

ENGAGE BLACK

Black●Vault CA

WatchGuard Integration Guide

VPN Certificate

December 11, 2017

© Engage Black
9565 Soquel Drive
Aptos, CA 95003
Phone +1 831.688.1021
1 877.ENGAGE4 (364.2434)
sales@engageblack.com
support@engageblack.com

About This Guide

Guide Type

Documented Integration — WatchGuard or a Technology Partner has provided documentation demonstrating integration

Guide Details

WatchGuard provides integration instructions to help our customers configure WatchGuard products to work with products created by other organizations. If you need more information or technical support about how to configure a third-party product, see the documentation and support resources for that product.

This guide describes the Black Vault Certificate Authority (CA) and the procedures to install, use, and troubleshoot the appliance.

Audience

This guide is for security professionals with knowledge of networking and basic security who configure and install the appliance, generate certificates, or monitor logs.

Purpose

The purpose of this guide is to explain how to configure, manage, and troubleshoot the Black Vault CA. This guide contains conceptual and reference information related to the procedures necessary to correctly operate this appliance.

Conventions

The Black Vault CA is configured and administered through a command line interface (CLI). The description of CLI commands follows these syntax conventions:

Curly brackets {} indicate required arguments.

A pipe symbol | indicates valid options for a command word or argument.

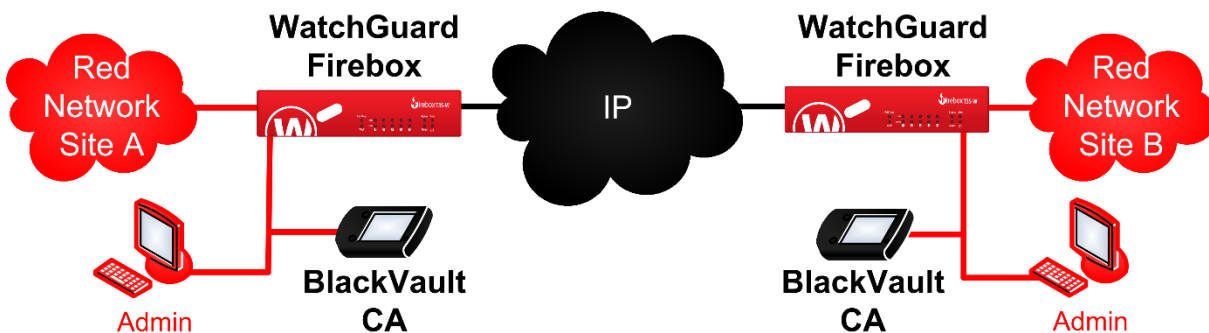
Windows sequences are shown as follows: Settings > Network Configuration

Introduction

VPNs are ubiquitous in enterprise networks. However, in today’s age they are getting less and less secure. The most common method of authentication between two endpoints is through a pre-shared key, which can be guessed, or figured out through social engineering. The more secure way to authenticate is through x.509 certificates, this is only more secure though, if the Certificate Authority you obtained your certificates from is secure. The BlackVault CA is a CA with an integrated Hardware Security Module (HSM) that ensures both maximum security and operational simplicity.



The BlackVault CA can safely protect your VPN by providing a reliable and secure source of authentication for the two endpoints of your VPN. It is easy to setup and use Certificate Authority that is simple to weave into your existing WatchGuard VPN, or a brand-new VPN.



To setup the Firebox to use certificates from the BlackVault CA, the following procedures must be accomplished:

- Create a CSR on both Fireboxes.
- Have the BlackVault CA sign the certificates.
- Import the Chain of Trust into the Fireboxes at both ends.
- Import the certificate into the Fireboxes at both ends.
- Configure the Gateway of the Fireboxes at both ends.
- Configure the Tunnel of the Fireboxes at both ends.

This Guide will walk through all the necessary steps to set up a VPN

WatchGuard Web UI Instructions

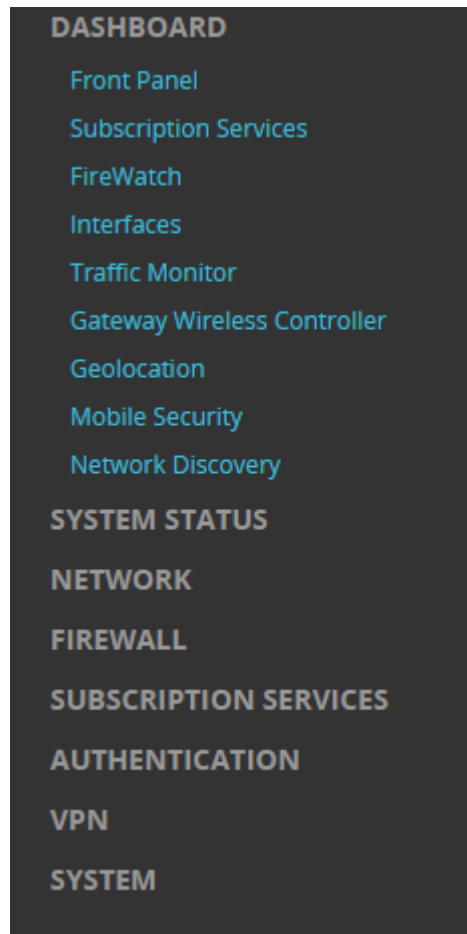
Setting Up Certificates

The first part of this guide is configuring the certificates that will be used in the VPNs

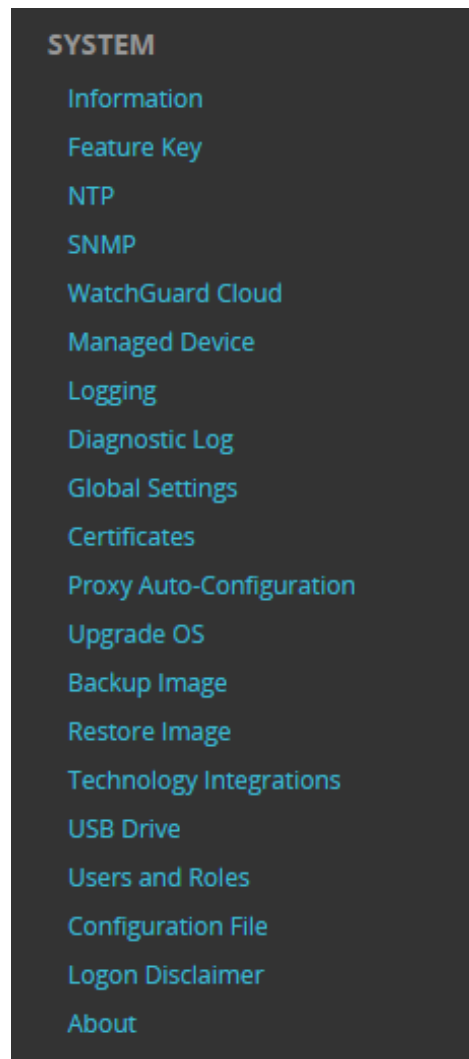
Site A

Creating A CSR

1. Log into the website of the site A's Firebox.
2. In the left-hand side of the page select "System".



3. In the drop-down menu select "Certificates".



4. In the Certificates web page click "Create Request".

Certificates



Show Trusted CAs for Proxies

5. The Certificate Request Wizard will open. Click “Next” to continue.

[Certificates](#) / [Create Request](#)

Welcome to the Certificate Request Wizard



To create a third-party CSR (certificate signing request) for this device, complete the steps in this wizard.

6. On the Choose the certificate Function page, select IPSec, Web Server, Other. Then click “Next” to continue.

[Certificates](#) / [Create Request](#)

Choose the Certificate Function

- Proxy Authority (re-signing CA certificate for outbound SSL/TLS content inspection)
- Proxy Server (server certificate for inbound SSL/TLS content inspection)
- IPSec, Web Server, Other

7. On the next page, fill out the details for the Subject Name, then click “Next” to continue.

[Certificates](#) / [Create Request](#)

Specify Details for the Subject Name

Name (CN)	<input type="text"/>	<i>(required)</i>
Department Name (OU)	<input type="text"/>	
Company Name (O)	<input type="text"/>	<i>(required)</i>
City/Location (L)	<input type="text"/>	
State/Province (ST)	<input type="text"/>	
Country (C)	<input type="text" value="US"/>	<i>(required)</i>

8. On the following page, fill out the Domain Information, then click “Next” to continue.

[Certificates](#) / [Create Request](#)

Specify Domain Information

Subject Name	<input type="text" value="CN=Testing, OU=Demo, O=Acme, L=Smallville, ST"/>	<i>(required)</i>
DNS Name	<input type="text" value="192.168.1.42"/>	<i>(required)</i>
IP Address	<input type="text"/>	
User Domain Name	<input type="text" value="admin@domain.com"/>	

- On the Next page select the Algorithm, Length, and Key Usage, then click “Next” to continue

Certificates / Create Request

Select the Algorithm, Length, and Key Usage

Algorithm	<input checked="" type="radio"/> RSA	<input type="radio"/> DSA	
Length	<input type="radio"/> 1024	<input checked="" type="radio"/> 2048	
Key Usage	<input type="radio"/> Encryption	<input type="radio"/> Signature	<input checked="" type="radio"/> Both

When you click **Next**, your CSR (Certificate Signing Request) will be generated.

- On the final Page, it will display the Certificate Signing Request. Copy it all to a notepad and save it. v

Certificate Request Wizard Completed

```
-----BEGIN CERTIFICATE REQUEST-----
MI IDEDCCAfgCAQAwYzELMAkGA1UEBhMCVVMxZDzANBgNVBAgTBkthbnNhc zETMBEG
A1UEBxMKU21hbGx2aWxsZTENMA sGA1UEChMEQWNTZT ENMA sGA1UECxMERGVtbzEQ
MA4GA1UEAxMHVGVzdGluZzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCA QoCggEB
AJvUH01ek14N9seCT0mTWS1vQYQxoyVe2eMiwyuLV91qvFPiOVH5xRCe t1kppwZ
Lc6eIJFS0cU2q57PK+mKXaVrnPMq3VKCbPA/w8XriVEmfVJK31SgGEu9mk5xHuQF
vr7fberSktizbp4T/MSedvZetDFvJDylVLyXy4oSWgoVOIgzC4nG11tnmX1KBgeJ
P0qGYiYmbiBnoXMLwU2gxjn2EyGoocp/H0fG57P+6zAVSs/Wdzdu4Tb+PYfzry0g2
7AaWTosL3ArhwLmnAsTi78+nnxzpoSeg5XPJWhHAqWA2Gsl0ibkyrP1Eir5iBm2r
b+FQezuZi3bXJNgpmci jri8CAwEAAaBoMGYGC SgGS Ib3DQEJDjFZMFcwKQYDVROR
BCIwIIIMMTkyLjE2OC4xLjQyqRBh2G1pbk Bkb21haW4uY29tMAsGA1UdDwQEAwIF
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUIAgIwDQYJKoZIhvcNAQELBQAD
ggEBAAYBXNCdx/73J+W9zyxnYYC7iD11csUBB3yBH61mekQHmNexVHqEzo3o8S
04bId26MYWNbjmRxtPTxMIx9EyrTiVOXs2GaJtFvaPtpuyf6yr/QIC5dpm0MM4kZ
jg9LfnWCzk06SooNgHJE1j1Aer2vvs0JOPMGV07iCIL3hCnpO/OxbRfE3CeolCS7
njyQtCVC3dqDDHbIOYhok23GbcELPVq+QVhA5UIFIFHOeX3RmD93r5y2Nw1Xmv7F
hC1aBcBpB0v470vRa iJbbigjX/eqNNLzre+4uncupqnipL6NkJE6Tcyfn3KtYW4g
UiwW8HutxlpK0k+uH+47p9XA2Y=
-----END CERTIFICATE REQUEST-----
```

To generate a signed certificate, copy the text of this Certificate Signing Request and provide it to your Certificate Authority.

After you have submitted the Certificate Signing Request to the Certificate Authority and have received the signed certificate, you can import the certificate to your device. Make sure the CA certificate is also imported. To import a signed certificate now, click **Finish & Import**.

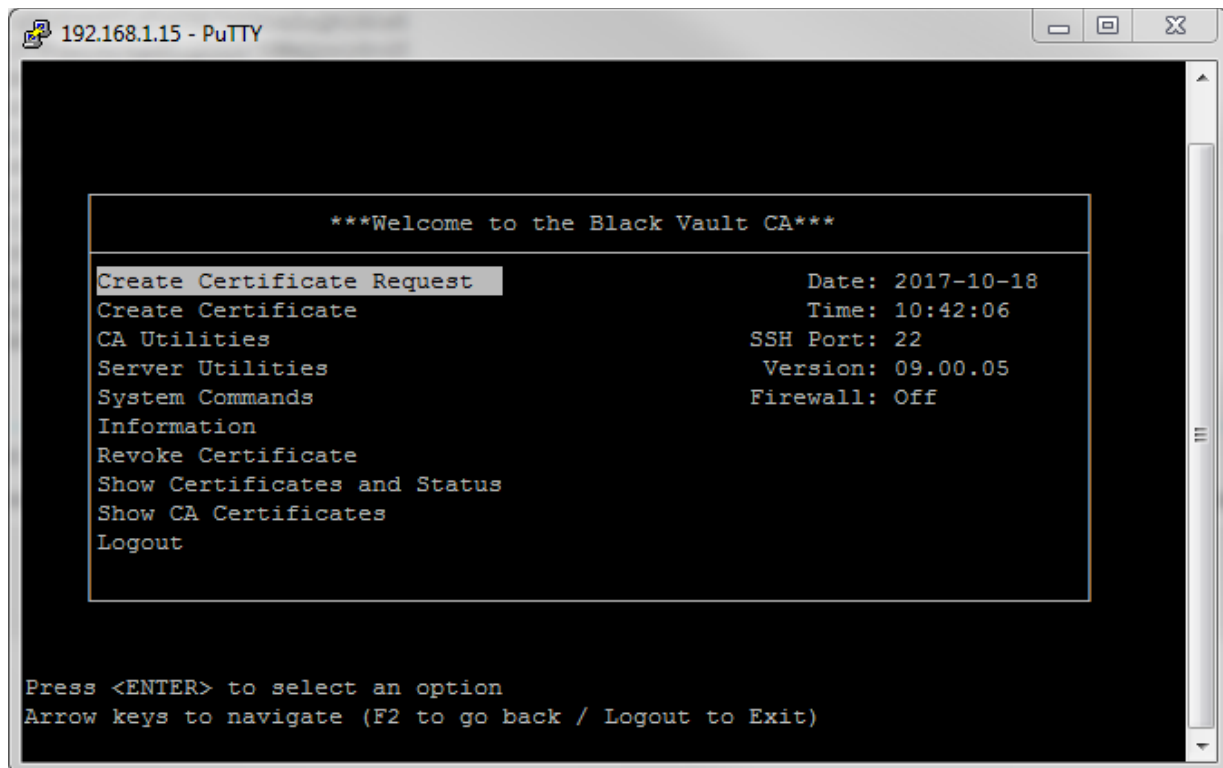
FINISH

FINISH & IMPORT

11. You have successfully completed creating a Certificate Signing Request.

Signing your CSR

1. Log into the BlackVault CA.
2. Select CA Utilities.



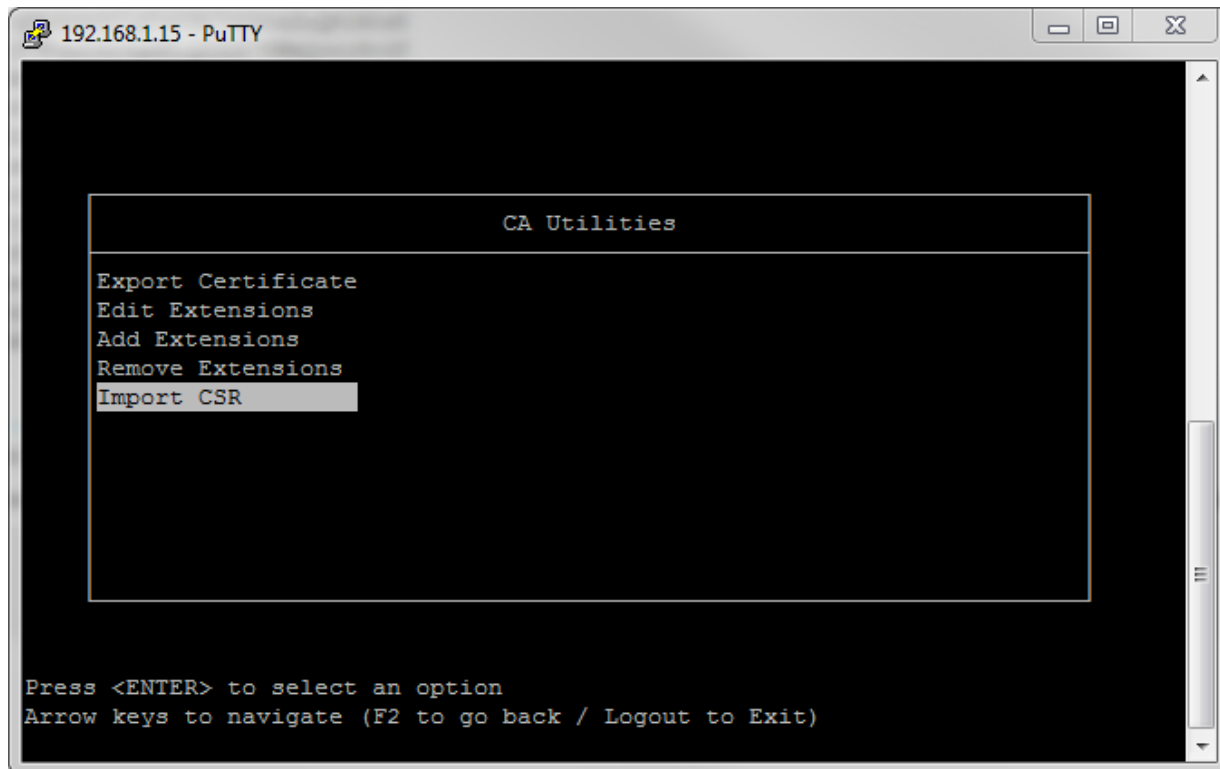
The screenshot shows a PuTTY terminal window titled "192.168.1.15 - PuTTY". The terminal displays a menu for the Black Vault CA. At the top, it says "***Welcome to the Black Vault CA***". Below this, there is a list of options: "Create Certificate Request" (highlighted), "Create Certificate", "CA Utilities", "Server Utilities", "System Commands", "Information", "Revoke Certificate", "Show Certificates and Status", "Show CA Certificates", and "Logout". To the right of these options, there is a column of status information: "Date: 2017-10-18", "Time: 10:42:06", "SSH Port: 22", "Version: 09.00.05", and "Firewall: Off". At the bottom of the terminal, there is a prompt: "Press <ENTER> to select an option" and "Arrow keys to navigate (F2 to go back / Logout to Exit)".

```
***Welcome to the Black Vault CA***

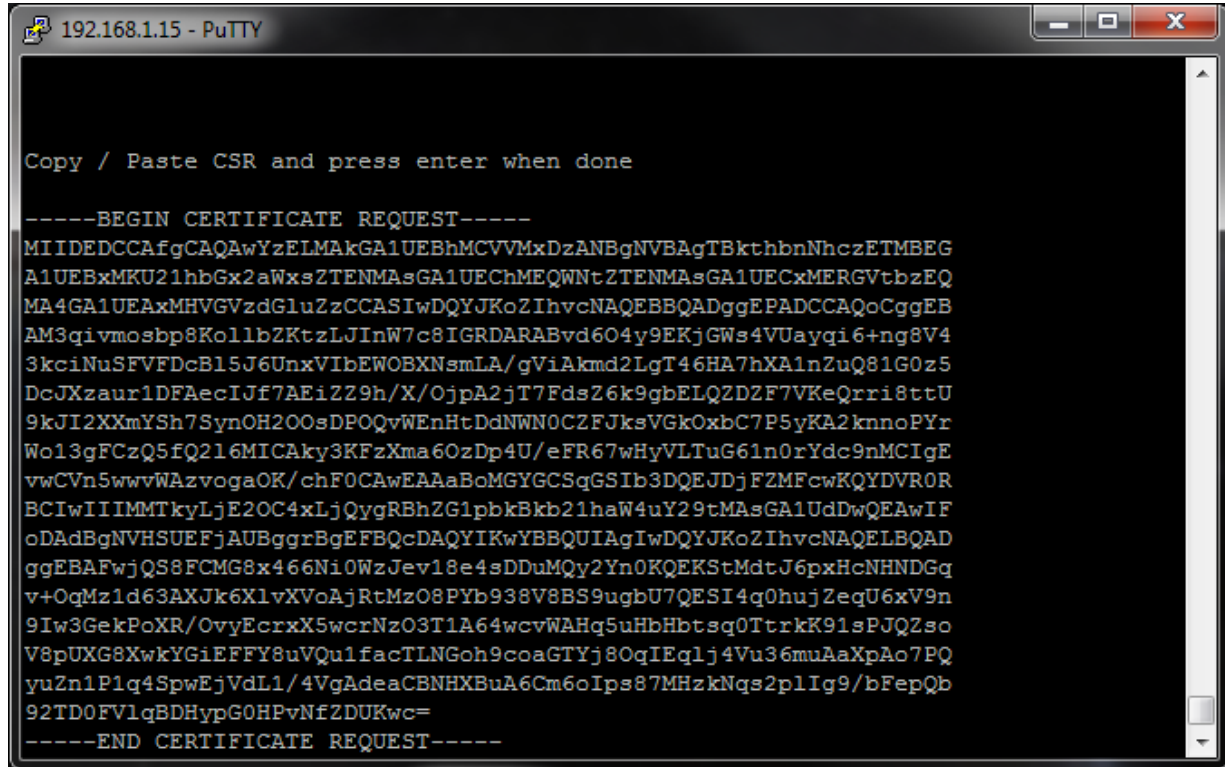
Create Certificate Request      Date: 2017-10-18
Create Certificate             Time: 10:42:06
CA Utilities                   SSH Port: 22
Server Utilities              Version: 09.00.05
System Commands               Firewall: Off
Information
Revoke Certificate
Show Certificates and Status
Show CA Certificates
Logout

Press <ENTER> to select an option
Arrow keys to navigate (F2 to go back / Logout to Exit)
```

3. Select Import CSR



4. Paste in the CSR that you just created.

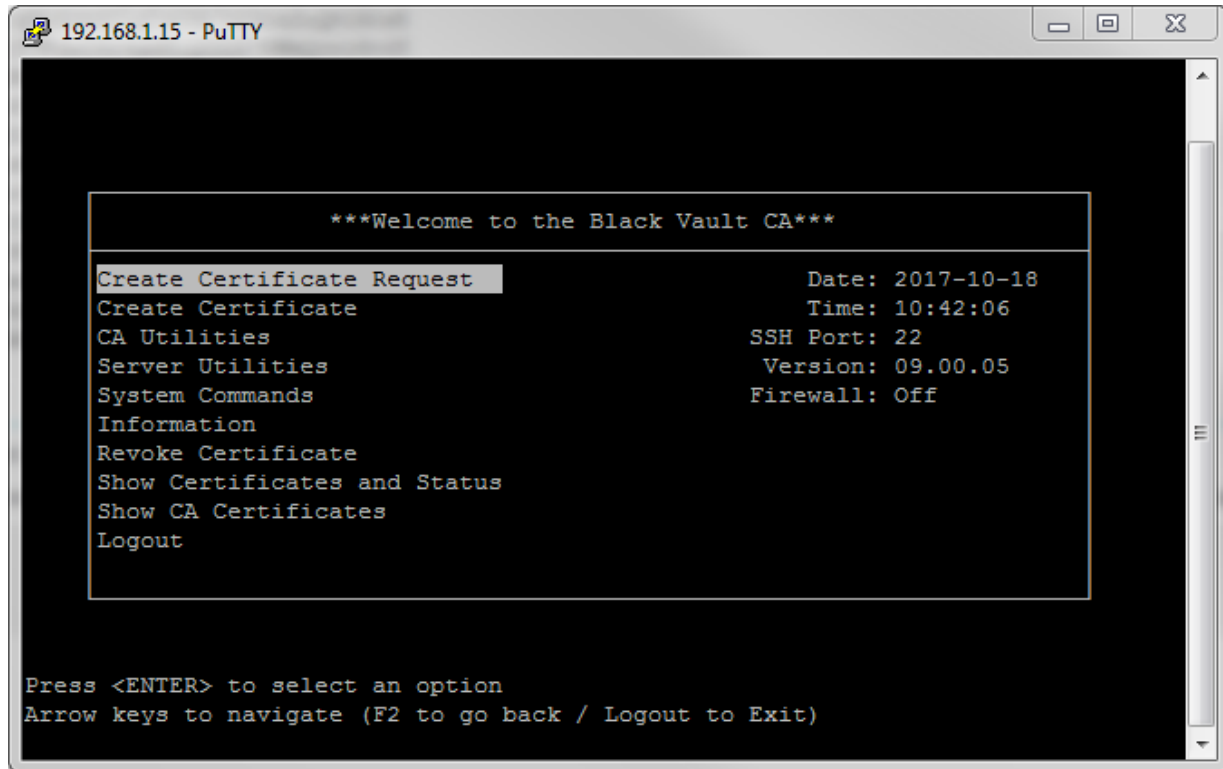


```
192.168.1.15 - PuTTY

Copy / Paste CSR and press enter when done

-----BEGIN CERTIFICATE REQUEST-----
MIIDEDCCAfgCAQAwYzELMAkGA1UEBhMCVVMxZzANBgNVBAGTBkthbnNhc2ETMBEG
A1UEBxMKU21hbGx2aWxsZTENMAsgA1UEChMEQWNTZTENMAsgA1UECjMERGVtbzEQ
MA4GA1UEAxMHVGVzdGluZzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AM3qivmosbp8KollbZKtzLJInW7c8IGRDARABvd604y9EKjGWS4VUayqi6+ng8V4
3kciNuSFVFDcB15J6UnxVIbEWOBXNsmLA/gViAkmd2LgT46HA7hXA1nZuQ81G0z5
DcJXzaur1DFAecIjf7AEiZ29h/X/OjpA2jT7FdsZ6k9gbELQZDZF7VKeQrri8ttU
9kJI2XXmYSh7SynOH200sDPOQvWEnHtDdNWN0CFJksVGkOxbC7P5yKA2knnOPYr
Wo13gFCzQ5fQ2l6MICAky3KFzXma6OzDp4U/eFR67wHyVLTuG61n0rYdc9nMCIgE
vwCVn5wwwWAzvogaOK/chFOCAwEAAABoMGYGCSqGSIB3DQEJDjFZMFcwKQYDVR0R
BCIwIIIMMTkyLjE2OC4xLjQyYgRBhZG1pbkKb21haW4uY29tMAsGA1UdDwQEAwIF
oDAdBgNVHSUEFjAUBgggrBgEFBQcDAQYIKwYBBQUIAgIwDQYJKoZIhvcNAQELBQAD
ggEBAFwjQS8FCMG8x466Ni0WzJev18e4sDDuMQy2Yn0KQEKStMdtJ6pxHcNHNDGq
v+OqMz1d63AXJk6XlvXVoAjRtMzO8PYb938V8BS9ugbU7QESI4q0hujZeqU6xV9n
9Iw3GekPoXR/OvyEcrxX5wcrNzO3T1A64wcvWAHq5uHbHbtsg0TtrkK91sPJQZso
V8pUXG8XwkYGiEFFY8uVQu1facTLNGoh9coaGTyJ80qIEq1j4Vu36muAaXpAo7PQ
yuZn1P1q4SpwEjVdL1/4VgAdeaCBNHBuA6Cm6oIps87MHzkNqs2plIq9/bFepQb
92TD0FVlqBDHypG0HPvNfZDUKwc=
-----END CERTIFICATE REQUEST-----
```

5. Now back out to the Main Menu and Select Create Certificate



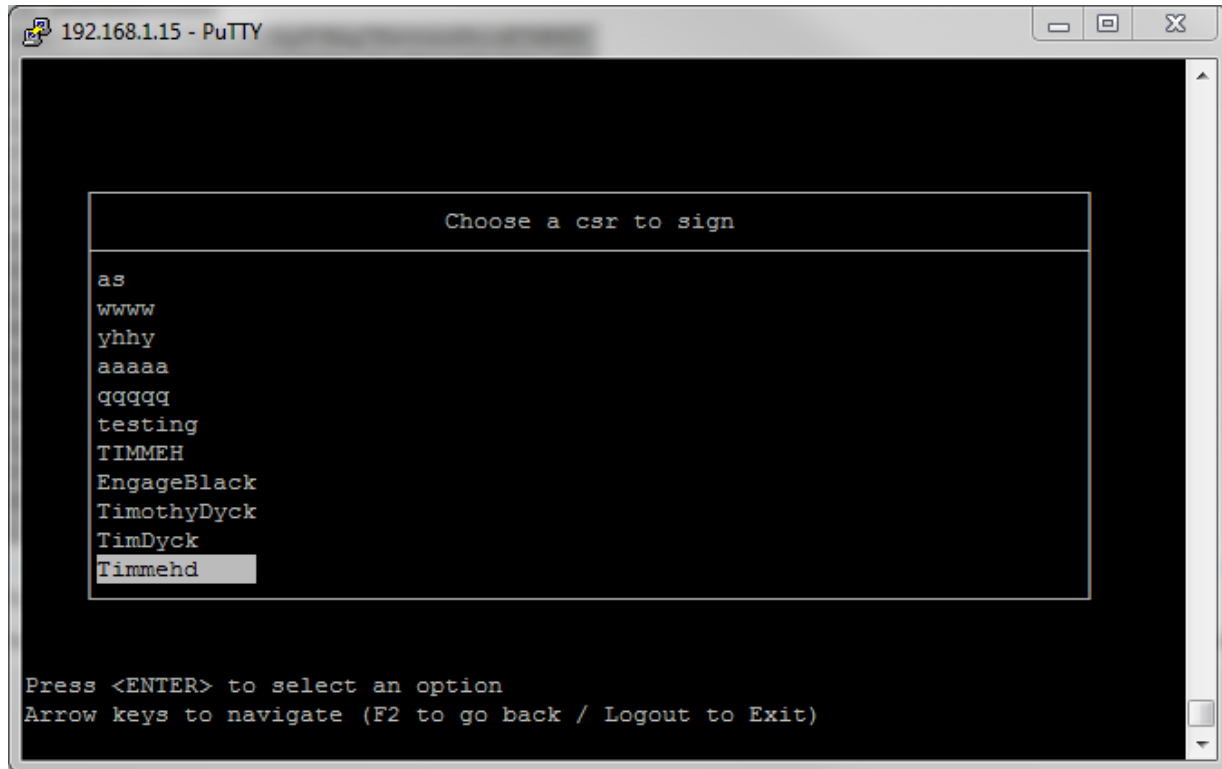
The screenshot shows a PuTTY terminal window titled "192.168.1.15 - PuTTY". The terminal displays a menu for the Black Vault CA. At the top, it says "***Welcome to the Black Vault CA***". Below this, there are two columns of text. The left column lists menu options: "Create Certificate Request" (highlighted with a grey bar), "Create Certificate", "CA Utilities", "Server Utilities", "System Commands", "Information", "Revoke Certificate", "Show Certificates and Status", "Show CA Certificates", and "Logout". The right column displays system information: "Date: 2017-10-18", "Time: 10:42:06", "SSH Port: 22", "Version: 09.00.05", and "Firewall: Off". At the bottom of the terminal, there are instructions: "Press <ENTER> to select an option" and "Arrow keys to navigate (F2 to go back / Logout to Exit)".

```
***Welcome to the Black Vault CA***

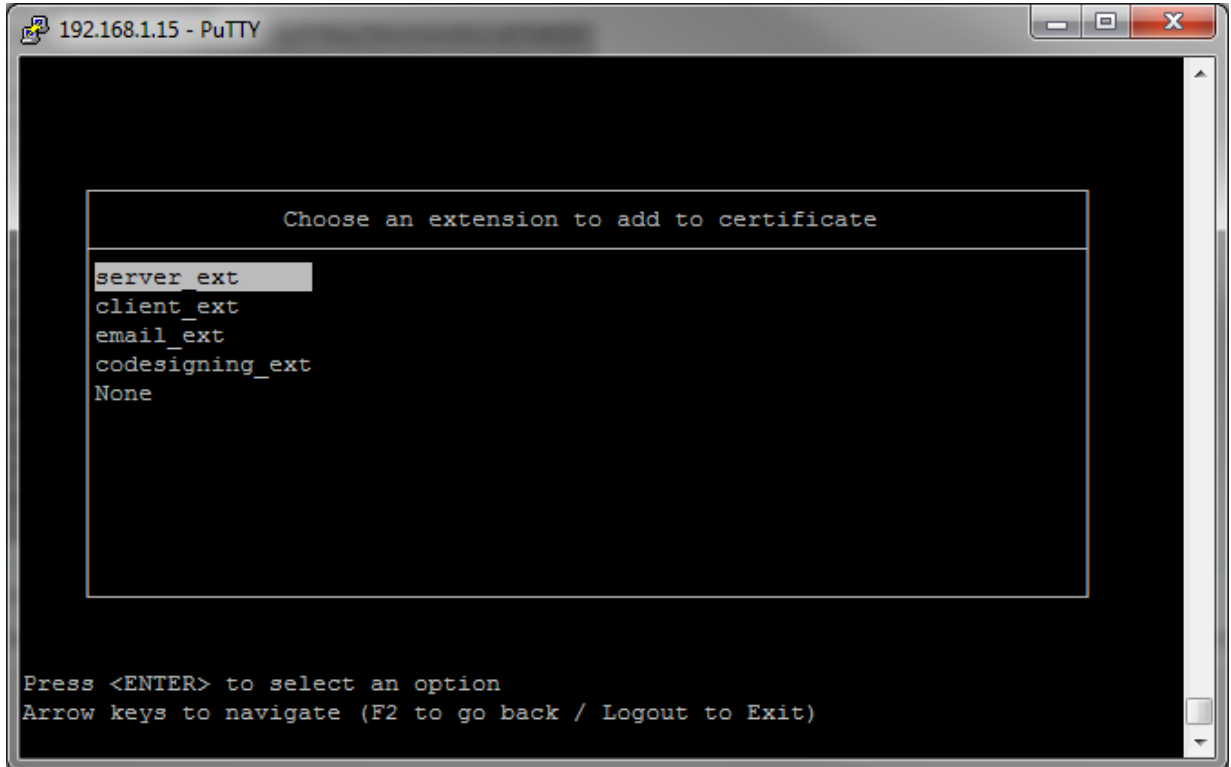
Create Certificate Request      Date: 2017-10-18
Create Certificate             Time: 10:42:06
CA Utilities                  SSH Port: 22
Server Utilities              Version: 09.00.05
System Commands               Firewall: Off
Information
Revoke Certificate
Show Certificates and Status
Show CA Certificates
Logout

Press <ENTER> to select an option
Arrow keys to navigate (F2 to go back / Logout to Exit)
```

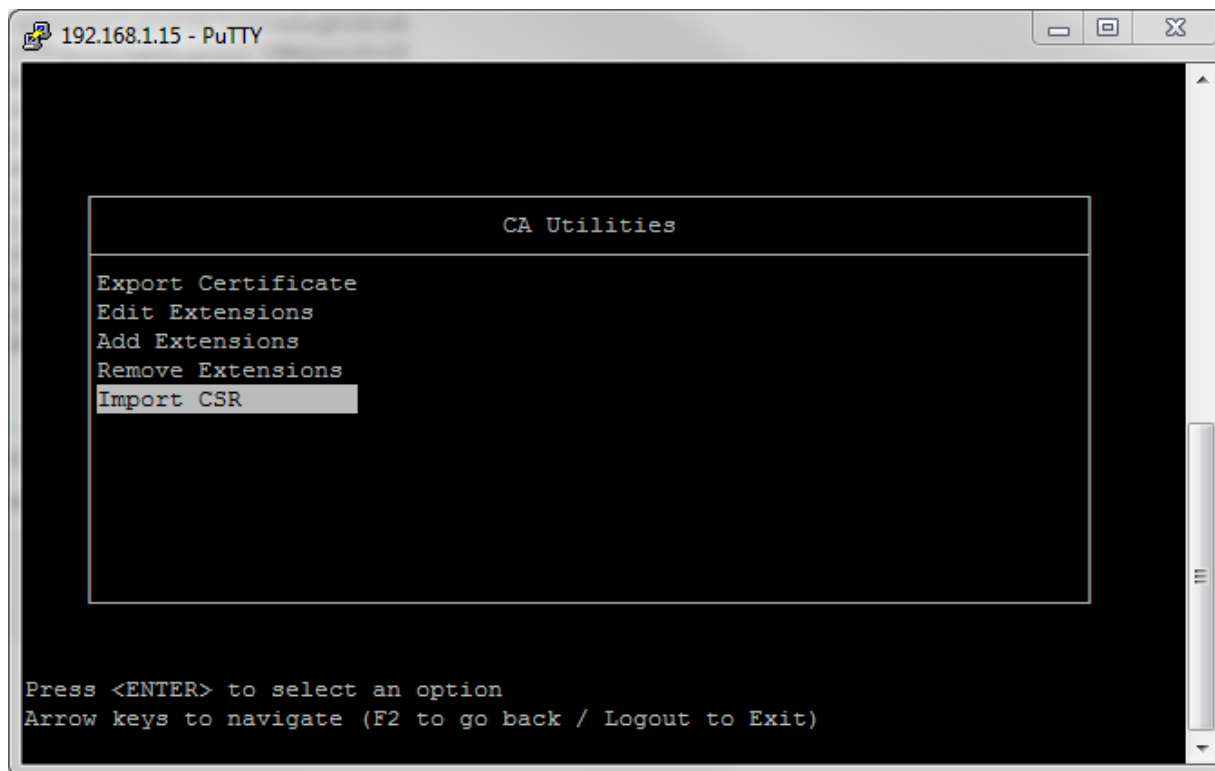
6. Select the Common Name of the CSR you wish to sign



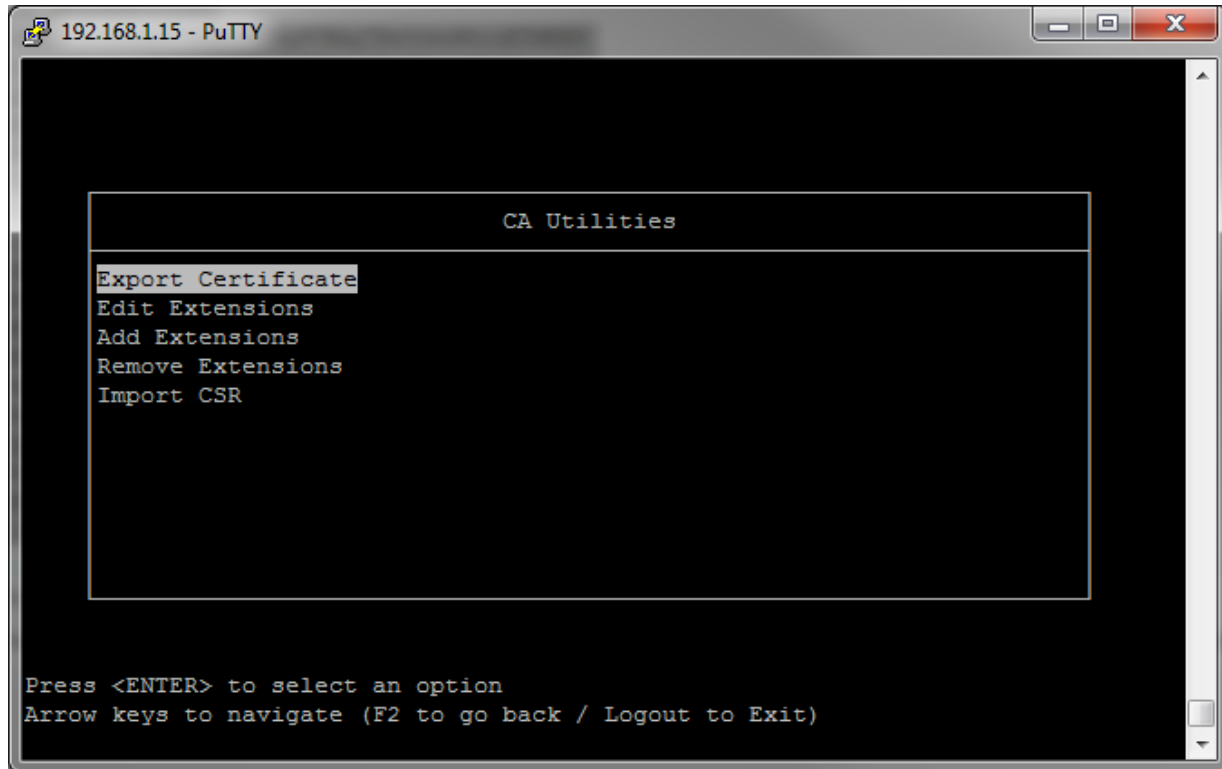
7. Select None when asked for extension type



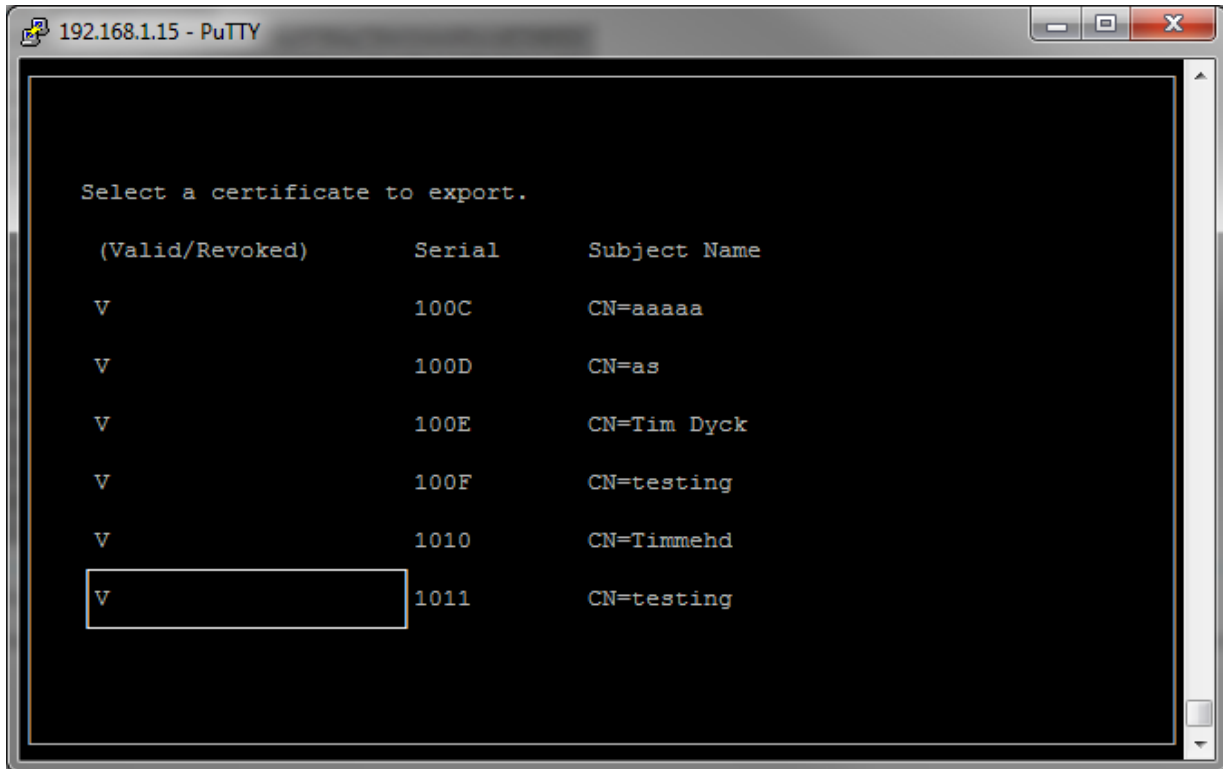
8. Back out to the main Menu and Select CA Utilities



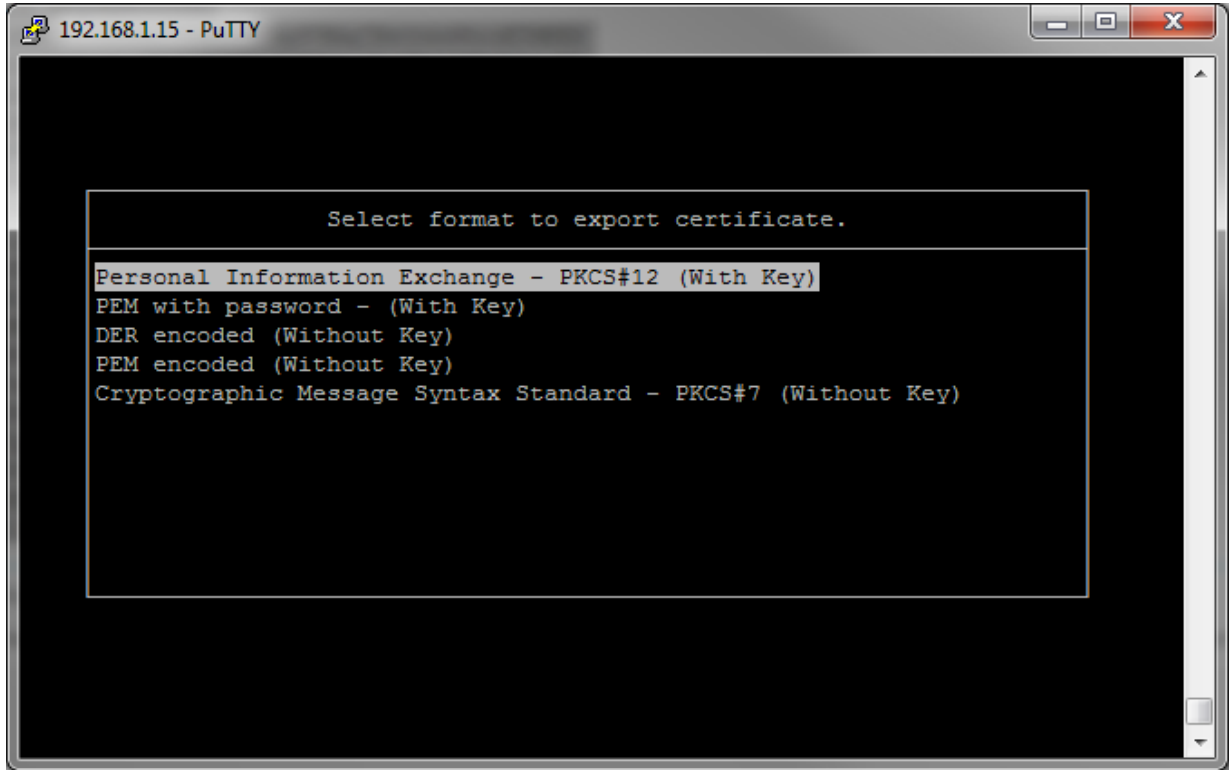
9. Select Export Certificate



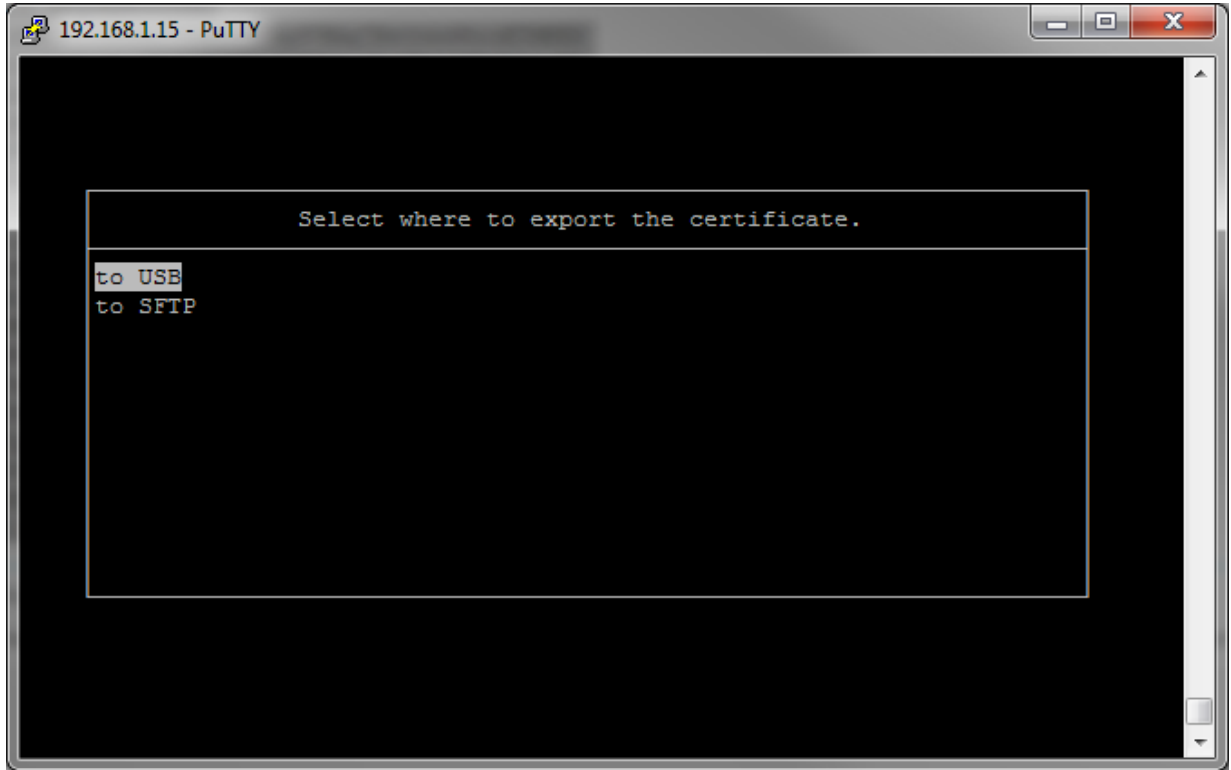
10. Select the Certificate that you just created



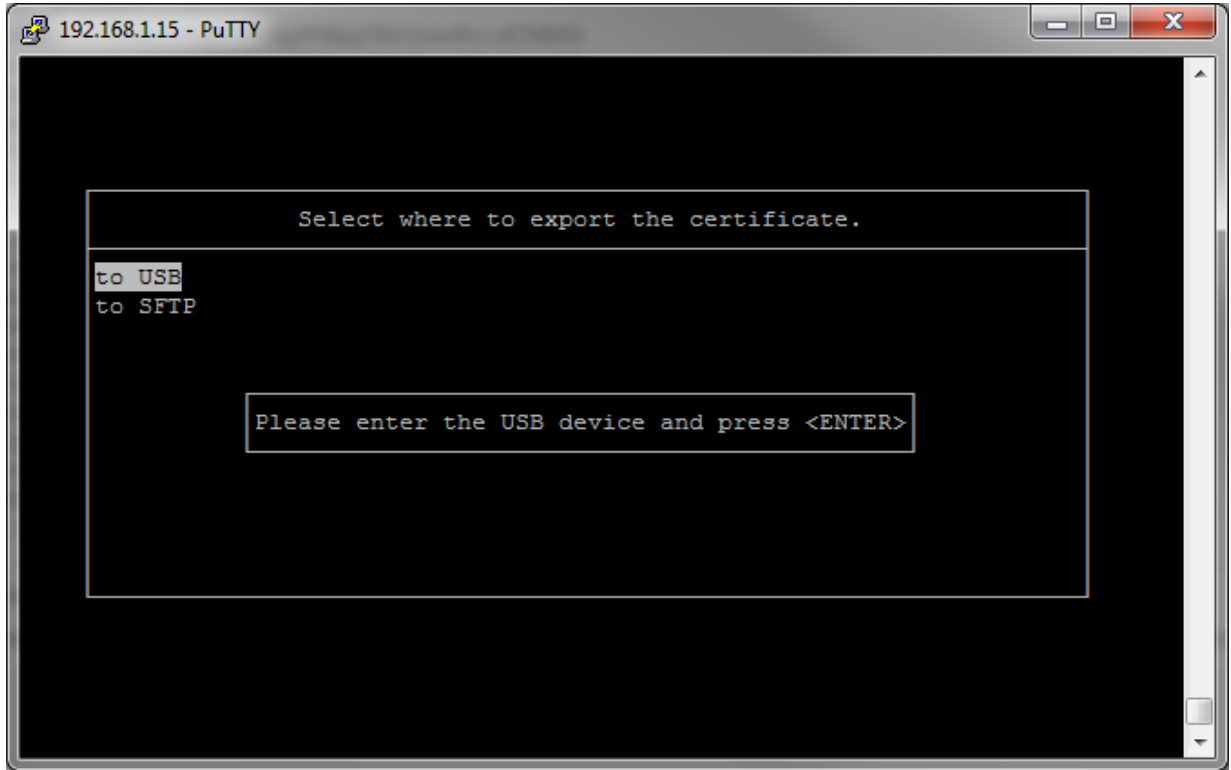
11. Select PEM encoded (Without Key)



12. Select To USB



13. Insert a flash drive to the BlackVault CA and press enter

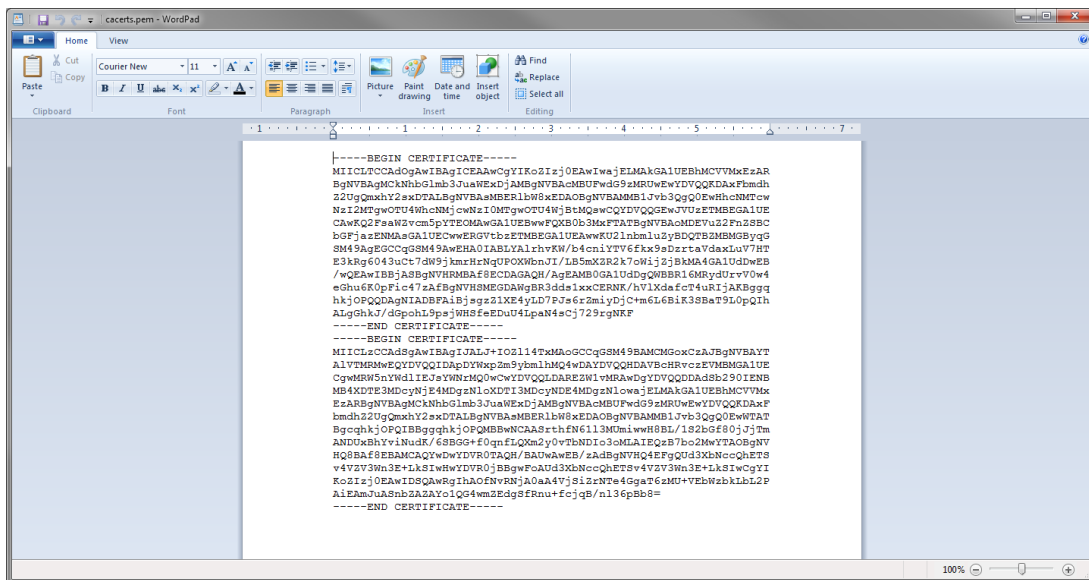


Obtaining the CA certificates

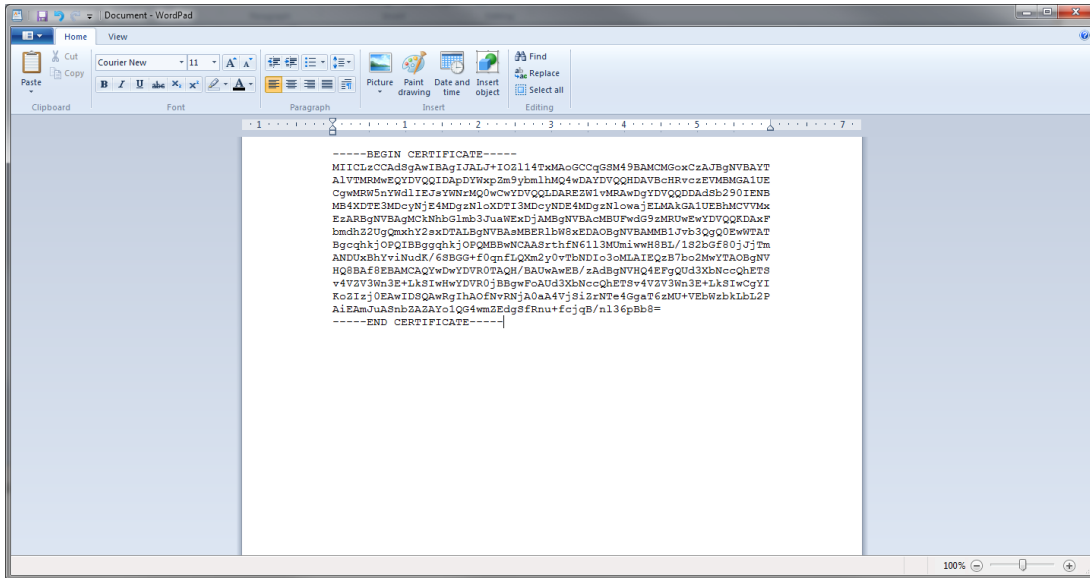
1. On a client computer load the website : IP_Address_Of_BVCA/cacerts.pem



2. Open the downloaded cacerts.pem in wordpad



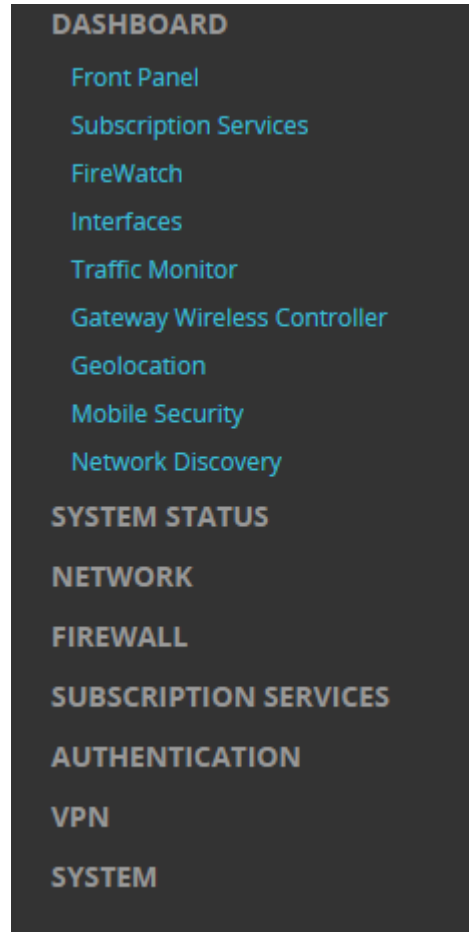
3. Cut the first certificate and in a new document paste it. Save this one as Signing.crt



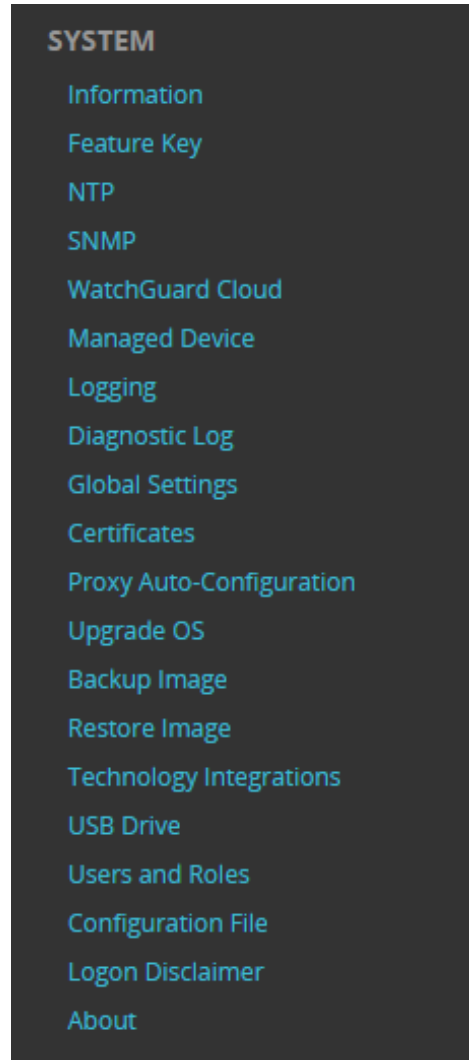
4. Save the remainder as root.crt

Importing the Certificates into Firebox

1. Log into the website of site A's Firebox.
2. In the left-hand side of the page select "System".



3. In the drop-down menu select “Certificates”.



4. On the certificates webpage, click “import Certificate/CRL”.

Certificates



Show Trusted CAs for Proxies

5. On the Import a Certificate page.

Certificates / Import

Import a Certificate | Import a CRL

Certificate Type
Base64 (PEM) certificate

Certificate Function

- Proxy Authority (re-signing CA certificate for outbound SSL/TLS content inspection)
- Proxy Server (server certificate for inbound SSL/TLS content inspection)
- Trusted CA for Proxies
- IPSec, Web Server, Other

Import Certificate File:
Choose File `ccert1.pem`

If your certificate requires a private key, make sure to paste the text from both the certificate and the private key in the text box.

```
-----BEGIN CERTIFICATE-----
MIICLzCCAdSgAwIBAgIJALJ+IOZI14TxMAoGCCqGSM49BAMCMGoxCzAJBgNVBAYT
AIVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMQ4wDAYDVQQHDAVhcHRvczEVMBMGGA1UE
CgwMRW5nYWdlIEJsYWNRMQ0wCwYDVQQLDAREZW1vMRAwDgYDVQQDDAdSb290IENB
MB4XDTE3MDcyNjE4MDgzNloXDTE3MDcyNDE4MDgzNlowajELMAkGA1UEBhMCVVMx
EzARBgNVBAGMCkNhbGImb3JuaWEwDjAMBgNVBAcMBUFWdG9zMRUwEwYDVQQKDAxP
bmdhZ2UgQmxhY2sxDALBgNVBAsMBERibW8xEDAOBgNVBAMMB1Jvb3QgQ0EwWTAT
BgqhkJOPQIBBggqhkJOPQMBBwNCAASrthfN6113MUmiwwH8BL/1S2bGf80jJtM
ANDUxBhYviNudK/6SBGG+f0qnfLQXm2y0vTbNDIo3oMLAIEQzB7bo2MwYTAOBgNV
HQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUd3XbNccQhETS
v4VZV3Wn3E+LkSlwHwYDVR0jBBgwFoAUd3XbNccQhETSv4VZV3Wn3E+LkSlwCgYI
KoZlj0EAwIDSQAwrGhAOfNvRNjA0aA4VjSiZrNte4GgaT6zMU+VEbWzblLbL2P
AIEAmJuASnbZAZAYo1QG4wmZEgSfRnu+fcjqB/nl36pBb8=
-----END CERTIFICATE-----
```

SAVE | CANCEL

- a. Under Certificate Function Select IPSec, Web Server, Other.
- b. Under Certificate File Click Choose file, then browse to where you saved Root.crt.
- c. Click Save.

6. On the Import a Certificate page.

Certificates / Import

Import a Certificate Import a CRL

Certificate Type
Base64 (PEM) certificate

Certificate Function

- Proxy Authority (re-signing CA certificate for outbound SSL/TLS content inspection)
- Proxy Server (server certificate for inbound SSL/TLS content inspection)
- Trusted CA for Proxies
- IPsec, Web Server, Other

Import Certificate File:
Choose File cacert2.pem

If your certificate requires a private key, make sure to paste the text from both the certificate and the private key in the text box.

```
-----BEGIN CERTIFICATE-----
MIICLTCCAdOgAwIBAgICEAAwCgYIKoZlZj0EAWlwajELMAkGA1UEBhMCVVMxEzAR
BgNVBAGMCkNhbgGimb3JuaWExDjAMBgNVBACMBUFWdG9zMRUwEwYDVQQKDAxDbmRl
Z2UgQm9uY2sxDALBgNVBAsMBERibW8xEDA0BgNVBAMMB1Jvb3QgQ0EwHhcNMTCw
NzI2MTgwOTU4W9jcmRrNzI0MTgwOTU4WjBtMQswCQYDVQQGEwJVUzETMBEGA1UE
CAwKQ2FsaWZvcn5pYTEOMAwGA1UEBwwFQXB0b3MxFTATBgNVBAoMDEVudDwEB
bGFjazENMAsGA1UECwwERGVtbzETMBEGA1UEAwwKU2lnbmluZyBDQTZBMGMGBYqG
SM49AgEGCCqGSM49AwEHAQIABLYAlrhvKW/b4cniYTV6fkx9sDzrtaVdaxLuV7HT
E3kRg6043uCT7dW9jkmrHrNqUPOXWbnJI/LB5mXZR2k7oWijzjBkMA4GA1UdDwEB
/wwQEAwIBBjASBgNVHRMBAf8ECDAGAQH/AgEAMBOGA1UdDgQWBRR16MRydUrv0w4
eGhu6K0pFic47zAfBgNVHSMEGDAWgBR3dds1xxCERNK/hVIXdafcT4uRljAKBggq
hkjOPQDAGNIADBFaiBjsgzZ1XE4yLD7PJs6rZmiyDjC+m6L6BiK3SBaT9L0pQlh
ALgGhkJ/dGpohL9psjWHSfeDU4LpaN4sCj729rgNKF
-----END CERTIFICATE-----
```

SAVE CANCEL

- Under Certificate Function Select IPsec, Web Server, Other.
- Under Certificate File Click Choose file, then browse to where you saved Signing.crt.
- Click Save.

7. On the Import a Certificate page.

Certificates / Import

Import a Certificate | Import a CRL

Certificate Type
Base64 (PEM) certificate

Certificate Function

- Proxy Authority (re-signing CA certificate for outbound SSL/TLS content inspection)
- Proxy Server (server certificate for inbound SSL/TLS content inspection)
- Trusted CA for Proxies
- IPsec, Web Server, Other

Import Certificate File:
Choose File No file chosen

If your certificate requires a private key, make sure to paste the text from both the certificate and the private key in the text box.

```
-----BEGIN CERTIFICATE-----
MIIC9TCCApugAwIBAgIACEBkwCgYIKoZiZj0EAWIwbTELMaGA1UEBhMCVVMxZzAR
BgNVBAGMCKNhGImb3JuaWExDjAMBgNVBACMBUFwdG9zMRUwEwYDVQKDAxZmmdh
ZZUgQmxhY2sxZDZALBgNVBAsMBERibW8xZzARBgNVBAMMCINpZ25pbmcgQ0EwHhcN
MTcxMTA3MTY1NDQyWWhcNMTkxMTA3MTY1NDQyWjBpMQswCQYDVQQGEwJVUzERMA8G
A1UECBMISWxsaW5vaXNMcEzARBgNVBACTCINiYXN0bG9uZDZALBgNVBAoTBEFj
bWUxZDA0BgNVBAStB1Rlc3RpbmcxETAPBgNVBAMTCEppbSBEdWNRMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA24EK+/W+6hyc+YRZCO5K3vxoNcU/OwNa
TjW4TI9+hflA0PNDEgSDCDIJWAIkv4Dao+Cd/WMhbC0nNta8lBnmF8Gp+AuhB0PB
M2WwWa8l0umEWB2AkSW08rj+UEel7TmA1y7KLTfivbRQ7FBiwChDXDTwKjE28/Z
+Dqp2KFjtED0Jnfi8tW87rFZ2xY+ot/DQWMdotHIZ+lwk2qL80PGgDBaUa2hVlK
Kb3px6ZJ6H3saSiJnLERoydQvH0mqJeSgl9sbh9zxHzny8uR6cDWcsPC+5iQxfyC
jmfqU6W81irAVFKznrWiPLoODxQ9MGxGHc47azbkHrxoagIi0j4ukwIDAQABO2Qw
YjAJBgNVHRMEAJAAAMCKGA1UdEQQiMCCCDE5Mi4xNjguMS40MoEQYWRtaW5AZG9t
YWIuLmNvbTALBgNVHQ8EBAMCBaAwHQYDVROIBBYwFAYIKwYBBQUHAWEGCCsGAQUF
CAICMAoGCCqGSM49BAMCA0gAMEUCIQCswQLVqp+n61CTCaGHRMw6PkogSFdhqYFP
Pqobg5W9jwlgGKVLmMvjrGrtNETWqC7oCxz7y6HJZNCvwjhlK/Czivg=
-----END CERTIFICATE-----
```

SAVE | CANCEL

- Under Certificate Function Select IPsec, Web Server, Other.
- Under Certificate File Click Choose file, then browse to where your flash drive and select the Certificate you exported from the BlackVault.
- Click Save.



Engage BlackVault CA WatchGuard Integration Guide

Site B

Repeat Process stated in site a for site b.

Setting up VPN

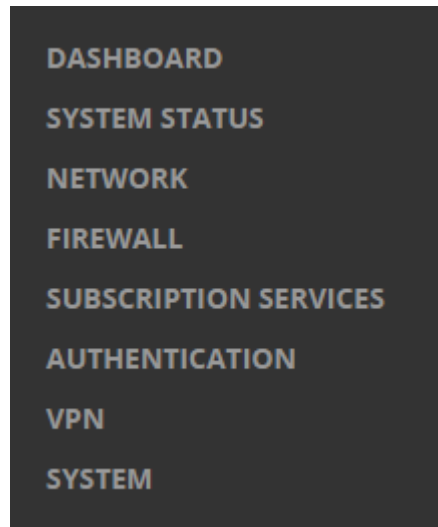
Before setting up the VPN it is a good idea to collect the following information

- Site A and B external IP addresses
- Site A and B internal network IP addresses
- Site A and B CN from their certificates

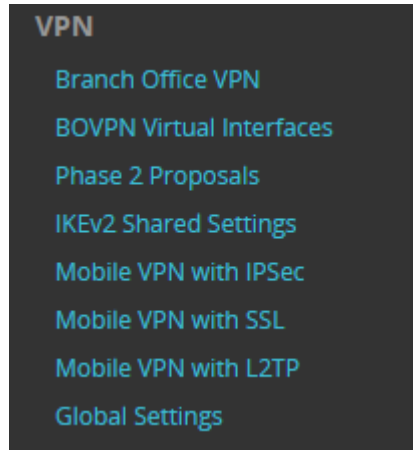
Site A

Configuring VPN

1. Log into the website of site A's FireBox.
2. In the Left-hand side of the page select "VPN"



3. Again, in the left-hand side of the page select "Branch Office VPN"



4. Under the Gateway section click "Add"

Gateways

NAME ↕	EDITABLE
gateway.1	Yes

[ADD](#) [EDIT](#) [REMOVE](#) [ENABLE](#) [DISABLE](#) [REPORT](#)

- a. In the General Settings Tab

General Settings | **Phase 1 Settings**

Credential Method

Use Pre-Shared Key

Use IPSec Firebox Certificate

Show All Certificates

ID	CERTIFICATE NAME	ALGORITHM	TYPE
20002	c=US st=Illinois l=Smallville o=Acme ou=Testing cn=Jim Duck	RSA	IPSec / Web
20001	c=US st=Kansas l=Smallville o=DEMO ou=DEMO cn=DEMO	RSA	IPSec / Web
29000	o=Engage Black cn=192.168.1.42	RSA	IPSec / Web

Gateway Endpoint

	LOCAL INTERFACE	LOCAL TYPE	LOCAL ID	REMOTE IP	REMOTE TYPE	REMOTE ID
--	-----------------	------------	----------	-----------	-------------	-----------

Start Phase 1 tunnel when Firebox starts

- i. For Credential method select "Use IPSec Firebox Certificate" then select the certificate you imported
- ii. For Gateway Endpoint Click "Add"

1. Under the Local Gateway Tab

Gateway Endpoint Settings ✕

A tunnel needs authentication on each side of the tunnel. Provide the configuration details for the gateway endpoints below.

Local Gateway **Remote Gateway**

External Interface: ⓘ

Specify the gateway ID for tunnel authentication.

By IP Address:

By Domain Name:

By User ID on Domain:

By x500 Name

- a. Select External Interface as “external”
- b. Under the “Specify the gateway ID for tunnel authentication.” Section select “By x500 Name”

2. Under the Remote Gateway Tab

The screenshot shows a dialog box titled "Gateway Endpoint Settings" with a close button (X) in the top right corner. Below the title is a descriptive text: "A tunnel needs authentication on each side of the tunnel. Provide the configuration details for the gateway endpoints below." There are three tabs: "Local Gateway", "Remote Gateway" (which is selected and highlighted in blue), and an unlabeled tab. Under the "Remote Gateway" tab, there are two sections. The first section is titled "Specify the remote gateway IP address for a tunnel." and contains two radio buttons: "Static IP Address" (which is selected) and "Dynamic IP Address". Next to the "Static IP Address" radio button is a text input field containing the value "192.168.1.43". The second section is titled "Specify the remote gateway ID for tunnel authentication." and contains four radio buttons: "By IP Address", "By Domain Name", "By User ID on Domain", and "By x500 Name" (which is selected). Next to the "By x500 Name" radio button is a text input field containing the value "c=US st=Kansas l=Smallville". Below these sections is a checkbox labeled "Attempt to resolve domain" which is currently unchecked. At the bottom right of the dialog box are two buttons: "OK" and "CANCEL".

- a. In the “Specify the remote gateway IP address for a tunnel.” Section enter the remote IP address
- b. In the “Specify the remote gateway ID for tunnel authentication” select “By x500 Name” then enter in the Common Name of the remote site’s certificate

3. Then click “Ok”

- b. In the Phase 1 Settings
 - i. Leave everything to their defaults
- c. Press Save

5. Under the Tunnels section click add

Tunnels

NAME ↕	EDITABLE
tunnel.1	Yes

ADD CLONE EDIT REMOVE REPORT MOVE UP MOVE DOWN SAVE ORDER

d. In the Addresses Tab

Tunnel Route Settings ×

Addresses NAT

Local IP

Choose Type

Network IP /

Remote IP

Choose Type

Network IP /

Direction

Enable broadcast routing over the tunnel

OK **CANCEL**

i. Under Addresses click "Add"

1. For Local IP

a. In Choose Type select Network IPv4,

- b. In Network IP add in the local network
 2. For Remote IP
 - a. In Choose Type select Network IPv4,
 - b. In Network IP add in the remote network
 3. For everything leave to defaults, then click "Ok"
 - ii. For everything else, leave to defaults then press "Save"

Site B

Repeat Process stated in Site A for Site B

WatchGuard System Manager Instructions

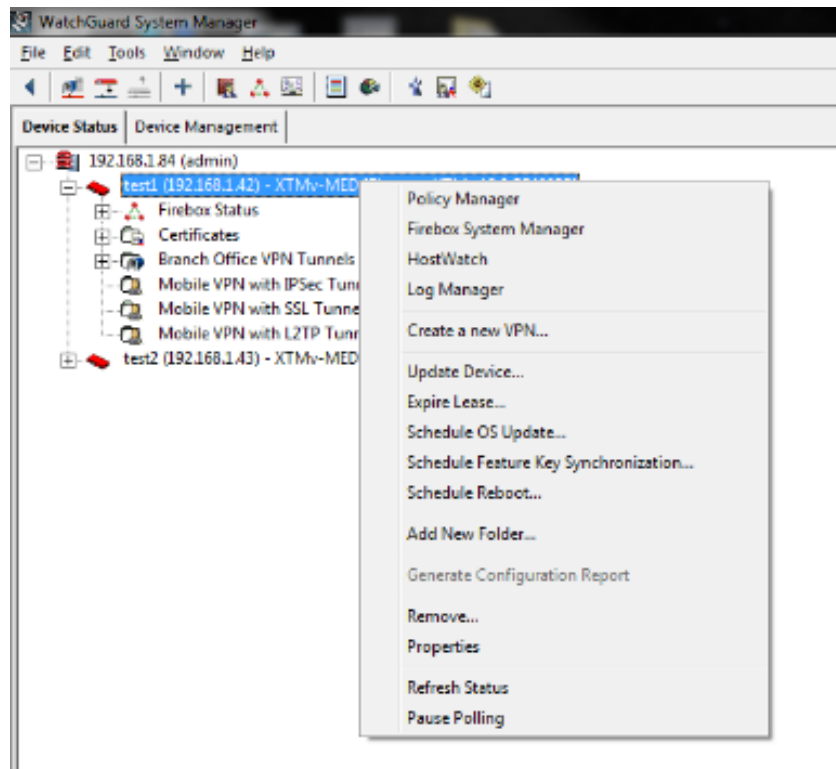
Setting Up Certificates

The first part of this guide is configuring the certificates that will be used in the VPNs

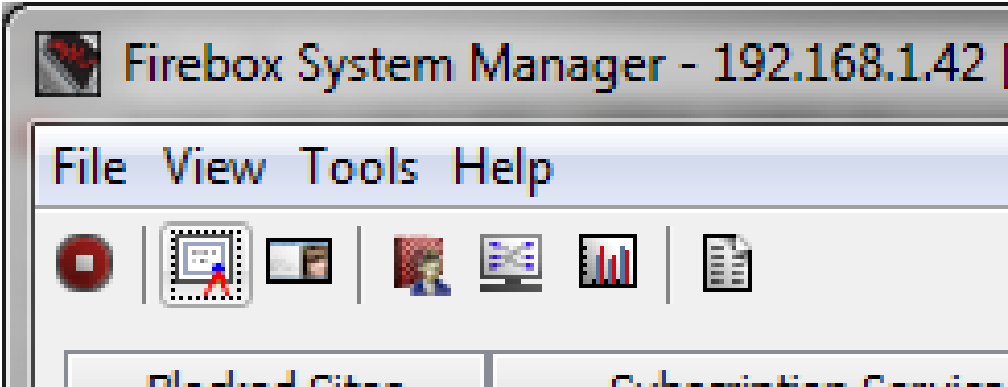
Site A

Creating A CSR

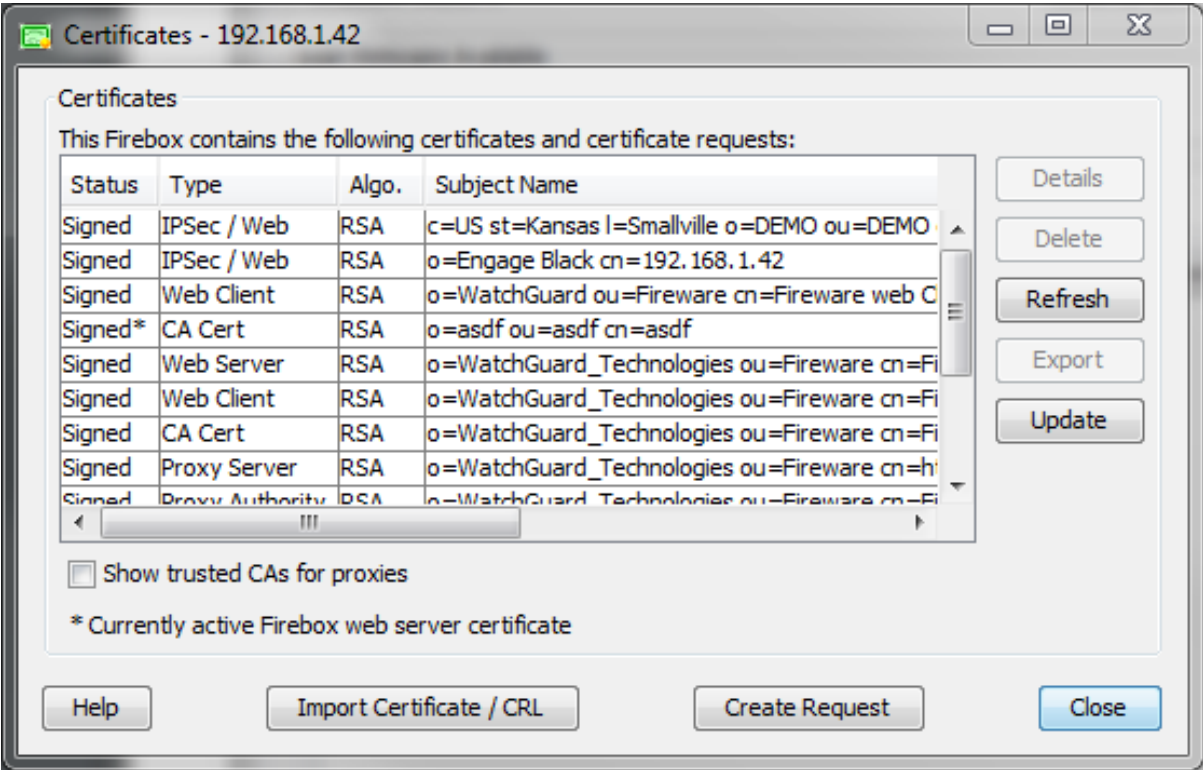
1. From the WatchGuard System Manager, open the system manager



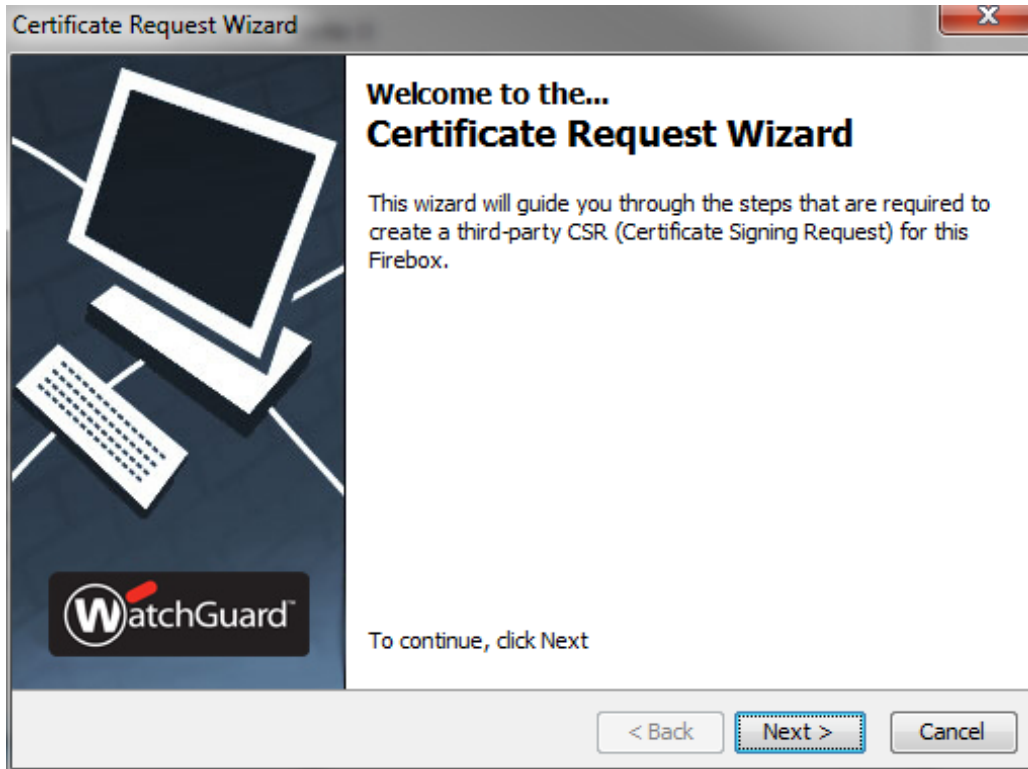
2. In the Firebox System Manager, click the Certificates Button



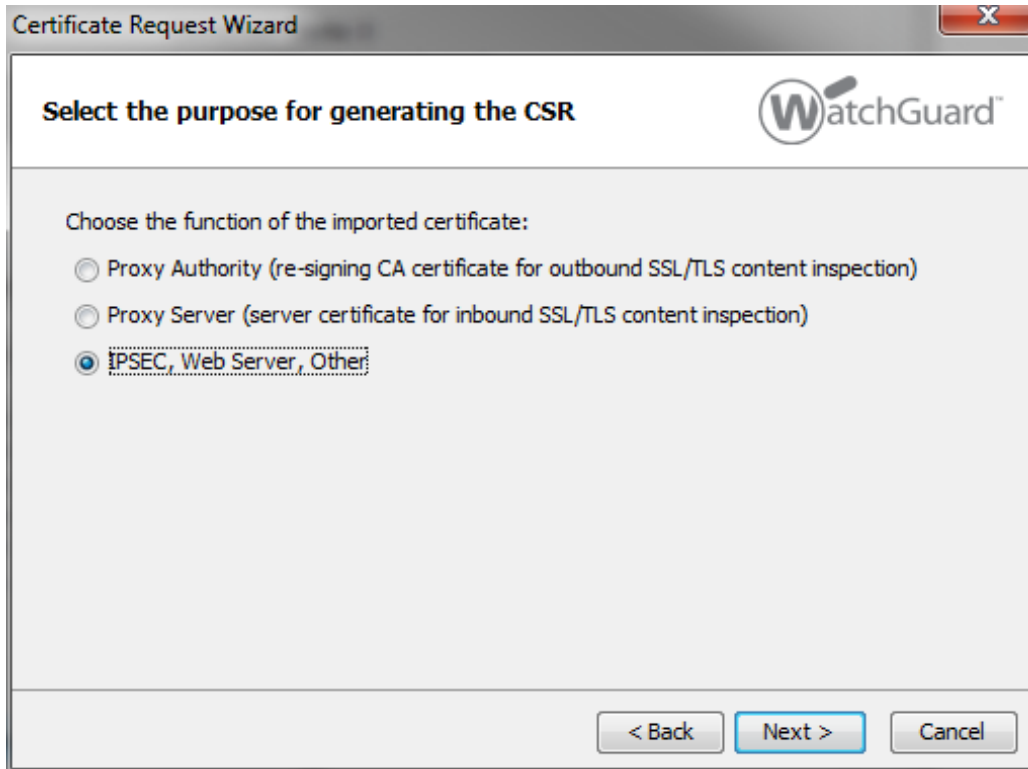
3. In the Certificates window, click Create Request Button



4. In the Certificate Request Wizard, press Next



5. Select the IPSEC, Web Server, Other radio button and press Next



6. Fill out the fields for the Subject-Name and press Next

Certificate Request Wizard

Configure the fields for the subject name. WatchGuard™

The information here will be used to generate the subject name

Name (CN): (required)

Department Name (OU):

Company Name (O): (required)

City/Location (L):

State/Province (ST):

Country (C): (required)

< Back Next > Cancel

7. Fill out the fields for the Domain Info and press Next

Certificate Request Wizard

Configure the remaining domain information. WatchGuard™

Subject Name: =Jim Duck, OU=Testing, O=Acme, L=Smallville, ST=Illinois, C=US (required)

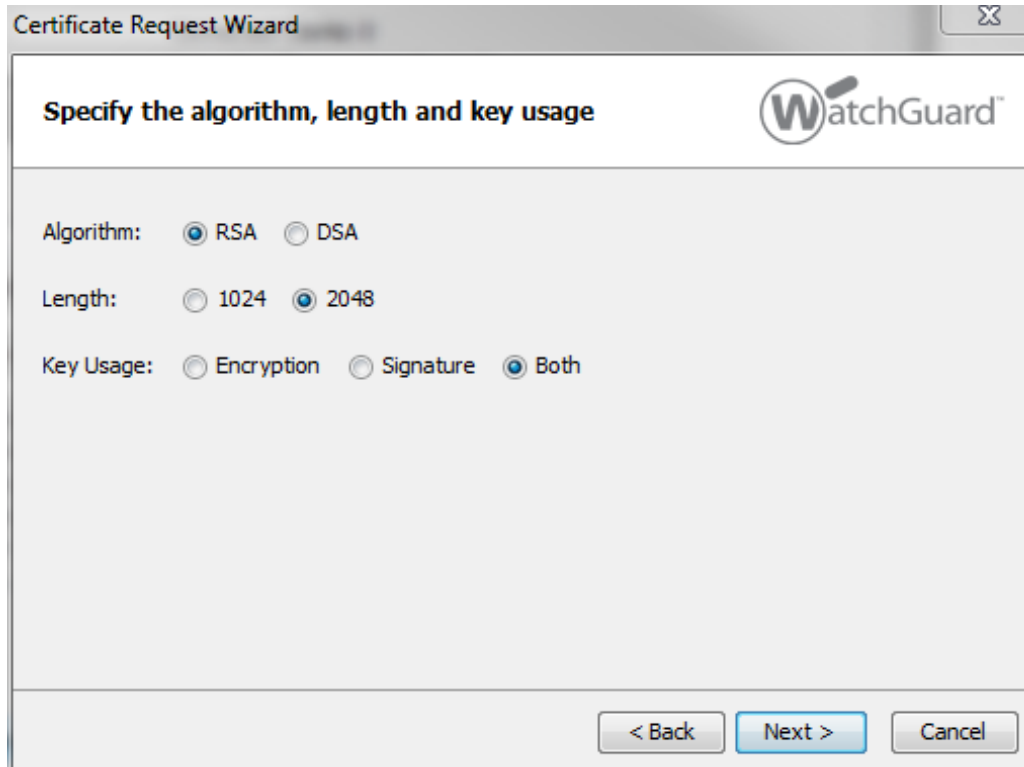
DNS Name: 192.168.1.42 (required)

IP Address: . . .

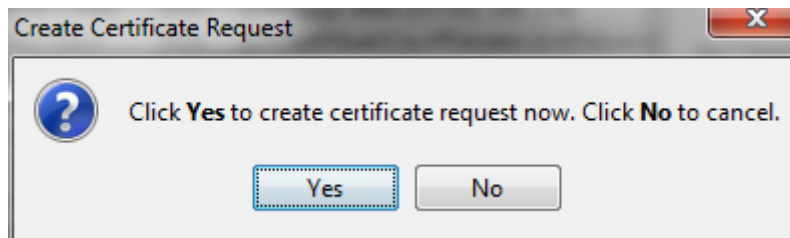
User Domain Name: admin@domain.com

< Back Next > Cancel

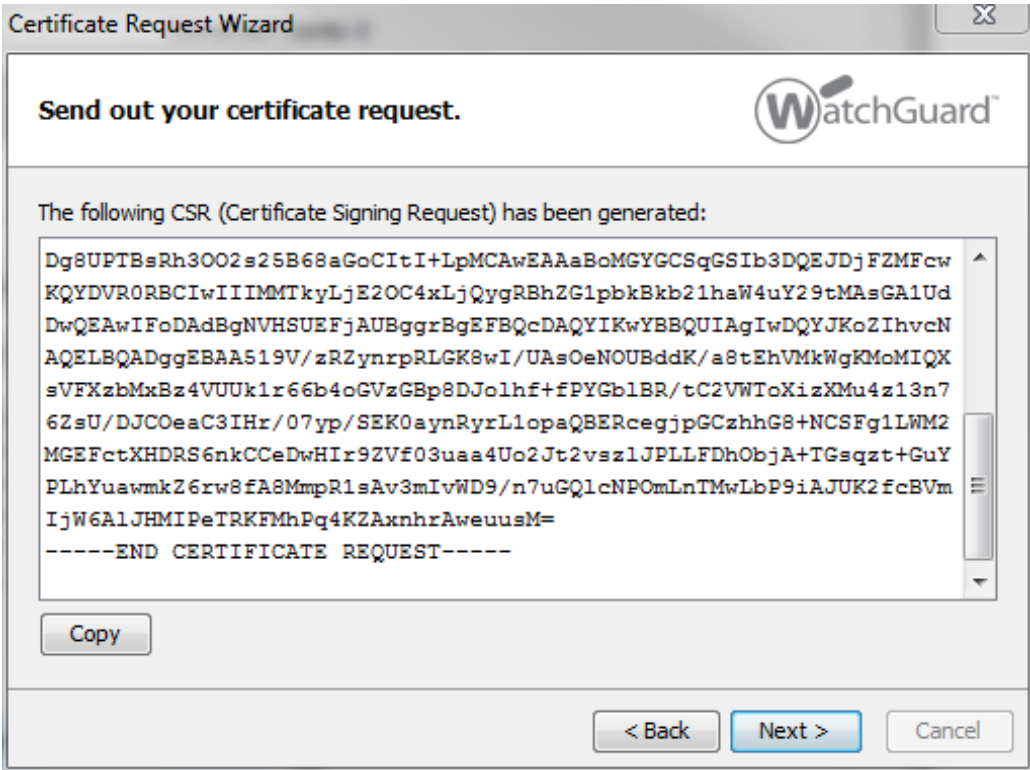
8. Configure the settings for generating the key and press next



9. In the Create Certificate Request Window that pops up, Press yes



- 10. Back in the Certificate Request Wizard window, the newly created certificate request will be displayed. Copy this into a notepad, save the notepad as `certificaterequestsiaea.csr` then click Next

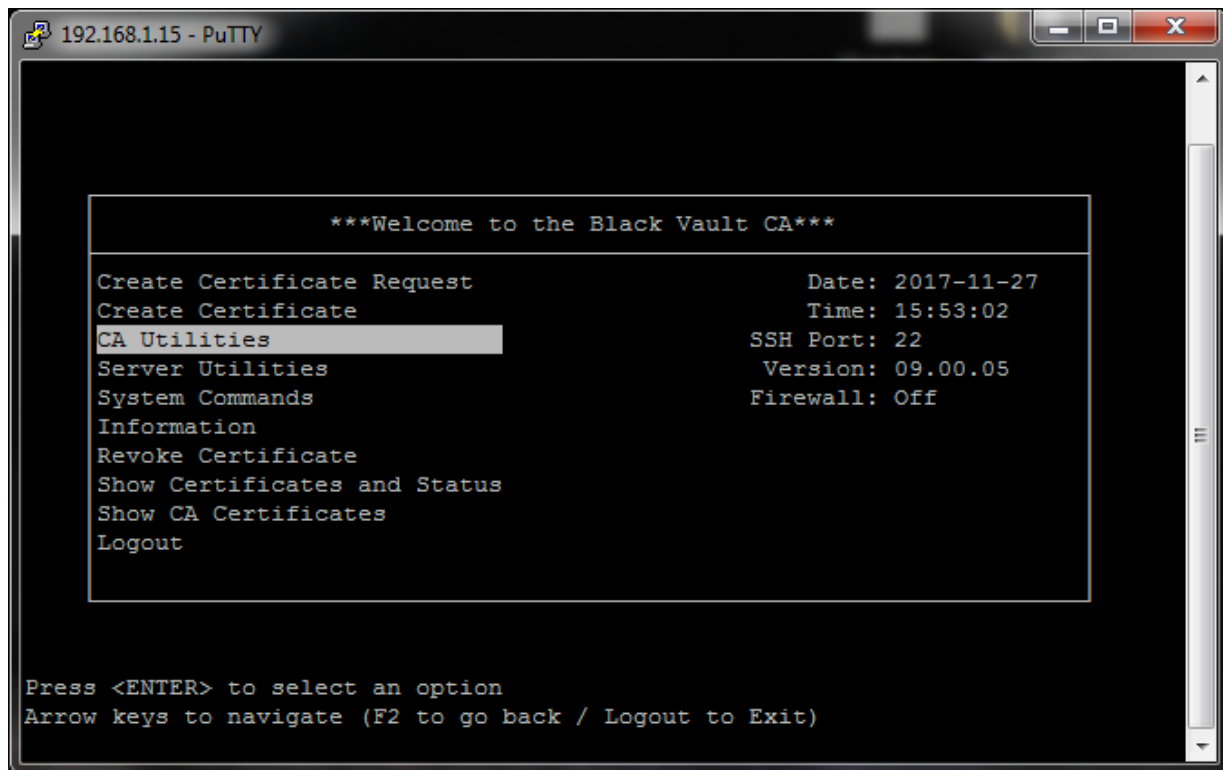


11. Press Finish



Signing your CSR

1. Log into the BlackVault CA as a operator user.
2. Select CA Utilities.



The screenshot shows a PuTTY terminal window titled "192.168.1.15 - PuTTY". The terminal displays a menu for the Black Vault CA. The menu items are: "Create Certificate Request", "Create Certificate", "CA Utilities" (highlighted), "Server Utilities", "System Commands", "Information", "Revoke Certificate", "Show Certificates and Status", "Show CA Certificates", and "Logout". To the right of the menu items, there is a status block: "Date: 2017-11-27", "Time: 15:53:02", "SSH Port: 22", "Version: 09.00.05", and "Firewall: Off". At the bottom of the terminal, there are instructions: "Press <ENTER> to select an option" and "Arrow keys to navigate (F2 to go back / Logout to Exit)".

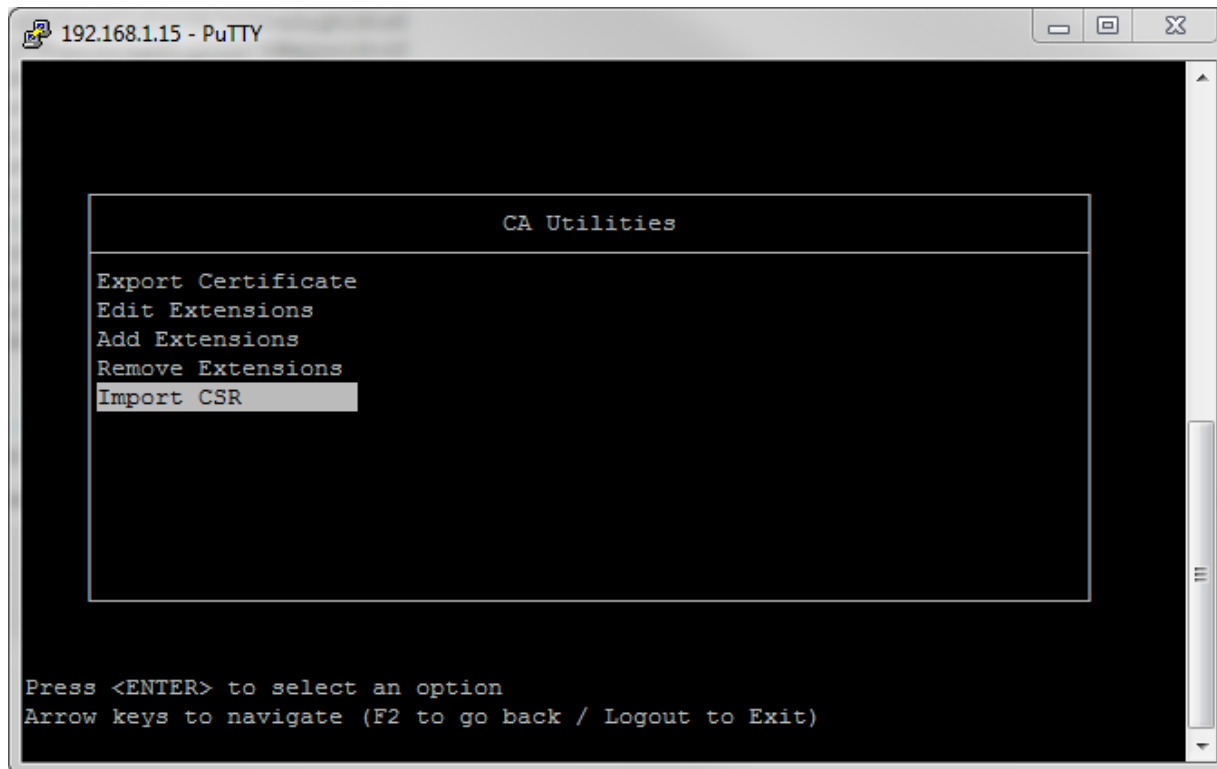
```
192.168.1.15 - PuTTY

***Welcome to the Black Vault CA***

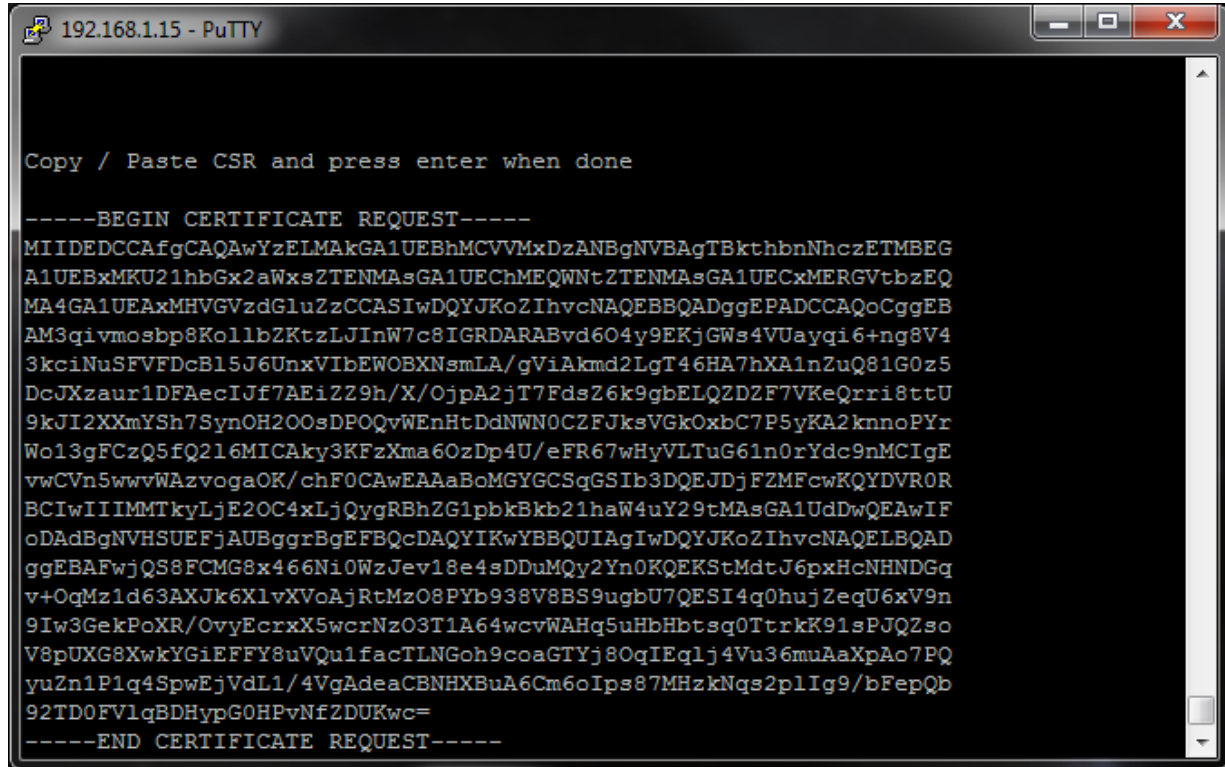
Create Certificate Request          Date: 2017-11-27
Create Certificate                  Time: 15:53:02
CA Utilities                        SSH Port: 22
Server Utilities                   Version: 09.00.05
System Commands                    Firewall: Off
Information
Revoke Certificate
Show Certificates and Status
Show CA Certificates
Logout

Press <ENTER> to select an option
Arrow keys to navigate (F2 to go back / Logout to Exit)
```

3. Select Import CSR



4. Paste in the CSR that you just created (saved in the file certificaterequestsita.csr).

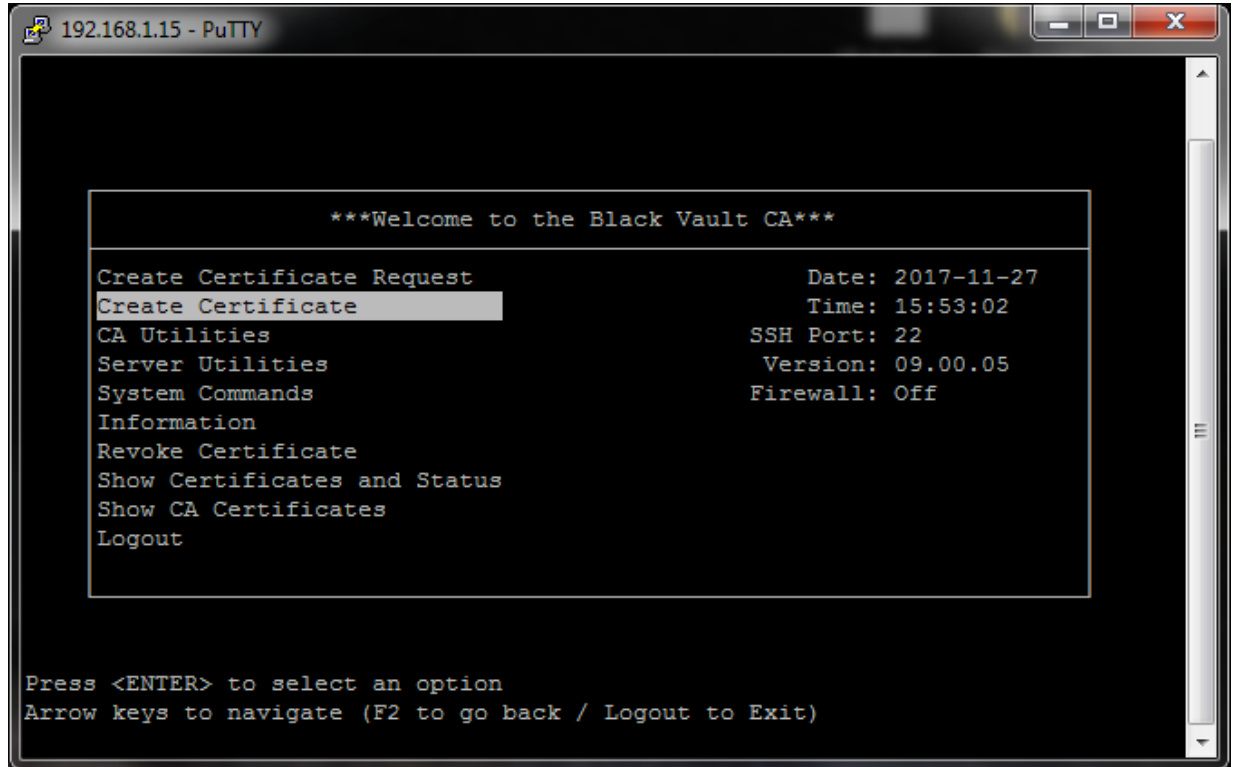


```
192.168.1.15 - PuTTY

Copy / Paste CSR and press enter when done

-----BEGIN CERTIFICATE REQUEST-----
MIIDEDCCAfgCAQAwYzELMAkGA1UEBhMCVVMxMzANBgNVBAgTBkthbnNhc2ETMBEG
A1UEBxMKU21hbGx2aWxsZTENMAsgA1UEChMEQWNTZTENMAsgA1UECzMERGVTbzEQ
MA4GA1UEAxMHVGVzdGluZzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AM3qivmosbp8KollbZKtzLJInW7c8IGRDARABvd604y9EKjGWS4VUayqi6+ng8V4
3kciNuSFVFDcBl5J6UnxVIbEWOBXNsmLA/gViAkmd2LgT46HA7hXA1nZuQ81G0z5
DcJXzaur1DFAecIJf7AEiZ29h/X/Ojpa2jT7FdsZ6k9gbELQZDZF7VKeQrri8ttU
9kJI2XXmYSh7SynOH200sDPOQvWEnHtDdNWN0CZFJksVGkOxbC7P5yKA2knoPYr
Wo13gFCzQ5fQ2l6MICAkY3KFzXma6OzDp4U/eFR67wHyVLTuG61n0rYdc9nMCIgE
vwCVn5wwwWAzvogaOK/chFOCAwEAAABoMGYGCsGqGSIB3DQEJJDjFZMFcwKQYDVR0R
BCIwIIIMMTkyLjE2OC4xLjQyYgRBhZG1pbkKb21haW4uY29tMAsGA1UdDwQEAwIF
oDAdBgNVHSUEFjAUBgggrBgEFBQcDAQYIKwYBBQUIAgIwDQYJKoZIhvcNAQELBQAD
ggEBAFwjQS8FCMG8x466Ni0WzJev18e4sDDuMQy2Yn0KQEKStMdtJ6pxHcNHNDGq
v+OqMz1d63AXJk6XlvXVoAjRtMzO8PYb938V8BS9ugbU7QESI4q0hujZeqU6xV9n
9Iw3GekPoXR/OvyEcrxX5wcrNzO3T1A64wcvWAHq5uHbHbtsg0TtrkK91sPJQZso
V8pUXG8XwkYGiEFFY8uVQu1facTLNGoh9coaGTyJ80qIEq1j4Vu36muAaXpAo7PQ
yuZn1P1q4SpwEjVdL1/4VgAdeaCBNHBuA6Cm6oIps87MHzkNqs2plIq9/bFepQb
92TD0FV1qBDHypG0HPvNfZDUKwc=
-----END CERTIFICATE REQUEST-----
```


5. Now back out to the Main Menu and Select Create Certificate



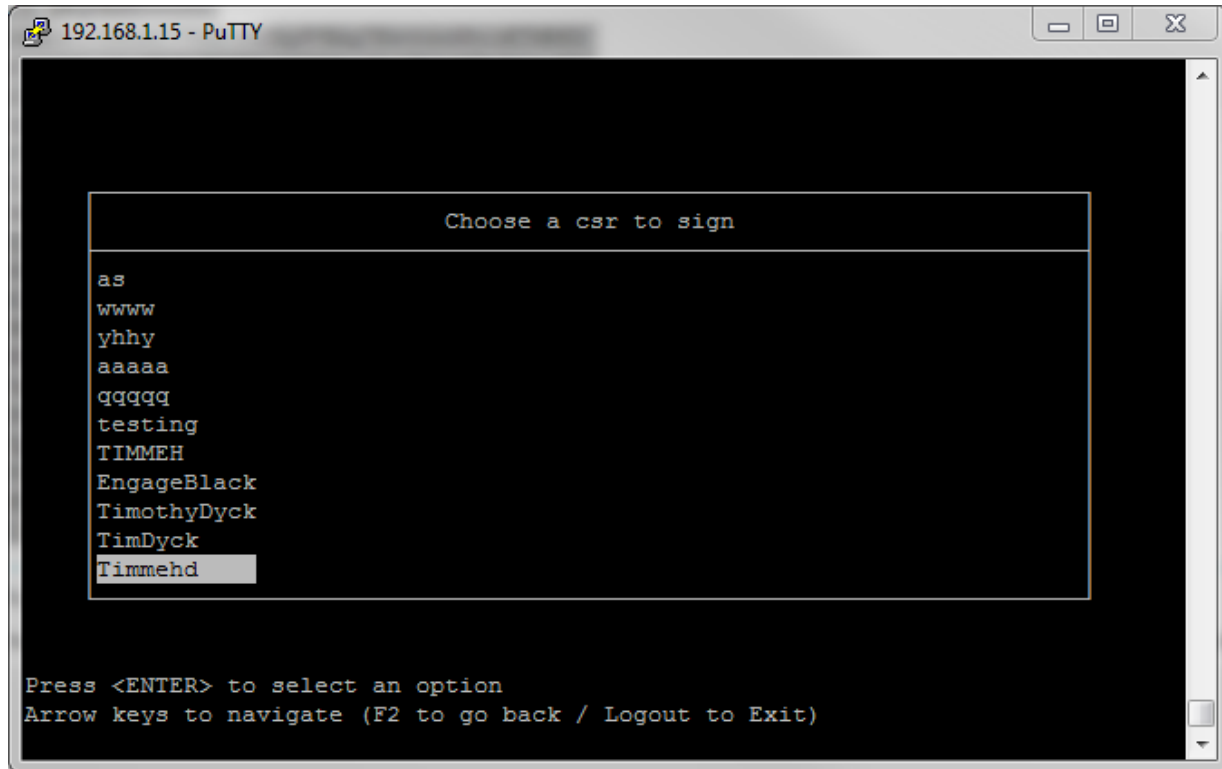
The screenshot shows a PuTTY terminal window titled "192.168.1.15 - PuTTY". The terminal displays a menu for the Black Vault CA. At the top, it says "***Welcome to the Black Vault CA***". Below this, there are two columns of text. The left column lists menu options: "Create Certificate Request", "Create Certificate" (which is highlighted with a grey bar), "CA Utilities", "Server Utilities", "System Commands", "Information", "Revoke Certificate", "Show Certificates and Status", "Show CA Certificates", and "Logout". The right column displays system information: "Date: 2017-11-27", "Time: 15:53:02", "SSH Port: 22", "Version: 09.00.05", and "Firewall: Off". At the bottom of the terminal, there are instructions: "Press <ENTER> to select an option" and "Arrow keys to navigate (F2 to go back / Logout to Exit)".

```
***Welcome to the Black Vault CA***

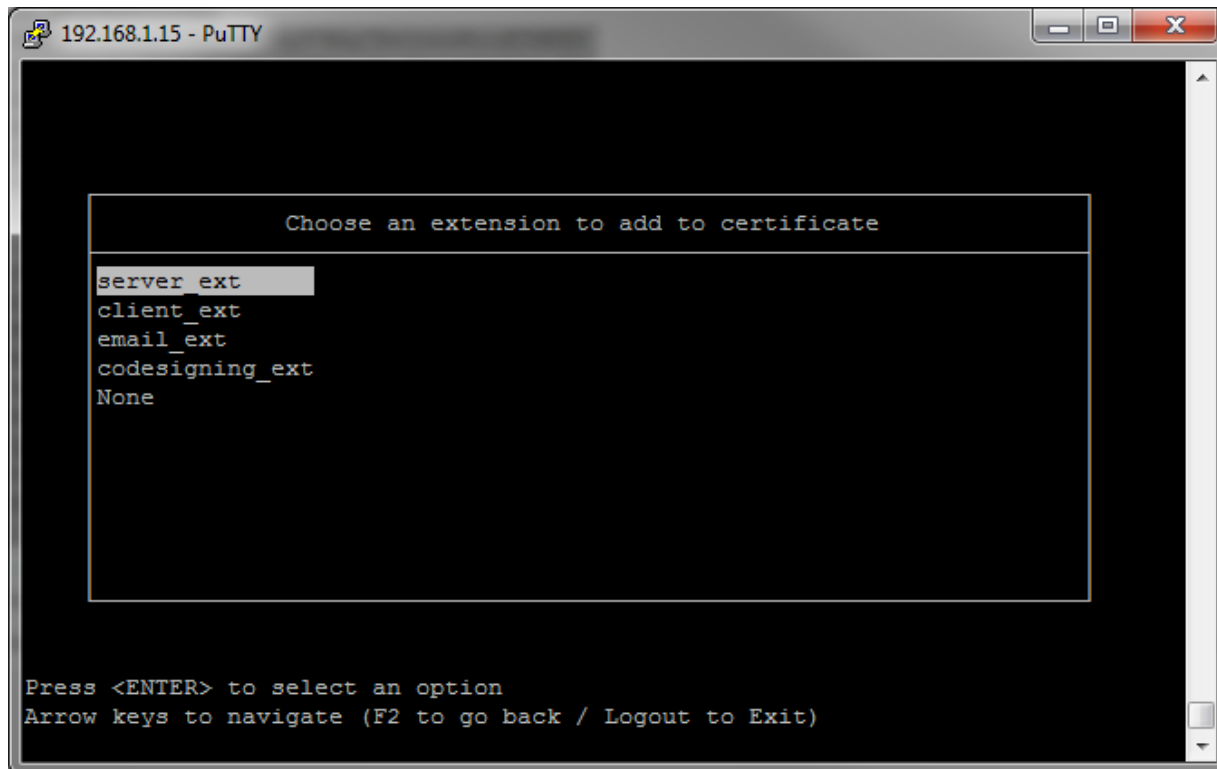
Create Certificate Request          Date: 2017-11-27
Create Certificate                  Time: 15:53:02
CA Utilities                       SSH Port: 22
Server Utilities                   Version: 09.00.05
System Commands                    Firewall: Off
Information
Revoke Certificate
Show Certificates and Status
Show CA Certificates
Logout

Press <ENTER> to select an option
Arrow keys to navigate (F2 to go back / Logout to Exit)
```

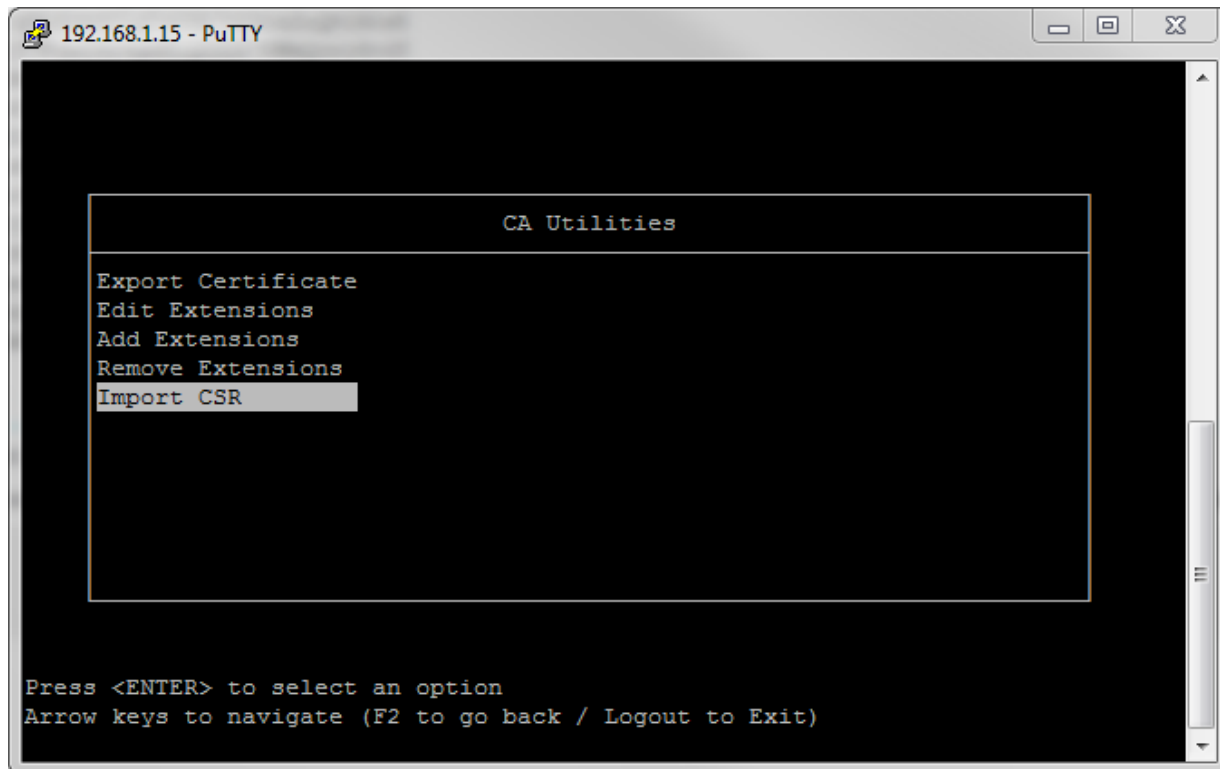
6. Select the Common Name of the CSR you wish to sign



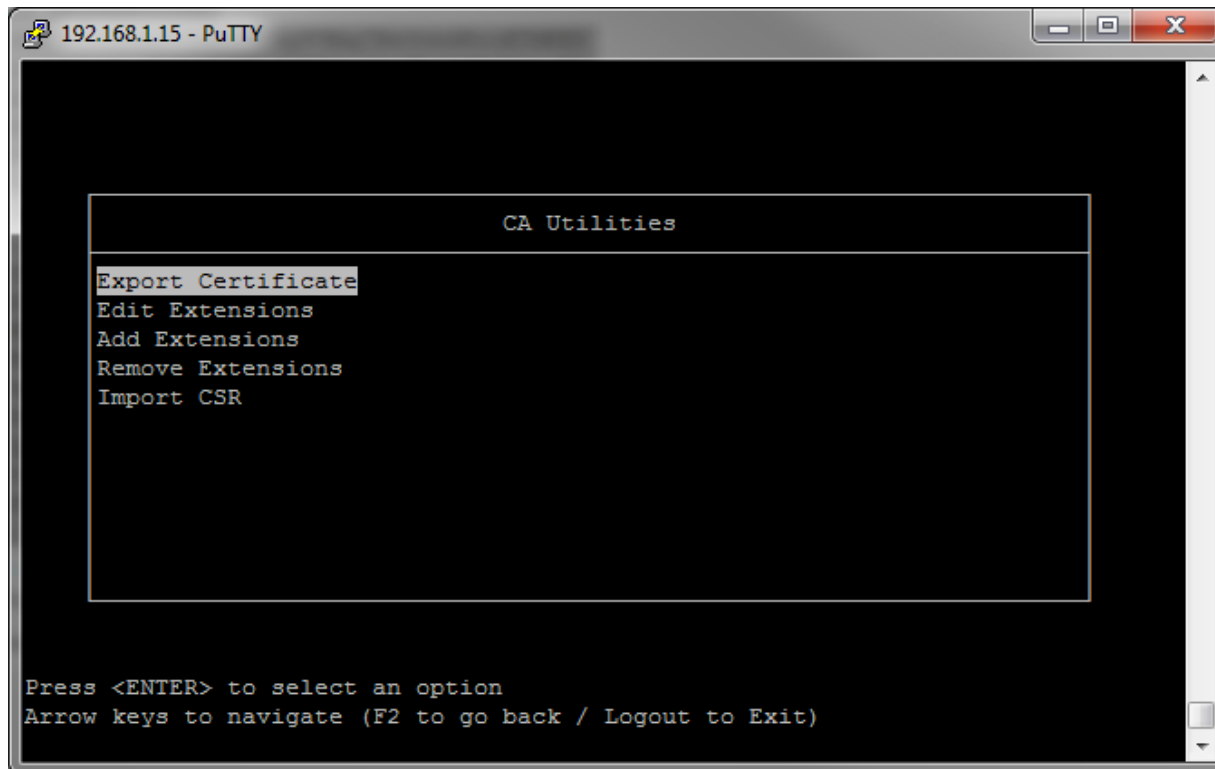
7. Select None when asked for extension type



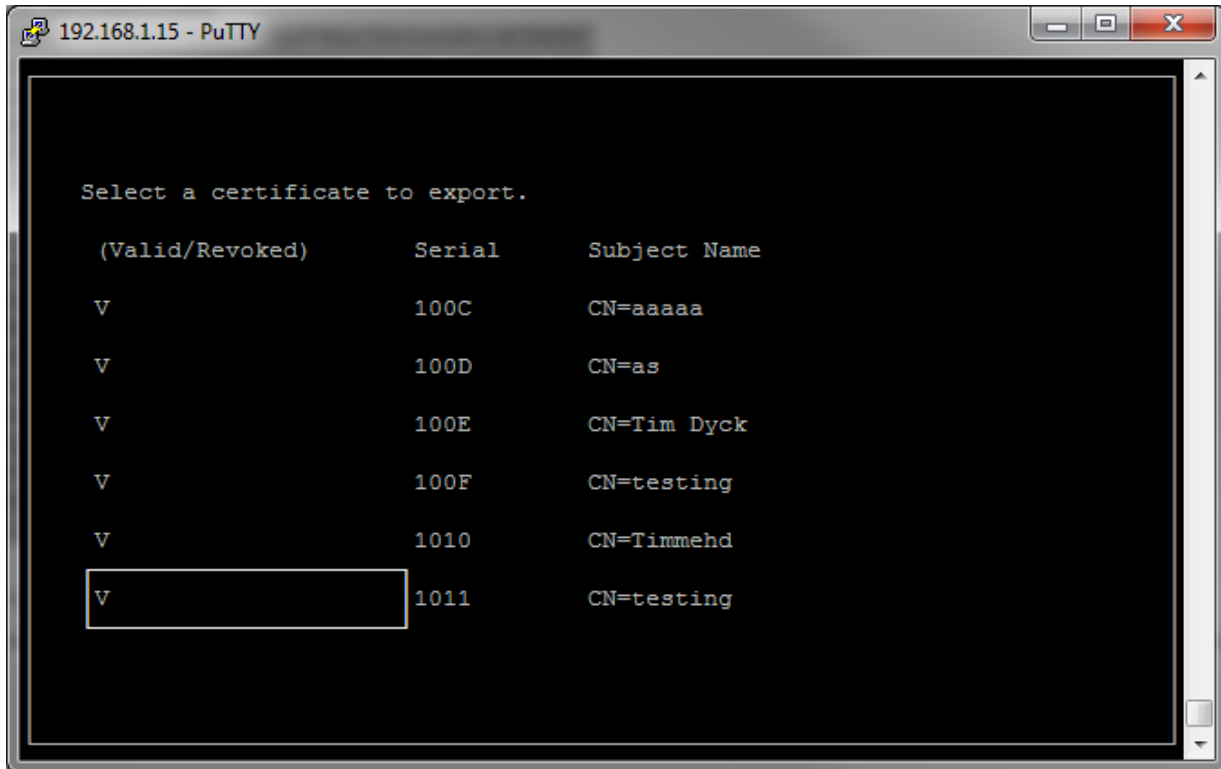
8. Back out to the main Menu and Select CA Utilities



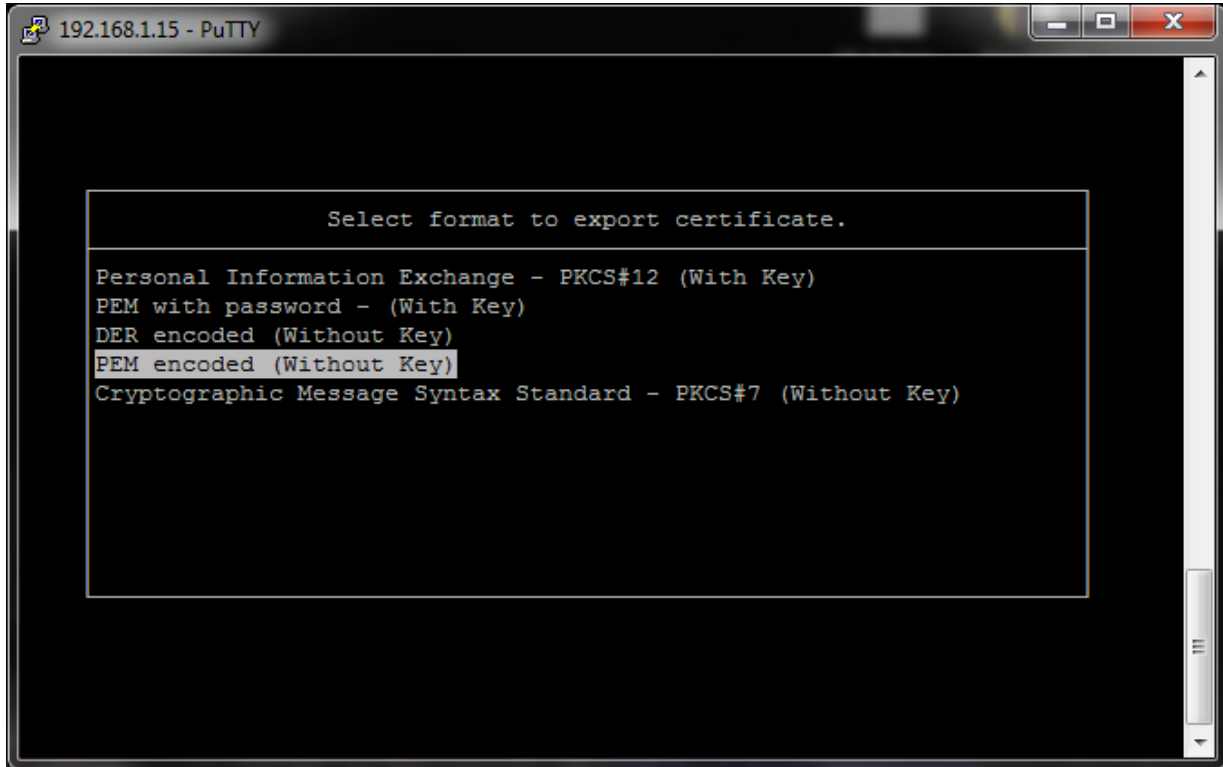
9. Select Export Certificate



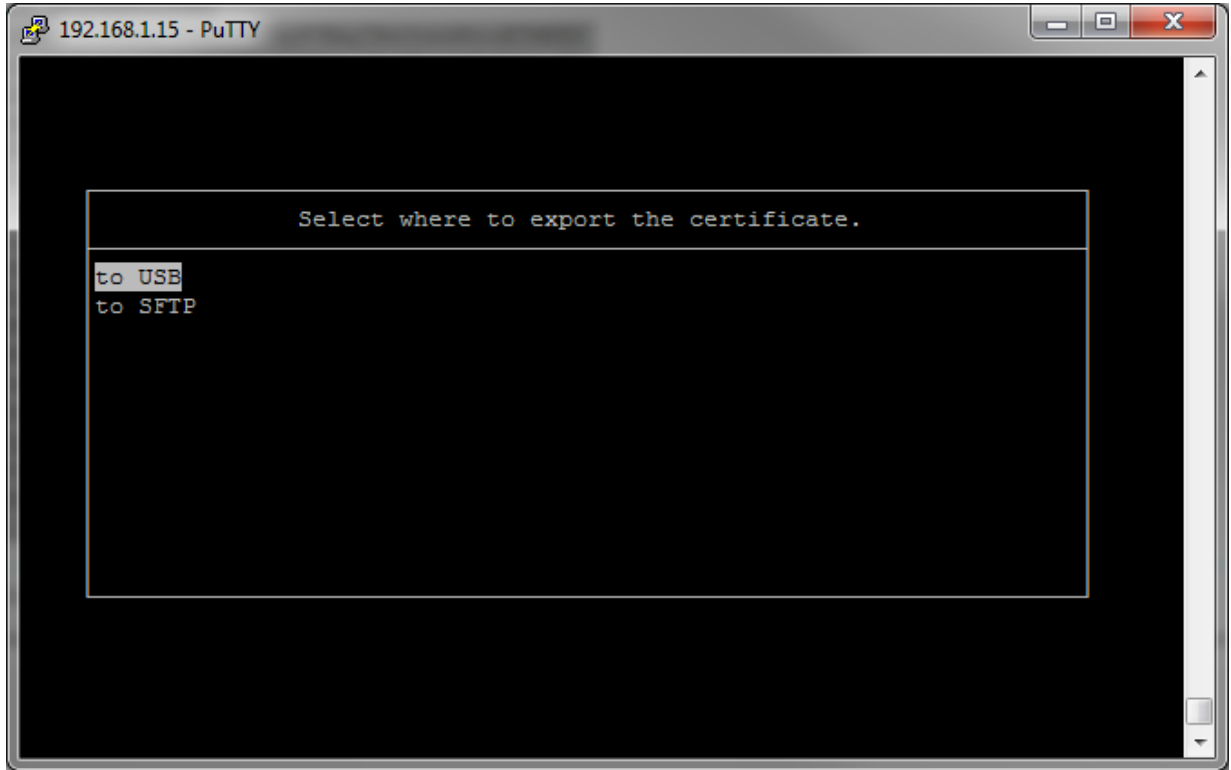
10. Select the Certificate that you just created



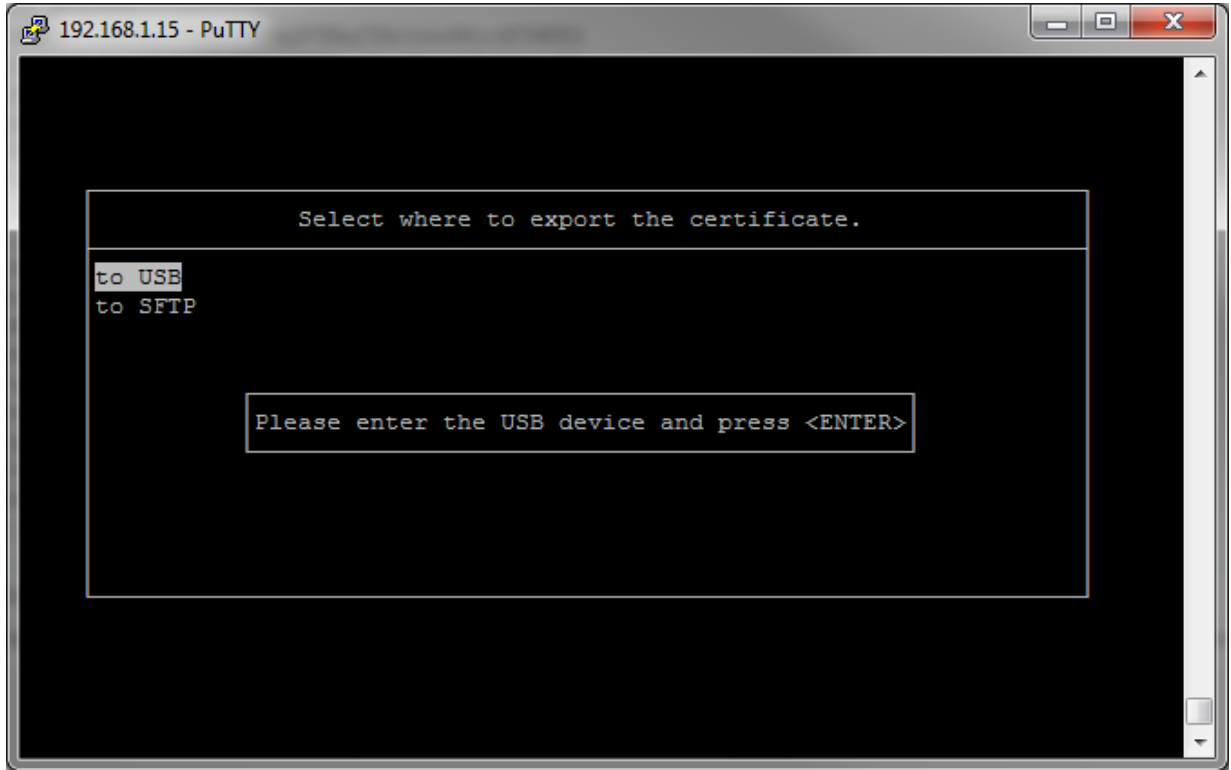
11. Select PEM encoded (Without Key)



12. Select To USB



13. Insert a flash drive to the BlackVault CA and press enter

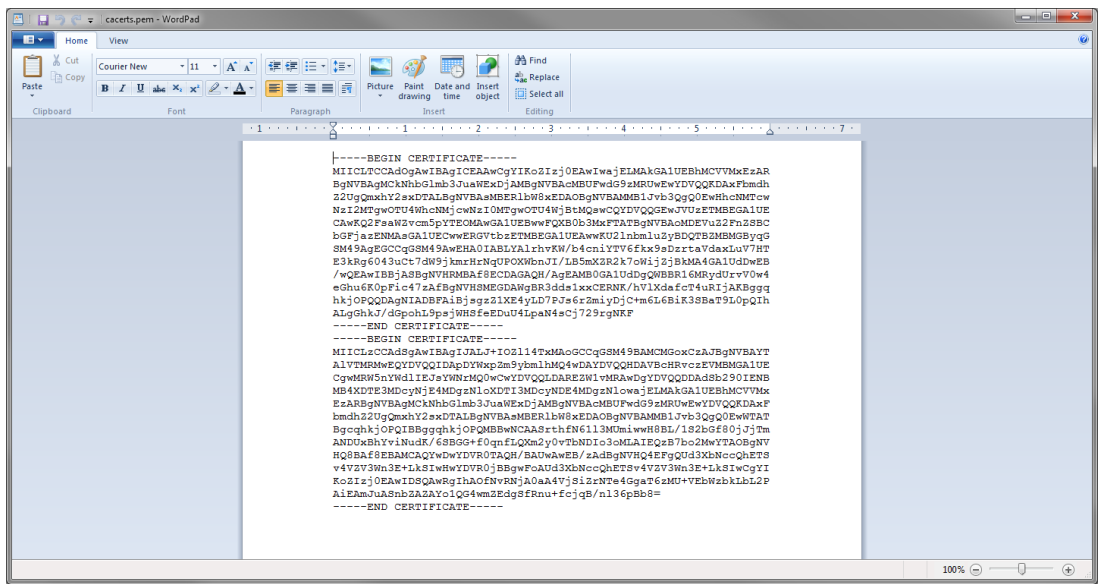


Obtaining the CA certificates

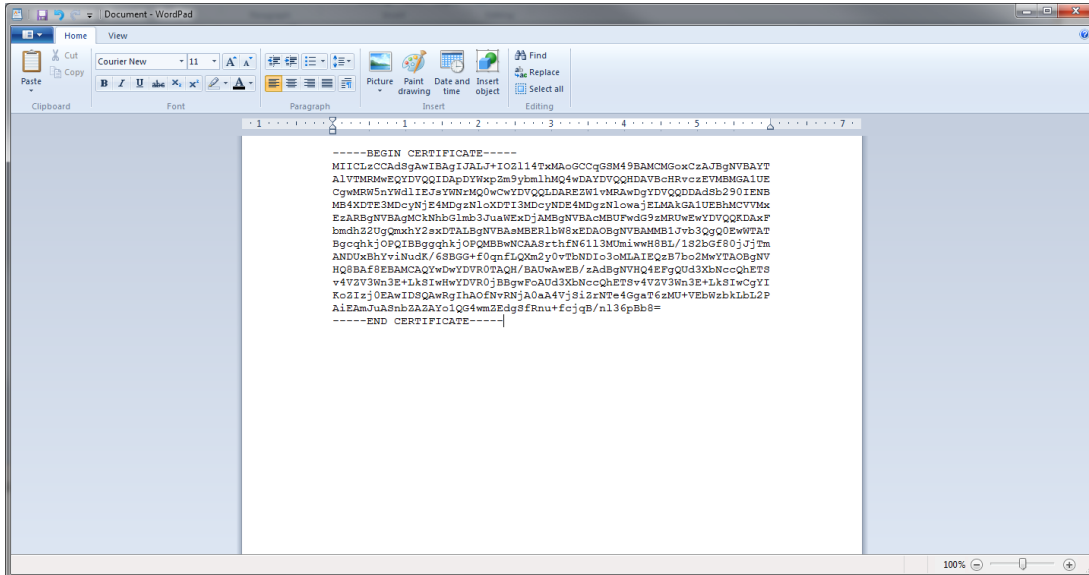
1. On a client computer load the website : IP_Address_Of_BVCA/cacerts.pem



2. Open the downloaded cacerts.pem in wordpad



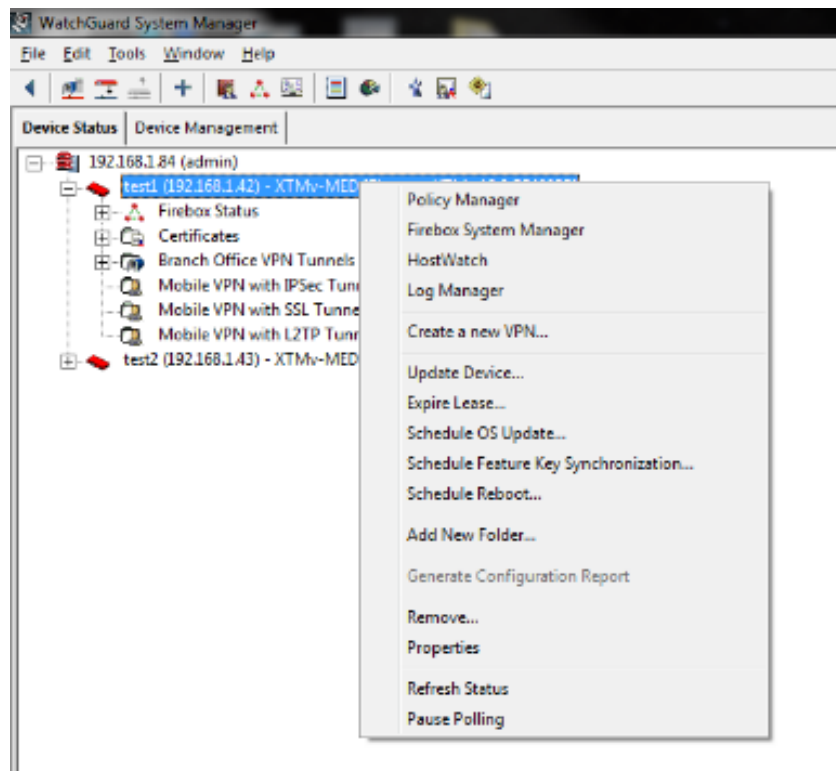
3. Cut the first certificate and in a new document paste it. Save this one as Signing.crt



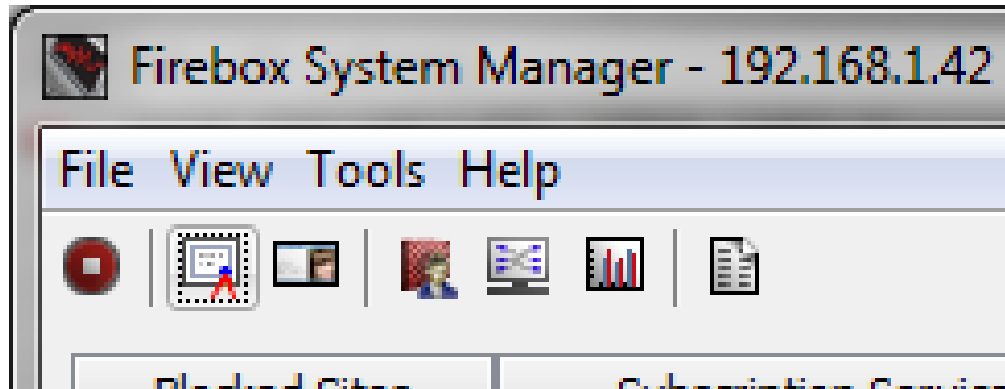
4. Save the remainder as root.crt

Importing the Certificates into Firebox

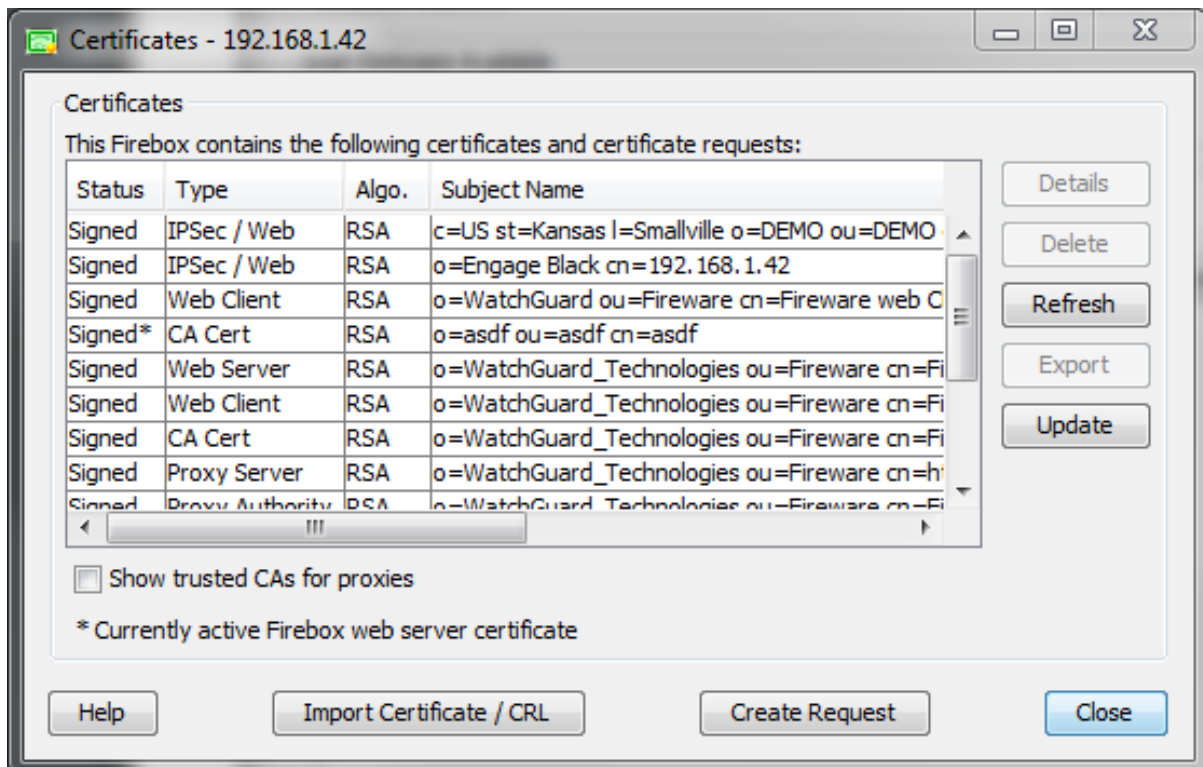
1. From the WatchGuard System Manager, open the system manager



2. In the Firebox System Manager, click the Certificates Button

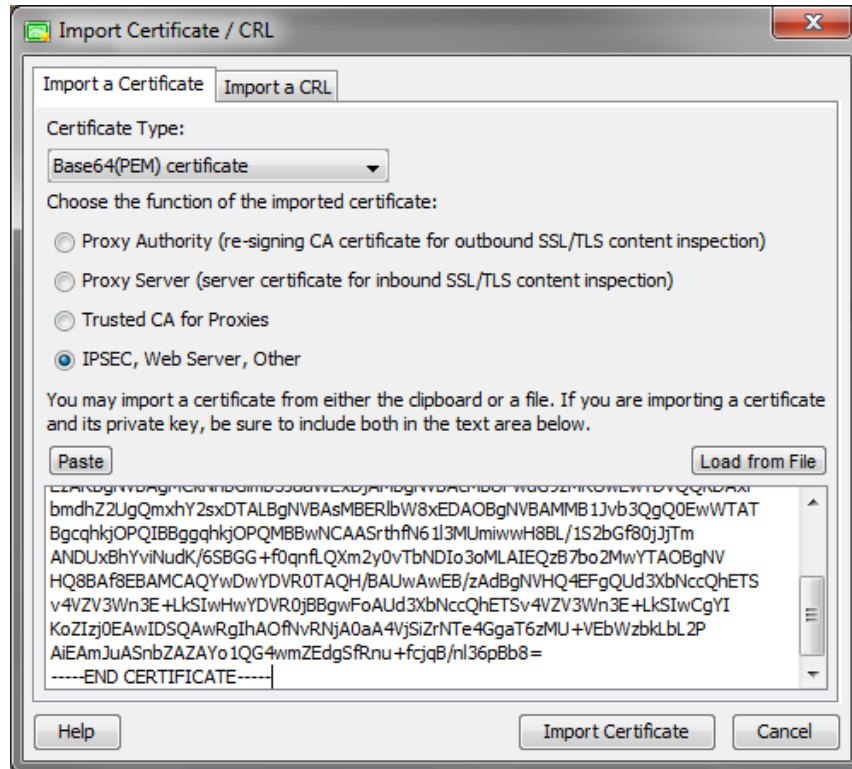


3. In the Certificates window, click Import Certificate/CRL Button

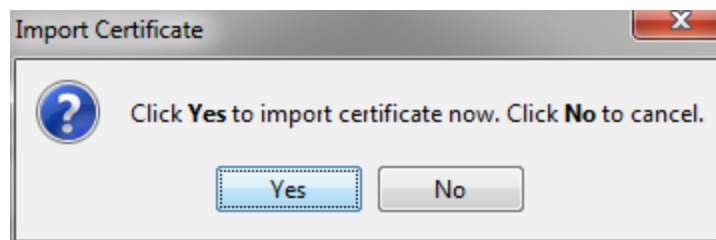


4. Click Import Certificate/CRL

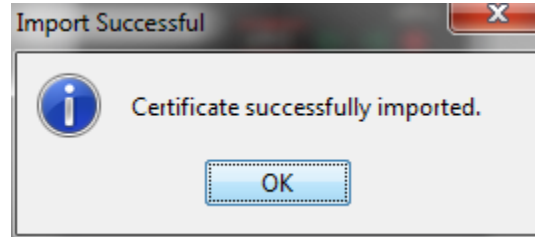
5. In the Import Certificate/CRL window



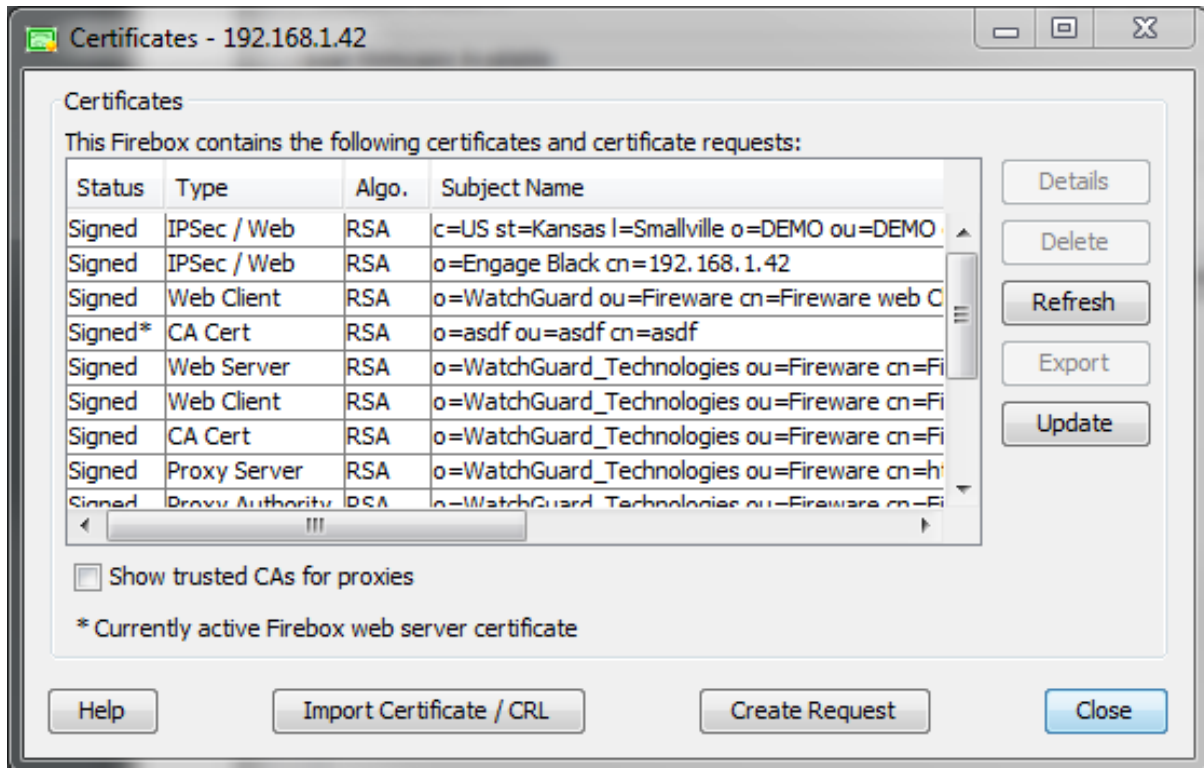
- Under Choose the function of the imported certificate, select the IPSEC, Web Server Other radio button
- Under Certificate File Click Choose file, then browse to where you saved Root.crt.
- Click Import Certificate
- An Import Certificate window will then appear, click Yes



- e. An Import Successful window next appears, click Yes

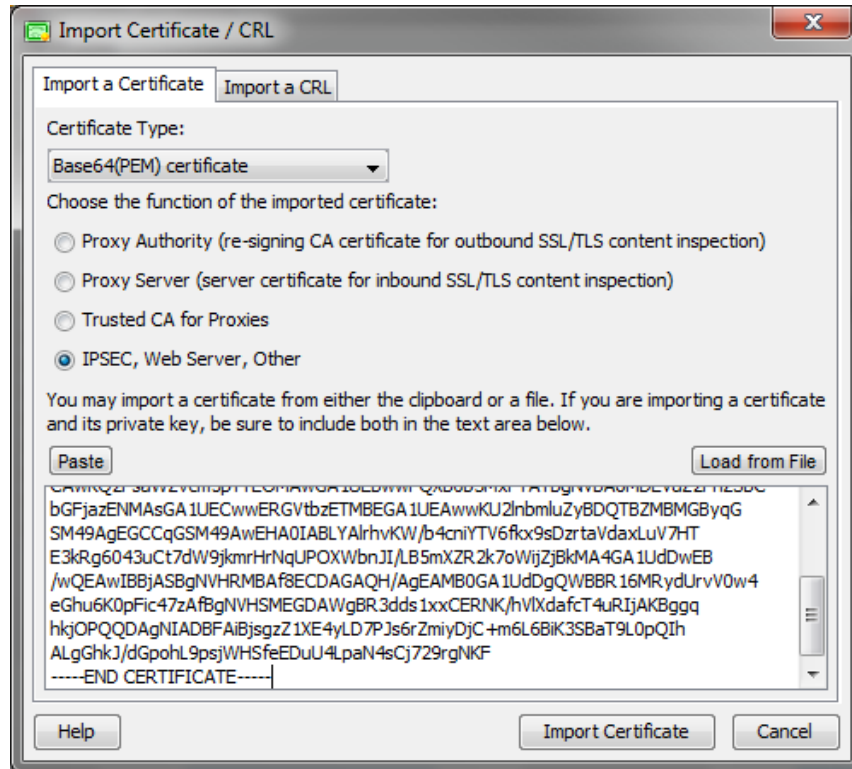


- 6. The Certificates windows will appear again, click Import Certificate/CRL Button

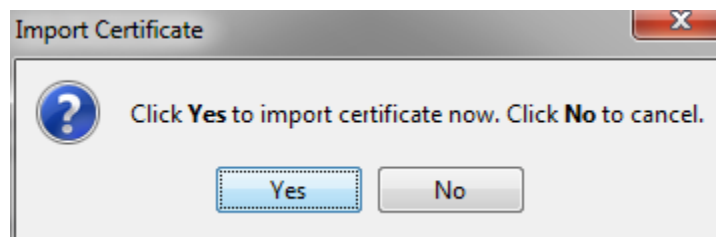


- 7. Click Import Certificate/CRL

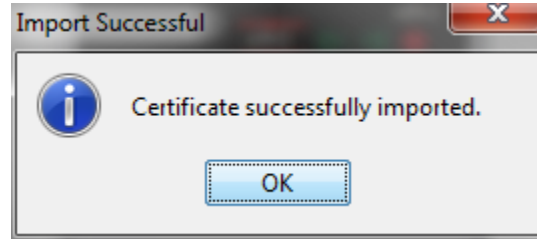
8. In the Import Certificate/CRL window



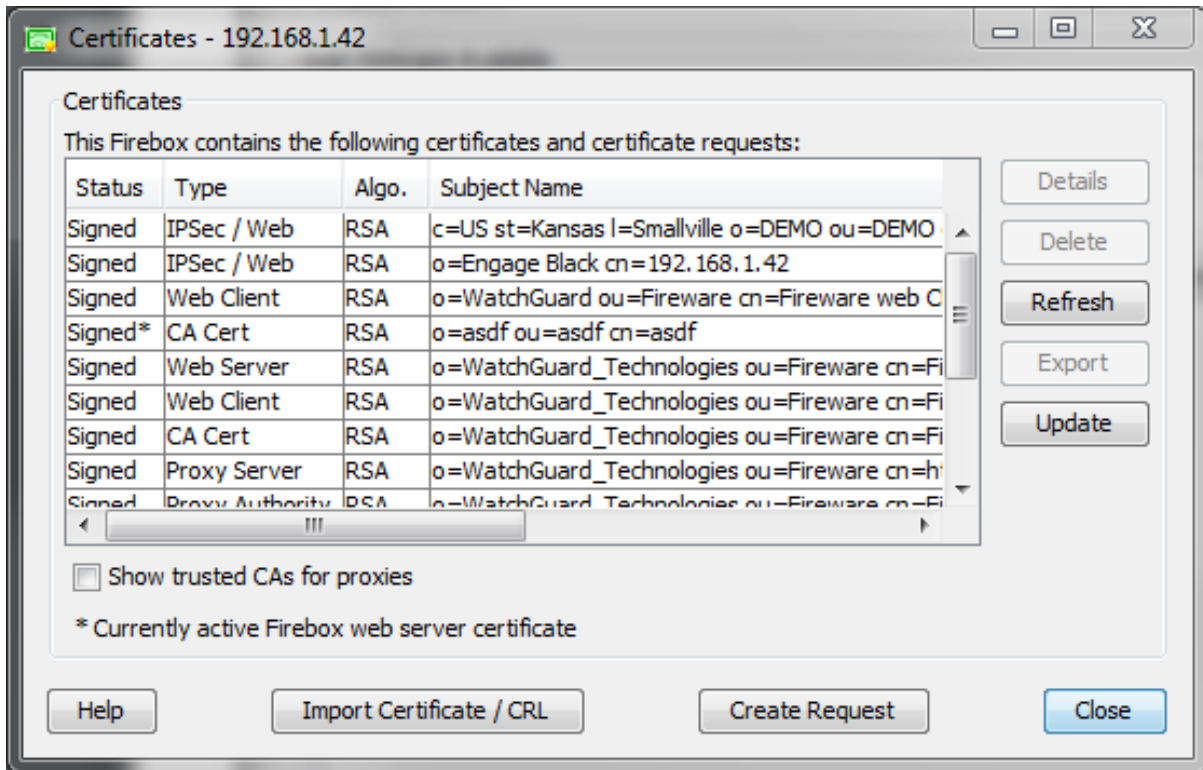
- Under Choose the function of the imported certificate, select the IPSEC, Web Server Other radio button
- Under Certificate File Click Choose file, then browse to where you saved Signing.crt.
- Click Import Certificate
- A Import Certificate window will then appear, click Yes



- e. An Import Successful window next appears, click Yes

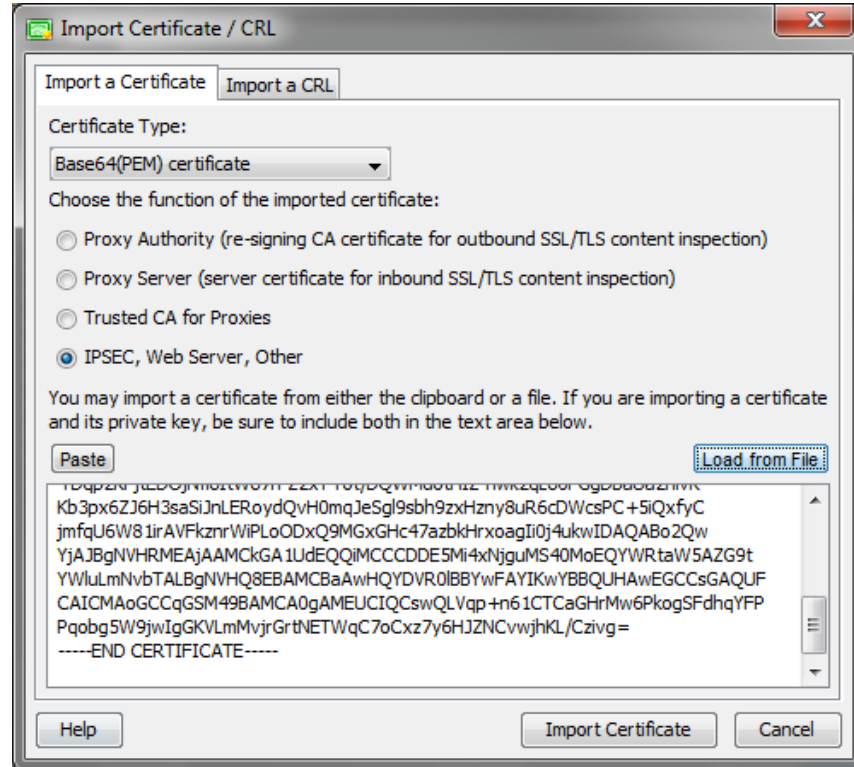


- 9. The Certificates windows will appear again, click Import Certificate/CRL Button

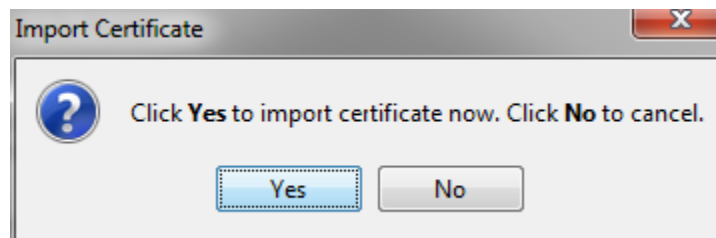


- 10. Click Import Certificate/CRL

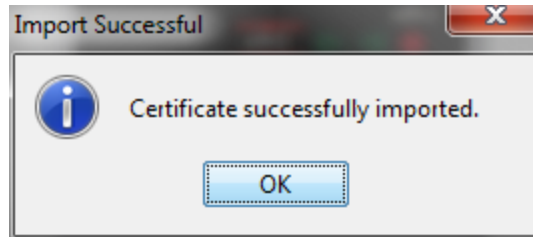
11. In the Import Certificate/CRL window



- Under Choose the function of the imported certificate, select the IPSEC, Web Server Other radios button
- Under Certificate File Click Choose file, then browse to where your flash drive and select the Certificate you exported from the BlackVault.
- Click Import Certificate
- A Import Certificate window will then appear, click Yes



- j. An Import Successful window next appears, click Yes



Site B

Repeat Process stated in site a for site b.

Setting up VPN

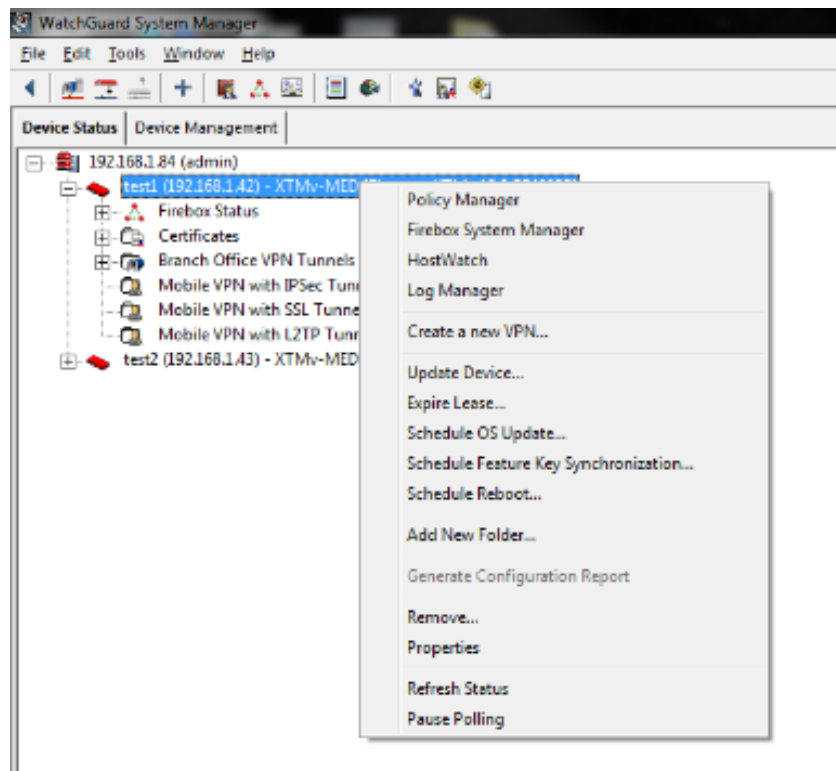
Before setting up the VPN the following information should be collected

- Site A and B external IP addresses
- Site A and B internal network IP addresses
- Site A and B X.500 Distinguished Names from their certificates
 - This can also be known as the Subject name.

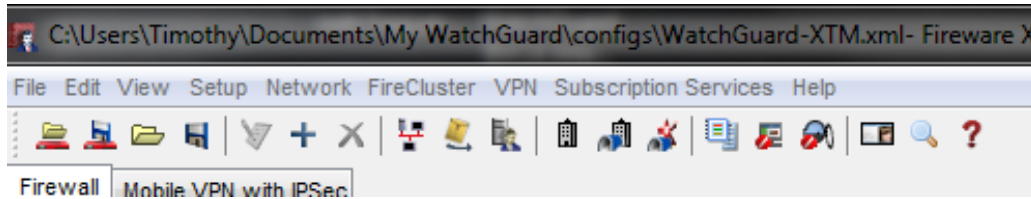
Site A

Configuring VPN

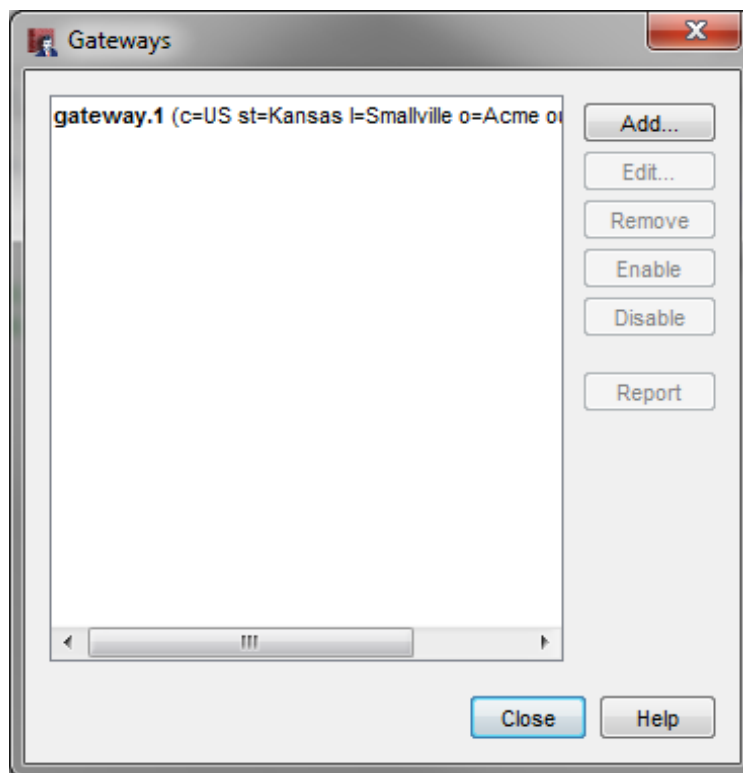
1. From the WatchGuard System Manager open the Policy Manager.



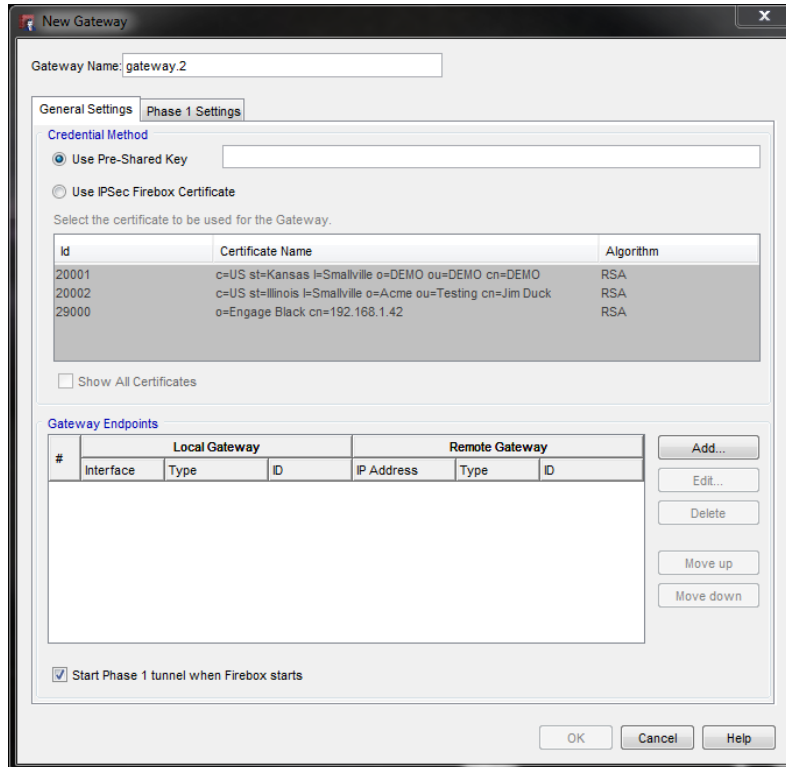
2. In the Policy Manager, click Branch Office Gateways



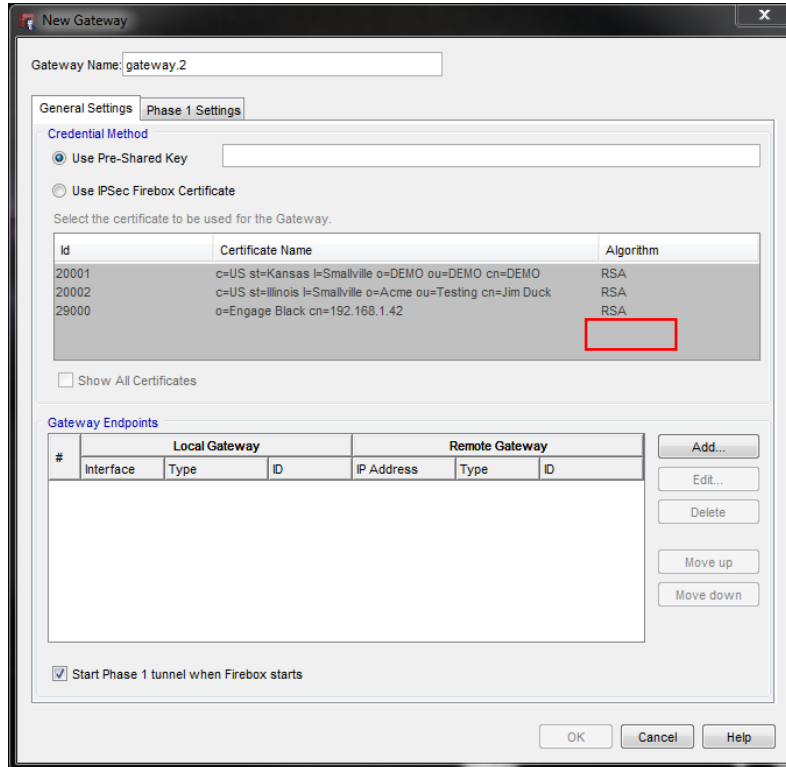
3. In the Gateways window, click add



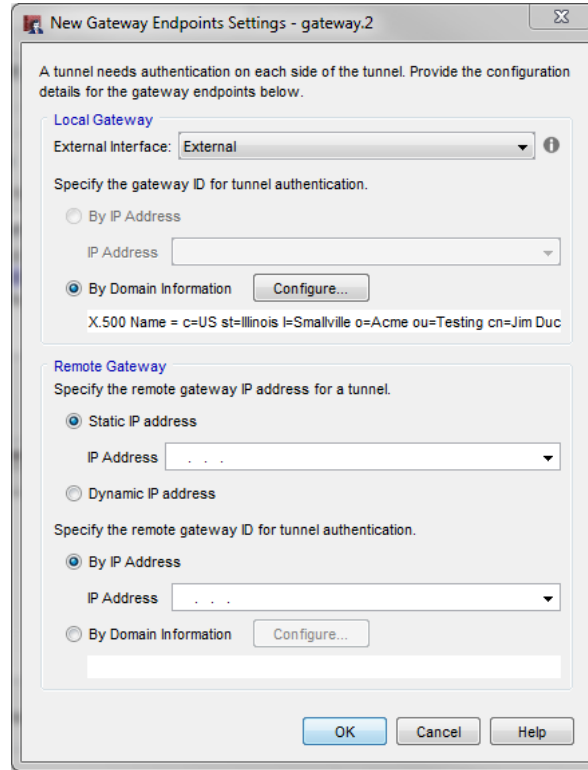
4. In the New Gateway window select the radio button that says, "Use IPsec Firebox Certificate" then select the certificate that was just generated



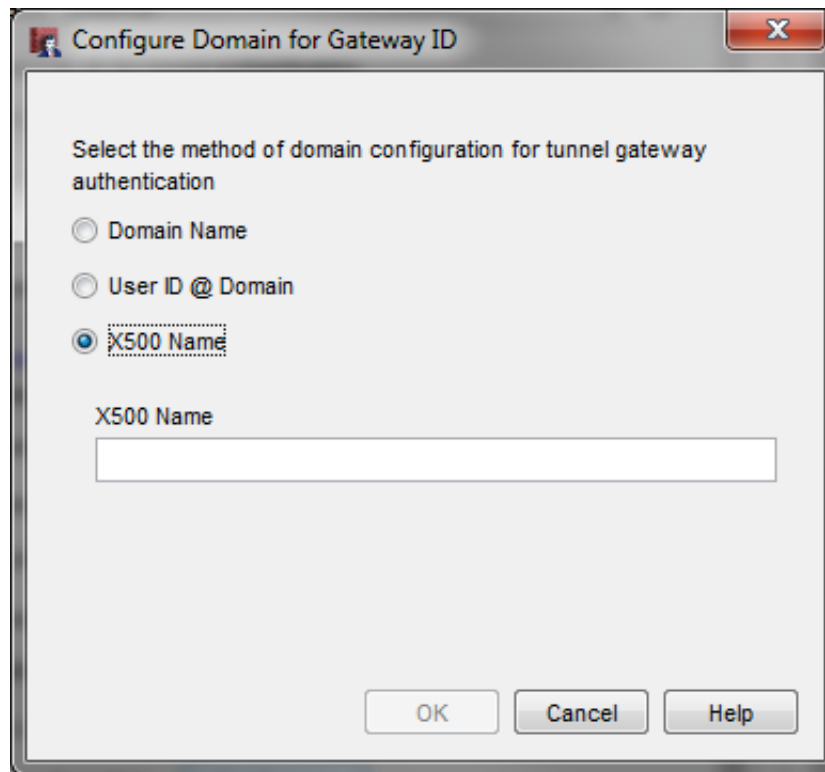
5. In the bottom half of the New Gateway window, under Gateway Endpoints click add



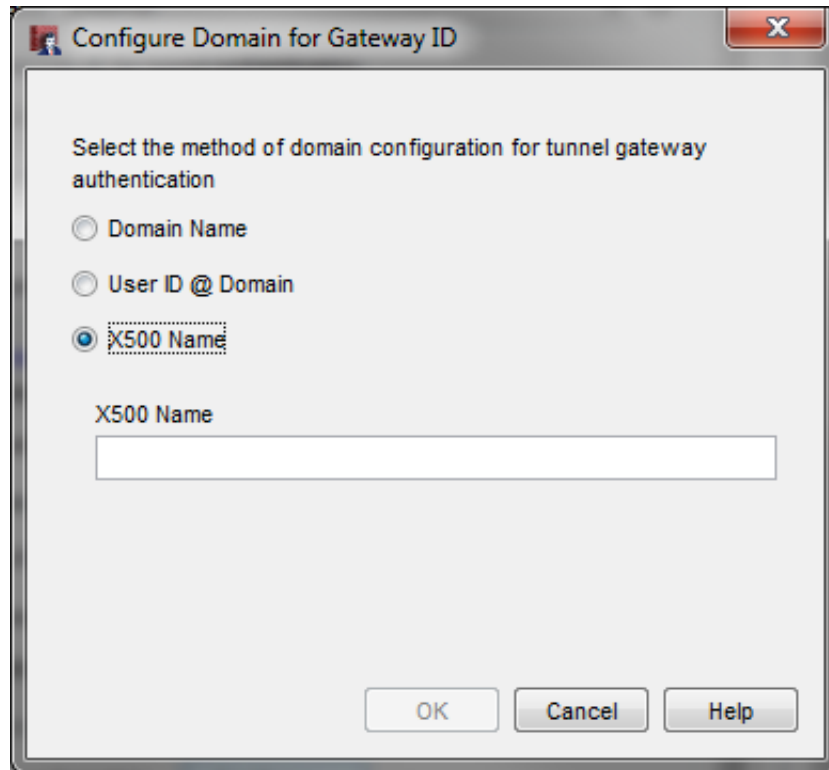
6. In the New Gateway Endpoints Settings Windows, do the following:



- a. In the Local Gateway subsection, Select the By Domain Information radio button, then click Configure
 - i. In the Configure Domain for Gateway ID window Select the X500 Name radio button the click OK

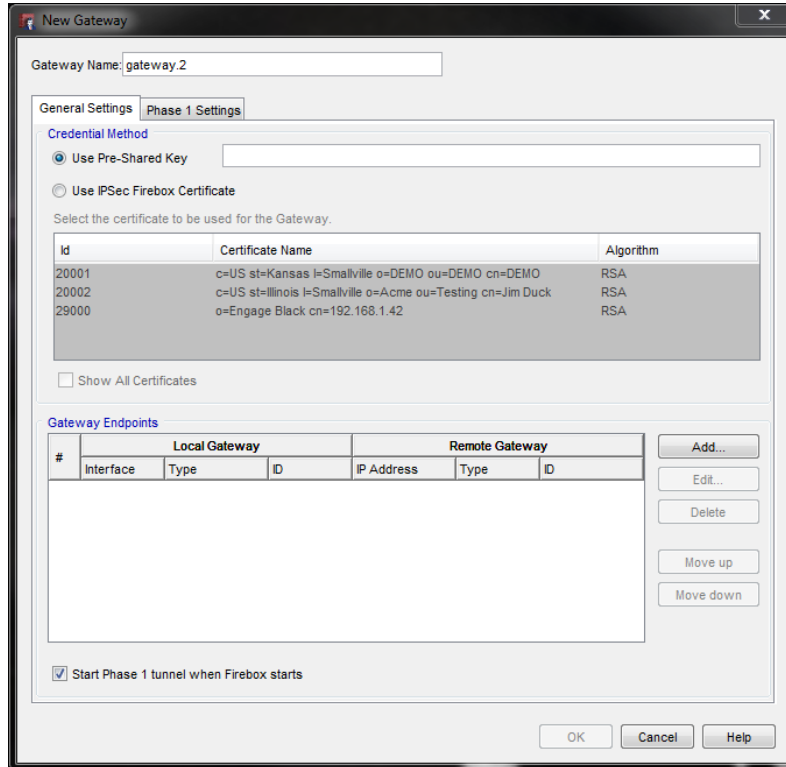


- b. In the Remote Gateway subsection, Select the Static IP Address radio button, then enter the IP Address of the remote gateway.
- c. Under Specify the remote gateway ID for tunnel authentication select the By Domain Information the click Configure
 - i. In the Configure Domain for Gateway ID select the X500 Name radio button then add in the X500 name of the certificate of the Site B then press OK

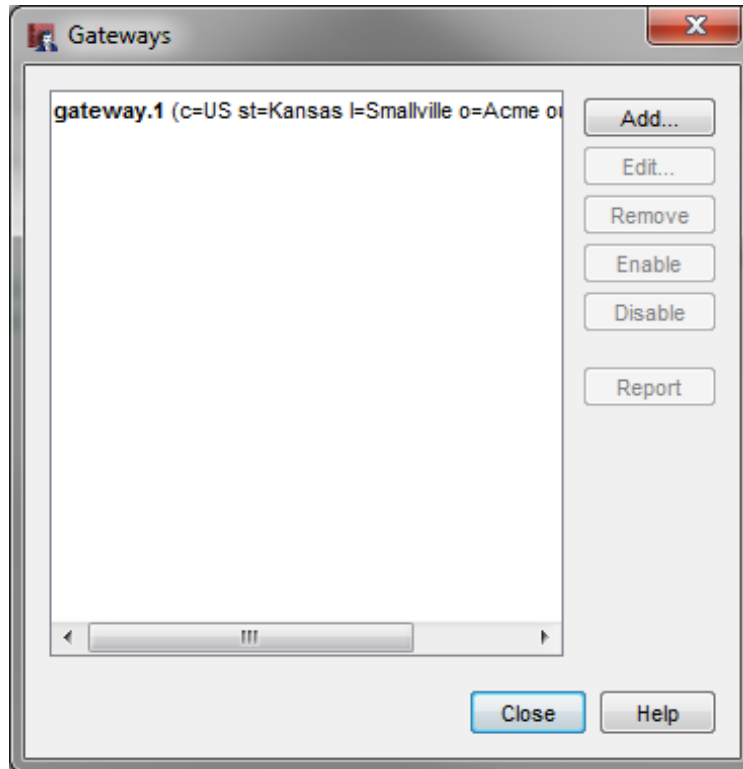


- d. In the New Gateway Endpoint Settings window click OK

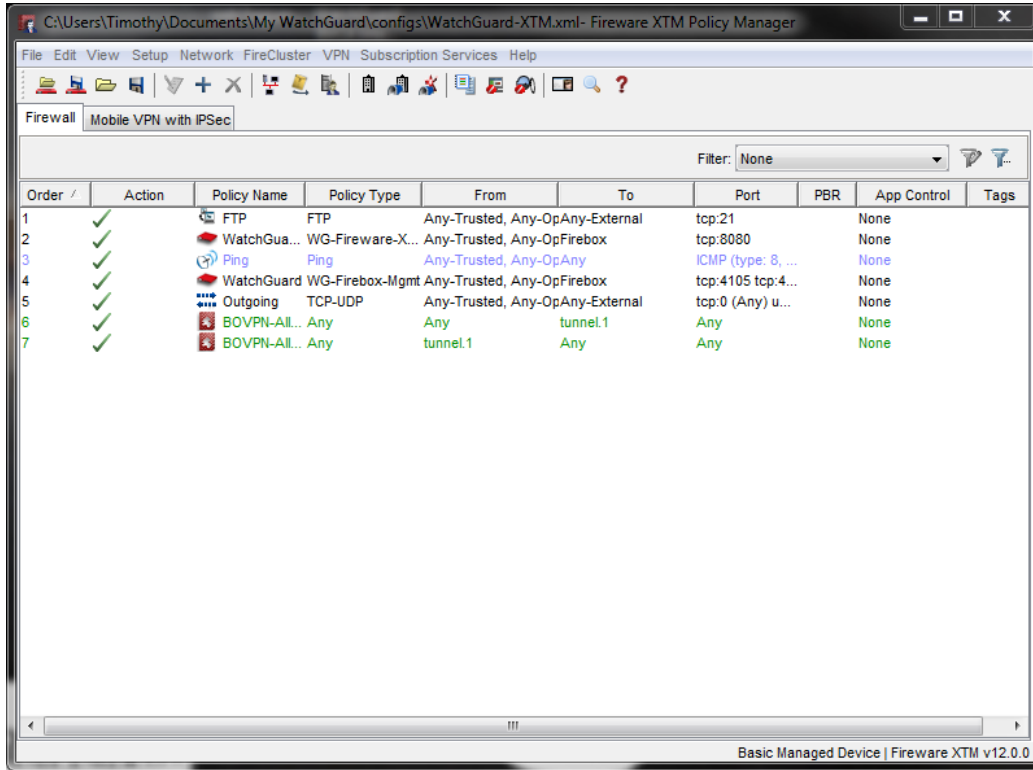
7. In the New Gateway window click OK



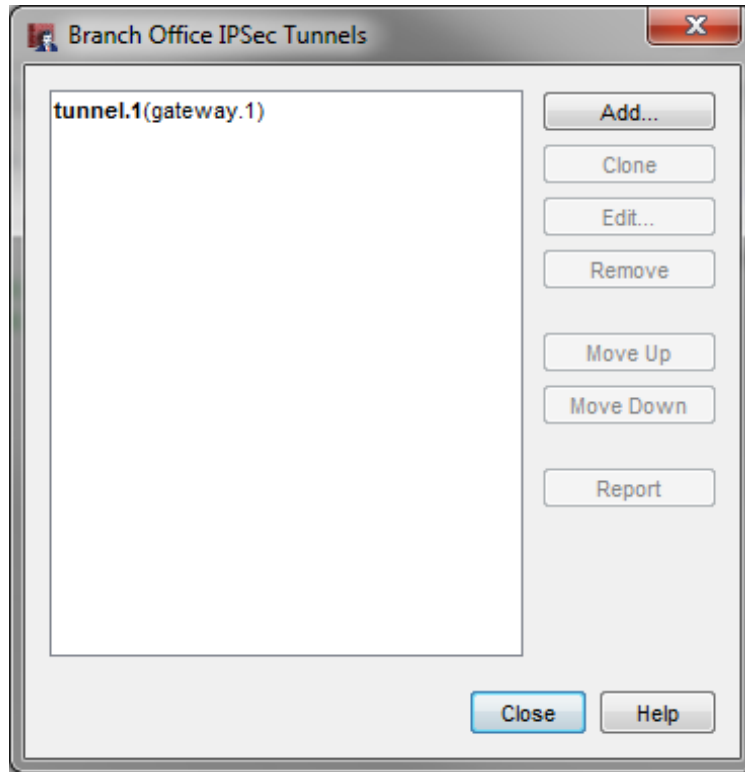
8. In the Gateways window click Close



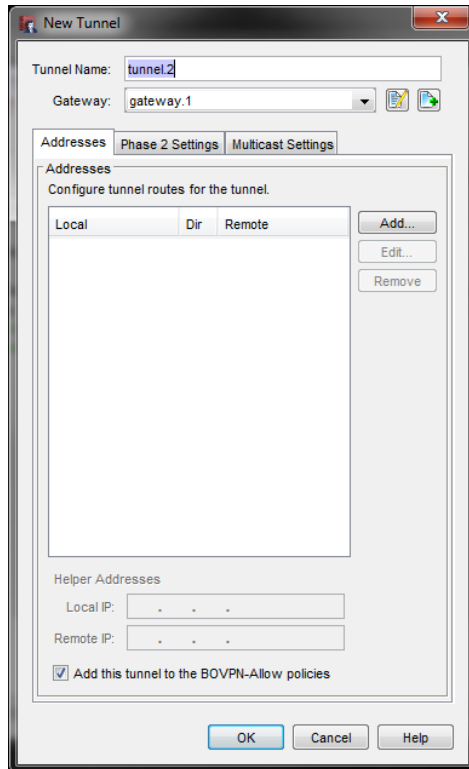
9. In the Policy Manager, click Branch Office Tunnels



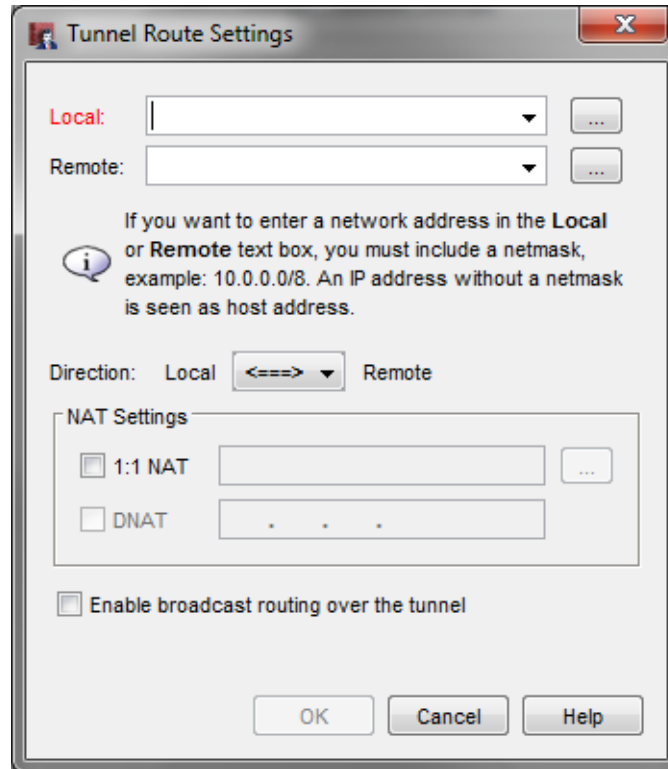
10. In the Branch Office IPsec Tunnels window click Add



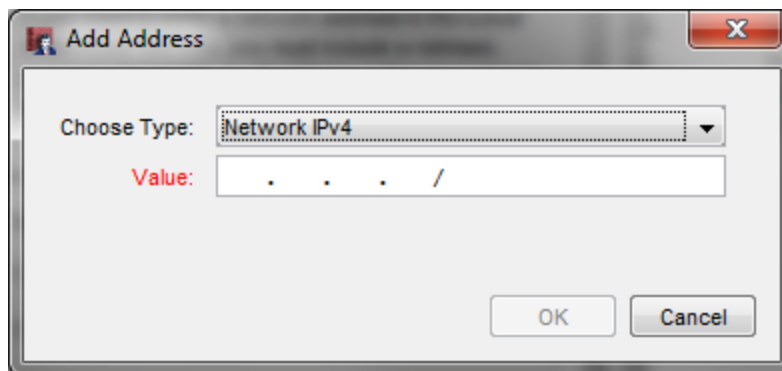
11. In the New Tunnel window do the following:



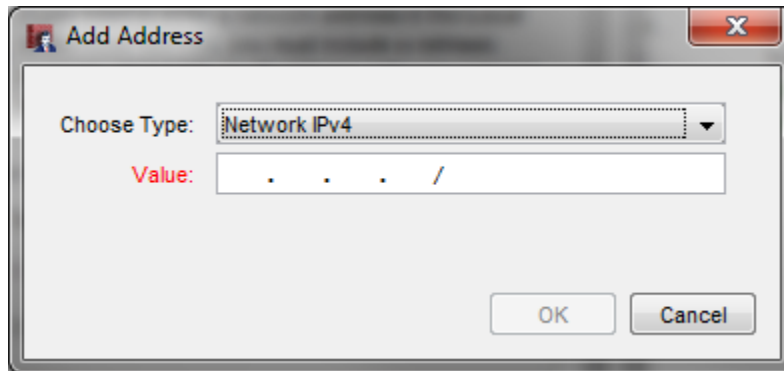
- a. In the Address Tab click the Add button



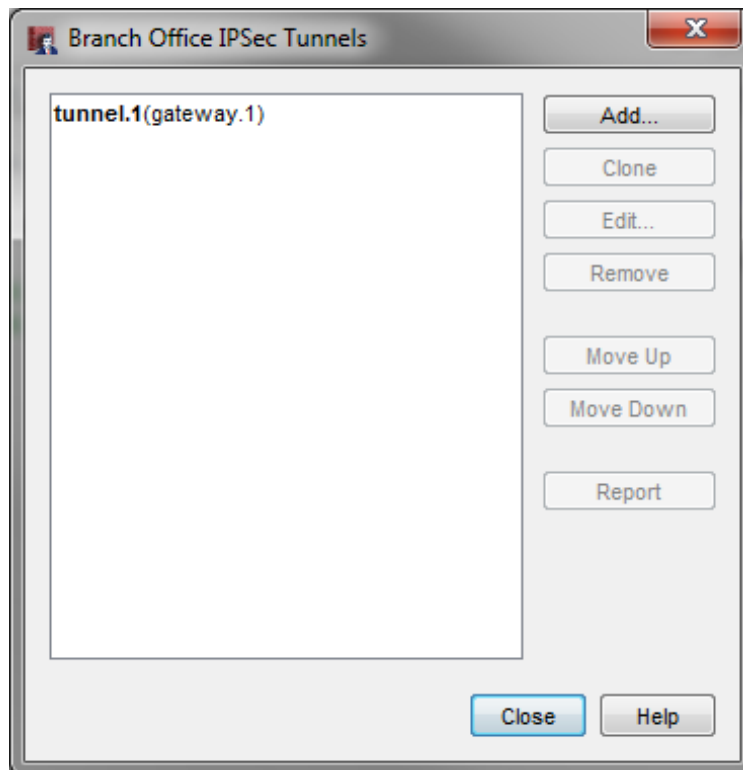
- i. In the tunnel Route Settings window click the ellipse next to Local
 1. In the Add Address window
 - a. Under "Choose Type" select Network IPv4
 - b. Under "Value" add in the local network
 - c. Press Ok



- ii. In the tunnel Route Settings window click the ellipse next to Remote
 1. In the Add Address window
 - a. Under “Choose Type” select Network IPv4
 - b. Under “Value” add in the remote network
 - c. Press Ok



- b. In the New Tunnel Window, leave everything else in the other tabs then click OK
- c. In the Branch Office IPsec Tunnels window click Close





Engage BlackVault CA WatchGuard Integration Guide

Site B

Repeat Process stated in Site A for Site B