

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 5
- Default Settings for PKI, on page 6
- Configuring CAs and Digital Certificates, on page 6
- Verifying the PKI Configuration, on page 25
- Configuration Examples for PKI, on page 26

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.

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, 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.

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 identify 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 10.3(3)F, Elliptic Curve Cyptography (ECC) key pair support is provided to generate and import the certificate on Cisco Nexus switches.



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
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.

L

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

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

SUMMARY STEPS

- 1. configure terminal
- 2. hostname hostname
- 3. ip domain-name name [use-vrf vrf-name]
- 4. exit
- 5. (Optional) show hosts
- 6. (Optional) copy running-config startup-config

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.
	Example:	
	<pre>switch# configure terminal switch(config)#</pre>	
Step 2	hostname hostname	Configures the hostname of the device.
	Example:	
	<pre>switch(config)# hostname DeviceA</pre>	
Step 3	ip domain-name name [use-vrf vrf-name]	Configures the IP domain name of the device. If you do not
	Example:	specify a VRF name, the command uses the default VRF.
	<pre>DeviceA(config) # ip domain-name example.com</pre>	
Step 4	exit	Exits configuration mode.
	Example:	
	switch(config)# exit switch#	
Step 5	(Optional) show hosts	Displays the IP domain name.
	Example:	
	switch# show hosts	
Step 6	(Optional) copy running-config startup-config	Copies the running configuration to the startup
	Example:	configuration.

 Command or Action	Purpose
 <pre>switch# copy running-config startup-config</pre>	

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.

SUMMARY STEPS

- 1. configure terminal
- 2. crypto key generate rsa [label label-string] [exportable] [modulus size]
- 3. exit
- 4. (Optional) show crypto key mypubkey rsa
- 5. (Optional) copy running-config startup-config

	Command or Action	Purpose	
Step 1	configure terminal	Enters glob	al configuration mode.
	Example:		
	<pre>switch# configure terminal switch(config)#</pre>		
Step 2	crypto key generate rsa [label <i>label-string</i>] [exportable] [modulus <i>size</i>]		an RSA key pair. The maximum number of key levice is 16.
	Example:	The label string is alphanumeric, case sensitive, and h	
	<pre>switch(config)# crypto key generate rsa exportable</pre>	maximum length of 64 characters. The default labels is the hostname and the FQDN separated by a period character (.).	ame and the FQDN separated by a period
			ulus values are 512, 768, 1024, 1536, and 2048. t modulus size is 512.
		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.
			the key pair is not exportable. Only exportable an be exported in the PKCS#12 format.
		Caution	You cannot change the exportability of a key pair.

L

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

Generating an ECC Key Pair

You can generate an ECC key pair to sign and/or encrypt and decrypt the security payload during security protocol exchanges for applications. You must generate the ECC key pair before you can obtain a certificate for your device. The ECC keys are stronger compared to RSA keys for a given length.

Beginning Cisco NX-OS Release 10.3(3)F, you can generate an ECC key pair to associate the Cisco NX-OS device with a trust point CA.

SUMMARY STEPS

- 1. configure terminal
- 2. crypto key generate ecc [label ecc-key-label] [exportable] [modulus size]
- **3.** no crypto key generate ecc [label *ecc-key-label*]
- 4. exit
- 5. (Optional) show crypto key mypubkey ecc
- 6. (Optional) copy running-config startup-config

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.
	Example:	
	<pre>switch# configure terminal switch(config)#</pre>	
Step 2	crypto key generate ecc [label ecc-key-label] [exportable] [modulus size]	Generates an RSA key pair. The maximum number of key pairs on a device is 16.
	Example:	The label string is alphanumeric, case sensitive, and has
	<pre>switch(config)# crypto key generate ecc exportable modulus 224</pre>	maximum length of 64 characters. The default label string is the hostname and the FQDN separated by a period character (.).

		Purpose	
			Valid modulus values are 224, 384, and 521. The default modulus size is 224.
		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.
			t, the key pair is not exportable. Only exportable can be exported in the PKCS#12 format.
		Caution	You cannot change the exportability of a key pair.
Step 3	no crypto key generate ecc [label ecc-key-label]	Deletes th	e ECC key.
	Example:		
	<pre>switch(config)# no crypto key generate ecc label label-name</pre>		
Step 4	exit	Exits conf	figuration mode.
	Example:		
	<pre>switch(config)# exit switch#</pre>		
Step 5	(Optional) show crypto key mypubkey ecc	Displays t	he generated ECC key.
	Example:		
	switch# show crypto key mypubkey ecc		
Step 6	(Optional) copy running-config startup-config	Copies the running configuration to the startup configuration.	
	Example:		tion.
	switch# copy running-config startup-config		

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.

SUMMARY STEPS

- **1**. configure terminal
- 2. crypto ca trustpoint name
- **3**. enrollment terminal
- 4. rsakeypair label
- 5. exit
- 6. (Optional) show crypto ca trustpoints

7. (Optional) copy running-config startup-config

DETAILED STEPS

	Command or Action	Purpose	
Step 1	configure terminal	Enters global configuration mode.	
	Example:		
	<pre>switch# configure terminal switch(config)#</pre>		
Step 2	crypto ca trustpoint <i>name</i>	Declares a trust point CA that the device should trust and enters trust point configuration mode.	
	<pre>Example: switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#</pre>	Note The maximum number of trustpoints that can be configured is 50.	
Step 3	enrollment terminal	Enables manual cut-and-paste certificate enrollment. The default is enabled.	
	<pre>Example: switch(config-trustpoint)# enrollment terminal</pre>	Note The Cisco NX-OS software supports only the manual cut-and-paste method for certificate enrollment.	
Step 4	rsakeypair label	Specifies the label of the RSA key pair to associate to this trust point for enrollment.	
	Example:		
	<pre>switch(config-trustpoint)# rsakeypair SwitchA</pre>	Note You can specify only one RSA key pair per CA.	
Step 5	exit	Exits trust point configuration mode.	
	Example:		
	<pre>switch(config-trustpoint)# exit switch(config)#</pre>		
Step 6	(Optional) show crypto ca trustpoints	Displays trust point information.	
	Example:		
	<pre>switch(config)# show crypto ca trustpoints</pre>		
Step 7	(Optional) copy running-config startup-config	Copies the running configuration to the startup	
	Example:	configuration.	
	<pre>switch(config)# copy running-config startup-config</pre>	3	

Related Topics

Generating an RSA Key Pair, on page 8

Configuring Certificate Mapping Filters

You can configure mapping filters to validate the CA certificates that are used for authentication. The mapping filters are used to match the CA certificate against a username.

Cisco NX-OS supports the following certificate mapping filters:

- %username%—Substitutes the user's login name.
- %hostname%—Substitutes the peer hostname.

Before you begin

Configure a cert-store for certificate authentication.

SUMMARY STEPS

- **1**. configure terminal
- 2. crypto certificatemap mapname map-name
- **3.** filter [subject-name subject-name | altname-email e-mail-ID | altname-upn user-principal-name]
- 4. exit
- 5. (Optional) crypto cert ssh-authorize [default | issuer-CAname] [map map-name1 [map-name2]]
- 6. (Optional) show crypto certificatemap
- 7. (Optional) show crypto ssh-auth-map
- 8. (Optional) copy running-config startup-config

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.
	Example:	
	<pre>switch# configure terminal switch(config)#</pre>	
Step 2	crypto certificatemap mapname map-name	Creates a new filter map.
	Example:	
	<pre>switch(config)# crypto certificatemap mapname filtermap1</pre>	
Step 3	filter [subject-name <i>subject-name</i> altname-email <i>e-mail-ID</i> altname-upn <i>user-principal-name</i>]	Configures one or more certificate mapping filters within the filter map. These certificate field attributes are supported
	Example:	in the filters: The validation passes if the certificate passes all of the filters configured in the map.
		filter subject-name CN=%username%
		or
		filter subject-name /C=IN/ST=KA/L=BLR/O=CISCO/OU=ABC/CN=%username%
		• altname-email—The e-mail address that must be present in the certificate as a subject alternative name. For example:
		filter altname-email %username%@cisco.com

	Command or Action	Purpose
		 altname-upn—The principal name that must be present in the certificate as a subject alternative name. For example:
		filter altname-upn %username%@%hostname%
		The validation passes if the certificate passes all of the filters configured in the map.
Step 4	exit	Exits certificate mapping filter configuration mode.
	Example:	
	<pre>switch(config-certmap-filter)# exit switch(config)#</pre>	
Step 5	<pre>(Optional) crypto cert ssh-authorize [default issuer-CAname] [map map-name1 [map-name2]] Example: switch(config)# crypto cert ssh-authorize default </pre>	Configures a certificate mapping filter for the Secure Shell (SSH) protocol. You can use the default filter map for SSH authorization or specify the issuer of the CA certificate. If you do not use the default map, you can specify one or two filter maps for authorization.
	map filtermap1	If you specify the issuer of the CA certificate, the certificate bound to the user account is validated as successful if it passes one of the configured maps.
Step 6	(Optional) show crypto certificatemap	Displays the certificate mapping filters.
	<pre>Example: switch(config)# show crypto certificatemap</pre>	
Step 7	(Optional) show crypto ssh-auth-map	Displays the mapping filters configured for SSH
	Example:	authentication.
	switch(config)# show crypto ssh-auth-map	
Step 8	(Optional) copy running-config startup-config	Copies the running configuration to the startup
	Example:	configuration.

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.



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.

SUMMARY STEPS

- 1. configure terminal
- 2. crypto ca authenticate name
- 3. exit
- 4. (Optional) show crypto ca trustpoints
- 5. (Optional) copy running-config startup-config

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.
	Example:	
	<pre>switch# configure terminal switch(config)#</pre>	
Step 2	crypto ca authenticate name	Prompts you to cut and paste the certificate of the CA. Use the same name that you used when declaring the CA.
	Example:	the same name that you used when declaring the CA.
	<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 MIIC4jCCAoygAwIBAgIQEWDSiayOGZRPSRIIjKOZejANBgkchkiG9wOBAQUFADCE kDEgMB4GC3cgSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCZAJBgNVBAYTAklC MRIWEAYDVQQIEw1LYXJuYXRha2ExEjAQBgNVBACTCUJhbmchbG9yZTEOMAwGA1UE CMFQ21zY28xEzARBgNVBASTOn51dHNOb3JhZ2UxEjAQBgNWBAMTCUFWYXJuYSBI QIAeFW0wNIAIMDMyMjQ2MzdaFW0w1vZAIMDMyMjUIMIdaMIGQVSAwHgYJKoZIhvch AQkBFhFhbWFuZGt1QCNpc2NvInNvbTEIMAkGA1UEBhMCSU4xEjAQBgNVBAgICUth cm5hdGFrYTESMBAGA1UEBMUQmFuZ2Fsb3JIMQ4wDAYDVQKEwJDaXNjbzEIMEBG A1UECMMChnV0c3RvcmFhZTESWBAGA1UEAxMJQXBhcm5hIENEMFwbQyJKoZIhvch AQEBBQADSwAwSAJBAM/7b3+DXJPANESIHHz1uNccNW87ypgzwucSNZXCMpeRXXI OzyFAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaCBvzCBvDALBgNVHQ8F BMCAcYwDW7DVR0TBQWYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJDWFyb2xs L0FWXJUYSUMENBInNybDAwSG5GIYQZmjcVAQDAgEAMA0GCSqGSIb3DQEF BQUAADEAHv60Q+8nE399TwwHGaCv3QNIJaaQMjcN0AFcT0rEyuyt/WYGPzksF9Ea NBG7E00N66zex0E0EfG1Vs6mXp1//w==</pre>	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.

L

	Command or Action	Purpose
	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	
Step 3	exit	Exits configuration mode.
	<pre>Example: switch(config)# exit switch#</pre>	
Step 4	(Optional) show crypto ca trustpoints Example: switch# show crypto ca trustpoints	Displays the trust point CA information.
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

Creating a Trust Point CA Association, on page 10

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.

SUMMARY STEPS

- 1. configure terminal
- 2. crypto ca trustpoint name
- **3.** revocation-check {crl [none] | none}
- 4. exit
- 5. (Optional) show crypto ca trustpoints
- 6. (Optional) copy running-config startup-config

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.
	Example:	
	<pre>switch# configure terminal switch(config)#</pre>	
Step 2	crypto ca trustpoint name	Specifies a trust point CA and enters trust point
	Example:	configuration mode.
	<pre>switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#</pre>	
Step 3	revocation-check {crl [none] none}	Configures the certificate revocation checking methods.
	Example:	The default method is crl .
	<pre>switch(config-trustpoint)# revocation-check none</pre>	The Cisco NX-OS software uses the certificate revocation methods in the order that you specify.
Step 4	exit	Exits trust point configuration mode.
	Example:	
	<pre>switch(config-trustpoint)# exit switch(config)#</pre>	
Step 5	(Optional) show crypto ca trustpoints	Displays the trust point CA information.
	Example:	
	<pre>switch(config)# show crypto ca trustpoints</pre>	
Step 6	(Optional) copy running-config startup-config	Copies the running configuration to the startup
	Example:	configuration.
	switch(config)# copy running-config startup-config	Į.

Related Topics

Authenticating the CA, on page 13 Configuring a CRL, on page 22

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.

SUMMARY STEPS

- 1. configure terminal
- 2. crypto ca enroll name
- **3**. exit
- **4.** (Optional) **show crypto ca certificates**
- 5. (Optional) copy running-config startup-config

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.
	Example:	
	<pre>switch# configure terminal switch(config)#</pre>	
Step 2	crypto ca enroll name	Generates a certificate request for an authenticated CA.
	<pre>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 MIBqzCARQCAQ&wHDEaMBGAIUEAwRKMMNYMtMS5jaKNjby5jb20wgZ&MDQX. KoZIhvcNAQEBDQDgY0AMIGJACGAL8AIUJ2NC7jUJIDVaSMpNIgJZkt8rl4IkK UJCGManNy4qk8VeMZZSILJ4JgTZKWdbIDkTTysnjuCXGvjb+wj0hEhv/y51T9 P2NUJBorngAnvEzgC7ysN/PyMKGgzhbVpj+rargZvHtGJ9IXTq4MoVKSCZXV88 VqyH0vEvAqMEAAGqTZAVEgkqhkiG90BCQcxCEMGanJ2MTIzMDYGCSqCSIb3DQE.</pre>	
Step 3	<pre>DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVNYMtMS5jaXNjby5jb22HBKwMH6IwDQX. KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GIFWgr PftrNcWUE/pw6HayfQ12T3ecgNwe12d15133YBF2bktExiI6U188nT0jg1XMjja4 8a23bNDpNsM8rklwA6hWrVL8NUZEFJxcdpjfngPNTZacJCUS6ZqKCMetbKytUx0- END CERTIFICATE REQUEST exit Example: switch(config-trustpoint)# exit</pre>	
	switch(config)#	
Step 4	(Optional) show crypto ca certificates	Displays the CA certificates.
	Example:	

	Command or Action	Purpose
	<pre>switch(config)# show crypto ca certificates</pre>	
Step 5	(Optional) copy running-config startup-config	Copies the running configuration to the startup
	Example:	configuration.
	<pre>switch(config)# copy running-config startup-config</pre>	

Related Topics

Creating a Trust Point CA Association, on page 10

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.

SUMMARY STEPS

- **1**. configure terminal
- 2. crypto ca import name certificate
- 3. exit
- 4. (Optional) show crypto ca certificates
- 5. (Optional) copy running-config startup-config

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.
	Example:	
	<pre>switch# configure terminal switch(config)#</pre>	
Step 2	crypto ca import name certificate	Prompts you to cut and paste the identity certificate for the
	Example:	CA named admin-ca.
	<pre>switch(config)# crypto ca import admin-ca certificate input (cut & paste) certificate in PEM format: BEGIN CERTIFICATE MIIEADCA6qgAwIEAGIKCjOCQAAAAAADDANBgkqhkiG9w0EAQUFADCBkDEgME40 CSqGSIb3DQEJARYRYMIhImRrZUBjaXNjby5jb20xCzAJBgNWAAYTAklOMRIWEAYI VQQIEwlLYXJuYXRha2ExEjAQBgNVEAcTCUJhbmchbG9yZTEOMAwGAlUEChMFQ21z Y28xEzARBgNVEAsTCn5ldHN0b3Jh22UxEjAQBgNVEAMTCUFWYXJuYSBDQTAeFW0W NIExMTIwMzAyADBaFw0wNjExMTIWMZEyADBaMBwxGjAYBgNVEAMTEVZ1z2FzITEu Y21zY28uY29tMIGMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu410 dQUWkjKjSICdpLfk5eJSmNQujGpzcuKsZPFXjF2UoiyeCYE8yIncWyw5E08rJ47</pre>	

	Command or Action	Purpose
	glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4WlaY/q2q4Gc	
	x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw	
	GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrF	
	bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW	
	pIGIMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE	
	BhMCSU4xEjAQBgNVBAgTCUthan5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3J1MQ4w	
	DAYDVQQKEwVDaXNjbzEIMBEGA1UECxMKbnV0c3RvcmFnZTESMBAGA1UEAxMJQXBh	
	an5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6	
	Ly9zc2UtMDgvQ2VydEVuan9sbC9BcGFylanElMjBDQS5janwwMKAuoCyGKmZpbGU6	
	Ly9cXHNzZS0w0FxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH	
	AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4LONlcnRFbnJvbGwvc3Nl	
	LTA4X0FwYXJuYSUyMENBImNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3N1LTA4	
	XEN1cnRFbnJvbGxcc3N1LTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF	
	AANBADbGBGsbe7GNLh9xe0TWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw	
	E36cIZu4WsExREqxbTk8ycx7V5o=	
	END CERTIFICATE	
Step 3	exit	Exits configuration mode.
	Example:	
	switch(config)# exit	
	switch#	
Step 4	(Optional) show crypto ca certificates	Displays the CA certificates.
	Example:	
	· · ·	
	switch# show crypto ca certificates	
Step 5	(Optional) copy running-config startup-config	Copies the running configuration to the startup
		configuration.
	Example:	• onin Bur wron.
	Example:	

Related Topics

Creating a Trust Point CA Association, on page 10

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.

Ø

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 20

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.

SUMMARY STEPS

- **1**. configure terminal
- 2. crypto ca export name pkcs12 bootflash:filename password
- 3. exit
- 4. copy booflash:filename scheme://server/ [url /]filename

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.
	Example:	
	<pre>switch# configure terminal switch(config)#</pre>	
Step 2	crypto ca export name pkcs12 bootflash:filename password	Exports the identity certificate and associated key pair and CA certificates for a trust point CA. The password is alphanumeric, case sensitive, and has a maximum length of 128 characters.
	Example:	
	<pre>switch(config)# crypto ca export admin-ca pkcs12 bootflash:adminid.p12 nbv123</pre>	
Step 3	exit	Exits configuration mode.
	Example:	
	<pre>switch(config)# exit switch#</pre>	

	Command or Action	Purpose
Step 4	copy booflash:filename scheme://server/ [url /]filename	Copies the PKCS#12 format file to a remote server.
	Example: switch# copy bootflash:adminid.p12 tftp:adminid.p12	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 13 Installing Identity Certificates, on page 18

Importing Identity Information in PKCS 12 or PKCS 7 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.

Ò

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.

SUMMARY STEPS

- 1. copy scheme:// server/[url /]filename bootflash:filename
- **2**. configure terminal
- 3. crypto ca import name [pksc12 | pkcs7] bootflash:filename
- 4. exit
- 5. (Optional) show crypto ca certificates
- 6. (Optional) copy running-config startup-config

	Command or Action	Purpose
Step 1	<pre>copy scheme:// server/[url /]filename bootflash:filename</pre>	Copies the PKCS#12 format file from the remote server.
	Example: switch# copy tftp:adminid.p12 bootflash:adminid.p12	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.

	Command or Action	Purpose
Step 2	configure terminal	Enters global configuration mode.
	Example:	
	<pre>switch# configure terminal switch(config)#</pre>	
Step 3	crypto ca import <i>name</i> [pksc12 pkcs7] bootflash: <i>filename</i>	Imports the identity certificate and associated key pair and CA certificates for trust point CA.
	Example:	
	<pre>switch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123</pre>	
Step 4	exit	Exits configuration mode.
	Example:	
	<pre>switch(config)# exit switch#</pre>	
Step 5	(Optional) show crypto ca certificates	Displays the CA certificates.
	Example:	
	switch# show crypto ca certificates	
Step 6	(Optional) copy running-config startup-config	Copies the running configuration to the startup
	Example:	configuration.
	switch# copy running-config startup-config	

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.

SUMMARY STEPS

- 1. copy scheme:[//server/[url /]]filename bootflash:filename
- 2. configure terminal
- 3. crypto ca crl request name bootflash:filename
- 4. exit
- 5. (Optional) show crypto ca crl name
- 6. (Optional) copy running-config startup-config

L

DETAILED STEPS

	Command or Action	Purpose
Step 1	copy scheme:[//server/[url /]]filename bootflash:filename	Downloads the CRL from a remote server.
	Example: switch# copy tftp:adminca.crl bootflash:adminca.crl	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 server, url, and filename arguments are case sensitive.
Step 2	configure terminal	Enters global configuration mode.
	Example:	
	<pre>switch# configure terminal switch(config)#</pre>	
Step 3	crypto ca crl request name bootflash:filename	Configures or replaces the current CRL with the one specified in the file.
	Example:	
	<pre>switch(config)# crypto ca crl request admin-ca bootflash:adminca.crl</pre>	
Step 4	exit	Exits configuration mode.
	Example:	
	<pre>switch(config)# exit switch#</pre>	
Step 5	(Optional) show crypto ca crl name	Displays the CA CRL information.
	Example:	
	switch# show crypto ca crl admin-ca	
Step 6	(Optional) copy running-config startup-config	Copies the running configuration to the startup
	Example:	configuration.
	switch# copy running-config startup-config	

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.

SUMMARY STEPS

- **1**. configure terminal
- 2. crypto ca trustpoint name
- 3. delete ca-certificate
- 4. delete certificate [force]

- 5. exit
- 6. (Optional) show crypto ca certificates [name]
- 7. (Optional) copy running-config startup-config

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.
	Example:	
	<pre>switch# configure terminal switch(config)#</pre>	
Step 2	crypto ca trustpoint name	Specifies a trust point CA and enters trust point
	Example:	configuration mode.
	<pre>switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#</pre>	
Step 3	delete ca-certificate	Deletes the CA certificate or certificate chain.
	Example:	
	<pre>switch(config-trustpoint)# delete ca-certificate</pre>	
Step 4	delete certificate [force]	Deletes the identity certificate.
	Example:	You must use the force option if the identity certificate you
	<pre>switch(config-trustpoint)# delete certificate</pre>	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	Exits trust point configuration mode.
	Example:	
	<pre>switch(config-trustpoint)# exit switch(config)#</pre>	
Step 6	(Optional) show crypto ca certificates [name]	Displays the CA certificate information.
	Example:	
	<pre>switch(config)# show crypto ca certificates admin-ca</pre>	
Step 7	(Optional) copy running-config startup-config	Copies the running configuration to the startup
	Example:	configuration.
	switch(config)# copy running-config startup-config	χ.

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.

SUMMARY STEPS

- 1. configure terminal
- 2. crypto key zeroize rsa label
- 3. exit
- 4. (Optional) show crypto key mypubkey rsa
- 5. (Optional) copy running-config startup-config

DETAILED STEPS

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

Related Topics

Generating Certificate Requests, on page 16

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.
show crypto ca certificates	Displays information about CA and identity certificates.
show crypto ca crl	Displays information about CA CRLs.
show crypto ca trustpoints	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.

8

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:

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.

Note

```
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----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRI1jK0ZejANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAk10
MRIwEAYDVQQIEw1LYXJuYXRha2ExEjAQBqNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ21zY28xEzARBqNVBAsTCm51dHN0b3JhZ2UxEjAQBqNVBAMTCUFwYXJuYSBD
{\tt QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN}
AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJOmFuZ2Fsb3J1MO4wDAYDVOOKEwVDaXNibzETMBEG
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGOwYjAuoCvgKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5vb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0E0EfG1Vs6mXp1//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----MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ KoZIhvcNAQEBBQADqY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIqJ2kt8r141KY 0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8 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-----

MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAk1OMRIwEAYD VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ21z Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZ1Z2FzLTEu Y21zY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47 glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR00BBYEFKCLi+2sspWEfgrR bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE ${\tt BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3J1MQ4w}$ DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh cm5h1ENBqhAFYNKJrLQZ1E9JEiWMrR16MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6 Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmE1MjBDQS5jcmwwMKAuoCyGKmZpbGU6 Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3N1LTA4L0N1cnRFbnJvbGwvc3N1 LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3N1LTA4 XEN1cnRFbnJvbGxcc3N1LTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF 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 29 Requesting an Identity Certificate, on page 32

Downloading a CA Certificate

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

Step 1 From the Microsoft Certificate Services web interface, click Retrieve the CA certificate or certificate revocation task

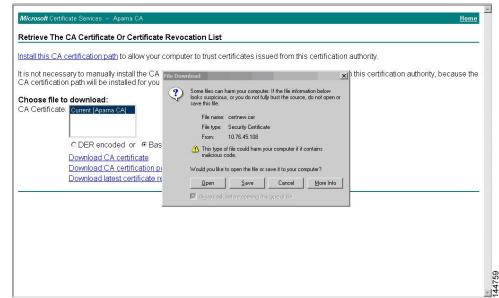
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure prog will be able to securely identify yourself to other people over the web, sign your e-mail messages, enc depending upon the type of certificate you request.	ram. Once you acquire a certificate, you rypt your e-mail messages, and more
Select a task:	
Retrieve the CA certificate or certificate revocation list	
Request a certificate	
Check on a pending certificate	
	Next >

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**.

istall this CA c	ertification path to allow your computer to trust certificates issued from this certification authority.
	ary to manually install the CA certification path if you request and install a certificate from this certification authority, because the path will be installed for you automatically.
hoose file to A Certificate:	download: Current (Apama CA)
	© DER encoded or ⊕ Base 64 encoded Download CA certificate
	Download CA certification path Download LA certificate revocation list

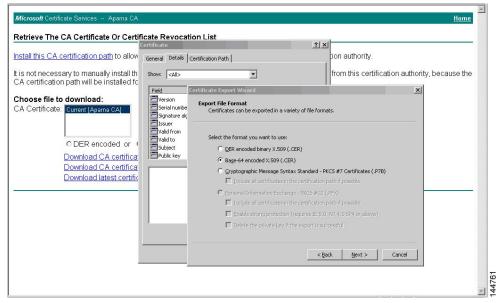
Step 3 Click **Open** in the File Download dialog box.



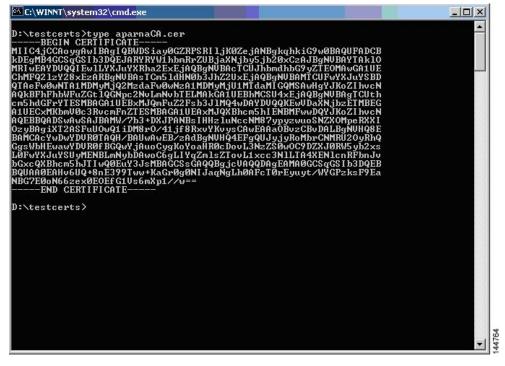
Step 4 In the Certificate dialog box, click **Copy to File** and click **OK**.

	Certificate		? ×	
<u>tall this CA certification path</u> to allow	General Details Certification	Path	tion a	uthority.
s not necessary to manually install th A certification path will be installed fc	Show: <all></all>	Value	from	this certification authority, because th
Noose file to download: A Certificate: C DER encoded or Download CA certificat Download latest certificat Download latest certificat	retor Version Serial number Signature algorithm Suser Valid to Subject Public key	Value V3 0560 D289 ACEH 1994 4F49 1 sha1RSA Apara CA, netstorage, Cisco 04 Mei 2005 4156137 04 Mei 2007 425117 Apara CA, netstorage, Cisco RSA (S12 Bits)	× 	

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

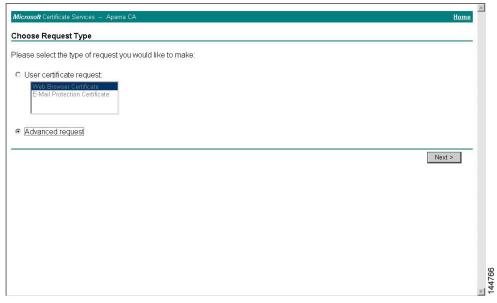
To request an identify certificate from a Microsoft Certificate server using a PKCS#12 certificate signing request (CRS), follow these steps:

Step 1

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

/elcome	
	our web browser, e-mail client, or other secure program. Once you acquire a certificate, you eople over the web, sign your e-mail messages, encrypt your e-mail messages, and more t.
elect a task:	
C Retrieve the CA certificate or certificate reve	ocation list
Request a certificate	
C Check on a pending certificate	
	Next >

Step 2 Click Advanced request and click Next.



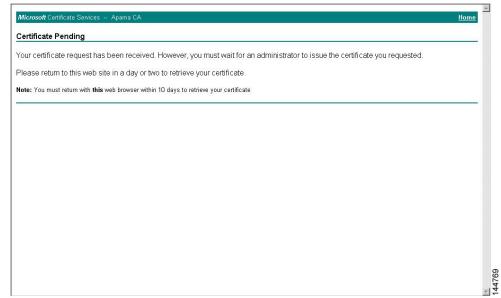
Step 3 Click Submit a certificate request using a base64 encoded PKCS#10 file or a renewal request using a base64 encoded PKCS#7 file and click Next.

ficrosoft Certificate Services Aparna CA	<u>Home</u>
dvanced Certificate Requests	
ou can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the rtification authority (CA) will determine the certificates that you can obtain.	
Submit a certificate request to this CA using a form.	
Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file	e.
Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station. You must have an enrollment agent certificate to submit a request for another user.	
N	lext >

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.

ubmit A Save	d Request	_
	encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web equest field to submit the request to the certification authority (CA).	
aved Request:		
Base64 Encoded Certificate Request (PKCS #10 or #7):	VqyHOVEVAgHEAAGTEANEGKebk1GSWDBCCexCBMG DjEpHCcwJQYDVRORACH/BBswGYIRVmVnYXHtHS5j KoZlhvcNAGEEBGALgYEAATGOKEB6GG6njOsDXXVH PftrNeUUE/pw6Hayf0laT3ecgNwel2d15133YBF2; 8a23bND9HaBKrlw46AhtwrUsUBUZEFAky0jfngPN END CERTIFICATE REQUEST • e	
dditional Attribut		
Attributes:		
	Submit >	

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



Step 6

6 Note that the CA administrator approves the certificate request.

🗃 Certification Authority							- 0 ×
Action View		3					
Tree	Request ID	Binary Request	Request Disposition Message	Request Subm	ission Date	Requester Name	Reque
Jortfication Authority (Local) Aparna CA Revoled Certificates Panding Requests Pailed Requests Failed Requests	116	BEGIN NE	Taken Under Submission	I (1 2/2005 s: All Tasks ► Refresh Help		SSE-00\IUSR_SS	
							▶

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

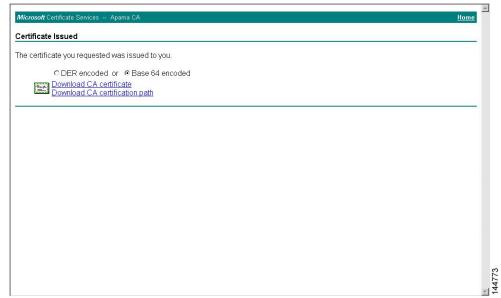
Welcome	
Vercome	_
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, , will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.	you e
Select a task:	
C Retrieve the CA certificate or certificate revocation list	
C Request a certificate	
Check on a pending certificate	
	-
Next >	

Step 8

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

Microsoft Certificate Services Aparna CA	ome	*
Check On A Pending Certificate Request		
Please select the certificate request you want to check: Saved-Request Certificate (12 Nopember 2005 20:30:22)		
Next >	ſ	
		2
		144772

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



Step 10

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

Microsoft Certificate Services Aparna CA		Home
Certificate Issued		
The certificate you requested was issued to		
C DER encoded or C Base 6		
Download CA certificate Download CA certification path	Some files can harm your computer If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.	
	File name: certnew.cer	
	File type: Security Certificate	
	From: 10.76.45.108	
	A This type of file could harm your computer if it contains malicious code.	
	Would you like to open the file or save it to your computer?	
	Open Save Cancel More Info	
	Always ask before opening this type of file	
	 Novaka azv. netnie nheturiä ruis öhe nuue. 	
		•

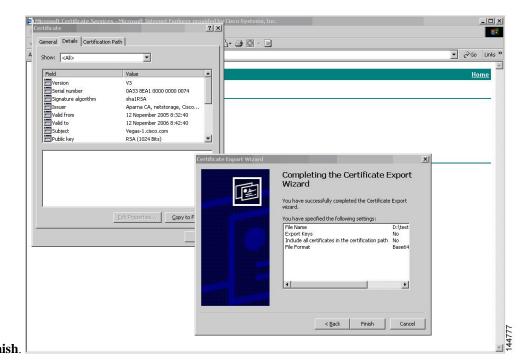
Step 11In the Certificate box, click Details tab and click Copy to File.... In the Certificate Export Dialog box, click Base-64
encoded X.509 (.CER), and click Next.

neral Details Certification	n Path	} 	
ow: <al></al>	•		💌 🤗 Go Link
Field	Value		Home
Version	V3		
Serial number	0A33 8EA1 0000 0000 0074 sha1RSA		
Signature algorithm Issuer	Aparna CA, netstorage, Cisco		
Valid from	12 Nopember 2005 8:32:40		
Valid to Subject	12 Nopember 2006 8:42:40		
Subject Public key	Vegas-1.cisco.com RSA (1024 Bits)	•	
-	,	Certificate Export Wizard	
		Certificates can be exported in a variety of file formats.	
		Select the format you want to use:	
		C DER encoded binary X.509 (.CER)	
	Edit Properties Copy to File	 Base-64 encoded X.509 (.CER) 	
		C gryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
	0	Include all certificates in the certification path if possible	
		Personal Information Exchange - PKC5 #12 (.PFX)	
		Indude all certificates in the certification path if possible	
		Enable strong protection (requires IE 5,0, NT 4.0 SP4 or above)	
		Delete the private key if the export is successful	
		< Back Next > Cancel	

Step 12

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

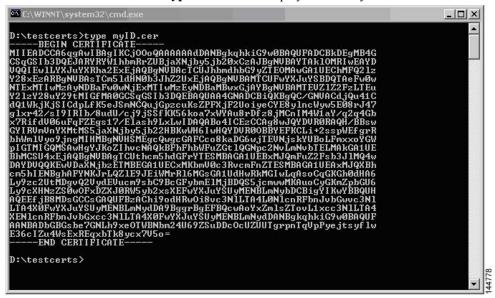
Microsoft Certificate Services - Microsoft Internet Explorer provided by Clisco Systems, Inc.	
Certificate ?X	11 A
🕻 General Details Certification Path	
A Show: <al></al>	▼ 🖉 Go Links ≫
Field Value	Home
Version V3	
Serial number 0A33 8EA1 0000 0000 0074	
Signature algorithm sha1RSA Issuer Aparna CA, netstorage, Cisco	
Valid from 12 Nopember 2005 8:32:40	
Valid to 12 Nopember 2006 8:42:40	
Subject Vegas-1. disco.com Public key RSA (1024 Bits)	
Public key RSA (1024 Bits)	
Certificate Export Wizard	×
File to Export	
Specify the name of the file you want to export	
Ele name:	
Edit Properties Copy to F D:\testcerts\myID.cer Browse	
< <u>Back</u> Next > Ca	ncel
	p
	144776
	4



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 16 Configuring Certificates on a Cisco NX-OS Device, on page 26

Revoking a Certificate

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

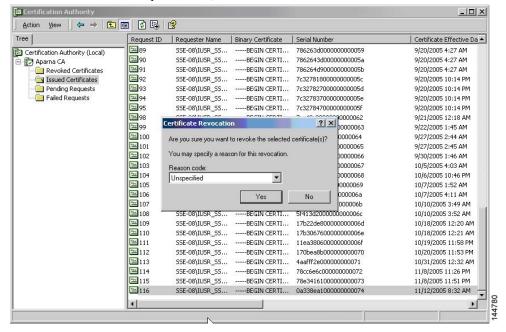
L

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.

ree	Request ID	Requester Name	Binary Certificate	Serial Number	Certificate Effective Da 🔺
Certification Authority (Local)	- 289	SSE-08\IUSR_SS	BEGIN CERTI	786263d000000000059	9/20/2005 4:27 AM
😰 Aparna CA	90	SSE-08\IUSR_SS	BEGIN CERTI	7862643d0000000005a	9/20/2005 4:27 AM
Revoked Certificates	91	SSE-08\IUSR_SS	BEGIN CERTI	786264d90000000005b	9/20/2005 4:27 AM
- 🔄 Issued Certificates	92	SSE-08\IUSR_SS	BEGIN CERTI	7c3278180000000005c	9/20/2005 10:14 PM
Pending Requests	93	SSE-08\IUSR_SS	BEGIN CERTI	7c3278270000000005d	9/20/2005 10:14 PM
	94	SSE-08\IUSR_SS	BEGIN CERTI	7c3278370000000005e	9/20/2005 10:14 PM
	95	SSE-08\IUSR_SS	BEGIN CERTI	7c3278470000000005f	9/20/2005 10:14 PM
	98	SSE-08\IUSR_SS	BEGIN CERTI	7ca48c2200000000062	9/21/2005 12:18 AM
	99	SSE-08\IUSR_SS	BEGIN CERTI	021a9d1a00000000063	9/22/2005 1:45 AM
	100	SSE-08\IUSR_SS	BEGIN CERTI	1c1013cf00000000064	9/27/2005 2:44 AM
	101	SSE-08\IUSR_SS	BEGIN CERTI	1c10d19100000000065	9/27/2005 2:45 AM
	102	SSE-08\IUSR_SS	BEGIN CERTI	2b4eb36700000000066	9/30/2005 1:46 AM
	103	SSE-08\IUSR_SS	BEGIN CERTI	458b6b4300000000067	10/5/2005 4:03 AM
	104	SSE-08\IUSR_SS	BEGIN CERTI	4eb5b32700000000068	10/6/2005 10:46 PM
	105	SSE-08\IUSR_SS	BEGIN CERTI	4f60084100000000069	10/7/2005 1:52 AM
	106	SSE-08\IUSR_SS	BEGIN CERTI	4fdf95640000000006a	10/7/2005 4:11 AM
	107	SSE-08\IUSR_SS	BEGIN CERTI	5f3e8c960000000006b	10/10/2005 3:49 AM
	108	SSE-08\IUSR_SS	BEGIN CERTI	5f413d200000000006c	10/10/2005 3:52 AM
	109	SSE-08\IUSR_SS	BEGIN CERTI	17b22de80000000006d	10/18/2005 12:20 AM
	110	SSE-08\IUSR_SS	BEGIN CERTI	17b306760000000006e	10/18/2005 12:21 AM
	111	SSE-08\IUSR_SS	BEGIN CERTI	11ea38060000000006f	10/19/2005 11:58 PM
	112	SSE-08\IUSR_SS	BEGIN CERTI	170bea8b00000000070	10/20/2005 11:53 PM
	113	SSE-08\IUSR_SS	BEGIN CERTI	4aafff2e00000000071	10/31/2005 12:32 AM
	114	SSE-08\IUSR_SS	BEGIN CERTI	78cc6e6c00000000072	11/8/2005 11:26 PM
	115	SSE-08\IUSR_SS	BEGIN CERTI	78e3416100000000073	11/8/2005 11:51 PM
	116	SSE-08\ILISP_SS	BEGIN CERTI	0a338ea100000000074	11/12/2005 8:32 AM
	4	Open			

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



Certification Authority (Local) Ig 15 SSE-08(LUSR_SS BEGIN CERTI 5dae53cd0000000000 6/30/2005 3:27 AM Image: Start Contributes Image: Start Contributes	ree	Request ID	Requester Name	Binary Certificate	Serial Number	Certificate Effective Date	
Aparna CA SEE-06{IUSR_SS BEGIN CERTI Sdd1/dd300000000010 6/30/2005 3:30 AM Issued Certificates Is 15 SSE-06{IUSR_SS BEGIN CERTI Sdd1/dd3000000000012 7/8/2005 3:21 AM Pending Requests Is 19 SSE-06{IUSR_SS BEGIN CERTI 261392400000000014 7/14/2005 5:20 AM Issued Certificates Is 19 SSE-06{IUSR_SS BEGIN CERTI 261392400000000014 7/14/2005 5:20 AM Is 22 SSE-06{IUSR_SS BEGIN CERTI 2645202000000000016 7/14/2005 5:26 AM Is 22 SSE-06{IUSR_SS BEGIN CERTI 2634572000000000017 7/14/2005 5:26 AM Is 22 SSE-06{IUSR_SS BEGIN CERTI 264504000000000017 7/14/2005 5:26 AM Is 22 SSE-06{IUSR_SS BEGIN CERTI 264504000000000017 7/14/2005 1:27 AM Is 22 SSE-06{IUSR_SS BEGIN CERTI 264504000000000017 7/14/2005 1:27 AM Is 22 SSE-06{IUSR_SS BEGIN CERTI 264504000000000017 7/14/2005 1:27 AM Is 22 SSE-06{IUSR_SS BEGI	Certification Authority (Local)	15	SSE-08\IUSR_SS	BEGIN CERTI	5dae53cd00000000000	6/30/2005 3:27 AM	
Revolucid Certificates G17 SSE-06(LUSR_SS BEGIN CERTI 52:247:1b00000000011 6/30/2005 5:46 AM Pending Requests G19 SSE-06(LUSR_SS BEGIN CERTI 16:4d+f600000000012 7/14/2005 5:00 AM Pending Requests G20 SSE-06(LUSR_SS BEGIN CERTI 26:10:324000000000013 7/14/2005 5:27 AM G21 SSE-06(LUSR_SS BEGIN CERTI 26:352000000000016 7/14/2005 5:27 AM G22 SSE-06(LUSR_SS BEGIN CERTI 26:350000000000016 7/14/2005 5:27 AM G22 SSE-06(LUSR_SS BEGIN CERTI 26:350000000000017 7/14/2005 5:27 AM G22 SSE-06(LUSR_SS BEGIN CERTI 26:350000000000017 7/14/2005 5:28 AM G22 SSE-06(LUSR_SS BEGIN CERTI 26:450000000000017 7/14/2005 5:28 AM G22 SSE-06(LUSR_SS BEGIN CERTI 26:45000000000018 7/14/2005 5:26 AM G22 SSE-06(LUSR_SS		16	SSE-08\JUSR_SS	BEGIN CERTI	5db140d3000000000010	6/30/2005 3:30 AM	
Pending Requests IB 19 SSE-08[USR_SS BEGIN CERTI 261C392400000000013 7/14/2005 5::00 AM Pailed Requests IB 20 SSE-08[USR_SS BEGIN CERTI 263L520200000000014 7/14/2005 5::16 AM IB 21 SSE-08[USR_SS		17	SSE-08\IUSR_SS	BEGIN CERTI	5e2d7c1b00000000011	6/30/2005 5:46 AM	
Failed Requests SE-08[USR_5S BEGIN CERTI 262b520200000000014 7/14/2005 5:16 AM C21 SSE-08[USR_SS	Issued Certificates	18	SSE-08\IUSR_SS	BEGIN CERTI	16db4f8f00000000012	7/8/2005 3:21 AM	
Image: Sec. 08[USR_5S	Pending Requests	19	SSE-08\JUSR_SS	BEGIN CERTI	261c392400000000013	7/14/2005 5:00 AM	
Image: 22 SSE-08[USR_SS BEGIN CERTI 2635b0000000000016 7/14/2005 5:28 AM Image: 23 SSE-08[USR_SS		20	SSE-08\IUSR_SS	BEGIN CERTI	262b520200000000014	7/14/2005 5:16 AM	
Image: 23 SSE-08[LUSR_SS BEGIN CERTI 2648504000000000017 7/14/2005 5:48 AM Image: 24 SSE-08[LUSR_SS		21	SSE-08\IUSR_SS	BEGIN CERTI	2634c7f200000000015	7/14/2005 5:27 AM	
Image: Constraint of the second constraint of th		22	SSE-08\IUSR_SS	BEGIN CERTI	2635b00000000000016	7/14/2005 5:28 AM	
Image: Sec: 08(LUSR_SS BEGIN CERTI 3f88cbf700000000019 7/19/2005 3:29 AM Image: Sec: 08(LUSR_SS BEGIN CERTI 3f88cbf700000000014 7/28/2005 3:86 AM Image: Sec: 08(LUSR_SS BEGIN CERTI 725b893600000000014 7/28/2005 3:86 AM Image: Sec: 08(LUSR_SS		23	SSE-08\IUSR_SS	BEGIN CERTI	2648504000000000017	7/14/2005 5:48 AM	
Image: Sec: 08(LUSR_SS		24	SSE-08\IUSR_SS	BEGIN CERTI	2a27635700000000018	7/14/2005 11:51 PM	
Image: 27 SSE-08[USR_SS BEGIN CERTI 725b89d800000000001b 7/28/2005 10:54 PM Image: 28 SSE-08[USR_SS		25	SSE-08\IUSR_SS	BEGIN CERTI	3f88cbf700000000019	7/19/2005 3:29 AM	
Image: Sec: 08(1USR_5S BEGIN CERTI 735a887800000000001c 7/29/2005 3:33 AM Image: Sec: 08(1USR_5S BEGIN CERTI 148511700000000001d 8/3/2005 11:30 PM Image: Sec: 08(1USR_5S BEGIN CERTI 148511700000000001d 8/3/2005 11:30 PM Image: Sec: 08(1USR_5S BEGIN CERTI 1497170100000000001e 8/3/2005 11:30 PM Image: Sec: 08(1USR_5S BEGIN CERTI 1467(455000000000001e) 8/3/2005 11:40 AM Image: Sec: 08(1USR_5S BEGIN CERTI 486ce80b0000000001e 8/1/2005 11:37 PM Image: Sec: 08(1USR_5S BEGIN CERTI 1467(45508000000000021 8/17/2005 11:37 PM Image: Sec: 08(1USR_5S BEGIN CERTI 1485568000000000000012 9/17/2005 11:37 PM Image: Sec: 08(1USR_5S BEGIN CERTI 360453d000000000002f 9/17/2005 11:37 PM Image: Sec: 08(1USR_5S BEGIN CERTI 360453d000000000002f 9/17/2005 11:37 PM Image: Sec: 08(1USR_5S BEGIN CERTI 360453d000000000002f 9/17/2005 11:37 PM Image: Sec: 08(1USR_5S BEGIN CERTI 3604563d0000000000002f <th< td=""><td></td><td>26</td><td>SSE-08\IUSR_SS</td><td>BEGIN CERTI</td><td>6e4b5f5f0000000001a</td><td>7/28/2005 3:58 AM</td><td></td></th<>		26	SSE-08\IUSR_SS	BEGIN CERTI	6e4b5f5f0000000001a	7/28/2005 3:58 AM	
Image: Sec-08[USR_5S BEGIN CERTI 148511c700000000001d 8/3/2005 11:30 PM Image: Sec-08[USR_5S BEGIN CERTI 147645550000000001e 8/4/2005 11:00 AM Image: Sec-08[USR_SS BEGIN CERTI 147c4555000000000001e 8/4/2005 11:00 AM Image: Sec-08[USR_SS BEGIN CERTI 147c455500000000000000 8/17/2005 31:58 AM Image: Sec-08[USR_SS BEGIN CERTI 466ce80000000000021 8/17/2005 11:37 PM Image: Sec-08[USR_SS BEGIN CERTI 466ce80000000000021 8/17/2005 11:37 PM Image: Sec-08[USR_SS BEGIN CERTI 14855ce80000000000021 8/17/2005 11:37 PM Image: Sec-08[USR_SS		27	SSE-08\IUSR_SS	BEGIN CERTI	725b89d80000000001b	7/28/2005 10:54 PM	
Image: Sec: 08(1USR_5S BEGIN CERTI 14a717010000000001e 8/4/2005 12:07 AM Image: Sec: 08(1USR_5S BEGIN CERTI 14rc45b500000000001f 8/4/2005 1:40 AM Image: Sec: 08(1USR_5S BEGIN CERTI 14rc45b5000000000001f 8/4/2005 1:40 AM Image: Sec: 08(1USR_5S BEGIN CERTI 14rc45b50000000000020 8/17/2005 3:85 AM Image: Sec: 08(1USR_5S BEGIN CERTI 4ca4a3aa000000000002f 9/1/2005 11:36 PM Image: Sec: 08(1USR_5S BEGIN CERTI 3465dd000000000003f 9/9/2005 11:1AM Image: Sec: 08(1USR_5S BEGIN CERTI 36145dd00000000002 9/1/2005 11:36 PM Image: Sec: 08(1USR_5S BEGIN CERTI 36145dd000000000002 9/9/2005 1:11 AM Image: Sec: 08(1USR_5S		28	SSE-08\IUSR_SS	BEGIN CERTI	735a88780000000001c	7/29/2005 3:33 AM	
Image: Size-08(IUSR_SS BEGIN CERTI 14fc4555000000000001f 8/14/2005 1:40 AM Image: Size-08(IUSR_SS BEGIN CERTI 14fc46se80b000000000002 8/17/2005 3:58 AM Image: Size-08(IUSR_SS BEGIN CERTI 46c4e30b0000000000021 8/17/2005 11:37 PM Image: Size-08(IUSR_SS BEGIN CERTI 4ca4a3aa000000000002f 9/1/2005 11:36 PM Image: Size-08(IUSR_SS		29	SSE-08\IUSR_SS	BEGIN CERTI	148511c70000000001d	8/3/2005 11:30 PM	
Image: SSE-08(LUSR_SS BEGIN CERTI 486ce80b00000000020 8/17/2005 3:58 AM Image: SSE-08(LUSR_SS BEGIN CERTI 486ce80b0000000001 8/17/2005 3:58 AM Image: SSE-08(LUSR_SS BEGIN CERTI 1aa55c8e000000000021 8/17/2005 11:37 PM Image: SSE-08(LUSR_SS BEGIN CERTI 1aa55c8e000000000026 9/1/2005 11:37 PM Image: SSE-08(LUSR_SS BEGIN CERTI 3f0845d0000000000005 9/9/2005 11:11 AM Image: SSE-08(LUSR_SS BEGIN CERTI 3f619b7e000000000042 9/9/2005 1:09 AM Image: SSE-08(LUSR_SS BEGIN CERTI 3f34-650000000000052 9/16/2005 1:09 AM Image: SSE-08(LUSR_SS BEGIN CERTI 7c3861e30000000000052 9/16/2005 1:09 AM Image: SSE-08(LUSR_SS BEGIN CERTI 7c3861e3000000000000000000000000000000000000		30	SSE-08\IUSR_SS	BEGIN CERTI	14a7170100000000001e	8/4/2005 12:07 AM	
Image: Signed State SSE-08[USR_5S BEGIN CERTI 4ca4a3aa000000000021 8/17/2005 11:37 PM Image: Signed State SSE-08[USR_5S BEGIN CERTI 3f0845d00000000002f 9/1/2005 11:36 PM Image: Signed State SSE-08[USR_5S BEGIN CERTI 3f0845d00000000002f 9/9/2005 11:11 AM Image: Signed State SSE-08[USR_5S BEGIN CERTI 3f0845d00000000002f 9/9/2005 11:90 AM Image: Signed State SSE-08[USR_5S BEGIN CERTI 3f0845d000000000052 9/16/2005 11:90 AM Image: Signed State SSE-08[USR_5S BEGIN CERTI 7c3861:8000000000006 9/20/2005 10:20 PM Image: Signed State SSE-08[USR_5S BEGIN CERTI 7c6es5100000000006 9/20/2005 11:20 PM		31	SSE-08\IUSR_SS	BEGIN CERTI	14fc45b50000000001f	8/4/2005 1:40 AM	
Image: SEC-08[USR_SS BEGIN CERTI 1aa55c8e00000000002f 9/1/2005 11:36 PM Image: SEC-08[USR_SS		32	SSE-08\IUSR_SS	BEGIN CERTI	486ce80b00000000020	8/17/2005 3:58 AM	
Image: SSE-08[IUSR_SS BEGIN CERTI 3f0845dd00000000003f 9/9/2005 1:11 AM Image: SSE-08[IUSR_SS BEGIN CERTI 3f019b7e000000000042 9/9/2005 1:09 AM Image: SSE-08[IUSR_SS BEGIN CERTI 3f019b7e0000000000052 9/16/2005 1:09 AM Image: SSE-08[IUSR_SS BEGIN CERTI 7c3861e30000000000052 9/16/2005 1:09 AM Image: SSE-08[IUSR_SS BEGIN CERTI 7c3861e3000000000000 9/20/2005 10:20 PM Image: SSE-08[IUSR_SS BEGIN CERTI 7c3861e3000000000061 9/20/2005 11:20 PM		33	SSE-08\IUSR_SS	BEGIN CERTI	4ca4a3aa000000000021	8/17/2005 11:37 PM	
Image: SE-08(IUSR_SS BEGIN CERTI 3f619b7e00000000042 9/9/2005 2:48 AM Image: SE-08(IUSR_SS BEGIN CERTI 3f619b7e000000000052 9/16/2005 1:09 AM Image: SE-08(IUSR_SS BEGIN CERTI 7c3861e300000000000052 9/20/2005 10:20 PM Image: SE-08(IUSR_SS BEGIN CERTI 7c3861e3000000000060 9/20/2005 10:20 PM Image: SE-08(IUSR_SS BEGIN CERTI 7c6ee35100000000061 9/20/2005 11:20 PM		47	SSE-08\IUSR_SS	BEGIN CERTI	1aa55c8e00000000002f	9/1/2005 11:36 PM	
Image: sse-o8lusr_ss BEGIN CERTI 6313c46300000000052 9/16/2005 1:09 AM Image: sse-o8lusr_ss BEGIN CERTI 7c3861e300000000060 9/20/2005 10:20 PM Image: sse-o8lusr_ss BEGIN CERTI 7c3861e300000000060 9/20/2005 10:20 PM Image: sse-o8lusr_ss BEGIN CERTI 7c6ee35100000000061 9/20/2005 11:20 PM		63	SSE-08\IUSR_SS	BEGIN CERTI	3f0845dd0000000003f	9/9/2005 1:11 AM	
Image: sse-o8ltUSR_ss BEGIN CERTI 7c3861e300000000060 9/20/2005 10:20 PM Image: sse-o8ltUSR_ss BEGIN CERTI 7c6ee35100000000061 9/20/2005 11:20 PM		1	SSE-08\IUSR_SS	BEGIN CERTI	3f619b7e00000000042	9/9/2005 2:48 AM	
7 SSE-08\IUSR_SSBEGIN CERTI 7c6ee35100000000061 9/20/2005 11:20 PM		82	SSE-08\IUSR_SS	BEGIN CERTI	6313c46300000000052	9/16/2005 1:09 AM	
		1 96	SSE-08\IUSR_SS	BEGIN CERTI	7c3861e3000000000060	9/20/2005 10:20 PM	
🔀 116 SSE-08\IUSR_55BEGIN CERTI 0a338ea100000000074 11/12/2005 8:32 AM		97	SSE-08\IUSR_SS	BEGIN CERTI	7c6ee35100000000061	9/20/2005 11:20 PM	
		116	SSE-08\IUSR_SS	BEGIN CERTI	0a338ea1000000000074	11/12/2005 8:32 AM	

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:

Step 1

ction <u>V</u> iew	(= =) 🔁	📧 🚰 🔂 🗄	3 😫				
All Tasks	Publish	Request ID	Requester Name	Binary Certificate	Serial Number	Certificate Effective Date	
Refresh	ty (Local)	- 👿 15	SSE-08\IUSR_SS	BEGIN CERTI	5dae53cd00000000000	6/30/2005 3:27 AM	
Export List	(Local)	16	SSE-08\IUSR_SS	BEGIN CERTI	5db140d3000000000010	6/30/2005 3:30 AM	
	rtificates	17	SSE-08\IUSR_SS	BEGIN CERTI	5e2d7c1b00000000011	6/30/2005 5:46 AM	
Properties	ficates	18	SSE-08\IUSR_SS	BEGIN CERTI	16db4f8f00000000012	7/8/2005 3:21 AM	
Help	quests	19	SSE-08\IUSR_SS	BEGIN CERTI	261c392400000000013	7/14/2005 5:00 AM	
– напес ке	quests	20	SSE-08\IUSR_SS	BEGIN CERTI	262b520200000000014	7/14/2005 5:16 AM	
		21	SSE-08\IUSR_SS	BEGIN CERTI	2634c7f200000000015	7/14/2005 5:27 AM	
		22	SSE-08\IUSR_SS	BEGIN CERTI	2635b00000000000016	7/14/2005 5:28 AM	
		23	SSE-08\IUSR_SS	BEGIN CERTI	2648504000000000017	7/14/2005 5:48 AM	
		24	SSE-08\IUSR_SS	BEGIN CERTI	2a27635700000000018	7/14/2005 11:51 PM	
		25	SSE-08\IUSR_SS	BEGIN CERTI	3f88cbf700000000019	7/19/2005 3:29 AM	
		26	SSE-08\IUSR_SS	BEGIN CERTI	6e4b5f5f0000000001a	7/28/2005 3:58 AM	
		27	SSE-08\IUSR_SS	BEGIN CERTI	725b89d80000000001b	7/28/2005 10:54 PM	
		28	SSE-08\IUSR_SS	BEGIN CERTI	735a88780000000001c	7/29/2005 3:33 AM	
		29	SSE-08\IUSR_SS	BEGIN CERTI	148511c70000000001d	8/3/2005 11:30 PM	
		30	SSE-08\IUSR_SS	BEGIN CERTI	14a717010000000001e	8/4/2005 12:07 AM	
		31	SSE-08\IUSR_SS	BEGIN CERTI	14fc45b50000000001f	8/4/2005 1:40 AM	
		32	SSE-08\IUSR_SS	BEGIN CERTI	486ce80b00000000020	8/17/2005 3:58 AM	
		33	SSE-08\IUSR_SS	BEGIN CERTI	4ca4a3aa000000000021	8/17/2005 11:37 PM	
		47	SSE-08\IUSR_SS	BEGIN CERTI	1aa55c8e0000000002f	9/1/2005 11:36 PM	
		63	SSE-08\IUSR_SS	BEGIN CERTI	3f0845dd0000000003f	9/9/2005 1:11 AM	
		66	SSE-08\IUSR_SS	BEGIN CERTI	3f619b7e00000000042	9/9/2005 2:48 AM	
		82	SSE-08\IUSR_SS	BEGIN CERTI	6313c46300000000052	9/16/2005 1:09 AM	
		96	SSE-08\IUSR_SS	BEGIN CERTI	7c3861e300000000000	9/20/2005 10:20 PM	
		97	SSE-08\IUSR_SS	BEGIN CERTI	7c6ee351000000000061	9/20/2005 11:20 PM	
		116	SSE-08\IUSR_SS	BEGIN CERTI	0a338ea1000000000074	11/12/2005 8:32 AM	-
		•		1		•	Ē

Tree	Request ID	Requester Name Binary Certificate	Serial Number	Certificate Effective Da
Certification Authority (Local)	15	SSE-08\IUSR_SSBEGIN CERTI	. 5dae53cd00000000000	6/30/2005 3:27 AM
Aparna CA	16	SSE-08\IUSR_SSBEGIN CERTI	. 5db140d3000000000010	6/30/2005 3:30 AM
Revoked Certificates	17	SSE-08\IUSR_SSBEGIN CERTI	. 5e2d7c1b00000000011	6/30/2005 5:46 AM
	18	SSE-08\IUSR_SSBEGIN CERTI	. 16db4f8f00000000012	7/8/2005 3:21 AM
Pending Requests	19	SSE-08\IUSR_SSBEGIN CERTI	. 261c392400000000013	7/14/2005 5:00 AM
	20	SSE-08\IUSR_SSBEGIN CERTI	. 262b52020000000014	7/14/2005 5:16 AM
	21	SSE-08\IUSR_SSBEGIN CERTI	. 2634c7f200000000015	7/14/2005 5:27 AM
	22	SSE-08\IUSR_SSBEGIN CERTI	. 2635b0000000000016	7/14/2005 5:28 AM
	23	SSE-08\IUSR_SSBEGIN CERTI	. 2648504000000000017	7/14/2005 5:48 AM
0	Revocation Li The last publishe	st ed CRL is still valid and can be used by clients.	Are you sure you want to publish a	2005 10:54 PM
0	The last publishe	ed CRL is still valid and can be used by clients.		2005 3:29 AM 2005 3:58 AM 2005 3:58 AM 2005 10:54 PM 2005 3:33 AM 005 11:30 PM 005 12:07 AM
0	The last publishe	ed CRL is still valid and can be used by clients. Yes No SSE-08\JUSR_SSBEGIN CERTI.		2005 3:29 AM 2005 3:58 AM 2005 10:54 PM 2005 10:54 PM 2005 11:30 PM 005 11:30 PM 005 11:40 AM
0	The last publishe	d CRL is still valid and can be used by clients. Yes No SSE-08\1USR_SSBEGIN CERTI SSE-08\1USR_SSBEGIN CERTI.	14fc45b500000000001f 486ce80b000000000020	2005 3:29 AM 2005 3:58 AM 2005 10:54 PM 2005 10:54 PM 2005 11:30 PM 005 11:30 PM 005 11:30 PM 005 11:07 AM 8/4/2005 1:40 AM
A	The last publishe	vd CRL is still valid and can be used by clients. Yes No SSE-08\[USR_SS BEGIN CERTI SSE-08\[USR_SS	. 14fc45b500000000001f . 486ce80b00000000020 . 4ca4a3aa00000000021	2005 3:29 AM 2005 3:58 AM 2005 10:54 PM 2005 10:54 PM 005 11:30 PM 005 12:07 AM 8/4/2005 1:40 AM 8/17/2005 3:58 AM 8/17/2005 11:37 PM
0	The last publishe	Ves No SSE-08/IUSR_SSBEGIN CERTI. SSE-08/IUSR_SSBEGIN CERTI. SSE-08/IUSR_SSBEGIN CERTI. SSE-08/IUSR_SSBEGIN CERTI.	14fc45b500000000001f 486ce80b00000000020 4ca4a3a00000000021 1aa55c8e0000000002f	2005 3:29 AM 2005 3:58 AM 2005 10:54 PM 2005 3:33 AM 005 11:30 PM 8/4/2005 11:30 AM 8/17/2005 3:58 AM 8/17/2005 11:37 PM 9/1/2005 11:36 PM
0	The last publishe	Yes No SSE-06(JUSR_SS BEGIN CERTI SSE-08(JUSR_SS BEGIN CERTI SSE-08(JUSR_SS BEGIN CERTI SSE-08(JUSR_SS	14fc45b50000000001f 466ce80b00000000020 4ca4a3aa000000000021 1aa55c8e0000000002f 3f0845dd000000003f	2005 3:29 AM 2005 3:58 AM 2005 10:54 PM 2005 10:54 PM 2005 11:30 PM 005 11:30 PM 005 11:30 PM 8/17/2005 11:37 PM 9/1/2005 11:36 PM 9/9/2005 11:36 PM
A	The last publishe	Yes No SSE-08\IUSR_SS BEGIN CERTI SSE-08\IUSR_SS BEGIN CERTI SSE-08\IUSR_SS	. 14fc45b500000000001f 486ce80b0000000020 4ca4a3aa00000000021 1aa55c8e00000000002f 3f0845d00000000003f 3f6195re000000000042	2005 3:29 AM 2005 3:58 AM 2005 10:54 PM 2005 10:54 PM 2005 11:30 PM 005 11:30 PM 005 12:07 AM 8/17/2005 11:40 AM 8/17/2005 11:37 PM 9/1/2005 11:36 PM 9/9/2005 11:13 AM
0	The last publishe	Yes No SSE-06(JUSR_SS BEGIN CERTI SSE-08(JUSR_SS BEGIN CERTI SSE-08(JUSR_SS BEGIN CERTI SSE-08(JUSR_SS	. 14fc45b500000000001f 486ce80b00000000020 4ca4a3aa00000000021 1aa55c8e0000000002f 3f619fz000000000042 6313c46300000000042	2005 3:29 AM 2005 3:58 AM 2005 10:54 PM 2005 10:54 PM 2005 11:30 PM 005 11:30 PM 005 11:30 PM 8/17/2005 11:37 PM 9/1/2005 11:36 PM 9/9/2005 11:36 PM
0	The last publishe	Yes No SSE-08\IUSR_SS BEGIN CERTI SSE-08\IUSR_SS BEGIN CERTI SSE-08\IUSR_SS BEGIN CERTI SSE-08\IUSR_SS	14fc45b500000000001f 486cc80b00000000021 4ca4s3a00000000021 1ae55c3e0000000002f 3f0845d400000000003f 3f0845d4000000000042 6313c46300000000052 7c3861e30000000052	2005 3:29 AM 2005 3:58 AM 2005 10:54 PM 2005 10:54 PM 2005 10:54 PM 2005 11:30 PM 005 12:07 AM 8/17/2005 11:40 AM 8/17/2005 11:35 PM 9/1/2005 11:36 PM 9/9/2005 11:11 AM 9/9/2005 2:48 AM
0	The last publishe	Yes No SSE-08(JUSR_SS BEGIN CERTI. SSE-08(JUSR_SS BEGIN CERTI. SSE-08(JUSR_SS	14fc45b500000000001f 466ce80b0000000020 4ca4a3aa00000000021 1a355c8e0000000002f 3f619b7e00000000003f 3f619b7e000000000042 6313c46300000000052 7c386123000000000560 7c5ee35100000000061	2005 3:29 AM 2005 3:58 AM 2005 3:58 AM 2005 3:58 AM 2005 3:33 AM 005 11:30 PM 005 11:30 PM 005 11:30 PM 005 11:30 PM 017/2005 3:40 AM 9/17/2005 11:30 FM 9/1/2005 11:30 FM 9/9/2005 11:11 AM 9/9/2005 1:09 AM

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:

Step 1 From the Microsoft Certificate Services web interface, click Retrieve the CA certificate or certificate revocation list

will t	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 be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more ending upon the type of certificate you request.
	ect a task: Pretrieve the CA certificate or certificate revocation list Prequest a certificate Preck on a pending certificate
-	Next >

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

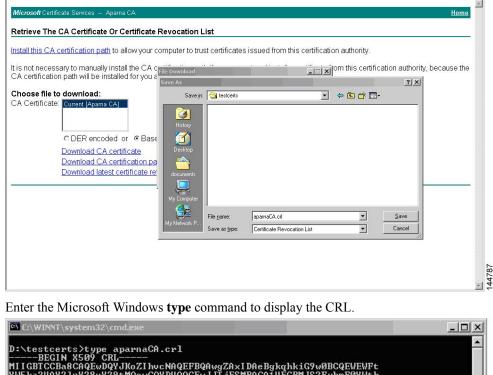
	e CA Certificate Or Certificate Revocation List	_
nstall this CA	certification path to allow your computer to trust certificates issued from this certification authority.	
	ssary to manually install the CA certification path if you request and install a certificate from this certification authority, because on path will be installed for you automatically.	the
Choose file	to download:	
CA Certificat	e: Current [Aparna CA]	
	CDER encoded or CBase 64 encoded	
	Download CA certificate	
	Download CA certification path	
	Download latest certificate revocation list	
		_

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

is not necessary to manually install the CA THE Download A certification path will be installed for you hoose file to download: A Certificate Ourrent [Aparna CA] C DER encoded or B Download CA certificate Download CA certificate Download Latest certificate C Der encoded or C Ba Download Latest certificate C Der encoded or C Ba Download Latest certificate C Der encoded or C Ba Download Latest certificate C Der encoded or C Ba Download Latest certificate C C C C C C C C C C C C C C C C C C C	ise the

Step 5

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



Related Topics

Configuring Certificate Revocation Checking Methods, on page 15

Importing the CRL

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

Step 1 Copy the CRL file to the Cisco NX-OS device bootflash. Device-1# copy tftp:apranaCA.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: shalWithRSAEncryption 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: 611B09A10000000002 Revocation Date: Aug 16 21:52:19 2005 GMT Serial Number: 4CDE464E0000000003 Revocation Date: Aug 16 21:52:29 2005 GMT Serial Number: 4CFC2B4200000000004 Revocation Date: Aug 16 21:52:41 2005 GMT Serial Number: 6C699EC20000000005 Revocation Date: Aug 16 21:52:52 2005 GMT Serial Number: 6CCF7DDC0000000006 Revocation Date: Jun 8 00:12:04 2005 GMT Serial Number: 70CC4FFF00000000007 Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 4D9B11160000000008 Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 52A8023000000000009 Revocation Date: Jun 27 23:47:06 2005 GMT CRL entry extensions: X509v3 CRL Reason Code: CA Compromise Serial Number: 5349AD46000000000A Revocation Date: Jun 27 23:47:22 2005 GMT CRL entry extensions: X509v3 CRL Reason Code: CA Compromise Serial Number: 53BD173C000000000B Revocation Date: Jul 4 18:04:01 2005 GMT

CRL entry extensions: X509v3 CRL Reason Code: Certificate Hold Serial Number: 591E7ACE0000000000 Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 5D3FD52E000000000D Revocation Date: Jun 29 22:07:25 2005 GMT CRL entry extensions: X509v3 CRL Reason Code: Key Compromise Serial Number: 5DAB7713000000000E Revocation Date: Jul 14 00:33:56 2005 GMT Serial Number: 5DAE53CD000000000F Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 5DB140D30000000000 Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 5E2D7C1B0000000011 Revocation Date: Jul 6 21:12:10 2005 GMT CRL entry extensions: X509v3 CRL Reason Code: Cessation Of Operation Serial Number: 16DB4F8F00000000012 Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 261C39240000000013 Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 262B52020000000014 Revocation Date: Jul 14 00:33:10 2005 GMT Serial Number: 2634C7F20000000015 Revocation Date: Jul 14 00:32:45 2005 GMT Serial Number: 2635B00000000000016 Revocation Date: Jul 14 00:31:51 2005 GMT Serial Number: 2648504000000000017 Revocation Date: Jul 14 00:32:25 2005 GMT Serial Number: 2A2763570000000018 Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 3F88CBF700000000019 Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 6E4B5F5F000000001A Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 725B89D8000000001B Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 735A88780000000001C Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 148511C70000000001D Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 14A71701000000001E Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 14FC45B5000000001F Revocation Date: Aug 17 18:30:42 2005 GMT Serial Number: 486CE80B00000000020 Revocation Date: Aug 17 18:30:43 2005 GMT Serial Number: 4CA4A3AA00000000021 Revocation Date: Aug 17 18:30:43 2005 GMT Serial Number: 1AA55C8E000000002F Revocation Date: Sep 5 17:07:06 2005 GMT Serial Number: 3F0845DD000000003F Revocation Date: Sep 8 20:24:32 2005 GMT Serial Number: 3F619B7E00000000042 Revocation Date: Sep 8 21:40:48 2005 GMT Serial Number: 6313C4630000000052 Revocation Date: Sep 19 17:37:18 2005 GMT Serial Number: 7C3861E300000000000 Revocation Date: Sep 20 17:52:56 2005 GMT Serial Number: 7C6EE35100000000061

Note The identity certificate for the device that was revoked (serial number 0A338EA100000000074) is listed at the end.