

Configuring Certificate Authorities and Digital Certificates

This chapter includes the following sections:

- About CAs and Digital Certificates, page 6-1
- Configuring CAs and Digital Certificates, page 6-6
- Example Configurations, page 6-16
- Maximum Limits, page 6-38
- Default Settings, page 6-39

About CAs 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.

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.

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

- Purpose of CAs and Digital Certificates, page 6-2
- Trust Model, Trust Points, and Identity CAs, page 6-2
- RSA Key-Pairs and Identity Certificates, page 6-3
- Multiple Trusted CA Support, page 6-3
- PKI Enrollment Support, page 6-4

Γ

- Manual Enrollment Using Cut-and-Paste Method, page 6-4
- Multiple RSA Key-Pair and Identity CA Support, page 6-4
- Peer Certificate Verification, page 6-5
- CRL Downloading, Caching, and Checking Support, page 6-5
- OCSP Support, page 6-5
- Import and Export Support for Certificates and Associated Key-Pairs, page 6-5

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, the 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 NX-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.
- 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.

PKI Enrollment Support

Enrollment is the process of obtaining an identity certificate for the switch that is used for applications such as 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 NX-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.

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 with 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 NX-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).

L

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 6-6
- Generating an RSA Key-Pair, page 6-6
- Creating a Trust Point CA Association, page 6-8
- Authenticating the CA, page 6-8
- Configuring Certificate Revocation Checking Methods, page 6-9
- Generating Certificate Requests, page 6-10
- Installing Identity Certificates, page 6-11
- Saving Your Configuration, page 6-12
- Ensuring Trust Point Configurations Persist Across Reboots, page 6-12
- Monitoring and Maintaining CA and Certificates Configuration, page 6-13

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.

Caution

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 of the switch, follow these steps:

	Command	Purpose
ep 1	<pre>switch# config terminal switch(config)#</pre>	Enters configuration mode.
ep 2	<pre>switch(config)# hostname SwitchA</pre>	Configures the host name (SwitchA) of the switch.
ep 3	SwitchA(config)# ip domain-name example.com	Configures the IP domain name (example.com) of the switch.

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, follow these steps:

Command	Purpose
switch# config terminal switch(config)#	Enters configuration mode.
switch(config) # crypto key generate rsa	Generates an RSA key-pair with the switch FQDN as the default label and 512 as the default modulus. By default, the key is no exportable.
	 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. Note The maximum number of key-pair you can configure on a switch is 16.
switch(config) # crypto key generate rsa label SwitchA modulus 768	Generates an RSA key-pair with the label SwitchA and modulus 768. Valid modulus values are 512, 768, 1024, 1536, and 2048 By default, the key is not exportable.
switch(config)# crypto key generate rsa exportable	FQDN as the default label and 512 as the default modulus. The key is exportable.
	Caution The exportability of a key-pair cannot be changed after key-pair generation.
	Note Only exportable key-pairs can be exported in PKCS#12 format.

Creating a Trust Point CA Association

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

	Command	Purpose
<pre>switch(config)# crypto ca trustpoint adm switch(config-trustpoint)#</pre>		Declares a trust point CA that the switch should trust and enters trust point configuration submode.
		Note The maximum number of trust point you can declare on a switch is 16.
	switch(config)# no crypto ca trustpoint admin-ca	Removes the trust point CA.
	<pre>switch(config-trustpoint)# enroll terminal</pre>	Specifies manual cut-and-paste certificate enrollment (default).
		Note Manual cut-and-paste certificate enrollment is the only method supported for enrollment.
	switch(config-trustpoint)# rsakeypair SwitchA	Specifies the label of the RSA key-pair to be associated to this trust point for the purpose of enrollment. It was generated earlier in the "Generating an RSA Key-Pair" section on page 6-6. Only one RSA key-pair can be specified per CA.
	switch(config-trustpoint)# no rsakeypair SwitchA	Disassociates the RSA key-pair from the tru point (default).
	<pre>switch(config-trustpoint)# end switch#</pre>	Exits trust point configuration submode.
	<pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration to ensure the configuration is persistent across reboots.

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.



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 the certificate of the CA by cutting and pasting the certificate from an e-mail message or a website, follow these steps:

MRTWEAYDVOOTEWII.VX.TuVXRba2EvEiAOBcNUBAcTCU.ThbmdbbG9vZTEOMAwGA1UE	
 input (cut & paste) CA certificate (chain) in PEM format; end the input with a line containing only END OF INPUT : BEGIN CERTIFICATE MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRI1jK0ZejANBgkqhkiG9w0BAQUFADCB kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklo MRIWEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBACTCUJhbmdhbG9yZTEOMAwGA1UE ChMFQ21zY28xEzARBgNVBAsTCm51dHN0b3JhZ2UxEjAQBgNVBAMTCUFWYXJuYSBD QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN AQkBFhFhbWFuZGt1QGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3J1MQ4wDAYDVQQKEwVDaXNjbzETMBEG A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHz1uNccNM87ypyzwuoSNZX0MpeRXXI OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs L0FwYXJUYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3N1LTA4XEN1cnRFbnJv 	mode.
BQUAA0EAHv6UQ+8me399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea NBG7E0oN66zex0E0EEfG1Vs6mXp1//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	Use the same nen declaring the n number of trust n authenticate to



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.

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 6-14), 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.

```
Note
```

You must authenticate the CA before configuring certificate revocation checking.

To configure certificate revocation checking methods, follow these steps:

Command	Purpose
<pre>switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#</pre>	Declares a trust point CA that the switch should trust and enters trust point configuration submode.
<pre>switch(config-trustpoint)# ocsp url http://crlcheck.cisco.com</pre>	Specifies the url for OCSP to use to check fo revoked certificates.
switch(config-trustpoint)# no ocsp url http://crlcheck.cisco.com	Removes the URL for OCSP.
<pre>switch(config-trustpoint)# revocation-check oscp</pre>	Specifies OCSP as the revocation checking method to be employed during verification o peer certificates issued by the same CA as that of this trust point.
	Note The OSCP URL must be configured before specifying OSCP as a revocation checking method.
<pre>switch(config-trustpoint)# revocation-check crl</pre>	Specifies CRL (default) as the revocation checking method to be employed during verification of peer certificates issued by the same CA as that of this trust point.
<pre>switch(config-trustpoint)# revocation-check crl oscp</pre>	Specifies CRL as the first revocation checking method and OCSP as the next method. If the CRL method fails (for example, due to the CRL is not found or has expired) to be used during verification of pee certificates issued by the same CA as that of this trust point, then OSCP is used.
	Note The OSCP URL must be configured before specifying OSCP as a revocation checking method.
<pre>switch(config-trustpoint)# revocation-check none</pre>	Does not check for revoked certificates.
switch(config-trustpoint)# no revocation-check	Reverts to default method.

Generating Certificate Requests

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 certaineates from the eri, fonot a these steps.	To generate a reque	st for signed	l certificates fron	n the CA, follow	these steps:
--	---------------------	---------------	---------------------	------------------	--------------

Command	Purpose
<pre>switch# config terminal switch(config)#</pre>	Enters configuration mode.
<pre>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: Vegas-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:172.22.31.162 The certificate request will be displayed BEGIN CERTIFICATE REQUEST MIIBqzCCARQCAQAwHDEAMBgGA1UEAXMRVmVnYXMtMS5jaXNjby5jb20wgZ&wDQYJ KoZIhvcNAQEBBQADgYOAMIGJAOGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8r141KY 0JC6MaNNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkScZxV8S VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCEMGbmJ2MTIzMDYGCSqGSIb3DQEJ DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt PftrNcWUE/pw6HayfQ12T3ecgNwe12d15133YBF2bktExiI6U188nT0jg1XMjja8 8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0= END CERTIFICATE REQUEST</pre>	Generates a certificate request fo an authenticated CA. Note The challenge password i 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.

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 textusing the CLI import facility.

To install an identity certificate received from the CA by e-mail or through a web browser, follow these steps:

Command	Purpose
<pre>switch# config terminal switch(config)#</pre>	Enters configuration mode.
<pre>switch(config)# crypto ca import admin-ca certificate input (cut & paste) certificate in PEM format: BEGIN CERTIFICATE MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAADDANBgkqhkiG9w0BAQUFADCBkDEgMB4G CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAk1OMRIwEAYD VQQIEw1LYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ21z Y28xEzARBgNVBAsTCm51dHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBAMBwxGjAYBgNVBAMTEVZ1Z2FzLTEu Y21zY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8y1ncWyw5E08rJ47 g1xr42/s19IRIb/8udU/cj9jS5fK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw GYIRVmVnYXMtMS5jaXNjby5jb22HBKwMbfiwHQJDVR00BBYEFKCLi+2sspWEfgrR bhWm1Vy09jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW pIGTMIGQMSAwHgYJKoZ1hvcNAQkBFhFhbWFuZGt1QGNpc2NvLmNvbTELMAkGA1UE BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3J1MQ4w DAXDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh cm5hIENBghAFYNKJrLQ21E9JEiWMrR16MGSGA1UdHwRkMGIwLqAsoCqGKGh0dHA6 Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmE1MjBDQS5jcmwMKAuoCyGKmZpBGU6 Ly9cXHNzZS0wOFxDZXJ0RW5yb2xSXEFwYXJUYSUyMENBLmNybDEIgYIKwYBBQUH AQEEfjB8MDSGCCSGAQUFBZAChi9odHRw0i8vc3N1LTA4L0N1cnRFbnJvbGwvc3N1 LTA4X0FwYXJUYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZm1sZTovL1xcc3N1LTA4 XEN1cnRFbnJvbGwcc3N1LTA4X0FwYXJUYSUyMENBLmNydDAHEgkqhki69w0BAQUF AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSUDDCOCUZUUTgrpnTqVpPyejtsyflw E36c1zu4WsExREqxbTk8ycx7V5o= END CERTIFICATE</pre>	 Prompts you to cut and paste the identity certificate for the CA name admin-ca. Note The maximum number of identify certificates you can configure on a switch is 16.

Saving Your Configuration

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

Ensuring Trust Point Configurations Persist Across Reboots

The trust point configuration is a normal Cisco NX-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 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 are 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 and save it to an external server (see the "Exporting and Importing Identity Information in PKCS#12 Format" section on page 6-13).



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 6-13
- Configuring a CRL, page 6-14
- Deleting Certificates from the CA Configuration, page 6-14
- Deleting RSA Key-Pairs from Your Switch, page 6-15
- Displaying Key-Pair and CA Information, page 6-16

Exporting and Importing Identity Information in PKCS#12 Format

You can export the identity certificate along with the RSA key-pair and CA certificate (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 later import the certificate and RSA key-pair to recover from a system crash on your switch or when you replace the supervisor modules.

Note

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

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

Command	Purpose
switch# config terminal switch(config)#	Enters configuration mode.
switch(config) # crypto ca export admin-ca pkcs12 bootflash:adminid.p12 nbv123	Exports the identity certificate and associated key-pair and CA certificates for trust point admin-ca to the file bootflash:adminid.p12 in PKCS#12 format, protected using password nbv123.
switch(config)# exit switch#	Returns to EXEC mode.
switch# copy bootflash:adminid.p12 tftp:adminid.p12	Copies the PKCS#12 format file to a TFTP server.

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

	Command	Purpose
Step 1	<pre>switch# copy tftp:adminid.p12 bootflash:adminid.p12</pre>	Copies the PKCS#12 format file from a TFTP server.

Γ

	Command	Purpose	
Step 2	<pre>switch# config terminal switch(config)#</pre>	Enters configuration mode.	
Step 3	<pre>switch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123</pre>	Imports the identity certificate and associated key-pair and CA certificates for trust point admin-ca from the file bootflash:adminid.p12 in PKCS#12 format, protected using password nbv123.	

<u>Note</u>

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 import the CRL from a file to a trust point, follow these steps:

	Command	Purpose
Step 1	<pre>switch# copy tftp:adminca.crl bootflash:adminca.crl</pre>	Downloads the CRL.
Step 2	<pre>switch# config terminal switch(config)#</pre>	Enters configuration mode.
Step 3	<pre>switch(config)# crypto ca crl request admin-ca bootflash:adminca.crl</pre>	Configures or replaces the current CRL with the one specified in the file.

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. 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, follow these steps:

	Command	Purpose
Step 1	<pre>switch# config t switch(config)#</pre>	Enters configuration mode.
Step 2	<pre>switch(config)# crypto ca trustpoint myCA</pre>	Enters trustpoint configuration submode.
Step 3	<pre>switch(config-trustpoint)# delete ca-certificate</pre>	Deletes the CA certificate or certificate chain.

	Command	Purpose
Step 4	<pre>switch(config-trustpoint)# delete certificate</pre>	Deletes the identity certificate.
	<pre>switch(config-trustpoint)# delete certificate force</pre>	Forces the deletion of the identity certificate.
		Note If the identity certificate being deleted is the last-most or only identity certificate in the device, you must use the force option 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 5	<pre>switch(config-trustpoint)# end switch#</pre>	Returns to EXEC mode.
Step 6	<pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration to ensure the configuration is persistent across reboots.

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:

Command	Purpose
switch# config terminal switch(config)#	Enters configuration mode.
<pre>switch(config)# crypto key zeroize rsa MyKey</pre>	Deletes the RSA key-pair whose label is MyKey.
switch(config)# end switch#	Returns to EXEC mode.
switch# copy running-config startup-config	Copies the running configuration to the startup configuration to ensure the configuration is persistent across reboots

S. Note

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 6-10.

Displaying Key-Pair and CA Information

To view key-pair and CA information, use the following commands in EXEC mode:

Command	Purpose
switch# show crypto key mypubkey rsa	Displays information about the switch's RSA public keys.
switch# show crypto ca certificates	Displays information on CA and identity certificates.
switch# show crypto ca crl	Displays information about CA CRLs.
switch# show crypto ca trustpoints	Displays information about CA trust points.

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 6-16
- Downloading a CA Certificate, page 6-19
- Requesting an Identity Certificate, page 6-24
- Revoking a Certificate, page 6-30
- Generating and Publishing the CRL, page 6-33
- Downloading the CRL, page 6-34
- Importing the CRL, page 6-36

Configuring Certificates on the MDS Switch

trustpoint: myCA; key: revokation methods: crl

Vegas-1(config)#

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

```
Step 1 Configure the switch FQDN.
    switch# config t
    Enter configuration commands, one per line. End with CNTL/Z.
    switch(config)# switchname Vegas-1
    Vegas-1(config)#
Step 2 Configure the DNS domain name for the switch.
    Vegas-1(config)# ip domain-name cisco.com
    Vegas-1(config)#
Step 3 Create a trust point.
    Vegas-1(config)# crypto ca trustpoint myCA
    Vegas-1(config)# do show crypto ca trustpoints
```

Step 4 Create an RSA key-pair for the switch.

```
Vegas-1(config)# crypto key generate rsa label myKey exportable modulus 1024
Vegas-1(config)# do show crypto key mypubkey rsa
key label: myKey
key size: 1024
exportable: yes
```

Vegas-1(config)#

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

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

- Step 6 Download the CA certificate from the Microsoft Certificate Service web interface (see the "Downloading a CA Certificate" section on page 6-19)
- **Step 7** Authenticate the CA that you want to enroll to the trust point.

```
Vegas-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
MRIwEAYDVQQIEw1LYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
\texttt{ChMFQ21zY28xEzARBgNVBAsTCm51dHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD}
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
{\tt AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xejAQBgNVBAgTCUth}
{\tt cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3J1MQ4wDAYDVQQKEwVDaXNjbzETMBEG}
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJOXBhcm5hIENBMFwwDOYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
----END CERTIFICATE----
 END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
Do you accept this certificate? [yes/no]:y
Vegas-1(config)#
Vegas-1(config) # do show crypto ca certificates
Trustpoint: myCA
CA certificate 0:
subject= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Yourcompany/O
U=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.
 - Vegas-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: Vegas-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----MIIBqzCCARQCAQAwHDEaMBqGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ KoZIhvcNAQEBBQADqY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8r141KY 0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt PftrNcWUE/pw6HayfQl2T3ecgNwel2dl5133YBF2bktExiI6Ul88nTOjglXMjja8 8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0= ----END CERTIFICATE REQUEST----

Vegas-1(config)#

- Step 9 Request an identity certificate from the Microsoft Certificate Service web interface (see the "Requesting an Identity Certificate" section on page 6-24).
- **Step 10** Import the identity certificate.

```
Vegas-1(config) # crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
----BEGIN CERTIFICATE-----
{\tt MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G}
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAk1OMRIwEAYD
VQQIEw1LYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ21z
Y28xEzARBgNVBAsTCm51dHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w
NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZ1Z2FzLTEu
Y21zY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFgFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
\texttt{pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE}
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3J1MQ4w
DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh
cm5h1ENBghAFYNKJrLQZ1E9JEiWMrR16MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6
Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmE1MjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AOEEfiB8MDsGCCsGAOUFBzAChi9odHRwOi8vc3N1LTA4L0N1cnRFbnJvbGwvc3N1
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3N1LTA4
XEN1cnRFbnJvbGxcc3N1LTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyf1w
E36cIZu4WsExREgxbTk8vcx7V5o=
----END CERTIFICATE-----
Vegas-1(config)# exit
Vegas-1#
```

Step 11 Verify the certificate configuration.

```
Vegas-1# show crypto ca certificates
Trustpoint: myCA
certificate:
subject= /CN=Vegas-1.cisco.com
issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/OU
=netstorage/CN=Aparna CA
serial=0A338EA100000000074
notBefore=Nov 12 03:02:40 2005 GMT
notAfter=Nov 12 03:12:40 2006 GMT
MD5 Fingerprint=3D:33:62:3D:B4:D0:87:A0:70:DE:A3:87:B3:4E:24:BF
purposes: sslserver sslclient ike
CA certificate 0:
subject= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Yourcompany/O
U=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 12 Save the certificate configuration to the startup configuration.
```

Vegas-1# copy running-config startup-config

Downloading a CA Certificate

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

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



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

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

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

tetrieve The CA Certificate Or Certificate Revocation List tetrieve The CA Certification path to allow your computer to trust certificates issued from this certification authority. is not necessary to manually installed the CA A certification path will be installed for you the Download Computer II the file information below the control of the product of the trust of the trust certificates issued for on open or the download: Computer II the file information below the control of the product of the control of the product of the trust of the trust the file Computer II the file information below the control of the control		
stall this CA certification path to allow your computer to trust certificates issued from this certification authority. is not necessary to manually install the CA. A certification path will be installed for you those file to download: CA Certificate: Current (Apama CA) © DER encoded or © Dem § ave Cancel More Info	Microsoft Certificate Services Apama CA	<u>Home</u>
is not necessary to manually install the CA A certification path will be installed for you thoose file to download: A Certificate: Current [Aparina CA] © DER encoded or ● Bas Download CA certificate Download CA certificate Download Latest certificate re Download latest certificate re	Retrieve The CA Certificate Or Certificate Revocation List	
is not necessary to manually install the CA A certification path will be installed for you thoose file to download: A Certificate: Current [Aparina CA] © DER encoded or ● Bas Download CA certificate Download CA certificate Download Latest certificate re Download latest certificate re		
A certification path will be installed for you A contribution path will be installed for you Choose file to download: C DER encoded or C DER encoded or	nstall this CA certification path to allow your computer to trust certificates issued from this certification authority.	
	CA certification path will be installed for you Choose file to download: CA Certificate: Current [Aparna CA] C DER encoded or C Bas Download CA certificate Download (CA certificate Download latest certificate re Down	ause the

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

stall this CA certification path to allow	Certificate		ion authority.
is not necessary to manually install th CA certification path will be installed fc	Show: <a>All>	Value	from this certification authority, because the
Corrent (Aparta CA)	Version Serial number Signature algorithm Issuer Valid from Valid from Valid to Subject Public key	V3 0560 D289 ACB4 1994 4F49 1 shaIRSA Aparna CA, nestorage, Cisco 04 Mei 2007 4:25:17 Aparna CA, nestorage, Cisco RSA (S12 Bits)	
		Edit Properties	

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

Install this CA certification path to allow It is not necessary to manually install th CA certification path will be installed fo Choose file to download: CA Certificate: Current (Apama CA) C DER encoded or (Download CA certifica Download Latest certifica	Version Signature alg Signature alg Valid from Valid from Public key Control Subject	ath xport Wizard Format the Format the format the format you want to use: PER encoded binary X.509 (.CER) Bage-64 encoded X.509 (.CER) Cytyptographic Message Syntax Stan produe al certificates in the certi presonal information Exchange PKC	dard - PKCS #7 Certificates (.P78) ficebon pedti if possible	cause the
		Induse of certificates in the certificates are consistent of the certificates and the certificates are consistent of the certificates are consist	fication path if possible s IE 5.0, NT 4.0 SP4 or above)	

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

<i>Microsoft</i> Certificate Services Aparna CA	Home	4
Retrieve The CA Certificate Or Certi Install this CA certification path to allow It is not necessary to manually install th CA certification path will be installed for Choose file to download: CA Certificate: Current [Aparna CA] C DER encoded or (Download CA certificat Download CA certificat Download CA certificat	Certificate Revocation List Certificate General Details Certificate Export Show: Cal> Field Version Specify the name of the file you want to export Subject Valid from Valid to Subject Ditestcerts/aparmaCA.cer Bgowse	
		144760

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

	Iertificate	? ×
stall this CA certification path to allow	General Details Certification Path	ion authority.
is not necessary to manually install th A certification path will be installed fc	Show: <all></all>	from this certification authority, because the
hoose file to download: A Certificate: C DER encoded or Download CA certifica Download latest certifica	Version Serial numbe Signature ale Bissuer Vvald from Vvald from Subject Public Key	Completing the Certificate Export Wizard You have successfully completed the Certificate Export weard. You have specified the following settings: The Name Diverse Export Keys Diverse Include all certification peth. No File Format: Base64
		< Back Finish Cancel

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 Click the **Request a certificate** radio button on the Microsoft Certificate Services web interface and click **Next**.



Step 2 Click the Advanced request radio button and click Next.

Microsoft Certificate Services Apama CA Home	*
Choose Request Type	
Please select the type of request you would like to make:	
O User certificate request: Web Browser Certificate E-Mail Protection Certificate	
e Advanced request	
Next >	
	144766

Step 3 Click 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	<u>Home</u>
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 >	

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 6-10 and "Configuring Certificates on the MDS Switch" section on page 6-16).

Microsoft Certificate Services Aparna CA Ho	ome
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:	
VqyHOvEXAgHBAAGgTEAVEBAAGhEIG90BCGCwCBHG Base64 Encoded KozItureNAQEEBCADGTEAKF6QeBojGBOXCHH Certificate Request PftrNeUUZ/pw6HagfQ12T3ecqNwe12d15133YBF2: (PKCS #ID or #F) Ba23DNDNBNBENEAKbANEUTLENUTEFJXcgjingPN END CERTIFICATE REQUEST	
Additional Attributes:	
Attributes:	
Submit >	Ī
	*

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

Microsoft Certificate Services Aparna CA	<u>Home</u>
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	
	1

Step 6 The CA administrator approves the certificate request.

Ertification Authority						<u> </u>
Action ⊻iew	1 🖸 🗟	ß				
Tree	Request ID	Binary Request	Request Disposition Message	Request Submission Date		Reques
Certification Authority (Local) Aparna CA Issued Certificates Pending Requests Failed Requests	116	BEGIN NE	Taken Under Submission	All Tasks Issue Refresh Help	SSE-00\IUSR_SS.	
Contains operations that can be performe		t.				Þ

Step 7 Click 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 Check on a pending certificate
Next >

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

Microsoft Certificate Services Aparna CA Home	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 >		
	ļ	144772
		4

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

flicrosoft Certificate Services Aparna CA	Home
ertificate Issued	
ne certificate you requested was issued to you.	
ODER encoded or @ Base 64 encoded	
Download CA certificate Download CA certification path	

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

Microsoft Certificate Services Aparna CA		Home
		IIIIIE
Certificate Issued		
The certificate you requested was issued t	о уои.	
ODER encoded or . ● Base 6	File Download	
Download CA certificate Download CA certification path	Some files can harm your computer. If the file information below looks supplicour, or you do not hilly trust the source, do not open or save the file.	
	File name: certnew.cer	
	File type: Security Certificate	
	From: 10.76.45.108	
	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	

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

Microsoft Fertificate Services - Microsoft Internet Explorer provided		
General Details Certification Path		
A Show: <all></all>		▼ 🖉 Go Links »
		A
Field Value		Home
Version V3 Serial number 0A33 8EA1 0000 0000 0074		
Signature algorithm sha1R5A		
Issuer Aparna CA, netstorage, Cisco Valid from 12 Nopember 2005 8:32:40		
Valid from 12 Nopember 2005 8:32:40		
Subject Vegas-1.cisco.com		
Public key RSA (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:	
	C DER encoded binary X.509 (.CER)	
Edit Properties Copy to File	Bage-64 encoded X.509 (.CER)	
	C Gryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
OK	\square Include all certificates in the certification path if possible	
	C Bersonal Information Exchange - PKC5 #12 (,PFX)	
	\square Indude all certificates in the certification path if possible	
	Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)	
	\square Delete the private <u>key</u> if the export is successful	
	< Back Next > C	ancel
		144775
		<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**.

2	Microsoft Certificate Service Certificate	es - Microsoft Internet Explorer pro	vided I	Cisco Systems, I	nc.					_ 🗆 ×	1
-	General Details Certification	Path]						1
A	Show: <all></all>	-							• @	Go Links »	1
П	Field	Value								Anter Home	1
Ш	- Version	V3								<u>110111e</u>	
Ш	Serial number	0A33 8EA1 0000 0000 0074 sha1R5A									
Ш	Issuer Valid from	Aparna CA, netstorage, Cisco									
Ш	Valid from	12 Nopember 2005 8:32:40 12 Nopember 2006 8:42:40									
Ш	Valid to	Vegas-1.cisco.com	_								
Ш	Public key	R5A (1024 Bits)	•								
Ш		l.	ertifica	Export Wizard				×			
Ш				Export							
Ш				ecify the name of th	file you want to e	xport					
Ш											
Ш	1			name:							
Ш		Edit Properties Copy to F	ļ	testcerts\myID.ce			Browse				
Ш											
L											
L											
L											
L											
L											
L						< <u>B</u> ack	Next > Can	cel			G
		_									144776
										~	14





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 BEGIN CERTIFICATE MI IEADCCA6ggMv IBagIKGjOOQAAAAAAAAAAAAAAAAAAAAABGKGVVABAQUFADCBkDEgMB4G CSgGSIb3DQEJARYRYWihbmRrZUBjaXNjby5jb20xCzAJBgNUBAYTAk1OMRIwEAYD UQQIEwILYXJuYXRha2ExEjAQBgNUBACTCUJhbmdhbG9vZTEOMAwGAIUEChMFQ21z Y28xEzARBgNUBASTCn51dHN0b3JhZ2UxEjAQBgNUBAMTCUJFwYXJuYSBDQTAeFw0w NTExMTIwMzAyMDBaFC0bJhZ2UxEjAQBgNUBAMTCUJFwYXJuYSBDQTAeFw0w NTExMTIWZAyMDBaFC0bJhZ2UxEjAQBgNUBAMTCUJFwYXJuYSBDQTAeFw0w NTExMTIWZAyMDBaFC0bJhZ2UxEjAQBgNUBAMTCUJFwYXJuYSBDQTAeFw0w NTExMTIWZAYHDGFMA0GCSgGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C Qq1WkjKjSICdqLfKSeJSmNCQujGpzcuKsZPFXjP2UoiyeCYE8yJncWwACdjQu41C qq1WkjKjSICdqLfKSeJSmNCQujGpzcuKsZPFXjP2UoiyeCYE8yJncWwACBB8rJ47 g1x+42/sI9IRIb/8udU/cj9jSSfKK56koa7xWWAu8rDfz8jMCnIM4WiaY/2Q4Gb x7RifdU06uFqFZEgs17/FLash9Lzku/DAQABo41CE2CCAg8wJQVDUR0RAQH/BBsv GYIRUmUnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDUR00BBYEFKCLi+2sspWEfgrR bhWmUUy09jngMIHMBgNUHSMEgcQwgcGAFCc08kaDG6wjTEUNjsKYUB0LFnxxoYGW JGTMTGQMSAwHgYJKoZIbwcNAQBBFhFhbWFUZG1JQGNpc2NvLmNbTELMAKGA1UE BhMCSU4xEjAQBgNUBAgTCUthcm5hdGFrYTESMBAGA1UEAxMJQmFuZ2Fsb3JIMQ4w DAYDUQQKEwUDaXNjb2ETMBEGA1UECXMKbmU0c3RvcmFnZTESMBAGA1UEAXMJQXBh cm5hiENBghAFYNKJrLQZIE9JEiWMrR16MGSGA1UdHwRHMGIWLAAsoCQGKGCMQHA6 Ly9czUtMDgvQ2UyUEUucm9sbC9BcGFybmE1MjBDQS5jcmwMKAnoCyGKAZpbGU6 Ly9czUtMDgvQ2UyUEUucm9sbC9BcGFybmE1MjBDQS5jcTwMMKAnoCyGKAZpbGU6 Ly9c2KIMZZSM0FxDZXJ0RW5yb2xSEFWYXJUYSUJMENBLmNybDLCBigYIKwBBQUH AAQEFjB8MDsGCCSGAQUFB2AChi9odHRw0i8uc3NLITA4L0N1ncRFbnJvbGwvc3N1 LIA4X0FwYXJUYSUJMENELmNydDA9BggrBgEFBQcwA0YZZNISZTouLixcc3N1LITA4 XENIcnFbnJvbGxcc3NLILA4X0FwYXJUYSUJMENELmNydDANBgkhkiG?v0BAQUF AANBADbGBGsbe7GNLM9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqUpPyejtsyflw E36c1Zu4WESEXREqxbItM8ycx7U5o= END CERTIFICATE	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.

e	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
	5 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
	E 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
	E 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
	E 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
	Sec. 110	SSE-08\IUSR_SS	BEGIN CERTI	17b3067600000000006e	10/18/2005 12:21 AM
	See 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
	Sec. 113	SSE-08\IUSR_SS	BEGIN CERTI	4aafff2e00000000071	10/31/2005 12:32 AM
	Sec. 114	SSE-08\IUSR_SS	BEGIN CERTI	78cc6e6c00000000072	11/8/2005 11:26 PM
	E 115	SSE-08\IUSR_SS	BEGIN CERTI	78e3416100000000073	11/8/2005 11:51 PM
	116	SSE-08\ILISP_SS	BEGIN CERTI	0a338ea1000000000074	11/12/2005 8:32 AM

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

e	Request ID	Requester Name	Binary Certificate	Serial Number	Certificate Effective Da
Certification Authority (Local)	89	SSE-08\IUSR_SS	BEGIN CERTI	786263d0000000000059	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	94	SSE-08\IUSR_SS	BEGIN CERTI	7c32783700000000005e	9/20/2005 10:14 PM
	95	SSE-08\IUSR_SS	BEGIN CERTI	7c32784700000000005f	9/20/2005 10:14 PM
	98		DE CIVI CED TI	al xt10000062	9/21/2005 12:18 AM
	99	ertificate Revocatio	n	?×p0000063	9/22/2005 1:45 AM
	100	Are you sure you want I	to revoke the selected	certificate(s)? 0000064	9/27/2005 2:44 AM
	101			0000065	9/27/2005 2:45 AM
	E 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	1		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	5F413d200000000000006c	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	11ea380600000000006f	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	SSE-08\IUSR_SS	BEGIN CERTI	78e34161000000000073	11/8/2005 11:51 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.

Control (Codd) Calificates	ectiveDate 🔄	Certificate Effect	Serial Number	Binary Certificate	Requester Name	Request ID	
Aparna CA Ign 16 SSE-08[IUSR_SS BEGIN CERTI 5db140d30000000010 6/30/2005 Revoked certificates Ign 16 SSE-08[IUSR_SS BEGIN CERTI 5db140d30000000011 6/30/2005 Pending Requests Ign 18 SSE-08[IUSR_SS BEGIN CERTI 16db147000000000011 7/14/2005 Paled Requests Ign 35E-08[IUSR_SS BEGIN CERTI 261/392400000000011 7/14/2005 Ign 21 SSE-08[IUSR_SS BEGIN CERTI 264/272000000000015 7/14/2005 Ign 22 SSE-08[IUSR_SS BEGIN CERTI 264/272000000000015 7/14/2005 Ign 23 SSE-08[IUSR_SS BEGIN CERTI 264/272000000000016 7/14/2005 Ign 24 SSE-08[IUSR_SS BEGIN CERTI 264/27200000000017 7/14/2005 Ign 24 SSE-08[IUSR_SS BEGIN CERTI 264/27200000000017 7/14/2005 Ign 26 SSE-08[IUSR_SS BEGIN CERTI 264/57600000000017 7/14/2005 Ign 26 SSE-08[IUSR_SS BEGIN CERTI 264/57600000000017 7/14/2005	27 AM	6/30/2005 3:27	5dae53cd00000000000f	BEGIN CERTI	SSE-08\IUSR_SS	15	ertification Authority (Local)
Revolved certificates	30 AM	6/30/2005 3:30	5db140d3000000000010	BEGIN CERTI	SSE-08\IUSR_SS	16	
Issued Certificates Issued Cerificates Issued Cerificates	46 AM	6/30/2005 5:46	5e2d7c1b00000000011	BEGIN CERTI	SSE-08\IUSR_SS	17	
Failed Requests 20 SSE-08[IUSR_SS BEGIN CERTI 262b520200000000014 7/14/2005 C2 SSE-08[IUSR_SS BEGIN CERTI 2634772000000000015 7/14/2005 C2 SSE-08[IUSR_SS BEGIN CERTI 2634772000000000016 7/14/2005 C2 SSE-08[IUSR_SS BEGIN CERTI 2634772000000000017 7/14/2005 C2 SSE-08[IUSR_SS BEGIN CERTI 2264577000000000017 7/14/2005 C2 SSE-08[IUSR_SS BEGIN CERTI 2267537000000000018 7/14/2005 C2 SSE-08[IUSR_SS BEGIN CERTI 2267537000000000018 7/14/2005 C2 SSE-08[IUSR_SS BEGIN CERTI 2267537000000000018 7/12/2005 C2 SSE-08[IUSR_SS BEGIN CERTI 2267537000000000018 7/28/2005 C2 SSE-08[IUSR_SS BEGIN CERTI 7556878000000000015 7/28/2005 C2 SSE-08[IUSR_SS BEGIN CERTI 7556878000000000016 8/4/2005 C2 SSE-08[IUSR_SS BEGIN CERTI <t< td=""><td>I AM</td><td>7/8/2005 3:21 A</td><td>16db4f8f000000000012</td><td>BEGIN CERTI</td><td>SSE-08\IUSR_SS</td><td>18</td><td></td></t<>	I AM	7/8/2005 3:21 A	16db4f8f000000000012	BEGIN CERTI	SSE-08\IUSR_SS	18	
Image: Section of the section of th	00 AM	7/14/2005 5:00	261c392400000000013	BEGIN CERTI	SSE-08\IUSR_SS	19	Pending Requests
Image: 22 SSE-08[UJSR_SS BEGIN CERTI 2635b00000000000016 7/14/2005 Image: 23 SSE-08[UJSR_SS BEGIN CERTI 264504000000000017 7/14/2005 Image: 24 SSE-08[UJSR_SS BEGIN CERTI 24450400000000019 7/14/2005 Image: 25 SSE-08[UJSR_SS BEGIN CERTI 348045700000000019 7/14/2005 Image: 26 SSE-08[UJSR_SS BEGIN CERTI 3480457000000000011 7/28/2005 Image: 28 SSE-08[UJSR_SS BEGIN CERTI 755b89800000000011 7/28/2005 Image: 29 SSE-08[UJSR_SS BEGIN CERTI 755b89800000000011 7/28/2005 Image: 29 SSE-08[UJSR_SS BEGIN CERTI 755b89800000000011 7/29/2005 Image: 29 SSE-08[UJSR_SS BEGIN CERTI 146511c700000000011 8/4/2005 Image: 20 SSE-08[UJSR_SS BEGIN CERTI 1465116700000000016 8/4/2005 Image: 20 SSE-08[UJSR_SS BEGIN CERTI 1464510700000000016 8/4/2005 Image: 20 SSE-08[UJSR_SS BEGIN CERTI 1464510500000000002 8/17/2005	16 AM	7/14/2005 5:16	262b520200000000014	BEGIN CERTI	SSE-08\IUSR_SS	20	Failed Requests
Image: Second LUSR_SS. BEGIN CERTI 2648504000000000017 7/14/2005 Image: Second LUSR_SS. BEGIN CERTI 22/635700000000018 7/14/2005 Image: Second LUSR_SS. BEGIN CERTI 368cbf700000000018 7/14/2005 Image: Second LUSR_SS. BEGIN CERTI 368cbf700000000018 7/28/2005 Image: Second LUSR_SS.	27 AM	7/14/2005 5:27	2634c7f200000000015	BEGIN CERTI	SSE-08\IUSR_SS	21	
Image: 24 SSE-08[IUSR_5S BEGIN CERTI 2427635700000000018 7/14/2005 Image: 25 SSE-08[IUSR_5S BEGIN CERTI 368abf700000000019 7/19/2005 Image: 26 SSE-08[IUSR_5S BEGIN CERTI 568abf700000000011 7/28/2005 Image: 27 SSE-08[IUSR_5S BEGIN CERTI 725a80780000000011 7/28/2005 Image: 28 SSE-08[IUSR_5S BEGIN CERTI 725a807800000000011 8/2/20205 Image: 29 SSE-08[IUSR_5S BEGIN CERTI 148511c7000000000011 8/2/2005 Image: 20 SSE-08[IUSR_5S BEGIN CERTI 1496116700000000011 8/4/2005 Image: 20 SSE-08[IUSR_5S BEGIN CERTI 14961167000000000011 8/4/2005 Image: 20 SSE-08[IUSR_5S BEGIN CERTI 14961167000000000011 8/4/2005 Image: 20 SSE-08[IUSR_5S BEGIN CERTI 14961167000000000011 8/4/2005 Image: 20 SSE-08[IUSR_5S BEGIN CERTI 14961167000000000012 8/17/2005 Image: 20 SSE-08[IUSR_5S BEGIN CERTI 146433a000000000021 8/17/2005<	28 AM	7/14/2005 5:28	2635b00000000000016	BEGIN CERTI	SSE-08\IUSR_SS	22	
Image: 25 SSE-08[IUSE_SS BEGIN CERTI 3/88cbf7000000000019 7/19/2005 Image: 26 SSE-08[IUSE_SS BEGIN CERTI 64b5f5f00000000011 7/28/2005 Image: 27 SSE-08[IUSE_SS BEGIN CERTI 725b89480000000011 7/28/2005 Image: 28 SSE-08[IUSE_SS BEGIN CERTI 725b894800000000011 7/28/2005 Image: 29 SSE-08[IUSE_SS BEGIN CERTI 735b894800000000011 8/3/2005 Image: 29 SSE-08[IUSE_SS BEGIN CERTI 148511c700000000001 8/4/2005 Image: 30 SSE-08[IUSE_SS BEGIN CERTI 147170100000000001 8/4/2005 Image: 31 SSE-08[IUSE_SS BEGIN CERTI 147170100000000000000000 8/4/2005 Image: 32 SSE-08[IUSE_SS BEGIN CERTI 146c4b5000000000000000000000000000 8/17/2005 Image: 33 SSE-08[IUSE_SS BEGIN CERTI 146c4b5000000000000000000000000000000000000	48 AM	7/14/2005 5:48	2648504000000000017	BEGIN CERTI	SSE-08\IUSR_SS	23	
Image: Section 2 SSE-08/LUSR_SS BEGIN CERTI 6e4b5/5f00000000001a 7/28/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 735a80780000000001b 7/28/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 735a80780000000001b 7/28/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 735a80780000000001c 7/29/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 149511c70000000001c 8/4/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 1497170100000000001c 8/4/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 1467455000000000002 8/17/2005 Image: SSE-08/LUSR_SS BEGIN CERTI <td>:51 PM</td> <td>7/14/2005 11:51</td> <td>2a27635700000000018</td> <td>BEGIN CERTI</td> <td>SSE-08\IUSR_SS</td> <td>24</td> <td></td>	:51 PM	7/14/2005 11:51	2a27635700000000018	BEGIN CERTI	SSE-08\IUSR_SS	24	
Image: 27 SSE-08[IUSE_SS BEGIN CERTI 725b89d80000000001b 7/28/2005 Image: 28 SSE-08[IUSE_SS BEGIN CERTI 73588780000000001c 7/29/2005 Image: 29 SSE-08[IUSE_SS BEGIN CERTI 74581270000000001c 7/29/2005 Image: 29 SSE-08[IUSE_SS BEGIN CERTI 1455112700000000001c 8/4/2005 Image: 29 SSE-08[IUSE_SS BEGIN CERTI 1467170100000000001 8/4/2005 Image: 29 SSE-08[IUSE_SS BEGIN CERTI 146745b500000000001 8/4/2005 Image: 29 SSE-08[IUSE_SS BEGIN CERTI 146745b500000000001 8/17/2005 Image: 20 SSE-08[IUSE_SS BEGIN CERTI 146745b5000000000002 8/17/2005 Image: 20 SSE-08[IUSE_SS BEGIN CERTI 146745b500000000000002 8/17/2005 Image: 20 SSE-08[IUSE_SS BEGIN CERTI 146745b40000000000000002 8/17/2005 Image: 20 SSE-08[IUSE_SS BEGIN CERTI 146745b400000000000000000000000000000000000	29 AM	7/19/2005 3:29	3f88cbf700000000019	BEGIN CERTI	SSE-08\IUSR_SS	25	
Image: 28 SSE-08[IUSR_SS BEGIN CERTI 735a887800000000001 7/29/2005 Image: 29 SSE-08[IUSR_SS BEGIN CERTI 148511c700000000001 8/3/2005 Image: 29 SSE-08[IUSR_SS BEGIN CERTI 1497170100000000001 8/4/2005 Image: 20 SSE-08[IUSR_SS BEGIN CERTI 14671701000000000001 8/4/2005 Image: 20 SSE-08[IUSR_SS BEGIN CERTI 1467455500000000001 8/4/2005 Image: 20 SSE-08[IUSR_SS BEGIN CERTI 1466ce80b00000000020 8/17/2005 Image: 20 SSE-08[IUSR_SS BEGIN CERTI 146c433a000000000021 8/17/2005 Image: 20 SSE-08[IUSR_SS BEGIN CERTI 146c433a0000000000021 8/17/2005 Image: 20 SSE-08[IUSR_SS BEGIN CERTI 3455c80000000000021 8/17/2005 Image: 20 SSE-08[IUSR_SS BEGIN CERTI 34545dd000000000000000015 9/9/2005 Image: 20 SSE-08[IUSR_SS BEGIN CERTI 34545dd00000000000000002 9/9/2005 Image: 20	58 AM	7/28/2005 3:58	6e4b5f5f0000000001a	BEGIN CERTI	SSE-08\IUSR_SS	26	
29 SSE-08/LUSR_SS BEGIN CERTI 148511c70000000001d 8/3/2005 30 SSE-08/LUSR_SS BEGIN CERTI 14717010000000001e 8/4/2005 31 SSE-08/LUSR_SS BEGIN CERTI 147170100000000001e 8/4/2005 32 SSE-08/LUSR_SS BEGIN CERTI 486ce0b0000000002 8/17/2005 33 SSE-08/LUSR_SS BEGIN CERTI 46c4b3ab00000000021 8/17/2005 34 SSE-08/LUSR_SS BEGIN CERTI 46c4b3ab00000000021 8/17/2005 35 SSE-08/LUSR_SS BEGIN CERTI 1485ccb000000000021 8/17/2005 36 SSE-08/LUSR_SS BEGIN CERTI 36045dd00000000002f 9/9/2005 36 SSE-08/LUSR_SS BEGIN CERTI 37645dd000000000002f 9/9/2005 36 SSE-08/LUSR_SS BEGIN CERTI 37645dd000000000002f 9/9/2005 36 SSE-08/LUSR_SS BEGIN CERTI 37645dd000000000002f 9/9/2005 36 SSE-08/LUSR_SS	:54 PM	7/28/2005 10:54	725b89d80000000001b	BEGIN CERTI	SSE-08\IUSR_SS	27	
Image: SSE-08/LUSR_SS BEGIN CERTI 14a7170100000000001e 8/4/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 14a7170100000000001e 8/4/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 14f45b5000000000002 8/17/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 46ce80b0000000002 8/17/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 4ce4a3aa00000000021 8/17/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 4ce4a3aa00000000002 9/1/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 3f645d000000000002 9/9/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 3f645d000000000002 9/9/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 3f645d0000000000002 9/9/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 3f645d0000000000002 9/9/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 3f645d0000000000002 9/9/2005	33 AM	7/29/2005 3:33	735a88780000000001c	BEGIN CERTI	SSE-08\IUSR_SS	28	
Image: SSE-08/LUSR_SS BEGIN CERTI 14fc45b500000000001f 8/4/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 486ce80b00000000002 8/17/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 486ce80b00000000002 8/17/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 4ca4a3aa00000000002 8/17/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 4ca4a3aa000000000002 9/1/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 3f0845dd00000000003 9/9/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 3f019b7e000000000042 9/9/2005	30 PM	8/3/2005 11:30	148511c700000000001d	BEGIN CERTI	SSE-08\IUSR_SS	29	
R SSE-08[IUSR_SS BEGIN CERTI 486ce80b000000000020 8/17/2009 R SSE-08[IUSR_SS BEGIN CERTI 4c4+33a0000000000021 8/17/2009 R SSE-08[IUSR_SS BEGIN CERTI 4c3+433a0000000000021 8/17/2009 R SSE-08[IUSR_SS BEGIN CERTI 4c3+52c8000000000021 9/1/2005 R SSE-08[IUSR_SS BEGIN CERTI 3f0495d000000000003f 9/9/2005 R SSE-08[IUSR_SS BEGIN CERTI 3f0495d00000000003f 9/9/2005 R SSE-08[IUSR_SS BEGIN CERTI 3f0495d00000000002 9/9/2005	07 AM	8/4/2005 12:07	14a7170100000000001e	BEGIN CERTI	SSE-08\IUSR_SS	30	
Image: SSE-08/LUSR_SS BEGIN CERTI 4ca+a3aa000000000021 8/17/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 1aa55c6e00000000002f 9/1/2005 Image: SSE-08/LUSR_SS BEGIN CERTI 3f0845d00000000003f 9/9/22005 Image: SSE-08/LUSR_SS BEGIN CERTI 3f0845d000000000002f 9/9/22005 Image: SSE-08/LUSR_SS BEGIN CERTI 3f0845d000000000002f 9/9/22005	DAM	8/4/2005 1:40 A	14fc45b500000000001f	BEGIN CERTI	SSE-08\IUSR_SS	31	
R 55E-08\IUSR_55 BEGIN CERTI 1aa55c8e00000000002f 9/1/2005 R 63 S5E-08\IUSR_55 BEGIN CERTI 3f0845dd00000000003f 9/9/2005 R 66 S5E-08\IUSR_55 BEGIN CERTI 3f619b7e000000000042 9/9/2005	58 AM	8/17/2005 3:58	486ce80b00000000020	BEGIN CERTI	SSE-08\IUSR_SS	32	
Image: SSE-081USR_SS BEGIN CERTI 3f0845dd00000000003f 9/9/2005 Image: SSE-081USR_SS BEGIN CERTI 3f619b7e00000000042 9/9/2005	:37 PM	8/17/2005 11:37	4ca4a3aa000000000021	BEGIN CERTI	SSE-08\IUSR SS	33	
66 55E-08\IUSR_55BEGIN CERTI 3f619b7e00000000042 9/9/2005	36 PM	9/1/2005 11:36	1aa55c8e0000000002f	BEGIN CERTI	SSE-08\IUSR SS	47	
	L AM	9/9/2005 1:11 A	3f0845dd0000000003f	BEGIN CERTI	SSE-08\IUSR_SS	63	
		9/9/2005 2:48 A	3f619b7e000000000042		· -		
82 55E-08\IUSR 55BEGIN CERTI 6313c46300000000052 9/16/2005	09 AM	9/16/2005 1:09	6313c46300000000052	BEGIN CERTI	SSE-08\IUSR SS	82	
		9/20/2005 10:20			. –		
		9/20/2005 11:20			· -		
		11/12/2005 8:32	0a338ea1000000000074		. –	116	

Generating and Publishing the CRL

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

2			•	B 2			
_	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	-, (,	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
1	- Failed Requ	ests	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	1aa55c8e00000000002f	9/1/2005 11:36 PM
			100 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
			100 96	SSE-08\IUSR_SS	BEGIN CERTI	7c3861e3000000000060	9/20/2005 10:20 PM
			100 97	SSE-08\IUSR_SS	BEGIN CERTI	7c6ee351000000000061	9/20/2005 11:20 PM
			116	SSE-08\IUSR_SS	BEGIN CERTI	0a338ea100000000074	11/12/2005 8:32 AM

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	
- 📄 Issued Certificates	18	SSE-08\IUSR_SS	BEGIN CERTI	16db4f8f000000000012	7/8/2005 3:21 AM	
📄 Pending Requests	1 9	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\IUSB_SS	BEGIN CERTI	2648504000000000017	7/14/2005 5:48 AM	
	L2X 20					
Certif	icate Revocation Li				2005 11:51 PM	
Certif					2005 11:51 PM 2005 3:29 AM	
Certif	icate Revocation Li	st	n be used by clients. A	re you sure you want to publish	2005 3:29 AM	
Certif	icate Revocation Li	st	n be used by clients. A	re you sure you want to publish	2005 3:29 AM	
Certif	icate Revocation Li	st d CRL is still valid and ca	·	re you sure you want to publish	2005 3:29 AM a new CRL? 2005 3:58 AM	
	icate Revocation Li	st	·	re you sure you want to publish	a new CRL? 2005 3:29 AM 2005 3:58 AM 2005 10:54 PM 2005 3:33 AM 005 11:30 PM	
Certif	icate Revocation Li	st d CRL is still valid and ca	·	re you sure you want to publish	a new CRL? 2005 3:29 AM 2005 3:58 AM 2005 10:54 PM 2005 3:33 AM	
Certif	icate Revocation Li	st d CRL is still valid and ca Yes SSE-08\IUSR_SS	s No	14fc45b50000000001f	2005 3:29 AM 2005 3:58 AM 2005 1:54 PM 2005 3:33 AM 005 11:30 PM 005 11:30 PM 8/4/2005 1:40 AM	
Certif	The last publishe	st d CRL is still valid and ca SSE-08\IUSR_SS SSE-08\IUSR_SS	s No BEGIN CERTI BEGIN CERTI	14fc45b500000000001f 486ce80b00000000020	2005 3:29 AM 2005 3:29 AM 2005 3:356 AM 2005 10:54 PM 2005 11:30 PM 005 11:30 PM 005 11:30 PM 005 12:07 AM 8/4/2005 1:40 AM 8/17/2005 3:56 AM	
Certil (1)	The last publishe	st d CRL is still valid and ca SSE-08\IUSR_SS SSE-08\IUSR_SS	s No	14fc45b50000000001f	2005 3:29 AM 2005 3:58 AM 2005 1:54 PM 2005 3:33 AM 005 11:30 PM 005 11:30 PM 8/4/2005 1:40 AM	
Certif	The last publishe	st d CRL is still valid and ca Ver SSE-08/IUSR_SS SSE-08/IUSR_SS SSE-08/IUSR_SS SSE-08/IUSR_SS	s No BEGIN CERTI BEGIN CERTI BEGIN CERTI	14fc45b50000000001f 486ce80b0000000020 4ca4a3aa00000000021 1aa55c8e0000000002f	2005 3:29 AM 2005 3:29 AM 2005 3:356 AM 2005 10:54 PM 2005 11:30 PM 005 11:30 PM 005 11:30 PM 005 12:07 AM 8/4/2005 1:40 AM 8/17/2005 3:56 AM	
Certif	The last publishe	st d CRL is still valid and ca Ver SSE-08/IUSR_SS SSE-08/IUSR_SS SSE-08/IUSR_SS SSE-08/IUSR_SS	s No	14fc45b50000000001f 486ce80b0000000020 4ca4a3aa00000000021 1aa55c8e0000000002f	2005 3:29 AM 2005 3:358 AM 2005 3:58 AM 2005 3:35 AM 005 11:30 PM 005 11:30 PM 005 12:07 AM 8/17/2005 3:58 AM 8/17/2005 3:137 PM	
Certif	The last publishe	st d CRL is still valid and ca SSE-08\1USR_SS SSE-08\1USR_SS SSE-08\1USR_SS SSE-08\1USR_SS SSE-08\1USR_SS SSE-08\1USR_SS SSE-08\1USR_SS	No BEGIN CERTI BEGIN CERTI BEGIN CERTI	14fc45b50000000001f 486ce80b0000000020 4ca4a3aa00000000021 1aa55c8e0000000002f	2005 3:29 AM 2005 3:58 AM 2005 10:54 PM 2005 11:30 PM 005 11:30 PM 005 12:07 AM 8/4/2005 1:40 AM 8/17/2005 3:58 AM 8/17/2005 11:36 PM	
	The last publishe	st d CRL is still valid and ca SSE-08\1USR_SS SSE-08\1USR_SS SSE-08\1USR_SS SSE-08\1USR_SS SSE-08\1USR_SS SSE-08\1USR_SS SSE-08\1USR_SS	No BEGIN CERTI BEGIN CERTI BEGIN CERTI BEGIN CERTI BEGIN CERTI	14fc45b500000000001f 486ce80b00000000020 4ca4a3aa000000000021 1aa55c8e0000000002f 3f0845dd000000003f	2005 3:29 AM 2005 3:29 AM 2005 3:35 AM 2005 10:54 PM 2005 3:33 AM 005 11:30 PM 005 11:30 PM 8/17/2005 1:40 AM 8/17/2005 1:40 AM 9/1/2005 1:40 AM 9/1/2005 1:137 PM 9/1/2005 1:137 PM	
Certif	The last publishe	st d CRL is still valid and ca SSE-08(1USR_SS SSE-08(1USR_SS SSE-08(1USR_SS SSE-08(1USR_SS SSE-08(1USR_SS SSE-08(1USR_SS SSE-08(1USR_SS SSE-08(1USR_SS SSE-08(1USR_SS) SSE-08(1USR_SS)	No BEGIN CERTI BEGIN CERTI BEGIN CERTI	14fc45b500000000001f 486ce80b0000000020 4ca4a3aa0000000021 1aa55c8e0000000002f 3f619b7e0000000003f 3f619b7e00000000042	2005 3:29 AM 2005 3:29 AM 2005 3:356 AM 2005 10:54 PM 2005 11:30 PM 005 11:30 PM 005 11:40 AM 8/1/2005 11:36 PM 9/1/2005 11:36 PM 9/1/2005 11:13 PM 9/9/2005 1:11 AM	
Certif	The last publishe	st d CRL is still valid and ca SSE-08(IUSR_SS) SSE-08(IUSR_SS) SSE-08(IUSR_	No BEGIN CERTI BEGIN CERTI BEGIN CERTI BEGIN CERTI	14fc45b500000000001f 486ce80b0000000020 4ca4a3aa00000000021 1aa55c8e0000000002f 3f0845dd0000000003f 3f619b7e000000000042 6313c46300000000052	2005 3:29 AM 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 11:30 PM 005 1:40 AM 8/17/2005 3:58 AM 8/17/2005 3:58 AM 9/1/2005 11:36 PM 9/9/2005 1:11 AM 9/9/2005 1:10 AM	

Downloading the CRL

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

Step 1 Click 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 C Request a certificate C Check on a pending certificate	
Next >	
	*

Step 2 Click the Download latest certificate revocation list link.



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

Accertificate Or Certificate Revocation List istall this CA certification path to allow your computer to trust certificates issued from this certification authority. is not necessary to manually install the CA File Download Choose file to download: CA Certificate: Current [Aparna CA] Choose file to download CA Certificate: Current [Aparna CA] Choose file to download ca certificate Cownload CA certificate: Download Latest certificater Ownload Latest certificater Ownload latest certificater Open Save it to your computer?	<i>ficrosoft</i> Certificate Services Aparna CA		<u>Home</u>
is not necessary to manually install the CA A certification path will be installed for you choose file to download: A Certificate: Current [Aparna CA] © DER encoded or © Ba Download CA certificate Download CA certificate Download Latest certificate Cancel More Info	etrieve The CA Certificate Or Certificate R	evocation List	
A certification path will be installed for you hoose file to download: A Certificate: Current [Aparna CA] C DER encoded or DER encoded or Download CA certificate Download CA certificate Download Latest certificate Download L	stall this CA certification path to allow your co	mputer to trust certificates issued from this certification authority.	
choose file to download: * save this file. cA Certificate: File name: certrificate c DER encoded or • Ba File type: Certificate Download CA certificate: Would you like to open the file or save it to your computer? Download latest certificate: Image: Demonstrate the file or save it to your computer?	A cortification path will be installed for you	Some files can harm your computer. If the file information below	because the
File type: Centificate Revocation List From: 10.76.45.108 © DER encoded or © Ba Download CA certificate Would you like to open the file or save it to your computer? Download latest certificate r Open Save Cencel More Info		save this file.	
Download CA certificate Would you like to open the file or save it to your computer? Download latest certificate r Open Save Cancel	A Certificate: Current (Aparna CA)	File type: Certificate Revocation List	
Download CA certification p Would you like to open the file or save it to your computer? Download latest certificate r Image: Cancel More Info	ODER encoded or ●Ba		
		Would you like to open the file or save it to your computer?	
	Download latest certificate r		
		The Lutter and provide advantage with a wine of the online	

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

Microsoft Certificate Services Apama CA			Home
Retrieve The CA Certificate Or Certificate F	Revocation List		
nstall this CA certification path to allow your co	emputer to trust certificates	issued from this certification authority.	
t is not necessary to manually install the CA c CA certification path will be installed for you a	ile Download Save As	om this certifica	tion authority, because the
Choose file to download: CA Certificate: Current (Apama CA)	Save As	. ← 🗈 🗳 💷-	
	History		
⊂ DER encoded or ● Base			
Download CA certificate Download CA certification pa	Desktop		
Download latest certificate re	documents		
	My Computer		
	My Network P Save as type:	aparnaCA.crl	Save Cancel
1		, ,	//

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



Importing the CRL

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

```
Copy the CRL file to the MDS switch bootflash.
Step 1
        Vegas-1# copy tftp:apranaCA.crl bootflash:aparnaCA.crl
Step 2
        Configure the CRL.
        Vegas-1# config t
        Vegas-1(config) # crypto ca crl request myCA bootflash:aparnaCA.crl
        Vegas-1(config)#
Step 3
        Display the contents of the CRL.
        Vegas-1(config) # do sh crypto ca crl myCA
        Trustpoint: myCA
        CRL:
        Certificate Revocation List (CRL):
                Version 2 (0x1)
                Signature Algorithm: sha1WithRSAEncryption
                Issuer: /emailAddress=admin@yourcompany.com/C=IN/ST=Karnatak
        Yourcompany/OU=netstorage/CN=Aparna CA
                Last Update: Nov 12 04:36:04 2005 GMT
                Next Update: Nov 19 16:56:04 2005 GMT
                CRL extensions:
                    X509v3 Authority Key Identifier:
                    keyid:27:28:F2:46:83:1B:AC:23:4C:45:4D:8E:C9:18:50:1
```

1.3.6.1.4.1.311.21.1:

Revoked Certificates: Serial Number: 611B09A10000000002 Revocation Date: Aug 16 21:52:19 2005 GMT Serial Number: 4CDE464E00000000003 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: 5349AD460000000000A Revocation Date: Jun 27 23:47:22 2005 GMT CRL entry extensions: X509v3 CRL Reason Code: CA Compromise Serial Number: 53BD173C0000000000B Revocation Date: Jul 4 18:04:01 2005 GMT CRL entry extensions: X509v3 CRL Reason Code: Certificate Hold Serial Number: 591E7ACE0000000000C 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: 5DAB77130000000000 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: 5E2D7C1B00000000011 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: 6E4B5F5F0000000001A
       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: 148511C7000000001D
       Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 14A717010000000001E
       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: 7C6EE3510000000061
       Revocation Date: Sep 20 18:52:30 2005 GMT
    Serial Number: 0A338EA100000000074
                                             <-- Revoked identity certificate
       Revocation Date: Nov 12 04:34:42 2005 GMT
    Signature Algorithm: sha1WithRSAEncryption
       0b:cb:dd:43:0a:b8:62:1e:80:95:06:6f:4d:ab:0c:d8:8e:32:
        44:8e:a7:94:97:af:02:b9:a6:9c:14:fd:eb:90:cf:18:c9:96:
        29:bb:57:37:d9:1f:d5:bd:4e:9a:4b:18:2b:00:2f:d2:6e:c1:
        1a:9f:1a:49:b7:9c:58:24:d7:72
```

Ø Note

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

Maximum Limits

Table 6-1 lists the maximum limits for CAs and digital certificate parameters.

Table 6-1 Maximum Limits for CA and Digital Certificate

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

Default Settings

Table 6-2 lists the default settings for CAs and digital certificate parameters.

Table 6-2 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