



# ENDPOINT PROTECTOR APPLIANCE

Manuel de l'Utilisateur Version 4.0.0.4

## Manuel de l'Utilisateur A20 / A50 / A100 / A250 / A500 / A1000 / A2000 / A4000



## Table des matières

### 1. Installation d'Endpoint Protector Appliance.. 1

1.1.	Livraison d'Endpoint Protector Appliance .....	1
1.2.	Connecter l'Appliance pour l'Installation Initiale .....	2
1.3.	Panneau frontal / arrière de l'Appliance Matériel .....	3
1.3.1.	Panneau arrière de l'Appliance A20 .....	3
1.3.2.	Panneau arrière de l'Appliance A50 et A100.....	3
1.3.3.	Panneau frontal de l'Appliance A20.....	3
1.3.4.	Panneau frontal de l'Appliance A50 et A100.....	4
1.3.5.	Panneau frontal de l'Appliance A250, A500 et A1000 .....	4
1.3.6.	Panneau frontal de l'Appliance A2000 – A4000 .....	5
1.4.	Configuration du disque dur de l'Appliance A2000 / A4000 .....	5
1.4.1.	Configuration du disque dur de l'Appliance A2000 .....	5
1.4.2.	Configuration du disque dur de l'Appliance A4000 .....	6
1.4.3.	Logiciels supplémentaires RAID 3ware® 3DM® pour le disque dur de l'Appliance A2000 et A4000 .....	6
1.5.	Accéder à l'Assistant d'Installation de l'Appliance avec un câble de réseau NORMAL (seulement pour l'A20) .....	7
1.6.	Accéder à l'Assistant d'Installation de l'Appliance directement avec un câble de réseau croisé (Modèle A50 et plus grand) .....	8
1.7.	Assistant d'Installation de l'Appliance .....	9
1.7.1.	Accord Licence Utilisateur Final - Accord Licence Appliance...	9
1.7.2.	Définir votre Mot de Passe d'Administrateur .....	10
1.7.3.	Établir le Fuseau Horaire .....	11
1.7.4.	Établir l'Adresse IP de l'Appliance.....	12
1.7.5.	Client Endpoint Protector – Repackaging MSI Automatique.	13
1.7.6.	Certificat du Serveur Appliance .....	14
1.7.7.	Finir l'Installation d'Endpoint Protector Appliance .....	15

### 2. Configuration Endpoint Protector Appliance 16

2.1.	Connecter l'Appliance au Réseau.....	16
2.2.	Accéder à l'Interface de l'Appliance à travers votre Réseau ..	16
2.3.	Se connecter à l'Interface de l'Appliance .....	17
2.4.	Assistant de Configuration de l'Appliance .....	18
2.5.	Paramètres de Base de l'Appliance .....	19

2.6. Politiques par Défaut de l'Appliance .....	21
2.7. Finir l'Assistant de Configuration d'Endpoint Protector Appliance	21

### 3. Paramètres de l'Appliance et Maintenance. 22

3.1. Informations sur le Serveur.....	22
3.2. Maintenance du Serveur .....	23
3.2.1. Paramètres du Réseau .....	23
3.2.2. Redémarrer l'Appliance .....	23
3.2.3. Restaurer l'Appliance aux Paramètres par Défaut d'Usine ...	23
3.3. Installation du Client Endpoint Protector pour l'Appliance .....	24
3.4. Mises à Jour en direct en ligne .....	26

### 4. Installer le Certificat Racine à votre Navigateur 27

4.1. Pour Microsoft Internet Explorer .....	27
4.2. Pour Mozilla Firefox .....	36

### 5. Support ..... 39

### 6. Note Importante / Démenti ..... 40

# 1. Installation d'Endpoint Protector Appliance

## 1.1. Livraison d'Endpoint Protector Appliance

Lors de recevoir l'Endpoint Protector Appliance le paquet contient:

- Endpoint Protector Appliance
- Câble d'Alimentation
- Câble de Réseau Croisé pour l'Installation Initiale de l'Appliance - autocollant jaune (pas inclus pour le modèle A20)
- Câble de Réseau pour connecter l'Appliance dans votre réseau
- Vis pour le montage dans le Rack (pas inclus pour le modèle A20)
- Rails d'assemblage extractibles (inclus uniquement pour les modèles A250, A500, A1000, A4000)
- Source d'alimentation externe (incluse et requise uniquement pour A20)



## 1.2. Connecter l'Appliance pour l'Installation Initiale

Connectez le câble d'alimentation à l'appareil et à une prise de courant.

Pour l'Appliance A20 connectez la source d'alimentation externe au A20 et à la prise de courant. Ensuite, connectez le câble bleu au port de réseau de l'A20 et puis au réseau.

Votre Appliance (modèles A50 à A4000) contient à l'arrière deux ports de réseau marqués avec jaune pour CONFIG (connexion de configuration) et bleu pour NET (connexion au réseau). L'Appliance A20 a un port de réseau.

Connectez le Câble de Réseau CROISÉ (autocollant jaune) au port de configuration CONFIG (marqué avec jaune) à l'arrière de l'appareil et connectez-le directement à un PC (Laptop, PC, Netbook).

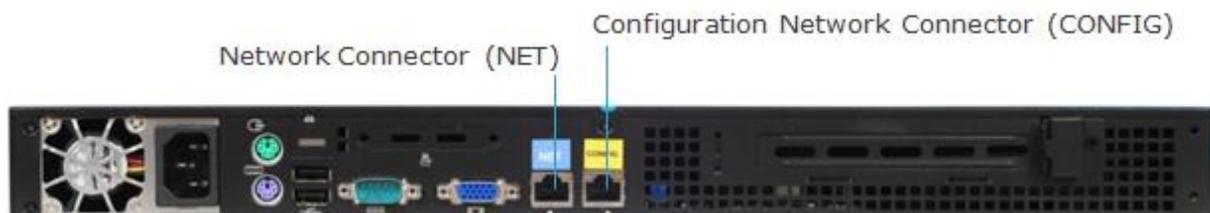
Démarrez l'Appliance en appuyant sur le bouton POWER.

## 1.3. Panneau frontal / arrière de l'Appliance Matériel

### 1.3.1. Panneau arrière de l'Appliance A20



### 1.3.2. Panneau arrière de l'Appliance A50 et A100

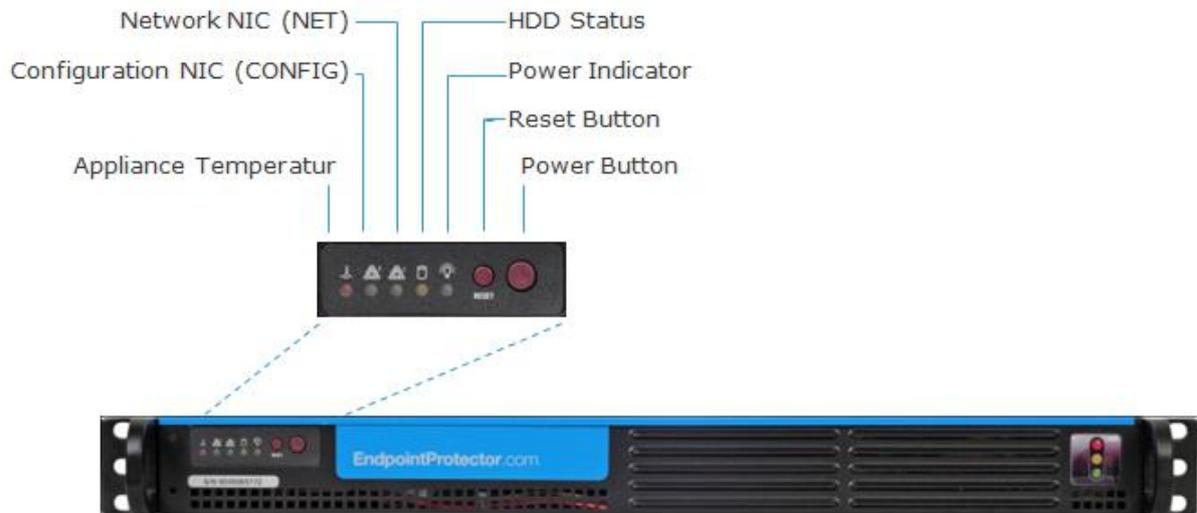


Le panneau arrière pour les modèles A250 jusqu'à A4000 ont des ports de réseau marqués comme dans l'image ci-dessus pour les modèles A50 et A100.

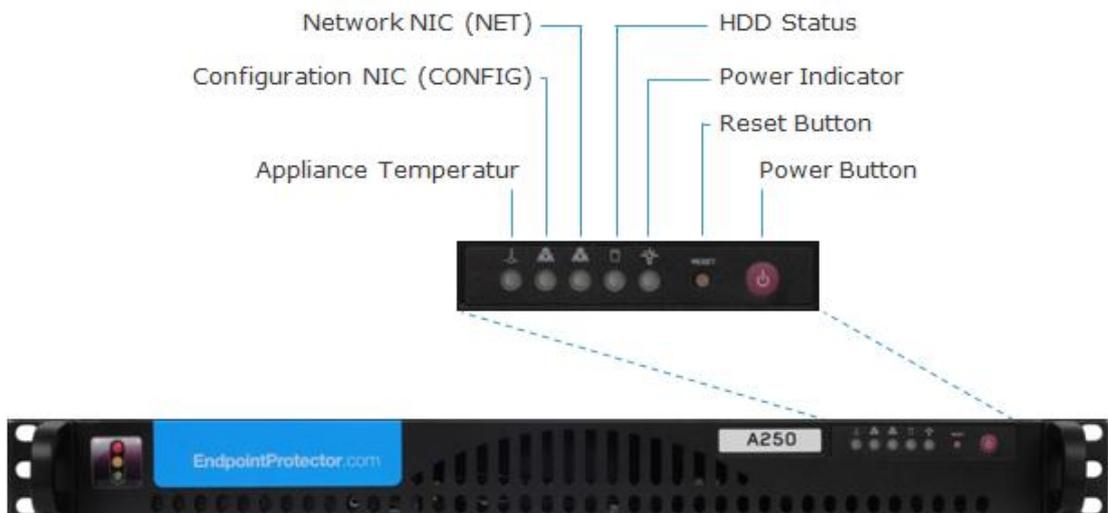
### 1.3.3. Panneau frontal de l'Appliance A20



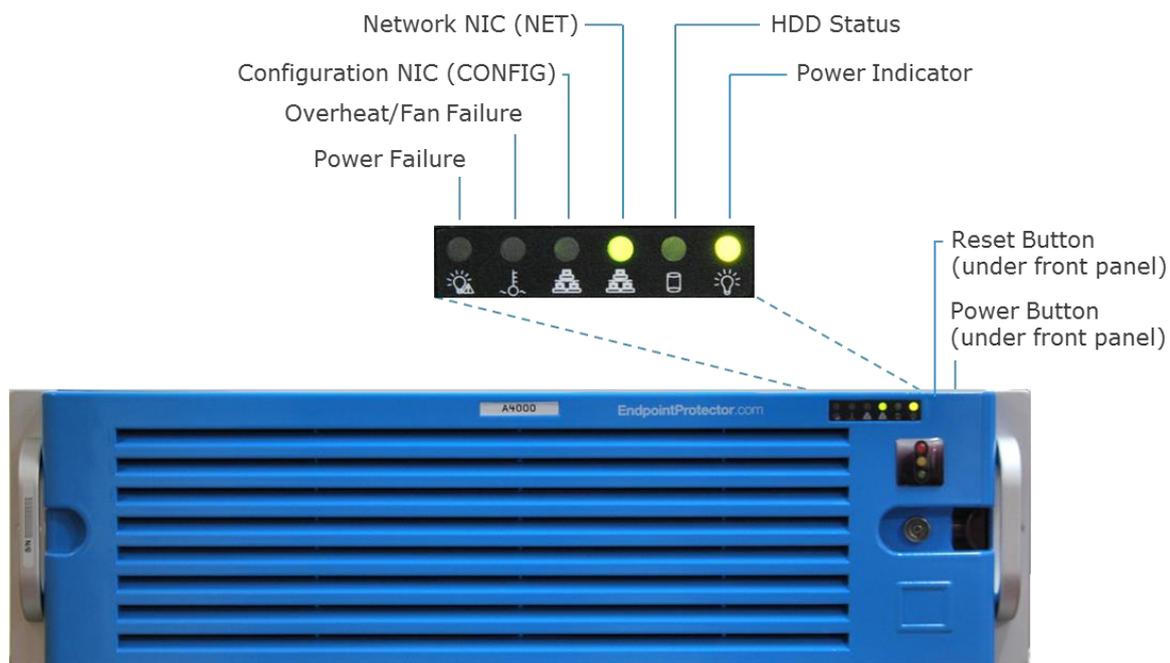
### 1.3.4. Panneau frontal de l'Appliance A50 et A100



### 1.3.5. Panneau frontal de l'Appliance A250, A500 et A1000

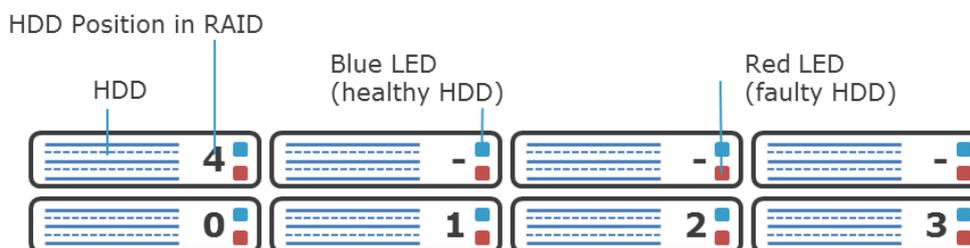


### 1.3.6. Panneau frontal de l'Appliance A2000 – A4000



## 1.4. Configuration du disque dur de l'Appliance A2000 / A4000

### 1.4.1. Configuration du disque dur de l'Appliance A2000

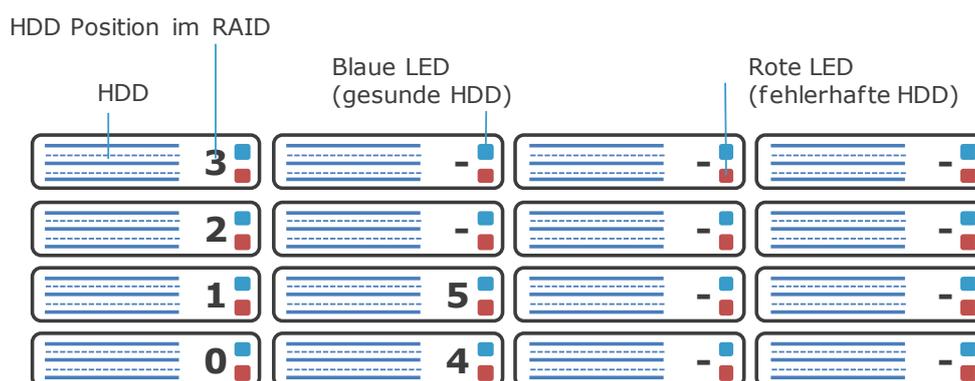


L'Appliance A2000 vient avec 4 disques durs dans une Configuration RAID 5. Les disques durs sont installés dans l'ordre 0-3.

En cas d'échec d'un disque dur, il peut être remplacé en le changeant avec un disque dur du même modèle.

Chaque baie de disque dur contient un LED bleu et rouge pour indiquer le statut du disque. Un indicateur bleu symbolise un disque dur sain, un indicateur rouge symbolise un disque dur mauvais. Un disque dur défectueux doit être remplacé immédiatement par un modèle identique.

### 1.4.2. Configuration du disque dur de l'Appliance A4000



L'Appliance A4000 vient avec 6 disques durs dans une Configuration RAID 5. Les disques durs sont installés dans l'ordre 0-5.

En cas d'échec d'un disque dur le disque dur peut être remplacé en le changeant avec un disque dur du même modèle.

Chaque baie de disque dur contient un LED bleu et rouge pour indiquer le statut du disque. Un indicateur bleu symbolise un disque dur sain, un indicateur rouge symbolise un disque dur mauvais. Un disque dur défectueux doit être remplacé immédiatement par un modèle identique.

### 1.4.3. Logiciels supplémentaires RAID 3ware® 3DM® pour le disque dur de l'Appliance A2000 et A4000

Les Appliances A2000 et A4000 disposent d'un logiciel supplémentaire configurable préinstallé de 3ware® que vous pouvez utiliser en tant qu'administrateur pour être averti de possibles erreurs sur un disque dur par une notification e-mail. Plus d'informations sur la configuration de ce logiciel supplémentaire peuvent être trouvées dans l'Annexe de ce Manuel de l'Utilisateur pour le " Manuel de l'Utilisateur 3ware 3DM® 2®."

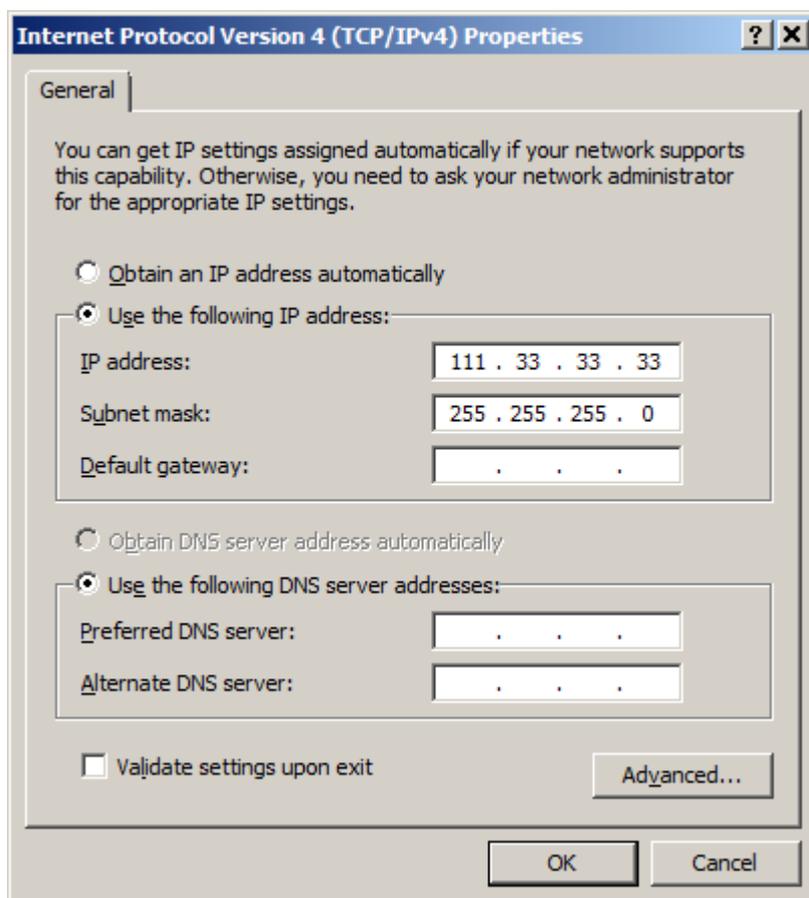
## 1.5. Accéder à l'Assistant d'Installation de l'Appliance avec un câble de réseau NORMAL (seulement pour l'A20)

Connectez le câble bleu au port de réseau de l'A20 et puis au réseau.

Vérifiez que les paramètres TCP/IPv4 soient:

Adresse IP 111.33.33.33

Subnet Mask 255.255.255.0



Puis accédez-le via votre navigateur internet en tapant l'adresse IP suivante

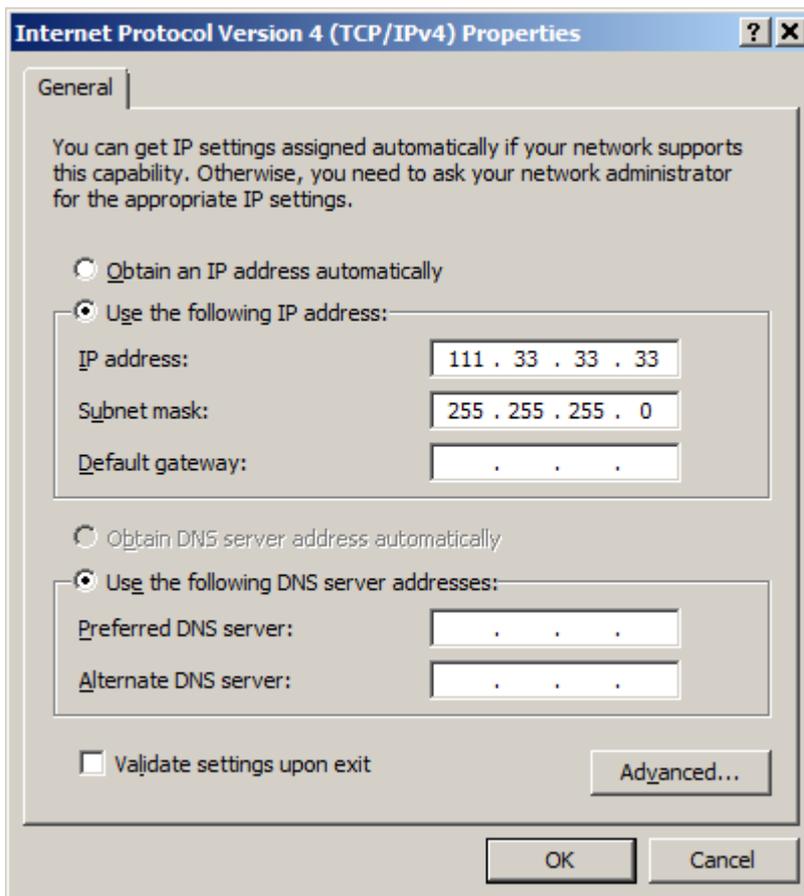
<http://111.33.33.111> dans la barre URL.

## 1.6. Accéder à l'Assistant d'Installation de l'Appliance directement avec un câble de réseau croisé (Modèle A50 et plus grand)

Avec votre ordinateur connectez-vous maintenant à l'Appliance à travers le câble croisé. Vérifiez que les paramètres TCP/IPv4 soient:

Adresse IP 111.33.33.33

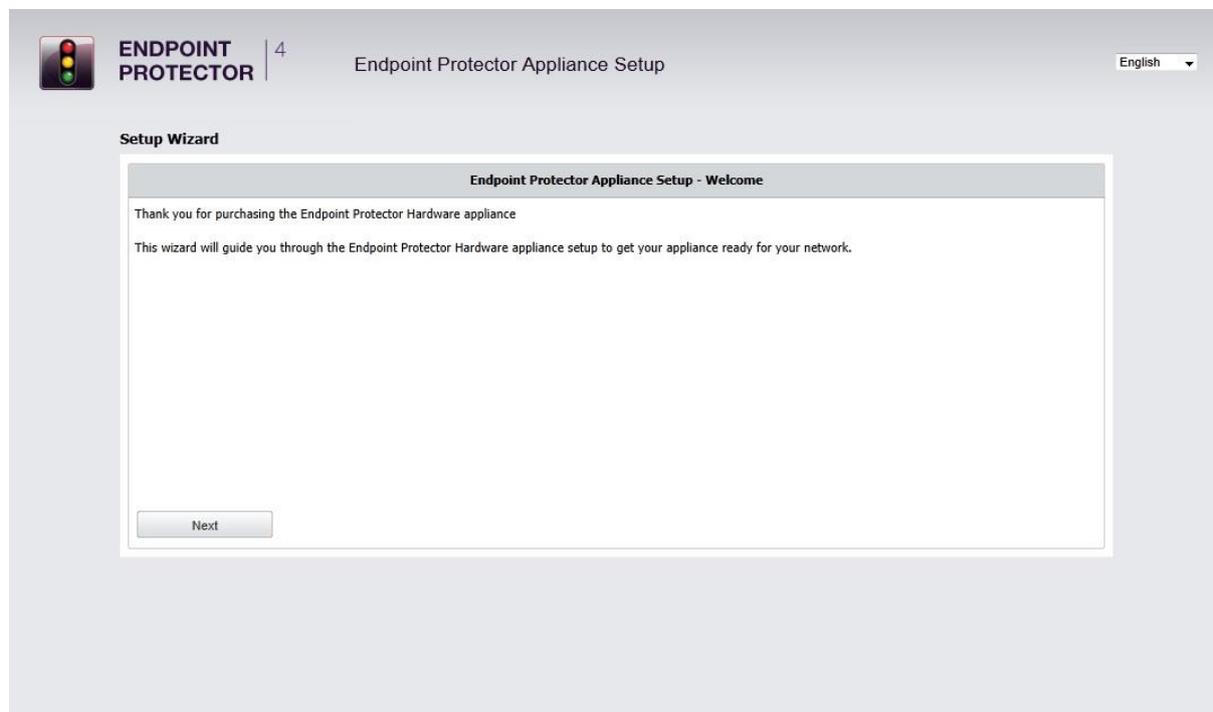
Subnet Mask 255.255.255.0



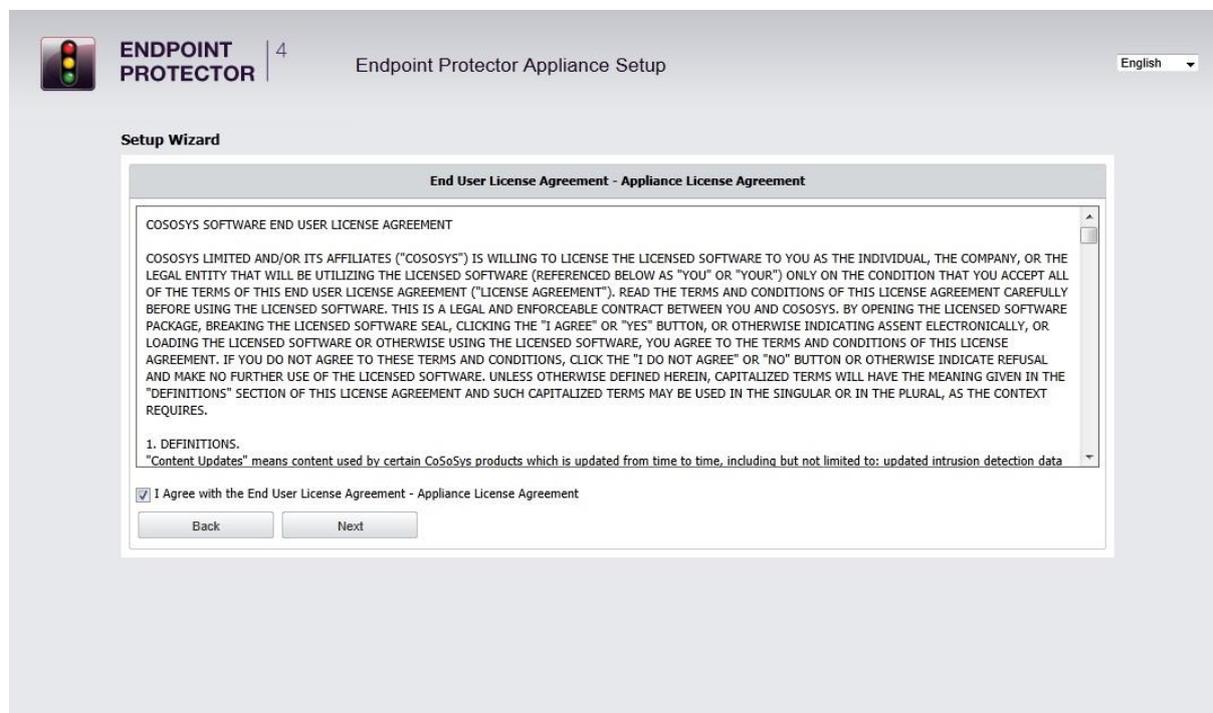
Puis accédez-le via votre navigateur internet en tapant l'adresse IP suivante  
<http://111.33.33.111> dans la barre URL.

## 1.7. Assistant d'Installation de l'Appliance

Cet assistant va vous guider dans l'installation du matériel Endpoint Protector Appliance pour rendre votre appareil prêt pour votre réseau.

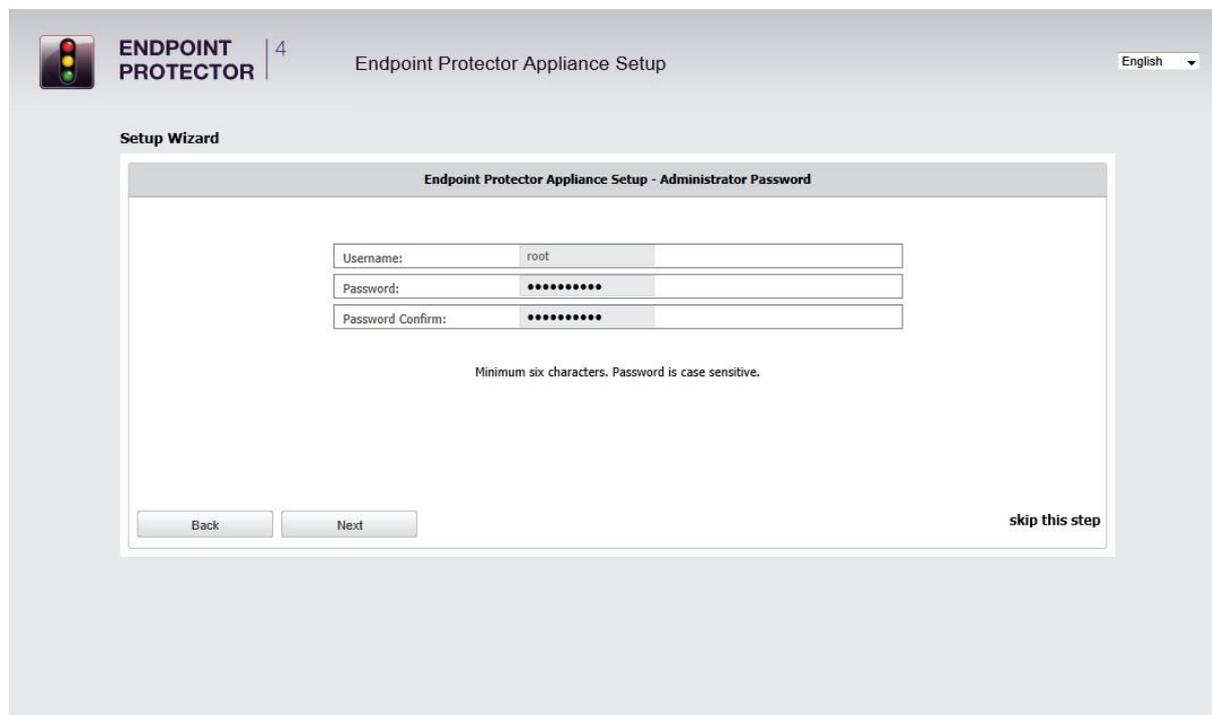


### 1.7.1. Accord Licence Utilisateur Final - Accord Licence Appliance



Pour continuer avec le processus d'installation, veuillez consulter l'Accord Licence Utilisateur Final - Accord Licence Appliance.

## 1.7.2. Définir votre Mot de Passe d'Administrateur



The screenshot shows the 'Endpoint Protector Appliance Setup - Administrator Password' screen. At the top left is the 'ENDPOINT PROTECTOR 4' logo. The page title is 'Endpoint Protector Appliance Setup' and the language is set to 'English'. The 'Setup Wizard' section contains three input fields: 'Username:' with the value 'root', 'Password:' with masked characters, and 'Password Confirm:' with masked characters. Below the fields is the instruction: 'Minimum six characters. Password is case sensitive.' At the bottom, there are 'Back' and 'Next' buttons, and a 'skip this step' link.

Saisissez et confirmez votre mot de passe d'administrateur. La longueur minimale est de 6 caractères et le mot de passe est sensible à la casse.

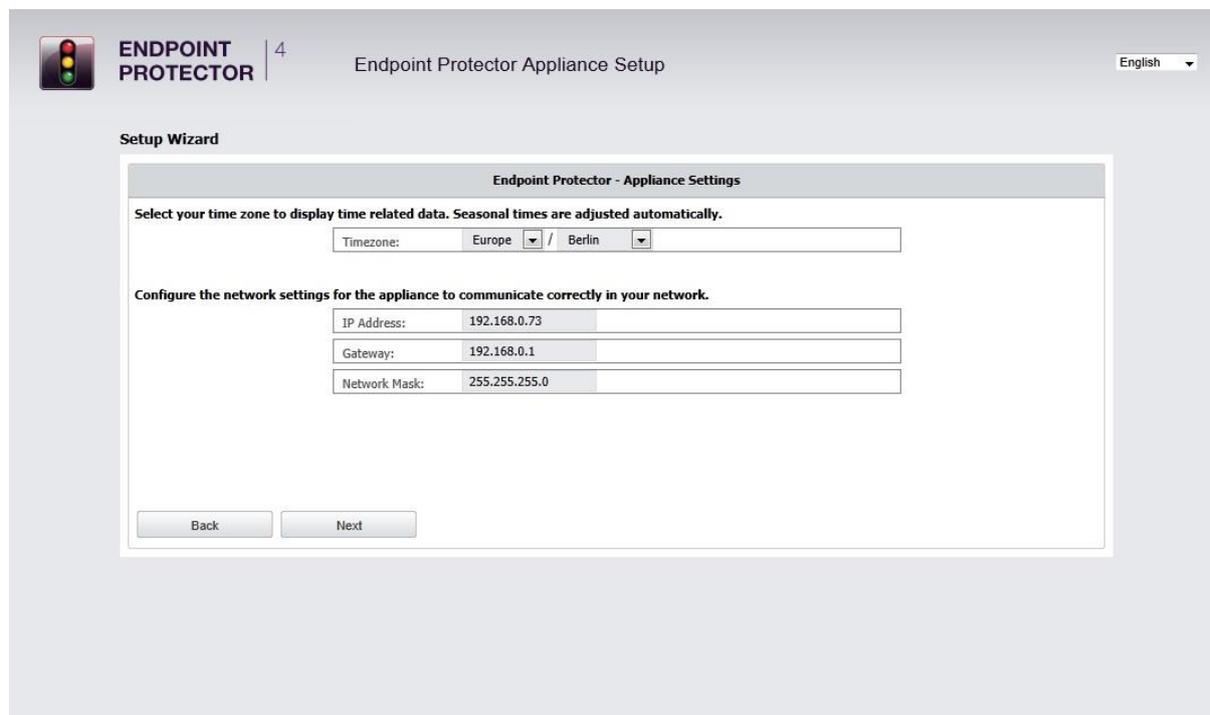
Le nom d'utilisateur et mot de passe pour l'Outil d'Administration et de Rapports d'Endpoint Protector 4 sont:

NOM D'UTILISATEUR: root

MOT DE PASSE: epp2011

Après saisir et confirmer votre mot de passe d'administrateur cliquez suite pour continuer.

### 1.7.3. Établir le Fuseau Horaire

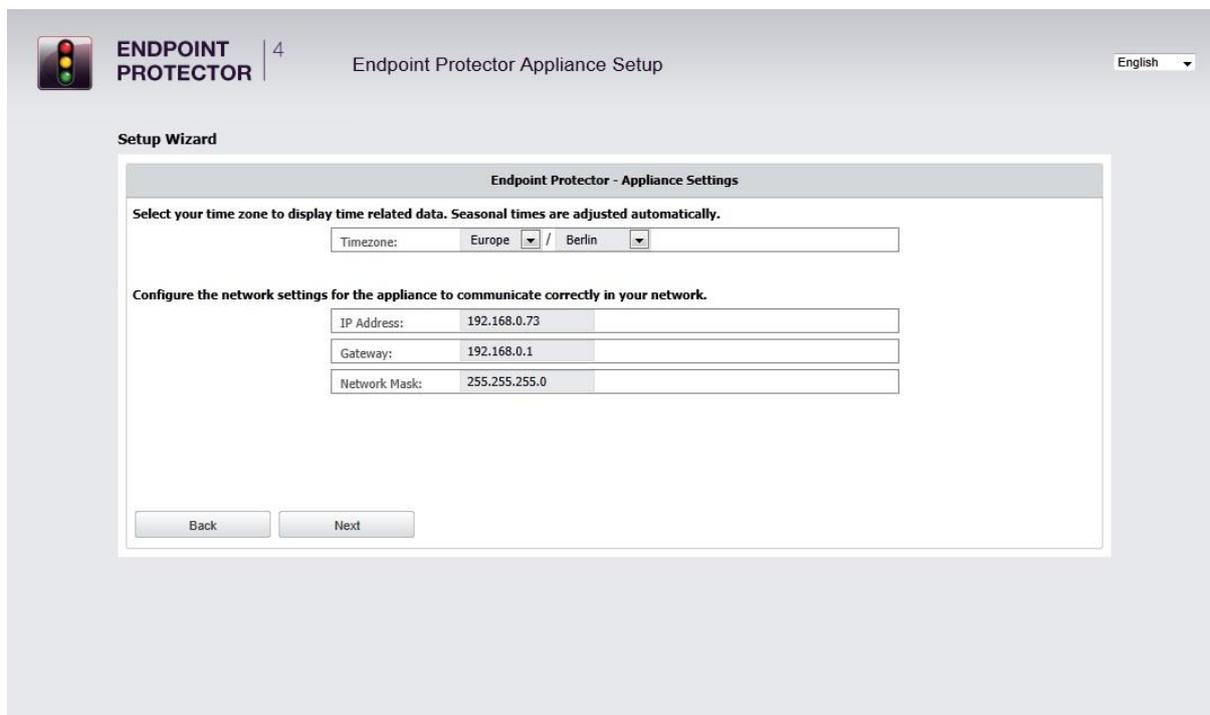


The screenshot shows the 'Endpoint Protector Appliance Setup' wizard at step 4. The interface includes the 'ENDPOINT PROTECTOR' logo, a step indicator '4', the title 'Endpoint Protector Appliance Setup', and a language dropdown set to 'English'. The main content area is titled 'Setup Wizard' and contains a window titled 'Endpoint Protector - Appliance Settings'. This window has two sections: 'Select your time zone to display time related data. Seasonal times are adjusted automatically.' with a 'Timezone:' field set to 'Europe / Berlin', and 'Configure the network settings for the appliance to communicate correctly in your network.' with three fields: 'IP Address: 192.168.0.73', 'Gateway: 192.168.0.1', and 'Network Mask: 255.255.255.0'. At the bottom of the window are 'Back' and 'Next' buttons.

Sélectionnez votre fuseau horaire pour afficher correctement les données liées au temps. Les changements saisonniers sont ajustés automatiquement.

Vous pouvez modifier ce paramètre ultérieurement du menu Appliance, en sélectionnant l'option Maintenance du Serveur.

## 1.7.4. Établir l'Adresse IP de l'Appliance



The screenshot shows the 'Endpoint Protector - Appliance Settings' window within a 'Setup Wizard'. The window is titled 'Endpoint Protector - Appliance Settings' and contains the following elements:

- Header:** 'Endpoint Protector' logo, a page number '4', the title 'Endpoint Protector Appliance Setup', and a language dropdown menu set to 'English'.
- Section: Setup Wizard**
- Section: Endpoint Protector - Appliance Settings**
- Text:** 'Select your time zone to display time related data. Seasonal times are adjusted automatically.'
- Form:** A 'Timezone:' field with two dropdown menus, currently showing 'Europe' and 'Berlin'.
- Text:** 'Configure the network settings for the appliance to communicate correctly in your network.'
- Form:** Three input fields:
  - IP Address: 192.168.0.73
  - Gateway: 192.168.0.1
  - Network Mask: 255.255.255.0
- Buttons:** 'Back' and 'Next' buttons at the bottom.

Indiquez une adresse IP pour votre Appliance sous laquelle il sera accessible dans votre réseau. Dans le cas où votre réseau utilise des IPs du type 192.168.0.0, alors l'adresse IP par défaut assignée à l'Endpoint Protector Appliance dans votre réseau est 192.168.0.201. Si cette adresse IP n'est pas assignée dans votre réseau, ce paramètre ne requiert pas de changements.

### NOTE!

La configuration du réseau doit répondre à la topologie de votre réseau. Par exemple, si votre réseau utilise des IPs de la classe A (par exemple 10.10.5.10) et il n'y a pas des sous-réseaux définis, alors les informations suivantes doivent être saisies :

IP Address: 10.10.5.10

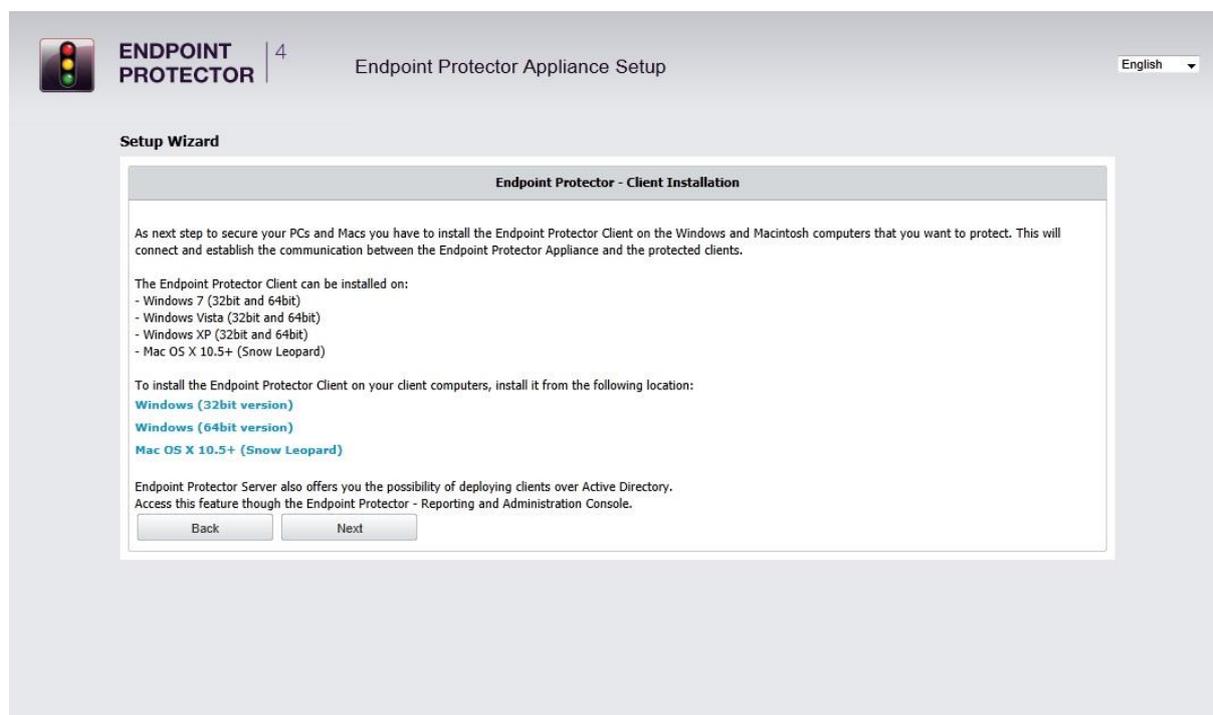
Gateway: 10.10.5.1

Network Mask: 255.255.255.0

Une adresse IP statique pour Endpoint Protector Appliance est nécessaire pour une communication stable et fonctionnelle entre l'Appliance et les clients protégés. Par conséquent DHCP n'est pas offert car l'adresse IP de l'Appliance doit être statique. Veuillez fournir aussi les paramètres Gateway, Network Mask, Network et Broadcast si les valeurs par défaut requièrent d'être changées.

Vous pouvez modifier ce paramètre ultérieurement du menu Appliance, en sélectionnant l'option Maintenance du Serveur.

## 1.7.5. Client Endpoint Protector – Repackaging MSI Automatique



Après configurer l'adresse IP statique du serveur Appliance, les fichiers MSI pour le client Endpoint Protector ont été automatiquement repackaged. L'adresse IP de votre serveur a été ajoutée au paquet MSI.

Pour le fichier d'installation Macintosh l'adresse IP de l'Appliance doit être saisie manuellement dans le processus d'installation du Client Endpoint Protector sur un ordinateur Mac OS X.

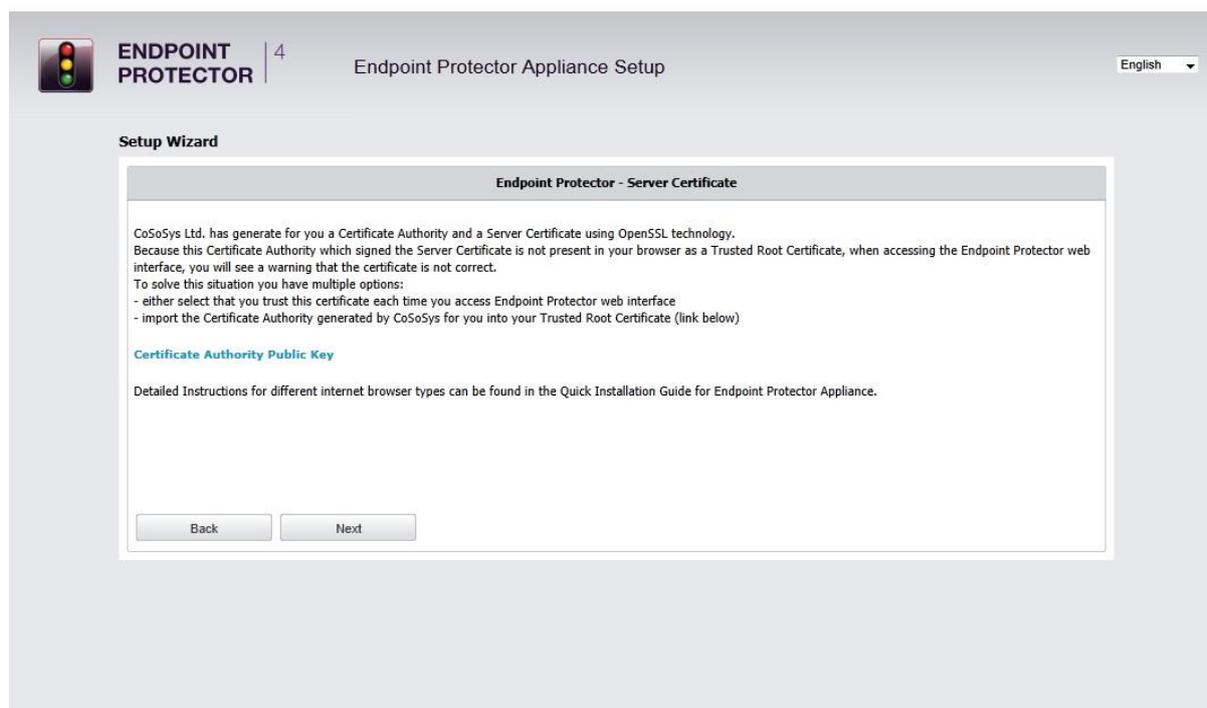
### 1.7.6. Certificat du Serveur Appliance

Après avoir défini une adresse IP statique, Endpoint Protector Appliance a créé pour votre Appliance un Certificat d'Autorité, à l'aide de la technologie OpenSSL. Cela vous permettra de vous connecter de façon sécurisée à l'interface d'administration Web de l'Appliance via votre réseau et il fournit également une communication sécurisée et cryptée entre l'Appliance et les ordinateurs clients protégés.

Nous vous recommandons d'ajouter le Certificat Racine d'Endpoint Protector Appliance à vos Certificats Racine de Confiance de votre navigateur Internet.

Sinon, lorsque votre navigateur Internet vous le demande, veuillez accepter le certificat invalide.

Des instructions détaillées sur la façon d'ajouter le Certificat Racine pour des différents types de navigateurs Internet peuvent être trouvées dans le chapitre 4. "Installer le Certificat Racine à votre Navigateur Internet".

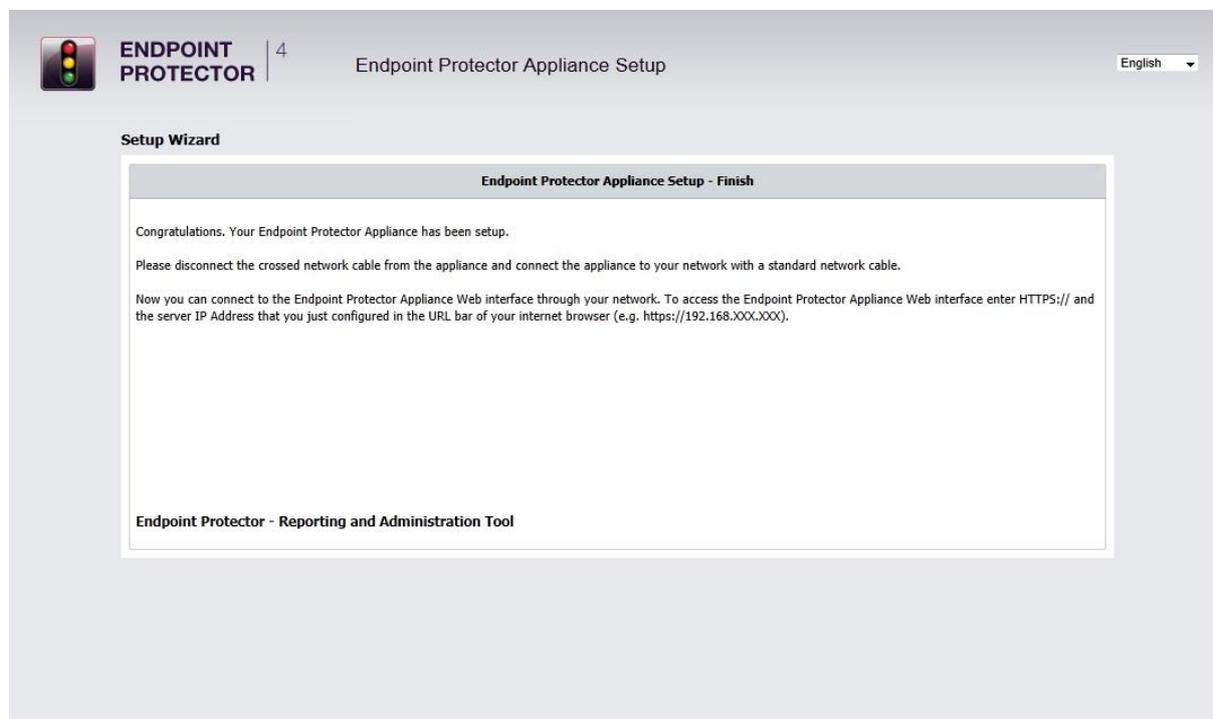


Si vous utilisez Internet Explorer avec la Configuration de Sécurité Renforcée activée, vous devez ajouter le site Endpoint Protector à la liste de sites de confiance du navigateur.

### 1.7.7. Finir l'Installation d'Endpoint Protector Appliance

Votre Endpoint Protector Appliance a été installé.

Veillez déconnecter maintenant le câble de réseau croisé de l'Appliance et continuer à connecter l'Appliance à votre réseau comme décrit dans la prochaine étape.



#### **NOTE!**

Sautez ce pas pour les modèles A20! Veuillez maintenir le câble bleu connecté.

# 2. Configuration Endpoint Protector Appliance

## 2.1. Connecter l'Appliance au Réseau

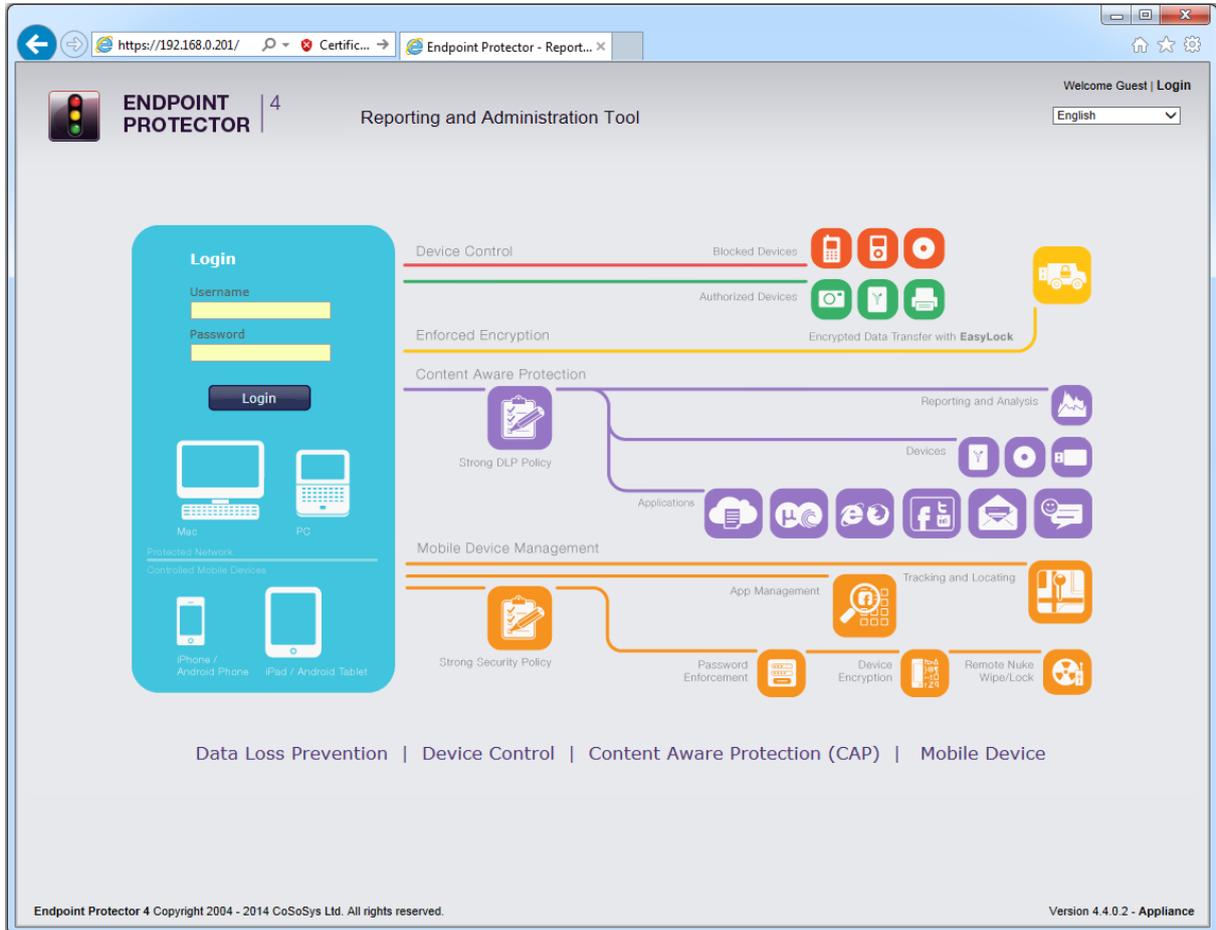
Après avoir attribué une adresse IP statique à l'Endpoint Protector Appliance dans le processus d'installation, vous pouvez maintenant connecter l'Appliance à votre réseau. Connectez l'Appliance à votre réseau avec un câble réseau standard via le connecteur réseau marqué avec NET (bleu) à l'arrière de l'appareil.

## 2.2. Accéder à l'Interface de l'Appliance à travers votre Réseau

Maintenant, vous pouvez vous connecter à l'interface Web d'Endpoint Protector Appliance via votre réseau. Pour accéder à l'Appliance connectez-vous à l'adresse IP statique que vous avez défini avant via https. Exemple par défaut: <https://192.168.0.201>.

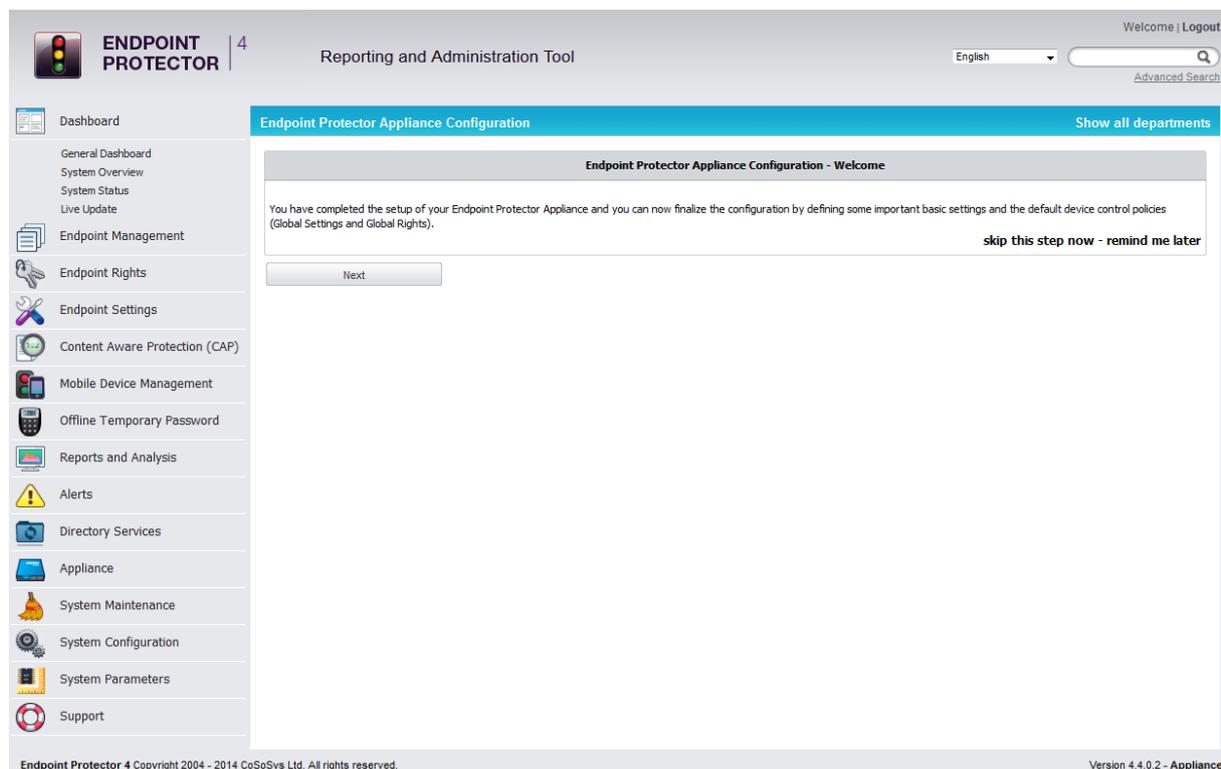
## 2.3. Se connecter à l'Interface de l'Appliance

Veillez saisir le nom d'utilisateur et mot de passe que vous avez défini pour Endpoint Protector Appliance dans l'étape d'installation précédente.



## 2.4. Assistant de Configuration de l'Appliance

Vous avez terminé la configuration de votre Endpoint Protector Appliance et vous pouvez maintenant finaliser la configuration en définissant certains paramètres importants de base et la politique par défaut de contrôle de dispositifs (Paramètres globaux) en suivant les étapes de l'Assistant de Configuration.



## 2.5. Paramètres de Base de l'Appliance

Veillez fournir ici tous les paramètres requis pour que l'Appliance fonctionne correctement. Choisissez quel droit défini ultérieurement aura priorité, quelle adresse E-mail est utilisée pour recevoir des alertes de système et quelles informations de contact sont affichées aux utilisateurs dans la boîte de dialogue Mot de Passe Offline Temporaire de la barre d'état système.

The screenshot displays the 'Endpoint Protector Appliance Configuration - System Settings' web interface. The page is divided into a left-hand navigation menu and a main configuration area. The navigation menu includes options like 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 configuration area is titled 'Endpoint Protector Appliance Configuration - System Settings' and contains several sections:

- Endpoint Protector Rights Functionality:** This section allows users to select their preferred rights functionality. It includes three radio buttons: 'Use computer rights', 'Use user rights', and 'Use both' (which is selected). Below these, there is a 'Priority' section with radio buttons for 'User rights' and 'Computer rights' (which is selected).
- E-mail Server Settings:** This section is for configuring an SMTP server. It includes fields for 'E-mail Type' (set to SMTP), 'Hostname' (smtp.example.com), 'SMTP Port' (25), 'Require SMTP Authentication' (checked), 'Username' (test@example.com), and 'Password' (masked with dots). An 'Encryption Type' dropdown is set to 'None'. A note states: '\*Note: Endpoint Protector Server will require a working Internet connection for this feature.'
- Proxy Server Settings:** This section includes fields for 'IP', 'Username', and 'Password'. A note states: '\*Note: This information refers to networks with configured Proxy server to allow access to Endpoint Protector Live Update.'
- Offline Temporary Password - Administrator Contact Details:** This section includes fields for 'Company Name' (+1-2222-5555501), 'Administrator Name' (Example), 'Administrator Phone Number' (0777255555), and 'Administrator E-mail' (alerts.email@example.com).

At the bottom of the configuration area, there are 'Back' and 'Next' buttons. The footer of the page contains the text 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and 'Version 4.4.0.2 - Appliance'.

En plus, vous pouvez sélectionner l'Intervalle d'Actualisation, activer/désactiver des fonctionnalités comme le Traçage des Fichiers et la Duplication des Fichiers et établir des paramètres par défaut pour les journaux générés.

The screenshot displays the 'Endpoint Protector Appliance Configuration - System Policies' page. The interface includes a left-hand navigation menu with categories like Dashboard, 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 features a 'Show all departments' link. It is divided into three sections: 'Mode', 'File Tracing and Shadowing', and 'Default Client Settings'. The 'Mode' section has 'Refresh Interval (sec):' set to 12 and 'Mode:' set to 'Normal'. The 'File Tracing and Shadowing' section has 'File Tracing:' checked, while 'File Shadowing:', 'Detect Copy Source:', and 'Network Share Tracing:' are unchecked. The 'Default Client Settings' section includes: 'Log Upload Interval (min):' 30, 'Local Log Size (MB):' 10, 'Shadow Interval (min):' 60, 'Shadow Size (MB):' 512, 'Minimum File Size for Shadowing (KB):' 0, 'Maximum File Size for Shadowing (KB):' 512, 'Notifier Language:' set to 'English', and 'Use Custom Client Notifications for this Language:' checked. 'Back' and 'Next' buttons are located at the bottom of the configuration area. The footer contains 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and 'Version 4.4.0.2 - Appliance'.

## 2.6. Politiques par Défaut de l'Appliance

Dans cette étape, vous pouvez définir la Politique par défaut de l'Appliance pour l'utilisation des dispositifs portables.

Cette Politique (Paramètres globaux) peut être changée plus tard.

The screenshot shows the 'Endpoint Protector Appliance Configuration - System Policies' page. The left sidebar contains navigation 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 'Default Rights' and contains a table with columns for device type, access policy, and device name. Below the table are 'Back' and 'Finish' buttons.

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

## 2.7. Finir l'Assistant de Configuration d'Endpoint Protector Appliance

Vous avez maintenant terminé l'installation et la configuration d'Endpoint Protector Appliance.

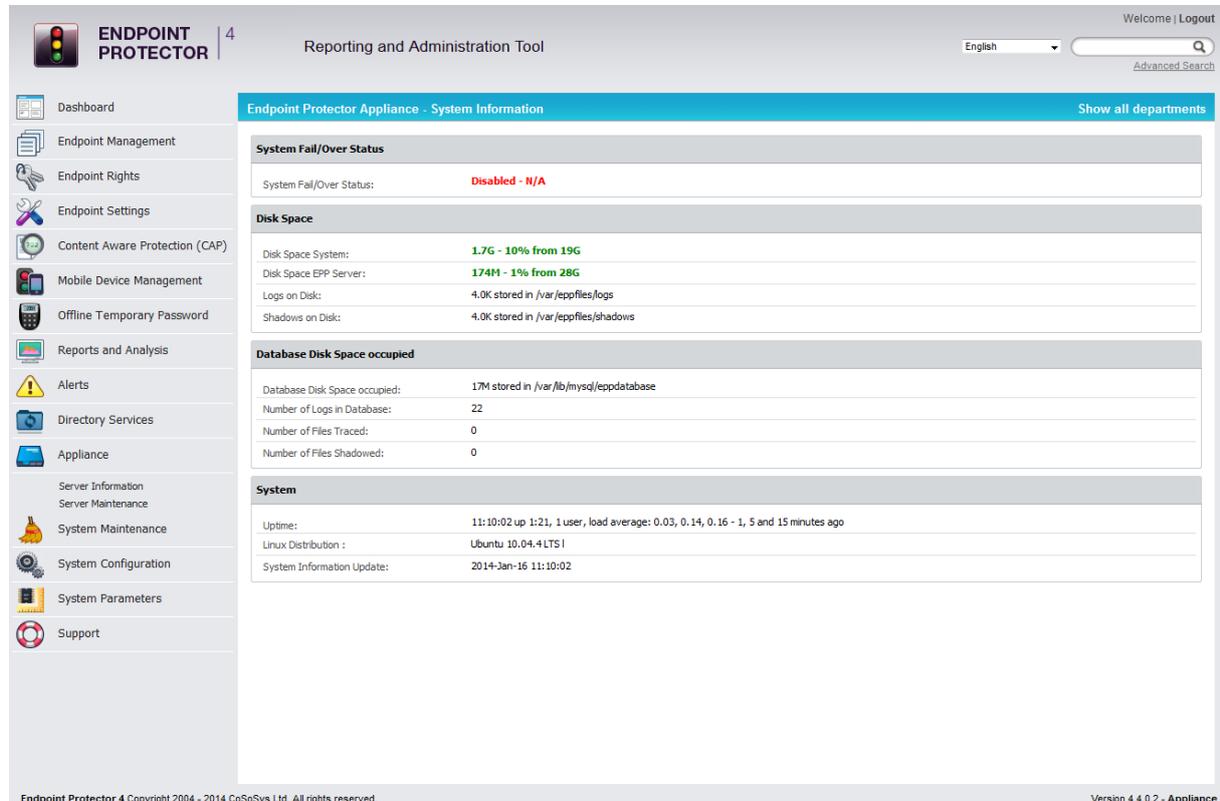
Maintenant, nous vous conseillons de déployer le client Endpoint Protector aux ordinateurs Windows et Macintosh que vous souhaitez protéger.

# 3. Paramètres de l'Appliance et Maintenance

Les Paramètres d'Endpoint Protector Appliance peuvent être accédés via le menu principal Appliance dans l'Outil d'Administration et de Rapports.

## 3.1. Informations sur le Serveur

Ici vous pouvez voir les informations sur l'état actuel du Serveur.



The screenshot displays the 'Endpoint Protector Appliance - System Information' page. The interface includes a sidebar with navigation options such as 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 shows the following 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 I
System Information Update:	2014-Jan-16 11:10:02

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

## 3.2. Maintenance du Serveur

The screenshot displays the 'Endpoint Protector Appliance - Server Maintenance' configuration interface. The left sidebar contains navigation options such as 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 divided into several 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 located 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 below 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 below 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'.

At the bottom of the page, the footer text reads: 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and 'Version 4.4.0.2 - Appliance'.

### 3.2.1. Paramètres du Réseau

Ici vous pouvez modifier les paramètres du réseau pour que l'Appliance puisse communiquer correctement dans votre réseau. Une description détaillée peut être trouvée dans le chapitre 1.7.4 "Établir l'Adresse IP de l'Appliance".

### 3.2.2. Rédémarrer l'Appliance

Vous avez l'option de redémarrer l'Appliance en cliquant sur le bouton Reboot.

### 3.2.3. Restaurer l'Appliance aux Paramètres par Défaut d'Usine

Une restauration aux paramètres d'usine effacera tous les paramètres, les politiques, les certificats et autres données sur l'appareil. Si vous revenez aux paramètres par défaut d'usine, tous les paramètres et la communication entre l'Appliance et les Clients Endpoint Protector seront interrompus. Une nouvelle installation complète de tous les clients Endpoint Protector sera également requise lors d'une nouvelle installation de l'Appliance.

## 3.3. Installation du Client Endpoint Protector pour l'Appliance

### NOTE!

Veillez-vous assurer d'activer les licences Endpoint Protector avant d'installer le client. Les licences peuvent être activées dans Configuration du Système-> Licences du Système.

The screenshot displays the 'Endpoint Protector Licensing System' interface. The top navigation bar includes 'Dashboard', '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', 'Client Software', 'Client Software Upgrade', 'Download EasyLock Software', 'System Administrators', 'System Departments', 'System Security', 'System Policies', 'System Settings', 'System Licensing', 'System Parameters', and 'Support'. The main content area is divided into three sections:

- System Status (Updates and Support):** Shows 'Number of total licenses present in the system: 0'. A table lists 'System', 'Status', and 'End Date'. Updates are 'No' and Support is 'No Support'. A 'Buy Now' button is present.
- Feature Status:** Shows a table of features with columns for 'Feature', 'Status', 'End Date', 'Total', 'Used', and 'Online'. Features include 'Device Control', 'Device Control and Content Aware Protection (CAP) for Windows', 'Device Control and Content Aware Protection (CAP) for Windows and Mac OS X', and 'Mobile Device Management', all with an 'Inactive' status.
- General License Information:** Shows a table with columns for 'Mode', 'Period', 'Endpoints', 'Mobile Endpoints', 'Device Control', 'Content Aware Protection (CAP)', 'Mobile Device Management', 'Updates', and 'Support'. Licenses include 'Trial' (30 Days, 50 Endpoints, 5 Mobile Endpoints) and 'Appetizer (Limited)' (1 Year, 5 Endpoints, 5 Mobile Endpoints).

At the bottom, there are buttons for 'Start Free Trial', 'Start Appetizer', 'Buy Licenses', 'Import Licenses', 'Paste Licenses', and 'List Licenses'. The footer indicates 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and 'Version 4.4.0.2 - Appliance'.

Comme prochaine étape pour sécuriser vos PCs et MACs, vous devez installer le Client Endpoint Protector sur les ordinateurs Windows et Macintosh que vous souhaitez protéger. Cela connectera et établira la communication entre Endpoint Protector Appliance et les clients protégés.

Pour installer le Client Endpoint Protector sur vos ordinateurs clients, téléchargez-le directement du menu Configuration du Système Logiciel Client de l'Appliance en saisissant l'adresse IP statique de l'Appliance dans un navigateur (par exemple <http://192.168.0.201>). Note: accédez-le via HTTP et pas HTTPS.

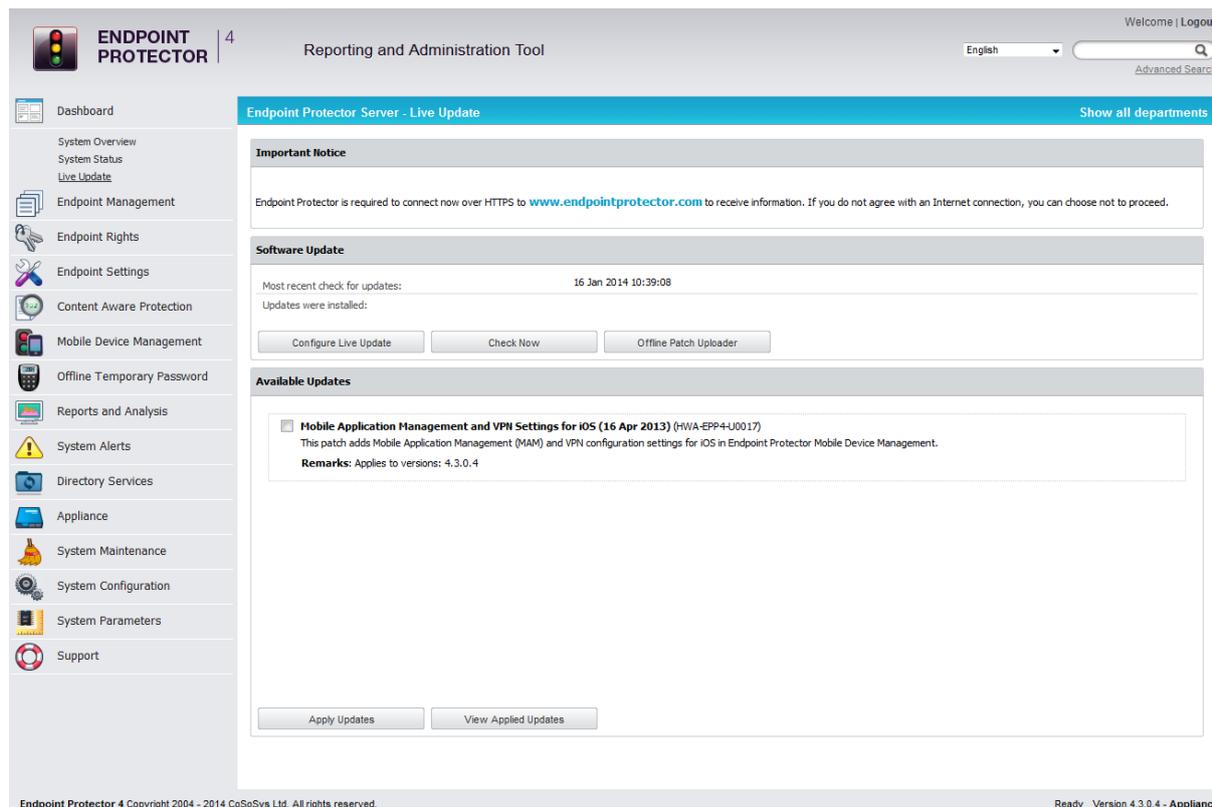
The screenshot displays the 'Endpoint Protector Reporting and Administration Tool' interface. The main content area is titled 'Endpoint Protector Server - Download Client Software' and includes a 'Show all departments' link. A note states: 'Note: Endpoint Protector Client version higher than 4.1.0.0 is required for Content Aware Protection.' Below this, it lists supported operating systems: 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), and Linux (Ubuntu, OpenSUSE). It provides instructions on where to download the client and how to install it, including fields for 'Endpoint Protector Server IP' (192.168.0.201), 'Endpoint Protector Server Port' (443), and 'Department Code' (defdep). A list of radio buttons allows selecting a version: 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, and Linux - OpenSUSE 11.4 - Version: 1.0.0-1. A 'Download selected version' button is present. At the bottom, it notes that the client for Windows can be deployed over Active Directory and refers to the 'Endpoint Protector - User Guide' for more information. The footer shows 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and 'Version 4.4.0.2 - Appliance'.

Active Directory peut être utilisé également pour déployer les clients Endpoint Protector. Cette fonctionnalité peut être trouvée dans le menu Endpoint Protector Services d'Annuaire.

### 3.4. Mises à Jour en direct en ligne

La fonctionnalité de Mises à Jour en direct vérifie en ligne s'il y a des mises à jour disponibles pour l'Appliance et pour le Client Endpoint Protector.

Vous avez le choix que l'Appliance vérifie s'il y a des mises à jour automatiquement ou manuellement. S'il y a des nouvelles mises à jour disponibles, elles seront installées uniquement quand l'administrateur les appliquera.

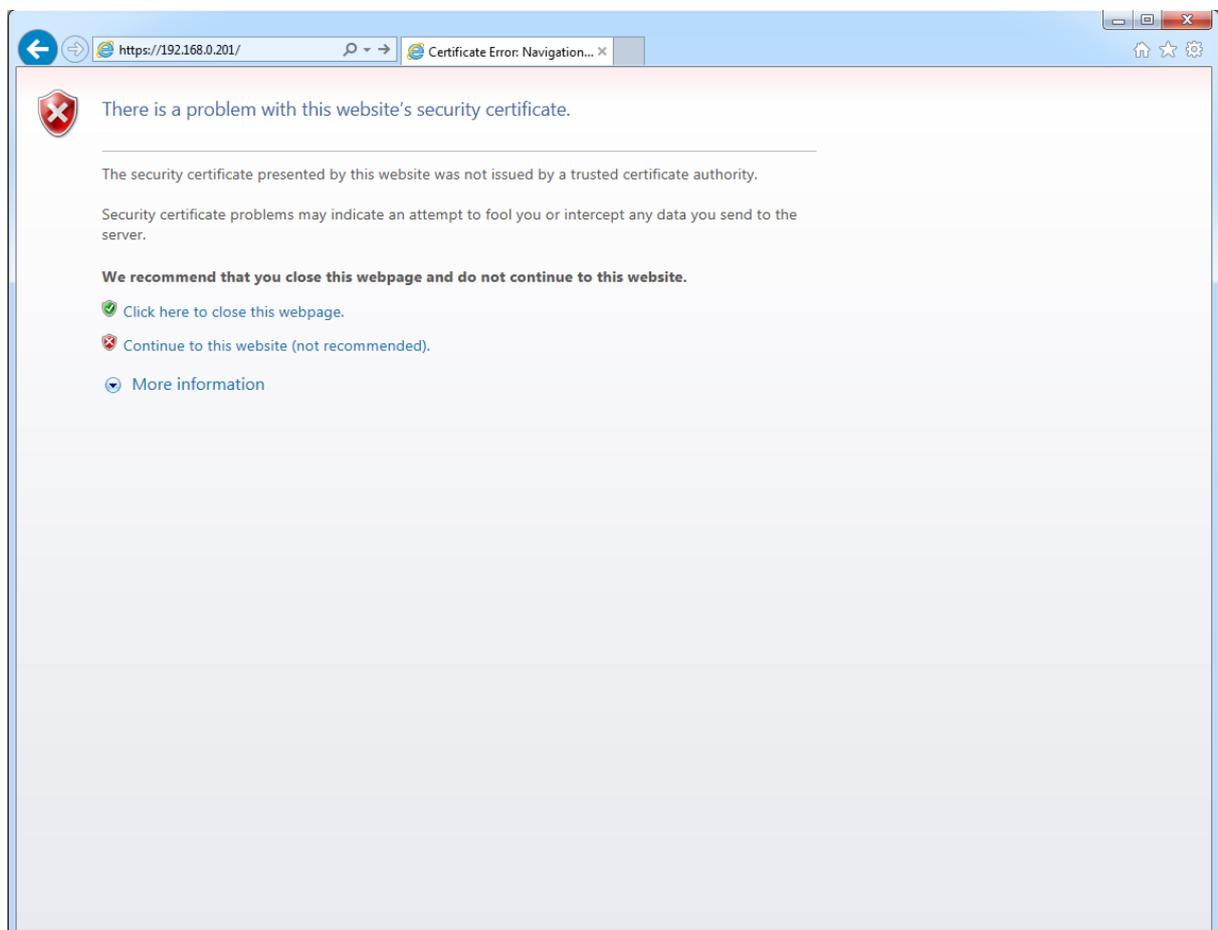


# 4. Installer le Certificat Racine à votre Navigateur

## 4.1. Pour Microsoft Internet Explorer

Ouvrez l'adresse IP de votre Outil d' Administration et de Rapports Endpoint Protector. (l'adresse IP statique de votre Appliance, ex. <https://192.168.0.201/>)

S'il n'y a pas de certificat dans votre navigateur, vous serez annoncé par une page d'Erreur de Certificat comme la capture ci-dessous.



Continuez votre navigation en cliquant  "Continuer à ce site web (pas recommandé)".

Maintenant, allez au fichier Certificat que vous avez téléchargé de l'Assistant d'Installation de l'Appliance->Certificat Serveur Appliance-> et installez le Certificat.

Cliquez le bouton Erreur de Certificat à côté de la barre d'adresses IE comme montré.

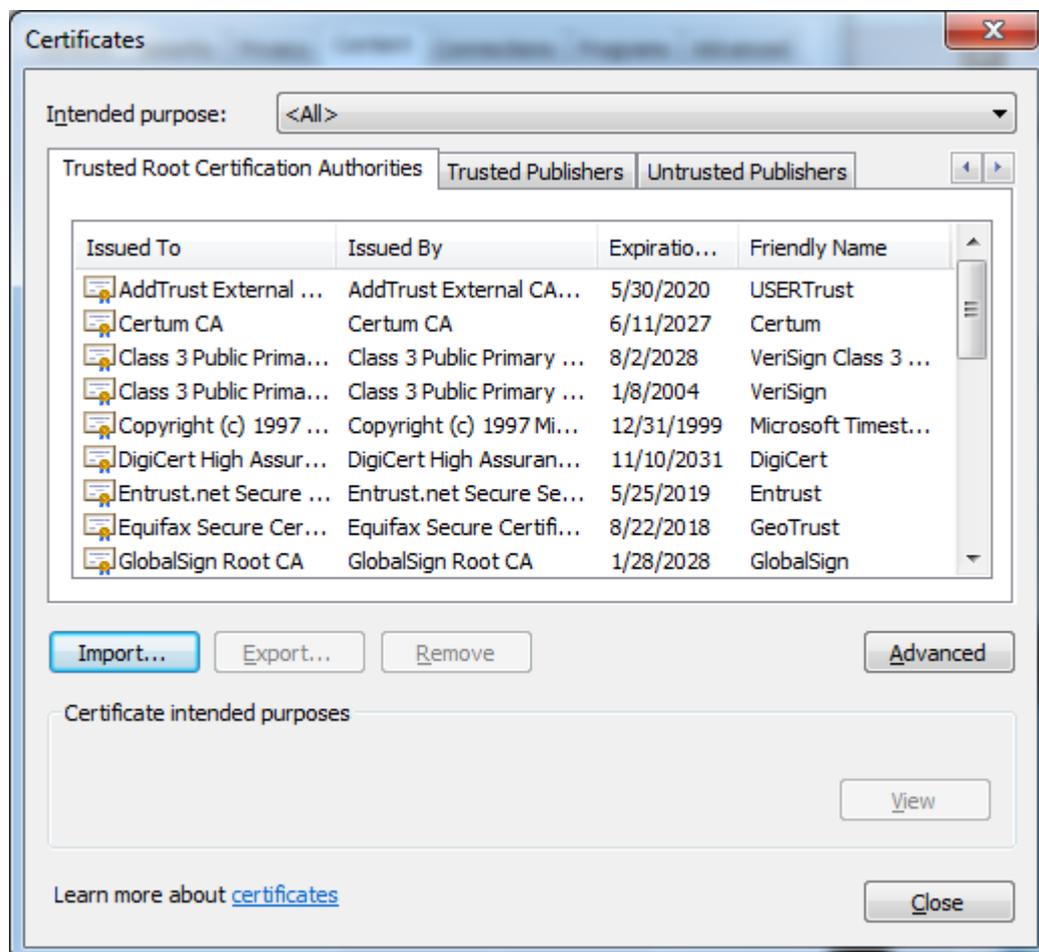
En cliquant le bouton "Erreur de Certificat", une fenêtre pop-up apparaît. Cliquez simplement "Voir certificats" dans la fenêtre pop-up.

Une autre fenêtre pop-up Certificat apparaîtra avec trois étiquettes: "Général", "Détails" et "Chemin de Certification"

Sélectionnez l'étiquette "Général" et puis cliquez le bouton "Installer Certificat..." ou allez à Outils-> Options Internet-> Contenu->Certificats.



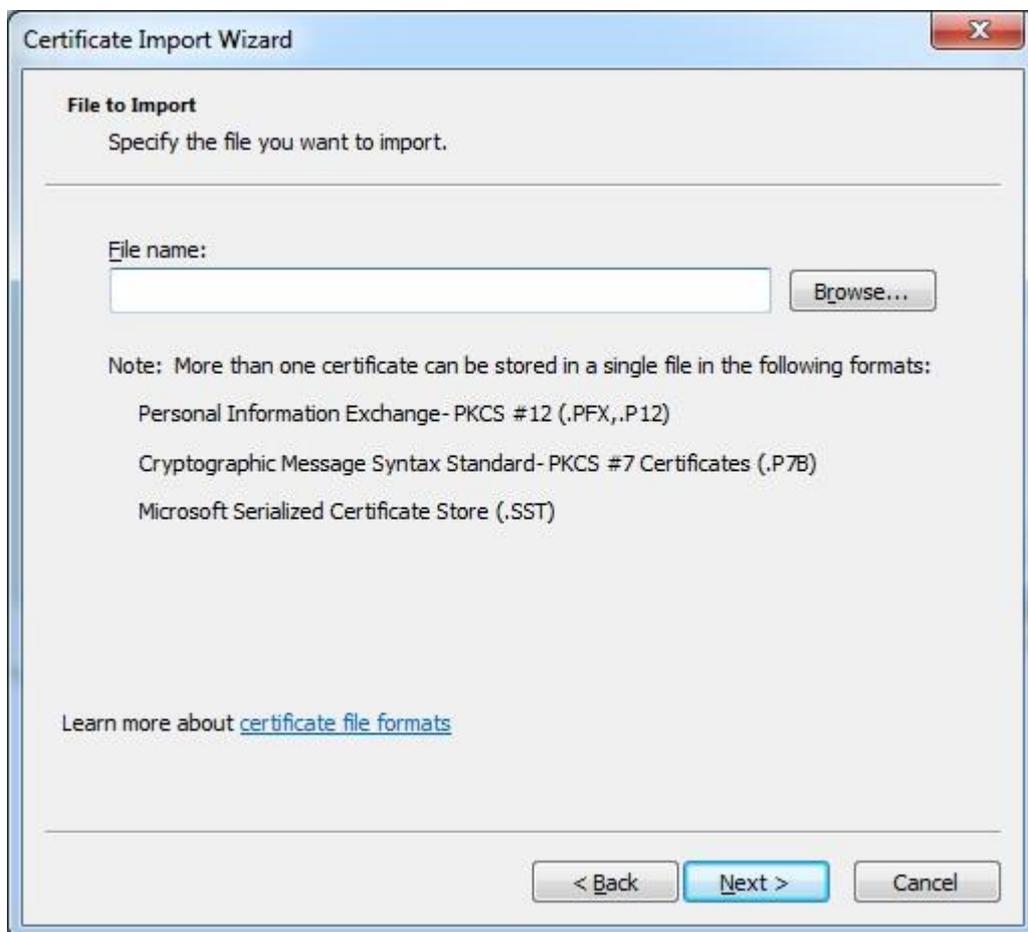
De la liste de Certificats, sélectionnez "Autorités de Certificats Racine de Confiance" et cliquez sur le bouton "Importer".



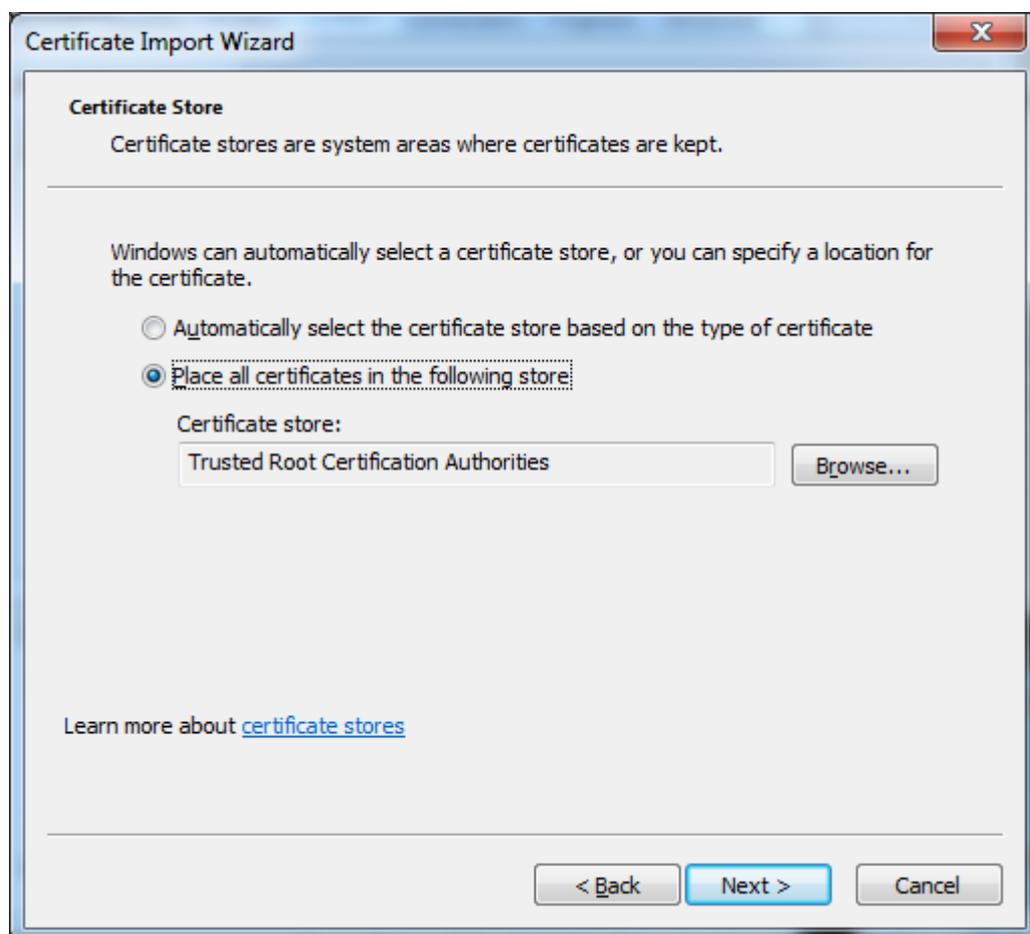
Une Bienvenue à l'Assistant d'Importation de Certificat apparaîtra. Simplement cliquez le bouton Suite.



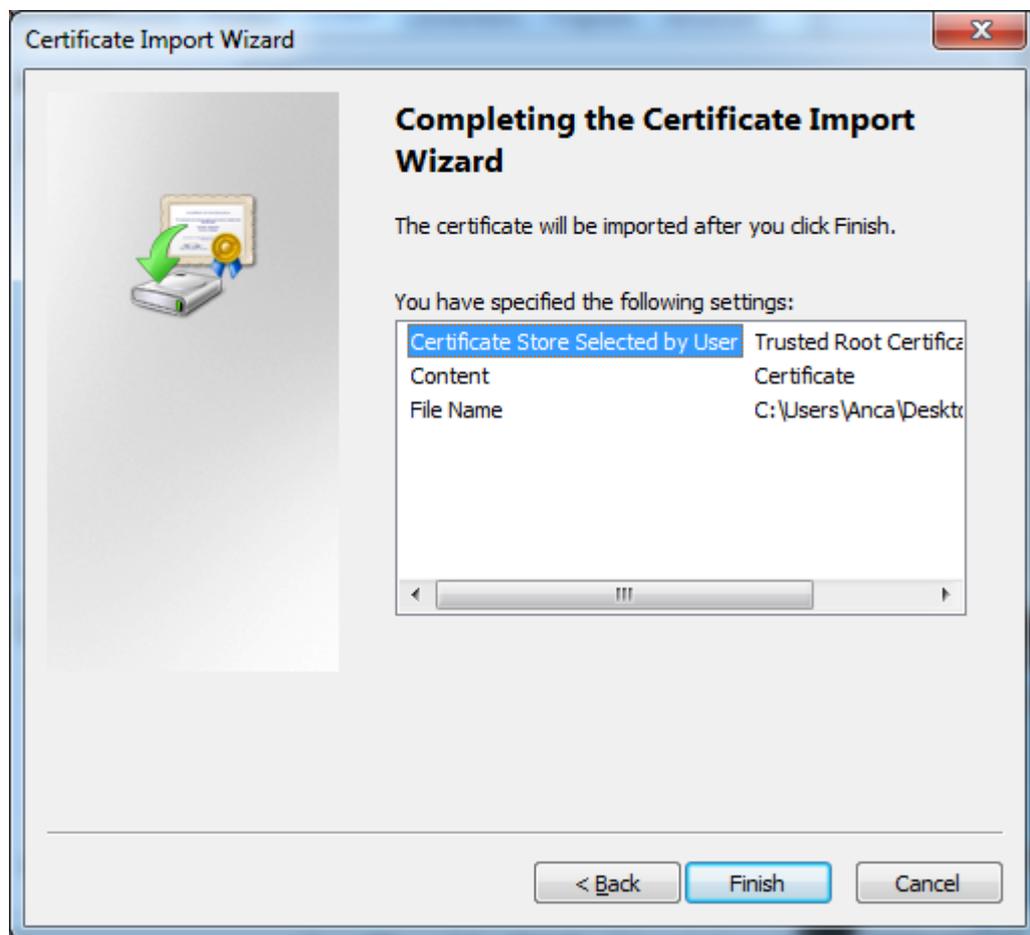
Parcourez pour le fichier Certificat que vous avez téléchargé de l'Assistant d'Installation de l'Appliance ->Certificat du Serveur Appliance.



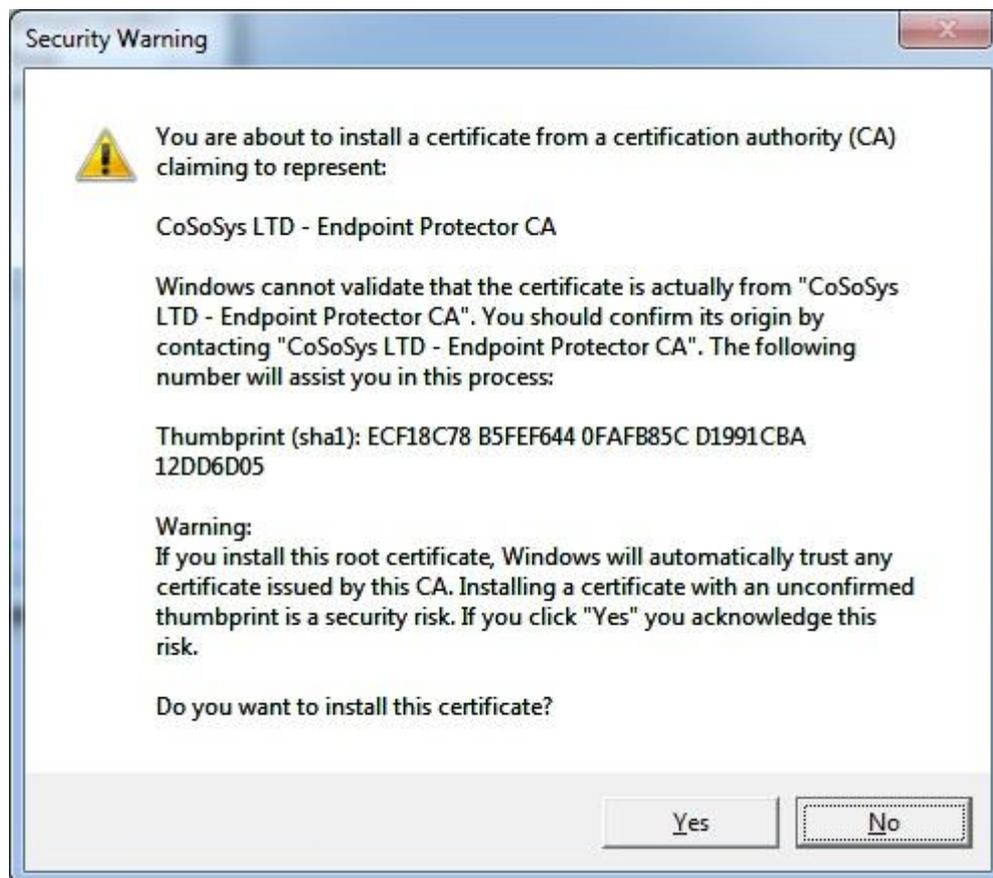
Dans la fenêtre Dépôt de Certificats, sélectionnez le bouton radio "Placer tous les certificats dans le dépôt suivant".



Une autre "Terminer l'Assistant d'Importation de Certificat" apparaît. Simplement cliquez le bouton "Finir".

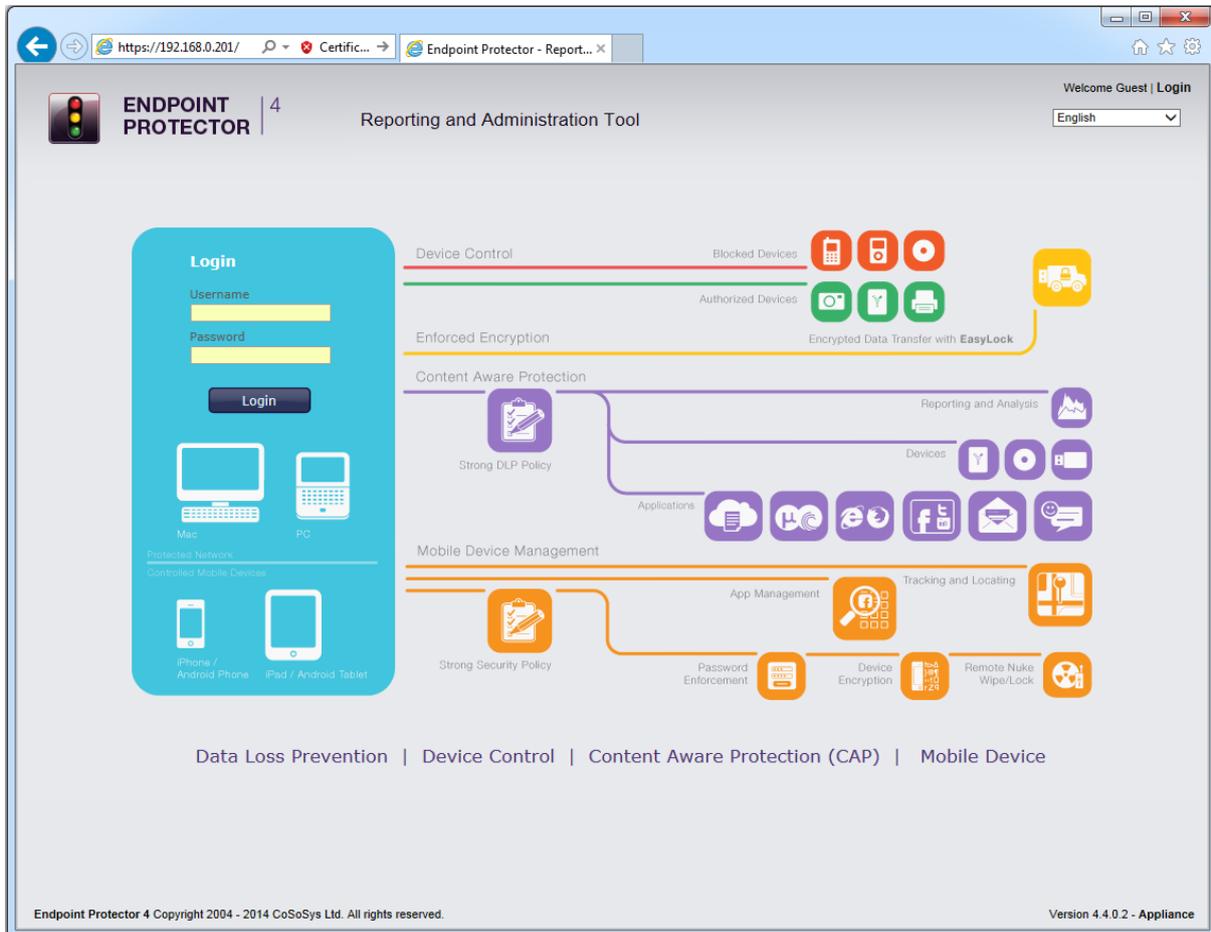


Une fenêtre d'Avertissement de Sécurité apparaît. Simplement cliquez "Oui".



Vous avez maintenant installé le Certificat avec succès.

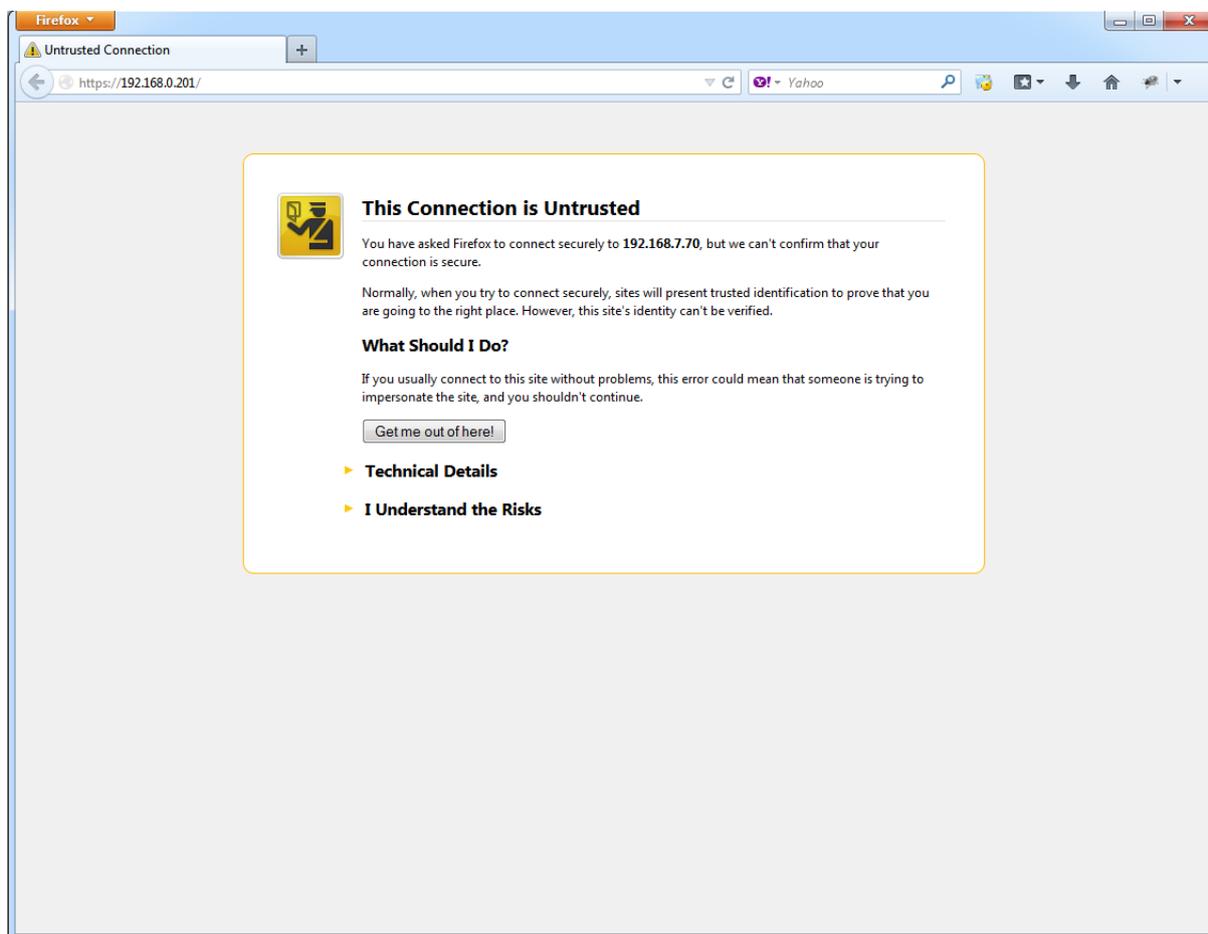
Fermez le navigateur Internet Explorer et essayez d'accéder à l'adresse IP de l'Outil d'Administration et de Rapports de nouveau.



## 4.2. Pour Mozilla Firefox

Ouvrez le Navigateur.

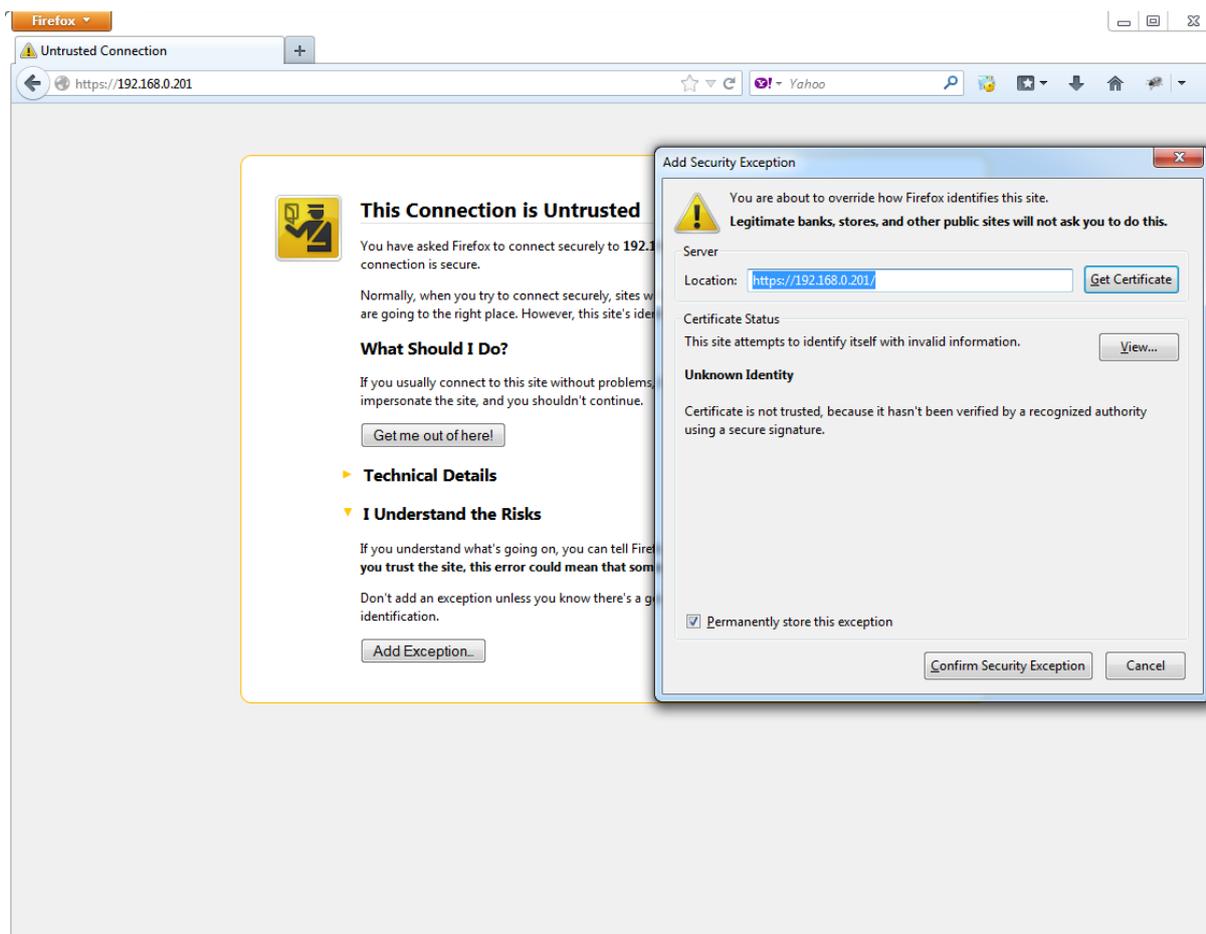
Ouvrez l'adresse IP de l'Outil de Rapports et Administration Endpoint Protector. (Votre adresse IP statique de l'Appliance, exemple <https://192.168.0.201/>).



De la capture Cette Connexion n'est Pas de Confiance ci-dessus, choisissez Je comprends les Risques. Cliquez Ajouter Exception.

La fenêtre d'Avertissement de Sécurité apparaît.

Simplement cliquez le bouton Obtenir le Certificat et puis le bouton Confirmer l'Exception de Sécurité.



Fermez le navigateur et démarrez-le de nouveau.

The screenshot shows the Endpoint Protector Reporting and Administration Tool interface. The browser window title is "Endpoint Protector - Reporting and Ad..." and the address bar shows "https://192.168.0.201/". The page header includes the "ENDPOINT PROTECTOR 4" logo, the title "Reporting and Administration Tool", and a "Welcome Guest | Login" message with a language dropdown set to "English".

The main interface features a central navigation area with several key sections:

- Login:** A blue sidebar on the left contains a login form with fields for "Username" and "Password", a "Login" button, and icons for "Mac" and "PC" under "Protected Network", and "iPhone / Android Phone" and "iPad / Android Tablet" under "Controlled Mobile Devices".
- Device Control:** Includes "Blocked Devices" (with icons for a phone, tablet, and camera) and "Authorized Devices" (with icons for a camera, mail, and printer).
- Enforced Encryption:** Features "Encrypted Data Transfer with EasyLock" and a truck icon.
- Content Aware Protection (CAP):** Includes "Strong DLP Policy", "Reporting and Analysis" (with a chart icon), "Applications" (with icons for various apps), and "Devices" (with icons for a phone, tablet, and laptop).
- Mobile Device Management:** Includes "Strong Security Policy", "App Management", "Tracking and Locating" (with a location pin icon), "Password Enforcement", "Device Encryption" (with a padlock icon), and "Remote Nuke Wipe/Lock" (with a bomb icon).

At the bottom of the interface, there is a navigation bar with the following links: "Data Loss Prevention | Device Control | Content Aware Protection (CAP) | Mobile Device".

The footer contains the text: "Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved." on the left and "Version 4.4.0.2 - Appliance" on the right.

# 5. Support

Dans le cas où vous avez besoin d'aide supplémentaire, comme les FAQs ou si vous nécessitez de support par e-mail, vous pouvez visiter le site web de support directement au <http://www.cososys.com/help.html>

## 6. Note Importante / Démenti

Les mesures de sécurité, par leur nature, sont capables de contournement. CoSoSys ne peut pas, et ne garantit pas que les données ou les dispositifs ne seront pas accédés par des personnes non autorisées, et CoSoSys décline toute garantie à cet effet dans toute la mesure permise par la loi.

© 2004 – 2014 CoSoSys Ltd.; Endpoint Protector Basic, EPPBasic, Endpoint Protector, My Endpoint Protector sont marques de CoSoSys Ltd. Tous droits réservés. Windows est une marque enregistrée de Microsoft Corporation. Macintosh, Mac OS X sont marques d'Apple Corporation. Tout autre nom et marque sont propriété de leurs propriétaires respectifs.