



Configuring Digital Certificates

This chapter describes how to configure digital certificates and includes the following sections:

- [Information About Digital Certificates, page 40-1](#)
- [Licensing Requirements for Digital Certificates, page 40-9](#)
- [Prerequisites for Local Certificates, page 40-10](#)
- [Guidelines and Limitations, page 40-10](#)
- [Configuring Digital Certificates, page 40-11](#)
- [Configuring CA Certificate Authentication, page 40-12](#)
- [Monitoring CRLs, page 40-20](#)
- [Configuring Identity Certificates Authentication, page 40-24](#)
- [Configuring Code Signer Certificates, page 40-29](#)
- [Authenticating Using the Local CA, page 40-31](#)
- [Managing the User Database, page 40-35](#)
- [Managing User Certificates, page 40-37](#)
- [Monitoring CRLs, page 40-38](#)
- [Feature History for Certificate Management, page 40-39](#)

Information About Digital Certificates

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

For authentication using digital certificates, at least one identity certificate and its issuing CA certificate must exist on an ASA. This configuration allows multiple identities, roots, and certificate hierarchies. The ASA evaluates third-party certificates against CRLs, also called authority revocation lists, all the way from the identity certificate up the chain of subordinate certificate authorities.

Descriptions of several different types of available digital certificates follow:

- A *CA certificate* is used to sign other certificates. It is self-signed and called a *root certificate*. A certificate that is issued by another CA certificate is called a *subordinate certificate*. For more information, see the “[Configuring CA Certificate Authentication](#)” section on page 40-12.
- CAs also issue *identity certificates*, which are certificates for specific systems or hosts. For more information, see the “[Configuring Identity Certificates Authentication](#)” section on page 40-24.
- *Code-signer certificates* are special certificates that are used to create digital signatures to sign code, with the signed code itself revealing the certificate origin. For more information, see the “[Configuring Code Signer Certificates](#)” section on page 40-29.

The local CA integrates an independent certificate authority feature on the ASA, deploys certificates, and provides secure revocation checking of issued certificates. The local CA provides a secure, configurable, in-house authority for certificate authentication with user enrollment through a website login page.

For more information, see the “[Authenticating Using the Local CA](#)” section on page 40-31, the “[Managing the User Database](#)” section on page 40-35, and the “[Managing User Certificates](#)” section on page 40-37.

**Note**

CA certificates and identity certificates apply to both site-to-site VPN connections and remote access VPN connections. Procedures in this document refer to remote access VPN use in the ASDM GUI.

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

For authentication using digital certificates, at least one identity certificate and its issuing CA certificate must exist on an ASA. This configuration allows multiple identities, roots, and certificate hierarchies. Descriptions of several different types of available digital certificates follow:

- A *CA certificate* is used to sign other certificates. It is self-signed and called a *root certificate*.
- A certificate that is issued by another CA certificate is called a *subordinate certificate*. For more information, see the “[Configuring CA Certificate Authentication](#)” section on page 40-14.

CAs are responsible for managing certificate requests and issuing digital certificates. A digital certificate includes information that identifies a user or device, such as a name, serial number, company, department, or IP address. A digital certificate also includes a copy of the public key for the user or device. A CA can be a trusted third party, such as VeriSign, or a private (in-house) CA that you establish within your organization.

**Tip**

For an example of a scenario that includes certificate configuration and load balancing, see the following URL: <https://supportforums.cisco.com/docs/DOC-5964>.

This section includes the following topics:

- [Public Key Cryptography](#), page 40-3
- [Certificate Scalability](#), page 40-3
- [Key Pairs](#), page 40-4
- [Trustpoints](#), page 40-4
- [Revocation Checking](#), page 40-5

- [The Local CA, page 40-7](#)
- [Using Certificates and User Login Credentials, page 40-8](#)

Public Key Cryptography

Digital signatures, enabled by public key cryptography, provide a way to authenticate devices and users. In public key cryptography, such as the RSA encryption system, each user has a key pair containing both a public and a private key. The keys act as complements, and anything encrypted with one of the keys can be decrypted with the other.

In simple terms, a signature is formed when data is encrypted with a private key. The signature is attached to the data and sent to the receiver. The receiver applies the public key of the sender to the data. If the signature sent with the data matches the result of applying the public key to the data, the validity of the message is established.

This process relies on the receiver having a copy of the public key of the sender and a high degree of certainty that this key belongs to the sender, not to someone pretending to be the sender.

Obtaining the public key of a sender is normally handled externally or through an operation performed at installation. For example, most web browsers are configured with the root certificates of several CAs by default. For VPN, the IKE protocol, a component of IPsec, can use digital signatures to authenticate peer devices before setting up security associations.

Certificate Scalability

Without digital certificates, you must manually configure each IPsec peer for each peer with which it communicates; as a result, each new peer that you add to a network would require a configuration change on each peer with which it needs to communicate securely.

When you use digital certificates, each peer is enrolled with a CA. When two peers try to communicate, they exchange certificates and digitally sign data to authenticate each other. When a new peer is added to the network, you enroll that peer with a CA and none of the other peers need modification. When the new peer attempts an IPsec connection, certificates are automatically exchanged and the peer can be authenticated.

With a CA, a peer authenticates itself to the remote peer by sending a certificate to the remote peer and performing some public key cryptography. Each peer sends its unique certificate, which was issued by the CA. This process works because each certificate encapsulates the public key for the associated peer, each certificate is authenticated by the CA, and all participating peers recognize the CA as an authenticating authority. The process is called IKE with an RSA signature.

The peer can continue sending its certificate for multiple IPsec sessions, and to multiple IPsec peers, until the certificate expires. When its certificate expires, the peer administrator must obtain a new one from the CA.

CAs can also revoke certificates for peers that no longer participate in IPsec. Revoked certificates are not recognized as valid by other peers. Revoked certificates are listed in a CRL, which each peer may check before accepting a certificate from another peer.

Some CAs have an RA as part of their implementation. An RA is a server that acts as a proxy for the CA, so that CA functions can continue when the CA is unavailable.

Key Pairs

Key pairs are RSA keys, which have the following characteristics:

- RSA keys can be used for SSH or SSL.
- SCEP enrollment supports the certification of RSA keys.
- For the purposes of generating keys, the maximum key modulus for RSA keys is 2048 bits. The default size is 1024. Many SSL connections using identity certificates with RSA key pairs that exceed 1024 bits can cause a high CPU usage on the ASA and rejected clientless logins.
- For signature operations, the supported maximum key size is 4096 bits. We recommend using a key size of at least 2048.
- You can generate a general purpose RSA key pair, used for both signing and encryption, or you can generate separate RSA key pairs for each purpose. Separate signing and encryption keys help to reduce exposure of the keys, because SSL uses a key for encryption but not signing. However, IKE uses a key for signing but not encryption. By using separate keys for each, exposure of the keys is minimized.

Trustpoints

Trustpoints let you manage and track CAs and certificates. A trustpoint is a representation of a CA or identity pair. A trustpoint includes the identity of the CA, CA-specific configuration parameters, and an association with one, enrolled identity certificate.

After you have defined a trustpoint, you can reference it by name in commands requiring that you specify a CA. You can configure many trustpoints.



Note

If an ASA has multiple trustpoints that share the same CA, only one of these trustpoints sharing the CA can be used to validate user certificates. To control which trustpoint sharing a CA is used for validation of user certificates issued by that CA, use the **support-user-cert-validation** command.

For automatic enrollment, a trustpoint must be configured with an enrollment URL, and the CA that the trustpoint represents must be available on the network and must support SCEP.

You can export and import the keypair and issued certificates associated with a trustpoint in PKCS12 format. This format is useful to manually duplicate a trustpoint configuration on a different ASA.

Certificate Enrollment

The ASA needs a CA certificate for each trustpoint and one or two certificates for itself, depending upon the configuration of the keys used by the trustpoint. If the trustpoint uses separate RSA keys for signing and encryption, the ASA needs two certificates, one for each purpose. In other key configurations, only one certificate is needed.

The ASA supports automatic enrollment with SCEP and with manual enrollment, which lets you paste a base-64-encoded certificate directly into the terminal. For site-to-site VPNs, you must enroll each ASA. For remote access VPNs, you must enroll each ASA and each remote access VPN client.

Proxy for SCEP Requests

The ASA can proxy SCEP requests between AnyConnect and a third-party CA. The CA only needs to be accessible to the ASA if it is acting as the proxy. For the ASA to provide this service, the user must authenticate using any of the methods supported by AAA before the ASA sends an enrollment request. You can also use host scan and dynamic access policies to enforce rules of eligibility to enroll.

The ASA supports this feature only with an AnyConnect SSL or IKEv2 VPN session. It supports all SCEP-compliant CAs, including IOS CS, Windows Server 2003 CA, and Windows Server 2008 CA.

Clientless (browser-based) access does not support SCEP proxy, although WebLaunch—clientless-initiated AnyConnect—does support it.

The ASA does not support polling for certificates.

The ASA supports load balancing for this feature.

Revocation Checking

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, because of security concerns or a change of name or association. CAs periodically issue a signed list of revoked certificates. Enabling revocation checking forces the ASA to check that the CA has not revoked a certificate each time that it uses the certificate for authentication.

When you enable revocation checking, the ASA checks certificate revocation status during the PKI certificate validation process, which can use either CRL checking, OCSP, or both. OCSP is only used when the first method returns an error (for example, indicating that the server is unavailable).

With CRL checking, the ASA retrieves, parses, and caches CRLs, which provide a complete list of revoked (and unrevoked) certificates with their certificate serial numbers. The ASA evaluates certificates according to CRLs, also called authority revocation lists, from the identity certificate up the chain of subordinate certificate authorities.

OCSP offers a more scalable method of checking revocation status in that it localizes certificate status through a validation authority, which it queries for status of a specific certificate.

Supported CA Servers

The ASA supports the following CA servers:

Cisco IOS CS, ASA Local CA, and third-party X.509 compliant CA vendors including, but not limited to:

- Baltimore Technologies
- Entrust
- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft Certificate Services
- RSA Keon
- Thawte

- VeriSign

CRLs

CRLs provide the ASA with one way of determining whether a certificate that is within its valid time range has been revoked by the issuing CA. CRL configuration is part of configuration of a trustpoint.

You can configure the ASA to make CRL checks mandatory when authenticating a certificate by using the **revocation-check crl** command. You can also make the CRL check optional by using the **revocation-check crl none** command, which allows the certificate authentication to succeed when the CA is unavailable to provide updated CRL data.

The ASA can retrieve CRLs from CAs using HTTP, SCEP, or LDAP. CRLs retrieved for each trustpoint are cached for a configurable amount of time for each trustpoint.

When the ASA has cached a CRL for longer than the amount of time it is configured to cache CRLs, the ASA considers the CRL too old to be reliable, or “stale.” The ASA tries to retrieve a newer version of the CRL the next time that a certificate authentication requires a check of the stale CRL.

The ASA caches CRLs for an amount of time determined by the following two factors:

- The number of minutes specified with the **cache-time** command. The default value is 60 minutes.
- The NextUpdate field in the CRLs retrieved, which may be absent from CRLs. You control whether the ASA requires and uses the NextUpdate field with the **enforcenextupdate** command.

The ASA uses these two factors in the following ways:

- If the NextUpdate field is not required, the ASA marks CRLs as stale after the length of time defined by the **cache-time** command.
- If the NextUpdate field is required, the ASA marks CRLs as stale at the sooner of the two times specified by the **cache-time** command and the NextUpdate field. For example, if the **cache-time** command is set to 100 minutes and the NextUpdate field specifies that the next update is 70 minutes away, the ASA marks CRLs as stale in 70 minutes.

If the ASA has insufficient memory to store all CRLs cached for a given trustpoint, it deletes the least recently used CRL to make room for a newly retrieved CRL.

OCSP

OCSP provides the ASA with a way of determining whether a certificate that is within its valid time range has been revoked by the issuing CA. OCSP configuration is part of trustpoint configuration.

OCSP localizes certificate status on a validation authority (an OCSP server, also called the *responder*) which the ASA queries for the status of a specific certificate. This method provides better scalability and more up-to-date revocation status than does CRL checking, and helps organizations with large PKI installations deploy and expand secure networks.



Note

The ASA allows a five-second time skew for OCSP responses.

You can configure the ASA to make OCSP checks mandatory when authenticating a certificate by using the **revocation-check ocsf** command. You can also make the OCSP check optional by using the **revocation-check ocsf none** command, which allows the certificate authentication to succeed when the validation authority is unavailable to provide updated OCSP data.

OCSP provides three ways to define the OCSP server URL. The ASA uses these servers in the following order:

1. The OCSP URL defined in a match certificate override rule by using the **match certificate** command).
2. The OCSP URL configured by using the **ocsp url** command.
3. The AIA field of the client certificate.

**Note**

To configure a trustpoint to validate a self-signed OCSP responder certificate, you import the self-signed responder certificate into its own trustpoint as a trusted CA certificate. Then you configure the **match certificate** command in the client certificate validating trustpoint to use the trustpoint that includes the self-signed OCSP responder certificate to validate the responder certificate. Use the same procedure for configuring validating responder certificates external to the validation path of the client certificate.

The OCSP server (responder) certificate usually signs the OCSP response. After receiving the response, the ASA tries to verify the responder certificate. The CA normally sets the lifetime of the OCSP responder certificate to a relatively short period to minimize the chance of being compromised. The CA usually also includes an **ocsp-no-check** extension in the responder certificate, which indicates that this certificate does not need revocation status checking. However, if this extension is not present, the ASA tries to check revocation status using the same method specified in the trustpoint. If the responder certificate is not verifiable, revocation checks fail. To avoid this possibility, use the **revocation-check none** command to configure the responder certificate validating trustpoint, and use the **revocation-check ocsp** command to configure the client certificate.

The Local CA

The local CA performs the following tasks:

- Integrates basic certificate authority operation on the ASA.
- Deploys certificates.
- Provides secure revocation checking of issued certificates.
- Provides a certificate authority on the ASA for use with browser-based and client-based SSL VPN connections.
- Provides trusted digital certificates to users, without the need to rely on external certificate authorization.
- Provides a secure, in-house authority for certificate authentication and offers straightforward user enrollment by means of a website login.

Storage for Local CA Files

The ASA accesses and implements user information, issued certificates, and revocation lists using a local CA database. This database resides in local flash memory by default, or can be configured to reside on an external file system that is mounted and accessible to the ASA.

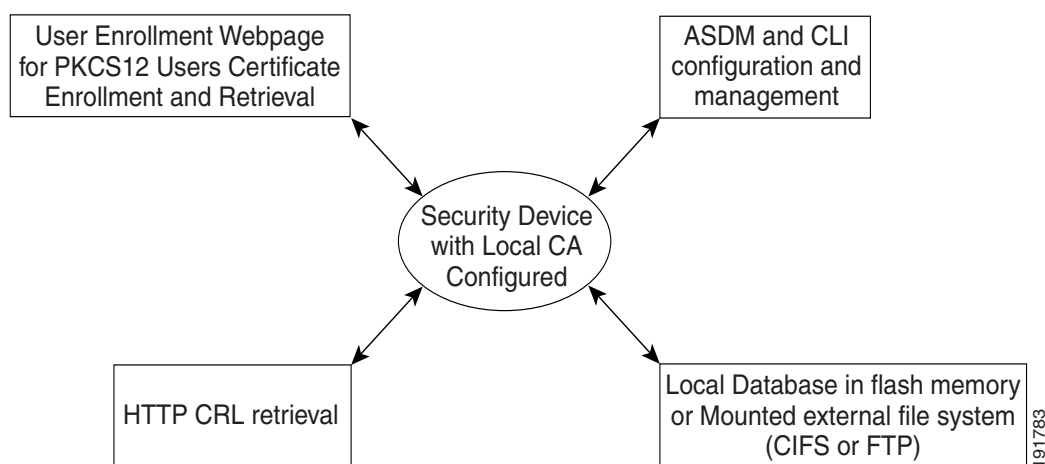
No limits exist on the number of users that can be stored in the local CA user database; however, if flash memory storage issues arise, syslog messages are generated to alert the administrator to take action, and the local CA could be disabled until the storage issues are resolved. Flash memory can store a database with 3500 users or less; however, a database of more than 3500 users requires external storage.

The Local CA Server

After you configure a local CA server on the ASA, users can enroll for a certificate by logging into a website and entering a username and a one-time password that is provided by the local CA administrator to validate their eligibility for enrollment.

As shown in [Figure 40-1](#), the local CA server resides on the ASA and handles enrollment requests from website users and CRL inquiries coming from other certificate validating devices and ASAs. Local CA database and configuration files are maintained either on the ASA flash memory (default storage) or on a separate storage device.

Figure 40-1 *The Local CA*



Using Certificates and User Login Credentials

The following section describes the different methods of using certificates and user login credentials (username and password) for authentication and authorization. These methods apply to IPsec, AnyConnect, and Clientless SSL VPN.

In all cases, LDAP authorization does not use the password as a credential. RADIUS authorization uses either a common password for all users or the username as a password.

This section includes the following topics:

- [Using User Login Credentials, page 40-8](#)
- [Using Certificates, page 40-9](#)

Using User Login Credentials

The default method for authentication and authorization uses the user login credentials.

- Authentication
 - Enabled by the authentication server group setting in the tunnel group (also called ASDM Connection Profile)
 - Uses the username and password as credentials
- Authorization

- Enabled by the authorization server group setting in the tunnel group (also called ASDM Connection Profile)
- Uses the username as a credential

Using Certificates

If user digital certificates are configured, the ASA first validates the certificate. It does not, however, use any of the DN fields from certificates as a username for the authentication.

If both authentication and authorization are enabled, the ASA uses the user login credentials for both user authentication and authorization.

- Authentication
 - Enabled by the authentication server group setting
 - Uses the username and password as credentials
- Authorization
 - Enabled by the authorization server group setting
 - Uses the username as a credential

If authentication is disabled and authorization is enabled, the ASA uses the primary DN field for authorization.

- Authentication
 - DISABLED (set to None) by the authentication server group setting
 - No credentials used
- Authorization
 - Enabled by the authorization server group setting
 - Uses the username value of the certificate primary DN field as a credential



Note

If the primary DN field is not present in the certificate, the ASA uses the secondary DN field value as the username for the authorization request.

For example, consider a user certificate that includes the following Subject DN fields and values:

`Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com`

If the Primary DN = EA (E-mail Address) and the Secondary DN = CN (Common Name), then the username used in the authorization request would be anyuser@example.com.

Licensing Requirements for Digital Certificates

Model	License Requirement
All models	Base License.

Prerequisites for Local Certificates

Local certificates have the following prerequisites:

- Make sure that the ASA is configured correctly to support certificates. An incorrectly configured ASA can cause enrollment to fail or request a certificate that includes inaccurate information.
- Make sure that the hostname and domain name of the ASA are configured correctly. To view the currently configured hostname and domain name, enter the **show running-config** command. For information about configuring the hostname and domain name, see the [“Configuring the Hostname, Domain Name, and Passwords” section on page 16-1](#).
- Make sure that the ASA clock is set accurately before configuring the CA. Certificates have a date and time that they become valid and expire. When the ASA enrolls with a CA and obtains a certificate, the ASA checks that the current time is within the valid range for the certificate. If it is outside that range, enrollment fails. For information about setting the clock, see the [“Setting the Date and Time” section on page 16-3](#).

Prerequisites for SCEP Proxy Support

Configuring the ASA as a proxy to submit requests for third-party certificates has the following requirements:

- AnyConnect Secure Mobility Client 3.0 or later must be running at the endpoint.
- The authentication method, configured in the connection profile for your group policy, must be set to use both AAA and certificate authentication.
- An SSL port must be open for IKEv2 VPN connections.
- The CA must be in auto-grant mode.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

- Supported in single and multiple context mode for a local CA.
- Supported in single context mode only for third-party CAs.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

Failover Guidelines

- Does not support replicating sessions in Stateful Failover.
- Does not support failover for local CAs.

IPv6 Guidelines

Does not support IPv6.

Additional Guidelines

- For ASAs that are configured as CA servers or clients, limit the validity period of the certificate to less than the recommended end date of 03:14:08 UTC, January 19, 2038. This guideline also applies to imported certificates from third-party vendors.
- You cannot configure the local CA when failover is enabled. You can only configure the local CA server for standalone ASAs without failover. For more information, see CSCty43366.
- When a certificate enrollment is completed, the ASA stores a PKCS12 file containing the user's keypair and certificate chain, which requires about 2 KB of flash memory or disk space per enrollment. The actual amount of disk space depends on the configured RSA key size and certificate fields. Keep this guideline in mind when adding a large number of pending certificate enrollments on an ASA with a limited amount of available flash memory, because these PKCS12 files are stored in flash memory for the duration of the configured enrollment retrieval timeout. We recommend using a key size of at least 2048.
- The **lifetime ca-certificate** command takes effect when the local CA server certificate is first generated (that is, when you initially configure the local CA server and issue the **no shutdown** command). When the CA certificate expires, the configured lifetime value is used to generate the new CA certificate. You cannot change the lifetime value for existing CA certificates.
- You should configure the ASA to use an identity certificate to protect ASDM traffic and HTTPS traffic to the management interface. Identity certificates that are automatically generated with SCEP are regenerated after each reboot, so make sure that you manually install your own identity certificates. For an example of this procedure that applies only to SSL, see the following URL: http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809fcf91.shtml.
- The ASA and the AnyConnect clients can only validate certificates in which the X520Serialnumber field (the serial number in the Subject Name) is in PrintableString format. If the serial number format uses encoding such as UTF8, the certificate authorization will fail.
- Use only valid characters and values for certificate parameters when you import them on the ASA.
- To use a wildcard (*) symbol, make sure that you use encoding on the CA server that allows this character in the string value. Although RFC 5280 recommends using either a UTF8String or PrintableString, you should use UTF8String because PrintableString does not recognize the wildcard as a valid character. The ASA rejects the imported certificate if an invalid character or value is found during the import. For example:

```
ERROR: Failed to parse or verify imported certificate ciscoasa(config)# Read
162*H+ytes as CA certificate:0U0= \Ivr"phÖV°3é%b0 CRYPTO_PKI(make trustedCerts list)
CERT-C: E ../cert-c/source/certlist.c(302) : Error #711h
CRYPTO_PKI: Failed to verify the ID certificate using the CA certificate in trustpoint
mm.
CERT-C: E ../cert-c/source/p7contnt.c(169) : Error #703h
crypto_certc_pkcs7_extract_certs_and_crls failed (1795):
crypto_certc_pkcs7_extract_certs_and_crls failed
CRYPTO_PKI: status = 1795: failed to verify or insert the cert into storage
```

Configuring Digital Certificates

This section describes how to configure local CA certificates. Make sure that you follow the sequence of tasks listed to correctly configure this type of digital certificate. This section includes the following topics:

- [Configuring CA Certificate Authentication, page 40-12](#)

- [Configuring CA Certificates for Revocation, page 40-20](#)
- [Configuring CRL Retrieval Policy, page 40-21](#)
- [Configuring CRL Retrieval Methods, page 40-21](#)
- [Configuring OCSP Rules, page 40-22](#)
- [Configuring Advanced CRL and OCSP Settings, page 40-23](#)

This section describes how to configure digital certificates for the ASA Services Module and includes the following topics:

- [Configuring CA Certificate Authentication, page 40-14](#)
- [Adding or Installing a CA Certificate, page 40-15](#)
- [Editing or Removing a CA Certificate Configuration, page 40-15](#)
- [Showing CA Certificate Details, page 40-16](#)
- [Configuring CA Certificates for Revocation, page 40-16](#)
- [Configuring CRL Retrieval Policy, page 40-17](#)
- [Configuring CRL Retrieval Methods, page 40-17](#)
- [Configuring OCSP Rules, page 40-18](#)
- [Configuring Advanced CRL and OCSP Settings, page 40-19](#)

Configuring CA Certificate Authentication

The CA Certificates pane displays the available certificates, identified by the issued to and issued by CA server, the date that the certificate expires, the associated trustpoints, and the certificate usage or purpose. In the CA Certificates pane, you can perform the following tasks:

- Authenticate self-signed or subordinate CA certificates.
- Install CA certificates on the ASA.
- Create a new certificate configuration.
- Edit an existing certificate configuration.
- Obtain a CA certificate manually and import it.
- Have the ASA use SCEP to contact the CA, and then automatically obtain and install the certificate.
- Display details and issuer information for a selected certificate.
- Access the CRL for an existing CA certificate.
- Remove the configuration of an existing CA certificate.
- Save the new or modified CA certificate configuration.
- Discard any changes and return the certificate configuration to the original settings.


This section includes the following topics:

- [Adding or Installing a CA Certificate, page 40-13](#)
- [Editing or Removing a CA Certificate Configuration, page 40-14](#)
- [Showing CA Certificate Details, page 40-14](#)

Adding or Installing a CA Certificate

You can add a new certificate configuration from an existing file, by manually pasting a certificate in PEM format, or by automatic enrollment using SCEP. SCEP is a secure messaging protocol that requires minimal user intervention and lets you enroll and install certificates using only the VPN Concentrator Manager.

To add or install a CA certificate, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Configuration > Remote Access VPN > Certificate Management > CA Certificates**.
- Step 2** Click **Add**.
- The Install Certificate dialog box appears. The selected trustpoint name appears in read-only format.
- Step 3** To add a certificate configuration from an existing file, click the **Install from a file** radio button (this is the default setting).
- Step 4** Enter the path and file name, or click **Browse** to search for the file. Then click **Install Certificate**.
- Step 5** The Certificate Installation dialog box appears with a confirmation message indicating that the certificate was successfully installed. Click **OK** to close this dialog box.
- Step 6** To enroll manually, click the **Paste certificate in PEM format** radio button.
- Step 7** Copy and paste the PEM format (base64 or hexadecimal) certificate into the area provided, then click **Install Certificate**.
- Step 8** The Certificate Installation dialog box appears with a confirmation message indicating that the certificate was successfully installed. Click **OK** to close this dialog box.
- Step 9** To enroll automatically, click the **Use SCEP** radio button. The ASA contacts the CA using SCEP, obtains the certificates, and installs them on the device. To use SCEP, you must enroll with a CA that supports SCEP, and you must enroll via the Internet. Automatic enrollment using SCEP requires that you provide the following information:
- The path and file name of the certificate to be automatically installed.
 - The maximum number of minutes to retry certificate installation. The default is one minute.
 - The number of retries for installing a certificate. The default is zero, which indicates unlimited retries within the retry period.
-  **Note** See [Prerequisites for SCEP Proxy Support](#) when choosing to use the SCEP method to install certificates.
-
- Step 10** To display additional configuration options for new and existing certificates, click **More Options**. The Configuration Options for CA Certificates pane appears.
- Step 11** To continue, see the [“Editing or Removing a CA Certificate Configuration”](#) section on page 40-14.
-

Editing or Removing a CA Certificate Configuration

To change or remove an existing CA certificate configuration, perform the following steps:

- Step 1** To change an existing CA certificate configuration, select it, and then click **Edit**.
- The Edit Options for CA Certificates pane appears. To change any of these settings, see the following sections for procedures:
- “Configuring CRL Retrieval Policy” section on page 40-21
 - “Configuring CRL Retrieval Methods” section on page 40-21
 - “Configuring OCSP Rules” section on page 40-22
 - “Configuring Advanced CRL and OCSP Settings” section on page 40-23
- Step 2** To remove a CA certificate configuration, select it, and then click **Delete**.



Note After you delete a certificate configuration, it cannot be restored. To recreate the deleted certificate, click **Add** to reenter all of the certificate configuration information.

Showing CA Certificate Details

To show detailed information about the selected CA certificate, click **Show Details** to display the Certificate Details dialog box, which includes the following three *display-only* tabs:

- The General tab displays the values for type, serial number, status, usage, public key type, CRL distribution point, the times within which the certificate is valid, and associated trustpoints. The values apply to both available and pending status.
- The Issued to tab displays the X.500 fields of the subject DN or certificate owner and their values. The values apply only to available status.
- The Issued by tab displays the X.500 fields of the entity granting the certificate. The values apply only to available status.

Configuring CA Certificate Authentication

The CA Certificates pane displays the available certificates, identified by the issued to and issued by CA server, the date that the certificate expires, the associated trustpoints, and the certificate usage or purpose. In the CA Certificates pane, you can perform the following tasks:

- Authenticate self-signed or subordinate CA certificates.
- Install CA certificates on the ASA.
- Create a new certificate configuration.
- Edit an existing certificate configuration.
- Obtain a CA certificate manually and import it.
- Display details and issuer information for a selected certificate.
- Access the CRL for an existing CA certificate.

- Remove the configuration of an existing CA certificate.
- Save the new or modified CA certificate configuration.
- Discard any changes and return the certificate configuration to the original settings.

Adding or Installing a CA Certificate

You can add a new certificate configuration from an existing file, by manually pasting a certificate in PEM format.

To add or install a CA certificate, perform the following steps:

-
- | | |
|---------------|---|
| Step 1 | In the main ASDM application window, choose Configuration > Device Management > Certificate Management > CA Certificates . |
| Step 2 | Click Add .

The Install Certificate dialog box appears. The selected trustpoint name appears in read-only format. |
| Step 3 | To add a certificate configuration from an existing file, click the Install from a file radio button (this is the default setting). |
| Step 4 | Enter the path and file name, or click Browse to search for the file. Then click Install Certificate . |
| Step 5 | To enroll manually, click the Paste certificate in PEM format radio button. |
| Step 6 | Copy and paste the PEM format (base64 or hexadecimal) certificate into the area provided, then click Install Certificate . |
| Step 7 | To display additional configuration options for new and existing certificates, click More Options .

The Configuration Options for CA Certificates pane appears. |
| Step 8 | Make your selections, and then click OK. To continue, see the “Editing or Removing a CA Certificate Configuration” section on page 40-15 . |
-

Editing or Removing a CA Certificate Configuration

To change or remove an existing CA certificate configuration, perform the following steps:

-
- | | |
|---------------|--|
| Step 1 | To change an existing CA certificate configuration, select it, and then click Edit .

The Edit Options for CA Certificates pane appears. To change any of these settings, see the following sections for procedures: <ul style="list-style-type: none">• “Configuring CRL Retrieval Policy” section on page 40-17• “Configuring CRL Retrieval Methods” section on page 40-17• “Configuring OCSP Rules” section on page 40-18• “Configuring Advanced CRL and OCSP Settings” section on page 40-19 |
| Step 2 | To remove a CA certificate configuration, select it, and then click Delete . |

**Note**

After you delete a certificate configuration, it cannot be restored. To recreate the deleted certificate, click **Add** to reenter all of the certificate configuration information.

Showing CA Certificate Details

To show detailed information about the selected CA certificate, click **Show Details** to display the Certificate Details dialog box, which includes the following three *display-only* tabs:

- The General tab displays the values for type, serial number, status, usage, public key type, CRL distribution point, the times within which the certificate is valid, and associated trustpoints. The values apply to both available and pending status.
- The Issued to tab displays the X.500 fields of the subject DN or certificate owner and their values. The values apply only to available status.
- The Issued by tab displays the X.500 fields of the entity granting the certificate. The values apply only to available status.

Configuring CA Certificates for Revocation

To configure CA certificates for revocation, perform the following site-to-site task in either single or multiple context mode:

-
- Step 1** In the ASDM application window, choose **Configuration > Site-to-Site VPN > Certificate Management > CA Certificates > Add** to display the Install Certificates dialog box. Then click **More Options**.
- Step 2** In the Configuration Options for CA Certificates pane, click the **Revocation Check** tab.
- Step 3** To disable revocation checking of certificates, click the **Do not check certificates for revocation** radio button.
- Step 4** To select one or more revocation checking methods (CRL or OCSP), click the **Check certificates for revocation** radio button.
- Step 5** In the Revocation Methods area, available methods appear on the left. Click **Add** to move a method to the right and make it available. Click **Move Up** or **Move Down** to change the method order.
- The methods you choose are implemented in the order in which you add them. If a method returns an error, the next revocation checking method activates.
- Step 6** Check the **Consider certificate valid if revocation checking returns errors** check box to ignore revocation checking errors during certificate validation.
- Step 7** Click **OK** to close the Revocation Check tab. Alternatively, to continue, see the [“Configuring CRL Retrieval Policy”](#) section on page 40-17.
-

Configuring CRL Retrieval Policy

To configure the CRL retrieval policy, perform the following steps:

-
- | | |
|---------------|--|
| Step 1 | In the ASDM application window, choose Configuration > Site-to-Site VPN > Certificate Management > CA Certificates > Add to display the Install Certificates dialog box. Then click More Options . |
| Step 2 | Check the Use CRL Distribution Point from the certificate check box to direct revocation checking to the CRL distribution point from the certificate being checked. |
| Step 3 | Check the Use Static URLs configured below check box to list specific URLs to be used for CRL retrieval. The URLs you select are implemented in the order in which you add them. If an error occurs with the specified URL, the next URL in order is taken. |
| Step 4 | In the Static Configuration area, click Add .

The Add Static URL dialog box appears. |
| Step 5 | In the URL field, enter the static URL to use for distributing the CRLs, and then click OK .

The URL that you entered appears in the Static URLs list. |
| Step 6 | To change the static URL, select it, and then click Edit . |
| Step 7 | To remove an existing static URL, select it, and then click Delete . |
| Step 8 | To change the order in which the static URLs appear, click Move Up or Move Down . |
| Step 9 | Click OK to close this tab. Alternatively, to continue, see the “Configuring CRL Retrieval Methods” section on page 40-17 . |
-

Configuring CRL Retrieval Methods

To configure CRL retrieval methods, perform the following steps:

-
- | | |
|---------------|---|
| Step 1 | In the ASDM application window, choose Configuration > Site-to-Site VPN > Certificate Management > CA Certificates > Add to display the Install Certificates dialog box. Then click More Options . |
| Step 2 | In the Configuration Options for CA Certificates pane, click the CRL Retrieval Methods tab. |
| Step 3 | Choose one of the following three retrieval methods: <ul style="list-style-type: none">• To enable LDAP for CRL retrieval, check the Enable Lightweight Directory Access Protocol (LDAP) check box. With LDAP, CRL retrieval starts an LDAP session by connecting to a named LDAP server, accessed by a password. The connection is on TCP port 389 by default. Enter the following required parameters:<ul style="list-style-type: none">– Name– Password– Confirm Password– Default Server (server name)– Default Port (389)• To enable HTTP for CRL retrieval, check the Enable HTTP check box. |

- Step 4** Click **OK** to close this tab. Alternatively, to continue, see the [“Configuring OCSP Rules”](#) section on page 40-18.
-

Configuring OCSP Rules

The ASA examines OCSP rules in priority order, and applies the first one that matches. X.509 digital certificates are an alternative to using CRLs.

**Note**

Make sure that you have configured a certificate map before you try to add OCSP rules. If a certificate map has not been configured, an error message appears. To configure a certificate map, choose **Configuration > Site-to-Site VPN > Advanced > Certificate to Connection Profile Maps > Rules > Add**.

To configure OCSP rules for obtaining revocation status of an X.509 digital certificate, perform the following steps:

- Step 1** In the ASDM application window, choose **Configuration > Site-to-Site VPN > Certificate Management > CA Certificates > Add** to display the Install Certificates dialog box. Then click **More Options**.
- Step 2** In the Configuration Options for CA Certificates pane, click the **OCSP Rules** tab.
- Step 3** Choose the certificate map to match to this OCSP rule. Certificate maps match user permissions to specific fields in a certificate. The name of the CA that the ASA uses to validate responder certificates appears in the Certificate field. The priority number for the rule appears in the Index field. The URL of the OCSP server for this certificate appears in the URL field.
- Step 4** To add a new OCSP rule, click **Add**.
The Add OCSP Rule dialog box appears.
- Step 5** Choose the certificate map to use from the drop-down list.
- Step 6** Choose the certificate to use from the drop-down list.
- Step 7** Enter the priority number for the rule.
- Step 8** Enter the URL of the OCSP server for this certificate.
- Step 9** When you are done, click **OK** to close this dialog box.
The newly added OCSP rule appears in the list.
- Step 10** To edit an existing OCSP rule, select it, and then click **Edit**.
- Step 11** To delete an OCSP rule, select it, and then click **Delete**.
- Step 12** Click **OK** to close this tab. Alternatively, to continue, see the [“Configuring Advanced CRL and OCSP Settings”](#) section on page 40-19.
-

Configuring Advanced CRL and OCSP Settings

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, because of security concerns or a change of name or association. CAs periodically issue a signed list of revoked certificates. Enabling revocation checking forces the ASA to check that the CA has not revoked the certificate being verified. The ASA supports two methods of checking revocation status: CRL and OCSP.

To configure additional CRL and OCSP settings, perform the following steps:

-
- | | |
|---------------|--|
| Step 1 | In the ASDM application window, choose Configuration > Site-to-Site VPN > Certificate Management > CA Certificates > Add to display the Install Certificates dialog box. Then click More Options . |
| Step 2 | In the Configuration Options for CA Certificates pane, click the Advanced tab. |
| Step 3 | In the CRL Options area, enter the number of minutes between cache refreshes. The default is 60 minutes. The range is 1-1440 minutes. To avoid having to retrieve the same CRL from a CA repeatedly, the ASA 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 ASA removes the least recently used CRL until more space becomes available. |
| Step 4 | Check the Enforce next CRL update check box to require valid CRLs to have a Next Update value that has not expired. Uncheck the Enforce next CRL update check box to let valid CRLs with no Next Update value or a Next Update value that has expired. |
| Step 5 | In the OCSP Options area, enter the URL for the OCSP server. The ASA uses OCSP servers according to the following order: <ol style="list-style-type: none">1. OCSP URL in a match certificate override rule2. OCSP URL configured in the selected OCSP Options attribute3. AIA field of a user certificate |
| Step 6 | By default, the Disable nonce extension check box is checked, which cryptographically binds requests with responses to avoid replay attacks. This process works by matching the extension in the request to that in the response, ensuring that they are the same. Uncheck the Disable nonce extension check box if the OCSP server you are using sends pregenerated responses that do not include this matching nonce extension. |
| Step 7 | In the Other Options area, choose one of the following options: <ul style="list-style-type: none">• Check the Accept certificates issued by this CA check box to indicate that the ASA should accept certificates from the specified CA.• Check the Accept certificates issued by the subordinate CAs of this CA check box to indicate that the ASA should accept certificates from the subordinate CA. |
| Step 8 | Click OK to close this tab, and then click Apply to save your configuration changes. |
-

What to Do Next

See the [“Monitoring CRLs” section on page 40-20](#).

Monitoring CRLs

To monitor CRLs, perform the following steps:

-
- Step 1** In the ASDM main application window, choose **Monitoring > Properties > CRL**.
- Step 2** In the CRL area, choose the CA certificate name from the drop-down list.
- Step 3** To display CRL details, click **View CRL**. For example:
- ```
CRL Issuer Name:
cn=asa4.cisco.com
LastUpdate: 09:58:34 UTC Nov 11 2009
NextUpdate: 15:58:34 UTC Nov 11 2009
Cached Until: 15:58:34 UTC Nov 11 2009
Retrieved from CRL Distribution Point:
 ** CDP Not Published - Retrieved via SCEP
Size (bytes): 224
Associated Trustpoints: LOCAL-CA-SERVER
```
- Step 4** When you are done, click **Clear CRL** to remove the CRL details and choose another CA certificate to view.
- 

## Configuring CA Certificates for Revocation

To configure CA certificates for revocation, perform the following steps:

- 
- Step 1** In the Configuration Options for CA Certificates pane, click the **Revocation Check** tab.
- Step 2** To disable revocation checking of certificates, click the **Do not check certificates for revocation** radio button.
- Step 3** To select one or more revocation checking methods (CRL or OCSP), click the **Check certificates for revocation** radio button.
- Step 4** In the Revocation Methods area, available methods appear on the left. Click **Add** to move a method to the right and make it available. Click **Move Up** or **Move Down** to change the method order.
- The methods that you choose are implemented in the order in which you add them. If a method returns an error, the next revocation checking method activates.
- Step 5** Check the **Consider certificate valid if revocation checking returns errors** check box to ignore revocation checking errors during certificate validation.
- Step 6** Click **OK** to close the Revocation Check tab. Alternatively, to continue, see the [“Configuring CRL Retrieval Policy” section on page 40-21](#).
-

## Configuring CRL Retrieval Policy

To configure the CRL retrieval policy, perform the following steps:

- 
- |               |                                                                                                                                                                                                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the Configuration Options for CA Certificates pane, click the <b>CRL Retrieval Policy</b> tab.                                                                                                                                                                  |
| <b>Step 2</b> | Check the <b>Use CRL Distribution Point from the certificate</b> check box to direct revocation checking to the CRL distribution point from the certificate being checked.                                                                                         |
| <b>Step 3</b> | Check the <b>Use Static URLs configured below</b> check box to list specific URLs to be used for CRL retrieval. The URLs you select are implemented in the order in which you add them. If an error occurs with the specified URL, the next URL in order is taken. |
| <b>Step 4</b> | In the Static Configuration area, click <b>Add</b> .<br><br>The Add Static URL dialog box appears.                                                                                                                                                                 |
| <b>Step 5</b> | In the URL field, enter the static URL to use for distributing the CRLs, and then click <b>OK</b> .<br><br>The URL that you entered appears in the Static URLs list.                                                                                               |
| <b>Step 6</b> | To change the static URL, select it, and then click <b>Edit</b> .                                                                                                                                                                                                  |
| <b>Step 7</b> | To remove an existing static URL, select it, and then click <b>Delete</b> .                                                                                                                                                                                        |
| <b>Step 8</b> | To change the order in which the static URLs appear, click <b>Move Up</b> or <b>Move Down</b> .                                                                                                                                                                    |
| <b>Step 9</b> | Click <b>OK</b> to close this tab. Alternatively, to continue, see the <a href="#">“Configuring CRL Retrieval Methods” section on page 40-21</a> .                                                                                                                 |
- 

## Configuring CRL Retrieval Methods

To configure CRL retrieval methods, perform the following steps:

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the Configuration Options for CA Certificates pane, click the <b>CRL Retrieval Methods</b> tab.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Step 2</b> | Choose one of the following three retrieval methods: <ul style="list-style-type: none"><li>• To enable LDAP for CRL retrieval, check the <b>Enable Lightweight Directory Access Protocol (LDAP)</b> check box. With LDAP, CRL retrieval starts an LDAP session by connecting to a named LDAP server, accessed by a password. The connection is on TCP port 389 by default. Enter the following required parameters:<ul style="list-style-type: none"><li>– Name</li><li>– Password</li><li>– Confirm Password</li><li>– Default Server (server name)</li><li>– Default Port (389)</li></ul></li><li>• To enable HTTP for CRL retrieval, check the <b>Enable HTTP</b> check box.</li><li>• To enable SCEP for CRL retrieval, check the <b>Enable Simple Certificate Enrollment Protocol (SCEP)</b> check box.</li></ul> |

- Step 3** Click **OK** to close this tab. Alternatively, to continue, see the “[Configuring OCSP Rules](#)” section on [page 40-22](#).
- 

## Configuring OCSP Rules

The ASA examines OCSP rules in priority order, and applies the first one that matches. X.509 digital certificates are an alternative to using CRLs.

**Note**

Make sure that you have configured a certificate map before you try to add OCSP rules. If a certificate map has not been configured, an error message appears. To configure a certificate map, choose **Configuration > Network (Client) Access, Advanced > IPsec > Certificate to Connection Profile Maps > Rules > Add**.

---

To configure OCSP rules for obtaining revocation status of an X.509 digital certificate, perform the following steps:

---

- Step 1** In the Configuration Options for CA Certificates pane, click the **OCSP Rules** tab.
- Step 2** Choose the certificate map to match to this OCSP rule. Certificate maps match user permissions to specific fields in a certificate. The name of the CA that the ASA uses to validate responder certificates appears in the Certificate field. The priority number for the rule appears in the Index field. The URL of the OCSP server for this certificate appears in the URL field.
- Step 3** To add a new OCSP rule, click **Add**.  
The Add OCSP Rule dialog box appears.
- Step 4** Choose the certificate map to use from the drop-down list.
- Step 5** Choose the certificate to use from the drop-down list.
- Step 6** Enter the priority number for the rule.
- Step 7** Enter the URL of the OCSP server for this certificate.
- Step 8** When you are done, click **OK** to close this dialog box.  
The newly added OCSP rule appears in the list.
- Step 9** To edit an existing OCSP rule, select it, and then click **Edit**.
- Step 10** To delete an OCSP rule, select it, and then click **Delete**.
- Step 11** Click **OK** to close this tab. Alternatively, to continue, see the “[Configuring Advanced CRL and OCSP Settings](#)” section on [page 40-23](#).
-

## Configuring Advanced CRL and OCSP Settings

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, because of security concerns or a change of name or association. CAs periodically issue a signed list of revoked certificates. Enabling revocation checking forces the ASA to check that the CA has not revoked the certificate being verified. The ASA supports two methods of checking revocation status: CRL and OCSP.

To configure additional CRL and OCSP settings, perform the following steps:

- 
- Step 1** In the Configuration Options for CA Certificates pane, click the **Advanced** tab.
- Step 2** In the CRL Options area, enter the number of minutes between cache refreshes. The default is 60 minutes. The range is 1-1440 minutes. To avoid having to retrieve the same CRL from a CA repeatedly, the ASA 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 ASA removes the least recently used CRL until more space becomes available.
- Step 3** Check the **Enforce next CRL update** check box to require valid CRLs to have a Next Update value that has not expired. Uncheck the **Enforce next CRL update** check box to let valid CRLs with no Next Update value or a Next Update value that has expired.
- Step 4** In the OCSP Options area, enter the URL for the OCSP server. The ASA uses OCSP servers according to the following order:
1. OCSP URL in a match certificate override rule
  2. OCSP URL configured in the selected OCSP Options attribute
  3. AIA field of a remote user certificate
- Step 5** By default, the **Disable nonce extension** check box is checked, which cryptographically binds requests with responses to avoid replay attacks. This process works by matching the extension in the request to that in the response, ensuring that they are the same. Uncheck the **Disable nonce extension** check box if the OCSP server you are using sends pregenerated responses that do not include this matching nonce extension.
- Step 6** In the Validation Policy area, choose one of the following options:
- Click the **SSL** radio button or the **IPsec** radio button to restrict the type of remote session that this CA can be used to validate.
  - Click the **SSL and IPsec** radio buttons to let the CA validate both types of sessions.
- Step 7** In the Other Options area, choose one of the following options:
- Check the **Accept certificates issued by this CA** check box to indicate that the ASA should accept certificates from the specified CA.
  - Check the **Accept certificates issued by the subordinate CAs of this CA** check box to indicate that the ASA should accept certificates from the subordinate CA.
- Step 8** Click **OK** to close this tab, and then click **Apply** to save your configuration changes.
-

## What to Do Next

See the “[Configuring Identity Certificates Authentication](#)” section on page 40-24.

# Configuring Identity Certificates Authentication

An identity certificate can be used to authenticate VPN access through the ASA. In the Identity Certificates Authentication pane, you can perform the following tasks:

- Add or import a new identity certificate.
- Display details of an identity certificate.
- Delete an existing identity certificate.
- Export an existing identity certificate.
- Install an existing identity certificate.
- Enroll for an identity certificate with Entrust.

This section includes the following topics:

- [Adding or Importing an Identity Certificate, page 40-24](#)
- [Showing Identity Certificate Details, page 40-26](#)
- [Deleting an Identity Certificate, page 40-27](#)
- [Exporting an Identity Certificate, page 40-27](#)
- [Generating a Certificate Signing Request, page 40-27](#)
- [Installing Identity Certificates, page 40-28](#)

## Adding or Importing an Identity Certificate

To add or import a new identity certificate configuration, perform the following:

- 
- |               |                                                                                                                                                                                             |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the main ASDM application window, choose <b>Configuration &gt; Remote Access VPN &gt; Certificate Management &gt; Identity Certificates</b> .                                            |
| <b>Step 2</b> | Click <b>Add</b> .<br><br>The Add Identity Certificate dialog box appears, with the selected trustpoint name displayed at the top.                                                          |
| <b>Step 3</b> | To import an identity certificate from an existing file, click the <b>Import the identity certificate from a file (PKCS12 format with Certificate(s) + Private Key)</b> radio button.       |
| <b>Step 4</b> | Enter the passphrase used to decrypt the PKCS12 file.                                                                                                                                       |
| <b>Step 5</b> | Enter the path name of the file, or click <b>Browse</b> to display the Import ID Certificate File dialog box. Find the certificate file, and then click <b>Import ID Certificate File</b> . |
| <b>Step 6</b> | To add a new identity certificate, click the <b>Add a new identity certificate</b> radio button.                                                                                            |
| <b>Step 7</b> | Click <b>New</b> to display the Add Key Pair dialog box.                                                                                                                                    |
| <b>Step 8</b> | Choose the <b>RSA</b> or <b>ECDSA</b> key type.                                                                                                                                             |



**Note**

The 4096-bit RSA keys are only supported on the 5580, 5585, or later platforms. If you are configuring a cryptography map to use an RSA or ECDSA trustpoint for authentication, you must first generate the key set. You can then create the trustpoint and reference it in the tunnel group configuration.

- Step 9** To use the default key pair name, click the **Use default keypair name** radio button.
- Step 10** To use a new key pair name, click the **Enter a new key pair name** radio button, and type the new name. The ASA supports multiple key pairs.
- Step 11** Choose the modulus size from the drop-down list. If you are not sure of the modulus size, consult Entrust.
- Step 12** Choose the key pair usage by clicking the **General purpose** radio button (default) or **Special** radio button. When you choose the **Special** radio button, the ASA generates two key pairs, one for signature use and one for encryption use. This selection indicates that two certificates are required for the corresponding identity.
- Step 13** Click **Generate Now** to create new key pairs, and then click **Show** to display the Key Pair Details dialog box, which includes the following *display-only* information:
- The name of the key pair whose public key is to be certified.
  - The time of day and the date when the key pair is generated.
  - The usage of an RSA key pair.
  - The modulus size (bits) of the key pairs: 512, 768, 1024, and 2048. The default is 1024.
  - The key data, which includes the specific key data in text format.
- Step 14** Click **OK** when you are done to close the Key Pair Details dialog box.
- Step 15** Choose a certificate subject DN to form the DN in the identity certificate. and then click **Select** to display the Certificate Subject DN dialog box.
- Step 16** Choose one or more DN attributes that you want to add from the drop-down list, enter a value, and then click **Add**. Available X.500 attributes for the Certificate Subject DN are the following:
- Common Name (CN)
  - Department (OU)
  - Company Name (O)
  - Country (C)
  - State/Province (ST)
  - Location (L)
  - E-mail Address (EA)
- Step 17** Click **OK** when you are done to close the Certificate Subject DN dialog box.
- Step 18** To create self-signed certificates, check the **Generate self-signed certificate** check box.
- Step 19** To have the identity certificate act as the local CA, check the **Act as local certificate authority and issue dynamic certificates to TLS proxy** check box.
- Step 20** To establish additional identity certificate settings, click **Advanced**.
- The Advanced Options dialog box appears, with the following three tabs: Certificate Parameters, Enrollment Mode, and SCEP Challenge Password.

**Note**

Enrollment mode settings and the SCEP challenge password are not available for self-signed certificates.

- Step 21** Click the **Certificate Parameters** tab, and then enter the following information:
- The FQDN, an unambiguous domain name, to indicate the position of the node in the DNS tree hierarchy.
  - The e-mail address associated with the identity certificate.
  - The ASA IP address on the network in four-part, dotted-decimal notation.
  - To add the ASA serial number to the certificate parameters, check the **Include serial number of the device** check box.
- Step 22** Click the **Enrollment Mode** tab, and then enter the following information:
- Choose the enrollment method by clicking the **Request by manual enrollment** radio button or the **Request from a CA** radio button.
  - The enrollment URL of the certificate to be automatically installed through SCEP.
  - The maximum number of minutes allowed to retry installing an identity certificate. The default is one minute.
  - The maximum number of retries allowed for installing an identity certificate. The default is zero, which indicates an unlimited number of retries within the retry period.
- Step 23** Click the **SCEP Challenge Password** tab, and then enter the following information:
- The SCEP password
  - The SCEP password confirmation
- Step 24** Click **OK** when you are done to close the Advanced Options dialog box.
- Step 25** Click **Add Certificate** in the Add Identity Certificate dialog box.
- The new identity certificate appears in the Identity Certificates list.
- Step 26** Click **Apply** to save the new identity certificate configuration.

## Showing Identity Certificate Details

To show detailed information about the selected identity certificate, click **Show Details** to display the Certificate Details dialog box, which includes the following three *display-only* tabs:

- The General tab displays the values for type, serial number, status, usage, public key type, CRL distribution point, the times within which the certificate is valid, and associated trustpoints. The values apply to both available and pending status.
- The Issued to tab displays the X.500 fields of the subject DN or certificate owner and their values. The values apply only to available status.
- The Issued by tab displays the X.500 fields of the entity granting the certificate. The values apply only to available status.

## Deleting an Identity Certificate

To remove an identity certificate configuration, select it, and then click **Delete**.



**Note** After you delete a certificate configuration, it cannot be restored. To recreate the deleted certificate, click **Add** to reenter all of the certificate configuration information.

## Exporting an Identity Certificate

You can export a certificate configuration with all associated keys and certificates in PKCS12 format, which is the public key cryptography standard, and can be base64 encoded or in hexadecimal format. A complete 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 certificates across a group of ASAs; for example, remote access clients calling in to a central organization that has several units to service the calls. These units must have equivalent certificate configurations. In this case, an administrator can export a certificate configuration and then import it across the group of ASAs.

To export an identity certificate, perform the following steps:

- Step 1** Click **Export** to display the Export Certificate dialog box.
- Step 2** Enter the name of the PKCS12 format file to use in exporting the certificate configuration. Alternatively, click **Browse** to display the Export ID Certificate File dialog box to find the file to which you want to export the certificate configuration.
- Step 3** Choose the certificate format by clicking the **PKCS12 Format** radio button or the **PEM Format** radio button.
- Step 4** Enter the passphrase used to encrypt the PKCS12 file for export.
- Step 5** Confirm the encryption passphrase.
- Step 6** Click **Export Certificate** to export the certificate configuration.

An information dialog box appears, informing you that the certificate configuration file has been successfully exported to the location that you specified.

## Generating a Certificate Signing Request

To generate a certificate signing request to send to Entrust, perform the following steps:

- Step 1** Click **Enroll ASA SSL VPN with Entrust** to display the Generate Certificate Signing Request dialog box.
- Step 2** In the Key Pair area, perform the following steps:
  - a. Choose one of the configured key pairs from the drop-down list.
  - b. Click **Show** to display the Key Details dialog box, which provides information about the selected key pair, including date and time generated, usage (general or special purpose), modulus size, and key data.

- c. Click **OK** when you are done to close Key Details dialog box.
  - d. Click **New** to display the Add Key Pair dialog box. To continue, go to Step 8 of the [“Adding or Importing an Identity Certificate”](#) section on page 40-24. When you generate the key pair, you can send it to the ASA or save it to a file.
- Step 3** In the Certificate Subject DN area, enter the following information:
- a. The FQDN or IP address of the ASA.
  - b. The name of the company.
  - c. The two-letter country code.
- Step 4** In the Optional Parameters area, perform the following steps:
- a. Click **Select** to display the Additional DN Attributes dialog box.
  - b. Choose the attribute to add from the drop-down list, and then enter a value.
  - c. Click **Add** to add each attribute to the attribute table.
  - d. Click **Delete** to remove an attribute from the attribute table.
  - e. Click **OK** when you are done to close the Additional DN Attributes dialog box.
- The added attributes appear in the Additional DN Attributes field.
- Step 5** Enter additional fully qualified domain name information if the CA requires it.
- Step 6** Click **Generate Request** to generate the certificate signing request, which you can then send to Entrust, or save to a file and send later.
- The Enroll with Entrust dialog box appears, with the CSR displayed.
- Step 7** To complete the enrollment process, click the **request a certificate from Entrust** link by copying and pasting the CSR provided and submitting it through the Entrust web form, provided at <http://www.entrust.net/cisco/>. Alternatively, to enroll at a later time, save the generated CSR to a file, then click the **enroll with Entrust** link on the Identity Certificates pane to complete the enrollment process.
- Step 8** Entrust issues a certificate after verifying the authenticity of your request, which may take several days. You then need to install the certificate by selecting the pending request in the Identity Certificate pane and clicking **Install**. Click **Close** to close the Enroll with Entrust dialog box.
- 

## Installing Identity Certificates

The Install button on the Identity Certificates pane is dimmed unless an enrollment is pending. Whenever the ASA receives a CSR, the Identity Certificates pane displays the pending ID certificate. When you select the pending Identity Certificate, the Install button activates.

When you transmit the pending request to a CA, the CA enrolls it and returns a certificate to the ASA. After you have received the certificate, click **Install** and highlight the appropriate identity certificate to complete the operation.

To installing a pending identity certificate, perform the following steps:

- 
- Step 1** In the Identity Certificates pane, click **Add** to display the Add Identity Certificate dialog box.
  - Step 2** In the Add Identity Certificate dialog box, click the **Add a new identity certificate** radio button.
  - Step 3** (Optional) Change the key pair or create a new key pair. A key pair is required.

- Step 4** Enter the Certificate Subject DN information, and then click **Select** to display the Certificate Subject DN dialog box.
- Step 5** Specify all of the subject DN attributes required by the CA involved, and then click **OK** to close the Certificate Subject DN dialog box.
- Step 6** In the Add Identity Certificate dialog box, click **Advanced** to display the Advanced Options dialog box.
- Step 7** To continue, see Steps 17 through 23 of the [“Configuring Identity Certificates Authentication”](#) section on page 40-24.
- Step 8** In the Add Identity Certificate dialog box, click **Add Certificate**.  
The Identity Certificate Request dialog box appears.
- Step 9** Enter the CSR file name of type, text, such as c:\verisign-csr.txt, and then click **OK**.
- Step 10** Send the CSR text file to the CA. Alternatively, you can paste the text file into the CSR enrollment page on the CA website.
- Step 11** When the CA returns the Identity Certificate to you, go to the Identity Certificates pane, select the pending certificate entry, and click **Install**.  
The Install Identity Certificate dialog box appears.
- Step 12** Choose one of the following options by clicking the applicable radio button:
- **Install from a file.**  
Alternatively, click **Browse** to search for the file.
  - **Paste the certificate data in base-64 format.**  
Paste the copied certificate data into the area provided.
- Step 13** Click **Install Certificate**.
- Step 14** Click **Apply** to save the newly installed certificate with the ASA configuration.
- 

## What to Do Next

See the [“Configuring Code Signer Certificates”](#) section on page 40-29.

# Configuring Code Signer Certificates

Code signing appends a digital signature to the actual executable code. This digital signature provides enough information to authenticate the signer, and ensure that the code has not been modified after being signed.

Code signer certificates are special certificates whose associated private keys are used to create digital signatures. The certificates used to sign code are obtained from a CA, in which the signed code reveals the certificate origin. You can import code signer certificates on the Code Signer pane, or choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Java Code Signer**.

In the Code Signer pane, you can perform the following tasks:

- Display details of a code signer certificate.
- Delete an existing code signer certificate.
- Import an existing code signer certificate.

- Export an existing code signer certificate.
- Enroll for a code signer certificate with Entrust.

This section includes the following topics:

- [Showing Code Signer Certificate Details, page 40-30](#)
- [Deleting a Code Signer Certificate, page 40-30](#)
- [Importing a Code Signer Certificate, page 40-30](#)
- [Exporting a Code Signer Certificate, page 40-31](#)

## Showing Code Signer Certificate Details

To show detailed information about the selected identity certificate, click **Show Details** to display the Certificate Details dialog box, which includes the following three *display-only* tabs:

- The General tab displays the values for type, serial number, status, usage, public key type, CRL distribution point, the times within which the certificate is valid, and associated trustpoints. The values apply to both available and pending status.
- The Issued to tab displays the X.500 fields of the subject DN or certificate owner and their values. The values apply only to available status.
- The Issued by tab displays the X.500 fields of the entity granting the certificate. The values apply only to available status.

## Deleting a Code Signer Certificate

To remove a code signer certificate configuration, select it, and then click **Delete**.

**Note**

After you delete a certificate configuration, it cannot be restored. To recreate the deleted certificate, click **Import** to reenter all of the certificate configuration information.

## Importing a Code Signer Certificate

To import a code signer certificate, perform the following steps:

- 
- Step 1** In the Code Signer pane, click **Import** to display the Import Certificate dialog box.
  - Step 2** Enter the passphrase used to decrypt the PKCS12-format file.
  - Step 3** Enter the name of the file to import, or click **Browse** to display the Import ID Certificate File dialog box and search for the file.
  - Step 4** Select the file to import and click **Import ID Certificate File**.  
The selected certificate file appears in the Import Certificate dialog box.
  - Step 5** Click **Import Certificate**.  
The imported certificate appears in the Code Signer pane.

**Step 6** Click **Apply** to save the newly imported code signer certificate configuration.

---

## Exporting a Code Signer Certificate

To export a code signer certificate, perform the following steps:

- 
- Step 1** In the Code Signer pane, click **Export** to display the Export Certificate dialog box.
- Step 2** Enter the name of the PKCS12 format file to use in exporting the certificate configuration.
- Step 3** In the Certificate Format area, to use the public key cryptography standard, which can be base64 encoded or in hexadecimal format, click the **PKCS12 format** radio button. Otherwise, click the **PEM format** radio button.
- Step 4** Click **Browse** to display the **Export ID Certificate File** dialog box to find the file to which you want to export the certificate configuration.
- Step 5** Select the file and click **Export ID Certificate File**.  
The selected certificate file appears in the Export Certificate dialog box.
- Step 6** Enter the passphrase used to decrypt the PKCS12 format file for export.
- Step 7** Confirm the decryption passphrase.
- Step 8** Click **Export Certificate** to export the certificate configuration.
- 

### What to Do Next

See the [“Authenticating Using the Local CA” section on page 40-31](#).

## Authenticating Using the Local CA

The local CA provides a secure, configurable in-house authority that resides on the ASA for certificate authentication to use with browser-based and client-based SSL VPN connections.

Users enroll by logging in to a specified website. The local CA integrates basic certificate authority operations on the ASA, deploys certificates, and provides secure revocation checking of issued certificates.

The local CA lets you perform the following tasks:

- Configure the local CA server.
- Revoke and un revoke local CA certificates.
- Update CRLs.
- Add, edit, and delete local CA users.

This section includes the following topics:

- [Configuring the Local CA Server, page 40-32](#)
- [Deleting the Local CA Server, page 40-34](#)

## Configuring the Local CA Server

To configure a local CA server on the ASA, perform the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > CA Server**.

**Step 2** To activate the local CA server, check the **Enable Certificate Authority Server** check box. The default setting is disabled (unchecked). After you enable the local CA server, the ASA generates the local CA server certificate, key pair, and necessary database files, then archives the local CA server certificate and key pair in a PKCS12 file.



**Note** Be sure to review all optional settings carefully before you enable the configured local CA. After you enable it, the certificate issuer name and key size server values cannot be changed.

The self-signed certificate key usage extension enables key encryption, key signature, CRL signature, and certificate signature.

**Step 3** When you enable the local CA for the first time, you must enter and confirm an alphanumeric Enable passphrase, which must have a minimum of seven, alphanumeric characters. The passphrase protects the local CA certificate and the local CA certificate key pair archived in storage, and secures the local CA server from unauthorized or accidental shutdown. The passphrase is required to unlock the PKCS12 archive if the local CA certificate or key pair is lost and must be restored.



**Note** The Enable passphrase is required to enable the local CA server. Be sure to keep a record of the Enable passphrase in a safe location.

**Step 4** Click **Apply** to save the local CA certificate and key pair, so the configuration is not lost if you reboot the ASA.

**Step 5** To change or reconfigure the local CA after the local CA has been configured for the first time, you must shut down the local CA server on the ASA by unchecking the **Enable Certificate Authority Server** check box. In this state, the configuration and all associated files remain in storage and enrollment is disabled.

After the configured local CA has been enabled, the following two settings are *display-only*:

- The Issuer Name field, which lists the issuer subject name and domain name, and is formed using the username and the subject-name-default DN setting as cn=FQDN. The local CA server is the entity that grants the certificate. The default certificate name is provided in the format, cn=hostname.domainname.
- The CA Server Key Size setting, which is used for the server certificate generated for the local CA server. Key sizes can be 512, 768, 1024, or 2048 bits per key. The default is 1024 bits per key. We recommend that you use a key size of at least 2048.

**Step 6** From the drop-down list, choose the client key size of the key pair to be generated for each user certificate issued by the local CA server. Key sizes can be 512, 768, 1024, or 2048 bits per key. The default is 1024 bits per key. We recommend that you use a key size of at least 2048.

**Step 7** Enter the CA certificate lifetime value, which specifies the number of days that the CA server certificate is valid. The default is 3650 days (10 years). Make sure that you limit the validity period of the certificate to less than the recommended end date of 03:14:08 UTC, January 19, 2038.



The local CA server automatically generates a replacement CA certificate 30 days before expiration, which enables the replacement certificate to be exported and imported onto any other devices for local CA certificate validation of user certificates that have been issued by the local CA after they have expired.

To notify users of the upcoming expiration, the following syslog message appears in the Latest ASDM Syslog Messages pane:

```
%ASA-1-717049: Local CA Server certificate is due to expire in days days and a replacement certificate is available for export.
```



**Note** When notified of this automatic rollover, the administrator must take action to make sure that the new local CA certificate is imported to all necessary devices before it expires.

**Step 8** Enter the client certificate lifetime value, which specifies the number of days that a user certificate issued by the CA server is valid. The default is 365 days (one year). Make sure that you limit the validity period of the certificate to less than the recommended end date of 03:14:08 UTC, January 19, 2038.

In the SMTP Server & Email Settings area, you set up e-mail access for the local CA server by specifying the following settings:

- a. Enter the SMTP mail server name or IP address. Alternatively, click the ellipses (...) to display the Browse Server Name/IP Address dialog box, where you can choose the server name or IP address. Click **OK** when you are done to close the Browse Server Name/IP Address dialog box.
- b. Enter the from address, from which to send e-mail messages to local CA users, in the format "adminname@hostname.com." Automatic e-mail messages carry one-time passwords to newly enrolled users and issue e-mail messages when certificates need to be renewed or updated.
- c. Enter the subject, which specifies the subject line in all messages that are sent to users by the local CA server. If you do not specify a subject, the default is "Certificate Enrollment Invitation."

**Step 9** To configure additional options, click the **More Options** drop-down arrow.

**Step 10** Enter the CRL distribution point, which is the CRL location on the ASA. The default location is `http://hostname.domain/+CSCOCA+/asa_ca.crl`.

**Step 11** To make the CRL available for HTTP download on a given interface and port, choose a publish-CRL interface from the drop-down list. Then enter the port number, which can be any port number from 1-65535. The default port number is TCP port 80.



**Note** You cannot rename the CRL; it always has the name, `LOCAL-CA-SERVER.crl`.

For example, enter the URL, `http://10.10.10.100/user8/my_crl_file`. In this case, only the interface with the specified IP address works and when the request comes in, the ASA matches the path, `/user8/my_crl_file` to the configured URL. When the path matches, the ASA returns the stored CRL file.

**Step 12** Enter the CRL lifetime in hours that the CRL is valid. The default for the CA certificate is six hours.

The local CA updates and reissues the CRL each time that a user certificate is revoked or unrevoked, but if no revocation changes occur, the CRL is reissued once every CRL lifetime. You can force an immediate CRL update and regeneration by clicking **Request CRL** in the CA Certificates pane.

**Step 13** Enter the database storage location to specify a storage area for the local CA configuration and data files. The ASA accesses and implements user information, issued certificates, and revocation lists using a local CA database. Alternatively, to specify an external file, enter the path name to the external file or click **Browse** to display the Database Storage Location dialog box.

**Step 14** Choose the storage location from the list of folders that appears, and click **OK**.

**Note**

Flash memory can store a database with 3500 users or less; a database of more than 3500 users requires external storage.

**Step 15** Enter a default subject (DN string) to append to a username on issued certificates. The permitted DN attributes are provided in the following list:

- CN (Common Name)
- SN (Surname)
- O (Organization Name)
- L (Locality)
- C (Country)
- OU (Organization Unit)
- EA (E-mail Address)
- ST (State/Province)
- T (Title)

**Step 16** Enter the number of hours for which an enrolled user can retrieve a PKCS12 enrollment file to enroll and retrieve a user certificate. The enrollment period is independent of the OTP expiration period. The default is 24 hours.

**Note**

Certificate enrollment for the local CA is supported only for clientless SSL VPN connections. For this type of connection, communications between the client and the ASA is through a web browser that uses standard HTML.

**Step 17** Enter the length of time that a one-time password e-mailed to an enrolling user is valid. The default is 72 hours.

**Step 18** Enter the number of days before expiration reminders are e-mailed to users. The default is 14 days.

**Step 19** Click **Apply** to save the new or modified CA certificate configuration. Alternatively, click **Reset** to remove any changes and return to the original settings.

## Deleting the Local CA Server

To remove the local CA server from the ASA, perform the following steps:

**Step 1** In the CA Server pane, click **Delete Certificate Authority Server**.

The Delete Certificate Authority dialog box appears.

**Step 2** To delete the CA server, click **OK**. To retain the CA server, click **Cancel**.

**Note**

After you delete the local CA server, it cannot be restored or recovered. To recreate the deleted CA server configuration, you must reenter all of the CA server configuration information.

## What to Do Next

See the [“Managing the User Database” section on page 40-35](#).

# Managing the User Database

The local CA user database includes user identification information and user status (enrolled, allowed, revoked, and so on). In the Manage User Database pane, you can perform the following tasks:

- Add a user to the local CA database.
- Change existing user identification information.
- Remove a user from the local CA database.
- Enroll a user.
- Update CRLs.
- E-mail OTPs to a user.
- View or regenerate (replace) an OTP.

This section includes the following topics:

- [Adding a Local CA User, page 40-35](#)
- [Sending an Initial OTP or Replacing OTPs, page 40-36](#)
- [Editing a Local CA User, page 40-36](#)
- [Deleting a Local CA User, page 40-37](#)
- [Allowing User Enrollment, page 40-37](#)
- [Viewing or Regenerating an OTP, page 40-37](#)

## Adding a Local CA User

To add a local CA user, perform the following steps:

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | To enter a new user into the local CA database, click <b>Add</b> to display the Add User dialog box.                                                                                                                                                                                                                                                                                                      |
| <b>Step 2</b> | Enter a valid username.                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Step 3</b> | Enter an existing valid e-mail address.                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Step 4</b> | Enter the subject (DN string). Alternatively, click <b>Select</b> to display the Certificate Subject DN dialog box.                                                                                                                                                                                                                                                                                       |
| <b>Step 5</b> | Choose one or more DN attributes that you want to add from the drop-down list, enter a value, and then click <b>Add</b> . Available X.500 attributes for the Certificate Subject DN are the following: <ul style="list-style-type: none"><li>• Common Name (CN)</li><li>• Department (OU)</li><li>• Company Name (O)</li><li>• Country (C)</li><li>• State/Province (ST)</li><li>• Location (L)</li></ul> |

- E-mail Address (EA)

**Step 6** Click **OK** when you are done to close the Certificate Subject DN dialog box.

**Step 7** Check the **Allow enrollment** check box to enroll the user, and then click **Add User**.

The new user appears in the Manage User Database pane.

---

## Sending an Initial OTP or Replacing OTPs

To automatically send an e-mail notice of enrollment permission with a unique OTP and the local CA enrollment URL to the newly added user, click **Email OTP**.

An Information dialog box appears indicating that the OTP was sent to the new user.

To automatically reissue a new OTP and send an e-mail notice with the new password to an existing or new user, click **Replace OTP**.

## Editing a Local CA User

To modify information about an existing local CA user in the database, perform the following steps:

---

**Step 1** Select the specific user and click **Edit** to display the Edit User dialog box.

**Step 2** Enter a valid username.

**Step 3** Enter an existing valid e-mail address.

**Step 4** Enter the subject (DN string). Alternatively, click **Select** to display the Certificate Subject DN dialog box.

**Step 5** Choose one or more DN attributes that you want to change from the drop-down list, enter a value, and then click **Add** or **Delete**. Available X.500 attributes for the Certificate Subject DN are the following:

- Common Name (CN)
- Department (OU)
- Company Name (O)
- Country (C)
- State/Province (ST)
- Location (L)
- E-mail Address (EA)

**Step 6** Click **OK** when you are done to close the Certificate Subject DN dialog box.

**Step 7** Check the **Allow enrollment** check box to reenroll the user, and then click **Edit User**.

The updated user details appear in the Manage User Database pane.

---

## Deleting a Local CA User

To remove the user from the database and any certificates issued to that user from the local CA database, select the user, and then click **Delete**.

**Note**

A deleted user cannot be restored. To recreate the deleted user record, click **Add** to reenter all of the user information.

## Allowing User Enrollment

To enroll the selected user, click **Allow Enrollment**.

The status of the user changes to “enrolled” in the Manage User Database pane.

**Note**

If the user is already enrolled, an error message appears.

## Viewing or Regenerating an OTP

To view or regenerate the OTP of the selected user, perform the following steps:

- 
- Step 1** Click **View/Regenerate OTP** to display the View & Regenerate OTP dialog box.  
The current OTP appears.
- Step 2** After you are done, click **OK** to close the View & Regenerate OTP dialog box.
- Step 3** To regenerate the OTP, click **Regenerate OTP**.  
The newly generated OTP appears.
- Step 4** Click **OK** to close the View & Regenerate OTP dialog box.
- 

### What to Do Next

See the [“Managing User Certificates” section on page 40-37](#).

## Managing User Certificates

To change the certificate status, perform the following steps:

- 
- Step 1** In the Manage User Certificates pane, select specific certificates by username or by certificate serial number.
- Step 2** Choose one of the following options:
- If the user certificate lifetime period runs out, to remove user access, click **Revoke**. The local CA also marks the certificate as revoked in the certificate database, automatically updates the information, and reissues the CRL.

- To restore access, select a revoked certificate and click **Unrevoke**. The local CA also marks the certificate as unrevoke in the certificate database, automatically updates the certificate information, and reissues an updated CRL.

**Step 3** Click **Apply** when you are done to save your changes.

---

## What to Do Next

See the [“Monitoring CRLs” section on page 40-38](#).

# Monitoring CRLs

To monitor CRLs, perform the following steps:

---

**Step 1** In the ASDM main application window, choose **Monitoring > Properties > CRL**.

**Step 2** In the CRL area, choose the CA certificate name from the drop-down list.

**Step 3** To display CRL details, click **View CRL**. For example:

```
CRL Issuer Name:
cn=asa4.cisco.com
LastUpdate: 09:58:34 UTC Nov 11 2010
NextUpdate: 15:58:34 UTC Nov 11 2010
Cached Until: 15:58:34 UTC Nov 11 2010
Retrieved from CRL Distribution Point:
 ** CDP Not Published - Retrieved via SCEP
Size (bytes): 224
Associated Trustpoints: LOCAL-CA-SERVER
```

**Step 4** When you are done, click **Clear CRL** to remove the CRL details and choose another CA certificate to view.

---

# Feature History for Certificate Management

Table 40-1 lists each feature change and the platform release in which it was implemented. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

**Table 40-1** Feature History for Certificate Management

| Feature Name           | Platform Releases | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Certificate management | 7.0(1)            | <p>Digital certificates (including CA certificates, identity certificates, and code signer certificates) provide digital identification for authentication. A digital certificate includes information that identifies a device or user, such as the name, serial number, company, department, or IP address. CAs are trusted authorities that “sign” certificates to verify their authenticity, thereby guaranteeing the identity of the device or user. CAs issue digital certificates in the context of a PKI, which uses public-key or private-key encryption to ensure security.</p> <p>We introduced the following screens:</p> <p>Configuration &gt; Remote Access VPN &gt; Certificate Management</p> <p>Configuration &gt; Site-to-Site VPN &gt; Certificate Management.</p> <p>We introduced or modified the following screens:</p> <p>Configuration &gt; Firewall &gt; Advanced &gt; Certificate Management &gt; CA Certificates</p> <p>Configuration &gt; Device Management &gt; Certificate Management &gt; CA Certificates.</p> |
| SCEP proxy             | 8.4(1)            | <p>We introduced this feature, which provides secure deployment of device certificates from third-party CAs.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

