Factory Default'.

The footer of the interface shows 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' on the left and 'Version 4.4.0.2 - Appliance' on the right.

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.

The screenshot displays the 'Endpoint Protector Reporting and Administration Tool' interface. The sidebar on the left contains various navigation options. The main content area is titled 'Endpoint Protector Licensing System' and includes a 'Show all departments' link. The 'System Status (Updates and Support)' section shows 'Number of total licenses present in the system: 0' and a table with columns for System, Status, and End Date. The 'Feature Status' section shows a table with columns for Feature, Status, End Date, Total, Used, and Online. The 'General License Information' section shows a table with columns for Mode, Period, Endpoints, Mobile Endpoints, Device Control, Content Aware Protection (CAP), Mobile Device Management, Updates, and Support. At the bottom, there are buttons for Start Free Trial, Start Appetizer, Buy Licenses, Import Licenses, Paste Licenses, and List Licenses.

Als nächsten Schritt zur Absicherung Ihrer Computer, müssen Sie den Endpoint Protector Client auf den Windows- und Macintosh-Computern installieren, die Sie schützen 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.

Endpoint Protector 4 | Reporting and Administration Tool

Welcome | Logout | English | Advanced Search

Endpoint Protector Server - Download Client Software | Show all departments

Endpoint Protector Client Installation

Note: Endpoint Protector Client version higher than 4.1.0.0 is required for Content Aware Protection.

The Endpoint Protector Client can be installed on:

- Windows 8 (32bit and 64bit)
- Windows 7 (32bit and 64bit)
- Windows Vista (32bit and 64bit)
- Windows XP (32bit and 64bit)
- Mac OS X 10.5+ (Snow Leopard)
- Mac OS X 10.4 (Tiger)
- Linux (Ubuntu, OpenSUSE)

To install the Endpoint Protector Client on your client computers, please download it from the following location:

To install the client software, please provide the Endpoint Protector Server IP and Port.

Endpoint Protector Server IP:

Endpoint Protector Server Port:

To install the client software under a certain department, please provide the Department Code.

Department Code:

☒ Windows (32bit version) - Version: 4.2.6.6
☒ Windows (64bit version) - Version: 4.2.6.6
☐ Mac OS X 10.5+ (Leopard) - Version: 1.2.3.1
☐ Mac OS X 10.4 (Tiger) - Version: 1.0.9.0
☐ Linux - Ubuntu 10.4+ LTS - Version: 1.0.0-1
☐ Linux - Ubuntu 12.4+ LTS - Version: 1.0.3-1
☐ Linux - OpenSUSE 11.4 - Version: 1.0.0-1

[Download selected version](#)

Endpoint Protector Client for Windows can be deployed over Active Directory.
For more information, please refer to [Endpoint Protector - User Guide](#).

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved. | Version 4.4.0.2 - Appliance

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

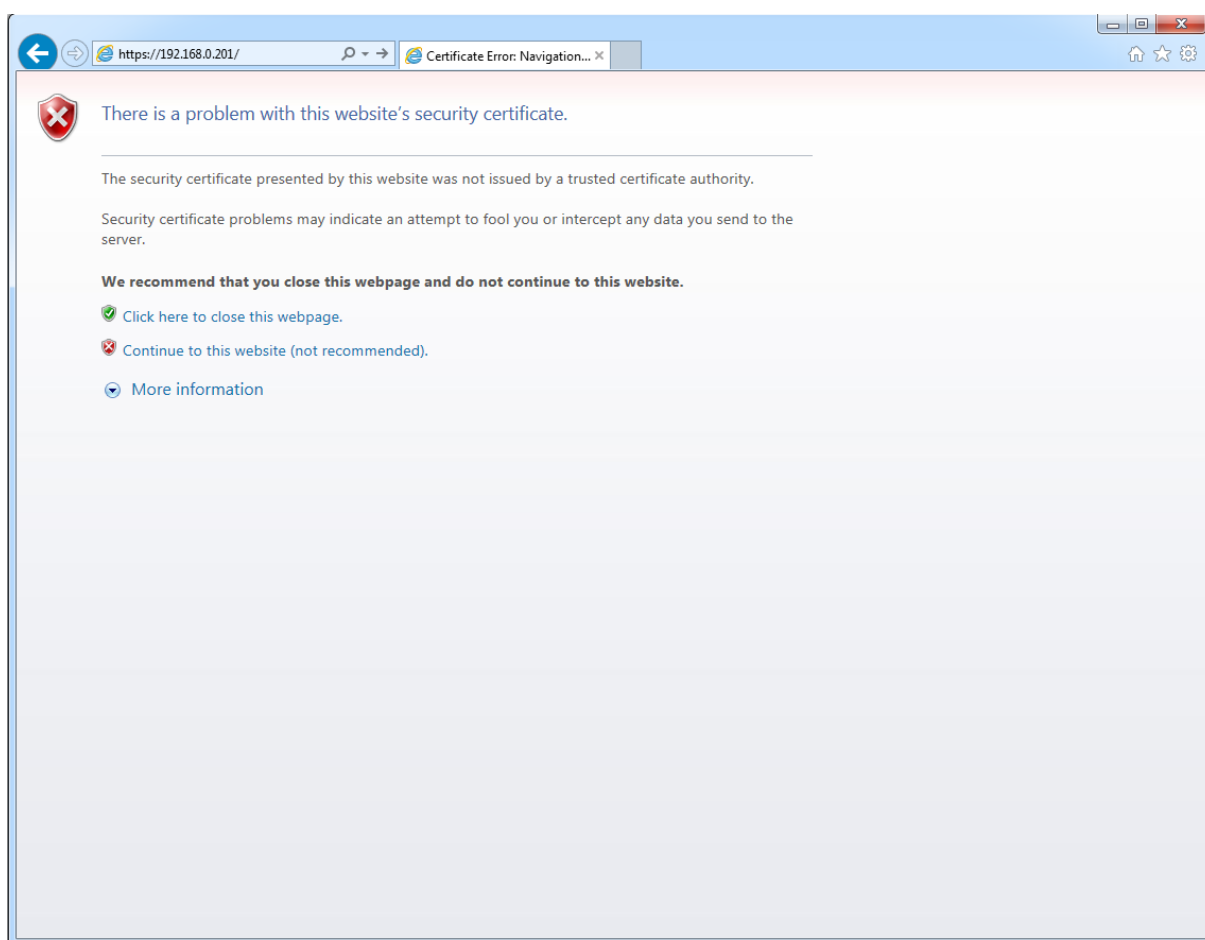
Wir empfehlen Ihnen das Root-Zertifikat der Endpoint Protector Appliance den vertrauenswürdigen Stammzertifikate Ihres Internet Browsers hinzuzufügen.

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/>).

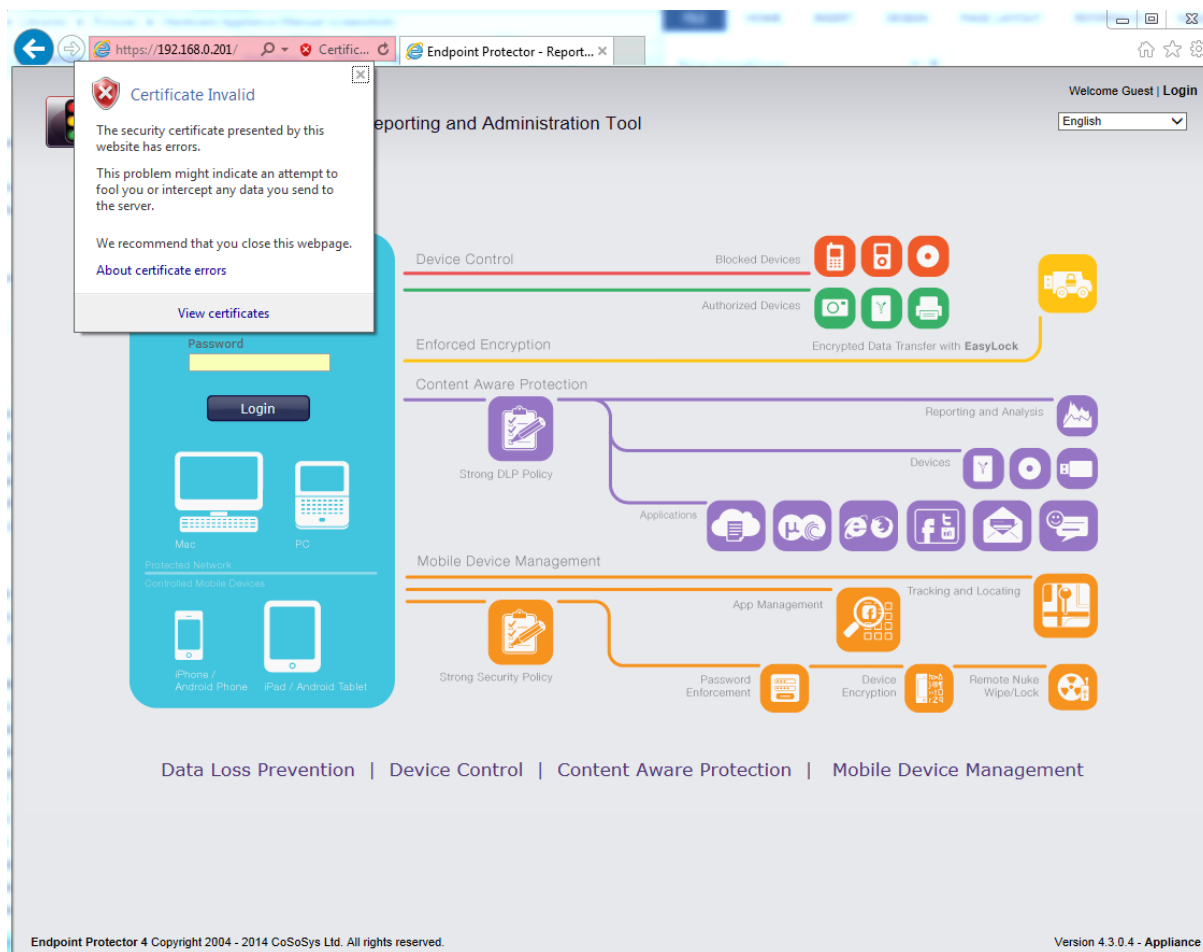
Wichtig ist für die nachfolgenden Schritte dass die IP-Adresse dem Internet Explorer bereits zuvor wie in Schritt 1.7.5 beschrieben den Vertrauenswürdigen Sites hinzugefügt wurde.



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.

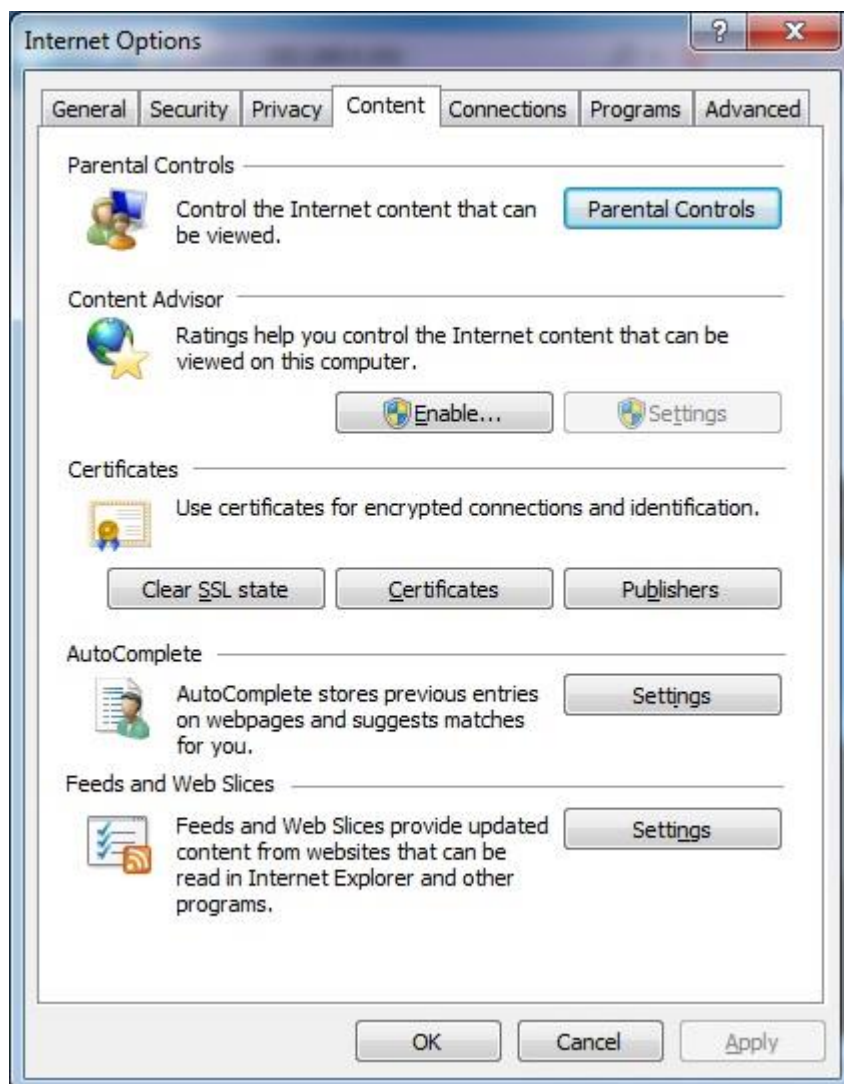
Klicken Sie auf die Schaltfläche „Zertifikatfehler“ gleich neben der Internet Explorer URL Adressleiste. Durch Anklicken der Taste " Zertifikatfehler", erscheint ein Pop-up Fenster.



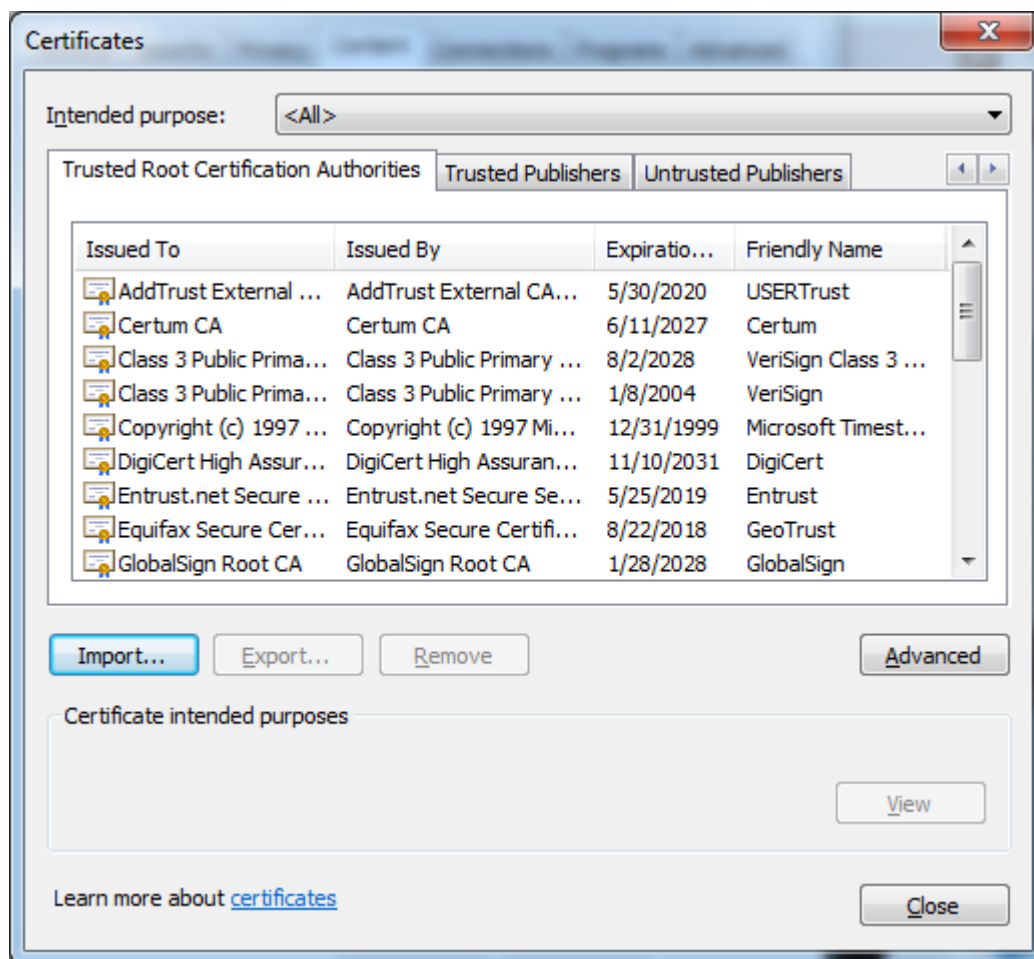
Klicken Sie jetzt auf Schaltfläche "Zertifikate anzeigen" in diesem Pop-up-Fenster.

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.



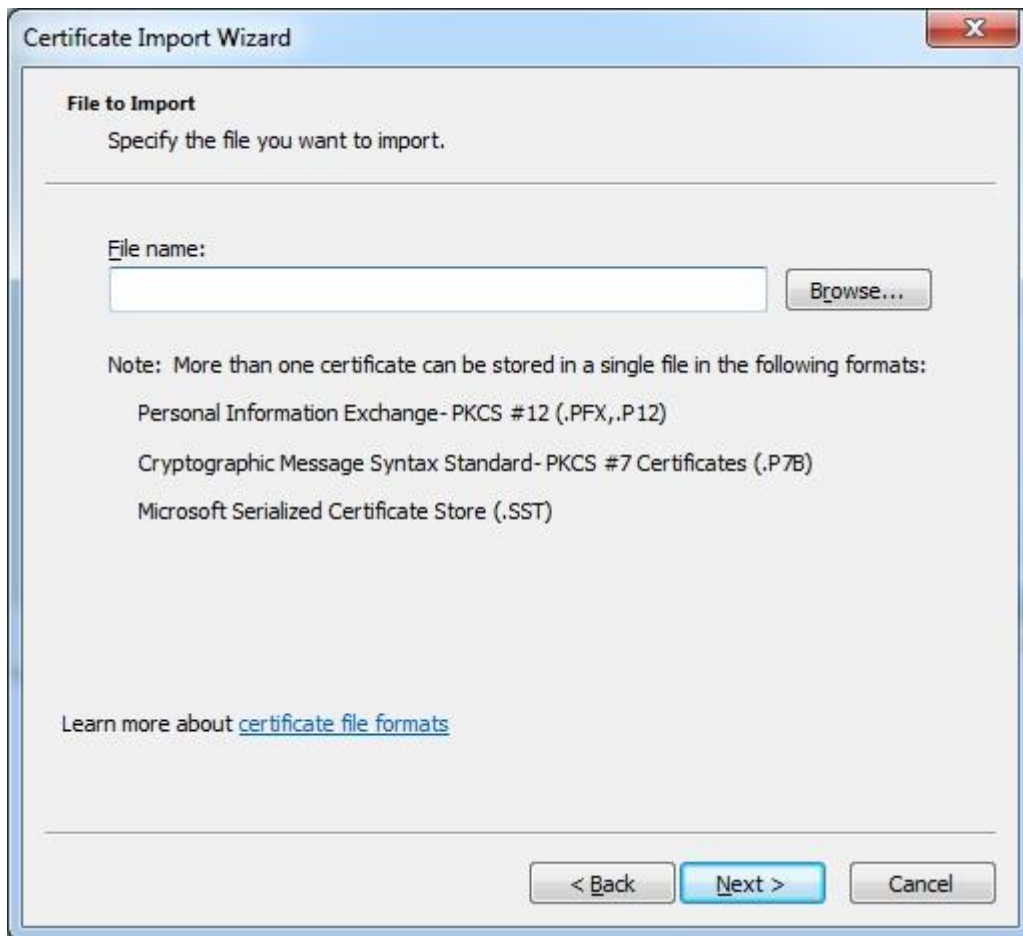
Aus der Liste waehlen Sie bitte "Vertrauenswürdige Zertifizierungsstellen" aus und klicken "Import".



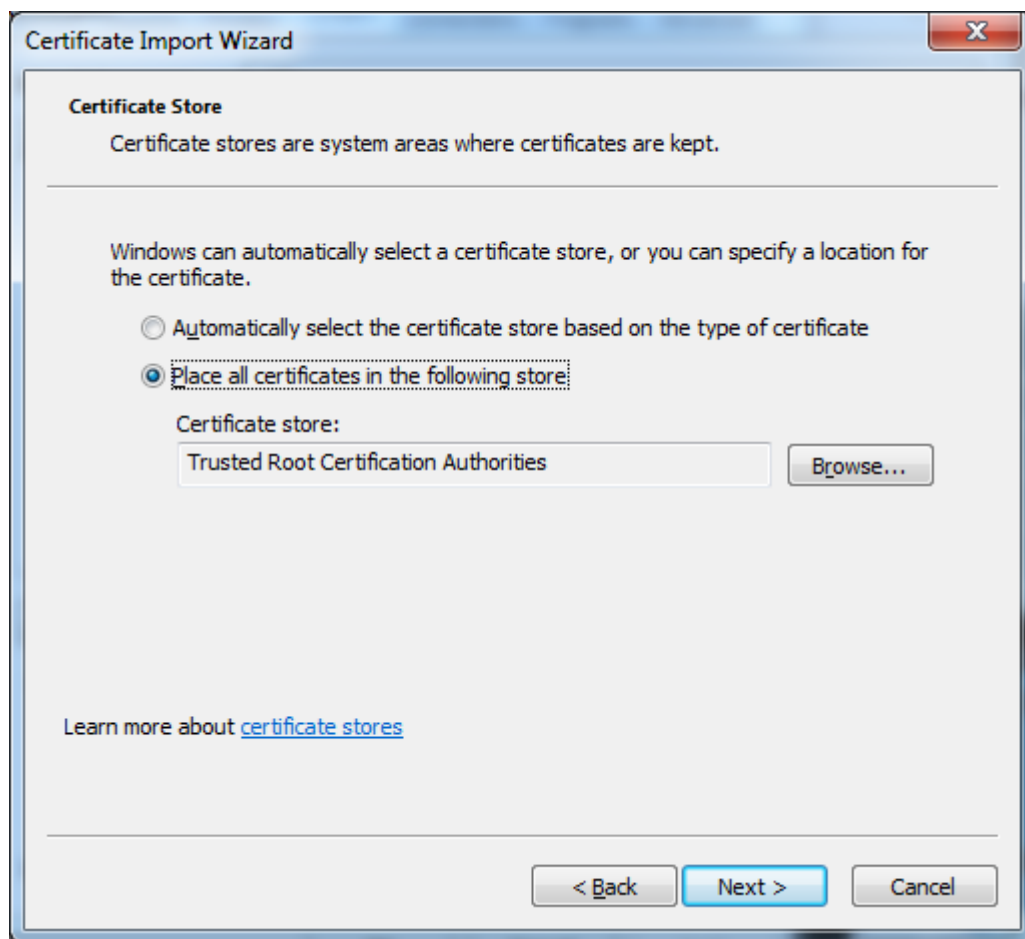
Ein Zertifikatimport-Assistent öffnet sich. Klicken Sie auf die Schaltfläche Weiter.



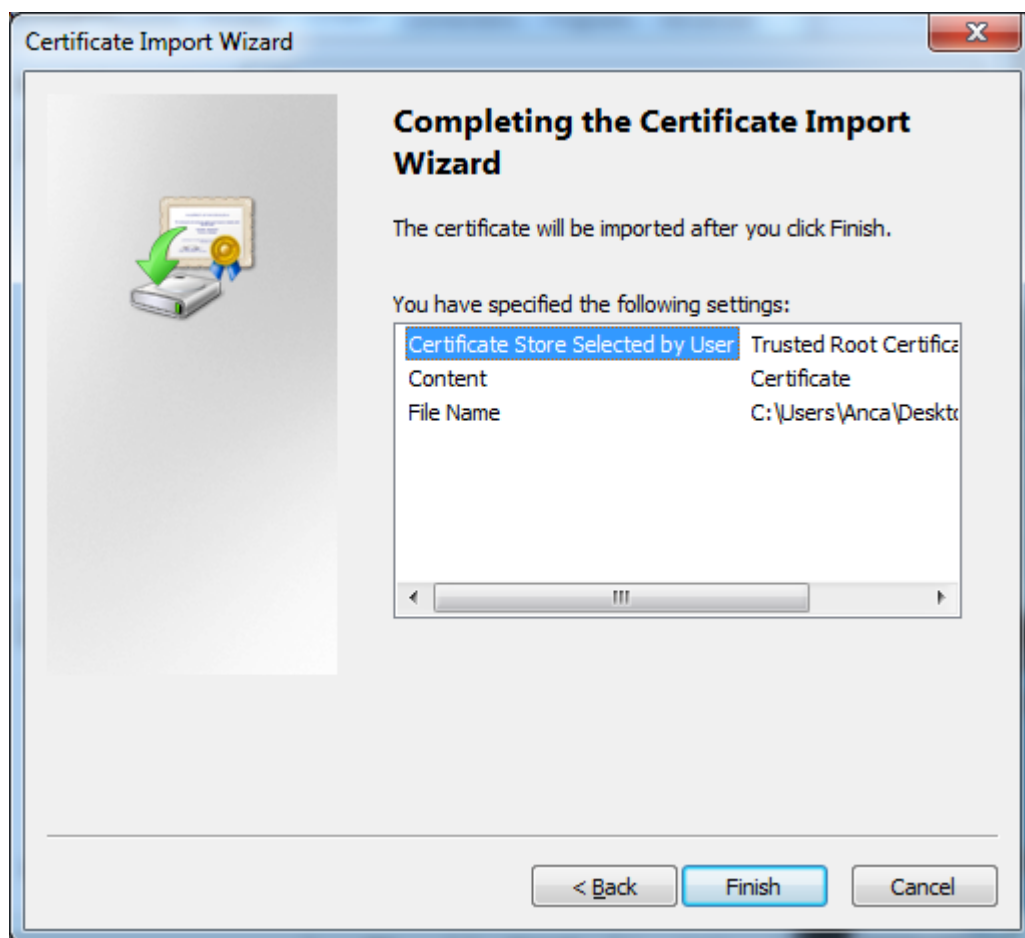
Klicken Sie auf "Durchsuchen".



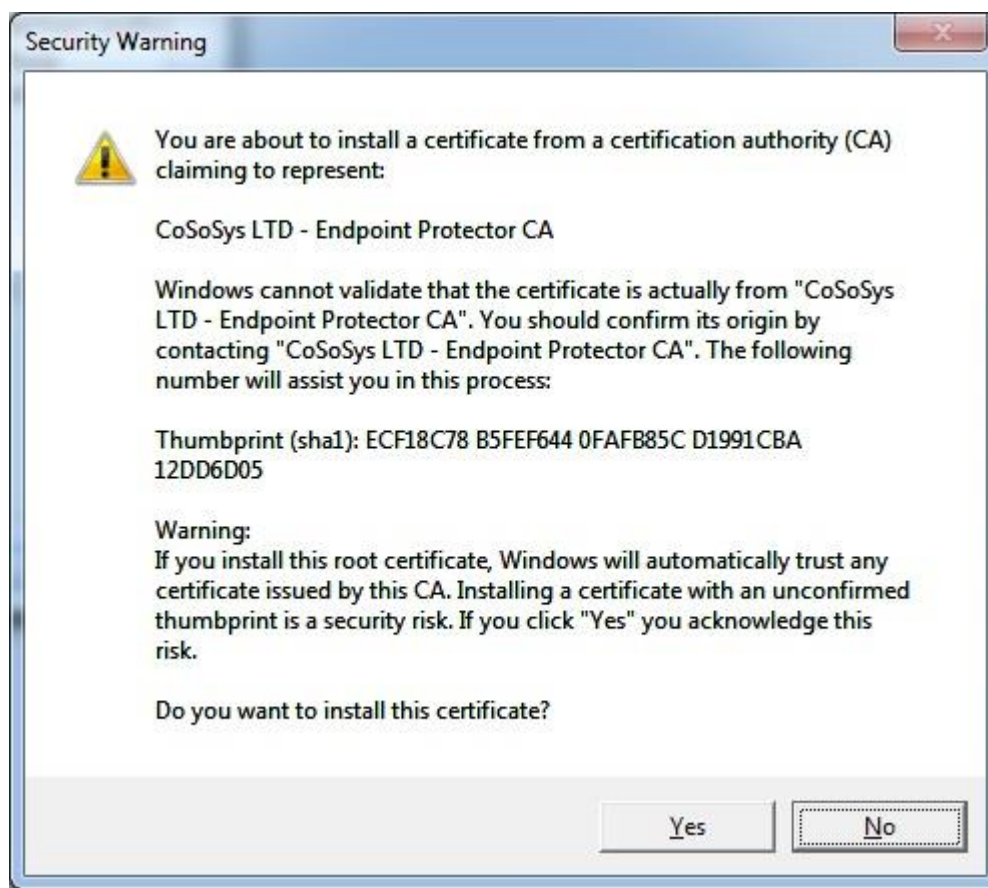
Im Zertifikatimport-Assistent wählen Sie bitte die zweite Option "Alle Zertifikate in folgendem Speicher speichern".



Klicken Sie auf „Weiter,“ um fortzufahren.

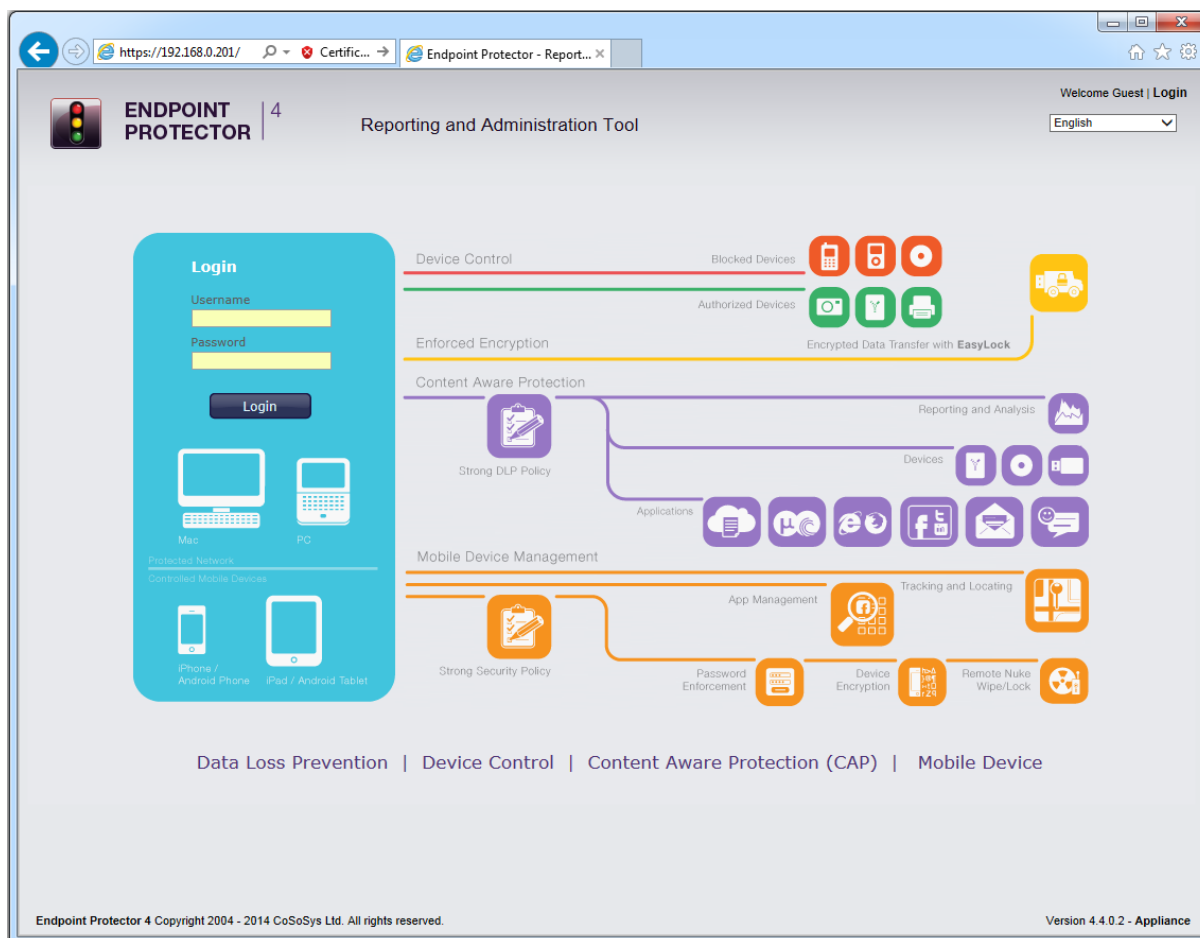


Klicken Sie auf „Fertig stellen“ um fortzufahren.



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

Sie haben nun erfolgreich das Zertifikat installiert.



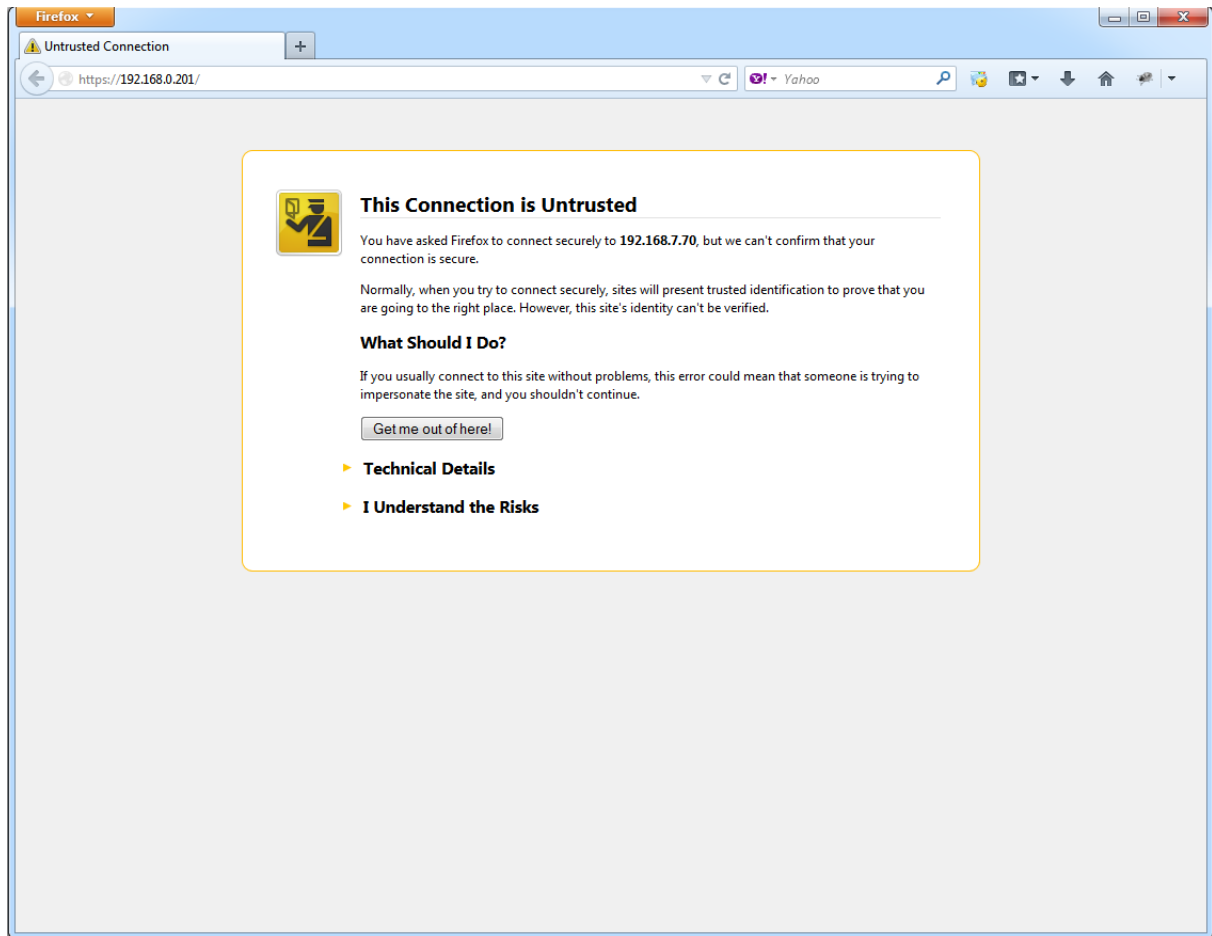
Schließen Sie jetzt bitte Internet Explorer und öffnen erneut das Endpoint Protector Administrations-Cockpit unter der IP-Adresse im Browser.

4.2. Für Mozilla Firefox

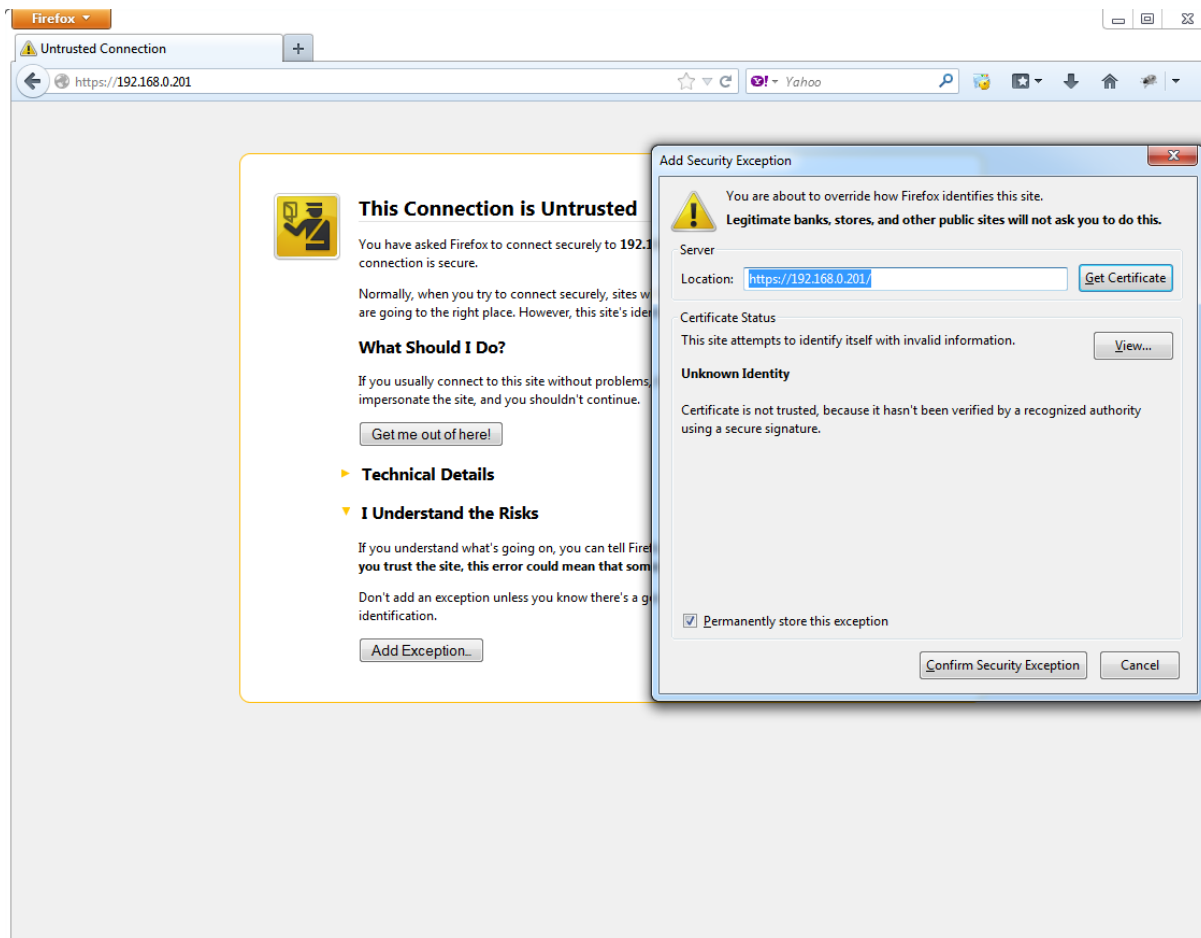
Starten sie Mozilla Firefox.

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.

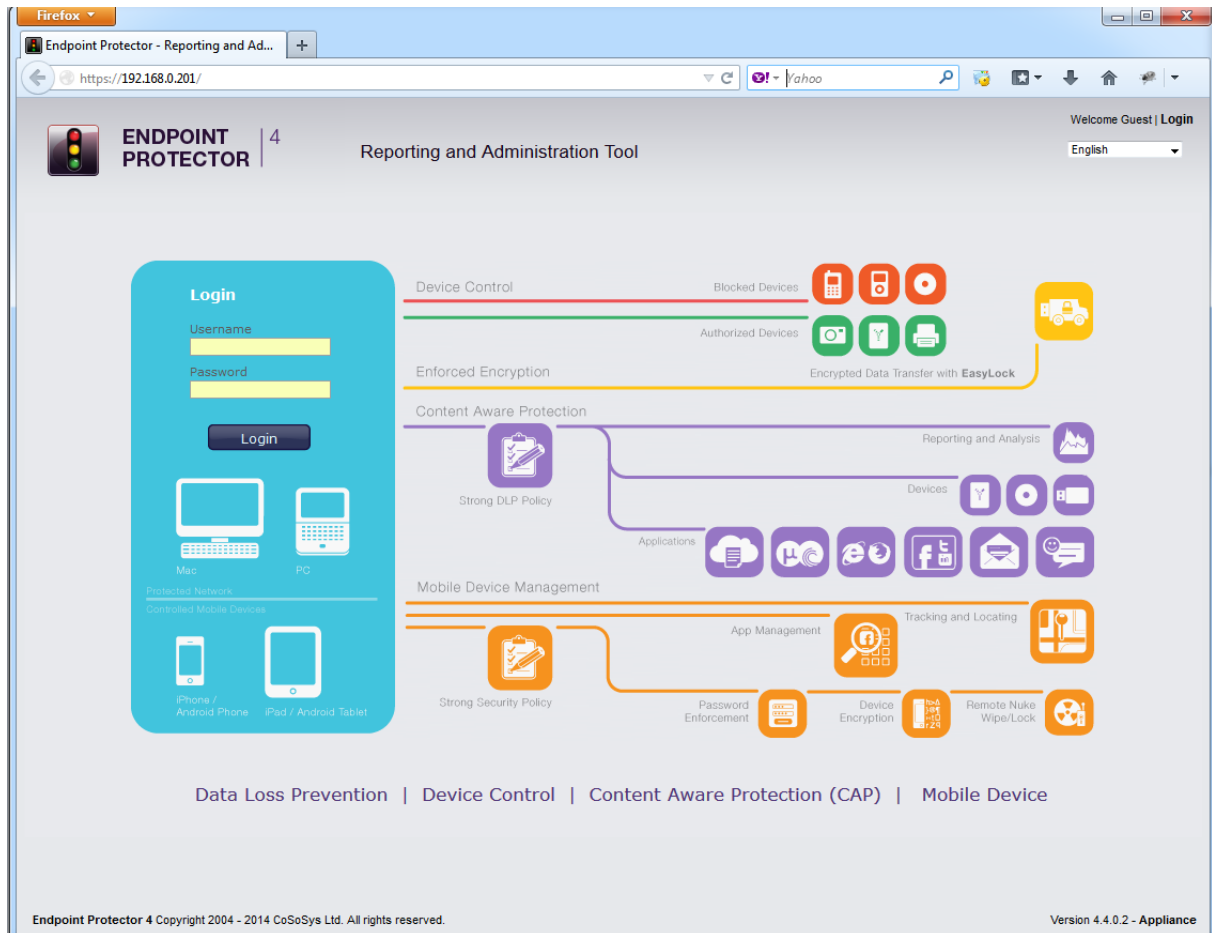


Klicken Sie auf „Ausnahme hinzufügen“. Ein Fester „Sicherheits-Ausnahmeregel hinzufügen“ öffnet sich.



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>.

© 2004 – 2014 CoSoSys Ltd.; Endpoint Protector Basic, EPPBasic, Endpoint Protector, My Endpoint Protector are trademarks of CoSoSys Ltd. All rights reserved. Windows is registered trademark of Microsoft Corporation. Macintosh, Mac OS X are trademarks of Apple Corporation. All other names and trademarks are property of their respective owners.