

Configuring Certificate Authorities and Digital Certificates

Public Key Infrastructure (PKI) support provides the means for the Cisco MDS 9000 Family switches to obtain and use digital certificates for secure communication in the network. PKI support provides manageability and scalability for IPsec/IKE and SSH.

This chapter includes the following sections:

- About CAs and Digital Certificates, page 34-1
- Configuring CAs and Digital Certificates, page 34-6
- Example Configurations, page 34-17
- Maximum Limits, page 34-36
- Default Settings, page 34-37

About CAs and Digital Certificates

This section provides information about certificate authorities (CAs) and digital certificates, and includes the following topics:

- Purpose of CAs and Digital Certificates, page 34-2
- Trust Model, Trust Points, and Identity CAs, page 34-2
- RSA Key-Pairs and Identity Certificates, page 34-2
- Multiple Trusted CA Support, page 34-3
- PKI Enrollment Support, page 34-4
- Manual Enrollment Using Cut-and-Paste Method, page 34-4
- Multiple RSA Key-Pair and Identity CA Support, page 34-4
- Peer Certificate Verification, page 34-5
- CRL Downloading, Caching, and Checking Support, page 34-5
- OCSP Support, page 34-5
- Import and Export Support for Certificates and Associated Key Pairs, page 34-5

Purpose of CAs and Digital Certificates

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 containing 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. The keys act as complements. 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 certificate is itself signed by a CA, a third party that is explicitly trusted by the receiver 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. Normally 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. The Internet Key Exchange (IKE), an essential component of IPsec, can use digital signatures to scalably authenticate peer devices before setting up security associations.

Trust Model, Trust Points, and Identity CAs

The trust model used in PKI support is hierarchical with multiple configurable trusted CAs. Each participating entity is configured with a list of CAs to be trusted so that the peer's certificate obtained during the security protocol exchanges can be verified, provided it has been issued by one of the locally trusted CAs. To accomplish this, CA's self signed root certificate (or certificate chain for a subordinate CA) is locally stored. 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* and is a mandatory step in trusting a CA.

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

The MDS switch can also enroll with a trust point to obtain an identity certificate (for example, for IPsec/IKE). This trust point is called an *identity CA*.

RSA Key-Pairs and Identity Certificates

You can generate one or more RSA key-pairs and associate each RSA key-pair with a trust point CA where the MDS switch intends to enroll to obtain an identity certificate. The MDS switch needs only one identity per CA, which consists of one key-pair and one identity certificate per CA.

Cisco MDS SAN-OS 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 switch 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 MDS switch trusts for peer certificate verification for any application (such as IKE or SSH).
- An MDS switch can have many trust points and all applications on the switch can trust a peer certificate issued by any of the trust point CAs.
- A trust point is not restricted to a specific application.
- An MDS switch enrolls with the CA corresponding to the trust point to obtain an identity certificate. You can enroll your switch with multiple trust points thereby obtaining 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 certificate extensions.
- 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 MDS switch.
- You can generate one or more RSA key-pairs on a switch 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 multiple identity certificates (each from a distinct CA) have been obtained, the certificate that an application selects to use in a security protocol exchange with a peer is application specific (see the "IPsec Digital Certificate Support" section on page 35-7 and the "SSH Authentication Using Digital Certificates" section on page 39-18).
- 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 (name) only once and does not issue multiple certificates with the same subject name. If you need more than one identity certificate for a CA, then define another trust point for the same CA, associate another key-pair to it, and have it certified, provided CA allows multiple certificates with the same subject name.

Multiple Trusted CA Support

An MDS switch can be configured to 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 switch with the specific CA that issued a certificate to a peer. Instead, you configure the switch with multiple trusted CAs that the peer trusts. A switch can then use a configured trusted CA to verify certificates offered by a peer that were not issued by the same CA defined in the identity of the switch.

Configuring multiple trusted CAs allows two or more switches enrolled under different domains (different CAs) to verify the identity of each other when using IKE to set up IPsec tunnels.

L

PKI Enrollment Support

Enrollment is the process of obtaining an identity certificate for the switch that is used for applications like IPsec/IKE or SSH. It occurs between the switch requesting the certificate and the certificate authority.

The PKI enrollment process for a switch involves the following steps:

- 1. Generate an RSA private and public key-pair on the switch.
- 2. Generate a certificate request in standard format and forward it to the CA.
- **3.** Manual intervention at the CA server by the CA administrator may be required to approve the enrollment request, when it is received by the CA.
- 4. Receive the issued certificate back from the CA, signed with the CA's private key.
- 5. Write the certificate into a nonvolatile storage area on the switch (bootflash).

Manual Enrollment Using Cut-and-Paste Method

Cisco MDS SAN-OS supports certificate retrieval and enrollment using a manual cut-and-paste method. Cut-and-paste enrollment literally means you must cut and paste the certificate requests and resulting certificates between the switch and the CA, as follows:

- 1. Create an enrollment certificate request, which is displayed in base64-encoded text form.
- 2. Cut and paste the encoded certificate request text in an e-mail message or in a web form and send it to the CA.
- **3.** Receive the issued certificate (in base64-encoded text form) from the CA in an e-mail message or in a web browser download.
- 4. Cut and paste the issued certificate to the switch using the certificate import facility.



Fabric Manager does not support cut and paste. Instead, it allows the enrollment request (certificate signing request) to be saved in a file to be sent manually to the CA.

Multiple RSA Key-Pair and Identity CA Support

Multiple identity CA support enables the switch to enroll with more than one trust point. This results in multiple identity certificates; each from a distinct CA. This allows the switch to participate in IPsec and other applications with many peers using certificates issued by appropriate CAs that are acceptable to those peers.

The multiple RSA key-pair support feature allows the switch to maintain a distinct key pair for each CA with which it is enrolled. Thus, it can match policy requirements for each CA without conflicting the requirements specified by the other CAs, such as key length. The switch 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 an MDS switch provides the means to verify peer certificates. The switch verifies certificates presented by peers during security exchanges pertaining to applications, such as IPsec/IKE and SSH. The applications verify the validity of the peer certificates presented to them. The peer certificate verification process involves the following steps:

- 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, two methods are supported: certificate revocation list (CRL) and Online Certificate Status Protocol (OCSP). A trust point uses one or both of these methods to verify that the peer certificate has not been revoked.

CRL Downloading, Caching, and Checking Support

Certificate revocation lists (CRLs) are maintained by CAs to give information of prematurely revoked certificates, and the CRLs are published in a repository. The download URL is made public and also specified in all issued certificates. A client verifying a peer's certificate should 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.

Cisco MDS SAN-OS allows the manual configuration of pre-downloaded of CRLs for the trust points, and then caches them in the switch bootflash (cert-store). During the verification of a peer certificate by IPsec or SSH, the issuing CA's CRL is consulted only if the CRL has already been cached locally and the revocation checking is configured to use CRL. Otherwise, CRL checking is not performed and the certificate is considered to be not revoked if no other revocation checking methods are configured. This mode of CRL checking is called CRL optional.

OCSP Support

Online Certificate Status Protocol (OCSP) facilitates online certificate revocation checking. You can specify an OCSP URL for each trust point. Applications choose the revocation checking mechanisms in a specified order. The choices are CRL, OCSP, none, or a combination of these 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 switch (for example, after a system crash) or to a replacement switch. The information in a PKCS#12 file consists of the RSA key-pair, the identity certificate, and the CA certificate (or chain).

Configuring CAs and Digital Certificates

This section describes the tasks you must perform to allow CAs and digital certificates your Cisco MDS switch device to interoperate. This section includes the following sections:

- Configuring the Host Name and IP Domain Name, page 34-6
- Generating an RSA Key-Pair, page 34-6
- Creating a Trust Point CA Association, page 34-8
- Copying Files to Bootflash, page 34-9
- Authenticating the CA, page 34-10
- Configuring Certificate Revocation Checking Methods, page 34-12
- Generating Certificate Requests, page 34-12
- Installing Identity Certificates, page 34-13
- Saving Your Configuration, page 34-13
- Ensuring Trust Point Configurations Persist Across Reboots, page 34-14
- Monitoring and Maintaining CA and Certificates Configuration, page 34-14

Configuring the Host Name and IP Domain Name

You must configure the host name and IP domain name of the switch if they are not already configured. This is required because switch FQDN is used as the subject in the identity certificate. Also, the switch FQDN is used as a default key label when none is specified during key-pair generation. For example, a certificate named SwitchA.example.com is based on a switch host name of SwitchA and a switch IP domain name of example.com.



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

To configure the host name and IP domain name, refer to the *Cisco MDS 9000 SAN-OS CLI* Configuration Guide.

Generating an RSA Key-Pair

RSA key-pairs are used to sign and/or encrypt and decrypt the security payload during security protocol exchanges for applications such as IKE/IPsec and SSH, and they are required before you can obtain a certificate for your switch.

To generate an RSA key-pair using Fabric Manager, follow these steps:

Step 1 Expand **Switches > Security** and then select **PKI** in the Information pane.

Step 2 Click the RSA Key-Pair tab.

You see the information shown in Figure 34-1.

RSA Key-Pair	Trust Point	Trust	Point Actions Trust Point D	etail
Switch	Name	Size	FileName	Exportable
V-172.22.31.18	34 test	rsa512	/isan/etc/certstore/test.key	false
v-190	test	rsa512	/isan/etc/certstore/test.key	false
v-188	test	rsa512	/isan/etc/certstore/test.key	false
v-185	test	rsa512	/isan/etc/certstore/test.key	false
sw-189	test	rsa512	/isan/etc/certstore/test.key	false
c-186	test	rsa512	/isan/etc/certstore/test.key	false

Figure 34-1 PKI RSA Key-Pair Information

Step 3 Click Create Row.

You see the Create RSA Key-Pair dialog box shown in Figure 34-2.

 ✓ <u>sw172-22-46-174</u> ✓ sw172-22-46-220 Switches: ✓ sw172-22-46-221 	
Name: Size: • rsa512 () rsa768 () rsa1024 () rsa1536 () rs	sa2048
Exportable	ose

Figure 34-2 Create RSA Key-Pair Dialog Box

- **Step 4** Select the switches for which you want to create the RSA key-pair.
- **Step 5** Assign a name to the RSA key-pair.
- **Step 6** Select the Size or modulus values. Valid modulus values are 512, 768, 1024, 1536, and 2048.

Note

The security policy (or requirement) at the local site (MDS switch) and at the CA (where enrollment is planned) are considered in deciding the appropriate key modulus.

Noto	

The maximum number of key-pairs you can configure on a switch is 16.

Step 7 Check the **Exportable** check box if you want the key to be exportable.



The exportability of a key-pair cannot be changed after key-pair generation.



Only exportable key-pairs can be exported in PKCS#12 format.

Step 8 Click **Create** to create the RSA Key-Pair.

Creating a Trust Point CA Association

To create a trust point CA association using Fabric Manager, follow these steps:

- **Step 1** Expand **Switches > Security** then select **PKI** in the Physical Attributes pane.
- **Step 2** Click the **Trust Point** tab in the Information Pane.

You see the information shown in Figure 34-3.

Figure 34-3 Trust Point Tab

Trust Point Detail	rust Point Actions	Tr	ist Point	-Pair Tru	RSA Kev
OCSP url	Revoke CheckMethods	air	KeyPa Name	Name	Switch
	crl		test	test	v-188

Step 3 Click Create Row.

You see the Create Trust Point dialog box shown in Figure 34-4.

Figure 34-4 Create Trust Point Dialog Box

SAN/Fabric sw-	isola-204/Switches/Security/PKI/Trust 🗙
Switch:	sw-isola-204 💌
TrustPointName:	
KeyPairName:	~
RevokeCheckMethods:	crl 💌
OCSPuri:	
	Create Close

- **Step 4** Select the switch for which you are creating the trust point CA from the **Switch** drop-down menu.
- **Step 5** Assign a name to the trust point CA.
- Step 6 Select a key-pair name to be associated with this trust point for enrollment. It was generated earlier in the "Generating an RSA Key-Pair" section on page 34-6. Only one RSA key-pair can be specified per CA.
- Step 7 From the RevokeCheckMethod drop-down menu, select the certificate revocation method that you would like to use (see Figure 34-4). You can use CRL, OCSP, CRL OCSP, or OCSP CRL to check for certificate revocation. The CRL OCSP option checks for revoked certificates first in the locally stored CRL. If not found, the switch uses OCSP to check the revoked certificates on the URL specified in Step 7.
- Step 8 Enter the OCSP URL if you selected an OCSP certificate revocation method.

Note

The OSCP URL must be configured before configuring the revocation checking method.

Step 9 Click **Create** to successfully create the trust point CA.

Copying Files to Bootflash

To copy files to bootflash using Device Manager, follow these steps:

- **Step 1** Choose **Admin > Flash Files**.
- **Step 2** Select bootflash in the Device field.

You see a list of flash files in the dialog box shown in Figure 34-5.

Figure	34-5	Flash	Files
--------	------	-------	-------

Device: bootfla 🔽	Partition: sup)-lo 💌 📸	
Name	Size M	lodified	_
bootflash		Feb 20 12:09:46 20	06
aaa_cnv.log	243	Aug 10 04:13:20 20	05
cboot-3-0-0-310	14.651M	Dec 20 06:32:10 20	05
cboot-3-0-0-346	14.659M	Feb 14 00:06:53 20	06
cert_init_debugs.t	1.345K	Feb 14 00:12:54 20	06
cisan-3-0-0-310	63.737M	Dec 20 06:31:47 20	05
cisan-3-0-0-346	63.690M	Feb 14 00:06:38 20	06
ips_cnvt.log	291	Aug 10 04:13:20 20	05
🗄 lost+found	12.288K	Jan 03 03:50:31 19	80
🗄 newer-fs	1.024K	Aug 10 04:55:32 20	05
radius_cnv.log	252	Aug 10 04:13:20 20	05
security_cnv.log	290	May 10 18:18:04 20	04
tacacs_cnv.log	252	Aug 10 04:13:20 20	05
Copy	Delete	Refresh Close	

Step 3 Click Copy.

You see the Copy Files dialog box shown in Figure 34-6.

Figure	34-6	Cop
--------	------	-----

4-6	Copy	Files	Dialog	Box

c-186 - Copy Files	X
Protocol:	⊙ tftp: ◯ ftp: ◯ scp: ◯ sftp: ◯ flashToFlash
ServerAddress:	171.71.55.12
RemoteUserName:	
RemotePassword:	
Server Source File:	
Switch Destination File:	bootflash: [device:][//partition][path]
	Apply Help Close

- Select tftp as the Protocol field. Step 4
- Click the Browse button to locate the appropriate file to copy to bootflash. Step 5
- Click Apply to apply these changes. Step 6

Authenticating the CA

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

Note

If the CA being authenticated is not a self-signed CA (that is, 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), then the full list of the CA certificates of all the CAs in the certification chain needs to be input during the CA authentication step. This is called the CA certificate chain of the CA being authenticated. The maximum number of certificates in a CA certificate chain is 10.

To authenticate a CA using Fabric Manager, follow these steps:

- Expand **Switches > Security** then select **PKI** in the Physical Attributes pane. Step 1
- Step 2 Click the **Trust Point Actions** tab in the Information pane.

You see the information shown in Figure 34-7.

Figure 34-7 **Trust Point Actions Tab**

		Deint Trust P	oint Actions Trust Point Detail			/54	AN/Fa
Switch	Name	Command	Url	Password	Last Command	Result	1
v-188	test	InoSelection			noSelection	Inone	

- Step 3 Click the Command field drop-down menu and select the appropriate option. Available options are caauth, cadelete, certreq, certimport, certdelete, pkcs12import, and pkcs12export. The caauth option is provided to authenticate a CA and install its CA certificate or certificate chain in a trust point.
- Step 4 Click the Browse button in the URL field and select the appropriate import certificate file from the Bootflash Files dialog box. It is the file name containing the CA certificate or chain in the bootflash:filename format.



You can authenticate a maximum of 10 trust points to a specific CA.



If you do not see the required file in the Import Certificate dialog box, make sure that you copy the file to bootflash. See "Copying Files to Bootflash" section on page 9.

Step 5 Click Apply Changes to save the changes.

Authentication is then confirmed or not confirmed depending on whether or not the certificate can be accepted after manual verification of its fingerprint.

Note

For subordinate CA authentication, the full chain of CA certificates ending in a self-signed CA is required because the CA chain is needed for certificate verification as well as for PKCS#12 format export.

Confirming CA Authentication

As mentioned in step 5 of "Authenticating the CA" section on page 34-10, CA authentication is required to be followed by CA confirmation in order to accept the CA certificate based on its fingerprint verification.

To confirm CA authentication using Fabric Manager, follow these steps:

- **Step 1** Expand **Switches > Security** and then select **PKI** in the Physical Attributes pane.
- **Step 2** Click the **Trust Point Actions** tab in the Information Pane.
- **Step 3** Make a note of the CA certificate fingerprint displayed in the IssuerCert FingerPrint column for the trust point row in question. Compare the CA certificate fingerprint with the fingerprint already communicated by the CA (obtained from the CA web site).

If the fingerprints match exactly, accept the CA with the **certconfirm** command in the Command drop-down menu. Otherwise, reject the CA with the **certnoconfirm** command.

Step 4 If you selected **certconfirm** in step 3, click Command and select the **certconfirm** action from the drop-down menu. Click **Apply Changes.**

If you selected **certnoconfirm** in step 3, click Command and select the **certnoconfirm** action drop-down menu. Click **Apply Changes**.

Configuring Certificate Revocation Checking Methods

During security exchanges with a client (for example, an IKE peer or SSH user), the MDS switch performs the certificate verification of the peer certificate sent by the client and the verification process may involve certificate revocation status checking.

You can use different methods for checking for revoked sender certificates. You can configure the switch to check the CRL downloaded from the CA (see the "Configuring a CRL" section on page 34-15), you can use OSCP if it is supported in your network, or both. Downloading the CRL and checking locally does not generate traffic in your network. However, certificates can be revoked between downloads and your switch would not be aware of the revocation. OCSP provides the means to check the current CRL on the CA. However, OCSP can generate network traffic that can impact network efficiency. Using both local CRL checking and OCSP provides the most secure method for checking for revoked certificates.



You must authenticate the CA before configuring certificate revocation checking.

Fabric Manager allows you to configure certificate revocation checking methods when you are creating a trust point CA. See "Creating a Trust Point CA Association" section on page 34-8.

Generating Certificate Requests

Figure 34-8

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

To generate a request for signed certificates from the CA using Fabric Manager, follow these steps:

- **Step 1** Expand **Switches > Security** and then select **PKI** in the Physical Attributes pane.
- **Step 2** Click the **Trust Point Actions** tab in the Information pane (see Figure 34-8).

Trust Point Actions Tab

RSA Key-Pair Trust Point Trust Point Actions Trust Point Detail Switch Name Command Url Password Command Result		1	3 🔒 🗳 🖌	1			/s	AN/F
	RSA Key	-Pair Tru	ust Point Trust P	oint Actions	Trust Point Detail			
	Switch	Name	Command	Url		Password	Result	

- Step 3 Select the certreq option from the Command drop-down menu. This generates a pkcs#10 certificate signing request (CSR) needed for an identity certificate from the CA corresponding to this trust point entry. This entry requires an associated key-pair. The CA certificate or certificate chain should already be configured through the caauth action. See "Authenticating the CA" section on page 34-10.
- Step 4 Enter the output file name for storing the generated certificate request. It will be used to store the CSR generated in PEM format. Use the format bootflash:filename. This CSR should be submitted to the CA to get the identity certificate. Once the identity certificate is obtained, it should be installed in this trust point. See "Installing Identity Certificates" section on page 34-13.
- **Step 5** Enter the *challenge* password to be included in the CSR.

183013

<u>Note</u>

e The challenge password is not saved with the configuration. This password is required in the event that your certificate needs to be revoked, so you must remember this password.

Step 6 Click **Apply Changes** to save the changes.

Installing Identity Certificates

You 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.

To install an identity certificate received from the CA using Fabric Manager, follow these steps:

- **Step 1** Expand **Switches > Security** and then select **PKI** in the Physical Attributes pane.
- Step 2 Click the Trust Point Actions tab, in the Information pane.
- Step 3 Select the certimport option from the Command drop-down menu to import an identity certificate in this trust point. The identity certificate is obtained from the corresponding CA for a CSR generated previously (see "Generating Certificate Requests" section on page 34-12).



The identity certificate should be available in PEM format in a file in bootflash.

- **Step 4** Enter the name of the certificate file that should have been copied to bootflash in the URL field in the bootflash:filename format.
- Step 5 Click Apply Changes to save your changes.

If successful, the values of the identity certificate and its related objects, like the certificate file name, are automatically updated with the appropriate values as per the corresponding attributes in the identity certificate.

Saving Your Configuration

Save your work when you make configuration changes or the information is lost when you exit.

To save your configuration using Fabric Manager, follow these steps:

- **Step 1** Expand **Switches** and then select **Copy Configuration** in the Physical Attributes pane.
- **Step 2** Select the switch configuration including the RSA key-pairs and certificates.
- **Step 3** Click **Apply Changes** to save the changes.

L

Ensuring Trust Point Configurations Persist Across Reboots

The trust point configuration is a normal Cisco SAN-OS 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 the that the configured certificates, key-pairs, and CRLs are persistent. Also, save the running configuration after deleting a certificate or key-pair to ensure the deletions permanent.

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

We also recommend that you create a password protected backup of the identity certificates nd save it to an external server (see the "Exporting and Importing Identity Information in PKCS#12 Format" section on page 34-14).



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

Monitoring and Maintaining CA and Certificates Configuration

The tasks in the section are optional. This section includes the following topics:

- Exporting and Importing Identity Information in PKCS#12 Format, page 34-14
- Configuring a CRL, page 34-15
- Deleting Certificates from the CA Configuration, page 34-16
- Deleting RSA Key-Pairs from Your Switch, page 34-16

Exporting and Importing Identity Information in PKCS#12 Format

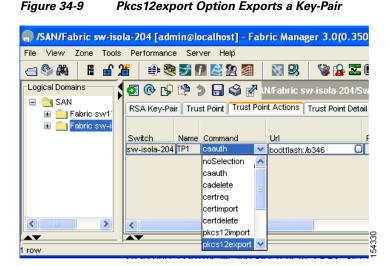
You can export the identity certificate along with the RSA key-pair and CA certificate of a trust point to a PKCS#12 file for backup purposes. You can later import the certificate and RSA key-pair to recover from a system crash on your switch or when you replace the supervisor modules.



Only bootflash: *filename* format is supported when specifying the export and import URL.

To export a certificate and key pair to a PKCS#12-formatted file using Fabric Manager, follow these steps:

- Step 1 Expand Switches > Security and then select PKI in the Physical Attributes pane.
- **Step 2** Click the **Trust Point Actions** tab in the Information Pane (see Figure 34-9).
- **Step 3** Select the **pkcs12export** option in the Command drop-down menu to export the key-pair, identity certificate, and the CA certificate or certificate chain in PKCS#12 format from the selected trust point.



- **Step 4** Enter the output file name as bootflash:filename to store the exported PKCS#12 identity.
- **Step 5** Enter the required password. The password is set for encoding the PKCS#12 data. On successful completion, the exported data is available in bootflash in the specified file.

Step 6 Click **Apply Changes** to save the changes.

To import a certificate and key pair formatted as a PKCS#12 formatted file, follow these steps:

- **Step 1** Expand **Switches > Security** and then select **PKI** in the Physical Attributes pane.
- **Step 2** Click the **Trust Point Actions** tab in the Information pane (see Figure 34-9).
- **Step 3** Select the **pkcs12import** option from the Command drop-down menu to import the key-pair, identity certificate, and the CA certificate or certificate chain in the PKCS#12 format to the selected trust point.
- **Step 4** Enter the input in the bootflash:filename format, containing the PKCS#12 identity.
- **Step 5** Enter the required password. The password is set for decoding the PKCS#12 data. On completion, the imported data is available in bootflash in the specified file.
- **Step 6** Click **Apply Changes** to save the changes.

On completion the trust point is created in the RSA key-pair table corresponding to the imported key-pair. The certificate information is updated in the trust point.



The trust point must be empty (with no RSA key-pair associated with it and no CA is associated with it using CA authentication) for the PKCS#12 file import to succeed.

Configuring a CRL

To configure the CRL from a file to a trust point using Fabric Manager, follow these steps:

Step 1 Click **Switches > Security > PKI** in the Physical Attributes pane.

- Step 2 Click the Trust Point Actions tab in the Information pane.
- **Step 3** Select the **crlimport** option from the Command drop-down menu to import the CRL to the selected trust point.
- **Step 4** Enter the input file name with the CRL in the bootflash:filename format, in the URL field.
- **Step 5** Click **Apply Changes** to save the changes.

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. Then after deleting the identity certificate, you can disassociate the RSA key-pair from a trust point. The certificate deletion is necessary to remove expired or revoked certificates, certificates whose key-pairs are compromised (or suspected to be compromised) or CAs that are no longer trusted.

To delete the CA certificate (or the entire chain in the case of a subordinate CA) from a trust point using Fabric Manager, follow these steps:

- **Step 1** Click **Switches > Security > PKI** in the Physical Attributes pane.
- Step 2 Click the Trust Point Actions tab in the Information pane.
- **Step 3** Select the **cadelete** option from the Command drop-down menu to delete the identity certificate from a trust point.



Note If the identity certificate being deleted is the last-most or only identity certificate in the device, you must use the **forcecertdelete** action to delete it. This ensures that the administrator does not mistakenly delete the last-most or only identity certificate and leave the applications (such as IKE and SSH) without a certificate to use.

Step 4 Click **Apply Changes** to save the changes.

To delete the identity certificate, click the **Trust Point Actions** tab and select the **certdelete** or **forcecertdelete** in the Command drop-down menu.

Deleting RSA Key-Pairs from Your Switch

Under certain circumstances you may want to delete your switch's RSA key-pairs. For example, if you believe the RSA key-pairs were compromised in some way and should no longer be used, you should delete the key-pairs.

To delete RSA key-pairs from your switch, follow these steps:

- **Step 1** Expand **Switches > Security** and then select **PKI** in the Physical Attributes pane.
- **Step 2** Click the **RSA Key-Pair** tab in the Information pane.
- Step 3 Click Delete Row.

Step 4 Click **Yes** or **No** in the Confirmation dialog box.

<u>Note</u>

After you delete RSA key-pairs from a switch, ask the CA administrator to revoke your switch's certificates at the CA. You must supply the challenge password you created when you originally requested the certificates. See "Generating Certificate Requests" section on page 34-12.

Example Configurations

This section shows an example of the tasks you can use to configure certificates and CRLs on the Cisco MDS 9000 Family switches using the Microsoft Windows Certificate server.

This section includes the following topics:

- Configuring Certificates on the MDS Switch, page 34-17
- Downloading a CA Certificate, page 34-19
- Requesting an Identity Certificate, page 34-24
- Revoking a Certificate, page 34-30
- Generating and Publishing the CRL, page 34-33
- Downloading the CRL, page 34-34
- Importing the CRL, page 34-36

Configuring Certificates on the MDS Switch

To configure certificates on an MDS switch using Fabric Manager, follow these steps:

- **Step 1** Choose **Switches** and set the LogicalName field to configure the switch host name.
- Step 2 Choose Switches > Interfaces > Management > DNS and set the DefaultDomainName field to configure.
- **Step 3** To create an RSA key-pair for the switch, follow these steps:
 - a. Choose Switches > Security > PKI and select the RSA Key-Pair tab.
 - b. Click Create Row and set the name and size field.
 - c. Check the Exportable check box and click Create.
- **Step 4** To create a trust point and associate the RSA key-pairs with it, follow these steps:
 - a. Choose Switches > Security > PKI and select the Trustpoints tab.
 - b. Click Create Row and set the TrustPointName field.
 - c. Select the RSA key-pairs from the KeyPairName drop-down menu.
 - d. Select the certificates revocation method from the CARevoke drop-down menu.
 - e. Click Create.
- **Step 5** Choose **Switches > Copy Configuration** and click **Apply Changes** to copy the running to startup configuration and save the trustpoint and key pair.

L

- **Step 6** Download the CA certificate from the CA that you want to add as the trustpoint CA.
- **Step 7** To authenticate the CA that you want to enroll to the trust point, follow these steps:.
 - a. Using Device Manager, choose Admin > Flash Files and select Copy and tftp copy the CA certificate to bootflash.
 - b. Using Fabric Manager, choose Switches > Security > PKI and select the TrustPoint Actions tab.
 - c. Select cauth from the Command drop-down menu.
 - d. Click ... in the URL field and select the CA certificate from bootflash.
 - e. Click Apply Changes to authenticate the CA that you want to enroll to the trust point.
 - f. Click the Trust Point Actions tab in the Information Pane.
 - **g.** Make a note of the CA certificate fingerprint displayed in the IssuerCert FingerPrint column for the trust point row in question. Compare the CA certificate fingerprint with the fingerprint already communicated by the CA (obtained from the CA web site). If the fingerprints match exactly, accept the CA by performing the **certconfirm** trust point action. Otherwise, reject the CA by performing the **certnoconfirm** trust point action.
 - **h.** If you select **certconfirm** in step g, select the **Trust Point Actions** tab, select **certconfirm** from the command drop-down menu and then click **Apply Changes**.
 - i. If you select **certnoconfirm** in step g, If you select **certconfirm** in step g, select the **Trust Point** Actions tab, select the **certnoconfirm** from the command drop-down menu and then click Apply Changes.
- **Step 8** To generate a certificate request for enrolling with that trust point, follow these steps:
 - a. Select the Trust Point Actions tab in the Information pane.
 - **b.** Select **certreq** from the Command drop-down menu. This generates a pkcs#10 certificate signing request (CSR) needed for an identity certificate from the CA corresponding to this trust point entry.
 - **c.** Enter the output file name for storing the generated certificate request. It should be specified in the bootflash:filename format and will be used to store the CSR generated in PEM format.
 - **d.** Enter the *challenge* password to be included in the CSR. The challenge password is not saved with the configuration. This password is required in the event that your certificate needs to be revoked, so you must remember this password.
 - e. Click Apply Changes to save the changes.
- **Step 9** Request an identity certificate from the CA.



The CA may require manual verification before issuing the identity certificate.

- **Step 10** To import the identity certificate, follow these steps:
 - a. Using Device Manager, choose Admin > Flash Files and select Copy and tftp copy the CA certificate to bootflash.
 - b. Using Fabric Manager, choose Switches > Security > PKI and select the TrustPoint Actions tab.
 - **c.** Select the **certimport** option from the Command drop-down menu to import an identity certificate in this trust point.



The identity certificate should be available in PEM format in a file in bootflash.

- **d.** Enter the name of the certificate file which was copied to bootflash, in the URL field in the bootflash:filename format.
- e. Click Apply Changes to save your changes.

If successful, the values of the identity certificate and its related objects, like the certificate file name, are automatically updated with the appropriate values as per the corresponding attributes in the identity certificate.

Downloading a CA Certificate

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

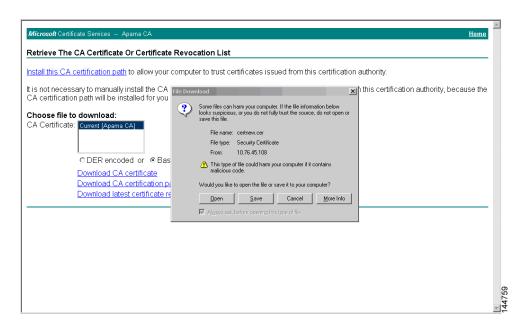
Step 1 Select the **Retrieve the CA certificate or certificate revocation task** radio button in the Microsoft Certificate Services web interface and click the **Next button**.

Microsoft Certificate Services Aparna CA	^
Incrosor centricate Services - Aparta CA	
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.	
Select a task: © Retrieve the CA certificate or certificate revocation list C Request a certificate C Check on a pending certificate	
Next >	
	7

Step 2 Select the CA certificate file to download from the displayed list. Click the **Base 64 encoded** radio button, and click the **Download CA certificate** link.

Microsoft Certificate Services Aparna CA Hor	ne
Retrieve The CA Certificate Or Certificate Revocation List	
nstall this CA certification path to allow your computer to trust certificates issued from this certification authority.	
is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because t CA certification path will be installed for you automatically.	he
Choose file to download: CA Certificate: Current [Aparna CA]	
C DER encoded or @ Base 64 encoded	
Download CA certificate Download CA certification path Download latest certificate revocation list	

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



Step 4 Click the **Copy to File** button in the Certificate dialog box and click **OK**.

	ertificate		? ×
stall this CA certification path to allow	General Details Certification	Path	tion authority.
is not necessary to manually install th A certification path will be installed fo	Show: <all></all>	Value	from this certification authority, because the
Choose file to download: CA Certificate: Current (Aparas CA) C DER encoded or Download CA certifica Download CA certifica Download latest certifica	Sersion Sersion Signature algorithm Issuer Vald from Vald to Subject Public key	V3 0560 D289 ACB4 1994 4F49 1 sha1R5A Aparna CA, netstorage, Cisco 04 Mei 2007 4:25:17 Aparna CA, netstorage, Cisco R5A (512 Bits) Edr Properties Copy to File	

Step 5 Select the Base-64 encoded X.509 (CER) on the Certificate Export Wizard dialog box and click Next.

nstall this CA certification path to allow	General Details	Certification Path	ion authority.
s not necessary to manually install th A certification path will be installed fc	Show: <al></al>		from this certification authority, because the
hoose file to download: A Certificate: Current (Apama CA)	Field Version Serial numbe Signature alc	Certificate Export Wizard Export File Format Certificates can be exported in a	variety of file formats.
© DER encoded or 《 Download CA certifica Download CA certifica Download latest certific	Valid from Valid from	Include al certificates Personal Information Exch Include al certificates	I (.CER) CER) what Standard - PKCS #7 Certificates (.P78) In the certification path if possible ange - PKCS #12 (.PFX) the certification path if possible on (requires IE 5.0, NT 4.0 SP4 on above)
			< <u>B</u> ack <u>N</u> ext > Cancel

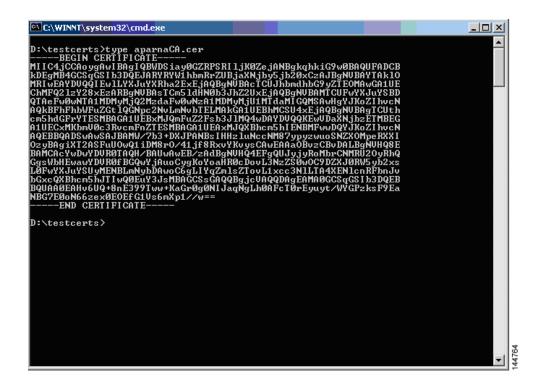
Step 6 Enter the destination file name in the File name: text box on the Certificate Export Wizard dialog box and click **Next**.

	Certificate	? X
stall this CA certification path to allow	General Details Certification Path	tion authority.
is not necessary to manually install th A certification path will be installed fc	Show: <al></al>	from this certification authority, because th
Choose file to download: CA Certificate: Current (Apama CA) C DER encoded or Download CA certifica Download CA certifica Download latest certifica	File to Export Specify the name of the file you want to expo Signature alg Valid from Valid from Public key	ort Btowse

Step 7 Click the **Finish** button on the Certificate Export Wizard dialog box.

C DER encoded or (Download CA certifica Download CA certifica Download CA certifica	cation authority, because the		Certificate General Details Certification Path Show: CAI> Field Certificate Export Wizard Version	Install this CA certification path to allow It is not necessary to manually install th CA certification path will be installed fc Choose file to download:
Seck Finish	te Export	You have successfully completed the Certificate Export wizard. You have specified the following settings: File Name Ditest Export Keys No Include all certification in the certification path No File Format Base64	Issuer Valid from Valid to Subject	Download CA certifica Download CA certifica

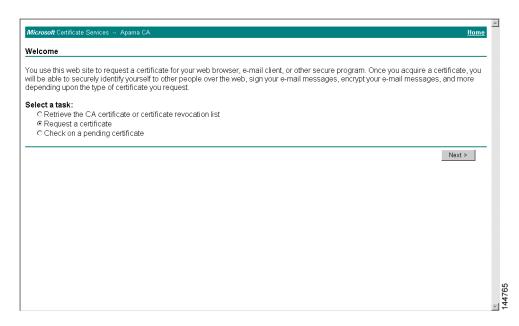
Step 8 Display the CA certificate stored in Base-64 (PEM) format using the Microsoft Windows **type** command.



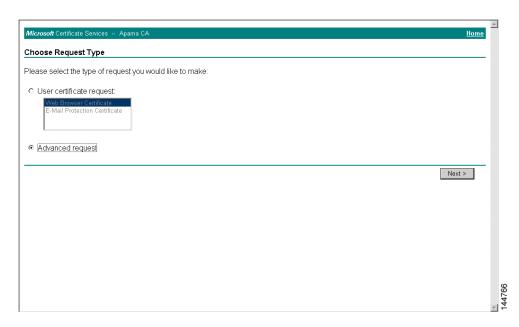
Requesting an Identity Certificate

To request an identify certificate from a Microsoft Certificate server using a PKCS#10 certificate signing request (CRS), follow these steps:

Step 1 Select the Request an identity certificate radio button on the Microsoft Certificate Services web interface and click **Next**.



Step 2 Select the Advanced Request radio button and click Next.



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

Microsoft Certificate Services Aparna CA	iome 🔺
Advanced Certificate Requests	
You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification 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.	
 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. 	
Next >]
	T

Step 4 Paste the base64 PKCS#10 certificate request in the Saved Request text box and click Next. The certificate request is copied from the MDS switch console (see the "Generating Certificate Requests" section on page 34-12 and "Configuring Certificates on the MDS Switch" section on page 34-17)

Microsoft Certificate Services Aparna CA <u>Home</u>
Submit A Saved Request
Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web server) into the request field to submit the request to the certification authority (CA).
Saved Request:
VqyHOvEv&gMBAAGgTzAVBgkqhkiG9w0BCQcxCBNG DjppRcew0qTVVRORAQH/BBawGYIRVMvNYMtHS5 Base64 Encoded KozInvcNQEEDQADyETAKT60KER6000,09BXZVH Certificate Request ptctNcUUE/yw6Hayf012T3ecgNvm12d1533YBF2; (PKCS #IO or #7): 6a23NDNPM8bkvLkuVECKTVAg0jfngPN END CERTIFICATE REQUEST
Additional Attributes:
Attributes:
Submit >

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

<i>Microsoft</i> Certificate Services Apama CA	Home -
Certificate Pending	
Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.	
Please return to this web site in a day or two to retrieve your certificate.	
Note: You must return with this web browser within 10 days to retrieve your certificate	
	ę

Step 6 The CA administrator approves the certificate request.

Ertification Authority						<u> </u>
Action ⊻iew	1 🔹 🖏	2				
Tree	Request ID	Binary Request	Request Disposition Message	Request Submission D	· ·	Reques
Certification Authority (Local) Aparna CA Issued Certificates Pending Requests Failed Requests	116	BEGIN NE	Taken Under Submission	All Tasks → Issue Refresh Help	SSE-08\IUSR_SS	
Contains operations that can be performe		t.				F

Step 7 Select the **Check on a pending certificate** radio button on the Microsoft Certificate Services web interface and click **Next**.

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

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

Microsoft Certificate Services Aparna CA	<u>Home</u>	4
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 >	
		144772
		144

Step 9 Select Base 64 encoded and click the Download CA certificate link.

Microsoft Certificate Services Apama CA	<u>Home</u>
Certificate Issued	
The certificate you requested was issued to you.	
C DER encoded or	
Download CA certificate Download CA certification path	

Step 10 Click **Open** on the File Download dialog box.

Microsoft Certificate Services Aparna CA		<u>Home</u>
Certificate Issued		
Certificate Issued The certificate you requested was issued to C DER encoded or C Base 6 Download CA certificate Download CA certification path	· · · · · · · · · · · · · · · · · · ·	

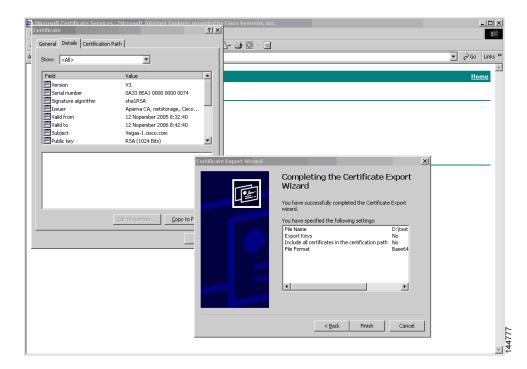
Step 11 Click the Details tab on the Certificate dialog and click the Copy to File button. Select the Base-64 encoded X.509 (.CER) radio button on the Certificate Export Wizard dialog box and click Next.

Microsoft Certificate Services - Microsoft Internet Explorer prov Certificate	ided by Cisco Systems, Inc.	
General Details Certification Path	, 1- 3 C - E	
A Show: <all></all>		▼ 🖉 Go Links ≫
		A
Field Value	A	<u>Home</u>
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.cisco.com Public key RSA (1024 Bits)	-	
Public Rey R5A (1024 bits)	Certificate Export Wizard	×
	Export File Format Certificates can be exported in a variety of file formats.	
	Select the format you want to use:	
Edit Properties Copy to File	DER encoded binary X.509 (.CER) Base-64 encoded X.509 (.CER)	
	Gryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
OK	Gryptographic message syntax standard - MCS #7 Certificates (.P76) Include all certificates in the certification path if possible	
	Personal Information Exchange - PKC5 #12 (.PEX)	
	 Include 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 > C	ancel
		75
		<u>144775</u>
		<u> </u>

Step 12 Enter the destination file name in the File name: text box on the Certificate Export Wizard dialog box, then click **Next**.

Microsoft Certificate Services - Microsoft Internet Explorer - Certificate	rnvided hy Cisco Systems, Inc.	<u> </u>
General Details Certification Path		
A Show: <all></all>		▼ 🖉 Go Links »
		<u> </u>
Field Value	· ·	<u>Home</u>
E Serial number 0A33 8EA1 0000 0000 0074		
Signature algorithm sha1RSA		
Issuer Aparna CA, netstorage, Cisco Valid from 12 Nopember 2005 8:32:40	n	
Valid to 12 Nopember 2006 8:42:40		
Subject Vegas-1.cisco.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: D:\testcerts\myID.cer Browse	
Edit Properties Copy to F	D:\testcerts\myID.cer Browse	
	< Back Next > Cancel	
	Zack Berr Cancer	76
		144776
		₹





Step 14 Display the identity certificate in base64-encoded format using the Microsoft Windows type command.

C:\WINNT\system32\cmd.exe	
D:\testcerts>type myID.cer BGIN CERTIFICATE MI IEADCCA6ggMv IBagIKGjOOQAAAAAAAAAAAAAAAAAAAAABGKGSv0BAQUFADCBkDEgMB4G CSgGSIb3DQEJARYRYWihbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAk1OMRIwEAYD UQQIEwILYXJuYXRha2ExEjAQBgNVBACTCUJhbmdhbG9vZTEOMAwGAIUEChMFQ21z Y28xEzARBgNVBASTCn51dHN0b3JhZ2UxEjAQBgNVBAMTCUJFwYXJuYSBDQTAeFw0w NTExMTIwMzayNDBaFC0bJhZ2UxEjAQBgNVBAMTCUJFwYXJuYSBDQTAeFw0w NTExMTIwMzayNDBaFC0bJhZ2UxEjAQBgNVBAMTCUJFwYXJuYSBDQTAeFw0w NTExMTIwMzayNDBaFC0bJhZ2UxEjAQBgNVBAMTCUJFwYXJuYSBDQTAeFw0w NTExMTIWZayNDBaFC0bJhZ2UxEjAQBgNVBAMTCUJFwYXJuYSBDQTAeFw0w NTExMTIWZayNDBaFC0bJhZ2UxEjAQBgNVBAMTCUJFwYXJuYSBDQTAeFw0w NTExMTIWZayNDBaFC0bJhZ2UxEjAQBgNVBAMTCUJFwYXJuYSBDQTAeFw0w NTExMTIWZayNDBaFC0bJhZ2UXEJAQBgNVBAMTEUZIZZFzLTEu Y21xY2vTHIGFMA0GCSgGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C dq1WkjKjSICdqLfK5eJSmNCQujGpzcuKsZPFXjP2UoiyeCYE8yJncWACdjQu41C dq1WkjKjSICdqLfK5eJSmNCQujGpzcuKsZPFXjP2UoiyeCYE8yJncWACdjQu41C dq1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjP2UoiyeCYE8yJncWNACdjQu41C dq1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjP2UoiyeCYE8yJncWNACdjQUDR0RADH/sBsv C7IRUmUnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDUR0BBYEFKCLi+2sspWEfgFR bhWmUUy09jngMIHMBgNUHSMEgcQwgCGAFCc08kaDGGwJTEUNjsKYUB0LFnxx0YGW JGTMTGQMSAuHgYJKoZIhvcNAQKBFhFhbWFUZG1IQGNpc2NvLmNbTELMAKGA1UE BhMCSU4xEjAQBgNUBAgTCULhcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3J1MQ4w DAYDUQQKEwUDAXNjb2ETMBEGA1UECXMKbmU0c3RvcmFnZTESMBAGA1UEAXMJQXBh cm5hiEMBghAFYNKJrLqZ1E9JEiWMrR16MGSGA1UdHwRMGIWLqAsoCQGKGAQBH0H6 Ly9czUtMDgvQ2UyUEUucm9sbC9BcGFybmE1MjBDQS5jcmwMKAnoCyGKRZpbGU6 Ly9czNHXZSX00FXDZXJ08H5yb2xsXEFvYXJUYSUJMENBLmNydDANEdgYKWBBQUH AAQEFjB8MDsGCCSGAQUFBZAChi9odHRw0i8uc3NLITA4L0N1ncRFbnJvGGwBQUH AANBADbGBGsbe7GNLH9xeOTWBNbm24U69ZSuDDcOcUZUUIgrpnTqUpPyejtsyf1w E36c1Zu4WsExREqxb1L84xc7U5o= END CERTIFICATE D:\testcerts>	28
	447

Revoking a Certificate

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

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

Step 2 Select All Tasks > Revoke Certificate.

ree	Request ID	Requester Name	Binary Certificate	Serial Number	Certificate Effective Da
Certification Authority (Local)	89	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
	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
Failed Requests	E 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
	Sec. 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	4aafff2e000000000071	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
	•	Open			

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

Certification Authority					_ 🗆 >
Action View 🛛 🗢 🔿 🗈	• 🔹 🖏	3			
ree	Request ID	Requester Name	Binary Certificate	Serial Number	Certificate Effective Da
Certification Authority (Local)	89 🔛	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
	92	SSE-08\IUSR_SS	BEGIN CERTI	7c3278180000000005c	9/20/2005 10:14 PM
	93	SSE-08\IUSR_SS	BEGIN CERTI	7c3278270000000005d	9/20/2005 10:14 PM
Failed Requests	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		DECTH CEDT	10000062	9/21/2005 12:18 AM
	99	Certificate Revocatio	n	?×p0000063	9/22/2005 1:45 AM
	100	Are you sure you want	to revoke the selected	certificate(s)? 0000064	9/27/2005 2:44 AM
	101	· ·		0000065	9/27/2005 2:45 AM
	See 102	You may specify a reas	on for this revocation.	0000066	9/30/2005 1:46 AM
	103	Reason code:		0000067	10/5/2005 4:03 AM
	104	Unspecified	_	0000068	10/6/2005 10:46 PM
	105	Tousboomed		0000069	10/7/2005 1:52 AM
	106		Yes	No 000006a	10/7/2005 4:11 AM
	107			000006b	10/10/2005 3:49 AM
	108	SSE-08\IUSR_SS	BEGIN CERTI	5F413d2000000000006c	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	17b3067600000000006e	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	170bea8b000000000070	10/20/2005 11:53 PM
	113	SSE-08\IUSR_SS	BEGIN CERTI	4aafff2e000000000071	10/31/2005 12:32 AM
	114	SSE-08\IUSR_SS	BEGIN CERTI	78cc6e6c00000000072	11/8/2005 11:26 PM
	115		BEGIN CERTI	78e3416100000000073	11/8/2005 11:51 PM
	116	SSE-08\IUSR_SS	BEGIN CERTI	0a338ea1000000000074	11/12/2005 8:32 AM
	•				
		N			

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

Certification Authority (Local)	-	Requester Name	Binary Certificate	Serial Number	Certificate Effective Date
	15	SSE-08\IUSR_SS	BEGIN CERTI	5dae53cd00000000000	6/30/2005 3:27 AM
🔁 Aparna CA	16	SSE-08\IUSR_SS	BEGIN CERTI	5db140d3000000000010	6/30/2005 3:30 AM
Revoked Certificates	17	SSE-08\IUSR_SS	BEGIN CERTI	5e2d7c1b00000000011	6/30/2005 5:46 AM
Issued Certificates	18	SSE-08\IUSR_SS	BEGIN CERTI	16db4f8f00000000012	7/8/2005 3:21 AM
Pending Requests	19	SSE-08\IUSR_SS	BEGIN CERTI	261c392400000000013	7/14/2005 5:00 AM
Failed Requests	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	14a7170100000000001e	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
	1 63	SSE-08\IUSR_SS	BEGIN CERTI	3f0845dd0000000003f	9/9/2005 1:11 AM
	100 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
	22 96	SSE-08\IUSR_SS	BEGIN CERTI	7c3861e3000000000060	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

Generating and Publishing the CRL

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

- 📴 Certification Authority <u>- 🗆 ×</u> Action View 🗈 🖬 😭 🐼 😫 All Tasks Publish Request ID Requester Name Binary Certificate Serial Number Certificate Effective Date 3 15 5dae53cd00000000000 6/30/2005 3:27 AM Refresh SSE-08\IUSR SS... -----BEGIN CERTI... y (Local) 2016 SSE-08\IUSR_SS... -BEGIN CERTI... 5db140d3000000000000 6/30/2005 3:30 AM Export List. 17 17 18 18 SSE-08\IUSR_SS... -----BEGIN CERTI... 5e2d7c1b00000000011 6/30/2005 5:46 AM Properties SSE-08\IUSR SS... -----BEGIN CERTI... 16db4f8f00000000012 7/8/2005 3:21 AM ficates 7/14/2005 5:00 AM iests SSE-08\IUSR_SS... -----BEGIN CERTI... 261c3924000000000013 Help 20 SSE-08\IUSR_SS... -----BEGIN CERTI... 7/14/2005 5:16 AM 262b520200000000014 21 SSE-08\IUSR_SS... -----BEGIN CERTI... 2634c7f200000000015 7/14/2005 5:27 AM 22 SSE-08\IUSR SS... -----BEGIN CERTI... 2635b000000000000016 7/14/2005 5:28 AM 23 SSE-08\IUSR_SS... -----BEGIN CERTI... 26485040000000000017 7/14/2005 5:48 AM 24 SSE-08\IUSR_SS... ------BEGIN CERTI... 2a27635700000000018 7/14/2005 11:51 PM 25 26 SSE-08\IUSR_SS... -----BEGIN CERTI... 3f88cbf7000000000019 7/19/2005 3:29 AM SSE-08\IUSR_SS... -----BEGIN CERTI... 6e4b5f5f00000000001a 7/28/2005 3:58 AM 27 SSE-08\IUSR_SS... -----BEGIN CERTI... 725b89d80000000001b 7/28/2005 10:54 PM 28 29 SSE-08\IUSR_SS... -----BEGIN CERTI... 735a887800000000001c 7/29/2005 3:33 AM SSE-08\IUSR_SS... -----BEGIN CERTI... 148511c70000000001d 8/3/2005 11:30 PM 30 31 SSE-08\IUSR_SS... -----BEGIN CERTI... 14a7170100000000001e 8/4/2005 12:07 AM SSE-08\IUSR_SS... -----BEGIN CERTI... 14fc45b500000000001f 8/4/2005 1:40 AM 32 SSE-08\IUSR_SS... -----BEGIN CERTI... 486ce80b00000000020 8/17/2005 3:58 AM 33 2017 SSE-08)TUSE SS... -----BEGIN CERTL... 4ca4a3aa000000000021 8/17/2005 11:37 PM SSE-08\IUSR_SS... -----BEGIN CERTI... 1aa55c8e00000000002f 9/1/2005 11:36 PM **1**63 SSE-08\IUSR_SS... -----BEGIN CERTI... 3f0845dd0000000003f 9/9/2005 1:11 AM **1**66 SSE-08\IUSR_SS... -----BEGIN CERTI... 3f619b7e000000000042 9/9/2005 2:48 AM 82 SSE-08\IUSR SS... -----BEGIN CERTI... 6313c463000000000052 9/16/2005 1:09 AM **10**96 SSE-08\IUSR_SS... -----BEGIN CERTI... 7c3861e3000000000000 9/20/2005 10:20 PM **3**97 SSE-08\IUSR_SS... ------BEGIN CERTI... 7c6ee351000000000061 9/20/2005 11:20 PM 116 -----BEGIN CERTI... SSE-08\IUSR_SS... 0a338ea100000000074 11/12/2005 8:32 AM 144782 Contains operations that can be performed on the object.
- Step 1 Select Action > All Tasks > Publish on the Certification Authority screen.

Step 2 Click Yes on the Certificate Revocation List dialog box to publish the latest CRL.

ree	Request ID	Requester Name	Binary Certificate	Serial Number	Certificate Effective Date	
Certification Authority (Local)	15	SSE-08\IUSR_SS	BEGIN CERTI	5dae53cd00000000000f	6/30/2005 3:27 AM	
🕅 Aparna CA	16	SSE-08\IUSR_SS	BEGIN CERTI	5db140d3000000000010	6/30/2005 3:30 AM	
Revoked Certificates	17	SSE-08\IUSR_SS	BEGIN CERTI	5e2d7c1b00000000011	6/30/2005 5:46 AM	
	18	SSE-08\IUSR_SS	BEGIN CERTI	16db4f8f000000000012	7/8/2005 3:21 AM	
Pending Requests	19	SSE-08\IUSR_SS	BEGIN CERTI	261c392400000000013	7/14/2005 5:00 AM	
Failed Requests	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\TUSE_SS	BEGIN CERTI	2648504000000000017	7/14/2005 5:48 AM	
	LEX 23	225 0040201 22011				
Certific	ate Revocation Li				🔀 2005 11:51 PM	
Certific					2005 11:51 PM 2005 3:29 AM	
	ate Revocation Li	st	n be used by clients. A	re you sure you want to publish	2005 3:29 AM	
Certific	ate Revocation Li	st	n be used by clients. A	re you sure you want to publish	2005 3:29 AM	
	ate Revocation Li	st od CRL is still valid and ca		re you sure you want to publish	2005 3:29 AM 2005 3:58 AM 2005 10:54 PM 2005 3:33 AM	
Certific	ate Revocation Li	st		re you sure you want to publish	2005 3:29 AM 2005 3:58 AM 2005 10:54 PM	
	ate Revocation Li	st ed CRL is still valid and ca	s No]	2005 3:29 AM 2005 3:58 AM 2005 10:54 PM 2005 3:33 AM 005 11:30 PM 005 12:07 AM	
	The last publishe	st ed CRL is still valid and ca Yes SSE-08\IUSR_SS	s No	14fc45b50000000001f	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 8/4/2005 1:40 AM	
	The last publishe	st ed CRL is still valid and ca Yes SSE-08\IUSR_SS	s No	14fc45b50000000001f	2005 3:29 AM 2005 3:58 AM 2005 10:54 PM 2005 3:33 AM 005 11:30 PM 005 12:07 AM	
	The last publishe	st d CRL is still valid and ca SSE-08\TUSR_SS SSE-08\TUSR_SS	s No	14fc45b500000000001f 486ce80b00000000020	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 8/4/2005 1:40 AM	
	The last publishe	st ed CRL is still valid and ca Ver SSE-08\[USR_SS SSE-08\[USR_SS SSE-08\[USR_SS	s No NoBEGIN CERTI	14fc45b50000000001f 486ce80b0000000020 4ca4a3aa00000000021	2005 3:29 AM 2005 3:258 AM 2005 3:358 AM 2005 10:54 PM 2005 11:30 PM 005 11:30 PM 005 12:07 AM 80/12/2005 3:358 AM	
	ate Revocation Li The last publishe I I I I I I I I I I I I I I I I I I I	st d CRL is still valid and ca SSE-08\TUSR_SS SSE-08\TUSR_SS SSE-08\TUSR_SS SSE-08\TUSR_SS SSE-08\TUSR_SS	s No	14fc45b500000000001f 486ce80b00000000020 4ca4a3aa00000000021 1aa55c8e0000000002f	2005 3:29 AM 2005 3:29 AM 2005 3:35 AM 2005 10:54 PM 2005 11:30 PM 005 11:30 PM 005 12:07 AM 8/17/2005 1:40 AM 8/17/2005 11:37 PM	
	the last published in	st d CRL is still valid and ca SSE-08(IUSR_SS SSE-08(IUSR_SS SSE-08(IUSR_SS SSE-08(IUSR_SS SSE-08(IUSR_SS SSE-08(IUSR_SS)	s No	14fc45b500000000001f 486ce80b00000000020 4ca4a3aa00000000021 1aa55c8e0000000002f 3f0845dd000000003f	2005 3:29 AM 2005 3:58 AM 2005 1:54 PM 2005 1:54 PM 2005 1:33 AM 005 11:30 PM 005 12:07 AM 8/4/2005 1:40 AM 8/17/2005 11:37 PM 9/1/2005 11:36 PM	
	ate Revocation Li The last published The last publi	st CRL is still valid and ca SSE-08(JUSR_SS SSE-08(JUSR_SS SSE-08(JUSR_SS SSE-08(JUSR_SS SSE-08(JUSR_SS SSE-08(JUSR_SS SSE-08(JUSR_SS	No BEGIN CERTI BEGIN CERTI BEGIN CERTI BEGIN CERTI BEGIN CERTI	14fc45b50000000001f 486ce80b0000000020 4ca4a3aa00000000021 1aa55c8e00000000002f 3f0a45d00000000003f 3f19b7e000000000042	2005 3:29 AM 2005 3:58 AM 2005 3:58 AM 2005 3:35 AM 2005 10:54 PM 2005 1:30 PM 005 11:30 PM 005 11:30 PM 8/17/2005 1:40 AM 8/17/2005 1:40 AM 9/1/2005 11:37 PM 9/1/2005 11:37 PM	
	ate Revocation Li The last publishe 7 31 7 32 7 33 7 47 7 53 7 56 7 56 7 56 7 56 7 56 7 56 7 56 7 56	st Ver SSE-08[1USR_SS SSE-	No BEGIN CERTI BEGIN CERTI BEGIN CERTI BEGIN CERTI	14fc45b50000000001f 486ce80b0000000020 4ca4a3aa00000000021 1aa55c8e00000000002f 3f0a45d00000000003f 3f19b7e000000000042	2005 3:29 AM 2005 3:25 AM 2005 10:54 PM 2005 3:33 AM 005 11:30 PM 005 11:30 PM 005 11:30 PM 005 11:40 AM 8/17/2005 11:13 PM 9/1/2005 11:13 PM 9/1/2005 11:13 PM 9/9/2005 11:11 AM	
	ate Revocation Li The last published The last publi	st d CRL is still valid and ca SSE-08(JUSR_SS) SSE-08(JUSR_SS) SSE-08(JUSR_	No BEGIN CERTI BEGIN CERTI	14fc45b500000000001f 486ce80b00000000020 4ca4a3aa00000000021 1aa55c8e00000000002f 3f0845d0000000003f 3f619b7e00000000042 6313c46300000000052	2005 3:29 AM 2005 3:29 AM 2005 3:58 AM 2005 10:54 PM 2005 11:30 PM 005 11:30 PM 005 11:30 PM 005 12:07 AM 8/17/2005 3:58 AM 8/17/2005 11:36 PM 9/1/2005 11:136 PM 9/9/2005 2:48 AM 9/16/2005 1:09 AM	

Γ

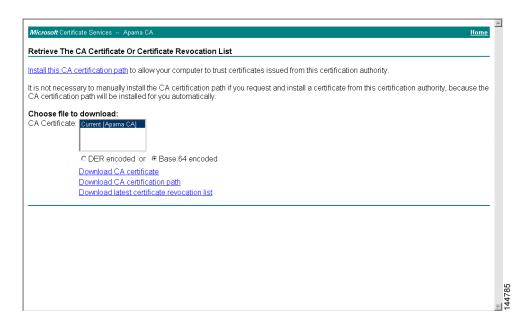
Downloading the CRL

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

Step 1 Select **Request the CA certificate or certificate revocation list** radio button on the Microsoft Certificate Services web interface and click **Next**.

	A.
Microsoft Certificate Services Aparna CA Home	
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.	
Select a task: © Retrieve the CA certificate or certificate revocation list © Request a certificate © Check on a pending certificate	
Next >	
	144784
	14

Step 2 Click the Download latest certificate revocation list link.



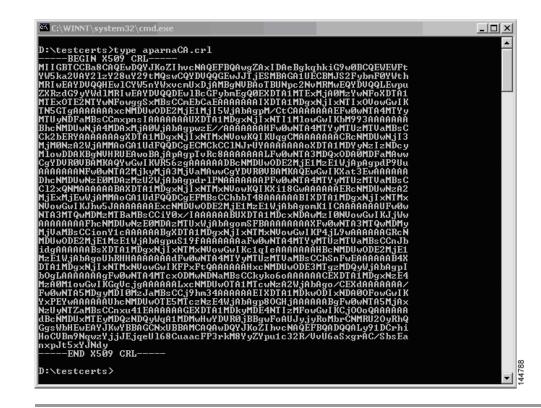
Step 3 Click **Save** in the File Download dialog box.

stall this CA certification path to allow your co	mputer to trust certificates issued from this certificati	on authority.
is not necessary to manually install the CA A certification path will be installed for you choose file to download: A Certificate: Current [Apama CA] C DER encoded or © Ba Download CA certificate Download CA certificate Download latest certificate	Download 2 Some files can harm your computer. If the file information below looks suspicious, or you do not fully itust the source, do not open or save this file. File name: cettcl crl File type: Cettricate Revocation List From: 10.76.45.108 Would you like to open the file or save it to your computer? Qpen Save Cancel More Info	In this certification authority, because the
	I Algers ask before opening this type of file	

Step 4 Enter the destination file name in the Save As dialog box and click **Save**.

Microsoft Certificate Services Aparna CA				Home
Retrieve The CA Certificate Or Certificate I	Revocation List			
Install this CA certification path to allow your co	omputer to trust certificates	issued from this certification authority.		
It is not necessary to manually install the CA c CA certification path will be installed for you ε	File Download Save As	om this certi	fication authorit	y, because the
Choose file to download: CA Certificate: Current [Aparna CA]	Save As Save jn: 🔄 testcerts			
	History			
○ DER encoded or	Desktop			
Download CA certification pa Download latest certificate re	documents			
	My Computer			
	File name:	apamaCA.crl	Save	
	Save as type:	Certificate Revocation List	Cancel	
				Ŧ

Step 5 Display the CRL using the Microsoft Windows **type** command.



Importingthe CRL

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

- **Step 1** Click **Switches > Security > PKI** in the Physical Attributes pane.
- **Step 2** Click the **Trust Point Actions** tab in the Information pane.
- **Step 3** Select the **crlimport** option from the Command drop-down menu to import the CRL to the selected trust point.
- Step 4 Enter the input file name with the CRL in the bootflash:filename format, in the URL field.
- **Step 5** Click **Apply Changes** to save the changes.



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

Maximum Limits

Table 34-1 lists the maximum limits for CAs and digital certificate parameters.

Feature	Maximum Limit
Trust points declared on a switch	16
RSA key-pairs generated on a switch	16
Identity certificates configured on a switch	16
Certificates in a CA certificate chain	10
Trust points authenticated to a specific CA	10

Table 34-1 Maximum Limits for CA and Digital Certificate

Default Settings

Table 34-2 lists the default settings for CAs and digital certificate parameters.

Table 34-2	Default CA and Digital Certificate Parameters
------------	---

Parameters	Default
Trust point	None
RSA key-pair	None
RSA key-pair label	Switch FQDN
RSA key-pair modulus	512
RSA key-pair exportable	Yes
Revocation check method of trust point	CRL.