Digital Certificates

This chapter describes how to configure digital certificates.

- About Digital Certificates, on page 1
- Guidelines for Digital Certificates, on page 8
- Configure Digital Certificates, on page 11
- How to Set Up Specific Certificate Types, on page 12
- Set a Certificate Expiration Alert (for Identity or CA Certificates), on page 26
- Monitoring Digital Certificates, on page 27
- History for Certificate Management, on page 27

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 responsible for managing certificate requests and issuing digital certificates. CAs are trusted authorities that “sign” certificates to verify their authenticity, thereby guaranteeing the identity of the device or user.

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. 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.
- CAs also issue identity certificates, which are certificates for specific systems or hosts.
- 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.

In a hierarchy with a root and two intermediate CA certificates, a CRL validation for remote access fail on the headend running 9.13 or later when the ID certificate is signed by one intermediate CA, but the CRL is

signed by another intermediate CA. The failure happens even if the headend trusts both the intermediates where both are signed by the same root.

Hence, each signer must maintain their own CRL. Each signer would then specify the location of the CRL in the url list of each certificate it signs. Alternatively, you can configure a url override in the trustpoint of each signer pointing to the correct CRL location.

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.

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.

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.

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 or Elliptic Curve Signature Algorithm (ECDSA) keys, which have the following characteristics:

- RSA keys can be used for SSH or SSL.
- SCEP enrollment supports the certification of RSA keys.
- The maximum RSA key size is 4096, and the default is 2048.
- The maximum ECDSA key length is 521, and the default is 384.
- 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 the 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 Secure Client 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 Secure Client SSL or IKEv2 VPN session. It supports all SCEP-compliant CAs, including Cisco IOS CS, Windows Server 2003 CA, and Windows Server 2008 CA.

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

Note The **revocation-check crl none**, which was removed in 9.13(1), was restored.

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.

Note Though the CRL server responds with HTTP flag "Connection: Keep-alive" to indicate a persistent connection, ASA does not request support for persistent connection. Change the settings on the CRL server to respond with "Connection: Close" when the list is sent.

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.

You could receive a *revocation check* failure for a user connection/certificate if you exceed the CRL size limit of 16 MB.

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. Large CRLs require significant computational overhead to parse them. Hence, for better performance, use many CRLs of smaller size rather than few large CRLs, or preferably, use OCSP.

See the following the cache sizes:

- Single context mode—128 MB
- Multiple context mode—16 MB per context

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 ocsp** command. You can also make the OCSP check optional by using the **revocation-check ocsp none** command, which allows the certificate authentication to succeed when the validation authority is unavailable to provide updated OCSP data.

Note The **revocation-check ocsp none**, which was removed in 9.13(1), was restored.

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.

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, Secure Client, 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.

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

Certificates

If user digital certificates are configured, the ASA first validates the certificate. It does not, however, use any of the DNs 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.

Guidelines for Digital Certificates

This section includes guidelines and limitations that you should check before configuring digital certificates.

Context Mode Guidelines

- Supported in single context mode only for third-party CAs.

Failover Guidelines

- Does not support replicating sessions in Stateful Failover.
- Does not support failover for local CAs.
- Certificates are automatically copied to the standby unit if you configure stateful failover. If you find a certificate is missing, use the **write standby** command on the active unit.

IPv6 Guidelines

Supports IPv6 OCSP and CRL URLs. You must enclose IPv6 addresses in square brackets, for example: *http://[0:0:0:0:0.18:0a01:7c16]*.

Local CA Certificates

- 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.
- 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.
- Thirty days before the local CA certificate expires, a rollover replacement certificate is generated, and a syslog message informs the administrator that it is time for local CA rollover. The new local CA certificate must be imported onto all necessary devices before the current certificate expires. If the administrator does not respond by installing the rollover certificate as the new local CA certificate, validations may fail.
- The local CA certificate rolls over automatically after expiration using the same keypair. The rollover certificate is available for export in base 64 format.

  The following example shows a base 64 encoded local CA certificate:


```
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHA
YJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3S
DOiDwZG9n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZ
TS1E4L0fSaC3uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZ
PrzoG1J8BFqdPa1jBGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYY
bP86tvbZ2yOVZR6aKFVI0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmu
BeGDKOncTknfgy0XM+fG5rb3qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

END OF CERTIFICATE
```


SCEP Proxy Support

- Ensure that the ASA and the Cisco ISE Policy Service Nodes are synchronized using the same NTP server.
- Secure 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.

Additional Guidelines

- The type of certificate you can use is constrained by the certificate types supported by the applications that will use the certificate. RSA certificates are generally supported by all applications that use certificates. But EDDSA certificates might not be supported by workstation operating systems, browsers, ASDM, or Secure Client. For example, you need to use an RSA certificate for remote access VPN identity and authentication. For site-to-site VPN, where the ASA is the application that uses the certificate, EDDSA is supported.
- 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.
- The ASA establishes LDAP/SSL connection only if one of the following certification criteria is satisfied:
  - The LDAP server certificate is trusted (exists in a trustpoint or the ASA trustpool) and is valid.
  - A CA certificate from servers issuing chain is trusted (exists in a trustpoint or the ASA trustpool) and all subordinate CA certificates in the chain are complete and valid.
- 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.
- 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 Secure Client 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. In ASA, these certificates are decoded to build them into internal data structures. Certificates with blank fields are construed as non-compliant with the decoding standards, and hence the installation validation fails. However, from version 9.16, blank values of optional fields does not impact decoding and installation validation criteria.
- 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"phÕV°3é¼þ0 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
```

Configure Digital Certificates

The following topics explain how to configure digital certificates.

Configure Reference Identities

When the ASA is acting as a TLS client, it supports rules for verification of an application server's identity as defined in RFC 6125. This RFC specifies procedures for representing the reference identities (configured on the ASA) and verifying them against the presented identities (sent from the application server). If the presented identity cannot be matched against the configured reference identity, the connection is not established and an error is logged.

The server presents its identity by including one or more identifiers in the server certificate presented to the ASA while establishing the connection. Reference identities are configured on the ASA, to be compared to the identity presented in a server certificate during connection establishment. These identifiers are specific instances of the four identifier types specified in RFC 6125. The four identifier types are:

- CN_ID: A Relative Distinguished Name (RDN) in a certificate subject field that contains only one attribute-type-and-value pair of type Common Name (CN), where the value matches the overall form of a domain name. The CN value cannot be free text. A CN-ID reference identifier does not identify an application service.
- DNS-ID: A subjectAltName entry of type dNSName. This is a DNS domain name. A DNS-ID reference identifier does not identify an application service.
- SRV-ID: A subjectAltName entry of type otherName whose name form is SRVName as defined in RFC 4985. A SRV-ID identifier may contain both a domain name and an application service type. For example, a SRV-ID of “_imaps.example.net” would be split into a DNS domain name portion of “example.net” and an application service type portion of “imaps.”
- URI-ID: A subjectAltName entry of type uniformResourceIdentifier whose value includes both (i) a “scheme” and (ii) a “host” component (or its equivalent) that matches the “reg-name” rule specified in RFC 3986. A URI-ID identifier must contain the DNS domain name, not the IP address, and not just the hostname. For example, a URI-ID of “sip:voice.example.edu” would be split into a DNS domain name portion of “voice.example.edu” and an application service type of “sip.”

A reference identity is created when configuring one with a previously unused name. Once a reference identity has been created, the four identifier types and their associated values can be added or deleted from the reference identity. The reference identifiers MAY contain information identifying the application service and MUST contain information identifying the DNS domain name.

Before you begin

- Reference identities are used when connecting to the Syslog Server and the Smart Licensing server only. No other ASA SSL client mode connections currently support the configuration or use of reference identities.

- ASA implements all the rules for matching the identifiers described in RFC 6125 except for pinned certificates and fallback for interactive clients.
- Ability to pin certificates is not implemented. Therefore, `No Match Found, Pinned Certificate` will not occur. Also, a user will not be given the opportunity to pin a certificate if a match is not found since our implementation is not an interactive client.

Procedure

Step 1 Go to **Configuration** > **Remote Access VPN** > **Advanced** > **Reference Identity**.

Configured Reference Identities are listed. You may **Add** a new one, choose and **Edit** an existing one, or choose and **Delete** an existing one. A reference identity that is in use, cannot be deleted.

Step 2 Create or modify the reference-ids by choosing **Add** or **Edit**.

Use this Add or Edit Reference Identity dialog box to choose and specify your reference ids.

- Multiple reference-ids of any type may be added to the reference identity.
- You cannot modify the name once it is set, delete and re-create a reference identity to change the name.

What to do next

Use the reference identity when configuring the Syslog and the Smart Call Home server connections.

How to Set Up Specific Certificate Types

After you have established trusted certificates, you can begin other fundamental tasks such as establishing identity certificates or more advanced configurations such as establishing local CA or code signing certificates.

Before you begin

Read about digital certificate information and establish trusted certificates. CA certificates with no private key are used by all VPN protocols and webvpn, and are configured in trustpoints to validate incoming client certificates. Similarly, a trustpool is a list of trusted certificates used by webvpn features to validate proxied connections to https servers and to validate the smart-call-home certificate.

Procedure

Step 1 An identity certificate is a certificate that is configured on the ASA along with a corresponding private key. It is used for outbound encryption or for signature generation when enabling SSL and IPsec services on the ASA and is obtained through trustpoint enrollment. To configure identity certificates, refer to Identity Certificates, on page 13.

Step 2 A local CA allows VPN clients to enroll for certificates directly from the ASA. This advanced configuration converts the ASA into a CA. To configure CAs, refer to CA Certificates, on page 19.

Step 3 If you are planning to use identity certificates as part of the webvpn java code signing feature, refer to Code Signer Certificate, on page 25.

What to do next

Set up a certificate expiration alert or monitor digital certificates and certificate management history.

Identity Certificates

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 an Identity Certificate, on page 13.
- Enable CMPv2 Enrollments as a Request from a CA
- Display details of an identity certificate.
- Delete an existing identity certificate.
- Export an Identity Certificate, on page 17.
- Set certificate expiration alerts.
- Enroll for an identity certificate with Entrust Generate a Certificate Signing Request, on page 17.

Add or Import an Identity Certificate

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

Procedure

Step 1 Choose **Configuration** > **Remote Access VPN** > **Certificate Management** > **Identity Certificates**.

Step 2 Click **Add**.

The **Add Identity Certificate** dialog box appears, with the selected trustpoint name displayed at the top.

Step 3 Click the **Import the identity certificate from a file (PKCS12 format with Certificate(s) + Private Key)** radio button to import an identity certificate from an existing file.

Step 4 Enter the passphrase used to decrypt the PKCS12 file.

Step 5 Enter the path name of the file, or click **Browse** to display the **Import ID Certificate File** dialog box. Find the certificate file, then click **Import ID Certificate File**.

Step 6 Click the **Add a new identity certificate** radio button to add a new identity certificate.

Step 7 Click **New** to display the **Add Key Pair** dialog box.

Step 8 Choose the **RSA**, **ECDSA**, or **EdDSA** key type.

Step 9 If you choose **EdDSA**, the **Edwards Curve** option appears. Click the EdDSA1 radio button.

Step 10 Click the **Use default keypair name** radio button to use the default key pair name.

Step 11 Click the **Enter a new key pair name** radio button, then enter the new name.

Step 12 Choose the modulus size from the drop-down list. If **Edwards Curve** is selected, choose Ed25519. If you are not sure of the modulus size, consult Entrust.

For ASA 9.16(1) and higher versions, ensure that you select an RSA modulus size of 2048 or bigger. CA Certificate validation fails when the RSA key size is smaller than 2048 bits. To override this restriction, enable the permit weak crypto option. (See Permit Weak Crypto for CA Certificates, on page 24).

Step 13 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 14 Click **Generate Now** to create new key pairs, 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, 2048, 3072, and 4096. The default is 2048.
- The key data, which includes the specific key data in text format.

Step 15 Click **OK** when you are done.

Step 16 Choose a certificate subject DN to form the DN in the identity certificate, then click **Select** to display the **Certificate Subject DN** dialog box.

Step 17 Choose one or more DN attributes that you want to add from the drop-down list, enter a value, 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 18 Click **OK** when you are done.

Step 19 Check the **Generate self-signed certificate** check box to create self-signed certificates.

Step 20 Check the **Act as local certificate authority and issue dynamic certificates to TLS proxy** check box to have the identity certificate act as the local CA.

Step 21 Click **Advanced** to establish additional identity certificate settings.

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 22 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.
- Check the **Include serial number of the device** check box to add the ASA serial number to the certificate parameters.

Step 23 Click the **Enrollment Mode** tab, 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. If you choose **Request from a CA**, for information about enabling CMPV2 enrollments, refer to Enable CMPv2 Enrollments as a Request from a CA , on page 16.
- Choose the enrollment protocol—scep, cmp, or est.

  Note
  Only RSA and ECDSA keys are supported for CMP certificate enrollment.

- 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 24 Click the **SCEP Challenge Password** tab, then enter the following information:

- The SCEP password
- The SCEP password confirmation

Step 25 Click **OK** when you are done.

Step 26 Check the **Enable CA flag in basic constraints extension** if this certificate should be able to sign other certificates.

The basic constraints extension identifies whether the subject of the certificate is a Certificate Authority (CA), in which case the certificate can be used to sign other certificates. The CA flag is part of this extension. The presence of these items in a certificate indicates that the certificate's public key can be used to validate certificate signatures. There is no harm in leaving this option selected.

Step 27 Click **Add Certificate** in the **Add Identity Certificate** dialog box.

The new identity certificate appears in the Identity Certificates list.

Step 28 Click **Apply** to save the new identity certificate configuration.

Step 29 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 trust points. 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.

Step 30 To remove an identity certificate configuration, select it, 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.

Enable CMPv2 Enrollments as a Request from a CA

To be positioned as a Security Gateway device in wireless LTE networks, ASA supports some certificate management functions using the Certificate Management Protocol (CMPv2). Using CMPv2 for enrollment of ASA device certificates, you can perform manual enrollment, for the first and secondary certificate from the CMPv2-enabled CA, or manual certificate updates, for replacement of a previously issued certificate using the same key pair. The received certificates are stored outside of the conventional configuration and are used in certificate-enabled IPsec configurations.

Note You will not have the full CMPv2 functionality on the ASA.

An initial request establishes trust with the CA and obtains the first certificate. A CA certificate must be preconfigured in a trustpoint. Authentication occurs when you acknowledge the fingerprint of the certificate that is being installed.

After clicking **Request from a CA** on the Enrollment Mode tab of the Advanced Options window, complete the following steps specific for CMPv2 enrollments:

Before you begin

- Follow the steps in Add or Import an Identity Certificate, on page 13.
- Carrier license must be included to enable CMP enrollment.

Procedure

Step 1 Choose CMP as the enrollment protocol and enter the CMP URL in the http:// area.

Step 2 To automatically generate new keypairs for all CMP manual and automatic enrollments, choose either **RSA** or **EDCSA**.

If you choose RSA, choose a value from the Modulus drop-down menu. If you choose EDCSA, choose a value from the elliptic-curve drop-down menu.

Step 3 (Optional) Click **Regenerate the key pair** to generate a key pair while renewing the certificate or prior to building the enrollment request.

Step 4 Click **Shared Key** and enter a value provided out of band by the CA. This value is used by the CA and ASA to confirm the authenticity and integrity of the messages that they exchange.

Step 5 Click **Signing Trustpoint** and enter the name of the trustpoint which contains a previously-issued device certificate used to sign the CMP enrollment request.

These options are only available when the trustpoint enrollment protocol is set to CMP. When a CMP trustpoint, the shared secret or the signing certificate can be specified, but not both.

Step 6 Click **Browse Certificate** to specify the CA certificate.

Step 7 (Optional) Click the **Auto Enroll** checkbox to trigger auto-enroll of CMPv2.

Step 8 At the Auto Enroll Lifetime field, enter the percentage of the absolute lifetime of the certificate after which auto-enroll will be necessary.

Step 9 Click **Auto Enroll Regenerate Key** to generate a new key while renewing the certificate.

Export an Identity Certificate

To export an identity certificate, perform the following steps:

Procedure

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.

Generate a Certificate Signing Request

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

Procedure

Step 1 Click **Enroll ASA SSL VPN with Entrust** to display the **Generate Certificate Signing Request** dialog box.

Step 2 Perform the following steps in the **Key Pair** area:

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.
d) Click **New** to display the **Add Key Pair** dialog box. When you generate the key pair, you can send it to the ASA or save it to a file.

Step 3 Enter the following information in the **Certificate Subject DN** area:
a) The FQDN or IP address of the ASA.
b) The name of the company.
c) The two-letter country code.

Step 4 Perform the following steps in the **Optional Parameters** area:
a) Click **Select** to display the **Additional DN Attributes** dialog box.
b) Choose the attribute to add from the drop-down list, 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.

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 Complete the enrollment process by clicking the **request a certificate from Entrust** link. Then copy and paste the CSR provided and submit 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.

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**.

Step 9 Click **Close** to close the **Enroll with Entrust** dialog box.

Install Identity Certificates

To install a new identity certificate, perform the following steps:

Procedure

Step 1 Click **Add**in the **Identity Certificates** pane to display the **Add Identity Certificate** dialog box.

Step 2 Click the **Add a new identity certificate** radio button.

Step 3 Change the key pair or create a new key pair. A key pair is required.

Step 4 Enter the certificate subject DN information, 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, 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 Add or Import an Identity Certificate, on page 13.

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, 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, then 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.

Step 15 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.

Step 16 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.

CA Certificates

This page is where you manage CA certificates. The following topics explain what you can do.

Add or Install a CA Certificate

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

Procedure

Step 1 Choose **Configuration** > **Remote Access VPN** > **Certificate Management** > **CA Certificates**.

Step 2 Click **Add**.

The **Install Certificate** dialog box appears.

Step 3 Click the **Install from a file** radio button to add a certificate configuration from an existing file (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 Click the **Paste certificate in PEM format** radio button to enroll manually.

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 Click the **Use SCEP** radio button to enroll automatically. 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.

Step 10 Click **More Options** to display additional configuration options for new and existing certificates.

The **Configuration Options for CA Certificates** pane appears.

Step 11 To change an existing CA certificate configuration, select it, then click **Edit**.

Step 12 To remove a CA certificate configuration, select it, 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.

Step 13 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 trust points. 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.

Configure CA Certificates for Revocation

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

Procedure

Step 1 Choose **Configuration** > **Site-to-Site VPN** > **Certificate Management** > **CA Certificates** > **Add** to display the **Install Certificates** dialog box. Then click **More Options**.

Step 2 Click the **Revocation Check** tab.

Step 3 Click the **Do not check certificates for revocation** radio button to disable revocation checking of certificates.

Step 4 Click the **Check certificates for revocation** radio button to select one or more revocation checking methods (CRL or OCSP).

Step 5 Click **Add** to move a revocation 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 information cannot be retrieved** check box to ignore revocation checking errors during certificate validation.

Step 7 Click **OK** to close the **Revocation Check** tab.

Configure CRL Retrieval Policy

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

Before you begin

- To assign static URLs,

Procedure

Step 1 Choose **Configuration** > **Site-to-Site VPN** > **Certificate Management** > **CA Certificates** > **Add** to display the **Install Certificates** dialog box. Then click **More Options**.

Step 2 Click the **CRL Retrieval Policy** tab.

Step 3 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 4 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 5 Click **Add** in the **CRL Distribution Point** tab.

Step 6 In the **Add CDP Rule** dialog box, select the certificate map, enter the index, and the URL.

Note
Ensure that you have configured certificate map on the device—Go to **Remote Access VPN** > **Network (Client) Access** > **Advanced** > **IPSec** > **Certificate to Connection Map** > **Rules** > **Add** .

ASA supports IPv4 or IPv6 based CDP and Static URLs. Enclose IPv6 addresses in square brackets, for example: *http://[0:0:0:0:0.18:0a01:7c16]*.

Step 7 Click **OK** to close this dialog box.

Configure CRL Retrieval Methods

To configure CRL retrieval methods, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Site-to-Site VPN** > **Certificate Management** > **CA Certificates** > **Add** to display the **Install Certificates** dialog box. Then click **More Options**.

Step 2 Click the **CRL Retrieval Methods** tab in the **Configuration Options for CA Certificates** pane.

Step 3 Choose one of the following three retrieval methods:

- 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:
  - **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.

Configure OCSP Rules

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

Before you begin

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.

Procedure

Step 1 Choose **Configuration** > **Site-to-Site VPN** > **Certificate Management** > **CA Certificates** > **Add** to display the **Install Certificates** dialog box. Then click **More Options**.

Step 2 Click the **OCSP Rules** tab in the **Configuration Options for CA Certificates** pane.

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 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 Click **OK** to close this tab.

Configure Advanced CRL and OCSP Settings

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

Procedure

Step 1 Choose **Configuration** > **Site-to-Site VPN** > **Certificate Management** > **CA Certificates** > **Add** to display the **Install Certificates** dialog box. Then click **More Options**.

Step 2 Click the **Advanced** tab in the **Configuration Options for CA Certificates** pane.

Step 3 Enter the number of minutes between cache refreshes in the **CRL Options** area. 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 Enter the URL for the OCSP server in the **OCSP Options** area. The ASA uses OCSP servers according to the following order:

a) OCSP URL in a match certificate override rule
b) OCSP URL configured in the selected OCSP Options attribute
c) 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 Choose one of the following options in the **Other Options** area:

- 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, then click **Apply** to save your configuration changes.

CA Server Management

Manage User Certificates

To change the certificate status, perform the following steps:

Procedure

Step 1 Select specific certificates by username or by certificate serial number in the **Manage User Certificates** pane.

Step 2 Choose one of the following options:

- Click **Revoke**to remove user access if the user certificate lifetime period runs out. The local CA also marks the certificate as revoked in the certificate database, automatically updates the information, and reissues the CRL.
- Select a revoked certificate and click **Unrevoke** to restore access. The local CA also marks the certificate as unrevoked 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.

Permit Weak Crypto for CA Certificates

When the following attributes are present, the CA certificate validation operation fails:

- Certificates signed with the SHA-1 with RSA encryption algorithm.
- Certificates with RSA key sizes smaller than 2048 bits.

However, you can override these restrictions by configuring the permit weak crypto option. When enabled, the ASA allows using the above attributes when validating certificates. We do not recommend permitting weak-crypto keys, because such keys are not as secure as the ones with higher key sizes.

Procedure

Step 1 Browse to **Configuration** > **Device Management** > **Certificate Management** > **Identity Certificate**, or **Configuration** > **Remote Access VPN** > **Certificate Management** > **Identity Certificate**, or **Configuration** > **Remote Access VPN** > **Certificate Management** > **Code Signer**.

Step 2 To permit key sizes that are smaller than 2048 bits and SHA-1 signature algorithms, under **Weak Crypto Configurations**, click the **Permit Weak Key Sizes and Hash Algorithms** check box.

Code Signer Certificate

Import a Code Signer Certificate

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

Procedure

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.

Export a Code Signer Certificate

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

Procedure

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.

Set a Certificate Expiration Alert (for Identity or CA Certificates)

ASA checks all the CA and ID certificates in the trust points for expiration once every 24 hours. If a certificate is nearing expiration, a syslog will be issued as an alert.

In addition to the renewal reminder, if an already expired certificate is found in the configuration, a syslog is generated once every day to rectify the configuration by either renewing the certificate or removing the expired certificate.

For example, assume that the expiration alerts are configured to begin at 60 days and repeat every 6 days after that. If the ASA is rebooted at 40 days, an alert is sent on that day, and the next alert is sent on the 36th day.

Note Expiration checking is not done on trust pool certificates. The Local CA trust point is treated as a regular trustpoint for expiration checking too.

Procedure

Step 1 Browse to **Configuration** > **Device Management** > **Certificate Management** > **Identity Certificate/CA Certificate**.

Step 2 Check the **Enable Certificate Expiration Alert** check box.

Step 3 Fill in the desired number of days:

- Send the first alert before—Configure the number of days (1 to 90) before expiration at which the first alert will go out.
- Repeat the alert for—Configure the alert frequency (1 to 14 days) if the certificate is not renewed. By default, the first alert is sent 60 days prior to expiration and once every week after until the certificate is renewed and removed. Additionally, an alert is sent on the day of the expiration and once every day after that, and irrespective of the alert configuration, an alert is sent every day during the last week of expiration.

Monitoring Digital Certificates

See the following commands for monitoring digital certificate status:

- **Monitoring > Properties > CRL**

  This pane shows CRL details.

- **Tools > Command Line Interface**

  This pane allows you to issue various non-interactive commands and view results.

History for Certificate Management

Table 1: History for Certificate Management

Feature Name	Platform Releases	Description
Certificate management	7.0(1)	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. We introduced the following screens: Configuration > Remote Access VPN > Certificate Management Configuration > Site-to-Site VPN > Certificate Management. We introduced or modified the following screens: Configuration > Firewall > Advanced > Certificate Management > CA Certificates Configuration > Device Management > Certificate Management > CA Certificates.
Certificate management	7.2(1)	
Certificate management	8.0(2)	
SCEP proxy	8.4(1)	We introduced this feature, which provides secure deployment of device certificates from third-party CAs.

Feature Name	Platform Releases	Description
Reference Identities	9.6(2)	TLS client processing now supports rules for verification of a server identity defined in RFC 6125, Section 6. Identity verification will be done during PKI validation for TLS connections to the Syslog Server and the Smart Licensing server only. If the presented identity cannot be matched against the configured reference identity, the connection is not established. We modifed the following screens: Configuration > Remote Access VPN > Advanced Configuration > Device Management > Logging > Syslog Servers > Add/Edit Configuration > Device Management > Smart Call Home
Local CA Server	9.12(1)	To make the FQDN of the enrollment URL configurable instead of using the ASA's configured FQDN, a new CLI option is introduced. This new option is added to the smpt mode of crypto ca server. We deprecated Local CA Server and will be removing in a later release—When ASA is configured as local CA server, it is enabled to issue digital certificates, publish Certificate Revocation Lists (CRLs), and securely revoke issued certificates. This feature has become obsolete and hence the crypto ca server command is deprecated.
Local CA Server	9.13(1)	We removed the local ca server support. Thus, the **crypto ca server** command and its subcommands are removed. We removed the following commands: **crypto ca server** and all of its subcommands.
Modifications to the CRL Distribution Point commands	9.13(1)	The static CDP URL configuration commands are removed and moved to the match certificate command. New/Modified screens: **Configuration** > **Device Management** > **Certificate Management** > **CA Certificates**
CRL cache size increased	9.13(1)	To prevent failure of large CRL downloads, the cache size was increased, and the limit on the number of entries in an individual CRL was removed. • Increased the total CRL cache size to 16 MB per context for multi-context mode. • Increased the total CRL cache size to 128 MB for single-context mode.
Restoration of bypass certificate validity checks option	9.15(1)	The option to bypass revocation checking due to connectivity problems with the CRL or OCSP server that was removed in 9.13(1) was restored.

Feature Name	Platform Releases	Description
Modifications to Match Certificate commands to support static CRL Distribution Point URL	9.15(1)	The static CDP URL configuration command allowed static CDPs to be mapped uniquely to each certificate in a chain that is being validated. However, only one such mapping was supported for each certificate. This modification allows statically configured CDPs to be mapped to a chain of certificates for authentication.
Modifications to the trustpoint keypair and crypto key generate commands	9.16(1)	Support for certificates with key sizes smaller than 2048 was removed. Any configuration using 512, 768 or 1024-bit options are transitioned to 2048 with due notification. Support to use SHA1 hashing algorithm for certification was removed. **Note** **crypto ca permit-weak-crypto** command was introduced to override these restrictions. The new key option - EDDSA was added to the existing RSA and ECDSA options.
Support for OCSP and CRL IPv6 URL	9.20(1)	Support to use IPv6 OCSP and CRL URLs were added. The IPv6 addresses must be enclosed in square brackets.