CHAPTER 35

Configuring Certificate Authorities and Digital Certificates

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

This chapter includes the following sections:

About CAs and Digital Certificates

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

Purpose of CAs and Digital Certificates

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

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

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

To validate the signature of the CA, the receiver must first know the CA's public key. Normally this process is handled out-of-band or through an operation done at installation. For instance, most web browsers are configured with the public keys of several CAs by default. The Internet Key Exchange (IKE), an essential component of IPsec, can use digital signatures to scalably authenticate peer devices before setting up security associations.

Trust Model, Trust Points, and Identity CAs

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

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

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

RSA Key-Pairs and Identity Certificates

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

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

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

- A trust point corresponds to a specific CA that the MDS switch trusts for peer certificate verification for any application (such as IKE or SSH).
- An MDS switch can have many trust points and all applications on the switch can trust a peer certificate issued by any of the trust point CAs.
- A trust point is not restricted to a specific application.
- An MDS switch enrolls with the CA corresponding to the trust point to obtain an identity certificate. You can enroll your switch with multiple trust points thereby obtaining a separate identity certificate from each trust point. The identity certificates are used by applications depending upon the purposes specified in the certificate by the issuing CA. The purpose of a certificate is stored in the certificate as certificate extensions.
- When enrolling with a trust point, you must specify an RSA key-pair to be certified. This key-pair must be generated and associated to the trust point before generating the enrollment request. The association between the trust point, key-pair, and identity certificate is valid until it is explicitly removed by deleting the certificate, key-pair, or trust point.
- The subject name in the identity certificate is the fully qualified domain name for the MDS switch.
- You can generate one or more RSA key-pairs on a switch and each can be associated to one or more trust points. But no more than one key-pair can be associated to a trust point, which means only one identity certificate is allowed from a CA.
- If multiple identity certificates (each from a distinct CA) have been obtained, the certificate that an application selects to use in a security protocol exchange with a peer is application specific (see the “IPsec Digital Certificate Support” section on page 36-7 and the “SSH Authentication Using Digital Certificates” section on page 37-18).
- You do not need to designate one or more trust points for an application. Any application can use any certificate issued by any trust point as long as the certificate purpose satisfies the application requirements.
- You do not need more than one identity certificate from a trust point or more than one key-pair to be associated to a trust point. A CA certifies a given identity (name) only once and does not issue multiple certificates with the same subject name. If you need more than one identity certificate for a CA, then define another trust point for the same CA, associate another key-pair to it, and have it certified, provided CA allows multiple certificates with the same subject name.

Multiple Trusted CA Support

An MDS switch can be configured to trust multiple CAs by configuring multiple trust points and associating each with a distinct CA. With multiple trusted CAs, you do not have to enroll a switch with the specific CA that issued a certificate to a peer. Instead, you configure the switch with multiple trusted CAs that the peer trusts. A switch can then use a configured trusted CA to verify certificates offered by a peer that were not issued by the same CA defined in the identity of the switch.

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

PKI Enrollment Support

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

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

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

Manual Enrollment Using Cut-and-Paste Method

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

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

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

OCSP Support

Online Certificate Status Protocol (OCSP) facilitates online certificate revocation checking. You can specify an OCSP URL for each trust point. Applications choose the revocation checking mechanisms in a specified order. The choices are CRL, OCSP, none, or a combination of these methods.

Import and Export Support for Certificates and Associated Key Pairs

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

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

Configuring CAs and Digital Certificates

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

- Generating Certificate Requests, page 35-10
- Installing Identity Certificates, page 35-11
- Ensuring Trust Point Configurations Persist Across Reboots, page 35-12
- Monitoring and Maintaining CA and Certificates Configuration, page 35-13

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

Step 1	`switch# config terminal`
	`switch(config)#`
		Enters configuration mode.

Step 2	`switch(config)# hostname SwitchA`	Configures the host name (SwitchA) of the switch.
Step 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
Step 1	switch# **config terminal** switch(config)#	Enters configuration mode.
Step 2	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 not 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-pairs 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**	Generates an RSA key-pair with the switch 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
Step 1	switch(config)# **crypto ca trustpoint admin-ca** switch(config-trustpoint)#	Declares a trust point CA that the switch should trust and enters trust point configuration submode. **Note** The maximum number of trust points you can declare on a switch is 16.
	switch(config)# **no crypto ca trustpoint admin-ca**	Removes the trust point CA.
Step 2	switch(config-trustpoint)# **enroll terminal**	Specifies manual cut-and-paste certificate enrollment (default). **Note** Manual cut-and-paste certificate enrollment is the only method supported for enrollment.
Step 3	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 35-6. Only one RSA key-pair can be specified per CA.
	switch(config-trustpoint)# **no rsakeypair SwitchA**	Disassociates the RSA key-pair from the trust point (default).
Step 4	switch(config-trustpoint)# **end** switch#	Exits trust point configuration submode.
Step 5	switch# **copy running-config startup-config**	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.

Note If the CA being authenticated is not a self-signed CA (that is, it is a subordinate CA to another CA, which itself may be a subordinate to yet another CA, and so on, finally ending in a self-signed CA), then the full list of the CA certificates of all the CAs in the certification chain needs to be input during the CA authentication step. This is called the *CA certificate chain* of the CA being authenticated. The maximum number of certificates in a CA certificate chain is 10.

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

	Command	Purpose
Step 1	switch# **config t** switch(config)#	Enters configuration mode.
Step 2	switch(config)# **crypto ca authenticate admin-ca** input (cut & paste) CA certificate (chain) in PEM format; end the input with a line containing only END OF INPUT : **-----BEGIN CERTIFICATE-----** **MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB** **kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO** **MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE** **ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD** **QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN** **AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth** **cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG** **A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN** **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**	Prompts you to cut and paste the certificate of the CA. Use the same name that you used when declaring the CA. **Note** The maximum number of trust points you can authenticate to a specific CA is 10.

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

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 35-14), 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

Step 1	`switch(config)#` **`crypto ca trustpoint admin-ca`**
	`switch(config-trustpoint)#`
		Declares a trust point CA that the switch should trust and enters trust point configuration submode.

Step 2	`switch(config-trustpoint)#` **`ocsp url http://crlcheck.cisco.com`**	Specifies the for OCSP to use to check for revoked certificates.
	`switch(config-trustpoint)#` **`no ocsp url http://crlcheck.cisco.com`**	Removes the URL for OCSP.
Step 3	`switch(config-trustpoint)#` **`revocation-check oscp`**	Specifies OCSP as the revocation checking method to be employed during verification of 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.
	`switch(config-trustpoint)#` **`revocation-check crl`**	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.
	`switch(config-trustpoint)#` **`revocation-check crl oscp`**	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 peer 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.
	`switch(config-trustpoint)#` **`revocation-check none`**	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 certificates from the CA, follow these steps:

	Command	Purpose
Step 1	switch# **config terminal** switch(config)#	Enters configuration mode.
Step 2	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----- MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY 0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8 8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0= -----END CERTIFICATE REQUEST-----	Generates a certificate request for an authenticated CA. **Note** The challenge password is not saved with the configuration. This password is required in the event that your certificate needs to be revoked, so you must remember this password.

Installing Identity Certificates

You receive the identity certificate from the CA by e-mail or through a web browser in base64 encoded text form. You must install the identity certificate from the CA by cutting and pasting the encoded text using 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
Step 1	switch# **config terminal** switch(config)#	Enters configuration mode.
Step 2	switch(config)# **crypto ca import admin-ca certificate** input (cut & paste) certificate in PEM format: **-----BEGIN CERTIFICATE-----** **MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G** **CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD** **VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz** **Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w** **NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu** **Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C** **dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47** **glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb** **x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw** **GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR** **bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW** **pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE** **BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w** **DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh** **cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6** **Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6** **Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH** **AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl** **LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4** **XENlcnRFbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF** **AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw** **E36cIZu4WsExREqxbTk8ycx7V5o=** **-----END CERTIFICATE-----**	Prompts you to cut and paste the identity certificate for the CA named admin-ca. **Note** The maximum number of identify certificates you can configure on a switch is 16.

Ensuring Trust Point Configurations Persist Across Reboots

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

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

We also recommend that you create a password protected backup of the identity certificates nd save it to an external server (see the "Exporting and Importing Identity Information in PKCS#12 Format" section on page 35-13).

Note 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 35-13
- Configuring a CRL, page 35-14
- Deleting Certificates from the CA Configuration, page 35-14
- Deleting RSA Key-Pairs from Your Switch, page 35-15
- Displaying Key-Pair and CA Information, page 35-15

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 bootflash:*filename* 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

Step 1	`switch# config terminal`
	`switch(config)#`
		Enters configuration mode.

Step 2	`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.

Step 3	`switch(config)# exit`
	`switch#`
		Returns to EXEC mode.

Step 4	`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	`switch# copy tftp:adminid.p12 bootflash:adminid.p12`	Copies the PKCS#12 format file from a TFTP server.

Step 2	`switch# config terminal`
	`switch(config)#`
		Enters configuration mode.

Step 3	`switch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123`	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.

Note :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	`switch# `**`copy tftp:adminca.crl`**
	`bootflash:adminca.crl`
		Download the CRL.

Step 2	`switch# `**`config terminal`**
	`switch(config)#`
		Enters configuration mode.

Step 3	`switch(config)# `**`crypto ca crl request admin-ca`**
	`bootflash:adminca.crl`
		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. Then after deleting the identity certificate, you can disassociate the RSA key-pair from a trust point. The certificate deletion is necessary to remove expired or revoked certificates, certificates whose key-pairs are compromised (or suspected to be compromised) or CAs that are no longer trusted.

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

	Command	Purpose

Step 1	`switch# `**`config t`**
	`switch(config)#`
		Enters configuration mode.

Step 2	`switch(config)# `**`crypto ca trustpoint myCA`**	Enters trustpoint configuration submode.

Step 3	`switch(config-trustpoint)# `**`delete`**
	`ca-certificate`
		Deletes the CA certificate or certificate chain.

Step 4	`switch(config-trustpoint)# `**`delete certificate`**	Deletes the identity certificate.

	`switch(config-trustpoint)# `**`delete certificate`**
	`force`
		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	`switch(config-trustpoint)# `**`end`**
	`switch#`
		Returns to EXEC mode.

Step 6	`switch# `**`copy running-config startup-config`**	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

Step 1	`switch# config terminal`
	`switch(config)#`
		Enters configuration mode.

Step 2	`switch(config)# crypto key zeroize rsa MyKey`	Deletes the RSA key-pair whose label is MyKey.

Step 3	`switch(config)# end`
	`switch#`
		Returns to EXEC mode.

Step 4	`switch# copy running-config startup-config`	Copies the running configuration to the startup configuration to ensure the configuration is persistent across reboots.

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 35-10.

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 35-16
- Downloading a CA Certificate, page 35-19
- Requesting an Identity Certificate, page 35-23
- Revoking a Certificate, page 35-29
- Generating and Publishing the CRL, page 35-32

- Downloading the CRL, page 35-33
- Importing the CRL, page 35-35

Configuring Certificates on the MDS Switch

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

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 35-19)

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
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO
MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
```

```
AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3J1MQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
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-----
MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
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 35-23).

Step 10 Import the identity certificate.

```
Vegas-1(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD
VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz
Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w
NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu
Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6
Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4
XENlcnRFbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----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=0A338EA1000000000074
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
```

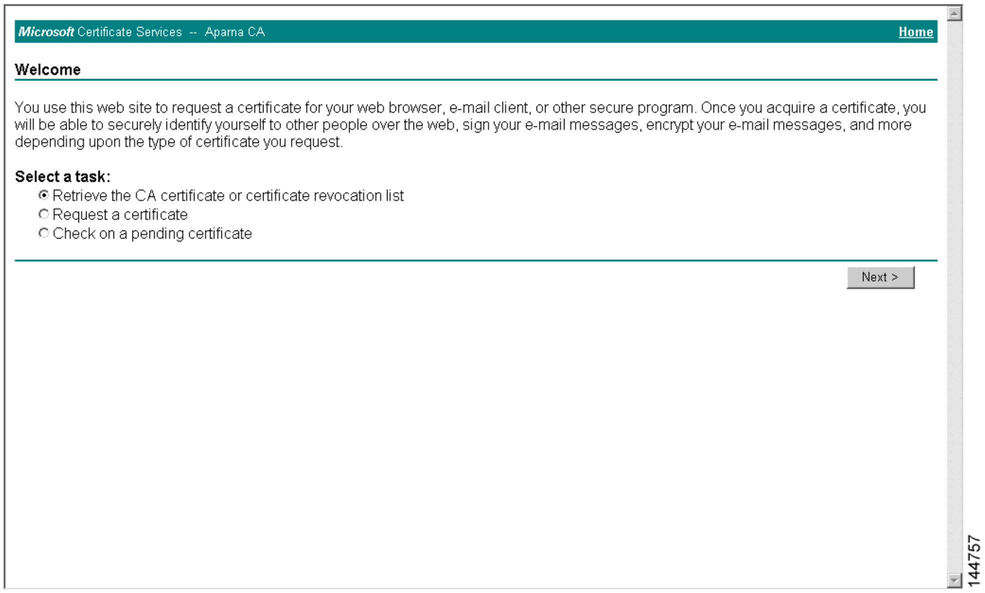
Step 12 Save the certificate configuration to the startup configuration.

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



Microsoft Certificate Services -- Aparna CA Home

Welcome

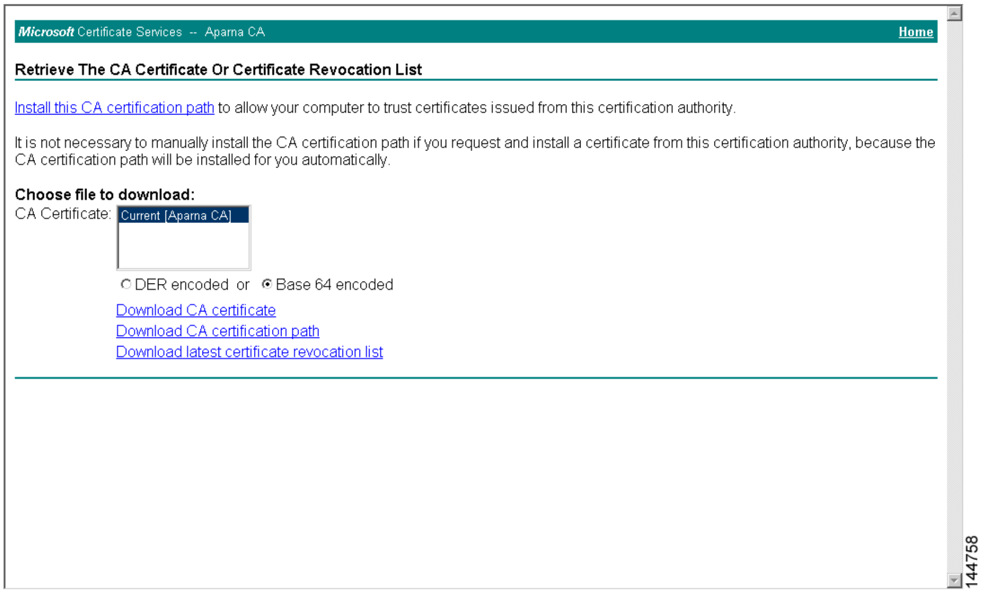
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the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

Select a task:

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

144757

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



Microsoft Certificate Services -- Aparna CA 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:

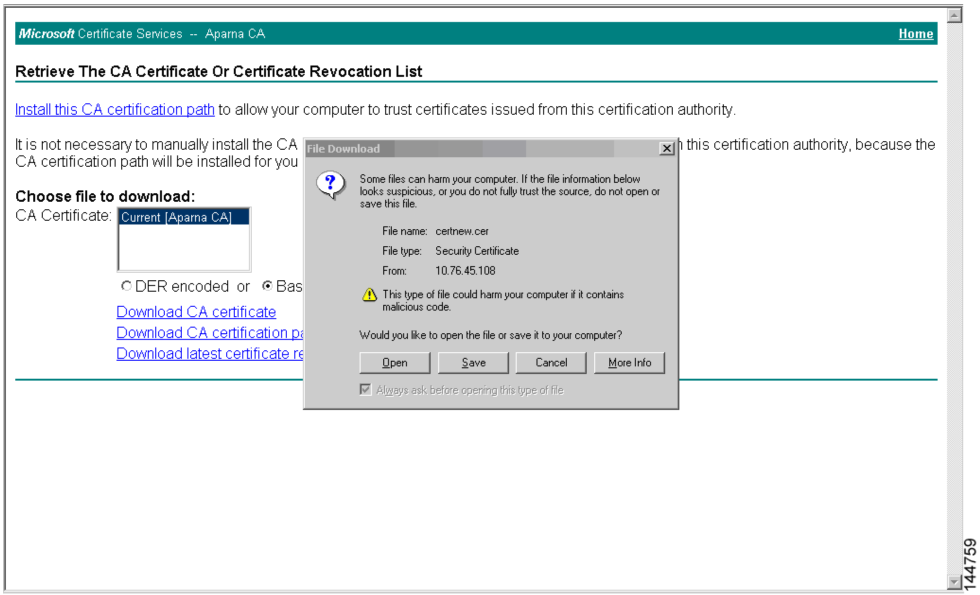
CA Certificate: Current [Aparna CA]

○ DER encoded or ● Base 64 encoded

Download CA certificate
Download CA certification path
Download latest certificate revocation list

144758

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



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 … this certification authority, because the CA certification path will be installed for you …

Choose file to download:
CA Certificate: Current [Aparna CA]

○ DER encoded or ● Bas…
Download CA certificate
Download CA certification pa…
Download latest certificate re…

File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: certnew.cer
File type: Security Certificate
From: 10.76.45.108

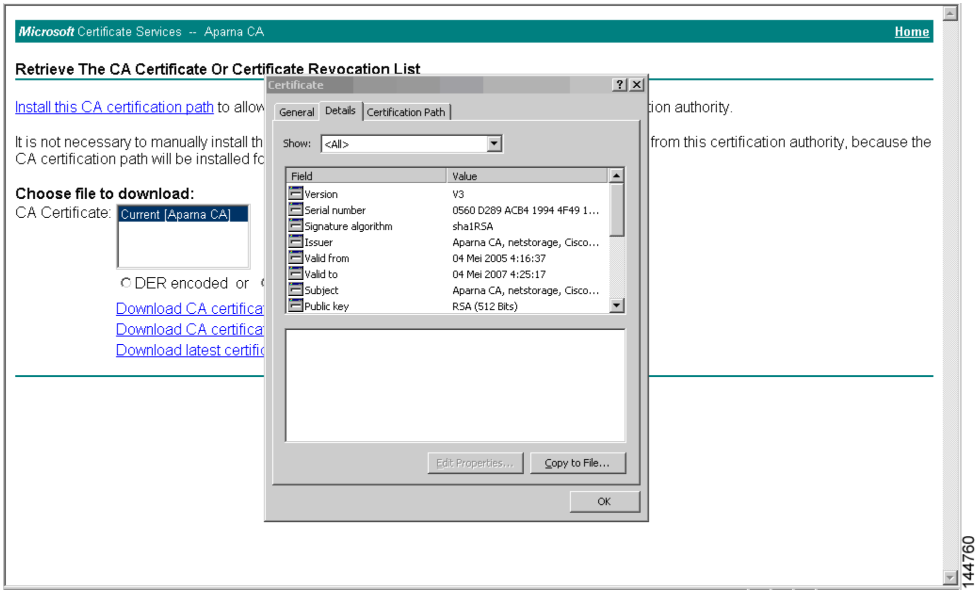
This type of file could harm your computer if it contains malicious code.

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



Microsoft Certificate Services -- Aparna CA **Home**

Retrieve The CA Certificate Or Certificate Revocation List

Install this CA certification path to allow … ion authority.

It is not necessary to manually install th… from this certification authority, because the CA certification path will be installed fo…

Choose file to download:
CA Certificate: Current [Aparna CA]

○ DER encoded or …
Download CA certifica…
Download CA certifica…
Download latest certifi…

Certificate

General | Details | Certification Path

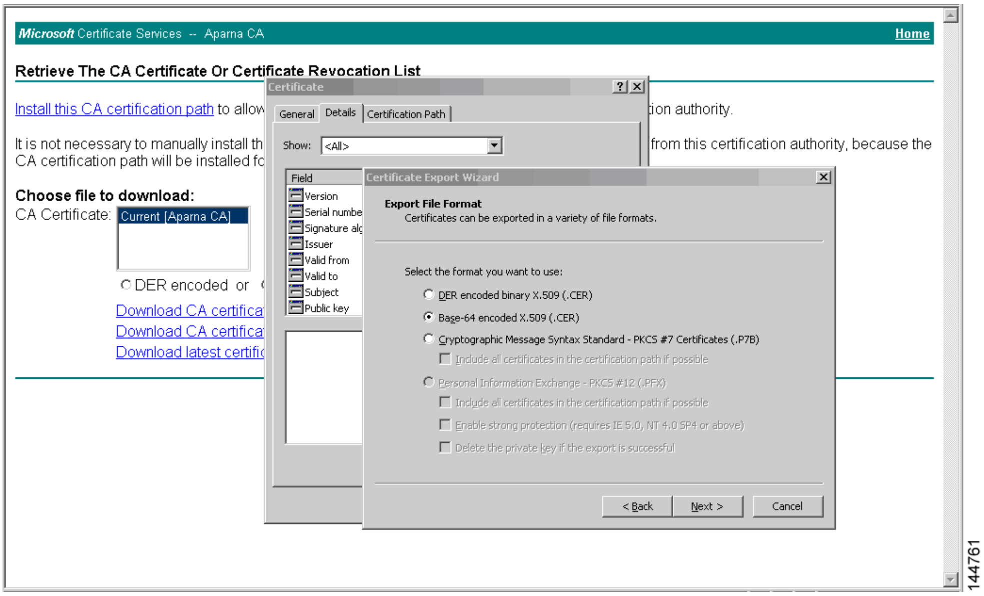
Show: <All>

Field	Value
Version	V3
Serial number	0560 D289 ACB4 1994 4F49 1...
Signature algorithm	sha1RSA
Issuer	Aparna CA, netstorage, Cisco...
Valid from	04 Mei 2005 4:16:37
Valid to	04 Mei 2007 4:25:17
Subject	Aparna CA, netstorage, Cisco...
Public key	RSA (512 Bits)

Edit Properties... | Copy to File...

OK

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



Microsoft Certificate Services -- Aparna CA — Home

Retrieve The CA Certificate Or Certificate Revocation List

Install this CA certification path to allow ... tion authority.

It is not necessary to manually install th... from this certification authority, because the CA certification path will be installed fo...

Choose file to download:

CA Certificate: Current [Aparna CA]

○ DER encoded or ○

Download CA certifica...

Download CA certifica...

Download latest certifi...

Certificate — General | Details | Certification Path — Show: <All>

Field: Version, Serial numbe..., Signature alg..., Issuer, Valid from, Valid to, Subject, Public key

Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

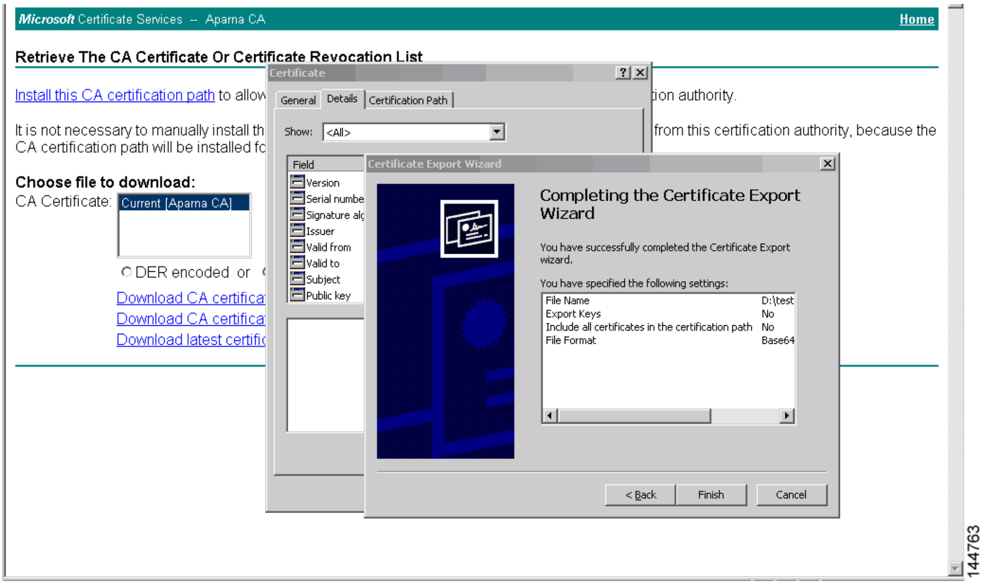
○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

□ Delete the private key if the export is successful

Step 6 Click the **Finish** button on the Certificate Export Wizard dialog box.



Microsoft Certificate Services -- Aparna CA — Home

Retrieve The CA Certificate Or Certificate Revocation List

Install this CA certification path to allow ... tion authority.

It is not necessary to manually install th... from this certification authority, because the CA certification path will be installed fo...

Choose file to download:

CA Certificate: Current [Aparna CA]

○ DER encoded or ○

Download CA certifica...

Download CA certifica...

Download latest certifi...

Certificate — General | Details | Certification Path — Show: <All>

Field: Version, Serial numbe..., Signature alg..., Issuer, Valid from, Valid to, Subject, Public key

Certificate Export Wizard

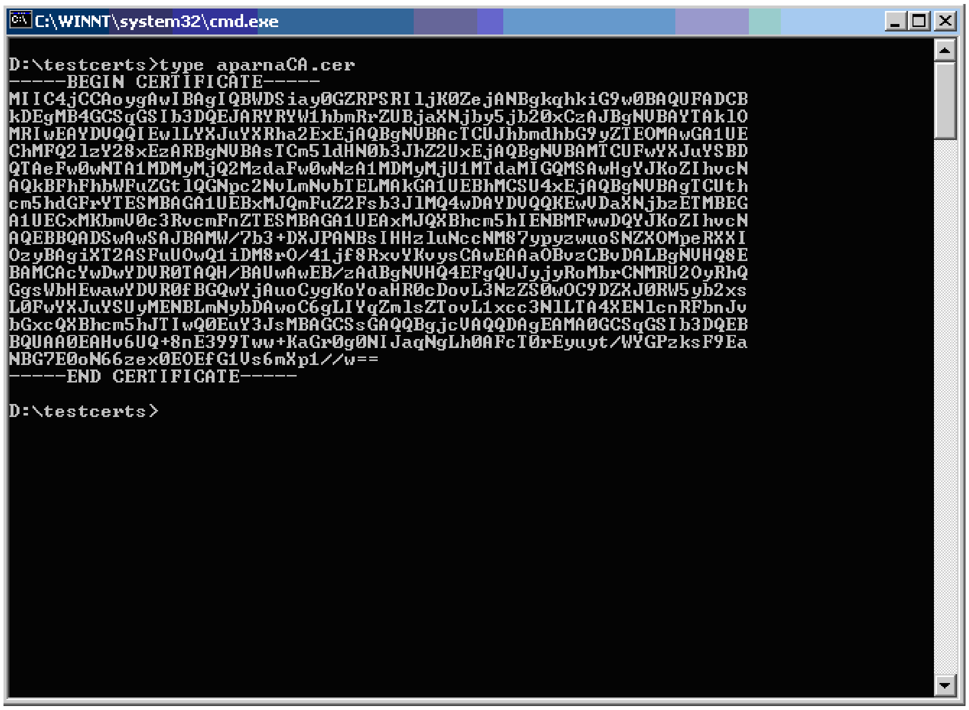
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	D:\test
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64

Step 7 Display the CA certificate stored in Base-64 (PEM) format using the Microsoft Windows **type** command.



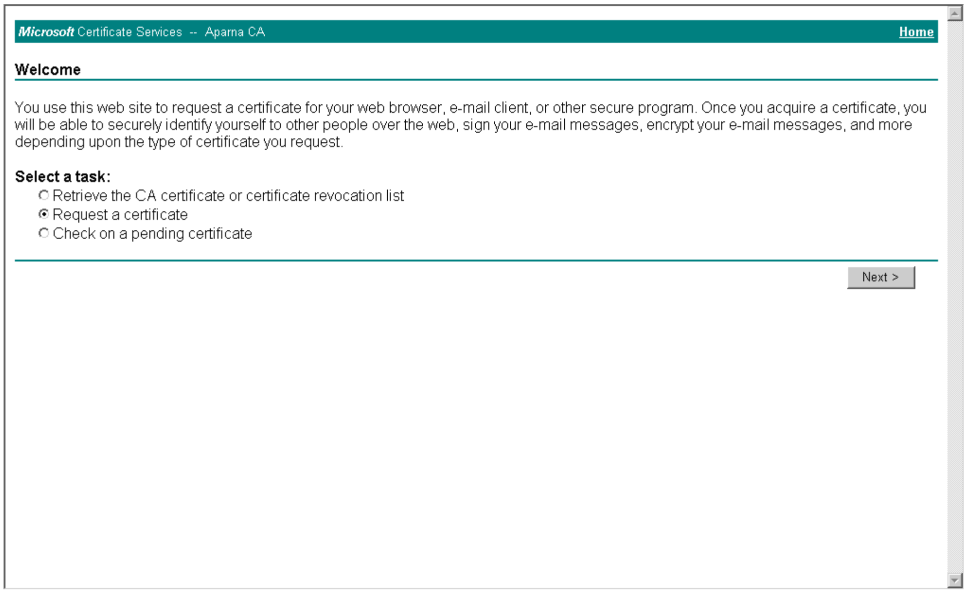
```
D:\testcerts>type aparnaCA.cer
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRI1jK0ZejANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO
MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
-----END CERTIFICATE-----

D:\testcerts>
```

Requesting an Identity Certificate

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

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



Microsoft Certificate Services -- Aparna CA

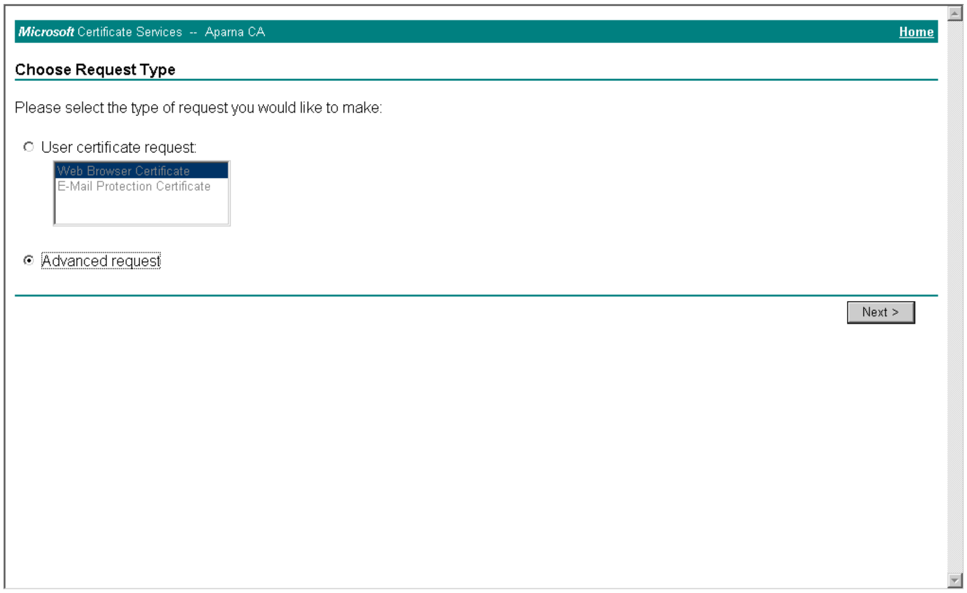
Welcome

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

Select a task:

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

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



Microsoft Certificate Services -- Aparna CA

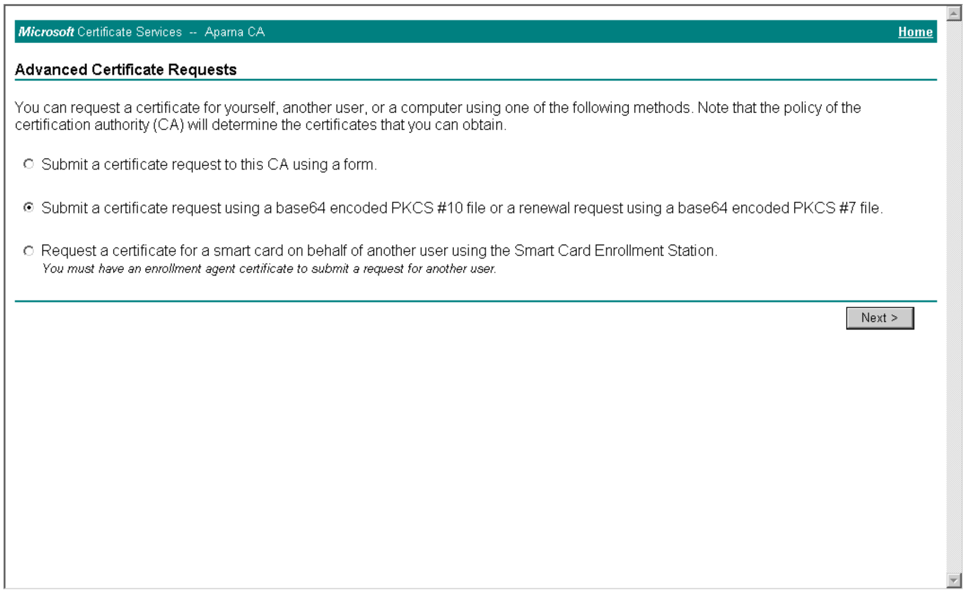
Choose Request Type

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

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

● Advanced request

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



Microsoft Certificate Services -- Aparna CA **Home**

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.

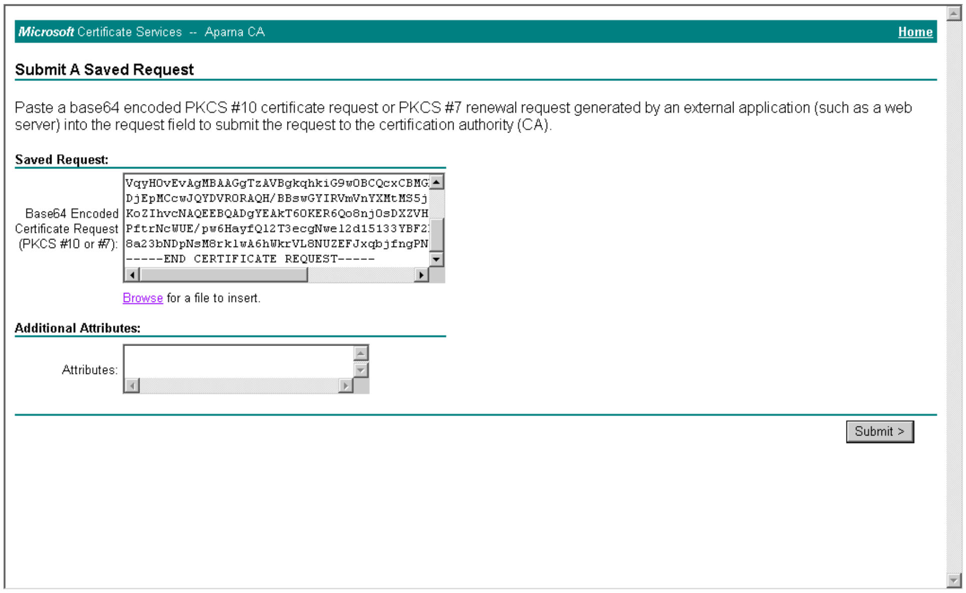
○ Submit a certificate request to this CA using a form.

● 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.

144767

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 35-10 and "Configuring Certificates on the MDS Switch" section on page 35-16)



Microsoft Certificate Services -- Aparna CA **Home**

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:

Base64 Encoded Certificate Request (PKCS #10 or #7):

```
VqyHOvEvAgMBAAGgTzAVBgkqhkiG9wOBCQcxCBMG
DjEpMCcwJQYDVRORAQH/BBswGYIRVmVnYXMtMS5j
KoZIhvcNAQEEBQADgYEAkT6OKER6Qo8njOsDXZVH
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPN
-----END CERTIFICATE REQUEST-----
```

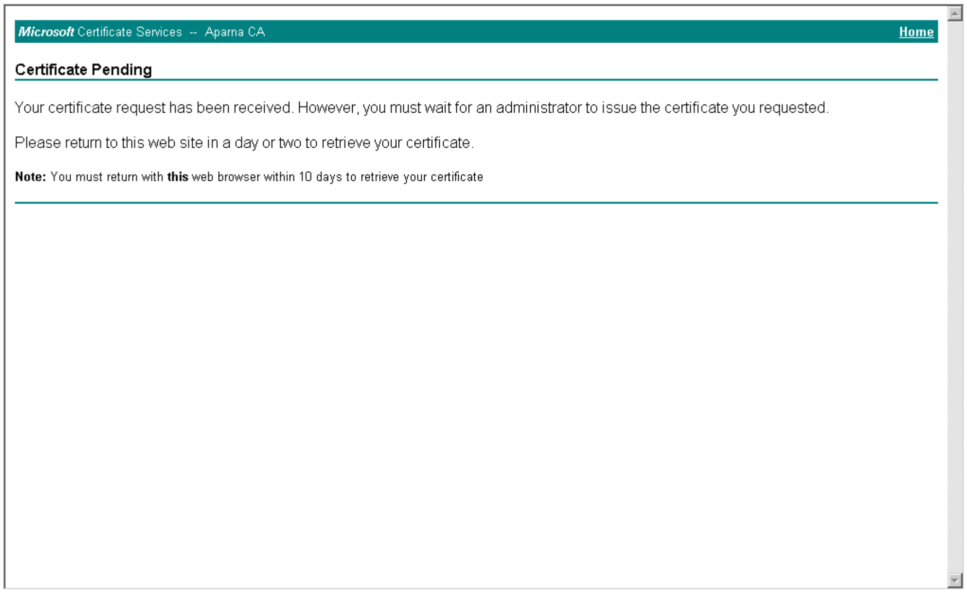
Browse for a file to insert.

Additional Attributes:

Attributes:

144768

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



Microsoft Certificate Services -- Aparna CA

Home

Certificate Pending

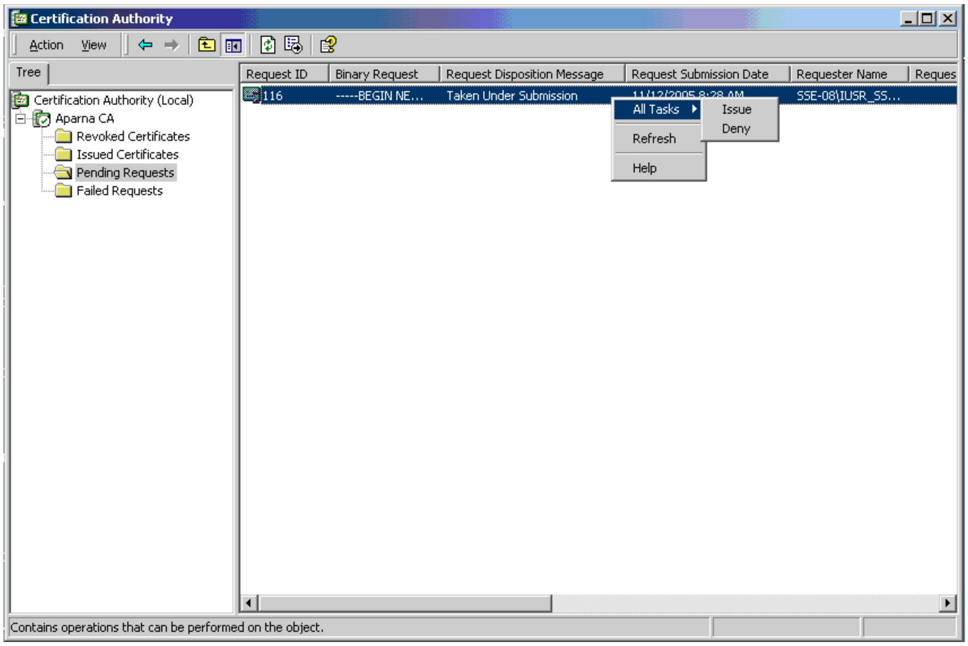
Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.

Please return to this web site in a day or two to retrieve your certificate.

Note: You must return with **this** web browser within 10 days to retrieve your certificate

144769

Step 6 The CA administrator approves the certificate request.

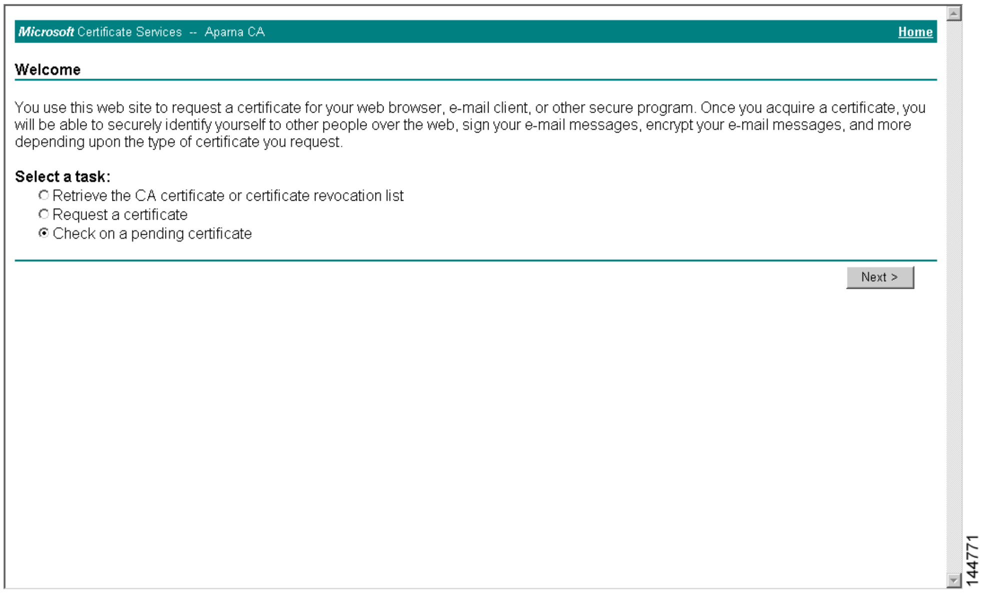


Request ID	Binary Request	Request Disposition Message	Request Submission Date	Requester Name	Reques
116	-----BEGIN NE...	Taken Under Submission	11/12/2005 8:28 AM	SSE-08\IUSR_SS...	

Contains operations that can be performed on the object.

144770

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



Microsoft Certificate Services -- Aparna CA   Home

Welcome

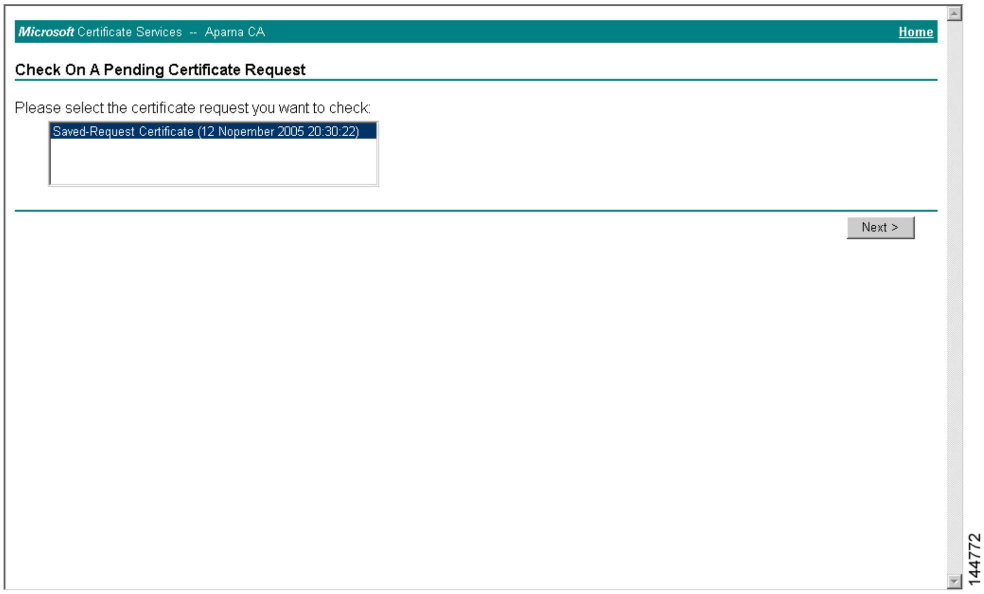
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the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

Select a task:

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

144771

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



Microsoft Certificate Services -- Aparna CA   Home

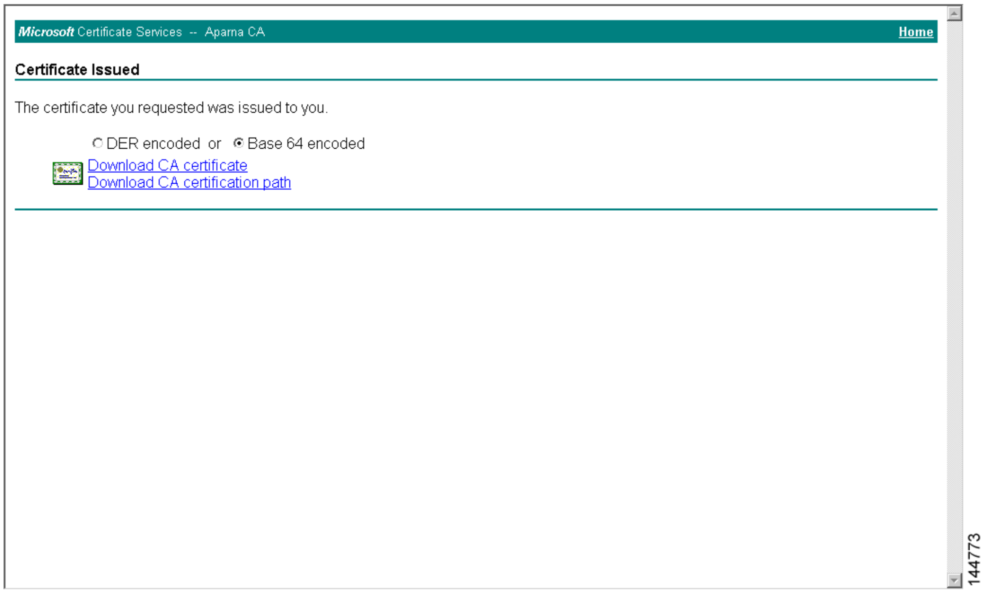
Check On A Pending Certificate Request

Please select the certificate request you want to check:

Saved-Request Certificate (12 Nopember 2005 20:30:22)

144772

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



Microsoft Certificate Services -- Aparna CA **Home**

Certificate Issued

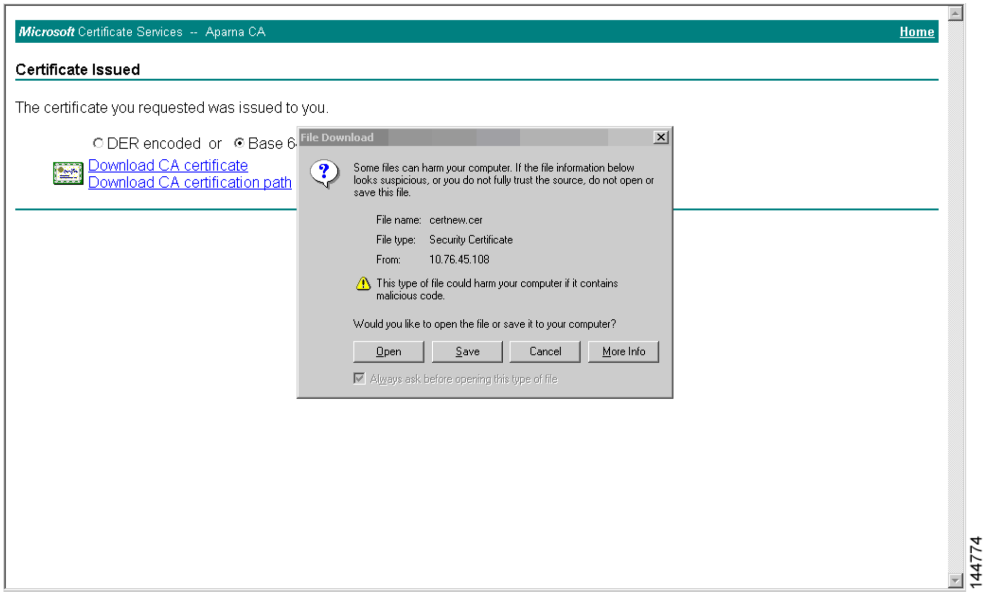
The certificate you requested was issued to you.

○ DER 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**

Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 6

Download CA certificate

Download CA certification path

File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: certnew.cer

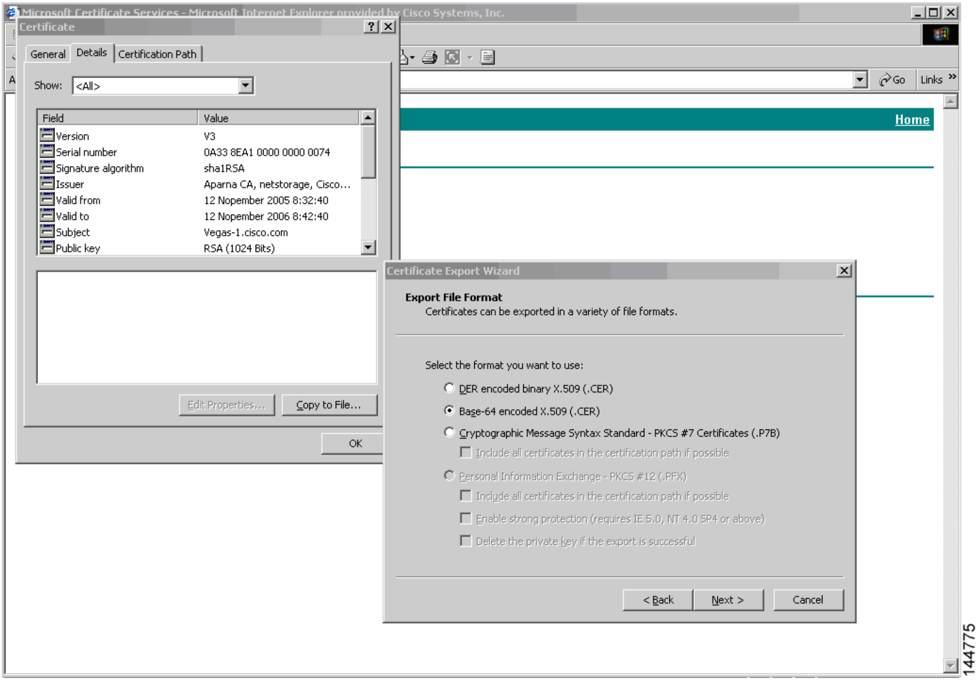
File type: Security Certificate

From: 10.76.45.108

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?

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



Show: <All>

Field	Value
Version	V3
Serial number	0A33 8EA1 0000 0000 0074
Signature algorithm	sha1RSA
Issuer	Aparna CA, netstorage, Cisco...
Valid from	12 Nopember 2005 8:32:40
Valid to	12 Nopember 2006 8:42:40
Subject	Vegas-1.cisco.com
Public key	RSA (1024 Bits)

Certificate Export Wizard

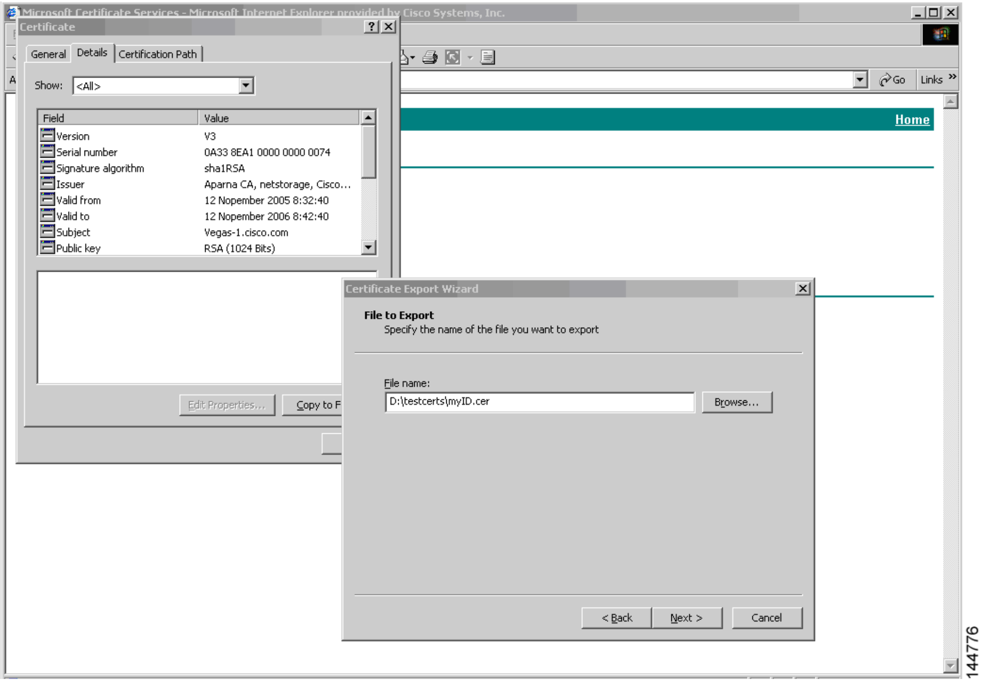
Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)
● Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
□ Delete the private key if the export is successful

< Back | Next > | Cancel

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


Microsoft Certificate Services - Microsoft Internet Explorer provided by Cisco Systems, Inc.
Certificate
General
Details
Certification Path
Go
Links
Home
Edit Properties...
Copy to F
144776

Show: <All>

Field	Value
Version	V3
Serial number	0A33 8EA1 0000 0000 0074
Signature algorithm	sha1RSA
Issuer	Aparna CA, netstorage, Cisco...
Valid from	12 Nopember 2005 8:32:40
Valid to	12 Nopember 2006 8:42:40
Subject	Vegas-1.cisco.com
Public key	RSA (1024 Bits)

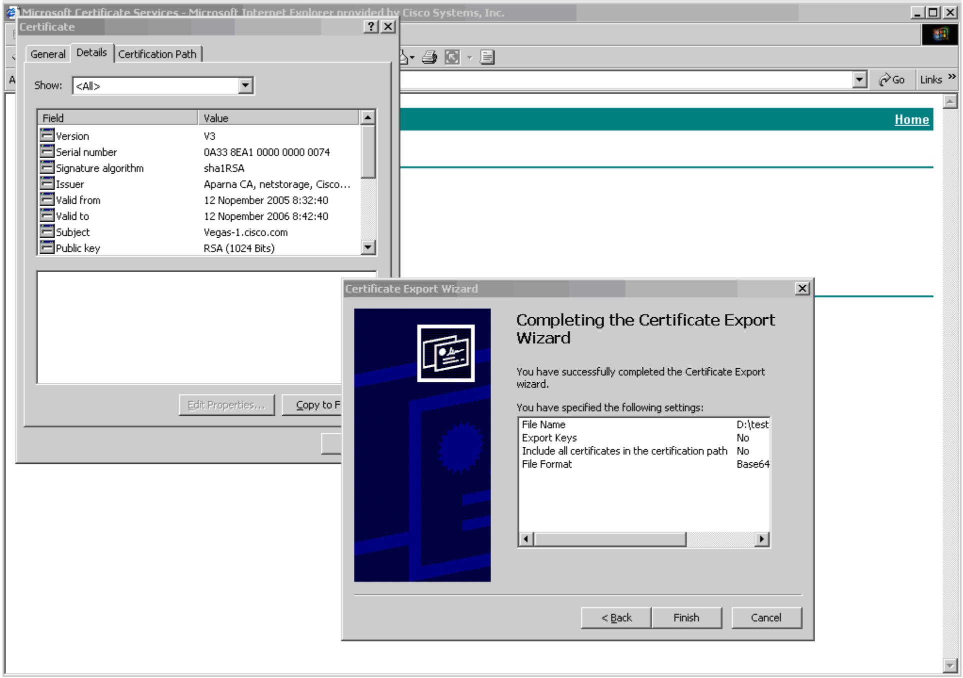
Certificate Export Wizard

File to Export
Specify the name of the file you want to export

File name: D:\testcerts\myID.cer Browse...

< Back | Next > | Cancel

Step 13 Click **Finish**.


Microsoft Certificate Services - Microsoft Internet Explorer provided by Cisco Systems, Inc.
Certificate
General
Details
Certification Path
Edit Properties...
Copy to F
Go
Links
Home
Certificate Export Wizard
< Back
Finish
Cancel

Show: <All>

Field	Value
Version	V3
Serial number	0A33 8EA1 0000 0000 0074
Signature algorithm	sha1RSA
Issuer	Aparna CA, netstorage, Cisco...
Valid from	12 Nopember 2005 8:32:40
Valid to	12 Nopember 2006 8:42:40
Subject	Vegas-1.cisco.com
Public key	RSA (1024 Bits)

Completing the Certificate Export Wizard

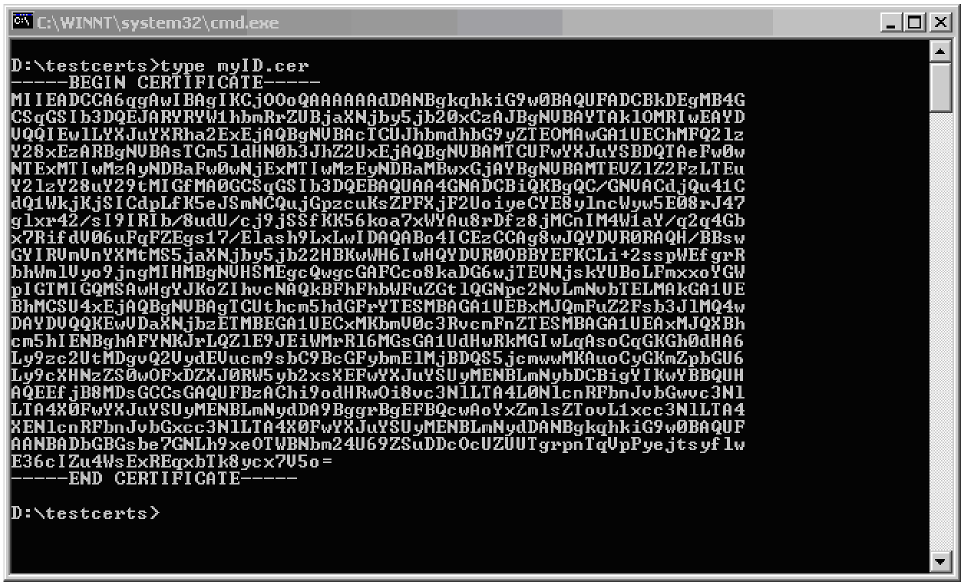
You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	D:\test
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64

144777

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



```
D:\testcerts>type myID.cer
-----BEGIN CERTIFICATE-----
MIIEADCCA6ggAwIBAgIKCjOOoQAAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD
VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz
Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w
NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu
Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYNKJrLQZlE9JEiWMrR16MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6
Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4
XENlcnRFbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----

D:\testcerts>
```

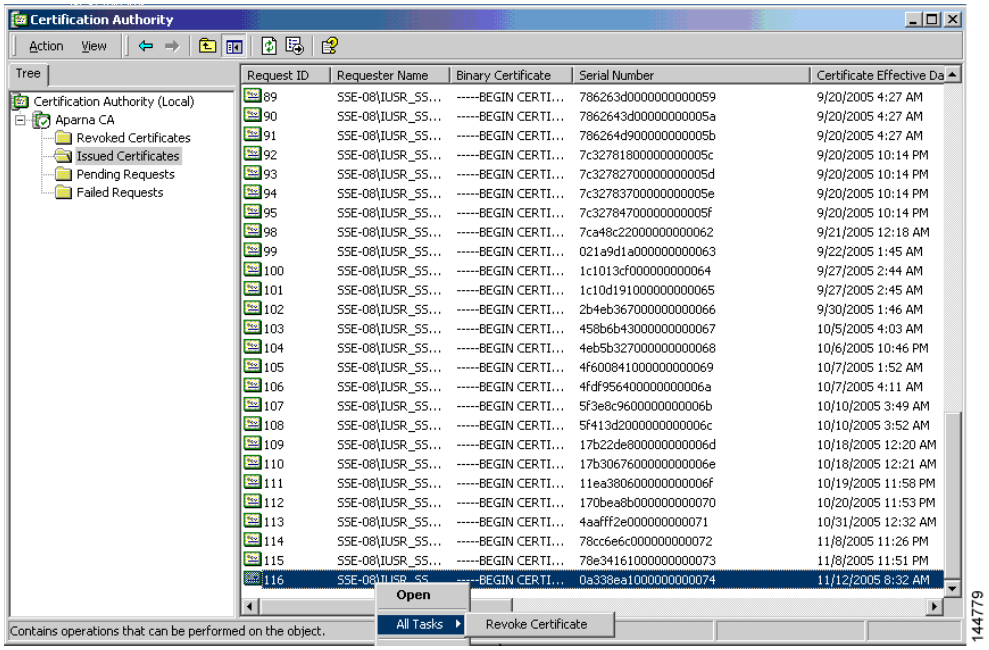
144778

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**.

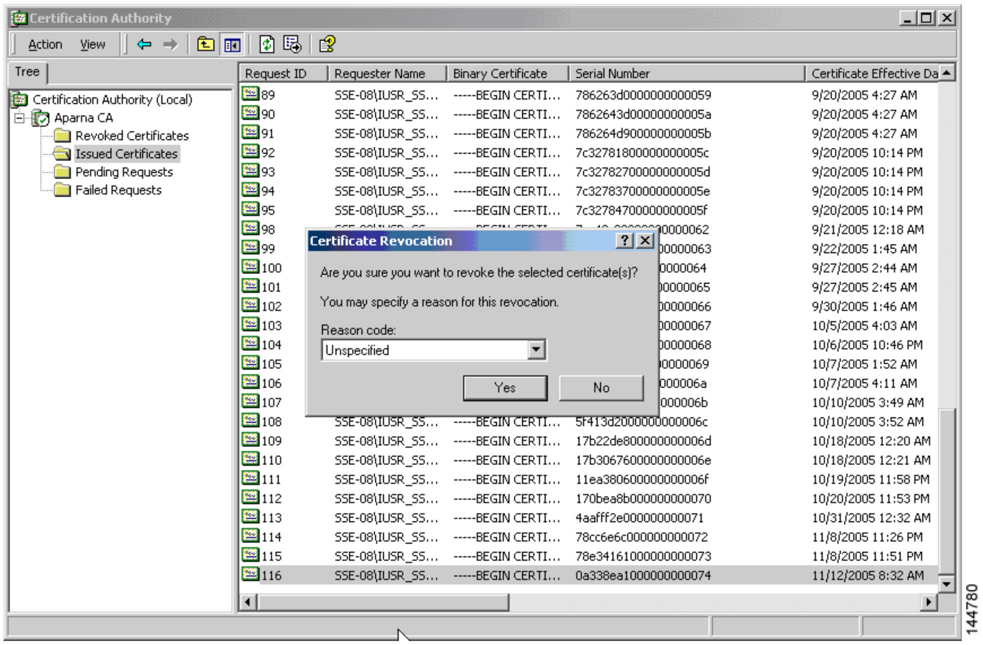


Request ID	Requester Name	Binary Certificate	Serial Number	Certificate Effective Da
89	SSE-08\IUSR_SS...	-----BEGIN CERTI...	786263d0000000000059	9/20/2005 4:27 AM
90	SSE-08\IUSR_SS...	-----BEGIN CERTI...	7862643d000000000005a	9/20/2005 4:27 AM
91	SSE-08\IUSR_SS...	-----BEGIN CERTI...	786264d900000000005b	9/20/2005 4:27 AM
92	SSE-08\IUSR_SS...	-----BEGIN CERTI...	7c32781800000000005c	9/20/2005 10:14 PM
93	SSE-08\IUSR_SS...	-----BEGIN CERTI...	7c32782700000000005d	9/20/2005 10:14 PM
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	SSE-08\IUSR_SS...	-----BEGIN CERTI...	7ca48c2200000000062	9/21/2005 12:18 AM
99	SSE-08\IUSR_SS...	-----BEGIN CERTI...	021a9d1a000000000063	9/22/2005 1:45 AM
100	SSE-08\IUSR_SS...	-----BEGIN CERTI...	1c1013cf000000000064	9/27/2005 2:44 AM
101	SSE-08\IUSR_SS...	-----BEGIN CERTI...	1c10d19100000000065	9/27/2005 2:45 AM
102	SSE-08\IUSR_SS...	-----BEGIN CERTI...	2b4eb36700000000066	9/30/2005 1:46 AM
103	SSE-08\IUSR_SS...	-----BEGIN CERTI...	458b6b43000000000067	10/5/2005 4:03 AM
104	SSE-08\IUSR_SS...	-----BEGIN CERTI...	4eb5b327000000000068	10/6/2005 10:46 PM
105	SSE-08\IUSR_SS...	-----BEGIN CERTI...	4f6008410000000000069	10/7/2005 1:52 AM
106	SSE-08\IUSR_SS...	-----BEGIN CERTI...	4fdf95640000000006a	10/7/2005 4:11 AM
107	SSE-08\IUSR_SS...	-----BEGIN CERTI...	5f3e8c960000000006b	10/10/2005 3:49 AM
108	SSE-08\IUSR_SS...	-----BEGIN CERTI...	5f413d200000000006c	10/10/2005 3:52 AM
109	SSE-08\IUSR_SS...	-----BEGIN CERTI...	17b22de80000000006d	10/18/2005 12:20 AM
110	SSE-08\IUSR_SS...	-----BEGIN CERTI...	17b306760000000006e	10/18/2005 12:21 AM
111	SSE-08\IUSR_SS...	-----BEGIN CERTI...	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...	78cc6e6c000000000072	11/8/2005 11:26 PM
115	SSE-08\IUSR_SS...	-----BEGIN CERTI...	78e341610000000000073	11/8/2005 11:51 PM
116	SSE-08\IUSR_SS...	-----BEGIN CERTI...	0a338ea1000000000074	11/12/2005 8:32 AM

Contains operations that can be performed on the object.

Send documentation comments to mdsfeedback-doc@cisco.com

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



Certificate Revocation

Are you sure you want to revoke the selected certificate(s)?

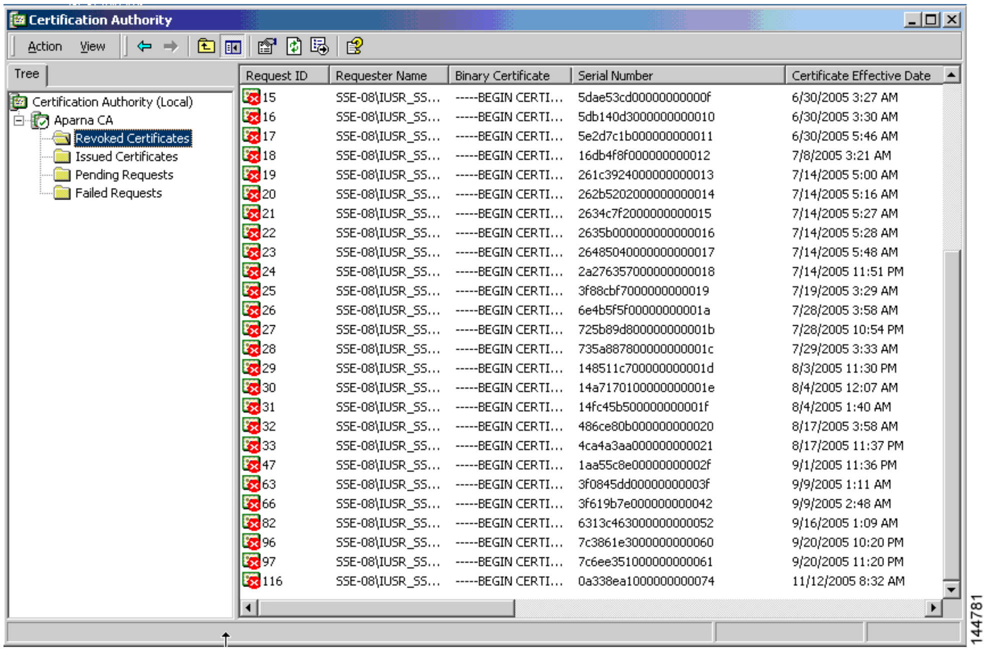
You may specify a reason for this revocation.

Reason code: Unspecified

Yes No

Request ID	Requester Name	Binary Certificate	Serial Number	Certificate Effective Da
89	SSE-08\IUSR_SS...	-----BEGIN CERTI...	786263d0000000000059	9/20/2005 4:27 AM
90	SSE-08\IUSR_SS...	-----BEGIN CERTI...	7862643d00000000005a	9/20/2005 4:27 AM
91	SSE-08\IUSR_SS...	-----BEGIN CERTI...	786264d900000000005b	9/20/2005 4:27 AM
92	SSE-08\IUSR_SS...	-----BEGIN CERTI...	7c32781800000000005c	9/20/2005 10:14 PM
93	SSE-08\IUSR_SS...	-----BEGIN CERTI...	7c32782700000000005d	9/20/2005 10:14 PM
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			0000062	9/21/2005 12:18 AM
99			00000063	9/22/2005 1:45 AM
100			0000064	9/27/2005 2:44 AM
101			00000065	9/27/2005 2:45 AM
102			00000066	9/30/2005 1:46 AM
103			00000067	10/5/2005 4:03 AM
104			00000068	10/6/2005 10:46 PM
105			0000069	10/7/2005 1:52 AM
106			000006a	10/7/2005 4:11 AM
107			000006b	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...	17b22de800000000006d	10/18/2005 12:20 AM
110	SSE-08\IUSR_SS...	-----BEGIN CERTI...	17b30676000000000006e	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...	78cc6e6c000000000072	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.

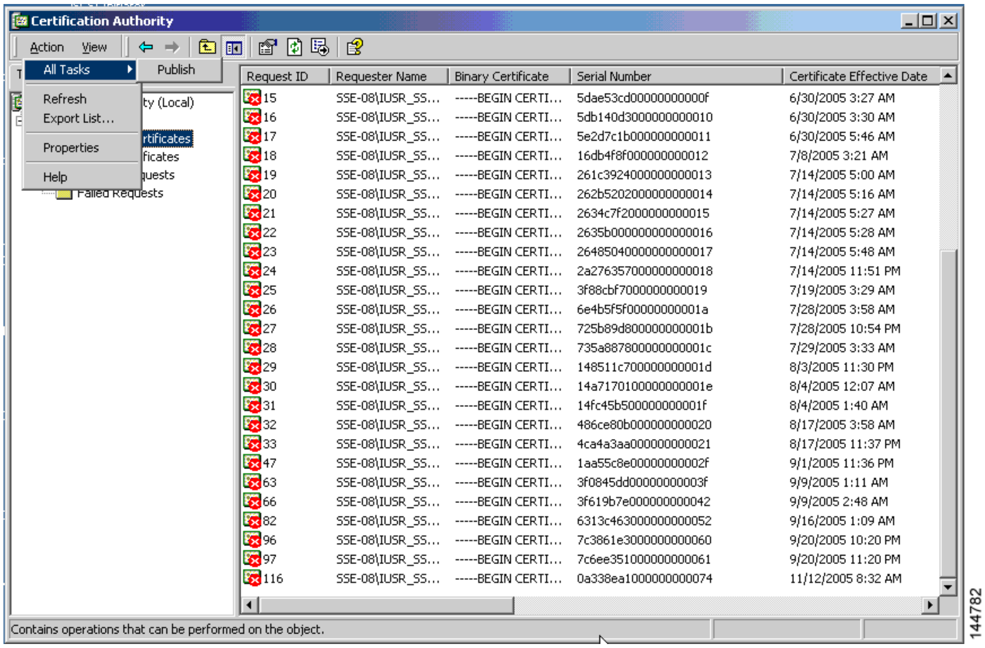


Request ID	Requester Name	Binary Certificate	Serial Number	Certificate Effective Date
15	SSE-08\IUSR_SS...	-----BEGIN CERTI...	5dae53cd00000000000f	6/30/2005 3:27 AM
16	SSE-08\IUSR_SS...	-----BEGIN CERTI...	5db140d3000000000010	6/30/2005 3:30 AM
17	SSE-08\IUSR_SS...	-----BEGIN CERTI...	5e2d7c1b000000000011	6/30/2005 5:46 AM
18	SSE-08\IUSR_SS...	-----BEGIN CERTI...	16db4f8f000000000012	7/8/2005 3:21 AM
19	SSE-08\IUSR_SS...	-----BEGIN CERTI...	261c3924000000000013	7/14/2005 5:00 AM
20	SSE-08\IUSR_SS...	-----BEGIN CERTI...	262b5202000000000014	7/14/2005 5:16 AM
21	SSE-08\IUSR_SS...	-----BEGIN CERTI...	2634c7f2000000000015	7/14/2005 5:27 AM
22	SSE-08\IUSR_SS...	-----BEGIN CERTI...	2635b000000000000016	7/14/2005 5:28 AM
23	SSE-08\IUSR_SS...	-----BEGIN CERTI...	26485040000000000017	7/14/2005 5:48 AM
24	SSE-08\IUSR_SS...	-----BEGIN CERTI...	2a276357000000000018	7/14/2005 11:51 PM
25	SSE-08\IUSR_SS...	-----BEGIN CERTI...	3f88cbf7000000000019	7/19/2005 3:29 AM
26	SSE-08\IUSR_SS...	-----BEGIN CERTI...	6e4b5f5f00000000001a	7/28/2005 3:58 AM
27	SSE-08\IUSR_SS...	-----BEGIN CERTI...	725b89d800000000001b	7/28/2005 10:54 PM
28	SSE-08\IUSR_SS...	-----BEGIN CERTI...	735a887800000000001c	7/29/2005 3:33 AM
29	SSE-08\IUSR_SS...	-----BEGIN CERTI...	148511c700000000001d	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...	14fc45b500000000001f	8/4/2005 1:40 AM
32	SSE-08\IUSR_SS...	-----BEGIN CERTI...	486ce80b000000000020	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
63	SSE-08\IUSR_SS...	-----BEGIN CERTI...	3f0845dd00000000003f	9/9/2005 1:11 AM
66	SSE-08\IUSR_SS...	-----BEGIN CERTI...	3f619b7e000000000042	9/9/2005 2:48 AM
82	SSE-08\IUSR_SS...	-----BEGIN CERTI...	6313c463000000000052	9/16/2005 1:09 AM
96	SSE-08\IUSR_SS...	-----BEGIN CERTI...	7c3861e3000000000060	9/20/2005 10:20 PM
97	SSE-08\IUSR_SS...	-----BEGIN CERTI...	7c6ee351000000000061	9/20/2005 11:20 PM
116	SSE-08\IUSR_SS...	-----BEGIN CERTI...	0a338ea1000000000074	11/12/2005 8:32 AM

Generating and Publishing the CRL

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

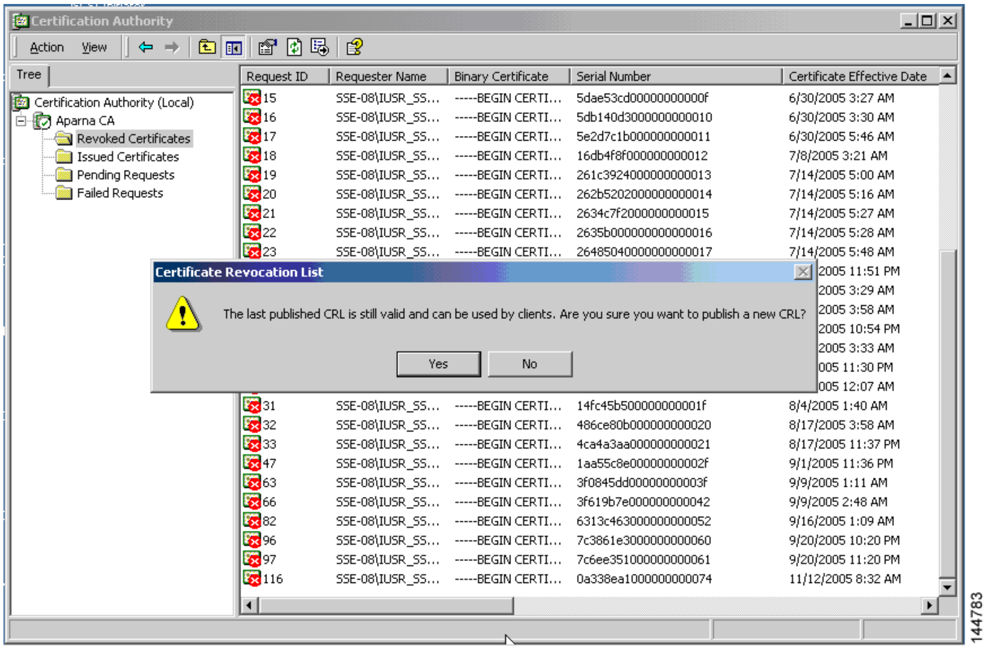
Step 1 Select **Action > All Tasks > Publish** on the Certification Authority screen.



Request ID	Requester Name	Binary Certificate	Serial Number	Certificate Effective Date
15	SSE-08\IUSR_SS...	-----BEGIN CERTI...	5dae53cd00000000000f	6/30/2005 3:27 AM
16	SSE-08\IUSR_SS...	-----BEGIN CERTI...	5db140d3000000000010	6/30/2005 3:30 AM
17	SSE-08\IUSR_SS...	-----BEGIN CERTI...	5e2d7c1b000000000011	6/30/2005 5:46 AM
18	SSE-08\IUSR_SS...	-----BEGIN CERTI...	16db4f8f000000000012	7/8/2005 3:21 AM
19	SSE-08\IUSR_SS...	-----BEGIN CERTI...	261c3924000000000013	7/14/2005 5:00 AM
20	SSE-08\IUSR_SS...	-----BEGIN CERTI...	262b5202000000000014	7/14/2005 5:16 AM
21	SSE-08\IUSR_SS...	-----BEGIN CERTI...	2634c7f2000000000015	7/14/2005 5:27 AM
22	SSE-08\IUSR_SS...	-----BEGIN CERTI...	2635b000000000000016	7/14/2005 5:28 AM
23	SSE-08\IUSR_SS...	-----BEGIN CERTI...	26485040000000000017	7/14/2005 5:48 AM
24	SSE-08\IUSR_SS...	-----BEGIN CERTI...	2a276357000000000018	7/14/2005 11:51 PM
25	SSE-08\IUSR_SS...	-----BEGIN CERTI...	3f88cbf7000000000019	7/19/2005 3:29 AM
26	SSE-08\IUSR_SS...	-----BEGIN CERTI...	6e4b5f5f00000000001a	7/28/2005 3:58 AM
27	SSE-08\IUSR_SS...	-----BEGIN CERTI...	725b89d800000000001b	7/28/2005 10:54 PM
28	SSE-08\IUSR_SS...	-----BEGIN CERTI...	735a887800000000001c	7/29/2005 3:33 AM
29	SSE-08\IUSR_SS...	-----BEGIN CERTI...	148511c700000000001d	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...	14fc45b500000000001f	8/4/2005 1:40 AM
32	SSE-08\IUSR_SS...	-----BEGIN CERTI...	486ce80b000000000020	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
63	SSE-08\IUSR_SS...	-----BEGIN CERTI...	3f0845dd00000000003f	9/9/2005 1:11 AM
66	SSE-08\IUSR_SS...	-----BEGIN CERTI...	3f619b7e000000000042	9/9/2005 2:48 AM
82	SSE-08\IUSR_SS...	-----BEGIN CERTI...	6313c463000000000052	9/16/2005 1:09 AM
96	SSE-08\IUSR_SS...	-----BEGIN CERTI...	7c3861e3000000000060	9/20/2005 10:20 PM
97	SSE-08\IUSR_SS...	-----BEGIN CERTI...	7c6ee351000000000061	9/20/2005 11:20 PM
116	SSE-08\IUSR_SS...	-----BEGIN CERTI...	0a338ea1000000000074	11/12/2005 8:32 AM

Contains operations that can be performed on the object.

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



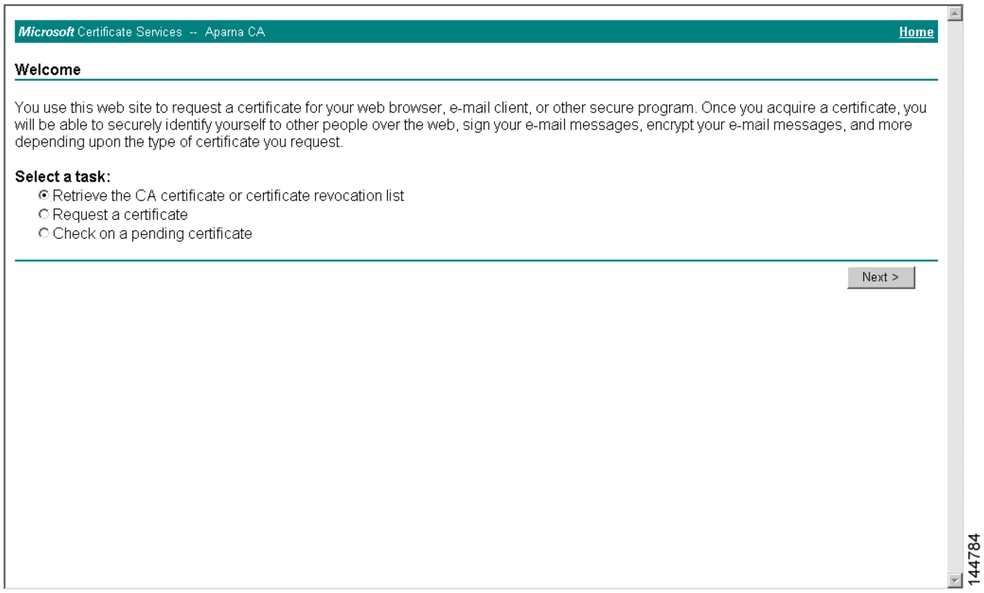
The last published CRL is still valid and can be used by clients. Are you sure you want to publish a new CRL?

Request ID	Requester Name	Binary Certificate	Serial Number	Certificate Effective Date
15	SSE-08\IUSR_SS...	-----BEGIN CERTI...	5dae53cd00000000000f	6/30/2005 3:27 AM
16	SSE-08\IUSR_SS...	-----BEGIN CERTI...	5db140d3000000000010	6/30/2005 3:30 AM
17	SSE-08\IUSR_SS...	-----BEGIN CERTI...	5e2d7c1b000000000011	6/30/2005 5:46 AM
18	SSE-08\IUSR_SS...	-----BEGIN CERTI...	16db4f8f000000000012	7/8/2005 3:21 AM
19	SSE-08\IUSR_SS...	-----BEGIN CERTI...	261c3924000000000013	7/14/2005 5:00 AM
20	SSE-08\IUSR_SS...	-----BEGIN CERTI...	262b5202000000000014	7/14/2005 5:16 AM
21	SSE-08\IUSR_SS...	-----BEGIN CERTI...	2634c7f2000000000015	7/14/2005 5:27 AM
22	SSE-08\IUSR_SS...	-----BEGIN CERTI...	2635b000000000000016	7/14/2005 5:28 AM
23	SSE-08\IUSR_SS...	-----BEGIN CERTI...	26485040000000000017	7/14/2005 5:48 AM
				2005 11:51 PM
				2005 3:29 AM
				2005 3:58 AM
				2005 10:54 PM
				2005 3:33 AM
				005 11:30 PM
				005 12:07 AM
31	SSE-08\IUSR_SS...	-----BEGIN CERTI...	14fc45b500000000001f	8/4/2005 1:40 AM
32	SSE-08\IUSR_SS...	-----BEGIN CERTI...	486ce80b000000000020	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
63	SSE-08\IUSR_SS...	-----BEGIN CERTI...	3f0845dd00000000003f	9/9/2005 1:11 AM
66	SSE-08\IUSR_SS...	-----BEGIN CERTI...	3f619b7e000000000042	9/9/2005 2:48 AM
82	SSE-08\IUSR_SS...	-----BEGIN CERTI...	6313c463000000000052	9/16/2005 1:09 AM
96	SSE-08\IUSR_SS...	-----BEGIN CERTI...	7c3861e3000000000060	9/20/2005 10:20 PM
97	SSE-08\IUSR_SS...	-----BEGIN CERTI...	7c6ee351000000000061	9/20/2005 11:20 PM
116	SSE-08\IUSR_SS...	-----BEGIN CERTI...	0a338ea1000000000074	11/12/2005 8:32 AM

Downloading the CRL

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

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



Microsoft Certificate Services -- Aparna CA   Home

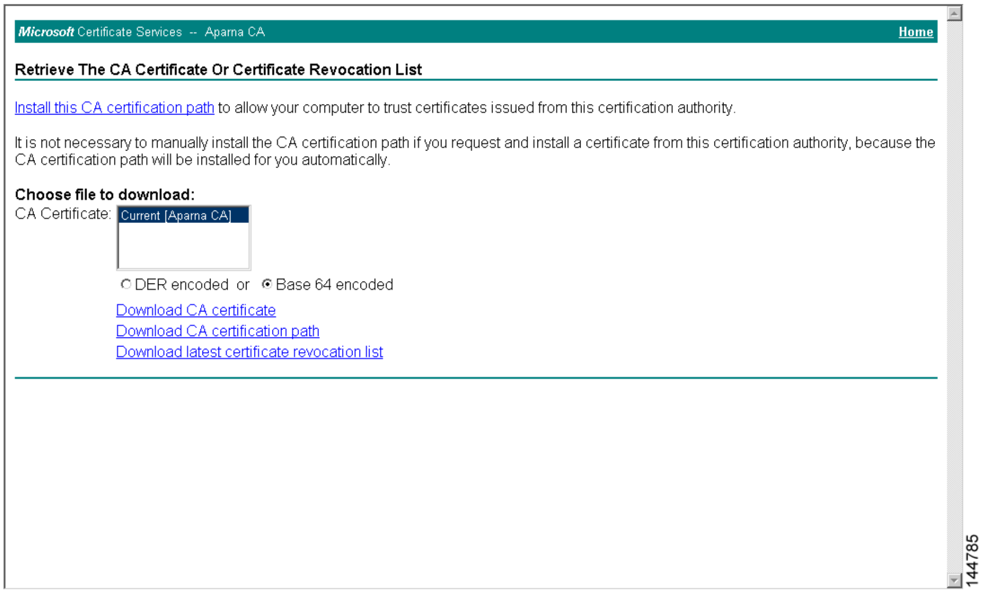
Welcome

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

Select a task:

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

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

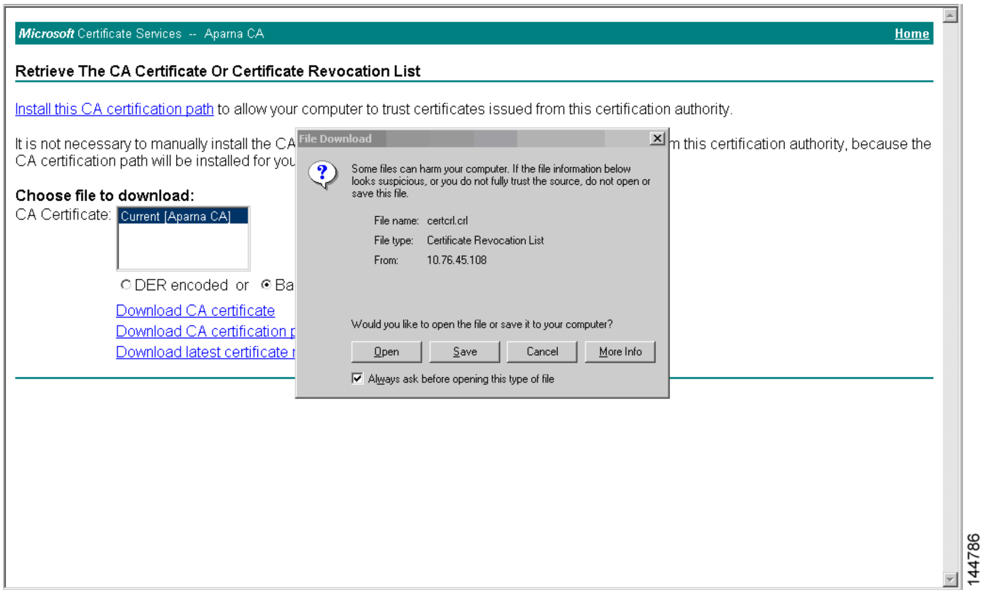
Choose file to download:

CA Certificate: Current [Aparna CA]

○ DER encoded or ● Base 64 encoded

Download CA certificate
Download CA certification path
Download latest certificate revocation list

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



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 … m this certification authority, because the CA certification path will be installed for you …

Choose file to download:
CA Certificate: Current [Aparna CA]

○ DER encoded or ● Ba…

Download CA certificate
Download CA certification p…
Download latest certificate r…

File Download

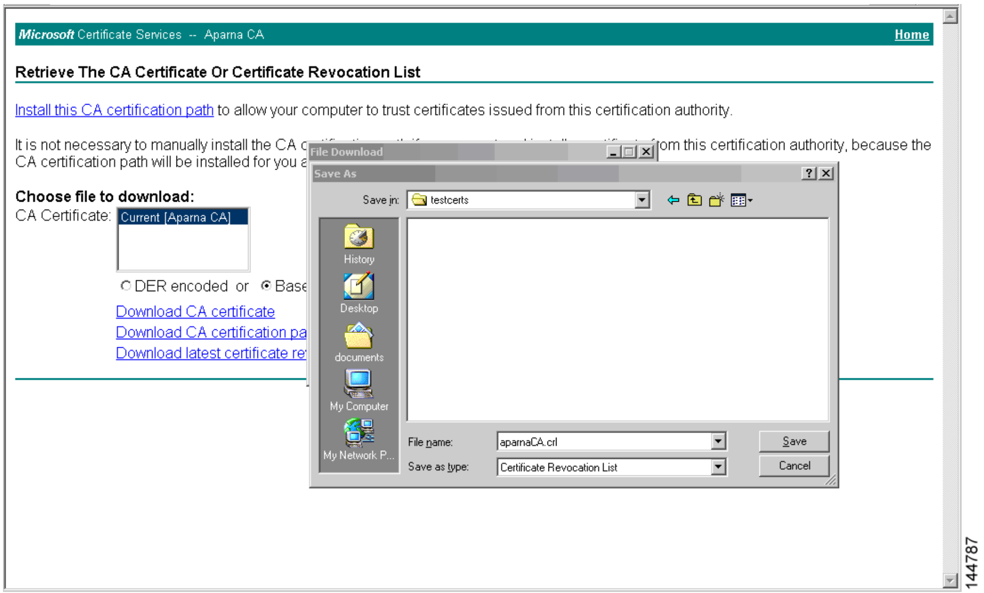
Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: certcrl.crl
File type: Certificate Revocation List
From: 10.76.45.108

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

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



Microsoft Certificate Services -- Aparna CA **Home**

Retrieve The CA Certificate Or Certificate 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 c… om this certification authority, because the CA certification path will be installed for you a…

Choose file to download:
CA Certificate: Current [Aparna CA]

○ DER encoded or ● Base…

Download CA certificate
Download CA certification pa…
Download latest certificate re…

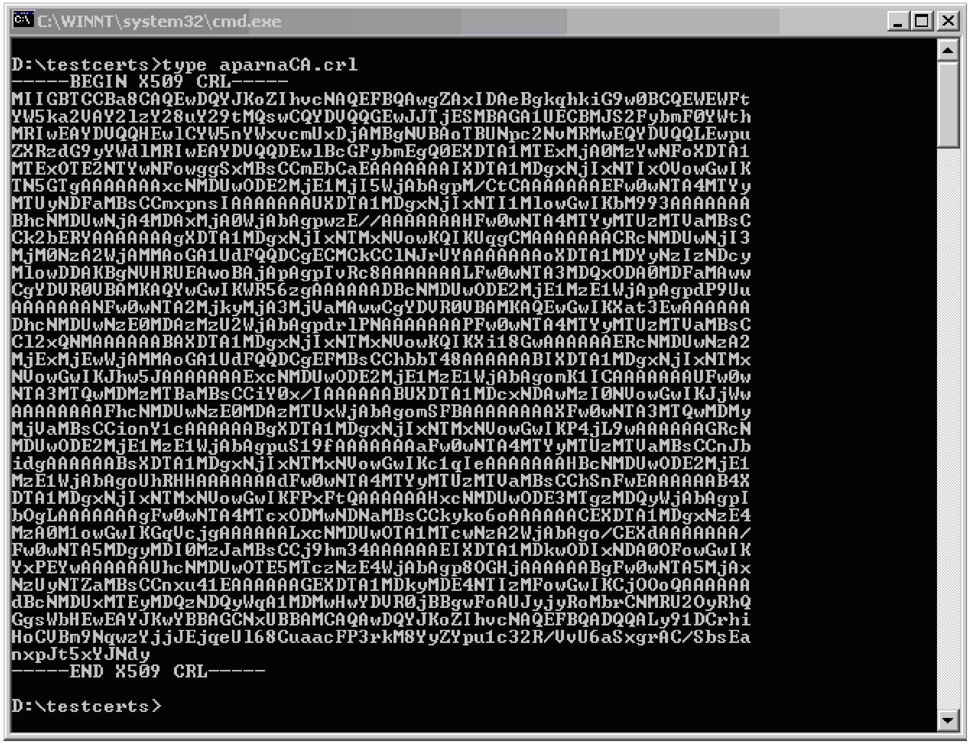
File Download

Save As

Save in: testcerts

File name: aparnaCA.crl
Save as type: Certificate Revocation List

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



```
D:\testcerts>type aparnaCA.crl
-----BEGIN X509 CRL-----
MIIGBTCCBa8CAQEwDQYJKoZIhvcNAQEFBQAwgZAxIDAeBgkqhkiG9w0BCQEWEWFt
YW5ka2VAY2lzY28uY29tMQswCQYDVQQGEwJJTjESMBAGA1UECBMJS2FybmF0YWth
MRIwEAYDVQQHEwlCYW5nYWxvcmUxDjAMBgNVBAoTBUNpc2NvMRMwEQYDVQQLEwpu
ZXRzdG9yYWdlMRIwEAYDVQQDEwlBcGFybmEgQ0EXDTA1MTExMjA0MzYwNFoXDTA1
MTExOTE2NTYwNFowggSxMBsCCmEbCaEAAAAAAAIXDTA1MDgxNjIxNTIxOVowGwIK
TN5GTgAAAAAAAxcNMDUwODE2MjE1MjI5WjAbAgpM/CtCAAAAAAAEFw0wNTA4MTYy
MTUyNDFaMBsCCmxpnsIAAAAAAAUXDTA1MDgxNjIxNTI1MlowGwIKbM993AAAAAAA
BhcNMDUwNjA4MDAxMjA0WjAbAgpwzE//AAAAAAAHFw0wNTA4MTYyMTUzMTVaMBsC
Ck2bERYAAAAAAAgXDTA1MDgxNjIxNTMxNVowKQIKUggCMAAAAAAACRcNMDUwNjI3
MjM0NzA2WjAMMAoGA1UdFQQDCgECMCkCClNJrUYAAAAAAAoXDTA1MDYyNzIzNDcy
MlowDDAKBgNVHRUEAwoBAjApAgpIvRc8AAAAAAALFw0wNTA3MDQxODA0MDFaMAww
CgYDVR0VBAMKAQYwGwIKWR56zgAAAAAADBcNMDUwODE2MjE1MzE1WjApAgpdP9Uu
AAAAAAANFw0wNTA2MjkyMjA3MjVaMAwwCgYDVR0VBAMKAQEwGwIKXat3EwAAAAAA
DhcNMDUwNzE0MDAzMzU2WjAbAgpdrlPNAAAAAAAPFw0wNTA4MTYyMTUzMTVaMBsC
Cl2xQNMAAAAAABAXDTA1MDgxNjIxNTMxNVowKQIKXi18GwAAAAAAERcNMDUwNzA2
MjExMjEwWjAMMAoGA1UdFQQDCgEFMBsCChbbT48AAAAAABIXDTA1MDgxNjIxNTMx
NVowGwIKJhw5JAAAAAAAExcNMDUwODE2MjE1MzE1WjAbAgomK1ICAAAAAAAUFw0w
NTA3MTQwMDMzMTBaMBsCCiY0x/IAAAAAABUXDTA1MDcxNDAwMzI0NVowGwIKJjWw
AAAAAAAAFhcNMDUwNzE0MDAzMTUxWjAbAgomSFBAAAAAAAAAXFw0wNTA3MTQwMDMy
MjVaMBsCCionY1cAAAAAABgXDTA1MDgxNjIxNTMxNVowGwIKP4jL9wAAAAAAGRcN
MDUwODE2MjE1MzE1WjAbAgpuS19fAAAAAAAaFw0wNTA4MTYyMTUzMTVaMBsCCnJb
idgAAAAAABsXDTA1MDgxNjIxNTMxNVowGwIKc1qIeAAAAAAAHBcNMDUwODE2MjE1
MzE1WjAbAgoUhRHHAAAAAAAdFw0wNTA4MTYyMTUzMTVaMBsCChSnFwEAAAAAAB4X
DTA1MDgxNjIxNTMxNVowGwIKFPxFtQAAAAAAHxcNMDUwODE3MTgzMDQyWjAbAgpI
bOgLAAAAAAAgFw0wNTA4MTcxODMwNDNaMBsCCkyko6oAAAAAACEXDTA1MDgxNzE4
MzA0M1owGwIKGqVcjgAAAAAALxcNMDUwOTA1MTcwNzA2WjAbAgo/CEXdAAAAAAA/
Fw0wNTA5MDgyMDI0MzJaMBsCCj9hm34AAAAAAEIXDTA1MDkwODIxNDA0OFowGwIK
YxPEYwAAAAAAUhcNMDUwOTE5MTczNzE4WjAbAgp8OGHjAAAAAABgFw0wNTA5MjAx
NzUyNTZaMBsCCnxu41EAAAAAAGEXDTA1MDkyMDE4NTIzMFowGwIKCjOOoQAAAAAA
dBcNMDUxMTEyMDQzNDQyWqA1MDMwHwYDVR0jBBgwFoAUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEFBQADQQALy91DCrhi
HoCVBm9NqwzYjjJEjqeUl68CuaacFP3rkM8YyZYpu1c32R/VvU6aSxgrAC/SbsEa
nxpJt5xYJNdy
-----END X509 CRL-----

D:\testcerts>
```

Importing the CRL

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

Step 1 Copy the CRL file to the MDS switch bootflash.

```
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: 611B09A1000000000002
        Revocation Date: Aug 16 21:52:19 2005 GMT
Serial Number: 4CDE464E000000000003
        Revocation Date: Aug 16 21:52:29 2005 GMT
    Serial Number: 4CFC2B42000000000004
        Revocation Date: Aug 16 21:52:41 2005 GMT
    Serial Number: 6C699EC2000000000005
        Revocation Date: Aug 16 21:52:52 2005 GMT
    Serial Number: 6CCF7DDC000000000006
        Revocation Date: Jun  8 00:12:04 2005 GMT
    Serial Number: 70CC4FFF000000000007
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 4D9B1116000000000008
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 52A80230000000000009
        Revocation Date: Jun 27 23:47:06 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            CA Compromise
Serial Number: 5349AD4600000000000A
        Revocation Date: Jun 27 23:47:22 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            CA Compromise
Serial Number: 53BD173C00000000000B
        Revocation Date: Jul  4 18:04:01 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            Certificate Hold
Serial Number: 591E7ACE00000000000C
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5D3FD52E00000000000D
        Revocation Date: Jun 29 22:07:25 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            Key Compromise
Serial Number: 5DAB771300000000000E
        Revocation Date: Jul 14 00:33:56 2005 GMT
    Serial Number: 5DAE53CD00000000000F
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5DB140D3000000000010
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5E2D7C1B000000000011
        Revocation Date: Jul  6 21:12:10 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            Cessation Of Operation
Serial Number: 16DB4F8F000000000012
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 261C3924000000000013
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 262B5202000000000014
        Revocation Date: Jul 14 00:33:10 2005 GMT
    Serial Number: 2634C7F2000000000015
        Revocation Date: Jul 14 00:32:45 2005 GMT
    Serial Number: 2635B000000000000016
        Revocation Date: Jul 14 00:31:51 2005 GMT
    Serial Number: 26485040000000000017
        Revocation Date: Jul 14 00:32:25 2005 GMT
    Serial Number: 2A276357000000000018
```

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

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

Maximum Limits

Table 35-1 lists the maximum limits for CAs and digital certificate parameters.

Table 35-1 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 35-2 lists the default settings for CAs and digital certificate parameters.

Table 35-2 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.