



Configuring PKI

This chapter describes the Public Key Infrastructure (PKI) support on the Cisco NX-OS device. PKI allows the device to obtain and use digital certificates for secure communication in the network and provides manageability and scalability for Secure Shell (SSH).

This chapter includes the following sections:

- [Information About PKI, on page 1](#)
- [Guidelines and Limitations for PKI, on page 6](#)
- [Default Settings for PKI, on page 6](#)
- [Configuring CAs and Digital Certificates, on page 7](#)
- [Verifying the PKI Configuration, on page 21](#)
- [Configuration Examples for PKI, on page 22](#)
- [Additional References for PKI, on page 42](#)

Information About PKI

This section provides information about PKI.

CAs and Digital Certificates

Certificate authorities (CAs) manage certificate requests and issue certificates to participating entities such as hosts, network devices, or users. The CAs provide centralized key management for the participating entities.

Digital signatures, based on public key cryptography, digitally authenticate devices and individual users. In public key cryptography, such as the RSA encryption system, each device or user has a key pair that contains both a private key and a public key. The private key is kept secret and is known only to the owning device or user only. However, the public key is known to everybody. Anything encrypted with one of the keys can be decrypted with the other. A signature is formed when data is encrypted with a sender's private key. The receiver verifies the signature by decrypting the message with the sender's public key. This process relies on the receiver having a copy of the sender's public key and knowing with a high degree of certainty that it really does belong to the sender and not to someone pretending to be the sender.

Digital certificates link the digital signature to the sender. A digital certificate contains information to identify a user or device, such as the name, serial number, company, department, or IP address. It also contains a copy of the entity's public key. The CA that signs the certificate is a third party that the receiver explicitly trusts to validate identities and to create digital certificates.

To validate the signature of the CA, the receiver must first know the CA's public key. Typically, this process is handled out of band or through an operation done at installation. For instance, most web browsers are configured with the public keys of several CAs by default.

Trust Model, Trust Points, and Identity CAs

The PKI trust model is hierarchical with multiple configurable trusted CAs. You can configure each participating device with a list of trusted CAs so that a peer certificate obtained during the security protocol exchanges can be authenticated if it was issued by one of the locally trusted CAs. The Cisco NX-OS software locally stores the self-signed root certificate of the trusted CA (or certificate chain for a subordinate CA). The process of securely obtaining a trusted CA's root certificate (or the entire chain in the case of a subordinate CA) and storing it locally is called *CA authentication*.

The information about a trusted CA that you have configured is called the *trust point* and the CA itself is called a *trust point CA*. This information consists of a CA certificate (or certificate chain in case of a subordinate CA) and certificate revocation checking information.

The Cisco NX-OS device can also enroll with a trust point to obtain an identity certificate to associate with a key pair. This trust point is called an *identity CA*.

CA Certificate Hierarchy

For secure services, you typically have multiple trusted CAs. The CAs are usually installed in all the hosts as a bundle. The NX-OS PKI infrastructure does support importing certificate chain. However, with the current CLIs, one chain at a time can be installed. This procedure can be cumbersome when there are several CA chains to be installed. This requires a facility to download CA bundles that could include several intermediate and root CAs.

Importing CA Bundle

The **crypto CA trustpoint** command binds the CA certificates, CRLs, identity certificates and key pairs to a named label. All files corresponding to each of these entities are stored in the NX-OS certstore directory (*/isan/etc/certstore*) and tagged with the trustpoint label.

To access the CA certificates, an SSL app only needs to point to the standard NX-OS cert-store and specify that as the CA path during SSL initialization. It does not need to be aware of the trustpoint label under which CAs are installed.

If clients need to bind to an identity certificate, the trustpoint label needs to be used as the binding point.

The import pkcs command is enhanced to install the CA certificates under a trustpoint label. This can be further enhanced to install a CA bundle. The import command structure is modified to add pkcs7 option which is used for providing CA bundle file in pkcs7 format.

Beginning with Cisco NX-OS Release 10.1(1), the pkcs7 file format is supported to unpack the CA bundle and install each CA chain under its own label. The labels are formed by appending an index to the main trustpoint label.

Once installed, there is no logical binding of all CA chains to a bundle.

RSA Key Pairs and Identity Certificates

You can obtain an identity certificate by generating one or more RSA key pairs and associating each RSA key pair with a trust point CA where the Cisco NX-OS device intends to enroll. The Cisco NX-OS device needs only one identity per CA, which consists of one key pair and one identity certificate per CA.

The Cisco NX-OS software allows you to generate RSA key pairs with a configurable key size (or modulus). The default key size is 512. You can also configure an RSA key-pair label. The default key label is the device fully qualified domain name (FQDN).

The following list summarizes the relationship between trust points, RSA key pairs, and identity certificates:

- A trust point corresponds to a specific CA that the Cisco NX-OS device trusts for peer certificate verification for any application (such as SSH).
- A Cisco NX-OS device can have many trust points and all applications on the device can trust a peer certificate issued by any of the trust point CAs.
- A trust point is not restricted to a specific application.
- A Cisco NX-OS device enrolls with the CA that corresponds to the trust point to obtain an identity certificate. You can enroll your device with multiple trust points which means that you can obtain a separate identity certificate from each trust point. The identity certificates are used by applications depending upon the purposes specified in the certificate by the issuing CA. The purpose of a certificate is stored in the certificate as a certificate extension.
- When enrolling with a trust point, you must specify an RSA key pair to be certified. This key pair must be generated and associated to the trust point before generating the enrollment request. The association between the trust point, key pair, and identity certificate is valid until it is explicitly removed by deleting the certificate, key pair, or trust point.
- The subject name in the identity certificate is the fully qualified domain name for the Cisco NX-OS device.
- You can generate one or more RSA key pairs on a device and each can be associated to one or more trust points. But no more than one key pair can be associated to a trust point, which means only one identity certificate is allowed from a CA.
- If the Cisco NX-OS device obtains multiple identity certificates (each from a distinct CA), the certificate that an application selects to use in a security protocol exchange with a peer is application specific.
- You do not need to designate one or more trust points for an application. Any application can use any certificate issued by any trust point as long as the certificate purpose satisfies the application requirements.
- You do not need more than one identity certificate from a trust point or more than one key pair to be associated to a trust point. A CA certifies a given identity (or name) only once and does not issue multiple certificates with the same name. If you need more than one identity certificate for a CA and if the CA allows multiple certificates with the same names, you must define another trust point for the same CA, associate another key pair to it, and have it certified.

Multiple Trusted CA Support

The Cisco NX-OS device can trust multiple CAs by configuring multiple trust points and associating each with a distinct CA. With multiple trusted CAs, you do not have to enroll a device with the specific CA that issued the certificate to a peer. Instead, you can configure the device with multiple trusted CAs that the peer

trusts. The Cisco NX-OS device can then use a configured trusted CA to verify certificates received from a peer that were not issued by the same CA defined in the identity of the peer device.

PKI Enrollment Support

Enrollment is the process of obtaining an identity certificate for the device that is used for applications like SSH. It occurs between the device that requests the certificate and the certificate authority.

The Cisco NX-OS device performs the following steps when performing the PKI enrollment process:

- Generates an RSA private and public key pair on the device.
- Generates a certificate request in standard format and forwards it to the CA.



Note The CA administrator may be required to manually approve the enrollment request at the CA server, when the request is received by the CA.

- Receives the issued certificate back from the CA, signed with the CA's private key.
- Writes the certificate into a nonvolatile storage area on the device (bootflash).

Manual Enrollment Using Cut-and-Paste

The Cisco NX-OS software supports certificate retrieval and enrollment using manual cut-and-paste. Cut-and-paste enrollment means that you must cut and paste the certificate requests and resulting certificates between the device and the CA.

You must perform the following steps when using cut and paste in the manual enrollment process:

- Create an enrollment certificate request, which the Cisco NX-OS device displays in base64-encoded text form.
- Cut and paste the encoded certificate request text in an e-mail or in a web form and send it to the CA.
- Receive the issued certificate (in base64-encoded text form) from the CA in an e-mail or in a web browser download.
- Cut and paste the issued certificate to the device using the certificate import facility.

Multiple RSA Key Pair and Identity CA Support

Multiple identity CAs enable the device to enroll with more than one trust point, which results in multiple identity certificates, each from a distinct CA. With this feature, the Cisco NX-OS device can participate in SSH and other applications with many peers using certificates issued by CAs that are acceptable to those peers.

The multiple RSA key-pair feature allows the device to maintain a distinct key pair for each CA with which it is enrolled. It can match policy requirements for each CA without conflicting with the requirements specified by the other CAs, such as the key length. The device can generate multiple RSA key pairs and associate each

key pair with a distinct trust point. Thereafter, when enrolling with a trust point, the associated key pair is used to construct the certificate request.

Peer Certificate Verification

The PKI support on a Cisco NX-OS device can verify peer certificates. The Cisco NX-OS software verifies certificates received from peers during security exchanges for applications, such as SSH. The applications verify the validity of the peer certificates. The Cisco NX-OS software performs the following steps when verifying peer certificates:

- Verifies that the peer certificate is issued by one of the locally trusted CAs.
- Verifies that the peer certificate is valid (not expired) with respect to current time.
- Verifies that the peer certificate is not yet revoked by the issuing CA.

For revocation checking, the Cisco NX-OS software supports the certificate revocation list (CRL). A trust point CA can use this method to verify that the peer certificate has not been revoked.

Certificate Revocation Checking

The Cisco NX-OS software can check the revocation status of CA certificates. The applications can use the revocation checking mechanisms in the order that you specify. The choices are CRL, NDcPP: OCSP for Syslog, none, or a combination of these methods.

CRL Support

The CAs maintain certificate revocation lists (CRLs) to provide information about certificates revoked prior to their expiration dates. The CAs publish the CRLs in a repository and provide the download public URL in all issued certificates. A client verifying a peer's certificate can obtain the latest CRL from the issuing CA and use it to determine if the certificate has been revoked. A client can cache the CRLs of some or all of its trusted CAs locally and use them later if necessary until the CRLs expire.

The Cisco NX-OS software allows the manual configuration of predownloaded CRLs for the trust points, and then caches them in the device bootflash (cert-store). During the verification of a peer certificate, the Cisco NX-OS software checks the CRL from the issuing CA only if the CRL has already been cached locally and the revocation checking is configured to use the CRL. Otherwise, the Cisco NX-OS software does not perform CRL checking and considers the certificate to be not revoked unless you have configured other revocation checking methods.

NDcPP: OCSP for Syslog

Online Certificate Status Protocol (OCSP) is a method to check certificate revocation when a peer has to retrieve this revocation information and then validate it to check the certificate revocation status. In this method, the certification revocation status is limited by the peer's ability to reach an OCSP responder through the cloud or by the certificate sender's performance in retrieving the certificate revocation-information.

When the remote syslog server shares the certificate which has an OCSP responder URL, the client sends the server certificate to an external OCSP responder (CA) server. The CA server validates this certificate and confirms if it is a valid or a revoked certificate. In this case, the client does not have to maintain the revoked certificate list locally.

Import and Export Support for Certificates and Associated Key Pairs

As part of the CA authentication and enrollment process, the subordinate CA certificate (or certificate chain) and identity certificates can be imported in standard PEM (base64) format.

The complete identity information in a trust point can be exported to a file in the password-protected PKCS#12 standard format. It can be later imported to the same device (for example, after a system crash) or to a replacement device. The information in a PKCS#12 file consists of the RSA key pair, the identity certificate, and the CA certificate (or chain).

Guidelines and Limitations for PKI

PKI has the following configuration guidelines and limitations:

- The maximum number of key pairs you can configure on a Cisco NX-OS device is 16.
- The maximum number of trust points you can declare on a Cisco NX-OS device is 16.
- The maximum number of identity certificates that you can configure on a Cisco NX-OS device are 16.
- The maximum number of certificates in a CA certificate chain is 10.
- The maximum number of trust points you can authenticate to a specific CA is 10.
- Configuration rollbacks do not support the PKI configuration.
- Beginning with Cisco NX-OS Release 9.3(5), Cisco NX-OS software supports NDcPP: OCSP for Syslog.



Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Default Settings for PKI

This table lists the default settings for PKI parameters.

Table 1: Default PKI Parameters

Parameters	Default
Trust point	None
RSA key pair	None
RSA key-pair label	Device FQDN
RSA key-pair modulus	512
RSA key-pair exportable	Enabled

Parameters	Default
Revocation check method	CRL

Configuring CAs and Digital Certificates

This section describes the tasks that you must perform to allow CAs and digital certificates on your Cisco NX-OS device to interoperate.

Configuring the Hostname and IP Domain Name

You must configure the hostname and IP domain name of the device if you have not yet configured them because the Cisco NX-OS software uses the fully qualified domain name (FQDN) of the device as the subject in the identity certificate. Also, the Cisco NX-OS software uses the device FQDN as a default key label when you do not specify a label during key-pair generation. For example, a certificate named DeviceA.example.com is based on a device hostname of DeviceA and a device IP domain name of example.com.



Caution Changing the hostname or IP domain name after generating the certificate can invalidate the certificate.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	hostname <i>hostname</i> Example: switch(config)# hostname DeviceA	Configures the hostname of the device.
Step 3	ip domain-name <i>name</i> [use-vrf <i>vrf-name</i>] Example: DeviceA(config)# ip domain-name example.com	Configures the IP domain name of the device. If you do not specify a VRF name, the command uses the default VRF.
Step 4	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 5	(Optional) show hosts Example:	Displays the IP domain name.

	Command or Action	Purpose
	switch# show hosts	
Step 6	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Generating an RSA Key Pair

You can generate an RSA key pairs to sign and/or encrypt and decrypt the security payload during security protocol exchanges for applications. You must generate the RSA key pair before you can obtain a certificate for your device.

Beginning Cisco NX-OS Release 9.3(3), you must explicitly generate RSA key pairs before you associate the Cisco NX-OS device with a trust point CA. Prior to Cisco NX-OS Releases 9.3(3), if unavailable, the RSA key pairs would be auto generated.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	crypto key generate rsa [label <i>label-string</i>] [exportable] [modulus <i>size</i>] Example: switch(config)# crypto key generate rsa exportable	<p>Generates an RSA key pair. The maximum number of key pairs on a device is 16.</p> <p>The label string is alphanumeric, case sensitive, and has a maximum length of 64 characters. The default label string is the hostname and the FQDN separated by a period character (.).</p> <p>Valid modulus values are 512, 768, 1024, 1536, and 2048. The default modulus size is 512.</p> <p>Note The security policy on the Cisco NX-OS device and on the CA (where enrollment is planned) should be considered when deciding the appropriate key modulus.</p> <p>By default, the key pair is not exportable. Only exportable key pairs can be exported in the PKCS#12 format.</p> <p>Caution You cannot change the exportability of a key pair.</p>

	Command or Action	Purpose
Step 3	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 4	(Optional) show crypto key mypubkey rsa Example: switch# show crypto key mypubkey rsa	Displays the generated key.
Step 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Creating a Trust Point CA Association

You must associate the Cisco NX-OS device with a trust point CA.

Before you begin

Generate the RSA key pair.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	crypto ca trustpoint name Example: switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#	Declares a trust point CA that the device should trust and enters trust point configuration mode. Note The maximum number of trustpoints that can be configured is 50.
Step 3	enrollment terminal Example: switch(config-trustpoint)# enrollment terminal	Enables manual cut-and-paste certificate enrollment. The default is enabled. Note The Cisco NX-OS software supports only the manual cut-and-paste method for certificate enrollment.

	Command or Action	Purpose
Step 4	rsakeypair <i>label</i> Example: <pre>switch(config-trustpoint)# rsakeypair SwitchA</pre>	Specifies the label of the RSA key pair to associate to this trust point for enrollment. Note You can specify only one RSA key pair per CA.
Step 5	exit Example: <pre>switch(config-trustpoint)# exit switch(config)#</pre>	Exits trust point configuration mode.
Step 6	(Optional) show crypto ca trustpoints Example: <pre>switch(config)# show crypto ca trustpoints</pre>	Displays trust point information.
Step 7	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Related Topics

[Generating an RSA Key Pair](#), on page 8

Authenticating the CA

The configuration process of trusting a CA is complete only when the CA is authenticated to the Cisco NX-OS device. You must authenticate your Cisco NX-OS device to the CA by obtaining the self-signed certificate of the CA in PEM format, which contains the public key of the CA. Because the certificate of the CA is self-signed (the CA signs its own certificate) the public key of the CA should be manually authenticated by contacting the CA administrator to compare the fingerprint of the CA certificate.



Note The CA that you are authenticating is not a self-signed CA when it is a subordinate CA to another CA, which itself may be a subordinate to yet another CA, and so on, finally ending in a self-signed CA. This type of CA certificate is called the *CA certificate chain* of the CA being authenticated. In this case, you must input the full list of the CA certificates of all the CAs in the certification chain during the CA authentication. The maximum number of certificates in a CA certificate chain is 10.

Before you begin

Create an association with the CA.

Obtain the CA certificate or CA certificate chain.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	crypto ca authenticate <i>name</i> Example: <pre>switch(config)# crypto ca authenticate admin-ca input (cut & paste) CA certificate (chain) in PEM format; end the input with a line containing only END OF INPUT : -----BEGIN CERTIFICATE----- MIIC4jCCAgwGfWFAglCBDSIayGZFRSLjkOzejAVBjckpkiC9wOFAQFADCB KDEjB4CCSgSI3DQEPFRMLHmRzLBJaXNj05jc20CzABjNEAYTAKD MRlEAVDQQIBWLLYXUyMra2EejaCBjNEAciUHorhbG9ZIEOMwGALUB ChMfQ1lz28EzAFBjMEAsIGf5lchN0b3JhZ2EjaCBjNEAMICUwYXU5SEU QjEeFw0NIAIMDMjQ2MzBfOwZAIIMDMjUIMiChMIGQMEwHjckZlncN AQEhHhWRUZ3L1QAp2MmNnNjEIMAKALUEHMCSU4EjaCBjNEAgIUth cnfndGhYTESMPCALUEBMQnRUZ2Fsb3UIMQ4wDAYDQQEwMDaXNj0zEIMBQ AUECMKotU0c3RvcmEhZIESMPCALUEwMQEhcnhEhENMFwDQkZlncN AQEhQADS4wSAEBAW/7b3+DXEANSIHHzLhNcdM87ypzwucSVZOPeKXI CzEPglXID2ASRU0QliDM8rO/4ljf8RwMkysCwEAsCBzCBMAlBjNHQ8E EwMCAc4wDwDROIPQH/BAU4wEB/zAcBjNHQEFcQUjyjRdMxCMR20yRtQ G9VGH5wMDROfEQWjAucYgkOcaH0cDvL3nzS0CC9DZKUW5yb2s L0FwXUuSjUMENBnNjD4w0GgJLycmlsZl0vL1xcccNlIT4VENlcrFbnU h3eQhcnhJTBwQElY3JEMFCCSgAQOBj0AQQDgEwMOCsGSI3DQEP EQPAQEAHMQH8E399IwwfEGr0gNLJcNjLh0AFcI0rEyut/WGCPzksfEA NBG7E0cN66zex0EOEfg1Vs6mXp1//w== -----END CERTIFICATE----- END OF INPUT Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12 Do you accept this certificate? [yes/no]: yes</pre>	<p>Prompts you to cut and paste the certificate of the CA. Use the same name that you used when declaring the CA.</p> <p>The maximum number of trust points that you can authenticate to a specific CA is 10.</p> <p>Note For subordinate CA authentication, the Cisco NX-OS software requires the full chain of CA certificates ending in a self-signed CA because the CA chain is needed for certificate verification as well as for PKCS#12 format export.</p>
Step 3	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 4	(Optional) show crypto ca trustpoints Example: <pre>switch# show crypto ca trustpoints</pre>	Displays the trust point CA information.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Related Topics

[Creating a Trust Point CA Association](#), on page 9

Configuring Certificate Revocation Checking Methods

During security exchanges with a client (for example, an SSH user), the Cisco NX-OS device performs the certificate verification of the peer certificate sent by the client. The verification process may involve certificate revocation status checking.

You can configure the device to check the CRL downloaded from the CA. Downloading the CRL and checking locally does not generate traffic in your network. However, certificates can be revoked between downloads and your device would not be aware of the revocation.

Before you begin

Authenticate the CA.

Ensure that you have configured the CRL if you want to use CRL checking.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	crypto ca trustpoint <i>name</i> Example: switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#	Specifies a trust point CA and enters trust point configuration mode.
Step 3	revocation-check {crl [none] none} Example: switch(config-trustpoint)# revocation-check none	Configures the certificate revocation checking methods. The default method is crl . The Cisco NX-OS software uses the certificate revocation methods in the order that you specify.
Step 4	exit Example: switch(config-trustpoint)# exit switch(config)#	Exits trust point configuration mode.
Step 5	(Optional) show crypto ca trustpoints Example: switch(config)# show crypto ca trustpoints	Displays the trust point CA information.

	Command or Action	Purpose
Step 6	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Related Topics

[Authenticating the CA](#), on page 10

[Configuring a CRL](#), on page 18

Generating Certificate Requests

You must generate a request to obtain identity certificates from the associated trust point CA for each of your device's RSA key pairs. You must then cut and paste the displayed request into an e-mail or in a website form for the CA.

Before you begin

Create an association with the CA.

Obtain the CA certificate or CA certificate chain.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	crypto ca enroll name Example: switch(config)# crypto ca enroll admin-ca Create the certificate request .. Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it. Password:nbv123 The subject name in the certificate will be: DeviceA.cisco.com Include the switch serial number in the subject name? [yes/no]: no Include an IP address in the subject name [yes/no]: yes ip address:172.22.31.162 The certificate request will be displayed... -----BEGIN CERTIFICATE REQUEST-----	Generates a certificate request for an authenticated CA. Note You must remember the challenge password. It is not saved with the configuration. You must enter this password if your certificate needs to be revoked.

	Command or Action	Purpose
	<pre>MIIBgCCARQAwHDEAMBGAUEFAwRrMhMmM5jaXNjby5jb20wczZwDQYK KzIlrvdVQEEBQDgyOAMIGAcGPAI8YlUA2NC7jUUDaSmqNlgJ2kt8rl4lK UOC6anNy4qk8vEMZSIL74JgJzWbbLDkITysrjuCG7jb+wj0hEnv/5lT9y P2NU8cmqShrvEzgC7ysN/Pymkcgzh5Vpj+zarq5AtG9lXtq4W6MSCzW8S VcyHDvEAgMFAAGjIzAVBjckkiC9w0BQcxCBMdonU2MILzMDCCSgSI63DQET DjEgMowUQDVR0ACh/BBswGIRrMhMmM5jaXNjby5jb20wczZwDQYK KzIlrvdVQEEBQDgyEAKI60KERQ8rj0sDKZMSFJzh86JtDz3Gcd99GlfWgt PfttrNWE/pw6HayfQlZT3ecgvel2hl5l33MEF2bktEciT6Ul88rIOjglMjja8 8s23hDp8v8rklwAGWkVLRNUERJcpjfrgNIZacUUS8ZqfMethXyUk0- -----END CERTIFICATE REQUEST-----</pre>	
Step 3	<p>exit</p> <p>Example:</p> <pre>switch(config-trustpoint)# exit switch(config)#</pre>	Exits trust point configuration mode.
Step 4	<p>(Optional) show crypto ca certificates</p> <p>Example:</p> <pre>switch(config)# show crypto ca certificates</pre>	Displays the CA certificates.
Step 5	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Related Topics

[Creating a Trust Point CA Association](#), on page 9

Installing Identity Certificates

You can receive the identity certificate from the CA by e-mail or through a web browser in base64 encoded text form. You must install the identity certificate from the CA by cutting and pasting the encoded text.

Before you begin

Create an association with the CA.

Obtain the CA certificate or CA certificate chain.

Procedure

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.

	Command or Action	Purpose
Step 2	<p>crypto ca import name certificate</p> <p>Example:</p> <pre>switch(config)# crypto ca import admin-ca certificate input (cut & paste) certificate in PEM format: -----BEGIN CERTIFICATE----- MIIEADCCAggAwIBAgIJOCj0AAAAcDANBjkiGwQEAQIDCEKIEgM4G CSqGSIb3DQEJRRUwIhRZUjEjaNjy5j20CzABjNEMAYTAkQMRlWEYD VQIIEWILXUuXPa2EeEjAQBjNEMAcTUHhndhG3yZIECMwCAUECHMQZ1z Y28EzARBjNEMAsIGrlchND03JhZUUEjAQBjNEMATICURWxUjSEQDAeR0w NIEBMTWzANDEaF0wNjEEMITWzEYANDBBwGjAYBjNEMIEVZlZ2ZlTEI Y21z28Y29MIGIAOCGCSqGSIb3DQEBAQAAQADBiQBgQC/GNACcjQ41C QlWgkjSICdLr5aBhNQ.rj3pzo.KsZFEKjF2ubiyeCME8ylndWwSE08r74 gJx42/sI9IRtb/8uU/cj9jSSfK56kca7wM7a.8dEz8jMChIMWlaY/q2qfG3 x7Rlfd0G4rFZEgsl7/Elash9LxwIDPQB04ICEzCAg8wQMDRORAH/BBw GyIRWnXOMMESjajNjy5j22HEW6H6IwQDVR0CBBEHLi+2ssqWEfgR hhVnlVyo9jng4IHMEjNHEBgcQvGAFCCo8aDG6vjTEMjSkUeBclmxxoiGw pIGIMIGQSAHjKJkZlnvQJEBHhHwRZGJGnc2NlnNbiEIMAKALUE BhMSU4eEjAQBjNEMAgIUthorhndGfYIESMAGALUEBhMQrFuzZtsb3JIMQ4w DAVDQQEwDaxNjzeEIMBEGALUECMKntOc3RvcmEhZIESMAGALUEBhMQEh orhTENBjAFYKUHqZlE9UEIWMRl0McGALUEBhRfMGUwlpsoCqFKG0dPA6 Iy9zc2UtdGvQ2VycEMvcr9sbC9BcFjbrEIMjHEQ55jcmwMkAncyChrtqbcU6 Iy9cXNzZS0CEdXJORW5jb2ssYERWxUjSUjMENEInNjDCEiGyIkWMBGJH AQEFjEBMdsCCsCAQFEzAChi9odHwOls8vc3NlITP4LQnlrFbnJbGwec3Nl ITP4MORWxUjSUjMENEInNjDCEiGyIkWMBGJH XENLcrFbnJbGwec3NlITP4MORWxUjSUjMENEInNjDCEiGyIkWMBGJH AANBAdGEG3oe7GNh9aeOIMBm24U69ZS.LDcOdZUUTgprlIqMPEyetsyElw E36cI.Zu4WsExREqxbTk8ycx7V5o= -----END CERTIFICATE-----</pre>	<p>Prompts you to cut and paste the identity certificate for the CA named admin-ca.</p> <p>The maximum number of identify certificates that you can configure on a device is 16.</p>
Step 3	<p>exit</p> <p>Example:</p> <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 4	<p>(Optional) show crypto ca certificates</p> <p>Example:</p> <pre>switch# show crypto ca certificates</pre>	Displays the CA certificates.
Step 5	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Related Topics

[Creating a Trust Point CA Association](#), on page 9

Ensuring Trust Point Configurations Persist Across Reboots

You can ensure that the trustpoint configuration persists across Cisco NX-OS device reboots.

The trust point configuration is a normal Cisco NX-OS device configuration that persists across system reboots only if you copy it explicitly to the startup configuration. The certificates, key pairs, and CRL associated with a trust point are automatically persistent if you have already copied the trust point configuration in the startup configuration. Conversely, if the trust point configuration is not copied to the startup configuration, the certificates, key pairs, and CRL associated with it are not persistent since they require the corresponding trust point configuration after a reboot. Always copy the running configuration to the startup configuration to ensure that the configured certificates, key pairs, and CRLs are persistent. Also, save the running configuration after deleting a certificate or key pair to ensure that the deletions permanent.

The certificates and CRL associated with a trust point automatically become persistent when imported (that is, without explicitly copying to the startup configuration) if the specific trust point is already saved in startup configuration.

We recommend that you create a password-protected backup of the identity certificates and save it to an external server.



Note Copying the configuration to an external server does include the certificates and key pairs.

Related Topics

[Exporting Identity Information in PKCS 12 Format](#), on page 16

Exporting Identity Information in PKCS 12 Format

You can export the identity certificate along with the RSA key pair and CA certificate (or the entire chain in the case of a subordinate CA) of a trust point to a PKCS#12 file for backup purposes. You can import the certificate and RSA key pair to recover from a system crash on your device or when you replace the supervisor modules.



Note You can use only the `bootflash:filename` format when specifying the export URL.

Before you begin

Authenticate the CA.

Install an identity certificate.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	crypto ca export name pkcs12 bootflash:filename password Example:	Exports the identity certificate and associated key pair and CA certificates for a trust point CA. The password is alphanumeric, case

	Command or Action	Purpose
	<pre>switch(config)# crypto ca export admin-ca pkcs12 bootflash:adminid.p12 nbv123</pre>	sensitive, and has a maximum length of 128 characters.
Step 3	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 4	copy bootflash:filename scheme://server/ [url /]filename Example: <pre>switch# copy bootflash:adminid.p12 tftp:adminid.p12</pre>	Copies the PKCS#12 format file to a remote server. For the <i>scheme</i> argument, you can enter tftp: , ftp: , scp: , or sftp: . The <i>server</i> argument is the address or name of the remote server, and the <i>url</i> argument is the path to the source file on the remote server. The <i>server</i> , <i>url</i> , and <i>filename</i> arguments are case sensitive.

Related Topics

[Generating an RSA Key Pair](#), on page 8

[Authenticating the CA](#), on page 10

[Installing Identity Certificates](#), on page 14

Importing Identity Information in PKCS 12 Format

You can import the certificate and RSA key pair to recover from a system crash on your device or when you replace the supervisor modules.



Note You can use only the bootflash:*filename* format when specifying the import URL.

Before you begin

Ensure that the trust point is empty by checking that no RSA key pair is associated with it and no CA is associated with the trust point using CA authentication.

Procedure

	Command or Action	Purpose
Step 1	copy scheme:// server/[url /]filename bootflash:filename Example: <pre>switch# copy tftp:adminid.p12 bootflash:adminid.p12</pre>	Copies the PKCS#12 format file from the remote server. For the <i>scheme</i> argument, you can enter tftp: , ftp: , scp: , or sftp: . The <i>server</i> argument is the address or name of the remote server, and the

	Command or Action	Purpose
		<i>url</i> argument is the path to the source file on the remote server. The <i>server</i> , <i>url</i> , and <i>filename</i> arguments are case sensitive.
Step 2	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 3	crypto ca import name [pkcs12] bootflash:filename Example: switch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.pl2 nbv123	Imports the identity certificate and associated key pair and CA certificates for trust point CA.
Step 4	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 5	(Optional) show crypto ca certificates Example: switch# show crypto ca certificates	Displays the CA certificates.
Step 6	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Configuring a CRL

You can manually configure CRLs that you have downloaded from the trust points. The Cisco NX-OS software caches the CRLs in the device bootflash (cert-store). During the verification of a peer certificate, the Cisco NX-OS software checks the CRL from the issuing CA only if you have downloaded the CRL to the device and you have configured certificate revocation checking to use the CRL.

Before you begin

Ensure that you have enabled certificate revocation checking.

Procedure

	Command or Action	Purpose
Step 1	copy scheme:[//server/[url /]]filename bootflash:filename	Downloads the CRL from a remote server.

	Command or Action	Purpose
	Example: <pre>switch# copy tftp:adminca.crl bootflash:adminca.crl</pre>	For the <i>scheme</i> argument, you can enter tftp: , ftp: , scp: , or sftp: . The <i>server</i> argument is the address or name of the remote server, and the <i>url</i> argument is the path to the source file on the remote server. The <i>server</i> , <i>url</i> , and <i>filename</i> arguments are case sensitive.
Step 2	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 3	crypto ca crl request name bootflash:filename Example: <pre>switch(config)# crypto ca crl request admin-ca bootflash:adminca.crl</pre>	Configures or replaces the current CRL with the one specified in the file.
Step 4	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 5	(Optional) show crypto ca crl name Example: <pre>switch# show crypto ca crl admin-ca</pre>	Displays the CA CRL information.
Step 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Deleting Certificates from the CA Configuration

You can delete the identity certificates and CA certificates that are configured in a trust point. You must first delete the identity certificate, followed by the CA certificates. After deleting the identity certificate, you can disassociate the RSA key pair from a trust point. You must delete certificates to remove expired or revoked certificates, certificates that have compromised (or suspected to be compromised) key pairs, or CAs that are no longer trusted.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example:	Enters global configuration mode.

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
Step 2	crypto ca trustpoint <i>name</i> Example: switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#	Specifies a trust point CA and enters trust point configuration mode.
Step 3	delete ca-certificate Example: switch(config-trustpoint)# delete ca-certificate	Deletes the CA certificate or certificate chain.
Step 4	delete certificate [force] Example: switch(config-trustpoint)# delete certificate	Deletes the identity certificate. You must use the force option if the identity certificate you want to delete is the last certificate in a certificate chain or only identity certificate in the device. This requirement ensures that you do not mistakenly delete the last certificate in a certificate chain or only the identity certificate and leave the applications (such as SSH) without a certificate to use.
Step 5	exit Example: switch(config-trustpoint)# exit switch(config)#	Exits trust point configuration mode.
Step 6	(Optional) show crypto ca certificates [<i>name</i>] Example: switch(config)# show crypto ca certificates admin-ca	Displays the CA certificate information.
Step 7	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Deleting RSA Key Pairs from a Cisco NX-OS Device

You can delete the RSA key pairs from a Cisco NX-OS device if you believe the RSA key pairs were compromised in some way and should no longer be used.



Note After you delete RSA key pairs from a device, ask the CA administrator to revoke your device's certificates at the CA. You must supply the challenge password that you created when you originally requested the certificates.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	crypto key zeroize rsa label Example: switch(config)# crypto key zeroize rsa MyKey	Deletes the RSA key pair.
Step 3	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 4	(Optional) show crypto key mypubkey rsa Example: switch# show crypto key mypubkey rsa	Displays the RSA key pair configuration.
Step 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Related Topics

[Generating Certificate Requests](#), on page 13

Verifying the PKI Configuration

To display PKI configuration information, perform one of the following tasks:

Command	Purpose
show crypto key mypubkey rsa	Displays information about the RSA public keys generated on the Cisco NX-OS device.

Command	Purpose
<code>show crypto ca certificates</code>	Displays information about CA and identity certificates.
<code>show crypto ca crl</code>	Displays information about CA CRLs.
<code>show crypto ca trustpoints</code>	Displays information about CA trust points.

Configuration Examples for PKI

This section shows examples of the tasks that you can use to configure certificates and CRLs on Cisco NX-OS devices using a Microsoft Windows Certificate server.



Note You can use any type of certificate server to generate digital certificates. You are not limited to using the Microsoft Windows Certificate server.

Configuring Certificates on a Cisco NX-OS Device

To configure certificates on a Cisco NX-OS device, follow these steps:

Procedure

Step 1

Configure the device FQDN.

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# hostname Device-1
Device-1(config)#
```

Step 2

Configure the DNS domain name for the device.

```
Device-1(config)# ip domain-name cisco.com
```

Step 3

Create a trust point.

```
Device-1(config)# crypto ca trustpoint myCA
Device-1(config-trustpoint)# exit
Device-1(config)# show crypto ca trustpoints
trustpoint: myCA; key:
revokation methods:  crl
```

Step 4

Create an RSA key pair for the device.

```
Device-1(config)# crypto key generate rsa label myKey exportable modulus 1024
Device-1(config)# show crypto key mypubkey rsa
```

```
key label: myKey
key size: 1024
exportable: yes
```

Step 5 Associate the RSA key pair to the trust point.

```
Device-1(config)# crypto ca trustpoint myCA
Device-1(config-trustpoint)# rsakeypair myKey
Device-1(config-trustpoint)# exit
Device-1(config)# show crypto ca trustpoints
trustpoint: myCA; key: myKey
revokation methods: crl
```

Step 6 Download the CA certificate from the Microsoft Certificate Service web interface.

Step 7 Authenticate the CA that you want to enroll to the trust point.

```
Device-1(config)# crypto ca authenticate myCA
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDsiay0GZRPSRI1jK0ZejaNBgkqhkiG9w0BAQFADCB
kDEgMB4GCSqGSIb3DQEJARYRYWlhbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAkIO
MRIwEAYDVQQIEw1LYXJuYXRha2ExEjAQBGNVBACTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ21zY28xEzARBGNVBAsTCm5ldHN0b3JhZ2UxEjAQBGNVBAMTCUFwYXJuYSBD
QTAEfw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdamIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWVufuZGt1QGNpc2NvLmNvbTELMakGALUEBhMCSU4xEjAQBGNVBAGTCUth
cm5hdGFrYTESMBAGALUEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVdaXNjbzETMBEG
A1UECzMKbmV0c3RvcmlFnZTESMBAGALUEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBSIHHzluNccNM87ypyzwuoSNZXOMperXXI
OzyBAGixT2ASFuUOWQ1iDM8rO/41jf8RxxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcyWdWYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyJyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAucCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBmNybDAwOC6gLIYqZmlsZTovL1xccc3N1LTA4XEN1cnRFbnJv
bGxcQXBhcm5hJTlWQ0EuY3JsbAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaQNgLh0AFcT0rEyuyt/WYGPzksF9EA
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
-----END CERTIFICATE-----
END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
Do you accept this certificate? [yes/no]:y
```

```
Device-1(config)# show crypto ca certificates
Trustpoint: myCA
CA certificate 0:
subject= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/
L=Bangalore/O=Yourcompany/OU=netstorage/CN=Aparna CA
issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/
L=Bangalore/O=Yourcompany/OU=netstorage/CN=Aparna CA
serial=0560D289ACB419944F4912258CAD197A
notBefore=May 3 22:46:37 2005 GMT
notAfter=May 3 22:55:17 2007 GMT
MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
purposes: sslserver sslclient ike
```

Step 8 Generate a request certificate to use to enroll with a trust point.

```
Device-1(config)# crypto ca enroll myCA
Create the certificate request ..
Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
```

```

For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password: nbv123
The subject name in the certificate will be: Device-1.cisco.com
Include the switch serial number in the subject name? [yes/no]: no
Include an IP address in the subject name [yes/no]: yes
ip address: 10.10.1.1
The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEAMBGA1UEAxMRVnVnYXMTMS5jaXNjby5jb20wgZ8wDQYJ
KoZlIhvcNAQEBAQAgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVA5MqNIGJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxblDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhhVpj+rargZvHtGJ91XTq4WoVksCzXv8S
VqyH0vEvAgMBAAGTzAVBggkqhkiG9w0BCQcxCBMGBmJ2MTIzMDYGCsQGSib3DQEJ
DjEpMccwJQYDVR0RAQH/BBswGYIRVnVnYXMTMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZlIhvcNAQEBAQAgYEAKT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt
PftrNcWUE/pw6HayfQ12T3ecgNwel2d15133YBF2bktExiI6U188nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----

```

Step 9 Request an identity certificate from the Microsoft Certificate Service web interface.

Step 10 Import the identity certificate.

```

Device-1(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCj00oQAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSib3DQEJARYRYWlhbmRrZUBjaXNjby5jb20xZCZAJBgNVBAYTAklOMRIwEAYD
VQOIEw1LYXJuYXRha2ExEjAQBGNVBAcTCUJhbmdbhG9yZTEOMAwGA1UEChMFQ21z
Y28xEzARBGNVBAsTCm5ldHN0b3JhZ2UxEjAQBGNVBAMTCUwYXJ5YXNjby5jb20x
NTEwMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwGjAYBgNVBAMTEVZlZ2FzLzEz
Y21zY28uY29tMIGfMA0GCSqGSib3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjkJSICdpLfk5eJSmNCQujGpzcKsZPFxfJ2UoiyeCYE8y1ncWYw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMcNIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCA8wJQYDVR0RAQH/BBsw
GYIRVnVnYXMTMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKLi+2sspWEfgrR
bhWmlVyo9jngMIHMBGNVHSMGcQwgcGAFCCo8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZlIhvcNAQkBFhFhbWVfZGt1QGNpc2NvLmNvbTELMakGA1UE
BhmCSU4xEjAQBGNVBAgTCUthcm5hdGFryTESMBAGA1UEBxMjQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVdaXNjbyETMBEGA1UECxmKbMvO3RvcMFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYnKJrLQZ1E9JEiWMRr16MGsGA1UdHwRkMG1wLQAsOCqGKGh0dHA6
Ly9zc2UtdMDgvdQ2VydeVucm9sbC9BcGFybmlmBDQ55jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxkZXJ0Rw5yb2xsXEFwYXJuYSUyMENBLmNybDcBbigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0N1cnRFbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNydA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4
XEN1cnRFbnJvbGwvc3NlLTA4X0FwYXJuYSUyMENBLmNydANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
Device-1(config)# exit
Device-1#

```

Step 11 Verify the certificate configuration.

Step 12 Save the certificate configuration to the startup configuration.

Related Topics

[Downloading a CA Certificate](#), on page 25

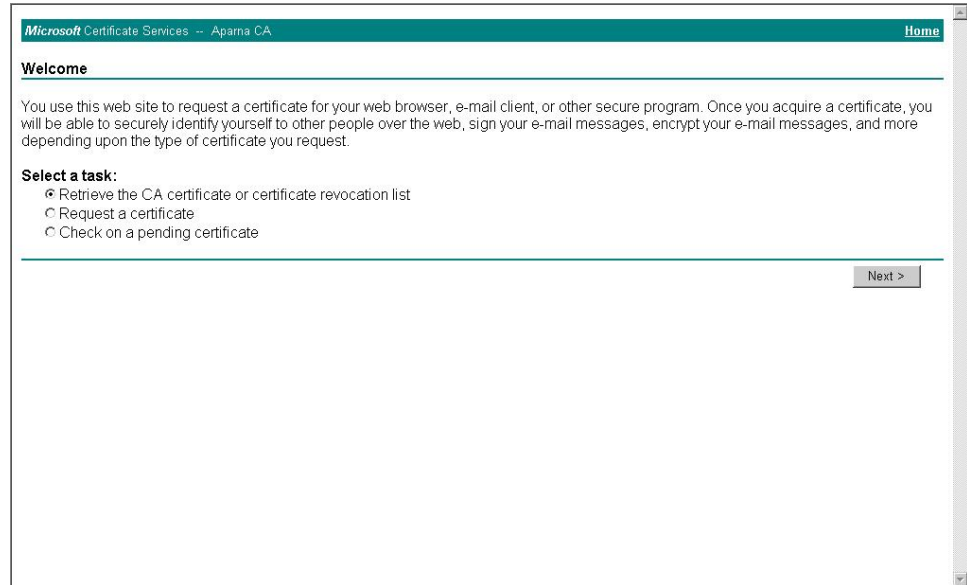
[Requesting an Identity Certificate](#), on page 28

Downloading a CA Certificate

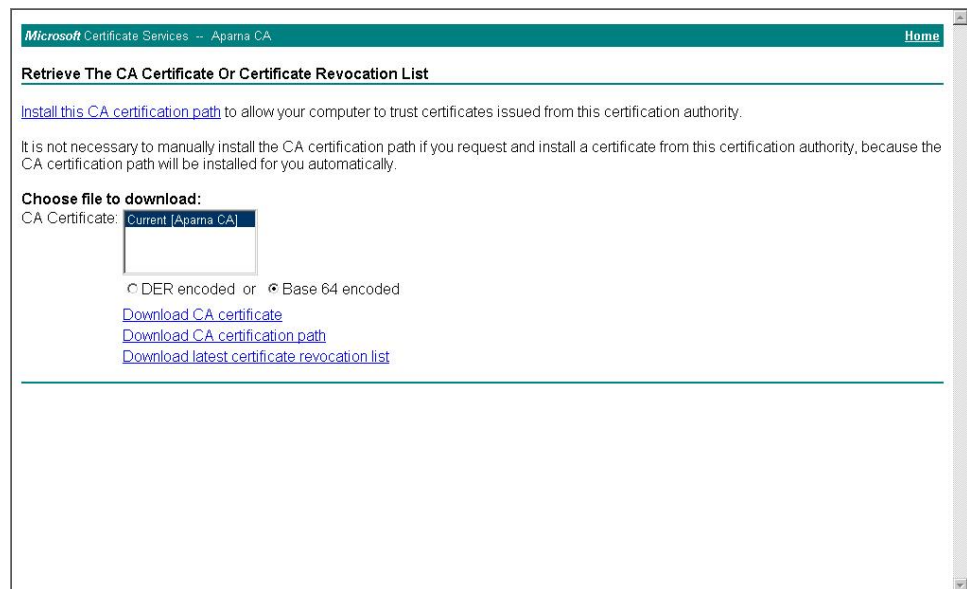
To download a CA certificate from the Microsoft Certificate Services web interface, follow these steps:

Procedure

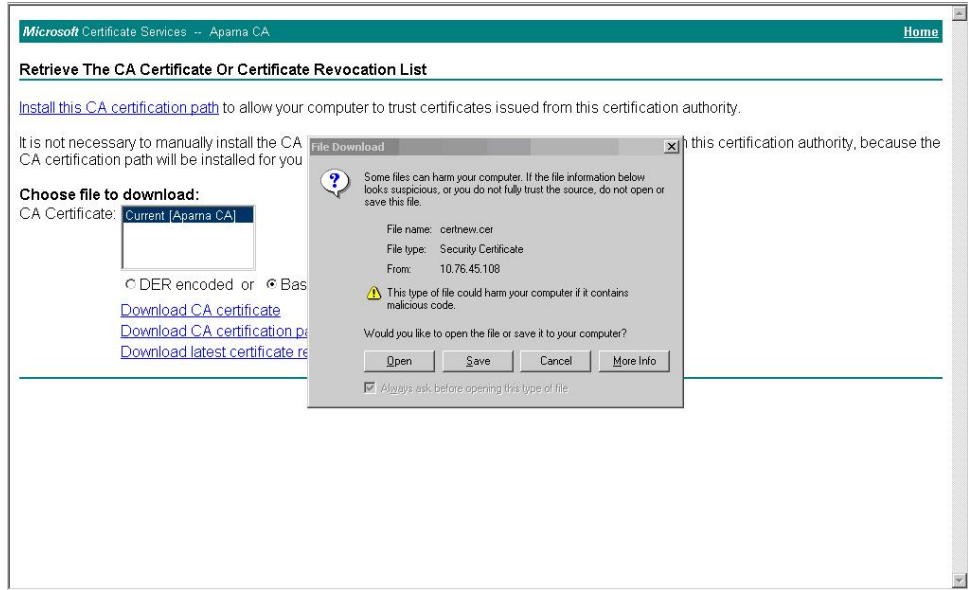
- Step 1** From the Microsoft Certificate Services web interface, click **Retrieve the CA certificate or certificate revocation task** and click **Next**.



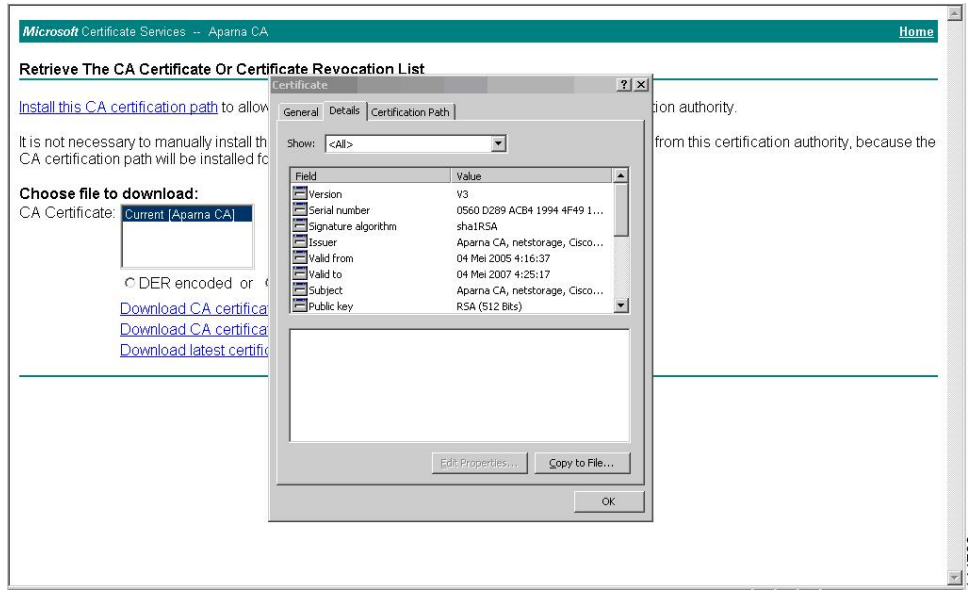
- Step 2** From the display list, choose the CA certificate file to download from the displayed list. Then click **Base 64 encoded** and click **Download CA certificate**.



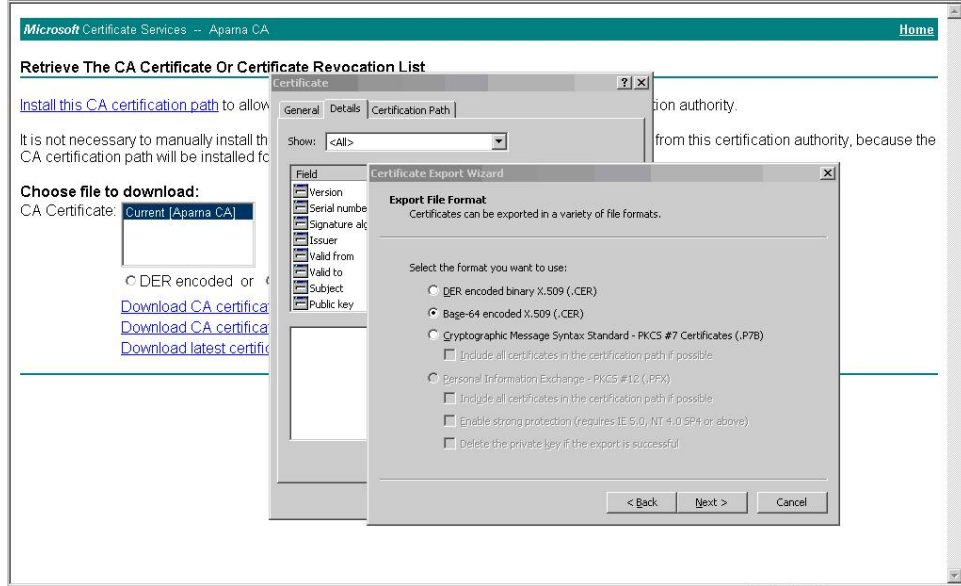
Step 3 Click **Open** in the File Download dialog box.



Step 4 In the Certificate dialog box, click **Copy to File** and click **OK**.



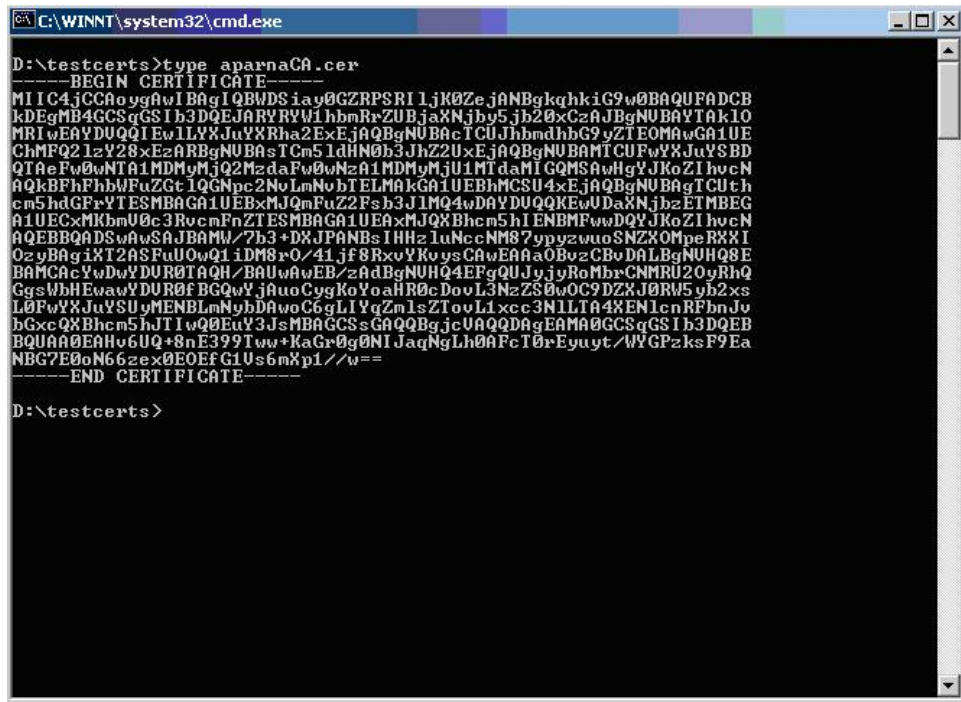
Step 5 From the Certificate Export Wizard dialog box, choose the **Base-64 encoded X.509 (CER)** and click **Next**.



Step 6 In the File name: text box on the Certificate Export Wizard dialog box, enter the destination file name and click **Next**.

Step 7 In the Certificate Export Wizard dialog box, click **Finish**.

Step 8 Enter the Microsoft Windows **type** command to display the CA certificate stored in Base-64 (PEM) format.



Requesting an Identity Certificate

To request an identify certificate from a Microsoft Certificate server using a PKCS#12 certificate signing request (CRS), follow these steps:

Procedure

Step 1

From the Microsoft Certificate Services web interface, click **Request a certificate** and click **Next**.

Microsoft Certificate Services -- Apama CA [Home](#)

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

[Next >](#)

144765

Step 2

Click **Advanced request** and click **Next**.

Microsoft Certificate Services -- Apama CA [Home](#)

Choose Request Type

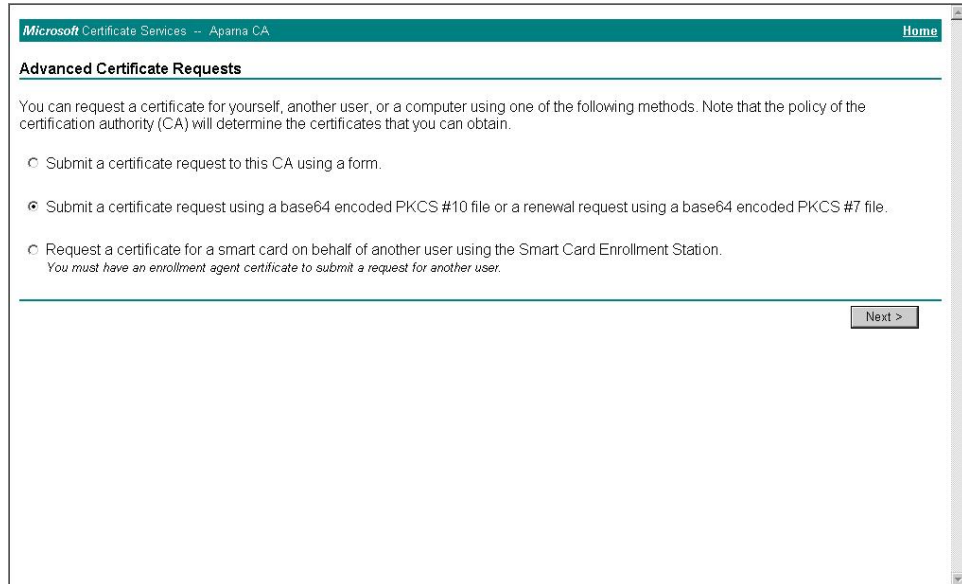
Please select the type of request you would like to make:

- User certificate request:
 - Web Browser Certificate
 - E-Mail Protection Certificate
- Advanced request

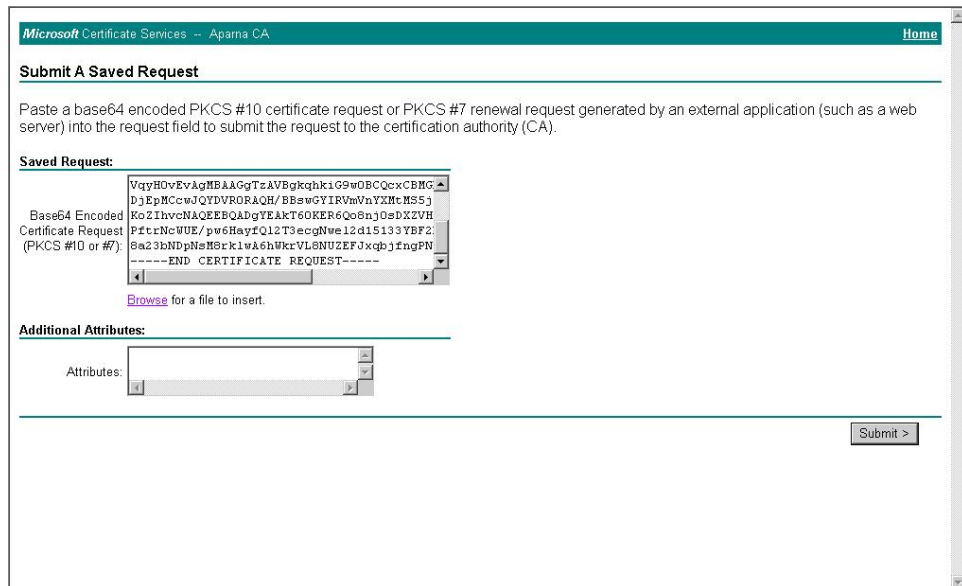
[Next >](#)

144766

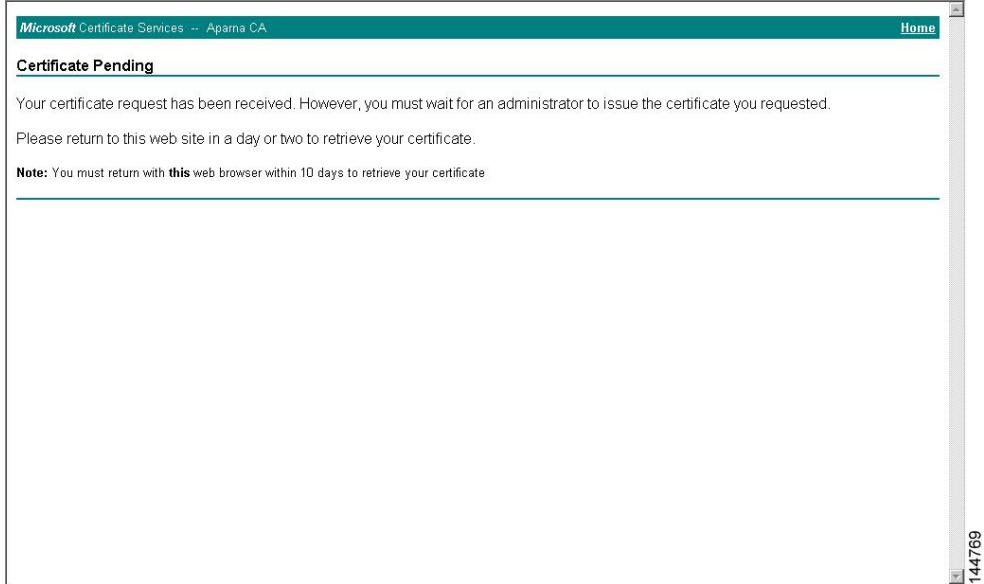
Step 3 Click **Submit a certificate request using a base64 encoded PKCS#10 file or a renewal request using a base64 encoded PKCS#7 file** and click **Next**.



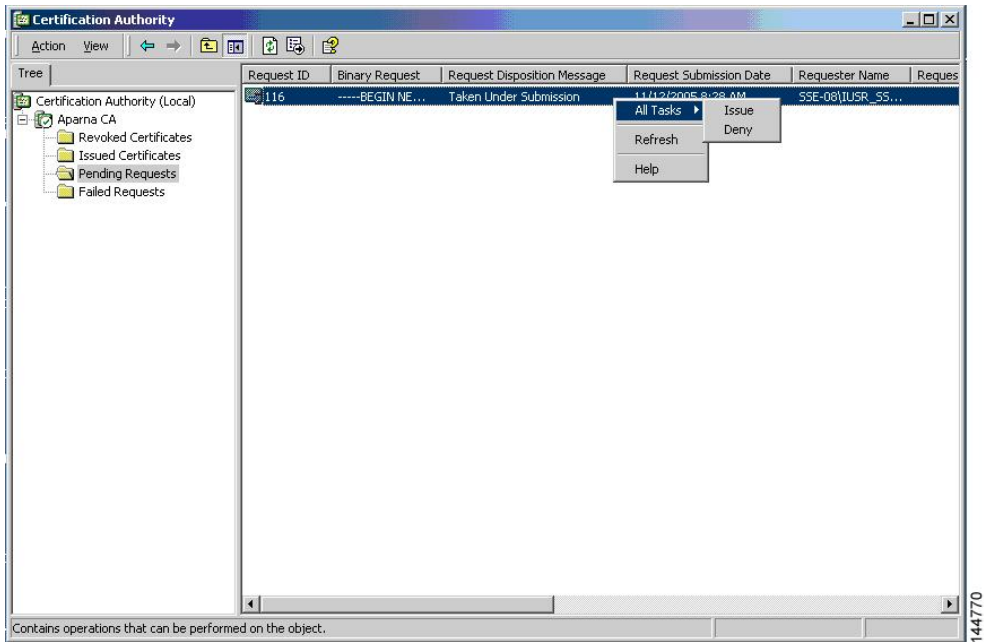
Step 4 In the **Saved Request** text box, paste the base64 PKCS#10 certificate request and click **Next**. The certificate request is copied from the Cisco NX-OS device console.



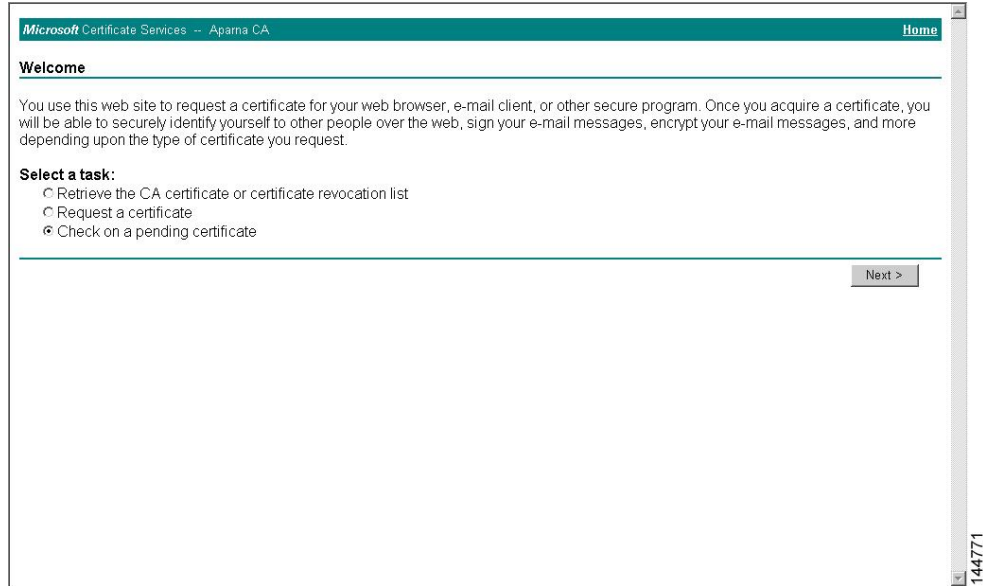
Step 5 Wait one or two days until the certificate is issued by the CA administrator.



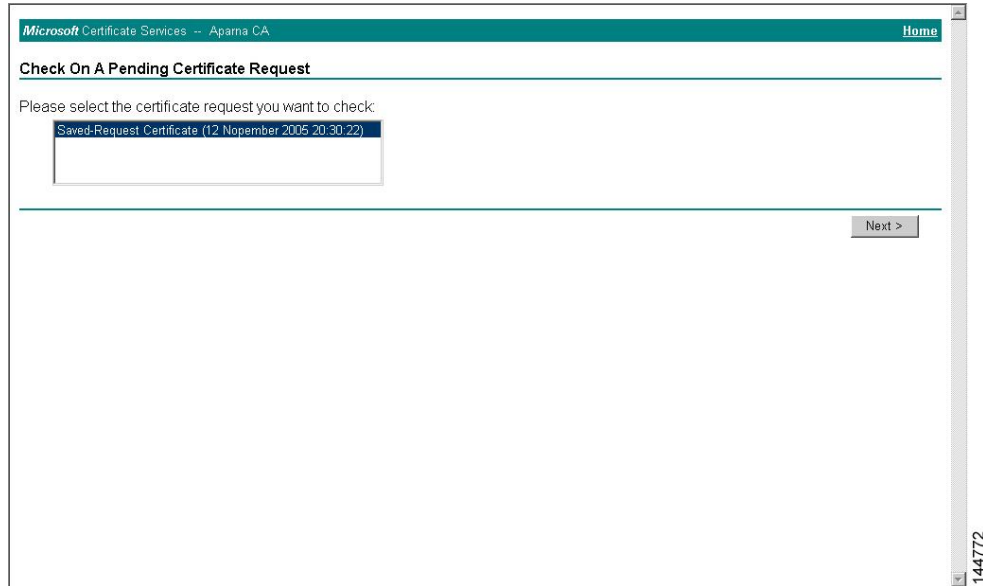
Step 6 Note that the CA administrator approves the certificate request.



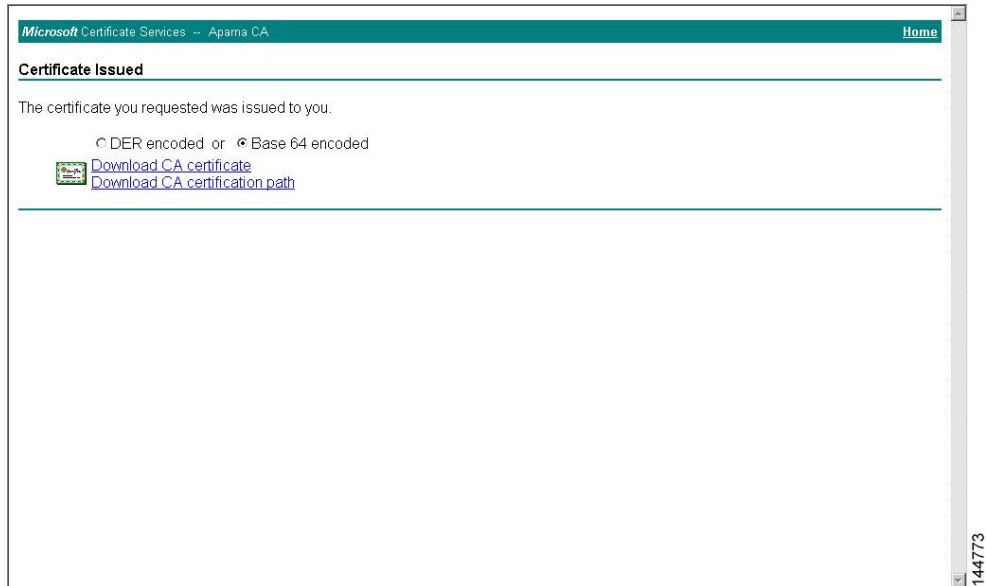
Step 7 From the Microsoft Certificate Services web interface, click **Check on a pending certificate** and click **Next**.



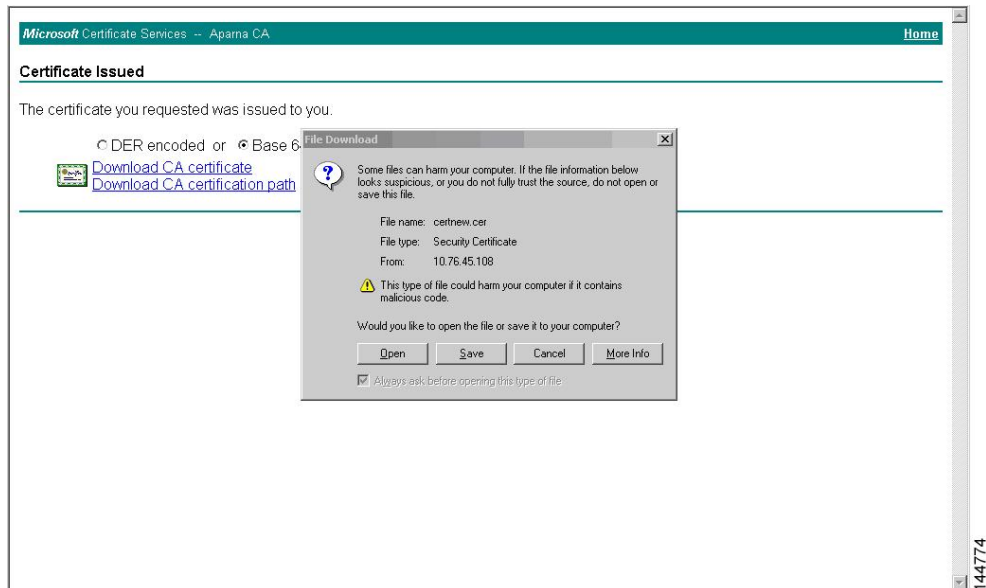
Step 8 Choose the certificate request that you want to check and click **Next**.



Step 9 Click **Base 64 encoded** and click **Download CA certificate**.

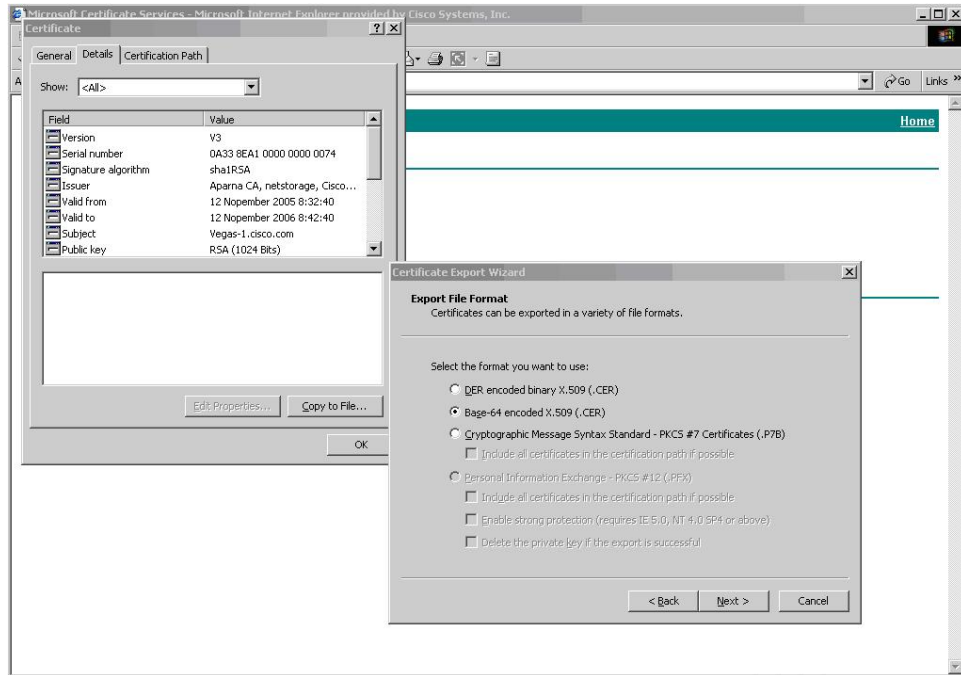


Step 10 In the File Download dialog box, click **Open**.



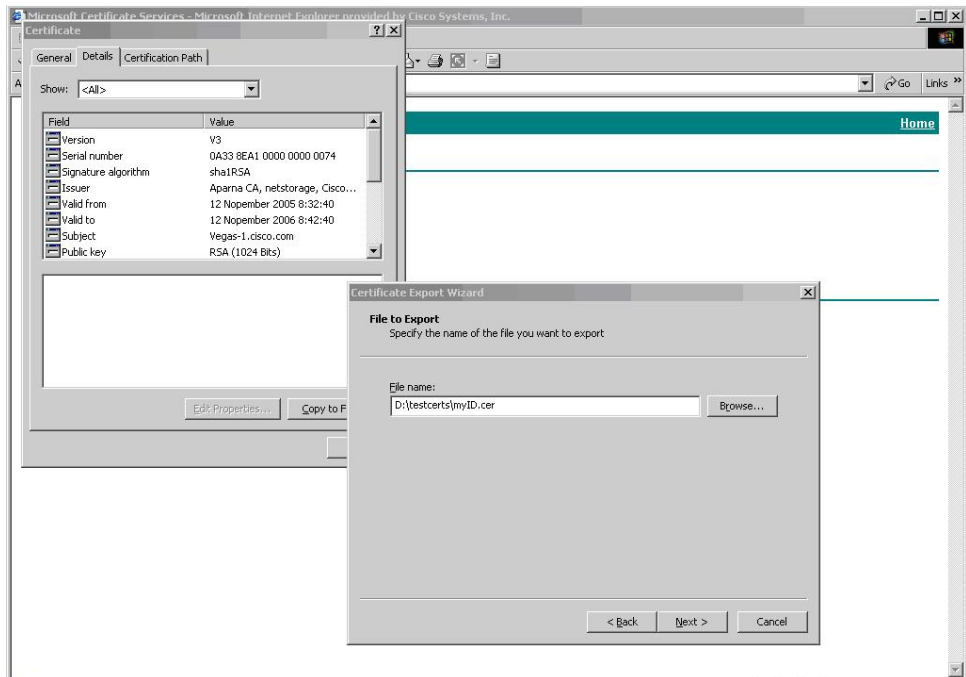
Step 11

In the Certificate box, click **Details** tab and click **Copy to File...**. In the Certificate Export Dialog box, click **Base-64 encoded X.509 (.CER)**, and click **Next**.

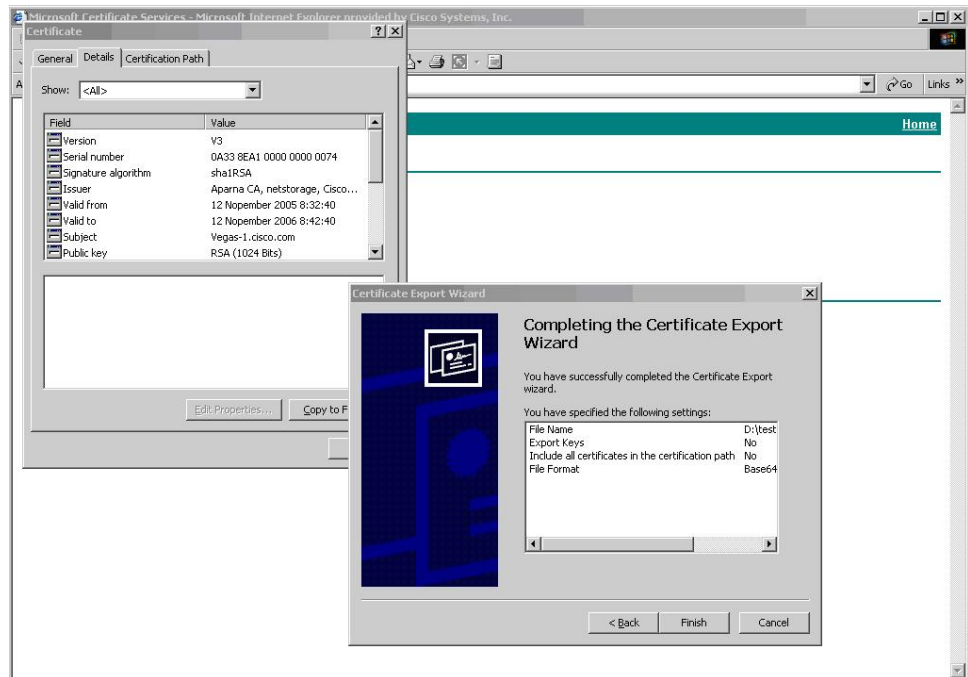


Step 12

In the File name: text box on the Certificate Export Wizard dialog box, enter the destination file name and

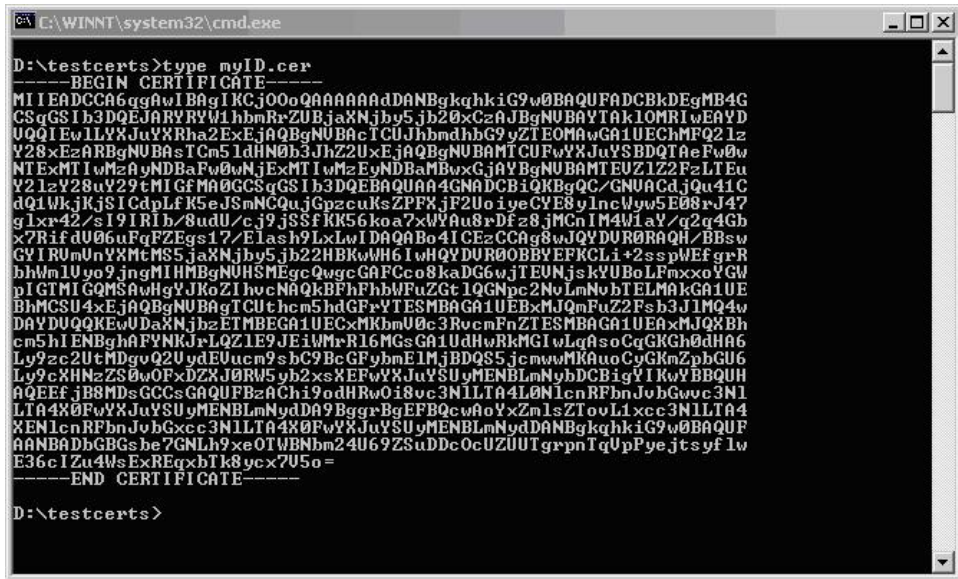


click **Next**.



Step 13 Click **Finish**.

Step 14 Enter the Microsoft Windows **type** command to display the identity certificate in base64-encoded format.



Related Topics

[Generating Certificate Requests](#), on page 13

[Configuring Certificates on a Cisco NX-OS Device](#), on page 22

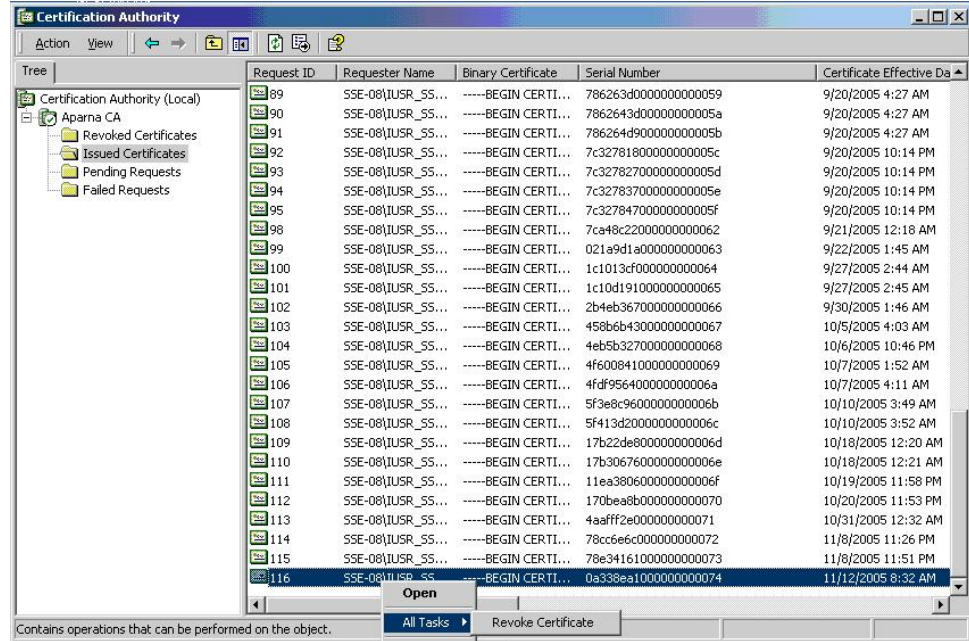
Revoking a Certificate

To revoke a certificate using the Microsoft CA administrator program, follow these steps:

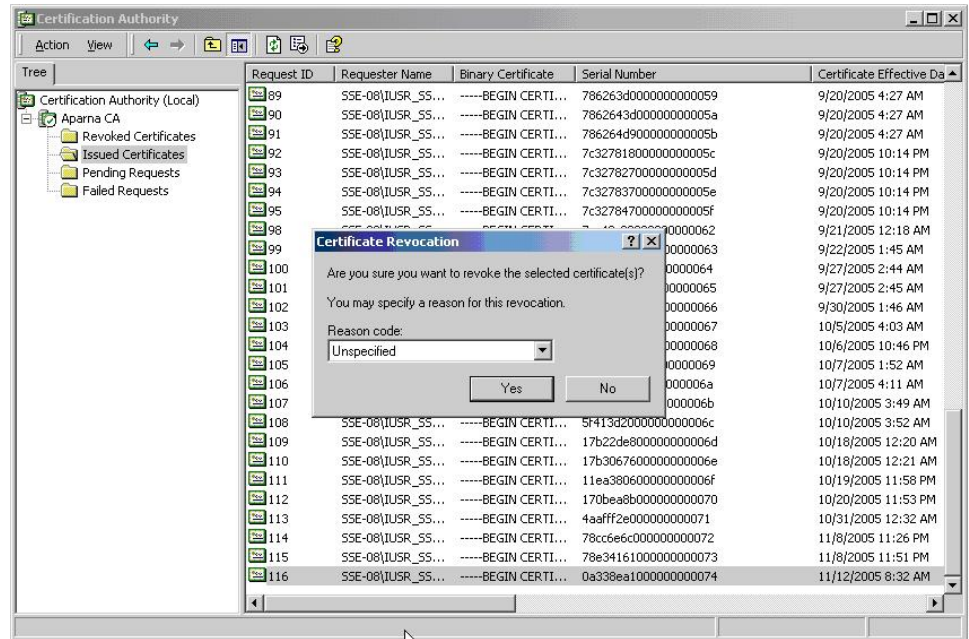
Procedure

Step 1 From the Certification Authority tree, click **Issued Certificates** folder. From the list, right-click the certificate that you want to revoke.

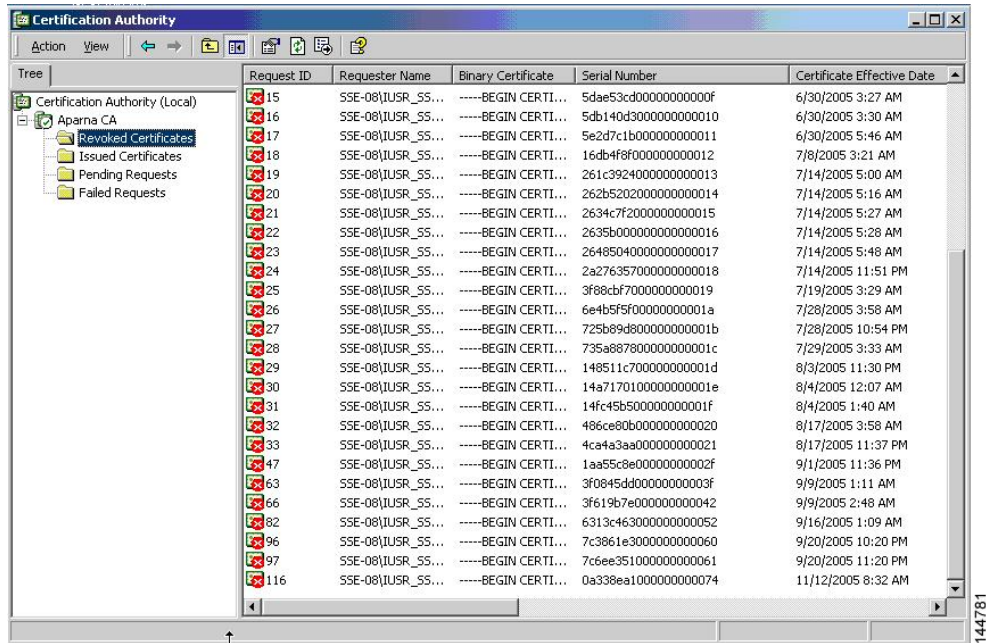
Step 2 Choose **All Tasks > Revoke Certificate**.



Step 3 From the Reason code drop-down list, choose a reason for the revocation and click **Yes**.



Step 4 Click the **Revoked Certificates** folder to list and verify the certificate revocation.

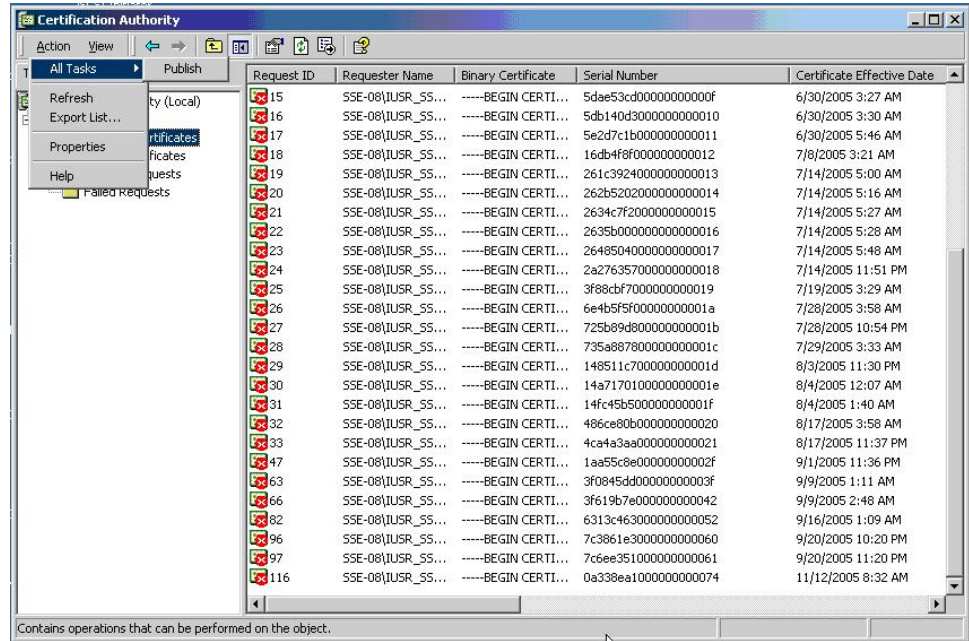


Generating and Publishing the CRL

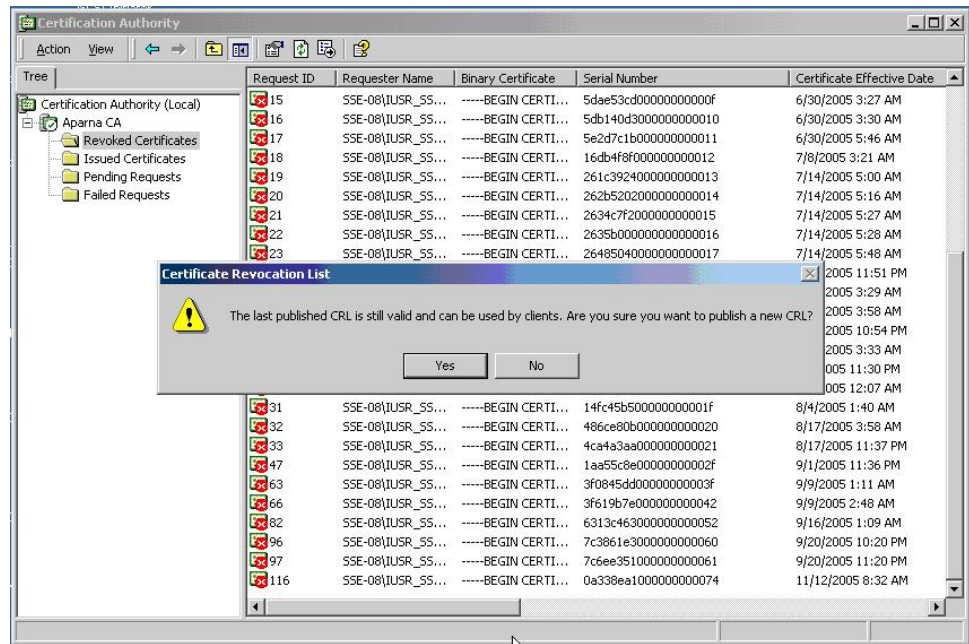
To generate and publish the CRL using the Microsoft CA administrator program, follow these steps:

Procedure

Step 1 From the Certification Authority screen, choose **Action > All Tasks > Publish**.



Step 2 In the Certificate Revocation List dialog box, click **Yes** to publish the latest CRL.

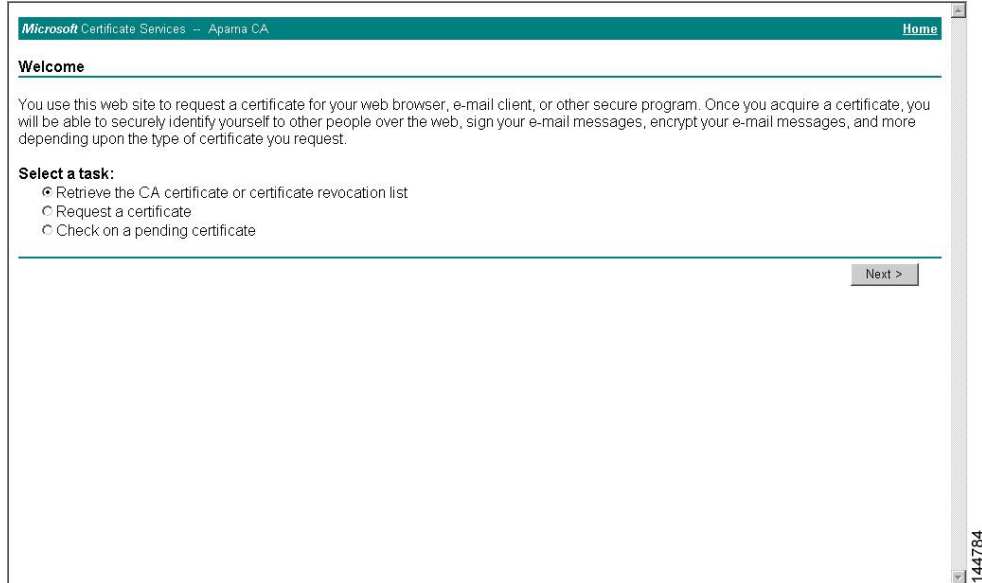


Downloading the CRL

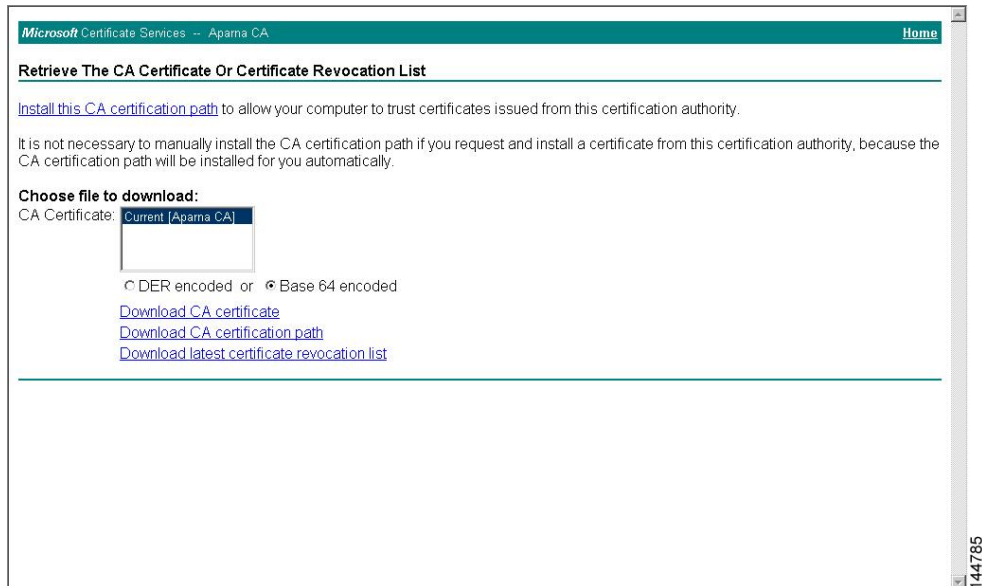
To download the CRL from the Microsoft CA website, follow these steps:

Procedure

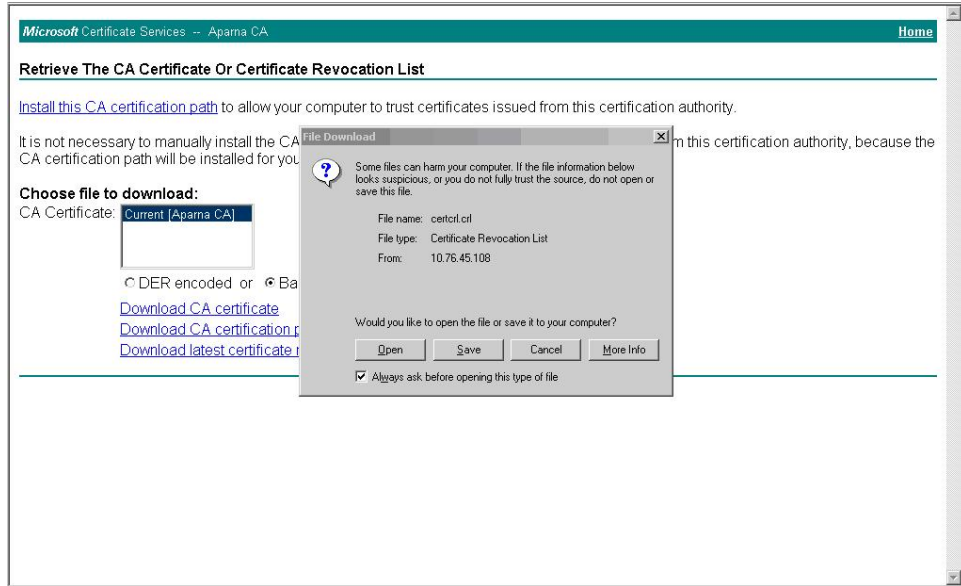
- Step 1** From the Microsoft Certificate Services web interface, click **Retrieve the CA certificate or certificate revocation list** and click **Next**.



- Step 2** Click **Download latest certificate revocation list**.

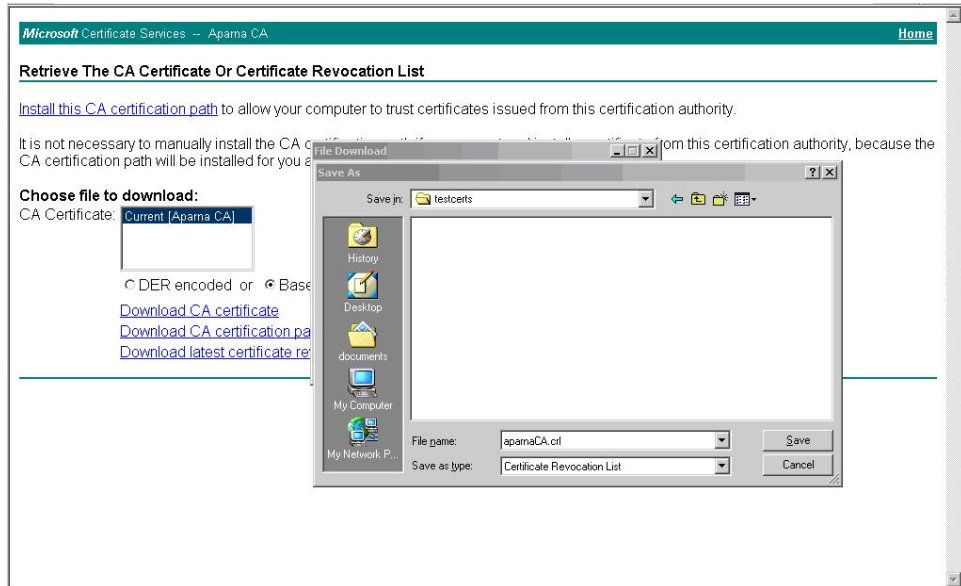


Step 3 In the File Download dialog box, click **Save**.



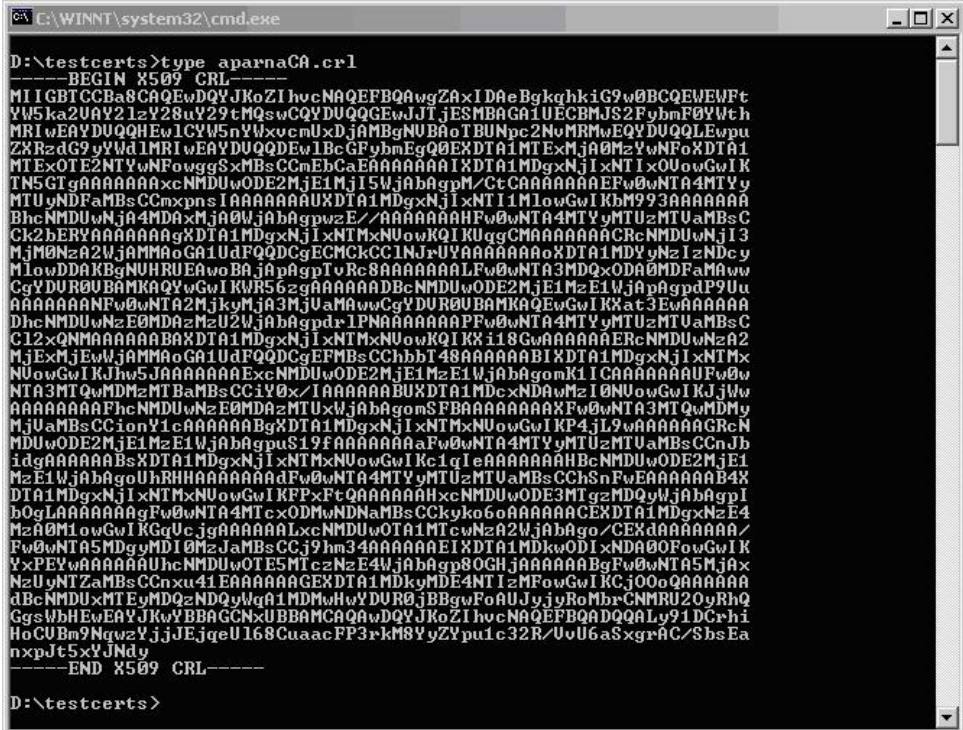
144786

Step 4 In the Save As dialog box, enter the destination file name and click **Save**.



144787

Step 5 Enter the Microsoft Windows **type** command to display the CRL.



```

C:\WINNT\system32\cmd.exe
D:\testcerts>type aparnaCA.crl
-----BEGIN X509 CRL-----
MIIGBTCCBa8CAQEWdQYJKoZlIhvcNAQEFBQAQwZAxiDAeBqkqhkig9w0BCQEWEWFt
YV5ka2UAY2IzY28uY29tMQswCQYDUQGEwJTIjESMBAGA1UECBMJLS2FybmF0eWt0
MRIwEAYDUQGEwJCIYVW5nYWxvcmUxJDAjMBgNUNBAoTUBnc2NvMRMwEQYDUQLWwpu
ZXRzdG9yYVdIMRIwEAYDUQDEw1BcGFybEg0Q0EkdTA1MTExMjA0MzYwNFoXDTA1
MTExOTFET2NTYwNFowGScMBsCCmEbCaEAAAAAAAAIkdTA1MDgxNjIjxNTIjxOUwGwIK
TN5GTgAAAAAAAAxcNMDUwODE2MjE1MjI1WjBhaGpM/CtCAAAAAAAAAEFw0wNTA4MTYy
MTUwMDFAmBSCCmXpnsIAAAAAAAAAUkdTA1MDgxNjIjxNTI1M1owGwIKhm923AAAAAAAA
BhcNMDUwNjA4MDAxMjA0MjE1MjE1WjBhaGpuzE//AAAAAAAAHFw0wNTA4MTYyMTUzMTUwMBsC
Ck2bERYAAAAAAAAgXDTA1MDgxNjIjxNTMxNUowKQIKUggCMAAAAAAAAAACrcNMDUwNjI3
MjM0NzA2WjAMMAoGA1UdFQDQCgECMCKCCINJRUyAAAAAAAAA0XDTA1MDYyNzIzNdcy
M1owDDAKBgnUHRUEAwoBAjBhaGpIURc8AAAAAAAAALFw0wNTA3MDQxODAwMDFAmAAww
CgYDUROUBAMKAQYwGwIKWR56zgAAAAAAAAADBCNMDUwODE2MjE1MzE1WjBhaGpDP9Uu
AAAAAAAAANFw0wNTA2MjE1MzE1MzE1WjBhaGpDUROUBAMKAQEWGwIKXat3EwAAAAAAAA
DhcNMDUwNzE0MDA2MzU2WjBhaGpdr1PNAAAAAAAAAAFw0wNTA4MTYyMTUzMTUwMBsC
C12xQNMMAAAAAAAAAAAXDTA1MDgxNjIjxNTMxNUowKQIKX118GwAAAAAAAAERcNMDUwNzA2
MjE1WjBhaGpDUROUBAMMAoGA1UdFQDQCgEFMBSCCghbht48AAAAAAAABIkdTA1MDgxNjIjxNTMx
NUowGwIKJhw5JAAAAAAAAAxcNMDUwODE2MjE1MzE1WjBhaGp0MzIjCAAAAAAAAAFw0w
NTA3MTQwMDMzMTBAMBSCCciY0x/IAAAAAAAAABUkdTA1MDcxNDAwMzE1OUwGwIKJjhw
AAAAAAAAAHFhcNMDUwNzE0MDA2MzU2WjBhaGp0MzE1WjBhaGp0MzE1WjBhaGp0MzE1Wj
MjUwMBSCCionY1cAAAAAAAAAgXDTA1MDgxNjIjxNTMxNUowGwIKP4jL9wAAAAAAAAACrcN
MDUwODE2MjE1MzE1WjBhaGp0MzE1WjBhaGp0MzE1WjBhaGp0MzE1WjBhaGp0MzE1Wj
idgAAAAAAAAAAXDTA1MDgxNjIjxNTMxNUowGwIKc1qIeAAAAAAAAAHbcNMDUwODE2MjE1
MzE1WjBhaGp0MzE1WjBhaGp0MzE1WjBhaGp0MzE1WjBhaGp0MzE1WjBhaGp0MzE1Wj
DTA1MDgxNjIjxNTMxNUowGwIKFPxFtQAAAAAAAAHxcNMDUwODE2MjE1MzE1WjBhaGp1
b0qLAAAAAAAAAgFw0wNTA4MTIjxODMwNDNaMBSCCkyo6oAAAAAAAAACEXDTA1MDgxNzE4
MzA0MTowGwIKGqUcJgAAAAAAAAALxcNMDUwOTA1MTc3NzA2WjBhaGp0MzE1WjBhaGp0
Fw0wNTA5MDgyMDIj0MzJAMBSCCj9hm34AAAAAAAAEIkdTA1MDkxMDUwMDIjxNDA0OFowGwIK
YxPEYwAAAAAAAAAUhcNMDUwOTE5MTczNzE4WjBhaGp0MzE1WjBhaGp0MzE1WjBhaGp0MzE1Wj
NzUwNTZAMBSCCnxxu41EAAAAAAAAAGEXDTA1MDkxMDE4NTEzMFowGwIKCj0OoQAAAAAA
dBcNMDUwMTYyMTUzMTUzMTUzMTUzMTUzMTUzMTUzMTUzMTUzMTUzMTUzMTUzMTUzMTUzMTUz
GgsWbHEwEAYJKoZlR00jBBAMCAQAwDQYJKoZIhvcNAQEFBQAADQALy91DCrhI
HoCUBn9NqWzYjJJEjgeU168CuaacFP3rkM8YyZyPu1c32R/Uu06a5xgrAC/SbsEa
nXpJt5xYJNdY
-----END X509 CRL-----

D:\testcerts>

```

Related Topics

[Configuring Certificate Revocation Checking Methods](#), on page 12

Importing the CRL

To import the CRL to the trust point corresponding to the CA, follow these steps:

Procedure

Step 1 Copy the CRL file to the Cisco NX-OS device bootflash.

```
Device-1# copy tftp:aparnaCA.crl bootflash:aparnaCA.crl
```

Step 2 Configure the CRL.

```
Device-1# configure terminal
Device-1(config)# crypto ca crl request myCA bootflash:aparnaCA.crl
Device-1(config)#
```

Step 3 Display the contents of the CRL.

```
Device-1(config)# show crypto ca crl myCA
Trustpoint: myCA
```



```
CRL:
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: /emailAddress=admin@yourcompany.com/C=IN/ST=Karnatak
Yourcompany/OU=netstorage/CN=Aparna CA
  Last Update: Nov 12 04:36:04 2005 GMT
  Next Update: Nov 19 16:56:04 2005 GMT
  CRL extensions:
    X509v3 Authority Key Identifier:
      keyid:27:28:F2:46:83:1B:AC:23:4C:45:4D:8E:C9:18:50:1
      1.3.6.1.4.1.311.21.1:
        ...
  Revoked Certificates:
    Serial Number: 611B09A1000000000002
      Revocation Date: Aug 16 21:52:19 2005 GMT
    Serial Number: 4CDE464E000000000003
      Revocation Date: Aug 16 21:52:29 2005 GMT
    Serial Number: 4CFC2B42000000000004
      Revocation Date: Aug 16 21:52:41 2005 GMT
    Serial Number: 6C699EC2000000000005
      Revocation Date: Aug 16 21:52:52 2005 GMT
    Serial Number: 6CCF7DDC000000000006
      Revocation Date: Jun  8 00:12:04 2005 GMT
    Serial Number: 70CC4FFF000000000007
      Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 4D9B1116000000000008
      Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 52A80230000000000009
      Revocation Date: Jun 27 23:47:06 2005 GMT
      CRL entry extensions:
        X509v3 CRL Reason Code:
          CA Compromise
    Serial Number: 5349AD46000000000000A
      Revocation Date: Jun 27 23:47:22 2005 GMT
      CRL entry extensions:
        X509v3 CRL Reason Code:
          CA Compromise
    Serial Number: 53BD173C000000000000B
      Revocation Date: Jul  4 18:04:01 2005 GMT
      CRL entry extensions:
        X509v3 CRL Reason Code:
          Certificate Hold
    Serial Number: 591E7ACE000000000000C
      Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5D3FD52E000000000000D
      Revocation Date: Jun 29 22:07:25 2005 GMT
      CRL entry extensions:
        X509v3 CRL Reason Code:
          Key Compromise
    Serial Number: 5DAB7713000000000000E
      Revocation Date: Jul 14 00:33:56 2005 GMT
    Serial Number: 5DAE53CD000000000000F
      Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5DB140D30000000000010
      Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5E2D7C1B0000000000011
      Revocation Date: Jul  6 21:12:10 2005 GMT
      CRL entry extensions:
        X509v3 CRL Reason Code:
          Cessation Of Operation
    Serial Number: 16DB4F8F0000000000012
      Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 261C39240000000000013
```

```

    Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 262B5202000000000014
    Revocation Date: Jul 14 00:33:10 2005 GMT
Serial Number: 2634C7F2000000000015
    Revocation Date: Jul 14 00:32:45 2005 GMT
Serial Number: 2635B000000000000016
    Revocation Date: Jul 14 00:31:51 2005 GMT
Serial Number: 26485040000000000017
    Revocation Date: Jul 14 00:32:25 2005 GMT
Serial Number: 2A276357000000000018
Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 3F88CBF7000000000019
    Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 6E4B5F5F00000000001A
    Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 725B89D800000000001B
    Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 735A887800000000001C
    Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 148511C700000000001D
    Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 14A7170100000000001E
    Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 14FC45B500000000001F
    Revocation Date: Aug 17 18:30:42 2005 GMT
Serial Number: 486CE80B000000000020
    Revocation Date: Aug 17 18:30:43 2005 GMT
Serial Number: 4CA4A3AA000000000021
    Revocation Date: Aug 17 18:30:43 2005 GMT
Serial Number: 1AA55C8E00000000002F
    Revocation Date: Sep 5 17:07:06 2005 GMT
Serial Number: 3F0845DD00000000003F
    Revocation Date: Sep 8 20:24:32 2005 GMT
Serial Number: 3F619B7E000000000042
    Revocation Date: Sep 8 21:40:48 2005 GMT
Serial Number: 6313C463000000000052
    Revocation Date: Sep 19 17:37:18 2005 GMT
Serial Number: 7C3861E3000000000060
    Revocation Date: Sep 20 17:52:56 2005 GMT
Serial Number: 7C6EE351000000000061
    Revocation Date: Sep 20 18:52:30 2005 GMT
Serial Number: 0A338EA1000000000074  <-- Revoked identity certificate
    Revocation Date: Nov 12 04:34:42 2005 GMT
Signature Algorithm: sha1WithRSAEncryption
0b:cb:dd:43:0a:b8:62:1e:80:95:06:6f:4d:ab:0c:d8:8e:32:
44:8e:a7:94:97:af:02:b9:a6:9c:14:fd:eb:90:cf:18:c9:96:
29:bb:57:37:d9:1f:d5:bd:4e:9a:4b:18:2b:00:2f:d2:6e:c1:
1a:9f:1a:49:b7:9c:58:24:d7:72

```

Note The identity certificate for the device that was revoked (serial number 0A338EA1000000000074) is listed at the end.

Additional References for PKI

This section includes additional information related to implementing PKI.

Related Documents for PKI

Related Topic	Document Title
Cisco NX-OS Licensing	<i>Cisco NX-OS Licensing Guide</i>
VRF configuration	<i>Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide</i>

Standards for PKI

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

