



CHAPTER 32

Configuring Certificates

Digital certificates provide digital identification for authentication. A digital certificate contains information that identifies a device or user, such as the name, serial number, company, department, or IP address. CAs issue digital certificates in the context of a PKI, which uses public-key/private-key encryption to ensure security. CAs are trusted authorities that “sign” certificates to verify their authenticity, thus guaranteeing the identity of the device or user.

A *CA certificate* is one used to sign other certificates. A CA certificate that is self-signed is called a *root certificate*; one issued by another CA certificate is called a *subordinate certificate*. CAs also issue *identity certificates*, which are the certificates for specific systems or hosts.

For authentication using digital certificates, there must be at least one identity certificate and its issuing CA certificate on a security appliance, which allows for multiple identities, roots and certificate hierarchies.

For More Information

[Authenticating, Enrolling for, and Managing Digital Certificates](#)

Authentication

The Authentication panel lets you authenticate a CA certificate, which associates the CA certificate with a trustpoint and installs it on the security appliance. You can edit an existing trustpoint configuration or you can create a new one.

If the trustpoint you select is configured for manual enrollment, you should obtain the CA certificate manually and import it here. If the trustpoint you select is configured for automatic enrollment, the security appliance uses the SCEP protocol to contact the CA, and then automatically obtains and installs the certificate.

Fields

- **Trustpoint Name**—Displays a list containing the trustpoints available from which to obtain the CA certificate. Click a trustpoint in the list and edit its configuration, or add a new trustpoint.
- **Edit**—Click to modify a trustpoint configuration currently appearing in the Trustpoint Name box.
- **New**—Add a new trustpoint configuration to the list.
- **Fingerprint**—Specify a key consisting of alphanumeric characters the security appliance uses to authenticate the CA certificate. If you provide a fingerprint, the security appliance compares it to the computed fingerprint of the CA certificate and accepts the certificate only if the two values match. If there is no fingerprint, the security appliance accepts the certificate without one.

- **Import from a file**—For manual enrollment only, identify a file from which to import the certificate. You can type the pathname of the file in the box or you can click Browse and search for the file.
 - Browse—Displays the Load Certificate File dialog box that lets you navigate to the file containing the certificate.
- **Enter the certificate text in base64 format**—For manual enrollment, enter the trustpoint configuration in base64 format.
- **Authenticate**—Complete the authentication procedure.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
			Multiple	
Routed	Transparent	Single	Context	System
•	•	•	•	•

For More Information

[Authenticating, Enrolling for, and Managing Digital Certificates](#)

Enrollment

The Enrollment panel lets you select a trustpoint configuration from the list, edit a trustpoint configuration or create a new one. However, for automatic enrollment, you cannot generate an enrollment request until you have authenticated the CA certificate.

For automatic enrollment, the security appliance contacts the CA using SCEP protocol, obtains the identity certificates, and installs them on the device. For manual enrollment, an enrollment request dialog box appears containing the certificate enrollment request. Use this enrollment request to obtain the identity certificate from the management interface of the CA. The identity certificate obtained must be in base64 or hexadecimal format. You can then import it in the Import Certificate dialog box.

Fields

- **Trustpoint Name**—Specify the trustpoint for which to generate the enrollment request. Select the name from a list, edit the name currently appearing in the box, or add a new trustpoint configuration.
- **Edit**—Modify the trustpoint configuration currently appearing in the Trustpoint Name box.
- **New**—Add a new trustpoint configuration to the list.
- **Enroll**—Initiate the enrollment process with the CA.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

For More Information

[Authenticating, Enrolling for, and Managing Digital Certificates](#)

Import Certificate

The Import Certificate panel lets you install the device certificate that you received from the CA during manual enrollment. To import certificates from a CA, there should be a CA certificate associated with the selected trustpoint. If not, the security appliance displays a warning.

Fields

- **Trustpoint Name**—Specify the name of the trustpoint from which you received the certificate. Select the name from a list, edit the name currently appearing in the box, or add a new trustpoint configuration.
- **Edit**—Modify the trustpoint configuration currently appearing in the Trustpoint Name box.
- **New**—Add a new trustpoint configuration to the list.
- **Import from a file**—Identify a file from which to import the identity certificate. You can type the pathname of the file in the box or you can click Browse and search for the file.
 - **Browse**—Displays the Load CA certificate file dialog box that lets you navigate to the file containing the certificate.
- **Enter the certificate text in base64 format**—For manual enrollment, lets you use cut and paste to transfer the certificate data to this security appliance from the source exported.



Note Additional information about importing certificates from the VPN 3000 Concentrator to the security appliance is available at the following URL:

http://www.cisco.com/en/US/docs/security/asa/asa72/vpn3000_upgrade/upgrade/guide/mimap.html#wp1047555

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Key Pair

RSA key pairs are required to enroll for identity certificates. The security appliance supports multiple key pairs.

Fields

- **Key-pair Name**—Displays the name given to the key pair(s).
- **Type**—Displays the type, which is RSA.
- **Usage**—Displays how an RSA key pair is to be used. There are two types of usage for RSA keys: general purpose, the default, and special. When you select Special, the security appliance generates two key pairs, one for signature use and one for encryption use. This implies that two certificates for the corresponding identity are required.
- **Size**—Displays the modulus size of the key pair(s): 512, 768, 1024, and 2048. The default modulus size is 1024.
- **Add**—Opens the Add Key Pair dialog box.
- **Show Details**—Displays the name, date generated, type, modulus size, usage and DER-encoded key data.
- **Delete**—Deletes the selected key pair.
- **Refresh**—Updates the display.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Add Key Pair

The Add Key Pair dialog box lets you add a new key pair to the list of key pairs.

Fields

- **Name**—Specify a name for the key pair(s): the default key <Default-RSA-Key> or a specific key. The security appliance uses the default key pair when a trustpoint has no key pairs configured.
- **Size**—Specify the modulus size of the key pair(s): 512, 768, 1024, and 2048. The default modulus size is 1024.
- **Type**—Specify the type, which can be RSA only.
- **Usage**—Specify how the key pair is to be used. There are two types of usage for RSA keys: general purpose, the default, or special. When you click Special, the security appliance generates two key pairs, one for signature use and one for encryption use. This implies that two certificates for the corresponding identity are required.
- **Generate Now**—Generate the key pair.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Key Pair Details

The Key-pair Details dialog box displays information about the selected key-pair.

Fields

- **Key Pair**—Displays the name given to the key pair.
- **Generation Time**—Displays time and date that the key was generated.
- **Type**—Displays the type of key pair (RSA).
- **Size**—Displays the modulus size. For RSA keys, the size can be 512, 768, 1024, or 2048. The default modulus size is 1024.
- **Usage**—Displays how an RSA key pair is to be used. There are two types of usage for RSA keys: general purpose, the default, and special. When the purpose of the key pair is Special, the security appliance generates two key pairs, one for signature use and one for encryption use. This implies that two certificates for the corresponding identity are required.
- **Key Data**—Displays the DER-encoded key data.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Manage Certificate

The Manage Certificates panel displays all of your certificates in a table and lets you add/edit a certificate, display certificate information, refresh a display and delete certificates from the security appliance.

Fields

- **Subject**—Identifies the owner of the certificate.
- **Type**—Identifies the type: CA, RA general, RA encryption, RA signature, identity.
- **Trustpoint**—Identifies the trustpoint.

- **Status**—Identifies the status: Available or Pending:
 - **Available** means that the CA has accepted the enrollment request and has issued an identity certificate.
 - **Pending** means that the enrollment request is still in process and that the CA has not issued the identity certificate yet.
- **Usage**—Identifies how the certificate is used: signature, general purpose, or encryption.
- **Add**—Displays the Add Certificate dialog box, which lets you add CA/RA/Identity certificates onto the security appliance. You can use this dialog box to import a certificate from a file you have exported or use cut and paste to enter a certificate onto the security appliance.
- **Show Details**—Displays the Certificate Details dialog box, which shows the following information about the selected certificate:
 - **General**—Displays the values for type, serial number, status, usage, CRL distribution point, and the time within which the certificate is valid. This applies to both available and pending status.
 - **Subject**— Displays the X.500 fields of the subject DN or certificate owner and their values. This applies only to available status.
 - **Issuer**—Displays the X.500 fields of the entity that granted the certificate. This applies only to available status.
- **Refresh**—Renews the display of the table in the Manage Certificates panel.
- **Delete**—Displays the Delete Certificate dialog box that asks you to confirm the certificate removal. If you delete a CA certificate, the security appliance deletes all the associated identity certificates as well.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

For More Information

[Authenticating, Enrolling for, and Managing Digital Certificates](#)

Add Certificate

The Add Certificate dialog box lets you manually add CA/RA/Identity certificates.

Fields

- **Trustpoint Name**—Specify the certificate to add to the Manage Certificates table.
- **Edit**—Modify the trustpoint configuration currently appearing in the Trustpoint Name box.
- **New**—Add a new trustpoint configuration to the list.
- **Certificate Type**—Specify the type: CA, RA general, RA encryption, RA signature, Identity.

- **Serial Number**—Include the serial number of the security appliance in the certificate.
- **Import from a file**—Identify a file from which to import the certificate. You can type the pathname of the file in the box or you can click Browse and search for the file.
 - **Browse**—Display the Add Certificate dialog box that lets you navigate to the file containing the certificate.
- **Enter the certificate text in base64 format**—Lets you use cut and paste to transfer the certificate data to this security appliance from the source text that was exported, which should be in hexadecimal format only.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
			Multiple	
Routed	Transparent	Single	Context	System
•	•	•	•	•

Trustpoint

A trustpoint represents a CA/identity pair and contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate.

Configuration

The Configuration panel lets you identify a CA, which can be a root CA, and have a self-signed certificate that contains its own public key. In the Configuration panel, you can add, edit, or delete a CA as a trustpoint, and request a CRL.

Fields

- **Trustpoint Name**—Displays the name of the trustpoint, for example, an IP address or a hostname.
- **Device Certificate Subject**—Displays the subject DN owning the certificate for the security appliance system.
- **CA Certificate Subject**—Displays the subject name of the CA certificate.
- **Add**—Opens the Add Trustpoint Configuration dialog box.
- **Edit**—Opens the Edit Trustpoint Configuration dialog box.
- **Delete**—Removes the selected trustpoint.
- **Request CRL**—Retrieves the Certificate Revocation List for the selected trustpoint. To view it, see Monitoring > Properties > CRL.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Add/Edit Trustpoint Configuration > Enrollment Settings Tab

The **Enrollment Settings** tab lets you add a trustpoint to the trustpoint table. The **Edit Trustpoint Configuration > Enrollment Settings** tab lets you modify information about the selected trustpoint.

Fields

- **Trustpoint Name**—Specify the name of the trustpoint corresponding to a CA. For example, this can be an IP address or a hostname.
- **Generate a self-signed certificate on enrollment**—Click to generate a self-signed device certificate for the security appliance during enrollment. This provides a way to create self-signed certificates for use when terminating SSL connections. This feature is not checked by default. When this option is checked, you can configure only the key pair and the certificate parameters.
- **Key Pair**—Select a previously defined key pair in the list. Before you add a trustpoint, you should configure a key pair. So if this list is empty, you can add the key pair by selecting **New Key Pair**.
- **Show Details**—Display information about the key pair including its name, when it was generated, its type (RSA), its modulus, its usage (general purpose or special) and the key data in DER-encoded format.
- **New Key Pair**—Open the **Add Key Pair** dialog box, which lets you enter a name, size, type, and usage for a new key pair.
- **Challenge Password**—Specify a challenge phrase that is registered with the CA during enrollment.
- **Confirm Challenge Password**—Verify the challenge password.
- **Use manual enrollment**—Specify intention to generate a PKCS10 certification request. The CA issues a certificate to the security appliance based on the request and the certificate is installed on the security appliance by importing the new certificate.
- **Use automatic enrollment**—Specify intention to use SCEP mode. When the indicated trustpoint is configured for SCEP enrollment, the security appliance then downloads the certificates using the SCEP protocol.
- **Enrollment URL**—Specify the name of the URL for automatic enrollment. The maximum length is 1000 characters (effectively unbounded).
- **Retry Period**—After requesting a certificate, the security appliance waits to receive a certificate from the CA. If the security appliance does not receive a certificate within the specified retry period, it sends another certificate request. Use this field to specify the number of minutes between attempts to send an enrollment request; the valid range is 1- 60 minutes. The default value is 1.
- **Retry Count**—After requesting a certificate, the security appliance waits to receive a certificate from the CA. If the security appliance does not receive a certificate within the specified retry period, it sends another certificate request. The security appliance repeats the request until either it receives a response or reaches the retry count specified. Use this field to specify the maximum number of attempts to send an enrollment request, the valid range is 0, 1-100 retries. The default value is 0, which means an unlimited number of retries.

- **Certificate Parameters**—Display the **Certificate Parameters** dialog box, which lets you specify attributes and their values to include in the certificate during enrollment, such as subject DN, FQDN, and so on.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Add/Edit Key Pair

The **Add Key Pair** dialog box lets you add a new key pair to the list of key pairs.

Fields

- **Name**—Specify a name for the key pair(s): the default key <Default-RSA-Key> or a specific key. The security appliance uses the default key pair when a trustpoint has no key pairs configured.
- **Size**—Specify the modulus size of the key pair(s): 512, 768, 1024, and 2048. The default modulus size is 1024.
- **Usage**—Specify how the key pair is to be used. There are two types of usage for RSA keys: general purpose, the default, or special. When you click **Special**, the security appliance generates two key pairs, one for signature use and one for encryption use. This implies that two certificates for the corresponding identity are required.
- **Generate Now**—Generate the key pair.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Certificate Parameters

The **Certificate Parameters** dialog box lets you specify the subject DN, FQDN, IP address to include during enrollment. Use this dialog box to include the device serial number.

Fields

- **Subject DN**—Specify the attributes and values to use for the X.500 name of the subject. The subject is the owner of the certificate.
 - Click **Edit** to display the **Edit DN** dialog box to select the attributes and values for the **Subject DN**.

- **FQDN**—Include the fully qualified domain name in the Subject Alternative Name extension of the certificate. The FQDN is the part of a URL that completely identifies the server program that a request is addressed to; for example www.examplesite.com.
- **E-mail**—Include the indicated e-mail address in the Subject Alternative Name extension of the certificate.
- **IP Address**—Include the indicated IP address in the Subject Alternative Name extension of the certificate.
- **Include device serial number**—Include the security appliance's serial number in the certificate during enrollment.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Edit DN

Edit DN

Select one of the following attributes in the **Attributes** list, type the value in the **Value** box, and click **Add**. Select as many as are needed.

Fields

- **Common Name (CN)**—An individual's given name; for example, Pat.
- **Department (OU)**—Organizational Unit or a subgroup of a larger organization such as an enterprise or a university; for example, Geology department.
- **Company Name (O)**—Organization such as an enterprise or university; for example, University of Oz.
- **Country (C)**—Two-letter designation for a specific country; for example, OZ.
- **State (St)**—State or Province within a country; for example, Kansas.
- **Location (L)**—Address of the subject; for example, 49 Wizard St.
- **Email Address (EA)**—Pat@univoz.org.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Add/Edit Trustpoint Configuration > Revocation Check Tab

The **Revocation Check** tab lets you specify whether to check certificates for revocation, and if you do, the method to use.

When a certificate is issued, it is valid for a fixed period of time. Sometimes a CA revokes a certificate before this time period expires; for example, due to security concerns or a change of name or association. CAs periodically issue a signed list of revoked certificates. Enabling revocation checking forces the security appliance to check that the CA has not revoked a certificate every time it uses that certificate for authentication.

The security appliance supports two methods for checking revocation status: CRL and OCSP.

Fields

- **Do not check certificates for revocation**—Select if you want the security appliance not to check certificates for revocation status.
- **Check certificates for revocation**—Select to have the security appliance check certificates for revocation status. You must also specify at least one revocation method.
- **Revocation methods**—Specify the revocation methods to use in checking certificates. If you specify more than one method, the security appliance applies methods in the order you set here. It uses the second method only if the first returns an error, for example, if the server is unavailable. Methods available include CRL and OCSP.
 - CRL—The security appliance retrieves, parses, and caches the complete certificate revocation list to determine the status of a certificate.
 - OCSP— The security appliance localizes certificate status on a Validation Authority, which it can query for the status of a specific certificate.
- **Add**—Click either CRL or OCSP in the left to add it as a revocation checking method.
- **Remove**—Click either CRL or OCSP in the right to remove it as a revocation checking method.
- **Move Up/Move Down**—Use these buttons to have the security appliance first use the method you prefer.
- **Consider certificate valid if revocation checking returns errors**—Check to have the security appliance accept a certificate even if errors occur during a revocation check.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Add/Edit Trustpoint Configuration > CRL Retrieval Policy Tab

The **CRL Retrieval Policy** tab lets you specify whether to retrieve CRLs from CRL DPs or from URLs listed in the **Static URLs** table.

Fields

- **Use CRL Distribution Point from the certificate**—Click to retrieve CRLs from the distribution point listed in the certificate.
- **Use Static URLs configured below**—Click to add up to five URLs from which the security appliance should attempt to obtain a CRL.
- **Add**—Displays the **Add Static URL** box. Use this box to add up to five URLs.
 - **URL:**—Select URL type: HTTP, LDAP, or SCEP.
 - **://**—Type the location that distributes the CRLs.
- **Edit**—Display the **Edit Static URL** box for you to modify the selected URL.
- **Delete**—Remove the selected URL.
- **Move Up**—Move the selected URL up in the table, until it is at the top.
- **Move Down**—Move the selected URL down in the table, until it is at the bottom.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Add/Edit Static URL**Fields**

- **URL:**—Select URL type: HTTP, LDAP, or SCEP.
- **://**—Type the location that distributes the CRLs.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Add/Edit Trustpoint Configuration > CRL Retrieval Method Tab

The **CRL Retrieval Method** tab lets you specify how to retrieve CRLs, including LDAP, HTTP and SCEP. You can enable all methods. If you enable several methods, ASDM uses them in the order you specify.

Fields

- **Enable Lightweight Directory Access Protocol (LDAP)**—Check to enable.
Specify LDAP parameters as follows:
 - **Name**—Identify the person who has access to the CRL on the server.
 - **Password**—Specify a password for the person listed under **Name**.
 - **Confirm Password**—Verify the password.
 - **Default Server**—Specify the hostname or IP address of the LDAP server.
 - **Default Port**—Specify the LDAP server port number. The default is 389.
- **Enable HTTP**—Specify HTTP as a protocol to use for CRL retrieval.
- **Enable Simple Certificate Enrollment Protocol (SCEP)**—Use the same method of retrieving the CRL as for enrollment, but not at enrollment time.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Add/Edit Trustpoint Configuration > OCSP Rules Tab

The OCSP Rules tab lets you configure OCSP certificate matching rules. These rules provide flexibility in that you can assign OCSP server URLs via a trustpoint

While you can configure multiple match rules for a trustpoint, only one match rule within a trustpoint can apply to a certificate map.

Fields

- **Certificate Map**—Displays the name of the certificate map to match to this OCSP rule. Certificate maps match user permissions to specific fields in a certificate. You must configure the certificate map before you configure OCSP rules (Configuration > VPN > IKE > Certificate Group Matching > Rules).
- **Trustpoint**—Displays the name of the trustpoint the security appliance uses to validate responder certificates.
- **Index**—Displays the priority number for the rule. The security appliance examines OCSP rules in priority order, and applies the first one that matches.
- **URL**—Specifies the URL for the OCSP server for this trustpoint.
- **Add**—Click to add a new OCSP rule.
- **Edit**—Click to edit an existing OCSP rule.
- **Delete**—Click to delete an OCSP rule.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Add/Edit Trustpoint OCSP Rule dialog box

You can configure OCSP rules for a trustpoint that override the OCSP server URL specified within the AuthorityInfoAccess (AIA) field of the remote user certificate.

- **Certificate Map**—Select the name of the certificate map to match to this OCSP rule. Certificate maps match user permission groups to specific fields in a certificate. Their function with OCSP is to let the security appliance access a particular OCSP server for revocation status, as well as to let you specify a trustpoint to validate the responder certificate. This lets you check revocation status via a trustpoint other than the trustpoint authenticating the remote user certificate.

You must configure the certificate map before you configure OCSP rules (Configuration > VPN > IKE > Certificate Group Matching > Rules).

- **Trustpoint**—Select the trustpoint that you want to use for this OCSP rule. You must have already configured this trustpoint.
- **Index**—Enter a number to determine the execution order of the match rules. The security appliance searches the match rules lowest to highest, according to this index, and applies the first rule that matches.
- **URL**—Specify the URL for the OCSP server for this trustpoint.

The security appliance uses OCSP servers in this order:

1. OCSP URL in a match certificate override rule (as configured here)
2. OCSP URL configured in the Add/Edit Trustpoint Configuration > Advanced Tab > OCSP Options attribute
3. AIA field of remote user certificate

If you do not set this URL attribute, the OCSP server specified the Advanced Tab > OCSP Options attribute applies, and if that is not set, the OCSP server in the Authority Info Access (AIA) extension of the remote user certificate applies. If the AIA does not have an AIA extension and you do not set a valid OCSP server here or in the Advanced tab, revocation status checking fails.

The security appliance supports only HTTP URLs, and you can specify only one URL per trustpoint.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Add/Edit Trustpoint Configuration > Advanced Tab

The **Advanced** tab lets you specify CRL and OCSP options. When a certificate is issued, it is valid for a fixed period of time. Sometimes a CA revokes a certificate before this time period expires; for example, due to security concerns or a change of name or association. CAs periodically issue a signed list of revoked certificates. Enabling revocation checking forces the security appliance to check that the CA has not revoked the certificate being verified.

The security appliance supports two methods of checking revocation status: CRL and OCSP.

Fields

- **CRL Options**

- **Cache Refresh Time**—Specify the number of minutes between cache refreshes. The default number of minutes is 60. The range is 1-1440.

To avoid having to retrieve the same CRL from a CA repeatedly, The security appliance can store retrieved CRLs locally, which is called CRL caching. The CRL cache capacity varies by platform and is cumulative across all contexts. If an attempt to cache a newly retrieved CRL would exceed its storage limits, the security appliance removes the least recently used CRL until more space becomes available.

- **Enforce next CRL update**—Require valid CRLs to have a Next Update value that has not expired. Clearing the box allows valid CRLs with no Next Update value or a Next Update value that has expired.

- **OCSP Options**

- **Server URL:**—Enter the URL for the OCSP server. The security appliance uses OCSP servers in the following order:

1. OCSP URL in a match certificate override rule (Add/Edit Trustpoint Configuration > OCSP Rules tab)
2. OCSP URL configured in this OCSP Options attribute
3. AIA field of remote user certificate

- **Disable nonce extension**—By default the OCSP request includes the nonce extension, which cryptographically binds requests with responses to avoid replay attacks. It works by matching the extension in the request to that in the response, ensuring that they are the same. Disable the nonce extension if the OCSP server you are using sends pre-generated responses that do not contain this matching nonce extension.

- **Accept certificates issued by this trustpoint**—Specify whether or not the security appliance should accept certificates from **Trustpoint Name**.
- **Accept certificates issued by the subordinate CAs of this trustpoint**
- **Use the configuration of this trustpoint to validate any remote user certificate issued by the CA corresponding to this trustpoint**—When enabled, the configuration settings active when a remote user certificate is being validated can be taken from this trustpoint if this trustpoint is authenticated to the CA that issued the remote certificate.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
			Multiple	
Routed	Transparent	Single	Context	System
•	•	•	•	•

Export

The **Export** panel lets you export a trustpoint configuration with all associated keys and certificates in PKCS12 format, which must be in base64 format. An entire trustpoint configuration includes the entire chain (root CA certificate, identity certificate, key pair) but not enrollment settings (subject name, FQDN and so on). This feature is commonly used in a failover or load balancing configuration to replicate trustpoints across a group of security appliances; for example, remote access clients calling in to a central organization that has several units to service the calls. These units must have equivalent trustpoint configurations. In this case, an administrator can export a trustpoint configuration and then import it across the group of security appliances.

Fields

- **Trustpoint Name**—Click a trustpoint in the list and edit its configuration, or add a new trustpoint configuration.
- **Edit**—Modify the trustpoint configuration currently appearing in the **Trustpoint Name** box
- **New**—Add a new trustpoint configuration to the list.
- **Encryption Passphrase**—Specify the passphrase used to encrypt the PKCS12 file for export.
- **Confirm Passphrase**—Verify the encryption passphrase.
- **Export to a file**—Specify the name of the PKCS12-format file to use in exporting the trustpoint configuration; PKCS12 is the public key cryptography standard, which can be base64 encoded or hexadecimal.
 - **Browse**—Display the **Select a File** dialog box that lets you navigate to the file to which you want to export the trustpoint configuration.
- **Display the trustpoint configuration in PKCS12 format**—Display the **Export Trustpoint Configuration** dialog box, which displays the trustpoint configuration in a text box. You can use cut and paste to extract the data and place it in the window of the **Import** panel. To exit, click **OK**.
- **Export**—Export the trustpoint configuration.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
			Multiple	
Routed	Transparent	Single	Context	System
•	•	•	•	•

Import

The **Import** panel lets you install an entire trustpoint configuration in PKCS12 format. An entire trustpoint configuration includes the entire chain (root CA certificate, RA certificate, identity certificate, key pair) but not enrollment sets (subject name, FQDN and so on). This feature is commonly used in a failover or load balancing configuration to replicate trustpoints across a group of security appliances; for example, remote access clients calling in to a central organization that has several units to service the calls. These units must have equivalent trustpoint configurations. In this case, an administrator can export a trustpoint configuration and then import it across the group of security appliances.

Fields

- **Trustpoint Name**—Identify the trustpoint. When importing from another security appliance for failover or load balancing, you can use the same trustpoint name as the security appliance from which the trustpoint configuration was exported. However make sure that a trustpoint/key pair with the same name does not already exist.
- **Decryption Passphrase**—Specify the encryption passphrase specified during the export of the trustpoint configuration.
- **Confirm Passphrase**—Verify the passphrase.
- **Import from a file**—Identify a file from which to import the certificate. The text imported from a file should be PKCS12 data, in either base64 or hexadecimal format. You can type the pathname of the file in the box or you can click **Browse** and search for the file.
 - **Browse**—Display the **Load Certificate File** dialog box that lets you navigate to the file containing the trustpoint configuration.
- **Enter the trustpoint configuration in PKCS12 format**—lets you paste the trustpoint configuration in PKCS12 format, which can be in either base64 or hexadecimal format. In this case, you use cut and paste to enter the data into the text box.
- **Import**—Import the trustpoint configuration.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Authenticating, Enrolling for, and Managing Digital Certificates

This section describes how to enroll for a digital certificate. Once enrolled, you can use the certificate for authenticating the device to VPN and SSL peers.

Summary of Configuration Steps

Here are the basic steps for enrolling with a CA and getting an identity certificate to use for authenticating tunnels. This example shows both automatic (SCEP) enrollment and manual enrollment. For information on fields not defined in this procedure, click the **Help** button.

1. Generating a key pair for the identity certificate. The key pair is RSA.
2. Creating a trustpoint.
3. Configuring an enrollment URL.
4. Authenticating the CA.
5. Enrolling with the CA, which places an identity certificate onto the security appliance.



Note

Authenticating and Enrolling are two separate phases of the process. You must authenticate. Then you can enroll using either automatic enrollment or manual enrollment.

Generating the Key Pair

Begin by generating a key pair for the certificate. Generated key pairs are identified by labels that you provide when you configure the key pair. RSA Key pairs come in two types: general purpose and usage. General purpose is the default type and generates a single pair of keys. Usage type generates two key pairs, one for signature use and one for encryption use, thus requiring two certificates for the corresponding identity.

To generate an RSA key pair using ASDM, follow this procedure:

- Step 1** Under **Configuration > Features > Device Administration > Certificate > Key Pair**, click **Add**.
- Step 2** Configure the information in the **Add Key Pair** dialog box:
- Step 3** Click **Generate Now**.
- Step 4** To view the key pair generated, click **Show Details**. ASDM displays information about the key pair.

Enrolling for a Certificate Using Automatic Enrollment (SCEP)

Create a trustpoint. A trustpoint represents a CA/identity pair and contains the identity of the CA, specific configuration parameters, and an association with one enrolled identity certificate.

To create a trustpoint, follow these steps:

- Step 1** Under **Configuration > Features > Device Administration > Certificate > Trustpoint > Configuration**, click **Add**.
- Step 2** Configure the basic information in the **Add Trustpoint Configuration** dialog box. For all other parameters, you can accept the default values.
 - a. **Trustpoint Name**—Type the trustpoint name in the **Trustpoint Name** box.

- b. **Enrollment URL**—In the **Enrollment Settings** panel, under the **Enrollment Mode** group box, for SCEP enrollment, click **Use automatic enrollment**. Then type the enrollment URL in the box. For example, type 10.20.30.40/cgi-bin/pkiclient.exe.
 - c. If you want password verification for the certificate, type the password into the **Challenge Password** and **Confirm Password** boxes. If you need to revoke the certificate, you can provide this password to the CA administrator to identify that you are the certificate owner. This password is not saved in the configuration, so you should make a note of it.
- Step 3** Configure the configuration parameters next. At the very least, you need to configure a subject name for the certificate using X.500 fields; for example, common name (CN) and organizational unit (OU).
- a. In the **Enrollment Settings** panel, select the key pair you configured for this trustpoint in the **Key Pair** list.
 - b. In the **Enrollment Settings** panel, click **Certificate Parameters**.
 - c. To add subject DN values, click **Edit** in the **Certificate Parameters** dialog box.
 - d. In the **Edit DN** box under **DN Attribute to be Added**, select an attribute in the **Attribute** list and type a value in the **Value** box. Then click **Add**. For example, first select **Command Name (CN)** and type Pat in the **Value** box; then select **Department (OU)** and type Engineering in the **Value** box.
 - e. After entering all subject DN information, click **OK**.
 - f. Optionally type values for **FQDN**, **E-mail**, and **IP Address**, and check the **Include device serial number** option.
 - g. Click **OK**.
- Step 4** Click **Apply**. If you have preview commands checked, ASDM displays the CLI commands based on the ASDM configuration for you to either send or cancel. Click **Send**. Do this for all features you configure using this procedure.
-

Authenticating to the CA

Authenticating to the CA puts the CA certificate onto the security appliance. If you configure the trustpoint for SCEP enrollment, the CA certificate is downloaded through SCEP. If not, you must paste the CA certificate into the text box or point to the file with the browse button. This section shows SCEP enrollment.

To authenticate to the CA, follow these steps:

- Step 1** Under **Configuration > Features > Device Administration > Certificate > Authentication**, select the name of the trustpoint in the **Trustpoint Name** list.
 - Step 2** Click **Authenticate**.
 - Step 3** When ASDM displays the **Authentication Successful** dialog, click **OK**.
-

Enrolling with the CA

After you have configured the trustpoint and authenticated with it, you can enroll for an identity certificate.

To enroll for an identity certificate using ASDM, follow these steps:

Step 1 Under **Configuration > Features > Device Administration > Certificate > Enrollment**, select the trustpoint in the **Trustpoint Name** list.

Step 2 Click **Enroll**.

After completing the action, ASDM displays the **Copy Trustpoint Configuration to Standby** dialog box, which tells you how to export the trustpoint configuration and how to check the enrollment status. This message is relevant only in a failover configuration; if you have not configured failover, you can ignore this step and click **OK**. If you have configured failover, you should follow the instructions in the dialog box to back up the certificate to the standby device.

Enrolling for a Certificate Using Manual Enrollment

Use this method when you receive an identity certificate from a CA through a means other than automatic enrollment.

Step 1 Under **Configuration > Features > Device Administration > Certificate > Trustpoint > Configuration**, click **Add**.

Step 2 On the **Add Trustpoint Configuration** dialog, type the name in the **Trustpoint Name** box.

Step 3 In the **Enrollment Settings** panel, select a key pair from the **Key Pair** list or add a new key pair by clicking **New Key Pair**.

Step 4 Optionally, type a password in the **Challenge Password** box and confirm it in the **Confirm Challenge Password** box.

Step 5 Click the **Use manual enrollment** option.

Step 6 Click **Certificate Parameters**.

- a. To add subject DN values, click **Edit** in the **Certificate Parameters** dialog box.
- b. In the **Edit DN** box under **DN Attribute to be Added**, select an attribute in the **Attribute** list and type a value in the **Value** box. Then click **Add**. For example, first select **Command Name (CN)** and type Pat in the **Value** box; then select **Department (OU)** and type Engineering in the **Value** box.
- c. After adding all subject DN attributes, click **OK**.
- d. Optionally, type values for **FQDN**, **E-mail**, and **IP Address**, and click the **Include device serial number** option.
- e. Click **OK**.

Step 7 Click on **Configuration > Features > Device Administration > Certificate > Enrollment** and select the trustpoint in the **Trustpoint Name** list.

Step 8 Click **Enroll**. The **Enrollment Request** dialog box displays, which describes what to do next. After reading the instructions, click **OK**.

Either send the request by e-mail or enroll using the CA's web interface.

Step 9 After you receive the certificate from the CA, click **Configuration > Features > Device Administration > Certificate > Import Certificate** and select the name of the trustpoint in the **Trustpoint Name** list.

Step 10 Select a method for importing the certificate.

- **Import from a File**—Type the filename or browse for the file. There must be a CA certificate associated with the selected trustpoint on your system and you must have received an identity certificate in a file from the CA.
- **Enter the certificate text in base64 format**—Paste the text from the identity certificate you received from the CA into the text box. For more information, click **Help**.

Step 11 Click **Import**.

Step 12 To save the certificate enrollment configuration to flash, click **Save**.

Additional Steps for a Failover Configuration

To back up the identity certificate, CA certificate, and keys to other security appliances in your network, first export them to a file or use the export feature to display the certificate in a popup window for copying and pasting onto another security appliance through the import feature.

Exporting the Certificate to a File or PKCS12 data

To export a trustpoint configuration, follow these steps:

-
- Step 1** Go to **Configuration > Features > Device Administration > Certificate > Trustpoint > Export**.
- Step 2** Fill in the **Trustpoint Name**, **Encryption Passphrase**, and **Confirm Passphrase** fields. For information on these fields, click **Help**.
- Step 3** Select a method for exporting the trustpoint configuration.
- **Export to a File**—Type the filename or browse for the file.
 - **Display the trustpoint configuration in PKCS12 format**—Display the entire trustpoint configuration in a text box and then copy it for importing. For more information, click **Help**.
- Step 4** Click **Export**.
-

Importing the Certificate onto the Standby Device

To import a trustpoint configuration, follow these steps:

-
- Step 1** Go to **Configuration > Features > Device Administration > Certificate > Trustpoint > Import**.
- Step 2** Fill in the **Trustpoint Name**, **Decryption Passphrase**, and **Confirm Passphrase** fields. For information on these fields, click **Help**. The decryption passphrase is the same as the encryption passphrase used when the trustpoint configuration was exported.
- Step 3** Select a method for importing the trustpoint configuration.
- **Import from a File**—Type the filename or browse for the file.
 - **Enter the trustpoint configuration in PKCS12 format**—Paste the entire trustpoint configuration from the exported source into a text box. For more information, click **Help**.
-

Managing Certificates

To manage certificates, go to **Configuration > Features > Device Administration > Certificate > Manage Certificates**.

You can use this panel to add a new certificate and delete a certificate. You can also display information about a certificate by clicking the **Show Detail** button. The **Certificate Details** dialog box displays three tables: **General**, **Subject** and **Issuer**.

The **General** table displays the following information:

- Type—CA, RA, or Identity.
- Serial number—Serial number of the certificate.
- Status—Available, in progress, error, fail.
- Usage—General purpose or signature.
- CRL DP—URL for of the distribution point containing the CRL for validating the certificate.
- Dates/times within which the certificate is valid— Valid from, valid to.

The **Subject** panel displays the following information:

- Name—The name of the person or entity that owns the certificate.
- Serial Number—The serial number of the security appliance.
- X.500 fields for the subject of the certificate—CN, OU, etc.
- Hostname of the certificate holder—For example, wland.com.
- Serial Number of the hostname—The serial number of the security appliance.

The **Issuer** panel displays the X.500 DN fields for the entity that granted the certificate.

- Common name (CN)
- Organizational unit or department (OU)
- Organization (O)
- Locality (L)
- State (ST)
- Country code (C)
- Email address of the issuer (EA)