Issuing certificates with Microsoft Certificate Authority for use on FortiGate units

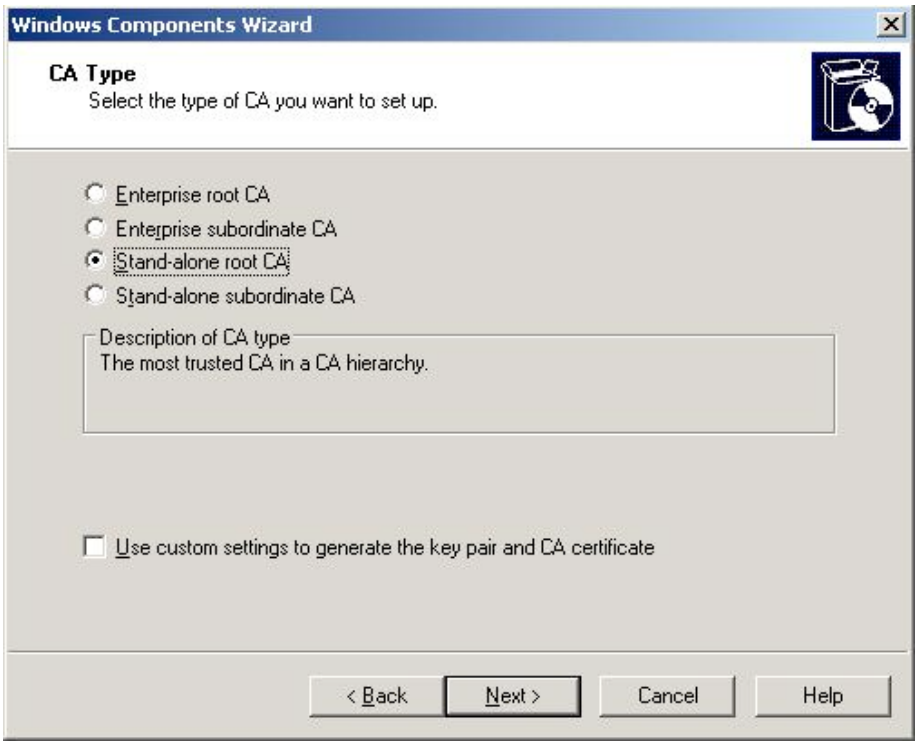
This article describes how to use a “stand-alone” Microsoft Certificate Authority (CA) to issue certificates for use on FortiGate units. Once the certificates have been installed on the FortiGate units, they can be used to establish an IPSec VPN tunnel between units.

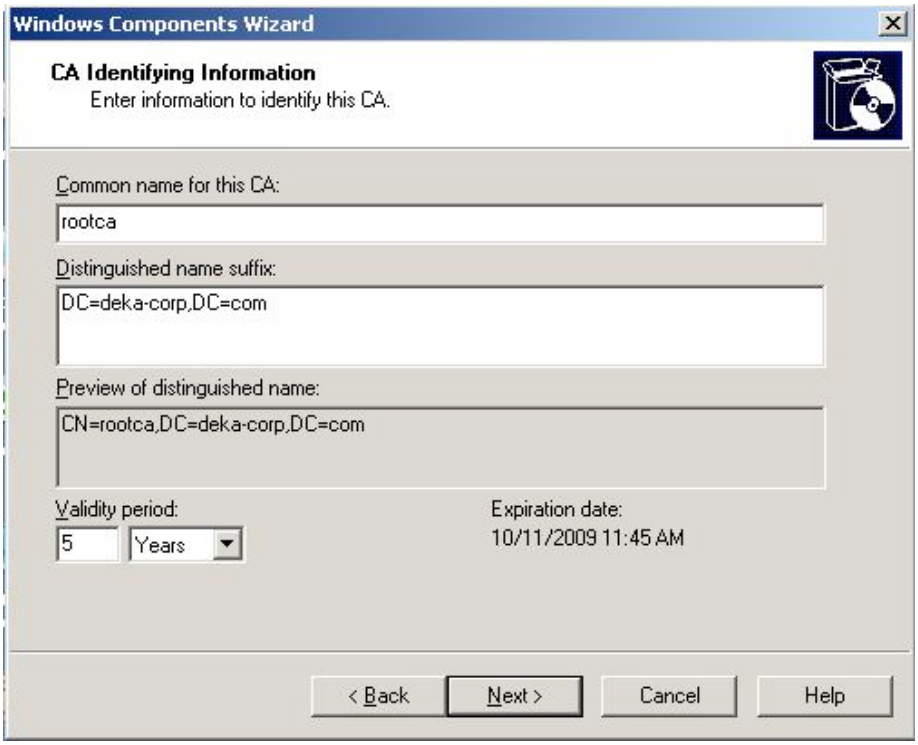
Microsoft CA Installation on Windows 2003 Server

There are two types of CA installations:

- “Enterprise” for Active Directory domain services. Some certificates are stored in AD.
- “Standalone” as a standard/generic type CA (this will be used for issuing FortiGate certificates).

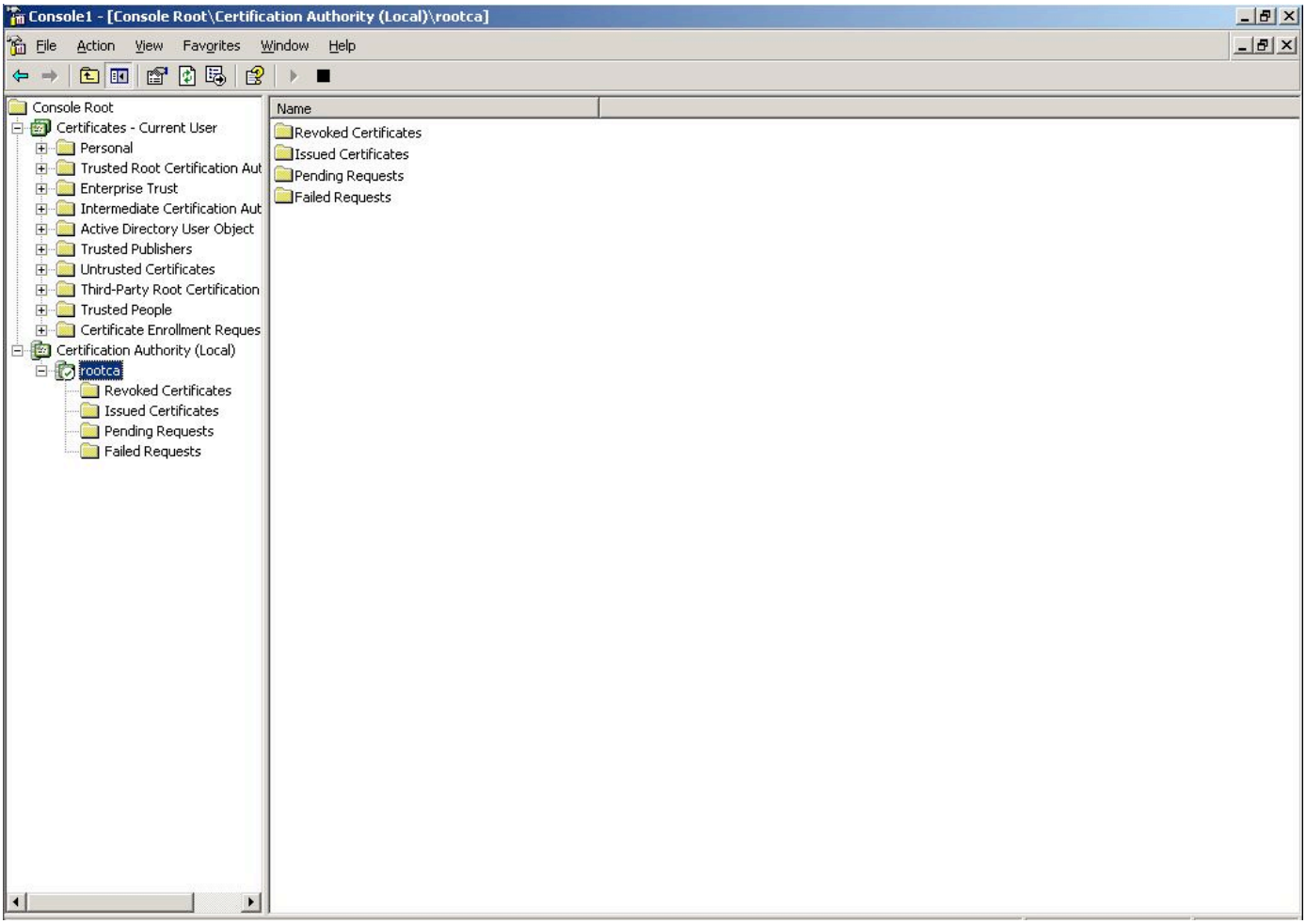
To install the CA, go to **Add/Remove Programs** > **Add/Remove Windows Components** > **Certificate Services**.





If IIS is installed, then a web based interface will be available to manage certificates upon installing the CA. Otherwise it is managed through a Microsoft Management Console (MMC).

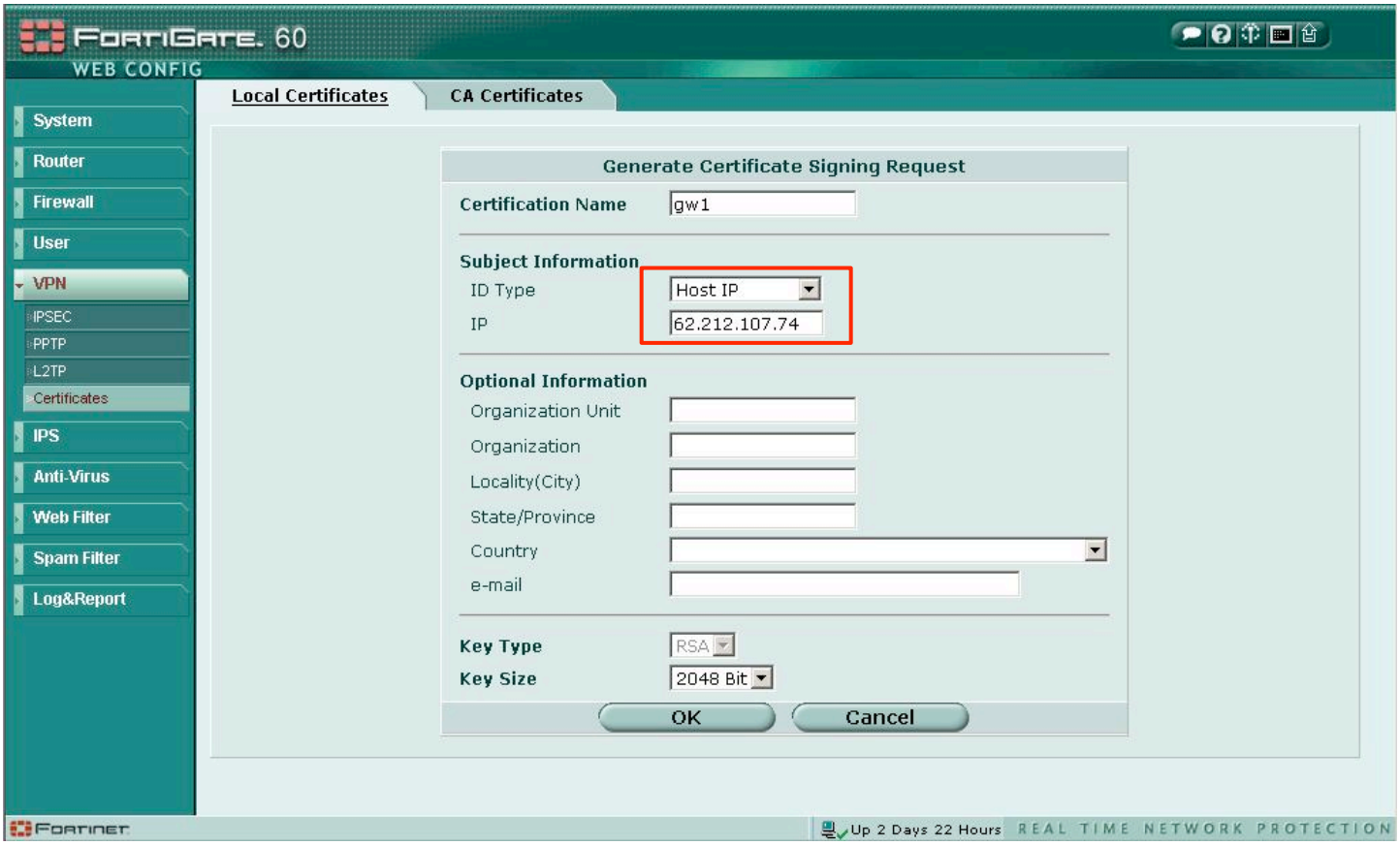
Managing the installed CA service with MMC and the 'Certificate Authority' snap-in module.



Exporting FortiGate certificate requests

In this example, two FortiGate units will use certificates to setup an IPSec VPN between them. The example below demonstrates the procedure performed on one FortiGate unit only. A similar procedure will have to be performed for the second unit.

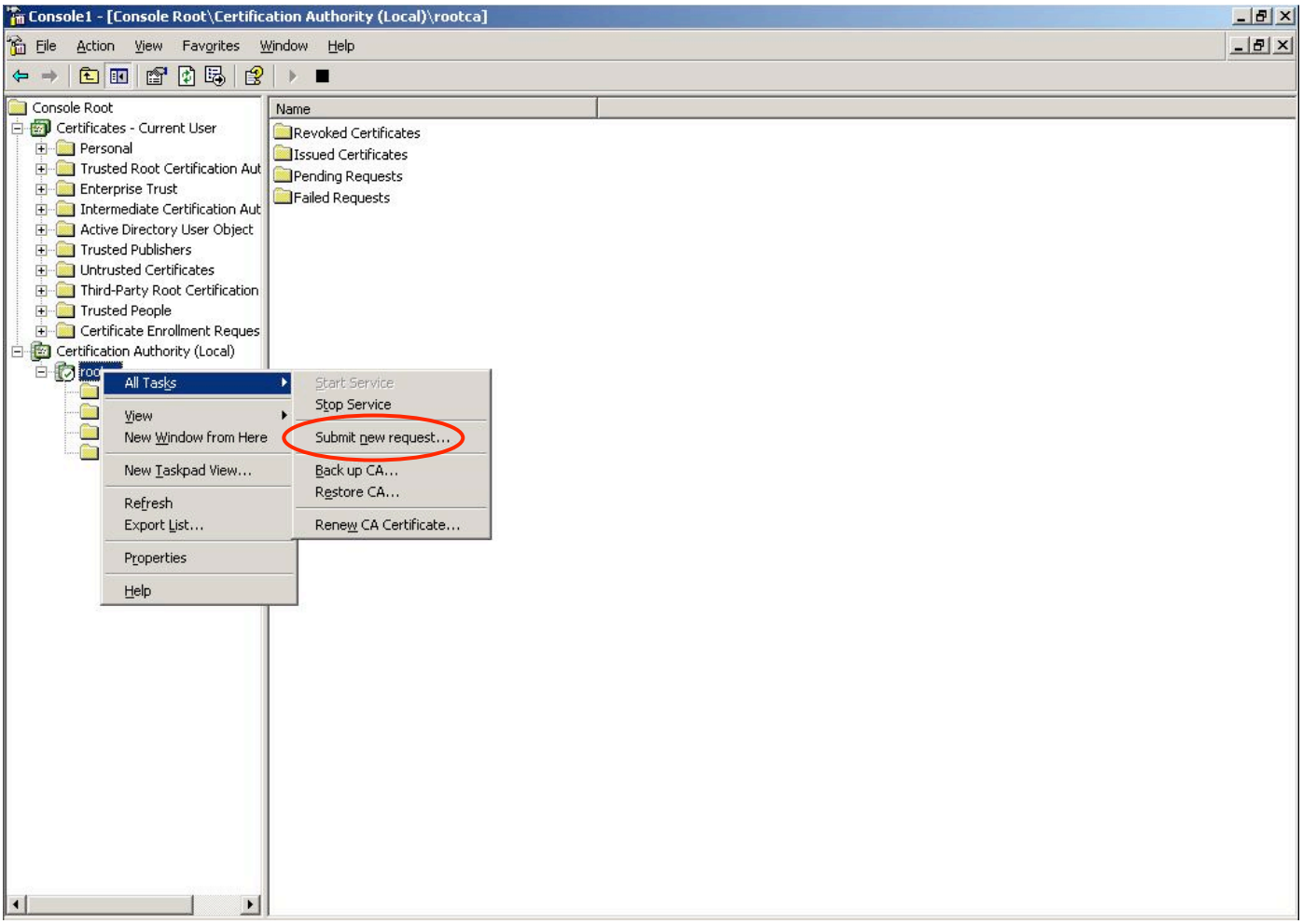
Generate a certificate request (i.e. a public key), to be signed by a CA. Enter an identifier for this certificate request. Here, the gateway's public IP address was used.



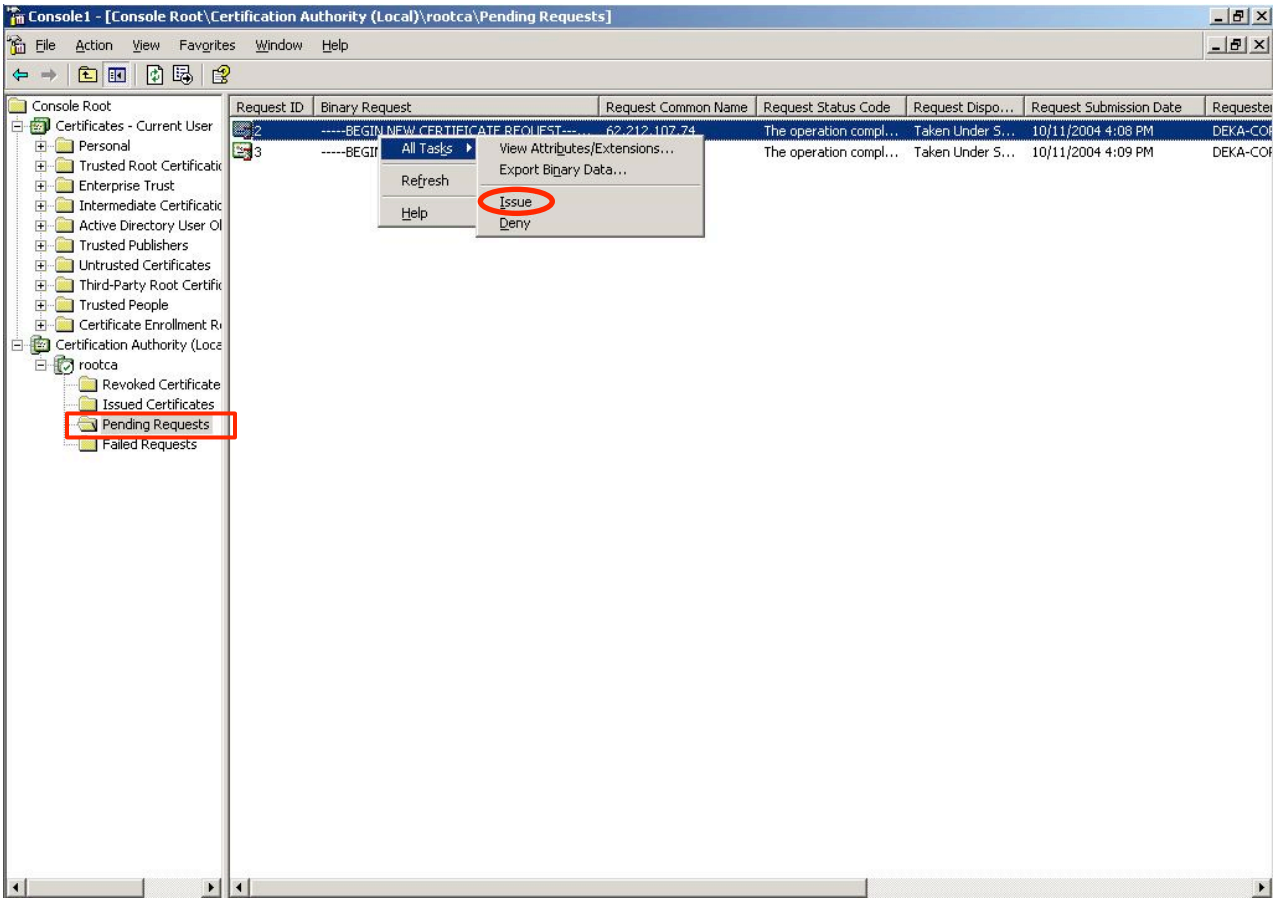
Certificate Request output example (filename is "gw1.csr"):


```
-----BEGIN CERTIFICATE REQUEST-----
MIICXDCCAUQCAQAwGTEXMBUGA1UEAxMONjIuMjEyLjEwOC4xODEwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC7AAlidX3rsEXEiQ2BKM/cIz1bWj3ZSQx1
HtDRzsvpgrAeWlcJvLG9wN1OYm3d+oyZoB+m6eMoWSeO9KNsjl1tyweIOwZDkdUY
P56Wt+SH/cIRAKB447kBhFBlkfFu4bpR39Ta7dusfLPMKoRbXOsWFOvaAu3eJ4k5
3qSbYf26AEvlCMQsXBazXydgiWQgswaPgPxL3afJ7vuDFaC6Zh2Qr7m2RACG0BRj
uLWVnymRMIkUTIXxmxBWymnx2PslFomm5HBJZl28uvLAA5gwYMdS1OfbiVRT+653
1jgha3X4ansWcFLKVDXDQkb0VDSLkYPM2GWeHt06gvkOcpoYD4xrAgMBAAEwDQYJ
KoZIhvcNAQEEBQADggEBAD2BfMsuG6fqYsPNxhf+R5WbKSV0C+Y/WPe524XM6SfW
vMt2jmj7YHFV7I/xpG/liyQx+x2X9pISkwECbfGYBLuewPNshD1rxB0hzlKioMF3
2KZfSvVb+DFzSLGfSF+/TYvidWOlmiIsgovibVc7oW3u2eXywhtWjHUHgQP3rL7p
fPuDff3zB/Ejx8T1X4DaC4Cl+DbPuCiwt0XmO5sAVOAfLRbyvOV/IrJhoIN0r2HI
2kDH+xfqJAJmb4bDERFJUjRMX4gKTdYVEs2LaEvOIkPffw4iSs2hVtvgdfWMWnH1
Ko+FaHdxLkv6POdSUYw9RUJyT9wB2U16/pqHky2tLLA=
-----END CERTIFICATE REQUEST-----
```

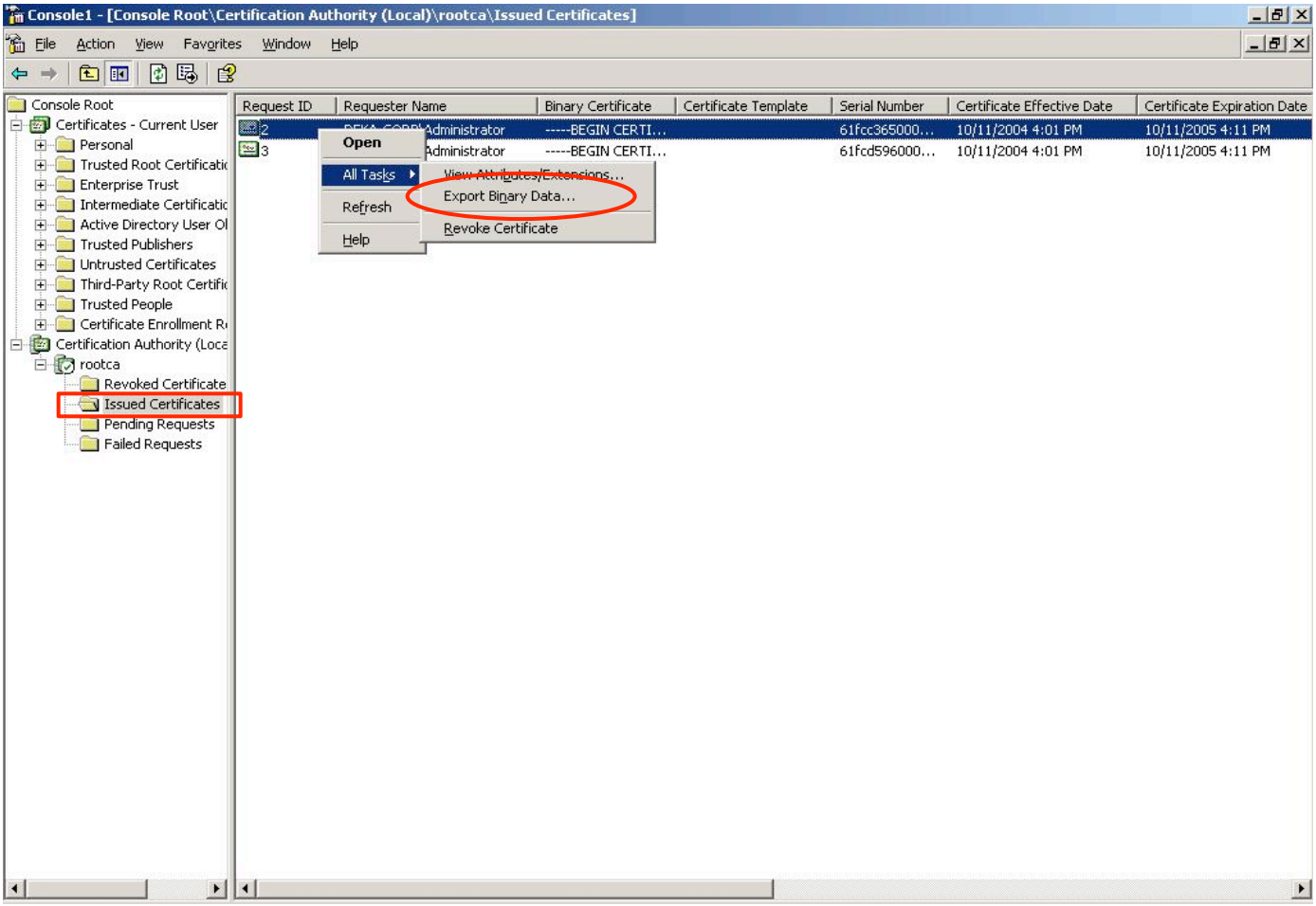
Submit the FortiGate unit's certificate request to the Microsoft CA for signing. During this procedure, the FortiGate unit's public key will be signed with the CA's private key.

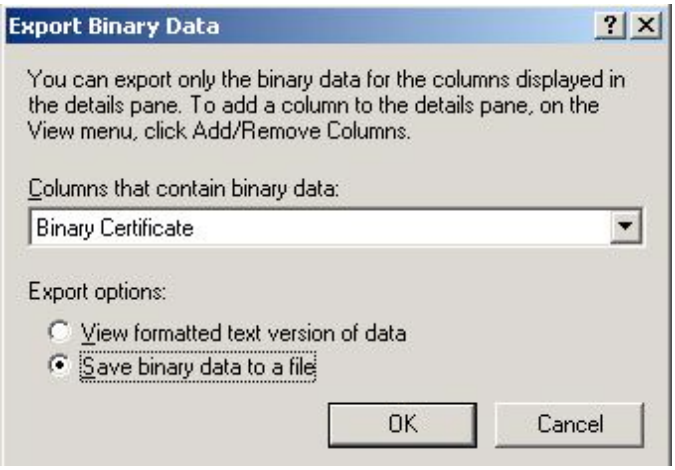


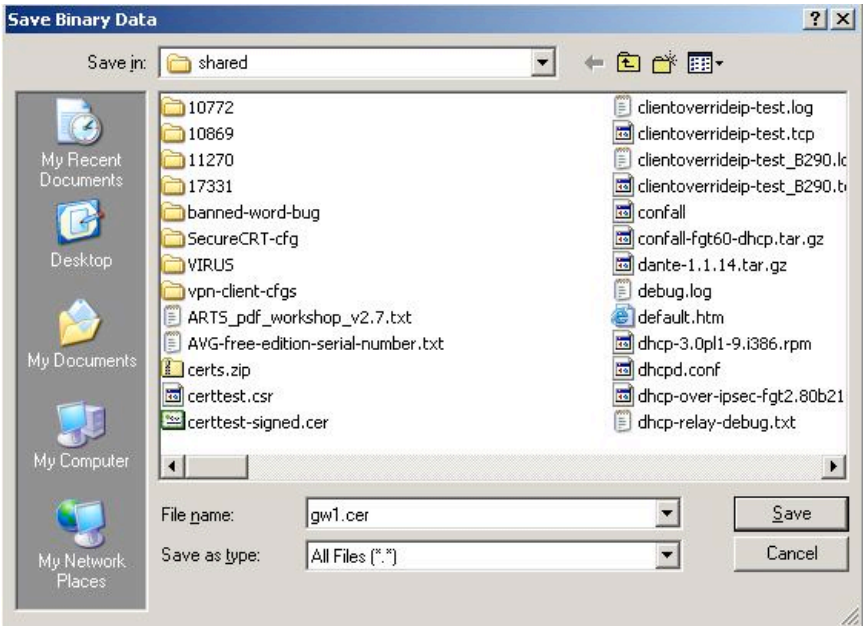
View the Pending Requests, and Issue (sign) the certificate request.



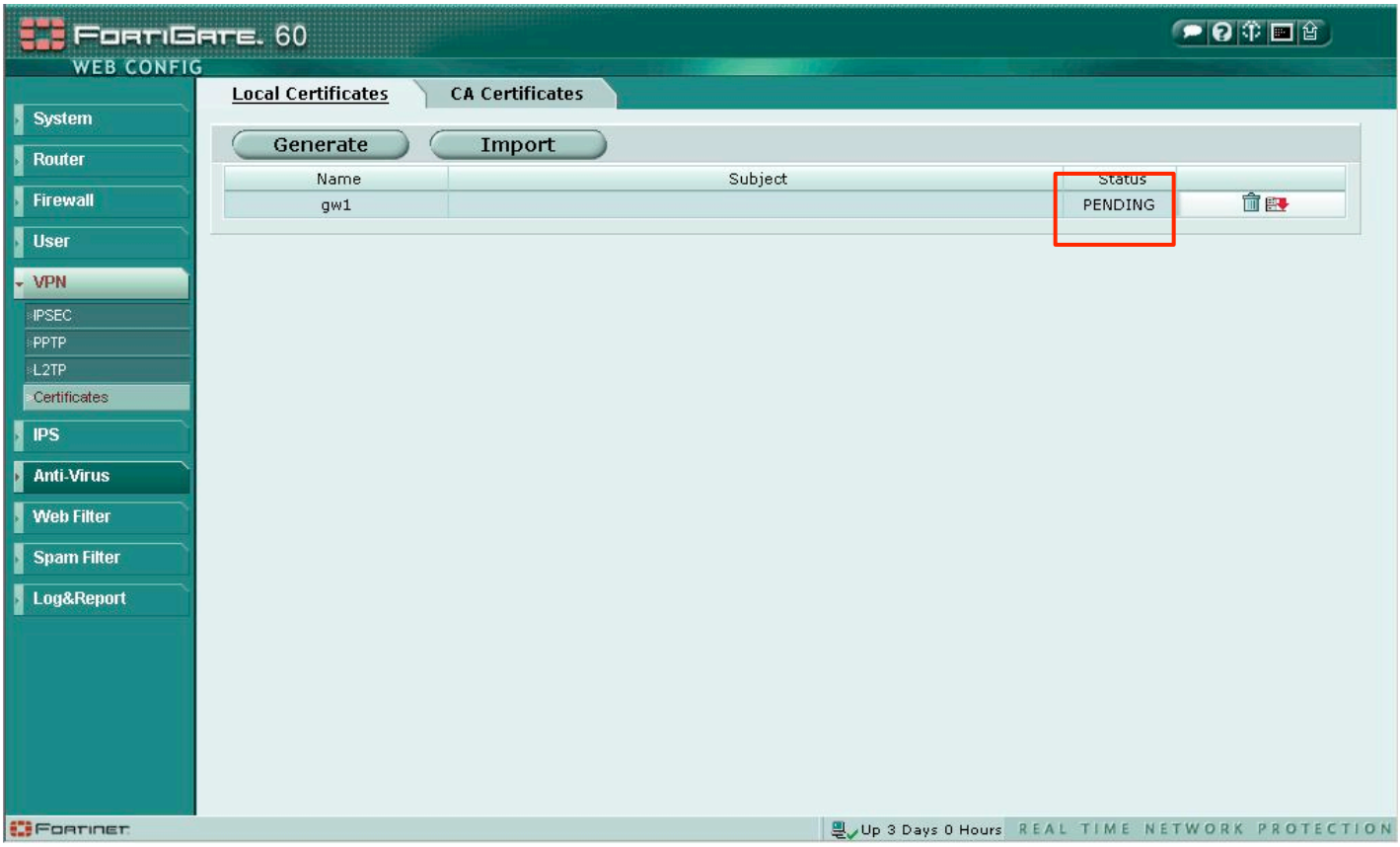
Once Issued, the certificate needs to be exported from the CA database, and imported back into the FortiGate unit.

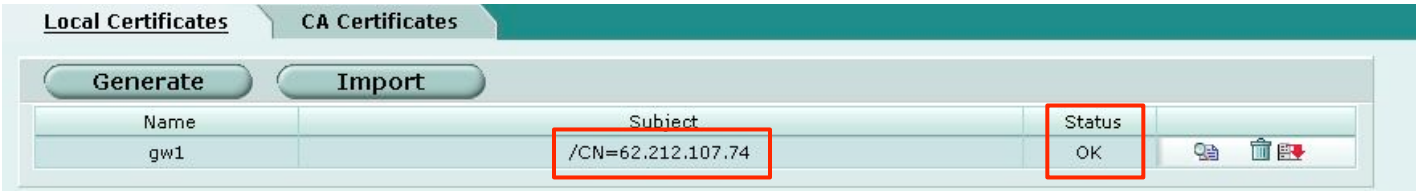

Console1 - [Console Root\Certification Authority (Local)\rootca\Issued Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Trusted Root Certificatio
Enterprise Trust
Intermediate Certificatio
Active Directory User Ol
Trusted Publishers
Untrusted Certificates
Third-Party Root Certific
Trusted People
Certificate Enrollment R
Certification Authority (Loca
rootca
Revoked Certificate
Issued Certificates
Pending Requests
Failed Requests
Request ID
Requester Name
Binary Certificate
Certificate Template
Serial Number
Certificate Effective Date
Certificate Expiration Date
2 Administrator -----BEGIN CERTI... 61fcc365000... 10/11/2004 4:01 PM 10/11/2005 4:11 PM
3 Administrator -----BEGIN CERTI... 61fcd596000... 10/11/2004 4:01 PM 10/11/2005 4:11 PM
Open
All Tasks
Refresh
Help
View Attributes/Extensions...
Export Binary Data...
Revoke Certificate


Export Binary Data
You can export only the binary data for the columns displayed in the details pane. To add a column to the details pane, on the View menu, click Add/Remove Columns.
Columns that contain binary data:
Binary Certificate
Export options:
View formatted text version of data
Save binary data to a file
OK
Cancel

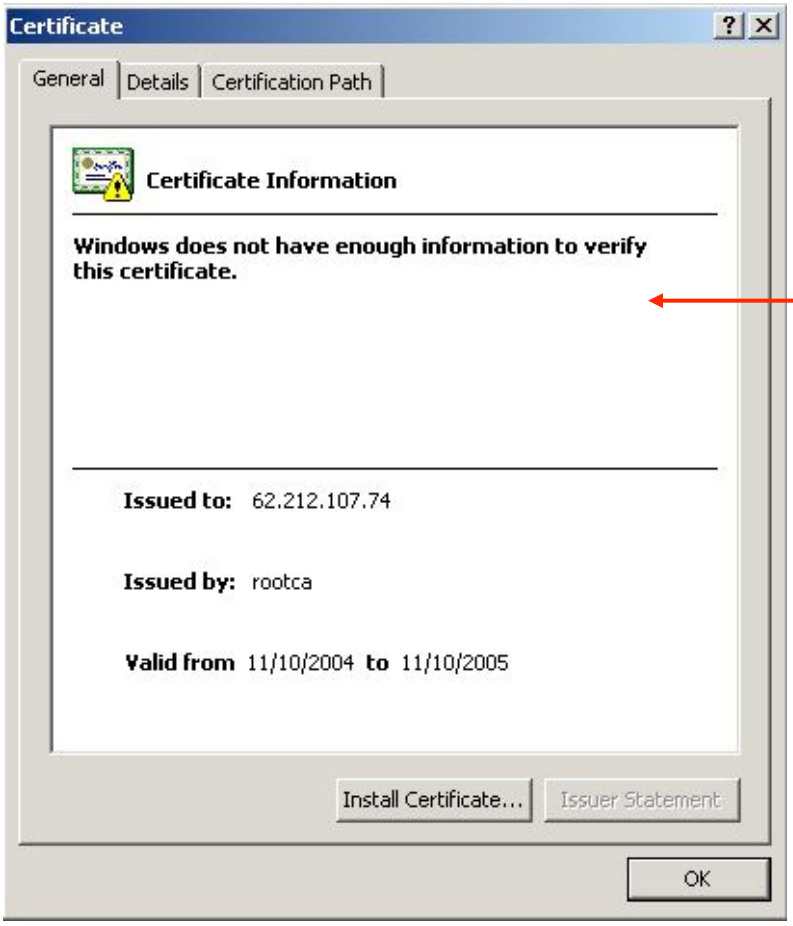


Each certificate (i.e. a signed certificate request), needs to be imported back into the respective FortiGate units. In the example below, the above-signed “gw1.csr” file (which becomes a “gw1.cer” file), gets imported back into the FortiGate unit.

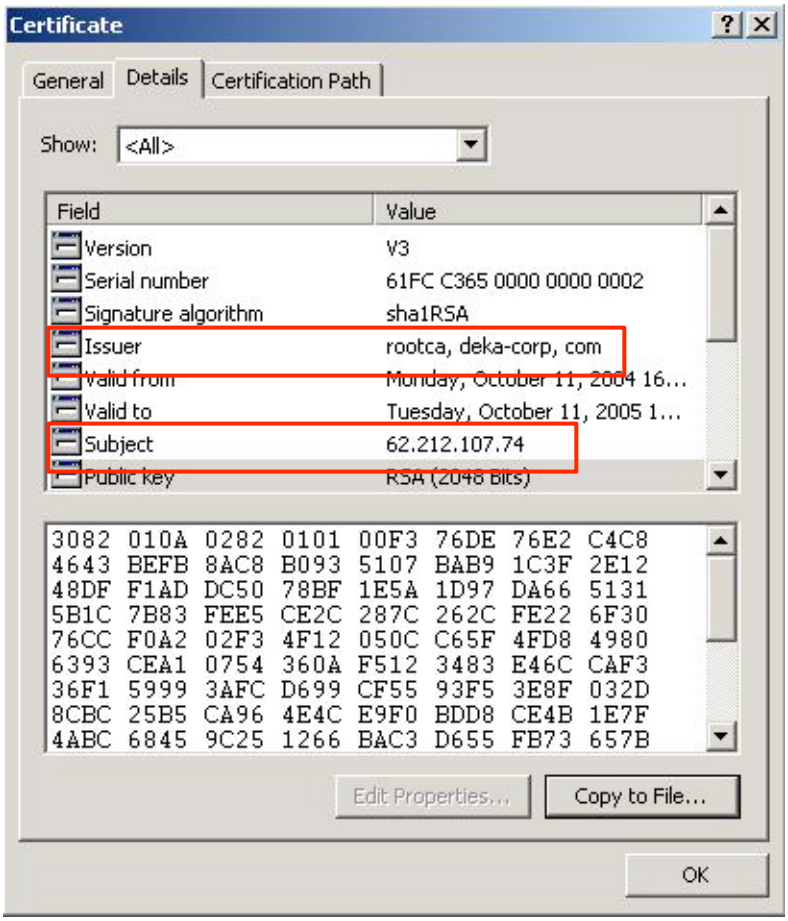




Note: Clicking on the certificate .cer file (on a different PC that does not have the root certificate installed) opens the following dialog box:



This message is due to the fact that the Root certificate is not installed.



The CA's certificate (i.e. the CA's self-signed public key), must now be imported into each Fortigate device. To export the root certificate, select it in the MMC Certification Authority (Local) snap-in, and right-click its Properties.

Viewing the installed root certificate on the CA host, using a mmc snap-in:

Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]

File Action View Favorites Window Help

- Console Root
  - Certificates - Current User
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Active Directory User Object
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authoritie
    - Trusted People
    - Certificate Enrollment Requests
  - Certification Authority (Local)
    - rootca
      - Revoked Certificates
      - Issued Certificates
      - Pending Requests
      - Failed Requests

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
FESTE, Public Notary Certs	FESTE, Public Notary Certs	1/1/2020	Secure Email, Server...	FESTE, Public Notary...
FESTE, Verified Certs	FESTE, Verified Certs	1/1/2020	Secure Email, Server...	FESTE, Verified Certs
First Data Digital Certificates Inc. ...	First Data Digital Certificates Inc. Ce...	7/3/2019	Server Authenticatio...	First Data Digital Cer...
FNMT Clase 2 CA	FNMT Clase 2 CA	3/18/2019	Secure Email, Server...	Fabrica Nacional de ...
GlobalSign Root CA	GlobalSign Root CA	1/28/2014	Secure Email, Server...	GlobalSign Root CA
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/14/2018	Secure Email, Client ...	GTE CyberTrust Glob...
GTE CyberTrust Root	GTE CyberTrust Root	4/4/2004	Secure Email, Client ...	GTE CyberTrust Root
GTE CyberTrust Root	GTE CyberTrust Root	2/24/2006	Secure Email, Client ...	GTE CyberTrust Root
http://www.valicert.com/	http://www.valicert.com/	6/26/2019	Secure Email, Server...	ValiCert Class 1 Polic...
http://www.valicert.com/	http://www.valicert.com/	6/26/2019	Secure Email, Server...	ValiCert Class 3 Polic...
http://www.valicert.com/	http://www.valicert.com/	6/26/2019	Secure Email, Server...	ValiCert Class 2 Polic...
IPS SERVIDORES	IPS SERVIDORES	12/30/2009	Secure Email, Server...	IPS SERVIDORES
Microsoft Authenticode(tm) Root ...	Microsoft Authenticode(tm) Root Au...	1/1/2000	Secure Email, Code S...	Microsoft Authentico...
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Auth...
Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	5/10/2021	<All>	Microsoft Root Certif...
NetLock Expressz (Class C) Tanusi...	NetLock Expressz (Class C) Tanusitv...	2/20/2019	Server Authenticatio...	NetLock Expressz (Cl...
NetLock Kozjegyzoi (Class A) Tanu...	NetLock Kozjegyzoi (Class A) Tanusit...	2/20/2019	Server Authenticatio...	NetLock Kozjegyzoi (...
NetLock Uzleti (Class B) Tanusitva...	NetLock Uzleti (Class B) Tanusitvany...	2/20/2019	Server Authenticatio...	NetLock Uzleti (Class...
NO LIABILITY ACCEPTED, (c)97 V...	NO LIABILITY ACCEPTED, (c)97 Veri...	1/8/2004	Time Stamping	VeriSign Time Stampi...
PTT Post Root CA	PTT Post Root CA	6/26/2019	Secure Email, Server...	KeyMail PTT Post Ro...
rootca	rootca	10/11/2009	<All>	<None>
Saunalahden Serveri CA	Saunalahden Serveri CA	6/26/2019	Secure Email, Server...	Saunalahden Serveri...
Saunalahden Serveri CA	Saunalahden Serveri CA	6/26/2019	Secure Email, Server...	Saunalahden Serveri...
Secure Server Certification Authority	Secure Server Certification Authority	1/8/2010	Server Authentication	VeriSign/RSA Secure ...
SecureNet CA Class A	SecureNet CA Class A	10/16/2009	Secure Email, Server...	SecureNet CA Class A
SecureNet CA Class B	SecureNet CA Class B	10/16/2009	Secure Email, Server...	SecureNet CA Class B
SecureNet CA Root	SecureNet CA Root	10/16/2010	Secure Email, Server...	SecureNet CA Root
SecureNet CA SGC Root	SecureNet CA SGC Root	10/16/2009	Secure Email, Server...	SecureNet CA SGC R...
SecureSign RootCA1	SecureSign RootCA1	9/15/2020	Secure Email, Server...	Japan Certification S...
SecureSign RootCA2	SecureSign RootCA2	9/15/2020	Secure Email, Server...	Japan Certification S...
SecureSign RootCA3	SecureSign RootCA3	9/15/2020	Secure Email, Server...	Japan Certification S...
SERVICIOS DE CERTIFICACION - ...	SERVICIOS DE CERTIFICACION - A....	3/9/2009	Secure Email, Server...	SERVICIOS DE CERT...
SIA Secure Client CA	SIA Secure Client CA	7/9/2019	Secure Email, Server...	Societa Interbancari...
SIA Secure Server CA	SIA Secure Server CA	7/9/2019	Secure Email, Server...	Societa Interbancari...
TC TrustCenter Class 1 CA	TC TrustCenter Class 1 CA	1/1/2011	Secure Email, Server...	TC TrustCenter Clas...
TC TrustCenter Class 2 CA	TC TrustCenter Class 2 CA	1/1/2011	Secure Email, Server...	TC TrustCenter Clas...

rootca Properties

Certificate Managers Restrictions | Auditing | Security

General | Policy Module | Exit Module | Extensions | Storage

Certification authority (CA)

Name: rootca

CA certificates:

Certificate #0

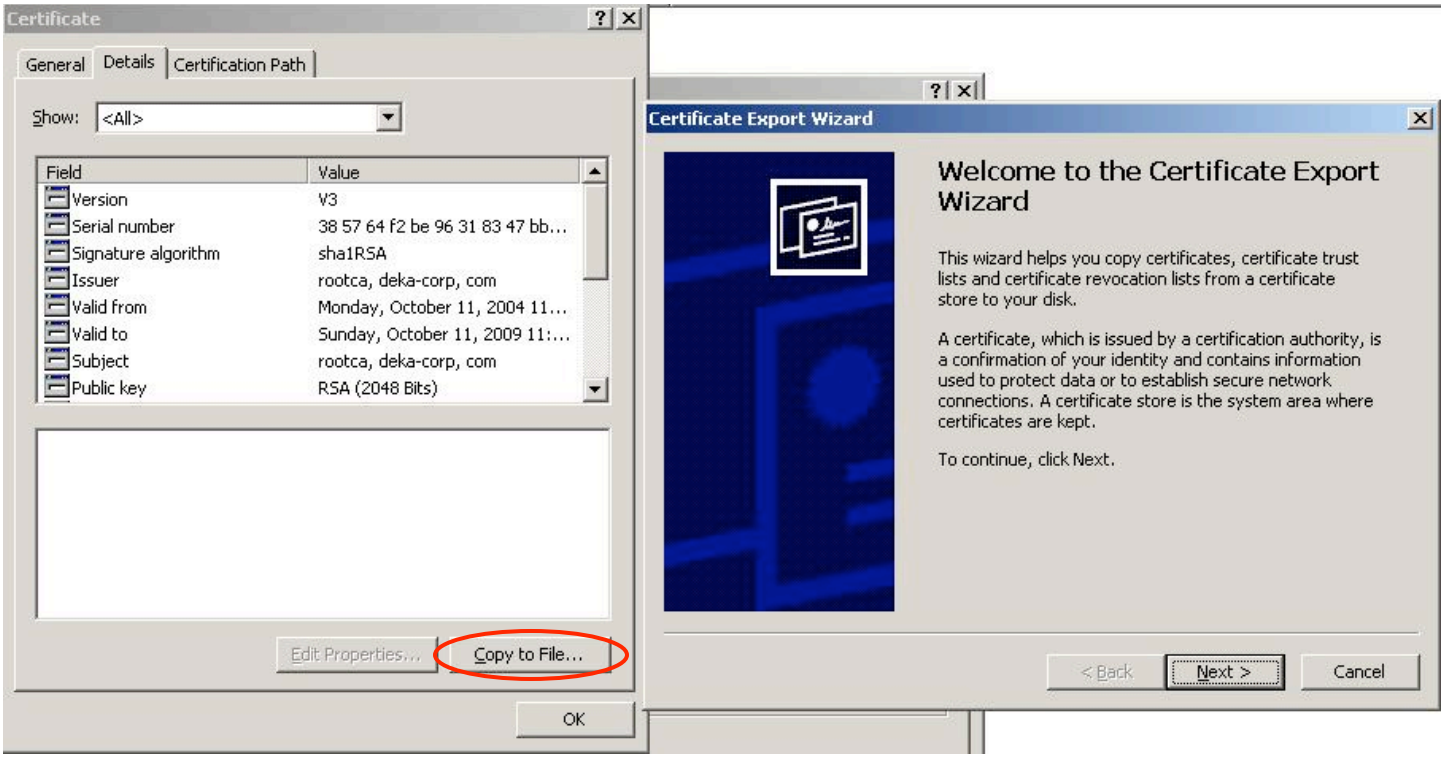
View Certificate

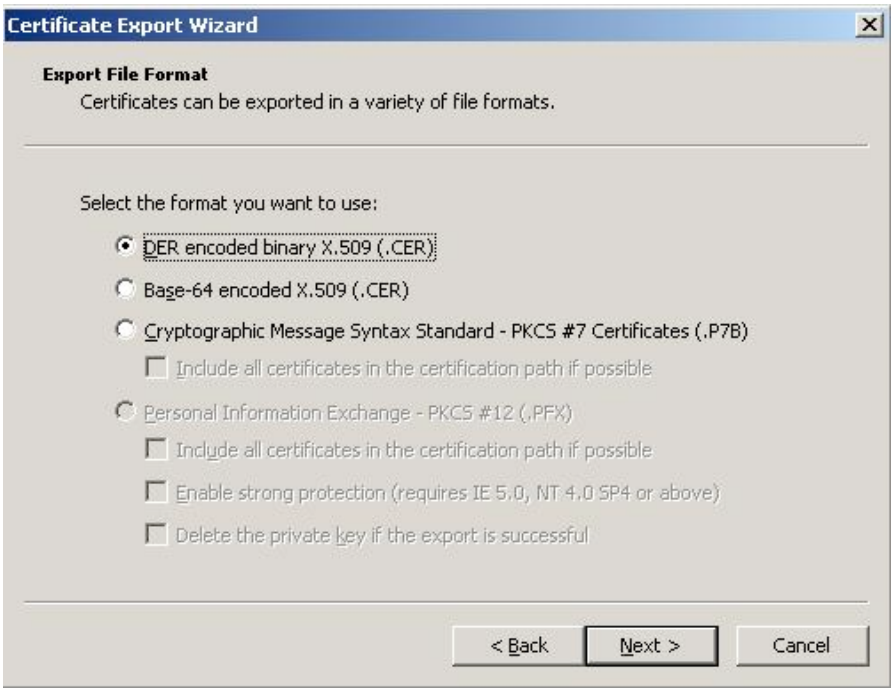
Cryptographic settings

CSP: Microsoft Strong Cryptographic Provider

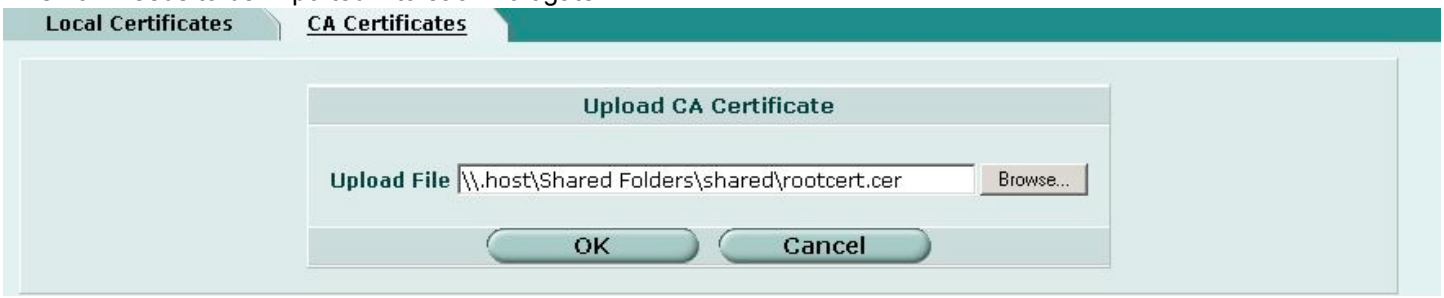
Hash algorithm: SHA-1

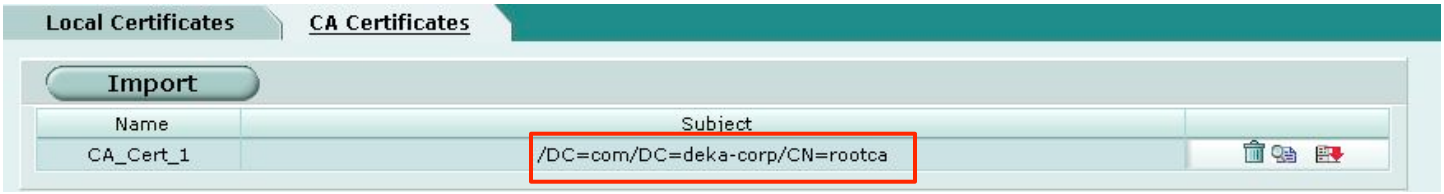
OK | Cancel | Apply





This now needs to be imported into each Fortigate.





The FortiGate units are ready to use certificates to setup an IPSec tunnel between them. For further details, see the *FortiGate VPN Guide* and *Administration Guide* as well as as the following Fortinet Knowledge Center articles:

- http://kc.forticare.com/default.asp?id=422&Lang=1
- http://kc.forticare.com/default.asp?id=730&Lang=1

Note: Viewing (clicking on) the Root CA .cer file on a PC that has not generated the certificate, will result in the following message:

Once installed, it will present the following:

Note: Re-viewing the gw1.cer on the PC with the root CA certificate installed, results in a proper verification and recognition of the certificate: