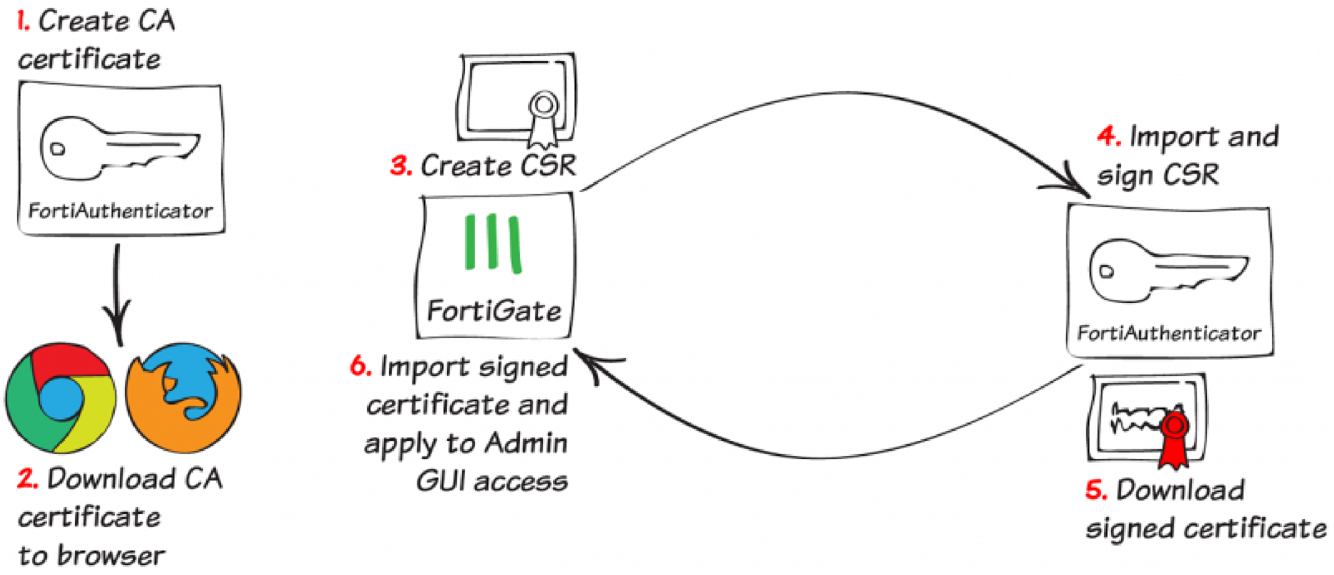
FortiAuthenticator as a Certificate Authority

For this recipe, you will configure the FortiAuthenticator as a Certificate Authority (CA). This will allow the FortiAuthenticator to sign certificates that the FortiGate will use to secure administrator GUI access.

This scenario includes creating a certificate request on the FortiGate, downloading the certificate to the network's computers, and then importing it to the FortiAuthenticator. You will sign the certificate with the FortiAuthenticator's own certificate, then download and import the signed certificate back to the FortiGate.

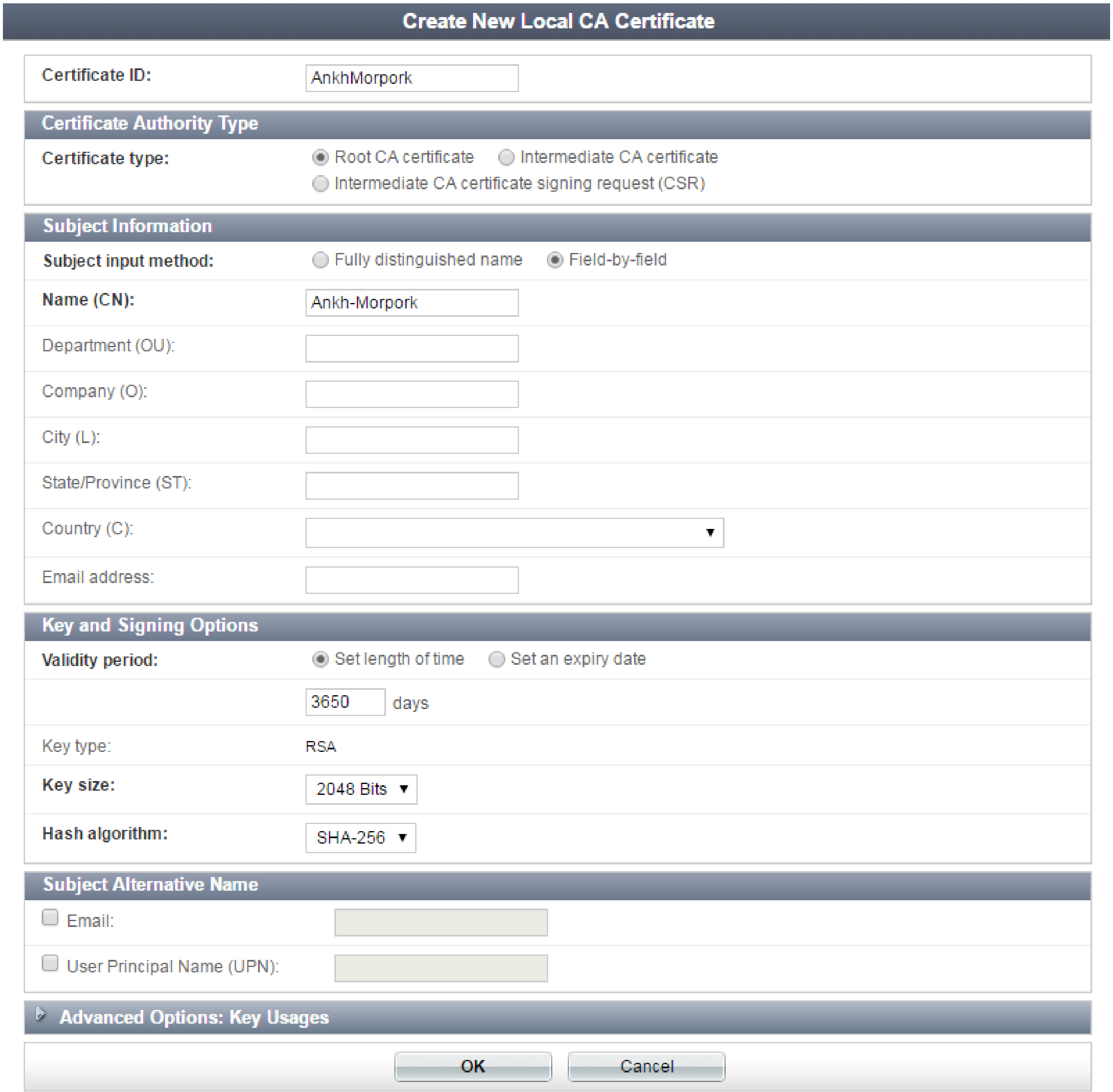
The process of downloading the certificate to the network's computers will depend on which web browser you use. Internet Explorer and Chrome use one certificate store, while Firefox uses another. This configuration includes both methods.


1. Create CA certificate
FortiAuthenticator
2. Download CA certificate to browser
3. Create CSR
FortiGate
6. Import signed certificate and apply to Admin GUI access
4. Import and sign CSR
FortiAuthenticator
5. Download signed certificate

1. Creating a new CA on the FortiAuthenticator

On the FortiAuthenticator, go to **Certificate Management > Certificate Authorities > Local CAs** and create a new CA.

Enter a **Certificate ID**, select **Root CA certificate**, and configure the key options as shown in the example.



Create New Local CA Certificate

Certificate ID: AnkhMorpork

Certificate Authority Type

Certificate type: ● Root CA certificate ○ Intermediate CA certificate ○ Intermediate CA certificate signing request (CSR)

Subject Information

Subject input method: ○ Fully distinguished name ● Field-by-field

Name (CN): Ankh-Morpork

Department (OU):

Company (O):

City (L):

State/Province (ST):

Country (C):

Email address:

Key and Signing Options

Validity period: ● Set length of time ○ Set an expiry date

3650 days

Key type: RSA

Key size: 2048 Bits

Hash algorithm: SHA-256

Subject Alternative Name

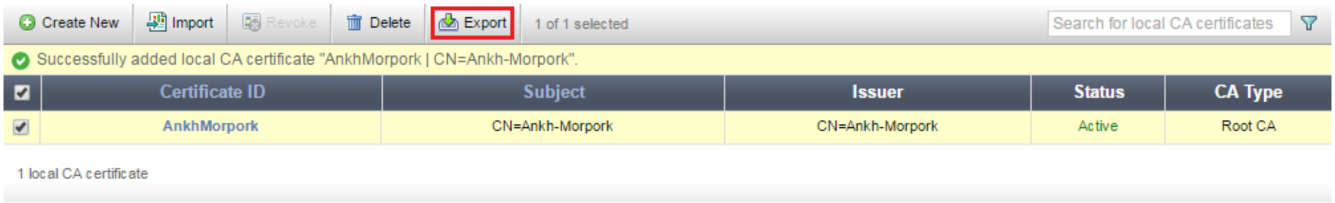
□ Email:

□ User Principal Name (UPN):

Advanced Options: Key Usages

Once created, highlight the certificate and select **Export**.

This will save a **.crt** file to your local drive.



Successfully added local CA certificate "AnkhMorpork | CN=Ankh-Morpork".

☑	Certificate ID	Subject	Issuer	Status	CA Type
☑	AnkhMorpork	CN=Ankh-Morpork	CN=Ankh-Morpork	Active	Root CA

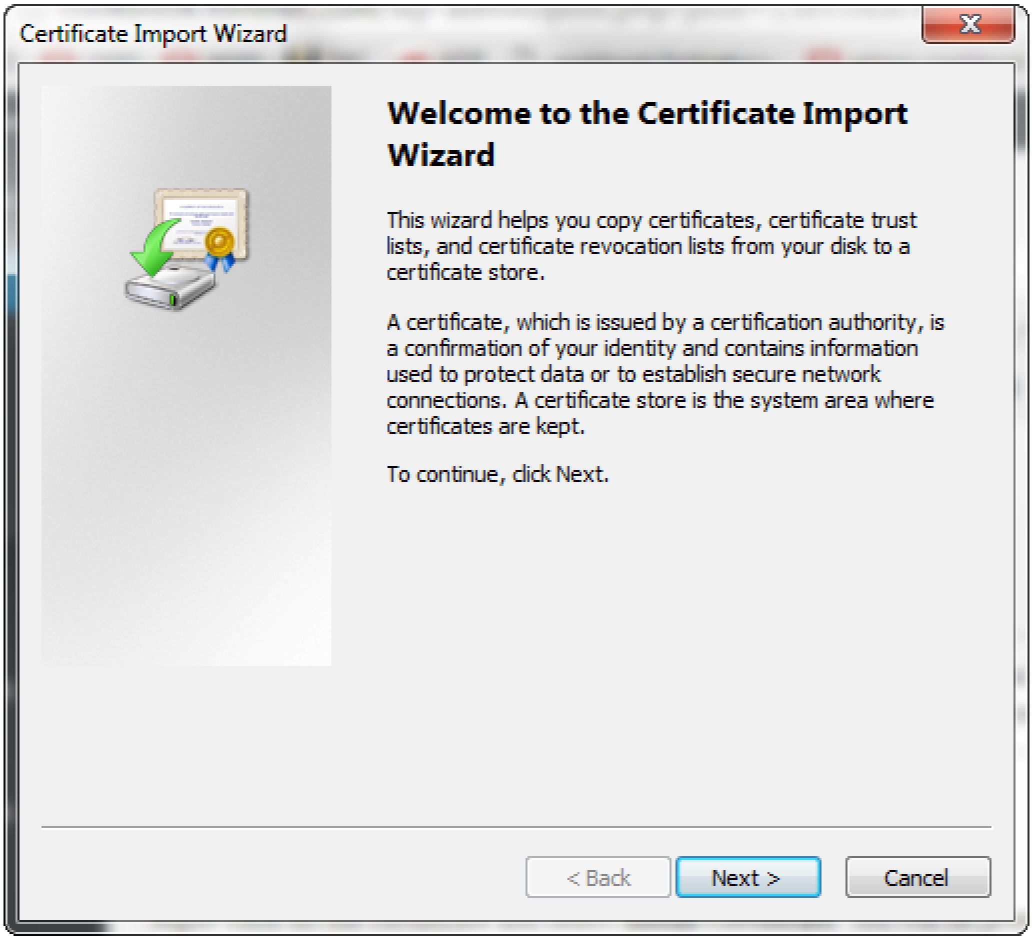
1 local CA certificate

2. Installing the CA on the network

The certificate must now be installed on the computers in your network as a trusted root CA. The steps below show different methods of installing the certificate, depending on your browser.

Internet Explorer and Chrome

In Windows Explorer, right-click on the certificate and select **Install Certificate**. Open the certificate and follow the **Certificate Import Wizard**.


Certificate Import Wizard

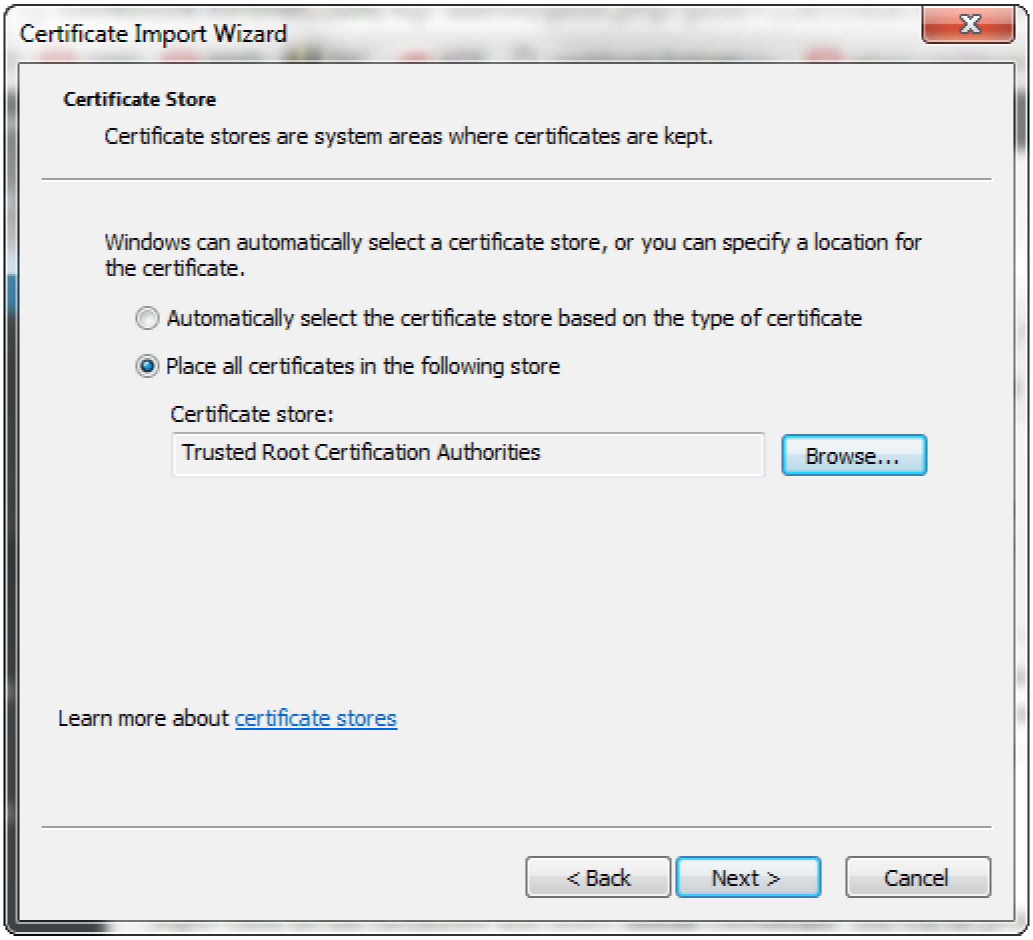
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Make sure to place the certificate in the **Trusted Root Certification Authorities** store.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

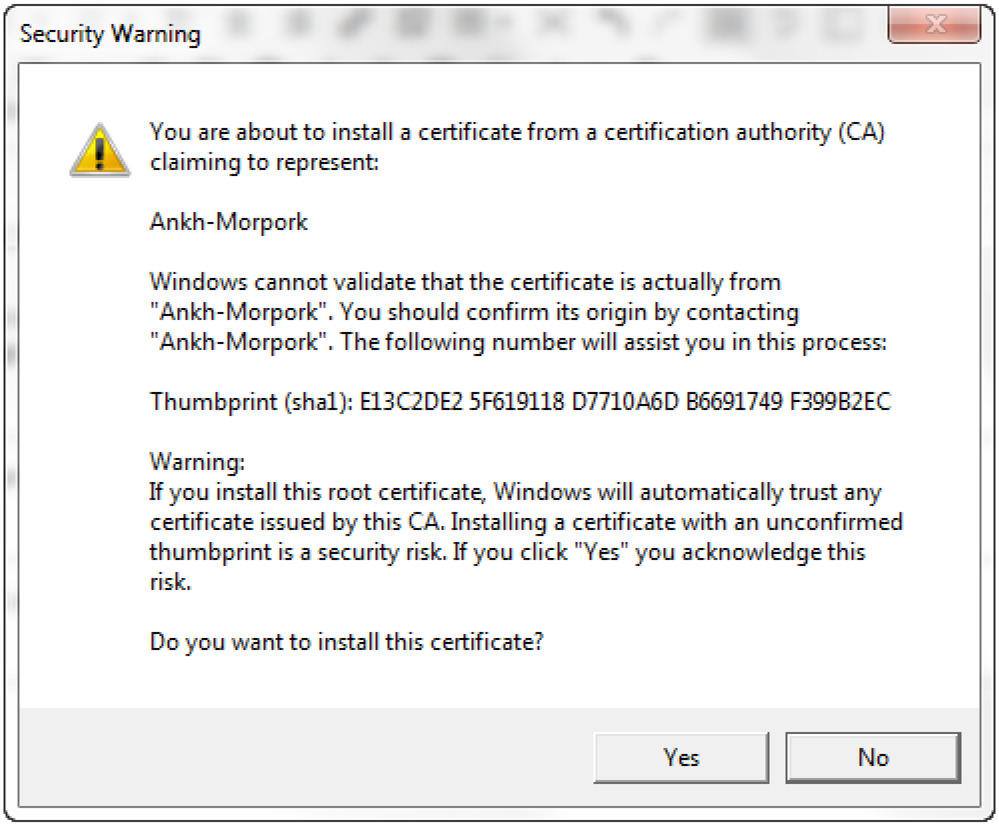
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Learn more about certificate stores

Finish the Wizard, and select **Yes** to confirm and install the certificate.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

Ankh-Morpork

Windows cannot validate that the certificate is actually from "Ankh-Morpork". You should confirm its origin by contacting "Ankh-Morpork". The following number will assist you in this process:

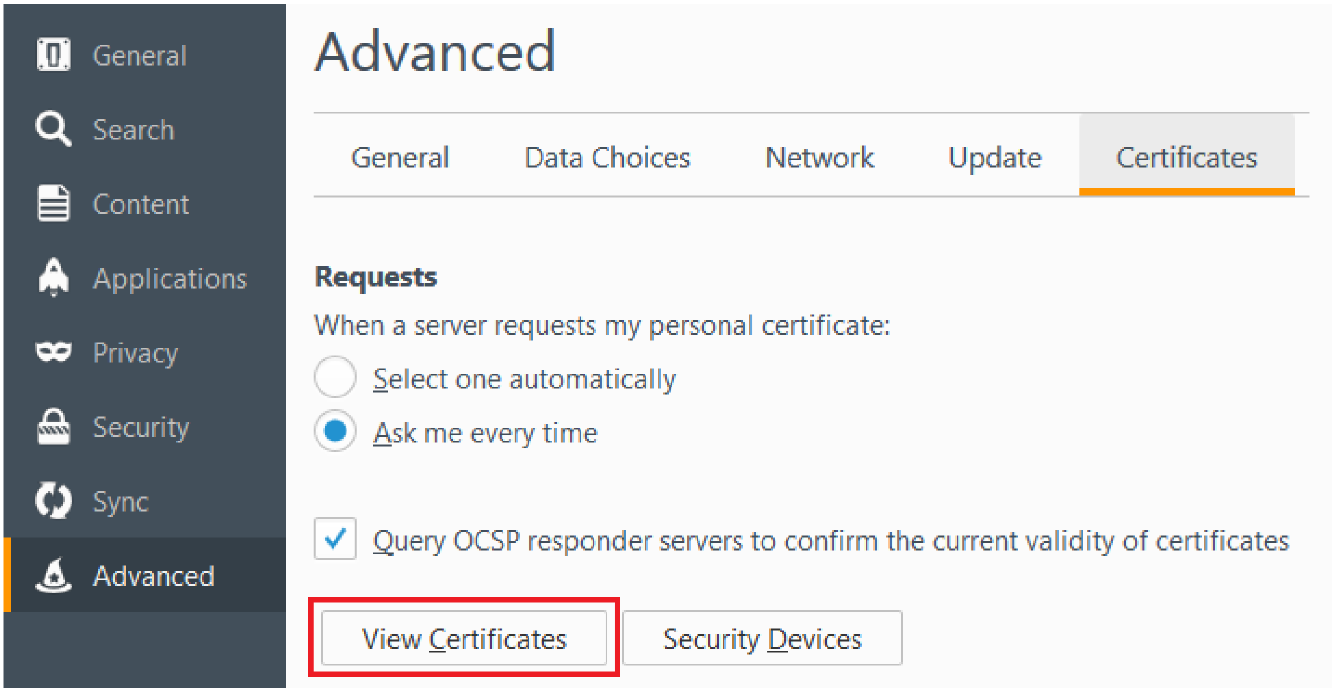
Thumbprint (sha1): E13C2DE2 5F619118 D7710A6D B6691749 F399B2EC

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Firefox

In the web browser, go to **Options > Advanced > Certificates** and select **View Certificates**.



Advanced

Requests

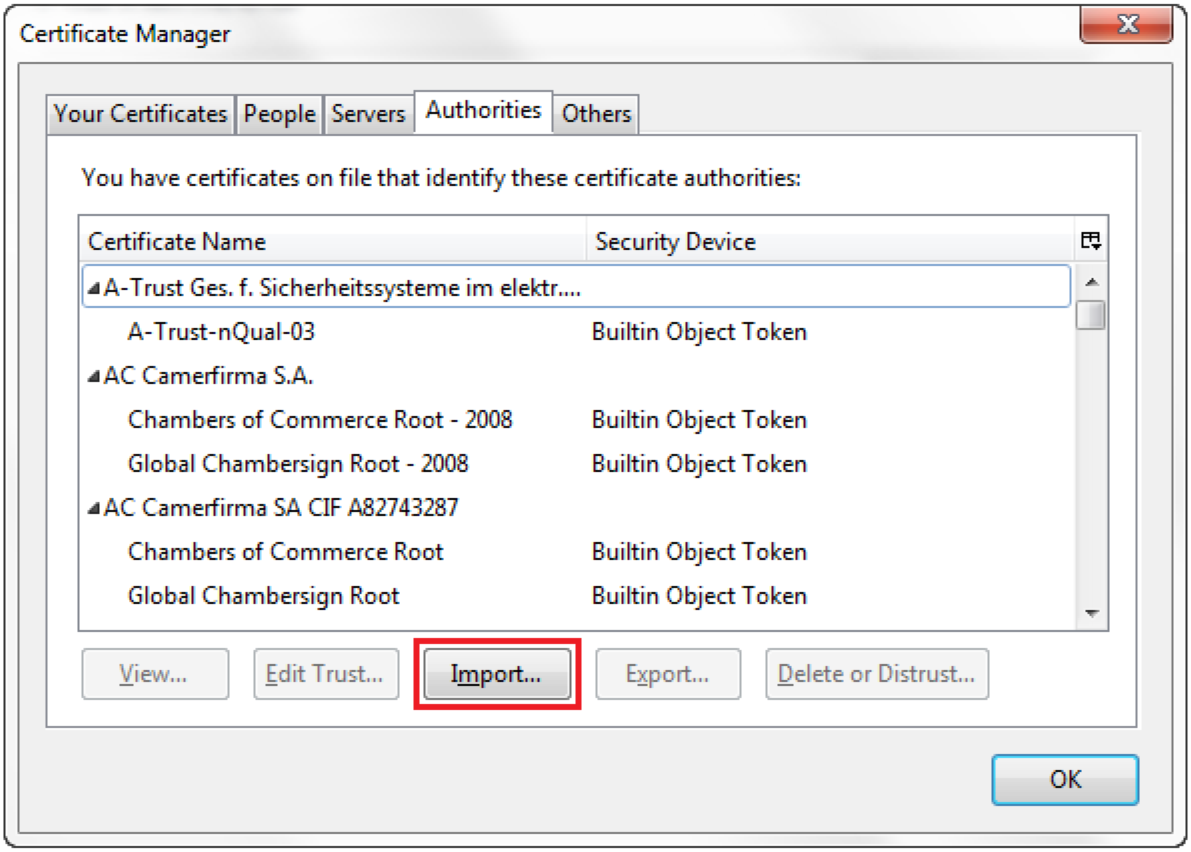
When a server requests my personal certificate:

○ Select one automatically

● Ask me every time

☑ Query OCSP responder servers to confirm the current validity of certificates

In the **Authorities** tab, select **Import**.

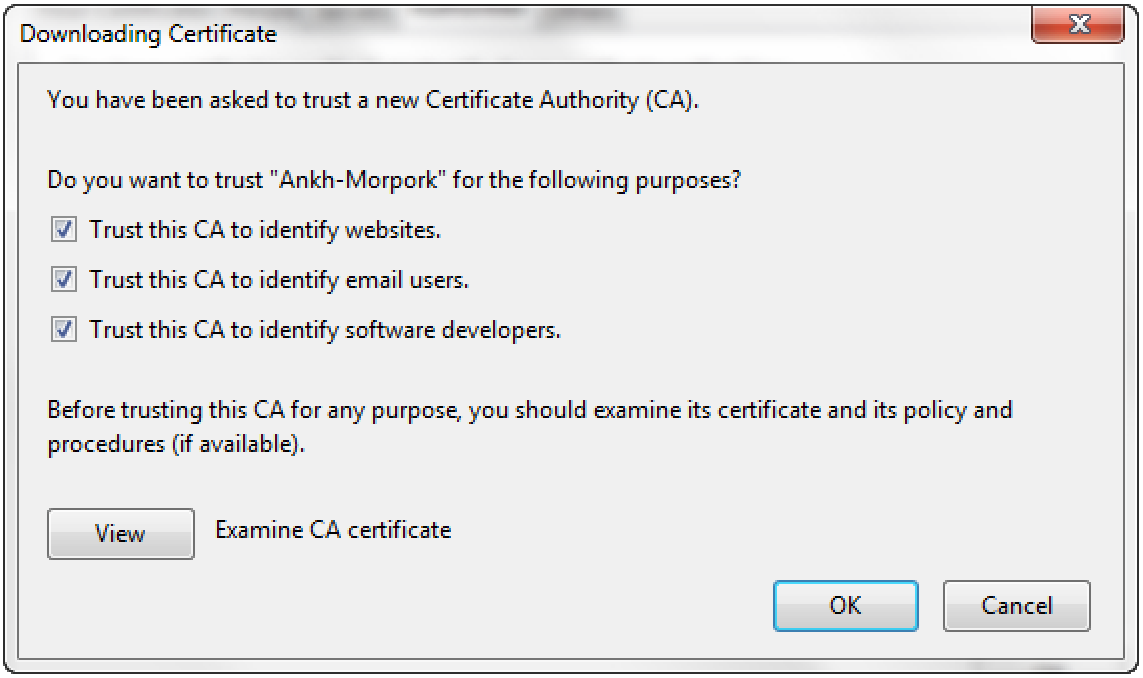

Certificate Manager

You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
◢A-Trust Ges. f. Sicherheitssysteme im elektr....	
A-Trust-nQual-03	Builtin Object Token
◢AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
◢AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	Builtin Object Token
Global Chambersign Root	Builtin Object Token

Find and open the root certificate.

You will be asked what purposes the certificate will be trusted to identify. Select all options, and select **OK**.


Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "Ankh-Morpork" for the following purposes?

☑ Trust this CA to identify websites.

☑ Trust this CA to identify email users.

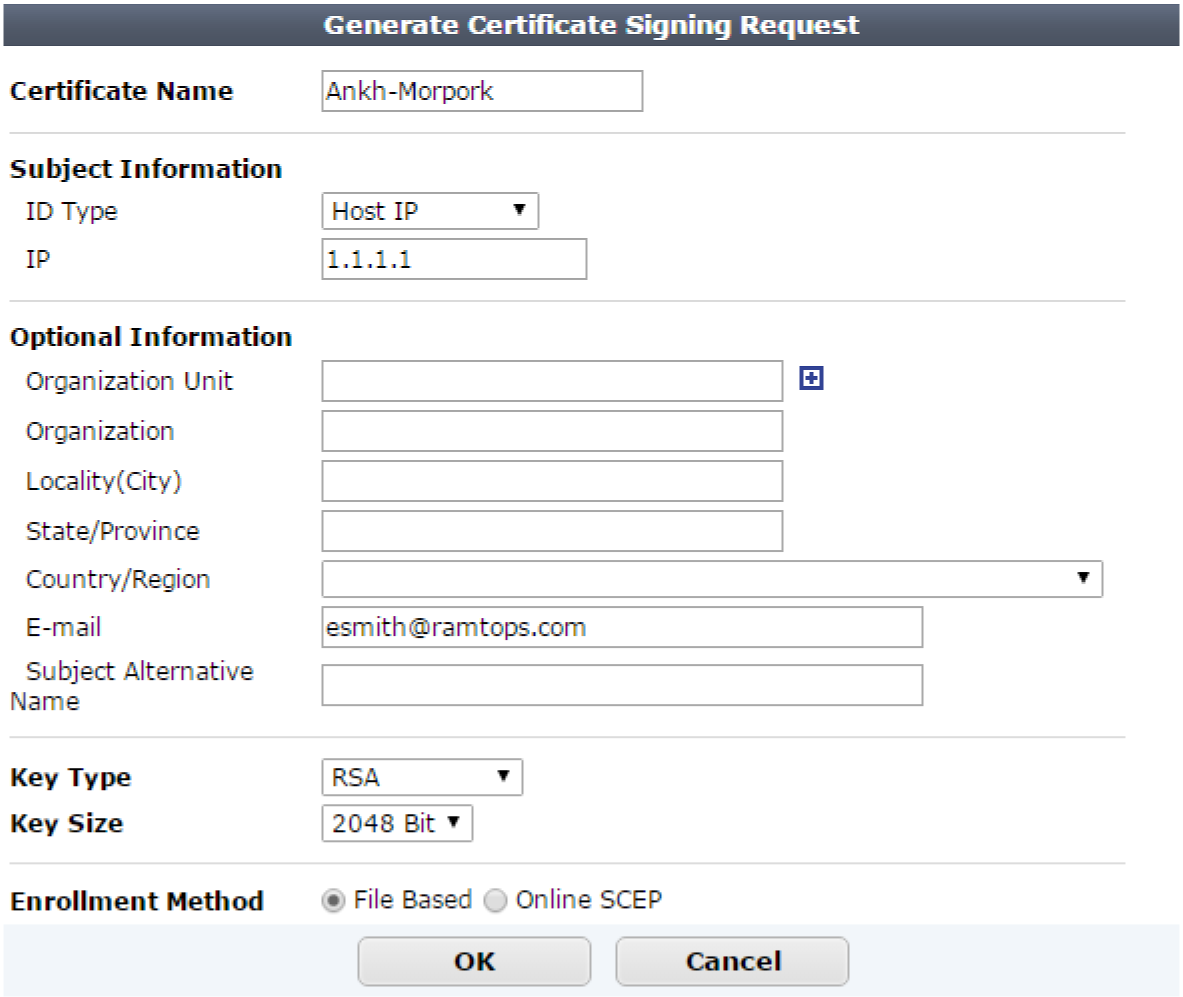
☑ Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

3. Creating a CSR on the FortiGate

On the FortiGate, go to **System > Certificates** and select **Generate** to create a new certificate signing request (CSR).

Enter a **Certificate Name**, the Internet facing IP address of the FortiGate, and a valid email address, then configure the key options as shown in the example.

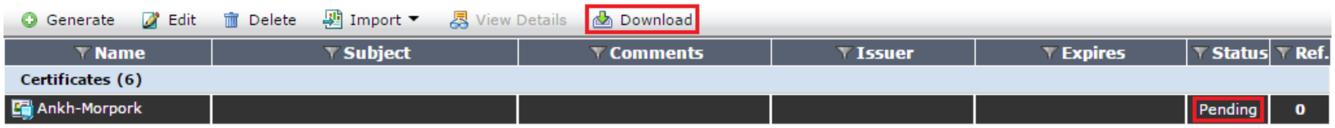


Generate Certificate Signing Request

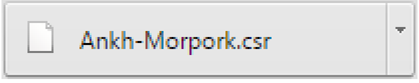
Certificate Name	Ankh-Morpork
Subject Information	
ID Type	Host IP ▾
IP	1.1.1.1
Optional Information	
Organization Unit	
Organization	
Locality(City)	
State/Province	
Country/Region	▾
E-mail	esmith@ramtops.com
Subject Alternative Name	
Key Type	RSA ▾
Key Size	2048 Bit ▾
Enrollment Method	● File Based ○ Online SCEP

Once created, the certificate will show a **Status** of **Pending**. Highlight the certificate and select **Download**.

This will save a **.csr** file to your local drive.



Name	Subject	Comments	Issuer	Expires	Status	Ref.
Certificates (6)						
Ankh-Morpork					Pending	0

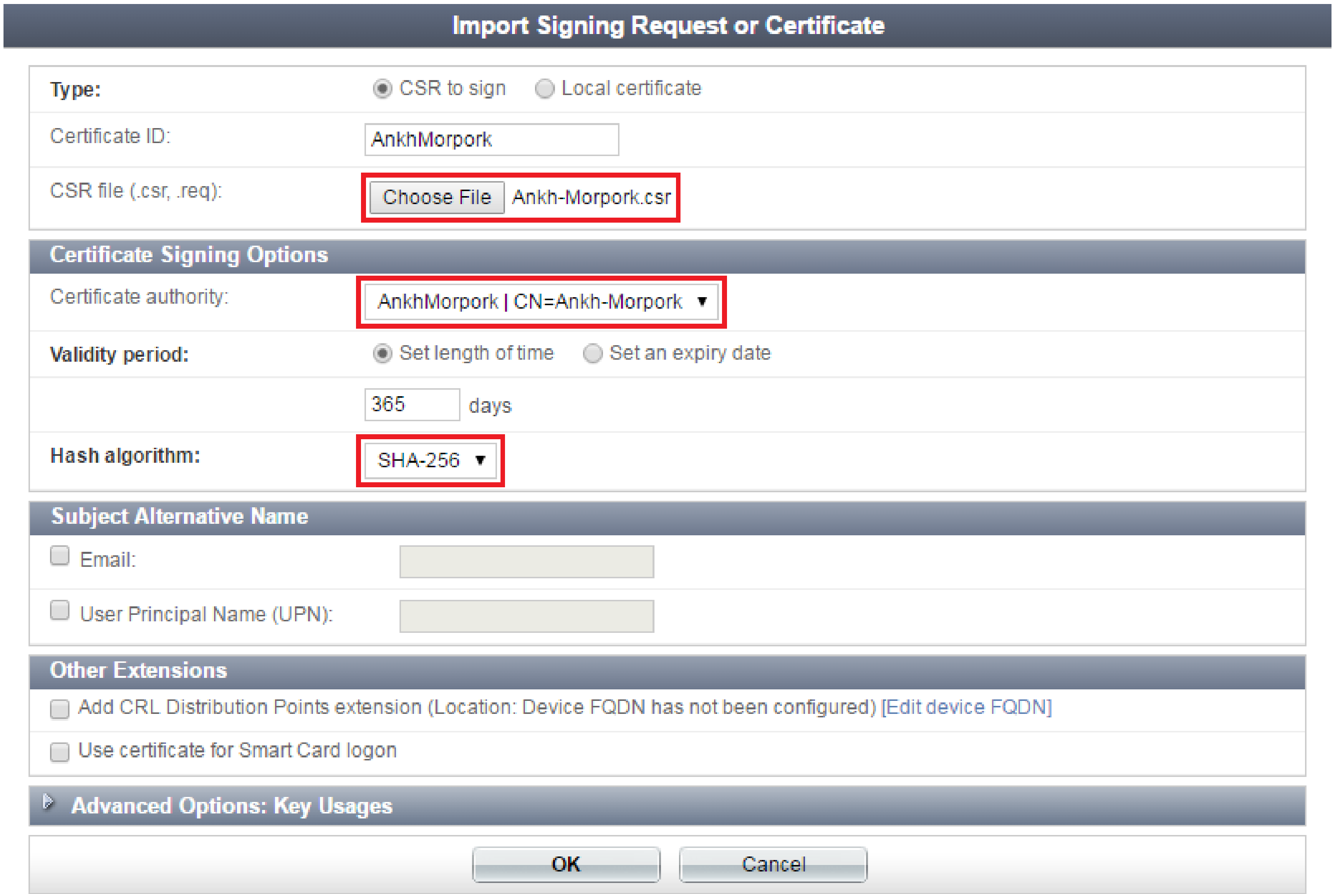


Ankh-Morpork.csr

4. Importing and signing the CSR on the FortiAuthenticator

Back on the FortiAuthenticator, go to **Certificate Management > End Entities > Users** and import the **.csr** certificate created earlier.

Make sure to select the **Certificate authority** from the dropdown menu and set the **Hash algorithm** to **SHA-256**, as configured earlier.



Import Signing Request or Certificate

Type:	● CSR to sign ○ Local certificate
Certificate ID:	AnkhMorpork
CSR file (.csr, .req):	Choose File Ankh-Morpork.csr

Certificate Signing Options

Certificate authority:	AnkhMorpork | CN=Ankh-Morpork ▾
Validity period:	● Set length of time ○ Set an expiry date
	365 days
Hash algorithm:	SHA-256 ▾

Subject Alternative Name

□ Email:

□ User Principal Name (UPN):

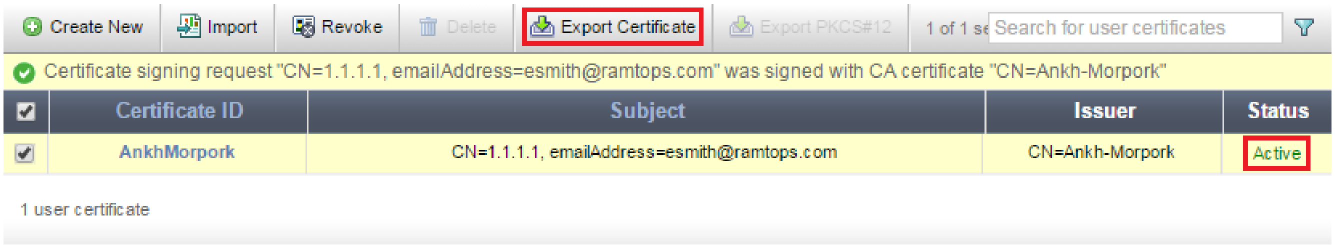
Other Extensions

□ Add CRL Distribution Points extension (Location: Device FQDN has not been configured) [Edit device FQDN]

□ Use certificate for Smart Card logon

Once imported, you should see that the certificate has been signed by the FortiAuthenticator, with a **Status** of **Active**. Highlight the certificate and select **Export Certificate**.

This will save a **.cer** file to your local drive.



Certificate signing request "CN=1.1.1.1, emailAddress=esmith@ramtops.com" was signed with CA certificate "CN=Ankh-Morpork"

☑	Certificate ID	Subject	Issuer	Status
☑	AnkhMorpork	CN=1.1.1.1, emailAddress=esmith@ramtops.com	CN=Ankh-Morpork	Active

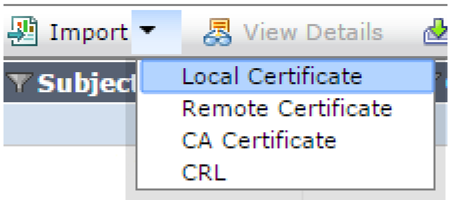
1 user certificate

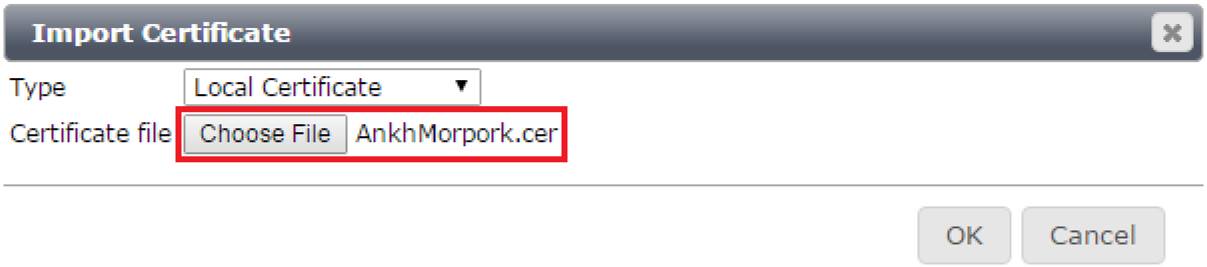
AnkhMorpork.cer

5. Importing the local certificate to the FortiGate

Back on the FortiGate, go to **System > Certificates** and select **Local Certificate** from the **Import** dropdown menu.

Browse to the **.cer** certificate you just created. Select **Open** and then select **OK**.

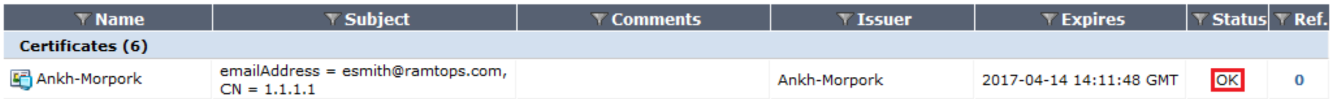



Import Certificate

Type: Local Certificate

Certificate file: Choose File AnkhMorpork.cer

You should now see that the certificate's **Status** has changed from **Pending** to **OK**. You may have to refresh your page to see the status change.

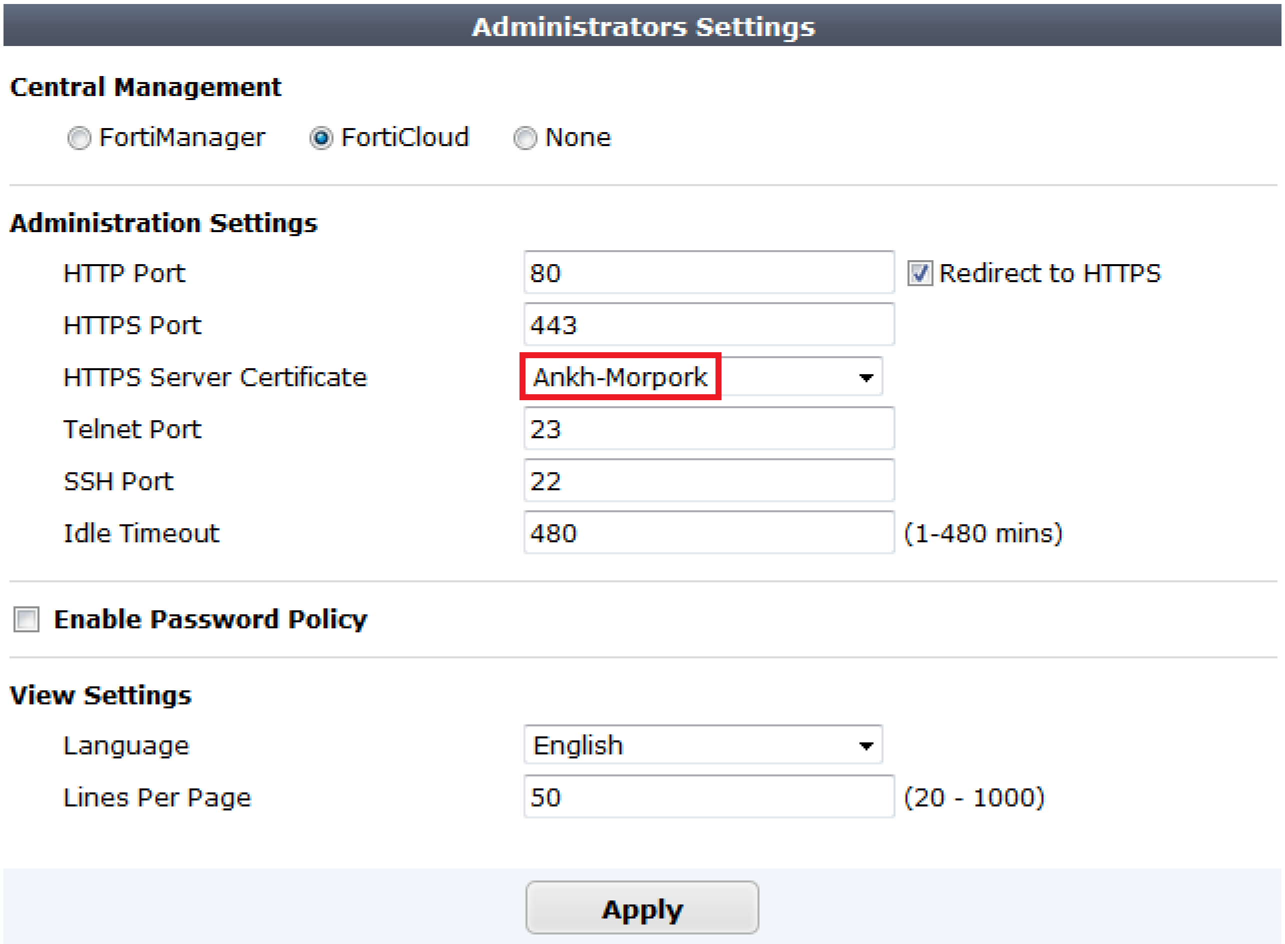


Name	Subject	Comments	Issuer	Expires	Status	Ref.
Certificates (6)						
Ankh-Morpork	emailAddress = esmith@ramtops.com, CN = 1.1.1.1		Ankh-Morpork	2017-04-14 14:11:48 GMT	OK	0

6. Configuring the certificate for the GUI

Go to **System > Admin > Settings**.

Under **Administration Settings**, set **HTTPS Server Certificate** to the certificate created/signed earlier, then select **Apply**.



Administrators Settings

Central Management

○ FortiManager ● FortiCloud ○ None

Administration Settings

HTTP Port	80	☑ Redirect to HTTPS
HTTPS Port	443	
HTTPS Server Certificate	Ankh-Morpork	
Telnet Port	23	
SSH Port	22	
Idle Timeout	480	(1-480 mins)

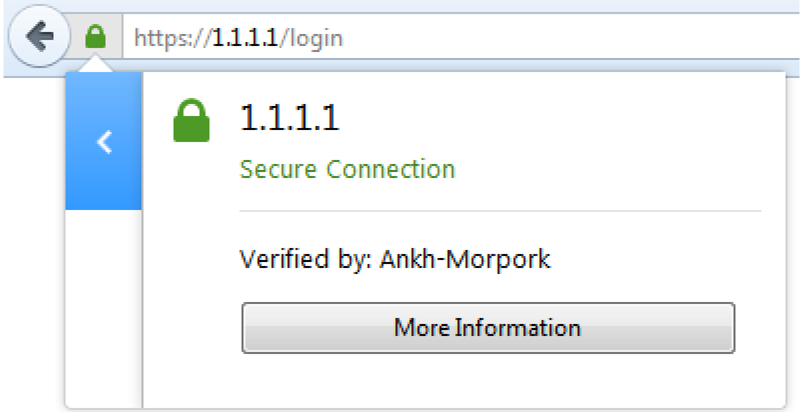
□ **Enable Password Policy**

View Settings

Language	English	
Lines Per Page	50	(20 - 1000)

7. Results

Close and reopen your browser, and go to the FortiGate admin login page. If you click on the lock icon next to the address bar, you should see that the certificate has been signed and verified by the FortiAuthenticator. As a result, no certificate errors will appear.



https://1.1.1.1/login

1.1.1.1

Secure Connection

Verified by: Ankh-Morpork