TechNote

SonicOS

How to Install and Request a Certificate

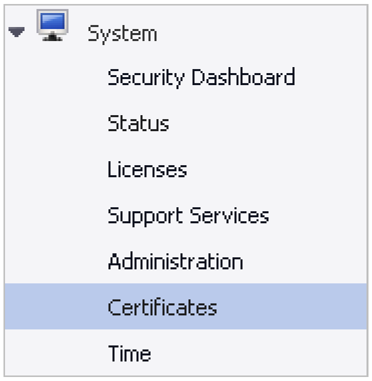
Introduction

This document contains procedures on how to:

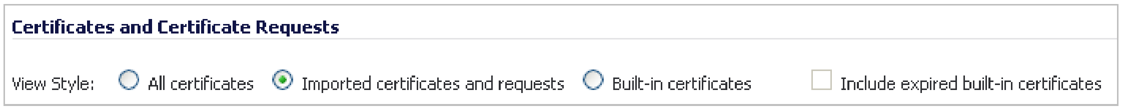
- Install CA Certificates (Trust Anchors and Intermediate CA Certificates).
- Request an End-Entity (Local) Certificate from a CA.
- Install an End-Entity Certificate.

Installing CA Certificates (Trust Anchors and Intermediate CA Certificates)

1. Log into SonicWALL Network Security Appliance portal. Navigate to **System > Certificates**.



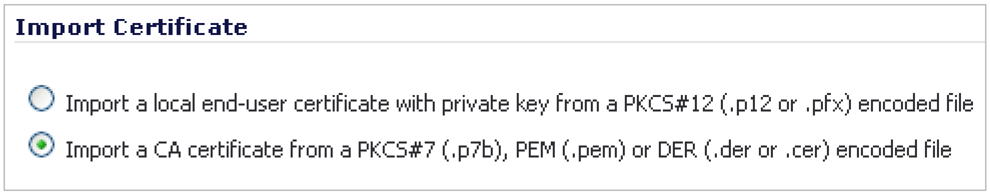
2. Select **Imported certificates and requests** from the View Style radio buttons.



Certificates and Certificate Requests

View Style: ○ All certificates ● Imported certificates and requests ○ Built-in certificates □ Include expired built-in certificates

3. Click **Import** and select **Import a CA certificate…** in the newly opened window.

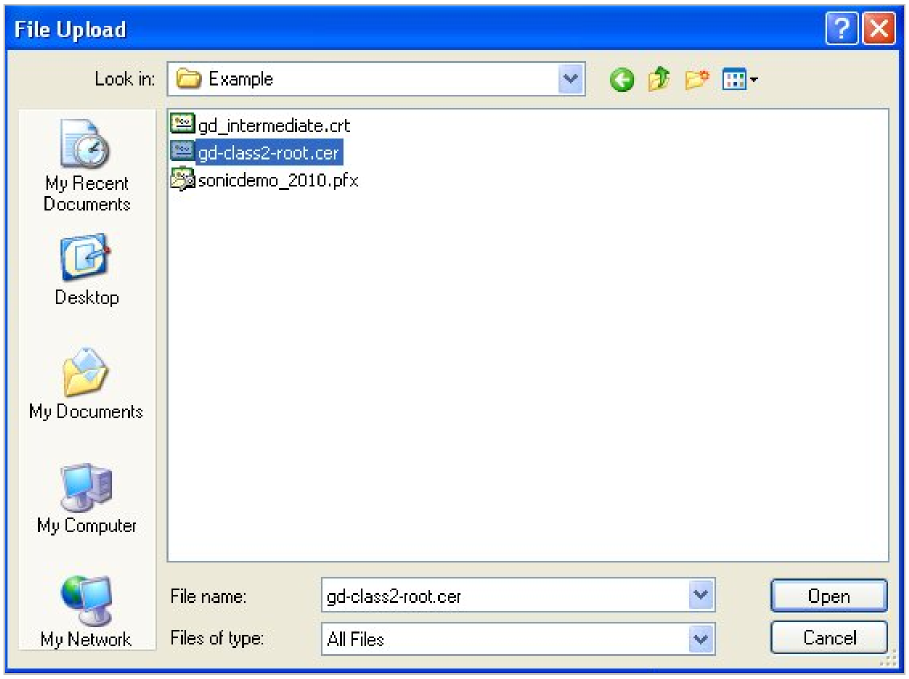


Import Certificate

○ Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file

● Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file

4. Click **Browse** to find and select your certificate.



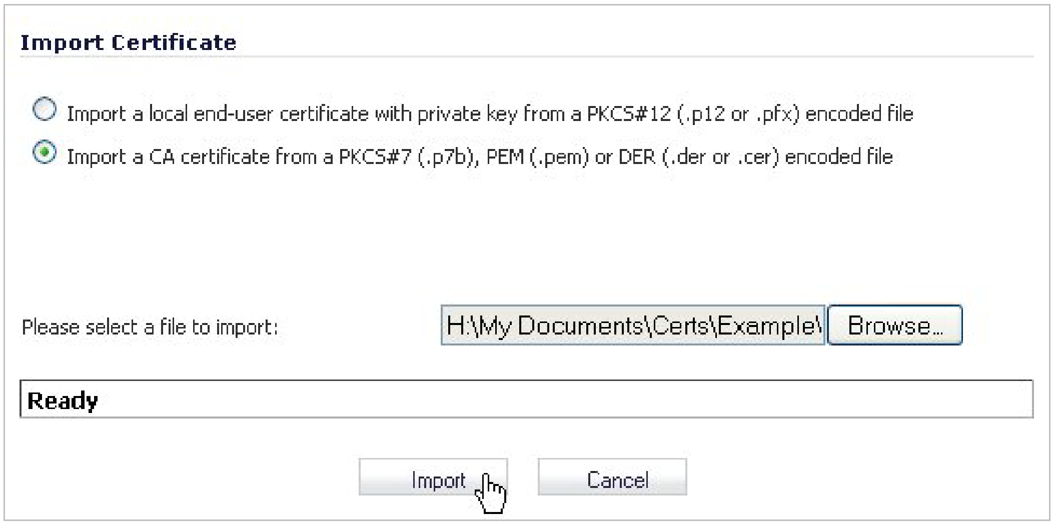
File Upload

Look in: Example

gd_intermediate.crt
gd-class2-root.cer
sonicdemo_2010.pfx

File name: gd-class2-root.cer
Files of type: All Files

5. After your certificate has been selected, click **Import**.



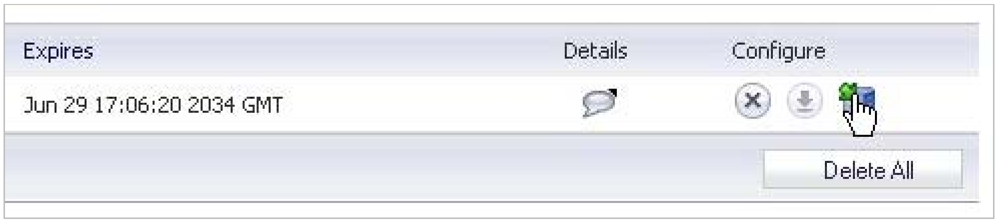
Import Certificate

○ Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file
● Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file

Please select a file to import: H:\My Documents\Certs\Example\

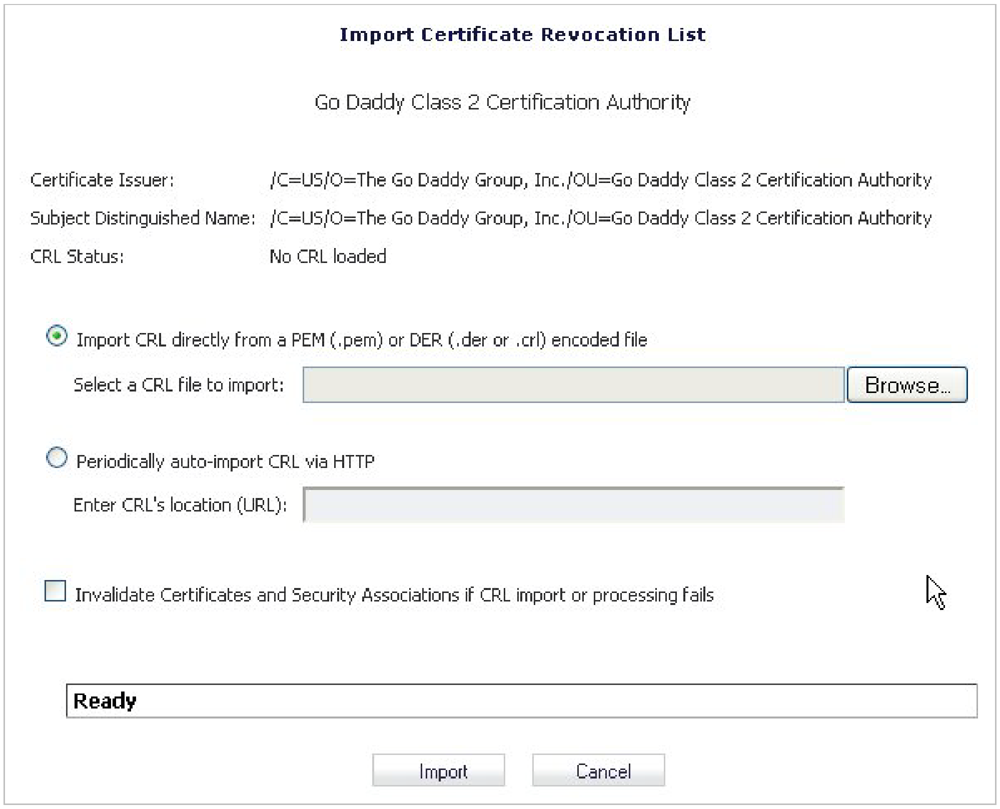
Ready

6. The imported certificate will appear with a green arrow icon next to it in the Configure column. If desired, click the **green arrow** to import a CRL.



Expires	Details	Configure
Jun 29 17:06:20 2034 GMT		

You will have the option to import a .PEM or .DER file, or point to a URL for periodic import. If the CRL import fails, an option is available to invalidate all certificates issued by this CA. The default option is to not require CRL processing.



Import Certificate Revocation List

Go Daddy Class 2 Certification Authority

Certificate Issuer: /C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority

Subject Distinguished Name: /C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority

CRL Status: No CRL loaded

● Import CRL directly from a PEM (.pem) or DER (.der or .crl) encoded file

Select a CRL file to import:

○ Periodically auto-import CRL via HTTP

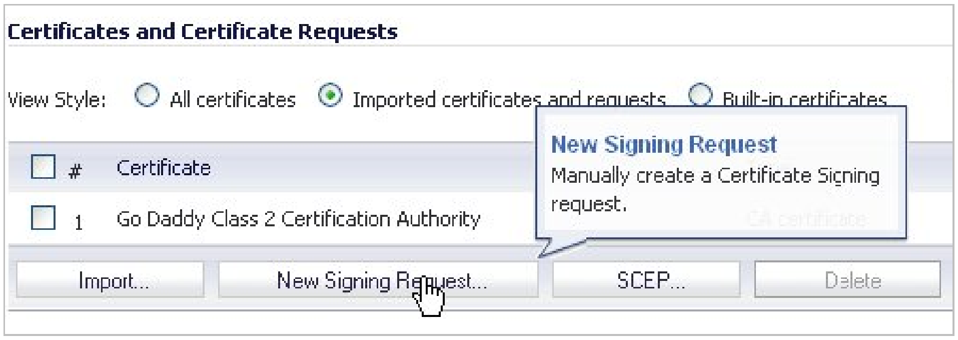
Enter CRL's location (URL):

□ Invalidate Certificates and Security Associations if CRL import or processing fails

Ready

Requesting an End-Entity (Local) Certificate from a CA

1. Click the **New Signing Request** button.



Certificates and Certificate Requests

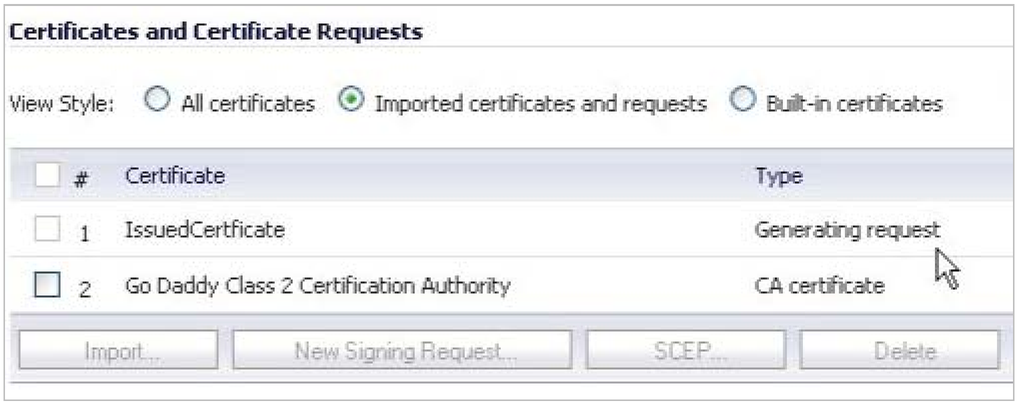
View Style: ○ All certificates ● Imported certificates and requests ○ Built-in certificates

□	#	Certificate
□	1	Go Daddy Class 2 Certification Authority

New Signing Request
Manually create a Certificate Signing request.

2. Fill in the desired form fields. The Subject Distinguished Name field will populate as you fill in various fields of the form. We suggest completing: Country, Organization, Department (Organizational Unit), and Common Name. Your site's security policy will determine the information needed.

3. Go to the **Subject Key Size** drop list and select the desired key size. Please be aware that a large key size will take an extensive amount of time to generate (especially on the smaller devices).

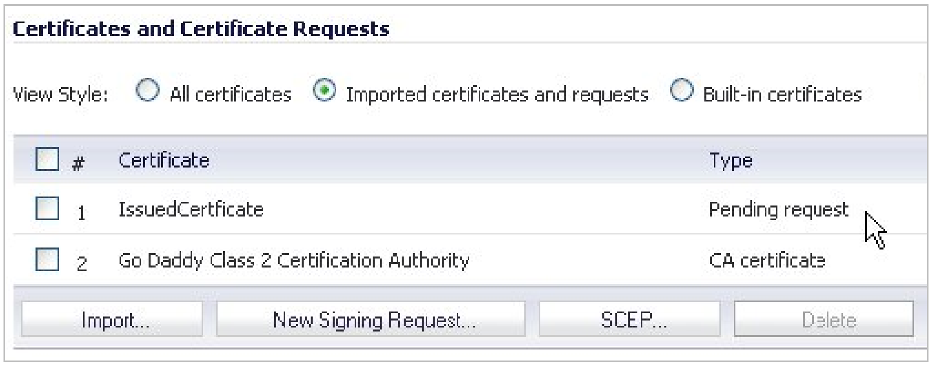


Certificates and Certificate Requests

View Style: ○ All certificates ● Imported certificates and requests ○ Built-in certificates

□	#	Certificate	Type
□	1	IssuedCertficate	Generating request
□	2	Go Daddy Class 2 Certification Authority	CA certificate

Once the key is generated, the status will update to **Pending Request**.

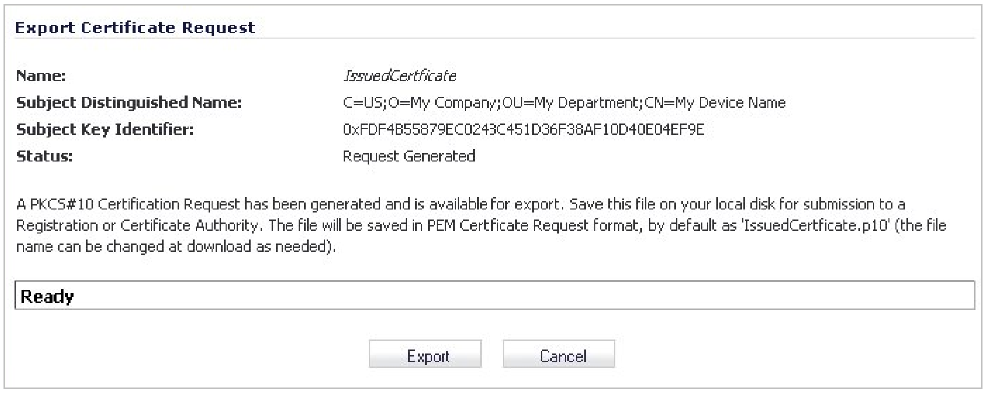


Certificates and Certificate Requests

View Style: ○ All certificates ● Imported certificates and requests ○ Built-in certificates

□	#	Certificate	Type
□	1	IssuedCertficate	Pending request
□	2	Go Daddy Class 2 Certification Authority	CA certificate

4. There are two options available:
   A. Manually export the CSR (as PEM-encoded PKCS #10 file) by selecting the **export icon.**



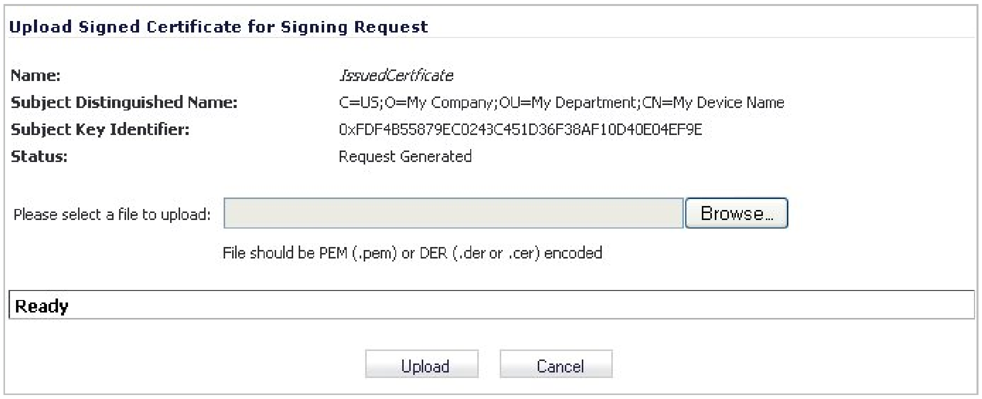
Export Certificate Request

Name:	*IssuedCertficate*
Subject Distinguished Name:	C=US;O=My Company;OU=My Department;CN=My Device Name
Subject Key Identifier:	0xFDF4B55879EC0243C451D36F38AF10D40E04EF9E
Status:	Request Generated

A PKCS#10 Certification Request has been generated and is available for export. Save this file on your local disk for submission to a Registration or Certificate Authority. The file will be saved in PEM Certficate Request format, by default as 'IssuedCertficate.p10' (the file name can be changed at download as needed).

Ready

If you manually export the CSR, you can then import the signed certificate as a .PEM or .DER file by clicking the **import icon**.



Upload Signed Certificate for Signing Request

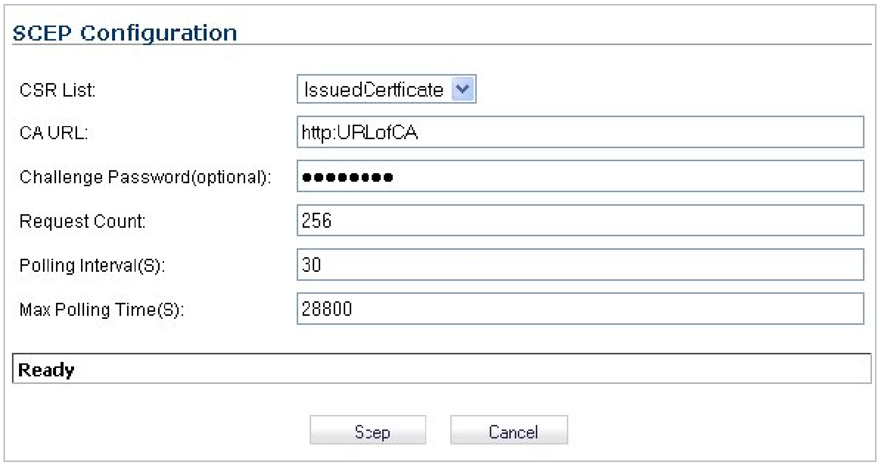
Name:	*IssuedCertficate*
Subject Distinguished Name:	C=US;O=My Company;OU=My Department;CN=My Device Name
Subject Key Identifier:	0xFDF4B55879EC0243C451D36F38AF10D40E04EF9E
Status:	Request Generated

Please select a file to upload:

File should be PEM (.pem) or DER (.der or .cer) encoded

Ready

   B. Select the **SCEP** button to send to your CA via SCEP.



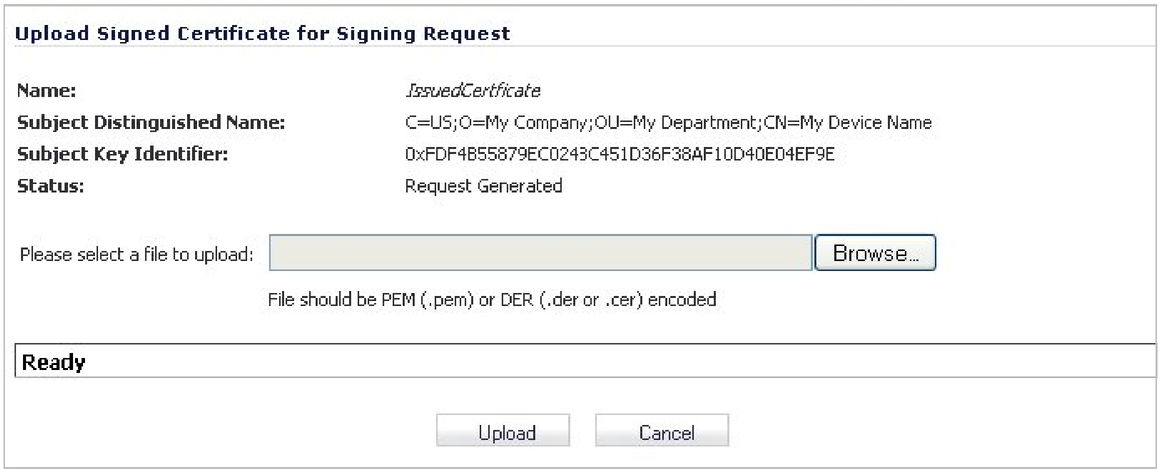
SCEP Configuration

CSR List:	IssuedCertficate
CA URL:	http:URLofCA
Challenge Password(optional):	••••••••
Request Count:	256
Polling Interval(S):	30
Max Polling Time(S):	28800

Ready

Installing an End-Entity Certificate

If you are importing a certificate matching a pending CSR, then import a .PEM or .DER file containing the certificate stated in previous procedures.



Upload Signed Certificate for Signing Request

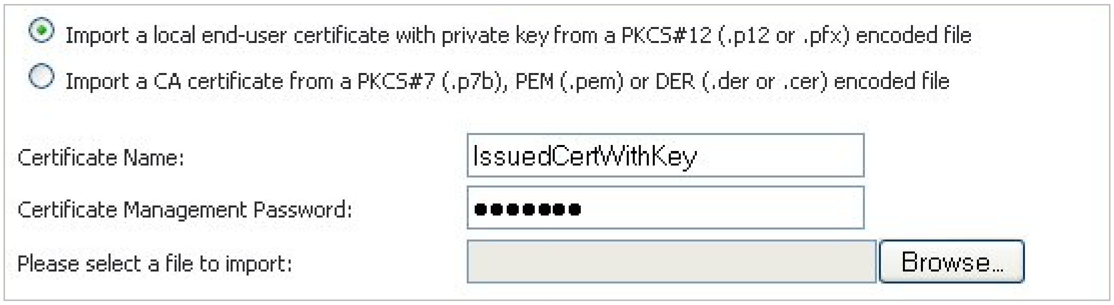
Name: *IssuedCertficate*
Subject Distinguished Name: C=US;O=My Company;OU=My Department;CN=My Device Name
Subject Key Identifier: 0xFDF4B55879EC0243C451D36F38AF10D40E04EF9E
Status: Request Generated

Please select a file to upload:

File should be PEM (.pem) or DER (.der or .cer) encoded

Ready

If you are importing a PKCS#12 independently issued by your CA, click the **Import** button and enter your choice of name and password. Then click the **Browse** button and select your file.

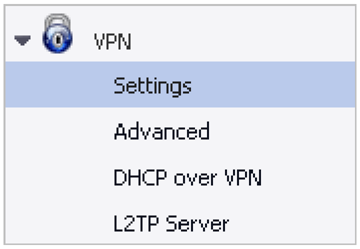


● Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file
○ Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file

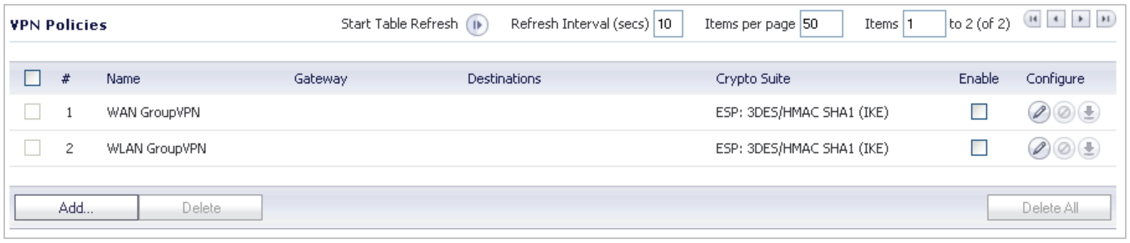
Certificate Name: IssuedCertWithKey
Certificate Management Password: ●●●●●●●
Please select a file to import:

Specifying that a Remote Peer will be Authenticating with Certificates

1. Navigate to **VPN > Settings**.



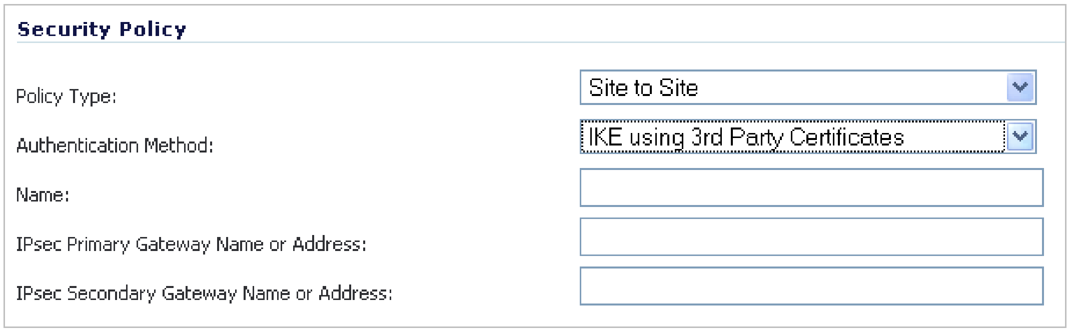
2. Click the **Add** button to bring up a VPN Policy configuration window.


VPN Policies

Start Table Refresh   Refresh Interval (secs) 10   Items per page 50   Items 1 to 2 (of 2)

☐	#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
☐	1	WAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	☐	
☐	2	WLAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	☐	

3. In the **Authentication Method** drop list, select **IKE using 3rd Party Certificates**.


Security Policy

Policy Type: Site to Site

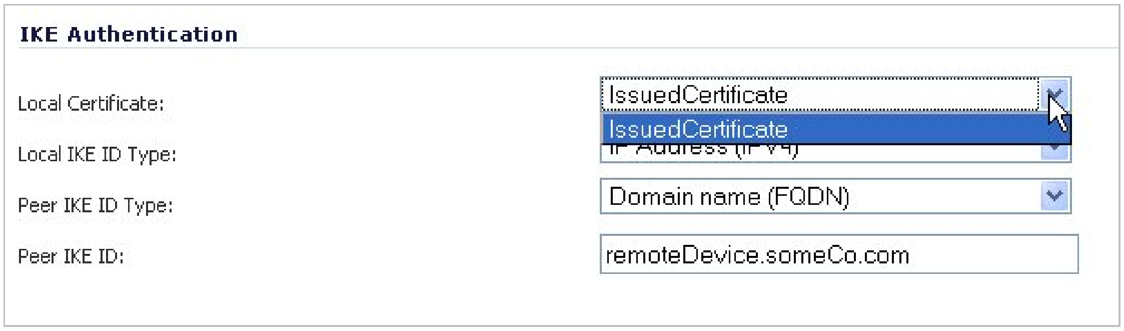
Authentication Method: IKE using 3rd Party Certificates

Name:

IPsec Primary Gateway Name or Address:

IPsec Secondary Gateway Name or Address:

4. Specify your certificate in the **Local Certificate** drop list.


IKE Authentication

Local Certificate: IssuedCertificate

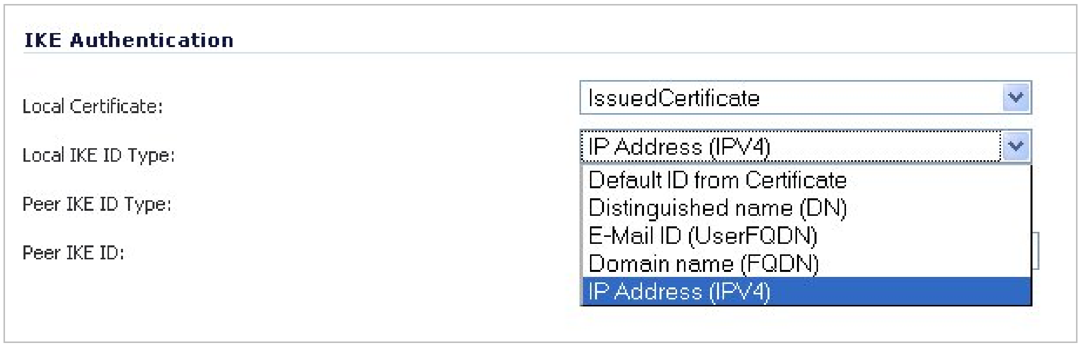
IssuedCertificate

Local IKE ID Type: IP Address (IPV4)

Peer IKE ID Type: Domain name (FQDN)

Peer IKE ID: remoteDevice.someCo.com

5. Specify the **Local IKE ID Type** from the drop list.
    - UserFQDN, FQDN, and IPv4 types always use the Subject Alt Name.
    - DN is always the Subject Name.
    - Default ID from Certificate will send the first Subject Alternative Name found of UserFQDN, FQDN, or IPv4 type. Otherwise, it will send the Subject Name as DN.



IKE Authentication

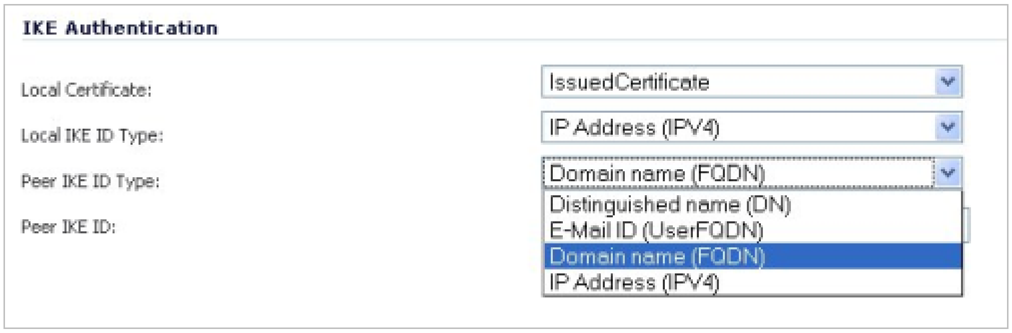
Local Certificate: IssuedCertificate

Local IKE ID Type: IP Address (IPV4)

Peer IKE ID Type:

Peer IKE ID:

6. Specify the **Peer IKE ID Type**. UserFQDN, FQDN, and IPv4 are only from subjectAltName.



IKE Authentication

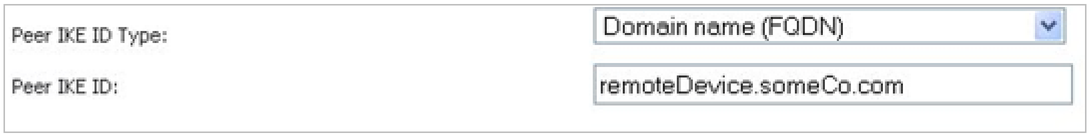
Local Certificate: IssuedCertificate

Local IKE ID Type: IP Address (IPV4)

Peer IKE ID Type: Domain name (FQDN)

Peer IKE ID:

7. Enter the **Peer IKE ID** – this is a string for UserFQDN, FQDN, or IPv4.



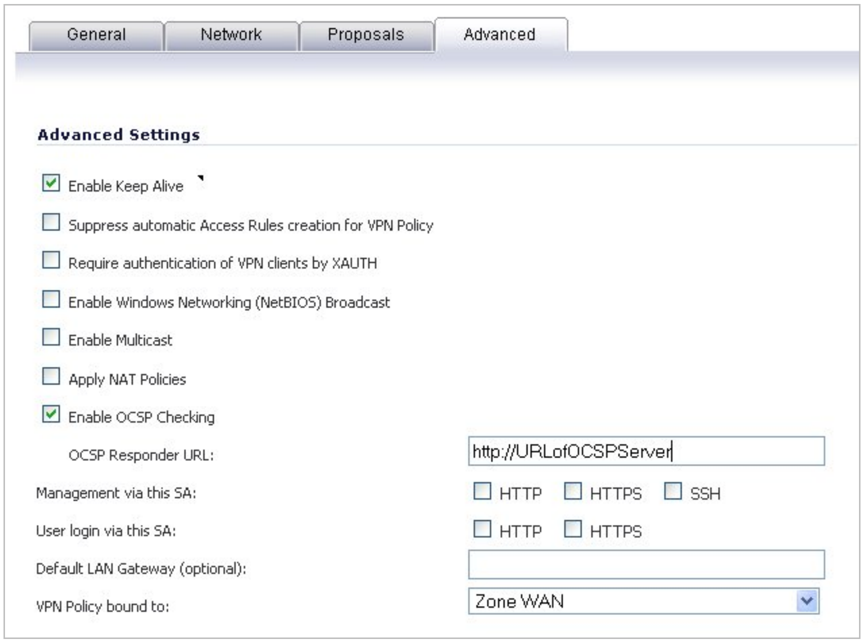
Peer IKE ID Type: Domain name (FQDN)

Peer IKE ID: remoteDevice.someCo.com

8. From the **Network** tab, select the appropriate networks for local and remote proxy.

9. In the **Proposals** tab, the **Exchange** drop list will provide three modes to choose from – Main, Aggressive, or IKEv2. Specify the mode and fill in IKE and IPsec parameters accordingly.

10. In the **Advanced** tab, OCSP Checking can be enabled if desired. Currently, only HTTP protocol is supported. The OCSP option is not available for IKEv2.



Advanced Settings

☑ Enable Keep Alive

□ Suppress automatic Access Rules creation for VPN Policy

□ Require authentication of VPN clients by XAUTH

□ Enable Windows Networking (NetBIOS) Broadcast

□ Enable Multicast

□ Apply NAT Policies

☑ Enable OCSP Checking

OCSP Responder URL: http://URLofOCSPServer

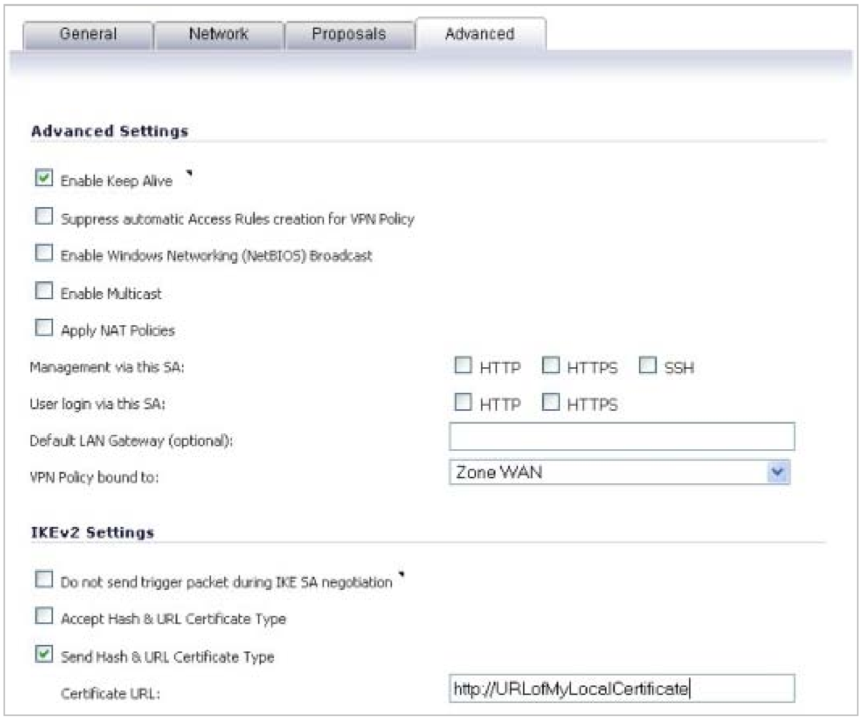
Management via this SA: □ HTTP □ HTTPS □ SSH

User login via this SA: □ HTTP □ HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Zone WAN

In IKEv2 mode, you can configure Hash & URL certification types if desired.



Advanced Settings

☑ Enable Keep Alive

□ Suppress automatic Access Rules creation for VPN Policy

□ Enable Windows Networking (NetBIOS) Broadcast

□ Enable Multicast

□ Apply NAT Policies

Management via this SA: □ HTTP □ HTTPS □ SSH

User login via this SA: □ HTTP □ HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Zone WAN

IKEv2 Settings

□ Do not send trigger packet during IKE SA negotiation

□ Accept Hash & URL Certificate Type

☑ Send Hash & URL Certificate Type

Certificate URL: http://URLofMyLocalCertificate