



CHAPTER **34**

Configuring Certificate Authorities and Digital Certificates

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

This chapter includes the following sections:

- [About CAs and Digital Certificates, page 34-1](#)
- [Configuring CAs and Digital Certificates, page 34-5](#)
- [Example Configurations, page 34-15](#)
- [Maximum Limits, page 34-37](#)
- [Default Settings, page 34-38](#)

About CAs and Digital Certificates

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

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

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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).

Send documentation comments to mdsfeedback-doc@cisco.com

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

- A trust point corresponds to a specific CA that the MDS switch trusts for peer certificate verification for any application (such as IKE or SSH).
- An MDS switch can have many trust points and all applications on the switch can trust a peer certificate issued by any of the trust point CAs.
- A trust point is not restricted to a specific application.
- An MDS switch enrolls with the CA corresponding to the trust point to obtain an identity certificate. You can enroll your switch with multiple trust points thereby obtaining a separate identity certificate from each trust point. The identity certificates are used by applications depending upon the purposes specified in the certificate by the issuing CA. The purpose of a certificate is stored in the certificate as certificate extensions.
- When enrolling with a trust point, you must specify an RSA key-pair to be certified. This key-pair must be generated and associated to the trust point before generating the enrollment request. The association between the trust point, key-pair, and identity certificate is valid until it is explicitly removed by deleting the certificate, key-pair, or trust point.
- The subject name in the identity certificate is the fully qualified domain name for the MDS switch.
- You can generate one or more RSA key-pairs on a switch and each can be associated to one or more trust points. But no more than one key-pair can be associated to a trust point, which means only one identity certificate is allowed from a CA.
- If multiple identity certificates (each from a distinct CA) have been obtained, the certificate that an application selects to use in a security protocol exchange with a peer is application specific (see the “[IPsec Digital Certificate Support](#)” section on page 35-7 and the “[SSH Authentication Using Digital Certificates](#)” section on page 39-18).
- You do not need to designate one or more trust points for an application. Any application can use any certificate issued by any trust point as long as the certificate purpose satisfies the application requirements.
- You do not need more than one identity certificate from a trust point or more than one key-pair to be associated to a trust point. A CA certifies a given identity (name) only once and does not issue multiple certificates with the same subject name. If you need more than one identity certificate for a CA, then define another trust point for the same CA, associate another key-pair to it, and have it certified, provided CA allows multiple certificates with the same subject name.

Multiple Trusted CA Support

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

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

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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.

Send documentation comments to mdsfeedback-doc@cisco.com

- Verifies that the peer certificate is valid (not expired) with respect to current time.
- Verifies that the peer certificate is not yet revoked by the issuing CA.

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

CRL Downloading, Caching, and Checking Support

Certificate revocation lists (CRLs) are maintained by CAs to give information of prematurely revoked certificates, and the CRLs are published in a repository. The download URL is made public and also specified in all issued certificates. A client verifying a peer's certificate should obtain the latest CRL from the issuing CA and use it to determine if the certificate has been revoked. A client can cache the CRLs of some or all of its trusted CAs locally and use them later if necessary until the CRLs expire.

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

OCSP Support

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

Import and Export Support for Certificates and Associated Key Pairs

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

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

Configuring CAs and Digital Certificates

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

- [Configuring the Host Name and IP Domain Name, page 34-6](#)
- [Generating an RSA Key-Pair, page 34-6](#)
- [Creating a Trust Point CA Association, page 34-8](#)
- [Authenticating the CA, page 34-8](#)
- [Configuring Certificate Revocation Checking Methods, page 34-9](#)

Send documentation comments to mdsfeedback-doc@cisco.com

- [Generating Certificate Requests, page 34-10](#)
- [Installing Identity Certificates, page 34-11](#)
- [Ensuring Trust Point Configurations Persist Across Reboots, page 34-12](#)
- [Monitoring and Maintaining CA and Certificates Configuration, page 34-13](#)

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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	<p>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.</p> <p>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.</p> <p>Note The maximum number of key-pairs you can configure on a switch is 16.</p>
	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	<p>Generates an RSA key-pair with the switch FQDN as the default label and 512 as the default modulus. The key is exportable.</p> <p> Caution The exportability of a key-pair cannot be changed after key-pair generation.</p> <p>Note Only exportable key-pairs can be exported in PKCS#12 format.</p>

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Creating a Trust Point CA Association

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

	Command	Purpose
Step 1	<code>switch(config)# crypto ca trustpoint admin-ca</code> <code>switch(config-trustpoint)#</code>	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.
	<code>switch(config)# no crypto ca trustpoint admin-ca</code>	Removes the trust point CA.
Step 2	<code>switch(config-trustpoint)# enroll terminal</code>	Specifies manual cut-and-paste certificate enrollment (default). Note Manual cut-and-paste certificate enrollment is the only method supported for enrollment.
Step 3	<code>switch(config-trustpoint)# rsakeypair SwitchA</code>	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 34-6. Only one RSA key-pair can be specified per CA.
	<code>switch(config-trustpoint)# no rsakeypair SwitchA</code>	Disassociates the RSA key-pair from the trust point (default).
Step 4	<code>switch(config-trustpoint)# end</code> <code>switch#</code>	Exits trust point configuration submode.
Step 5	<code>switch# copy running-config startup-config</code>	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.

Send documentation comments to mdsfeedback-doc@cisco.com

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	<pre>switch# config t switch(config)#</pre>	Enters configuration mode.
Step 2	<pre>switch(config)# crypto ca authenticate admin-ca input (cut & paste) CA certificate (chain) in PEM format; end the input with a line containing only END OF INPUT : -----BEGIN CERTIFICATE----- MIIC4jCCAoygAwIBAgIQBWDsiay0GZRPSRI1jK0ZeJANBgkqhkiG9w0BAQUFADCB kDEgMB4GCSqGSIb3DQEJARYRYWlhbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAk1O MR1wEAYDVQQQEiEwLllyXJYuYXRha2EzEjAQBGNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE ChMFQ21zY28xEzARBGNVBAStCm5ldHN0b3JhZ2UxEjAQBGNVBAMTCUFwYXJlYU91 QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN AQkBFhFhbWVfZGt1QGNpc2NvLmNvbTEuMAkGA1UEBhMCSU4xEjAQBGNVBAgTCUth cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVdZXNjbzETMBEG A1UECzMkMmV0c3RvcnFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN AQEBBQADSAwSAJBAMW/7b3+DXJPANBSIHHzluNccNM87ypyzwuoSNZXOMperXXI OzyBAGiXT2ASFuUoWq1iDM8rO/41jf8RxyYKvysCAwEAAaOBvzCBvDALBgNVHQ8E BAMCACYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFggQUJyJyRoMbrCNMRU2OyRhQ GgsWbHEwawYDVR0fBGQWYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs L0FwYXJlYU91YU91MENBLmNybDAAwOC6gLIYqZmlsZTovL1xc3N1LTA4XEN1cnRfbnJv bGxcQXBhcm5hJTlwaQ0EuY3JSMGAGCSsGAQQBgjcVAQQDAGEAMA0GCSqGSIb3DQE BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaNgLh0AFcT0rEyuYt/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</pre>	<p>Prompts you to cut and paste the certificate of the CA. Use the same name that you used when declaring the CA.</p> <p>Note The maximum number of trust points you can authenticate to a specific CA is 10.</p>



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 34-14), 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. OSCP provides the means to check the current CRL on the CA. However, OSCP can generate network traffic that can impact network efficiency. Using both local CRL checking and OSCP provides the most secure method for checking for revoked certificates.

Send documentation comments to mdsfeedback-doc@cisco.com



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 ocsp	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 ocsp	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.

Send documentation comments to mdsfeedback-doc@cisco.com

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

	Command	Purpose
Step 1	<pre>switch# config terminal switch(config)#</pre>	Enters configuration mode.
Step 2	<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----- MIIBqzCCARQCAQAwHDEaMBGGA1UEAxMRVmVnYXNjby5jb20wgZ8wDQYJ KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8r141KY 0JC6ManNy4qxk8VeMXZSiLJ4JgTzKwDxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhhVpj+rargZvHtGJ91XTq4WoVksCzXv8S VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCsGSIb3DQEJ DjEpMCCwJQYDVR0RAQH/BBswGYIRVmVnYXNjby5jb22HBKwWH6IwDQYJ KoZIhvcNAQEEBQADgYEAKT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt PftrNcWUE/pw6HayfQl2T3ecgNwe12d15133YBF2bktExiI6U188nTOjg1XMjja8 8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0= -----END CERTIFICATE REQUEST-----</pre>	<p>Generates a certificate request for an authenticated CA.</p> <p>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.</p>

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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----- MIIEADCCA6qgAwIBAgIKCj0OoQAAAAAADANBgkqhkiG9w0BAQUFADCBkDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAK1OMRIwEAYDVQQIEw1LYXJuYXRha2EzEjAQBgNVBACTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ21zY28xEzARBgNVBAStCm5ldHN0b3JhZ2UxEjAQBGNVBAmtCUFwYXJuYSBDQTAeFw0wNTEwMTIwMzAyNDBaFw0wNjEwMTIwMzEyNDBaMBwGjAYBgNVBAMTEVZlZ2FzLTEuY21zY28uY29tMIGfMA0GCsGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41Cdq1WkJKjSICdP1fK5eJSmNCQujGpzcKsZPFxjF2UoiyeCYE8y1ncWYw5E08rJ47g1xr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4GbX7RifdV06uFqFZEgs17/Elash9LxLwIDAQABO4ICEzCCAg8wJQYDVR0RAQH/BBswGYIRVnVnYXMTMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrRbhWmlVyo9jngMIHMBGNVHSMEGcQwgcGAFCCo8kaDG6wjTEVNjskYUBoLFmxxoYGWpIGTMIGQMSAwHgYJKoZiHvcNAQkBFhFhbWfuZGt1QGNpc2NvLmNvbTELMakGA1UEBhmCSU4xEjAQBgNVBAGTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDAxNjZETMBEGA1UECzMkbnV0c3RvcnFnZTESMBAGA1UEAxMJQXBhcm5hIENBghAFYnKJrLQZ1E9JEiWMrR16MGsGA1UdHwRkMGtWlQAsocCqGKGh0dHA6Ly9zcmU2UtdMDgVQ2VydeVUcm9sbC9BcGFybmE1MjBDQs5jcmwMKAUocYgKzpbGU6Ly9cXHNzZS0wOFxZDZlJ0Rw5yb2xsXEFwYXJuYSUyMENBLmNybDCBbigYIKwYBBQUHAEQEFjB8MDSGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3NlLTA4X0FwYXJuYSUyMENBLmNydA9BggrBgEFBQcwAoYxZmlsZTovL1xccc3NlLTA4XEN1cnRFbnJvbGwvc3NlLTA4X0FwYXJuYSUyMENBLmNydANBgkqhkiG9w0BAQUFAANBAdBGBGsb7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflwE36cIZu4WsExREqxbTk8ycx7V5o=-----END CERTIFICATE-----	Prompts you to cut and paste the identity certificate for the CA named admin-ca. Note The maximum number of identity 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 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 and save it to an external server (see the “Exporting and Importing Identity Information in PKCS#12 Format” section on page 34-13).



Note

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

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Monitoring and Maintaining CA and Certificates Configuration

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

- [Exporting and Importing Identity Information in PKCS#12 Format, page 34-13](#)
- [Configuring a CRL, page 34-14](#)
- [Deleting Certificates from the CA Configuration, page 34-14](#)
- [Deleting RSA Key-Pairs from Your Switch, page 34-15](#)
- [Displaying Key-Pair and CA Information, page 34-15](#)

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	<code>switch# config terminal</code> <code>switch(config)#</code>	Enters configuration mode.
Step 2	<code>switch(config)# crypto ca export</code> <code>admin-ca pkcs12 bootflash:adminid.p12</code> <code>nbv123</code>	Exports the identity certificate and associated key-pair and CA certificates for trust point <code>admin-ca</code> to the file <code>bootflash:adminid.p12</code> in PKCS#12 format, protected using password <code>nbv123</code> .
Step 3	<code>switch(config)# exit</code> <code>switch#</code>	Returns to EXEC mode.
Step 4	<code>switch# copy bootflash:adminid.p12</code> <code>tftp:adminid.p12</code>	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	<code>switch# copy tftp:adminid.p12</code> <code>bootflash:adminid.p12</code>	Copies the PKCS#12 format file from a TFTP server.
Step 2	<code>switch# config terminal</code> <code>switch(config)#</code>	Enters configuration mode.
Step 3	<code>switch(config)# crypto ca import</code> <code>admin-ca pkcs12 bootflash:adminid.p12</code> <code>nbv123</code>	Imports the identity certificate and associated key-pair and CA certificates for trust point <code>admin-ca</code> from the file <code>bootflash:adminid.p12</code> in PKCS#12 format, protected using password <code>nbv123</code> .



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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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 switch(config-trustpoint)# delete certificate force	Deletes 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.

Send documentation comments to mdsfeedback-doc@cisco.com

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 34-10.

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 34-16](#)
- [Downloading a CA Certificate, page 34-19](#)
- [Requesting an Identity Certificate, page 34-23](#)
- [Revoking a Certificate, page 34-29](#)
- [Generating and Publishing the CRL, page 34-32](#)

Send documentation comments to mdsfeedback-doc@cisco.com

- [Downloading the CRL, page 34-33](#)
- [Importing the CRL, page 34-35](#)

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 34-19)**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
kDEGMb4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjb20xMjB0xMjB0xMjB0xMjB0
MRIwEAYDVQQIEw1LYXJuYXRha2ExEjAQBGNVBACTCUJhbmdbG9yZTEOMAwGA1UE
ChMFQ21zY28xEzARBGNVBAStCm5ldHN0b3JhZ2UxEjAQBGNVBAMTCUFwYXJuYSBD
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
```


Send documentation comments to mdsfeedback-doc@cisco.com

```
AQkBFhFhbWfUzGtLQGNpc2NvLmNvbTELMakGA1UEBhMCSU4xEjAQBGNVBAGTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2FsY2Fsb3JlMQ4wDAYDVQKKEwVdaXNjbzETMBEG
A1UECzMKbmV0c3RvcnFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBSIHHzluNccNM87ypyzwuoSNZXOMperXXI
OzyBAGixT2ASFuUOWQ1iDM8rO/41jf8RxyYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyJyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJlYSUyMENBLmNybDAwOC6gLIYqZmlsZTovL1xccc3NlLTA4XENlcnRFbnJv
bGxlcXhcm5hJTIwQ0EueY3JsbGAgCSsGAQQBgjcvVAQQAQAgEAMA0GCSqGSIb3DQEB
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-----
MIIBqzCCARQCAQAwHDEaMBGGA1UEAxMRVnVnYXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8r14lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKwDxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSczXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMgbmJ2MTIzMDYGCsGSIb3DQEB
DjEpMCcwJQYDVR0RAQH/BBswGIIRVnVnYXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEBBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6U188nTOjg1XMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----
```

```
Vegas-1(config)#
```

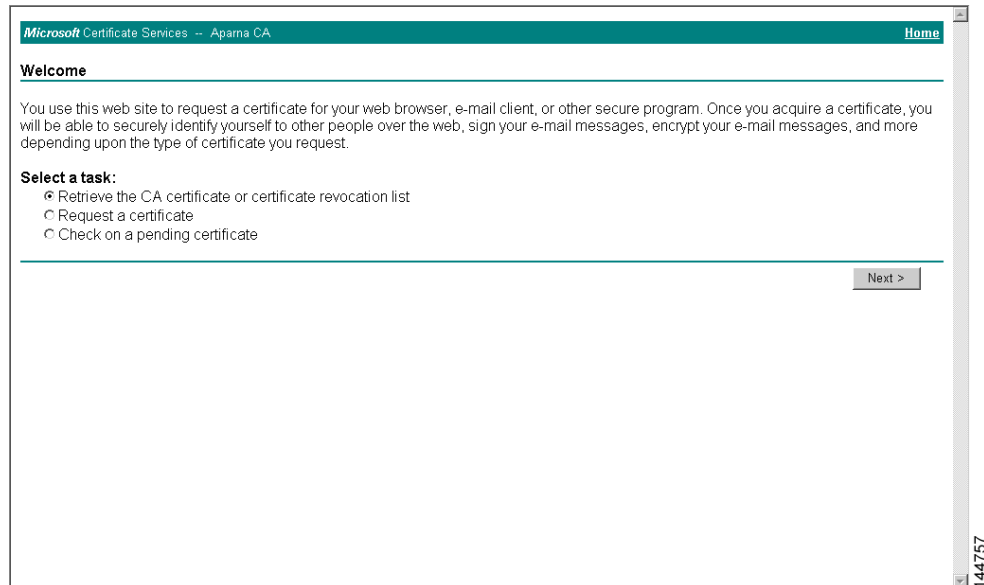
Step 9 Request an identity certificate from the Microsoft Certificate Service web interface (see the “Requesting an Identity Certificate” section on page 34-23).

Send documentation comments to mdsfeedback-doc@cisco.com

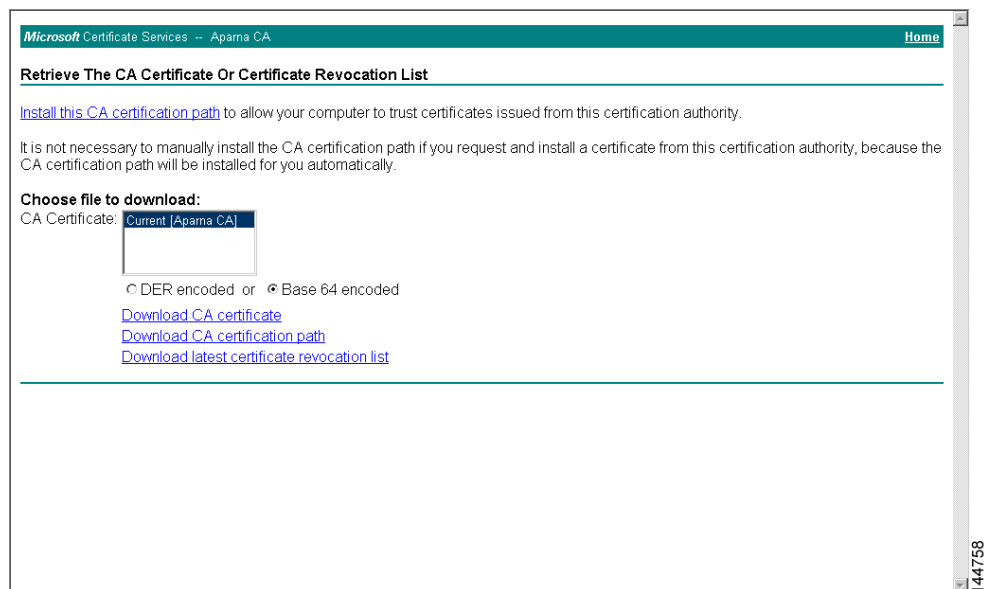
Downloading a CA Certificate

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.

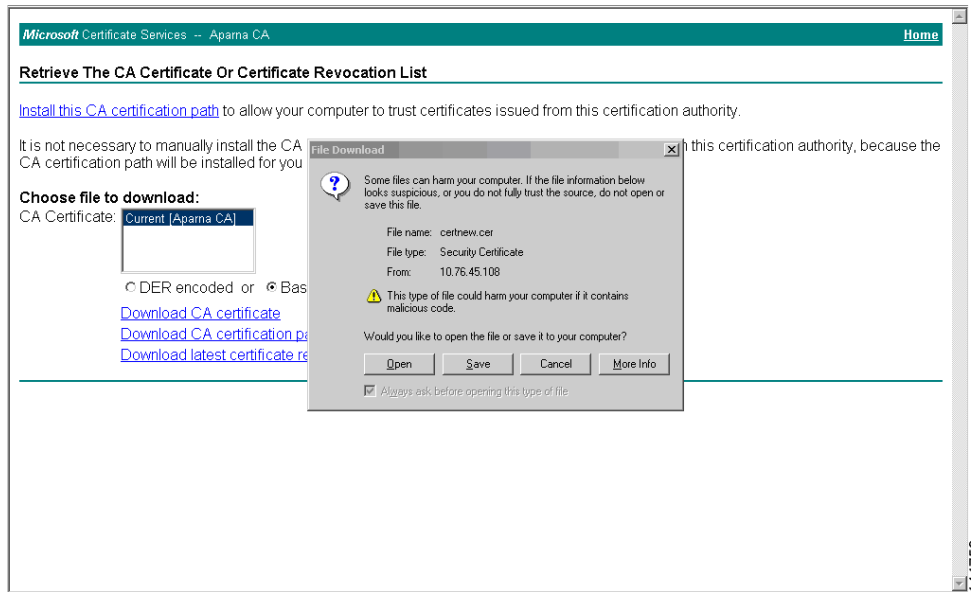


- Step 2** Select the CA certificate file to download from the displayed list. Click the **Base 64 encoded** radio button, and click the **Download CA certificate** link.

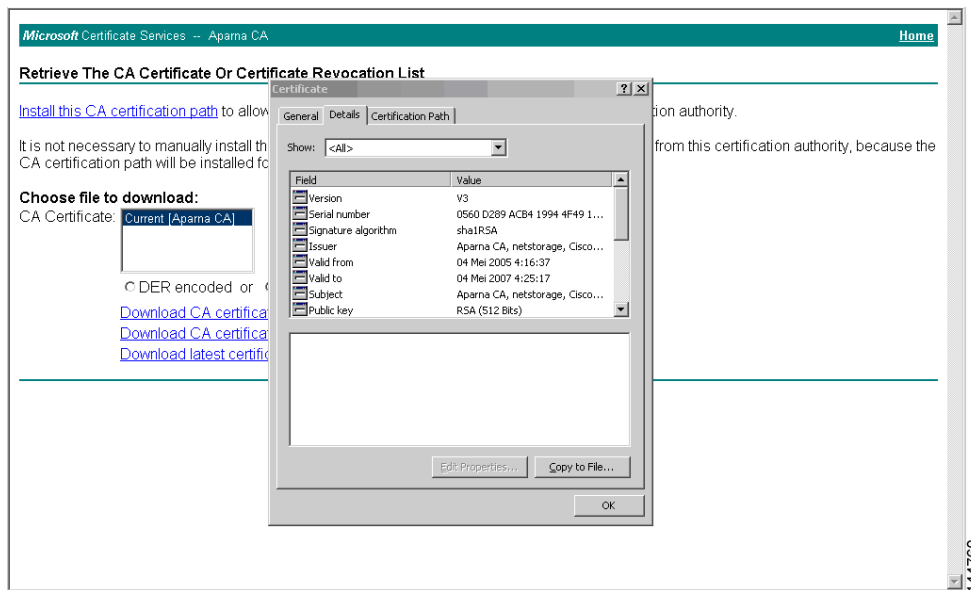


- Step 3** Click the **Open** button in the File Download dialog box.

Send documentation comments to mdsfeedback-doc@cisco.com

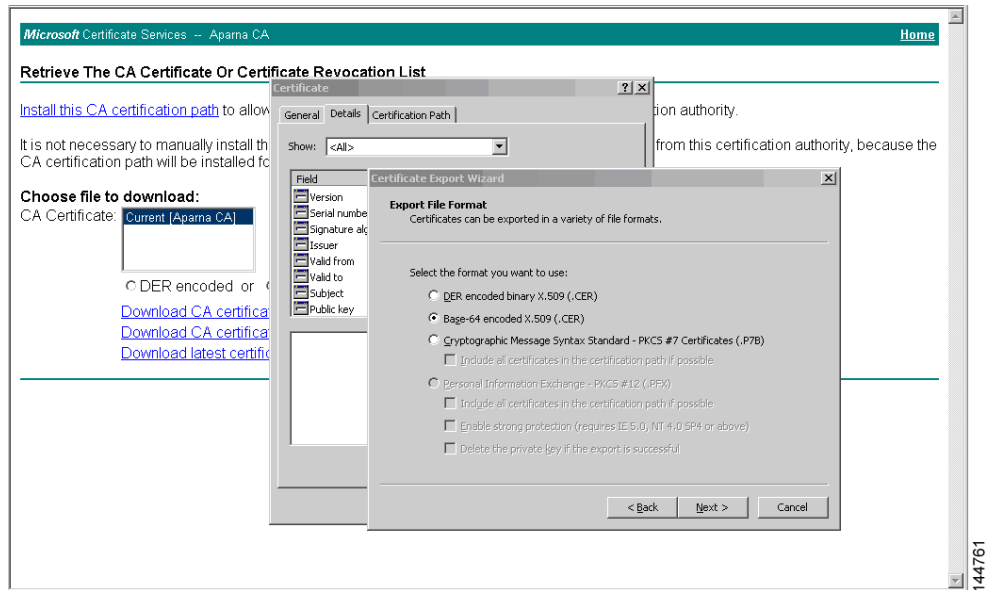


Step 4 Click the **Copy to File** button in the Certificate dialog box and click **OK**.

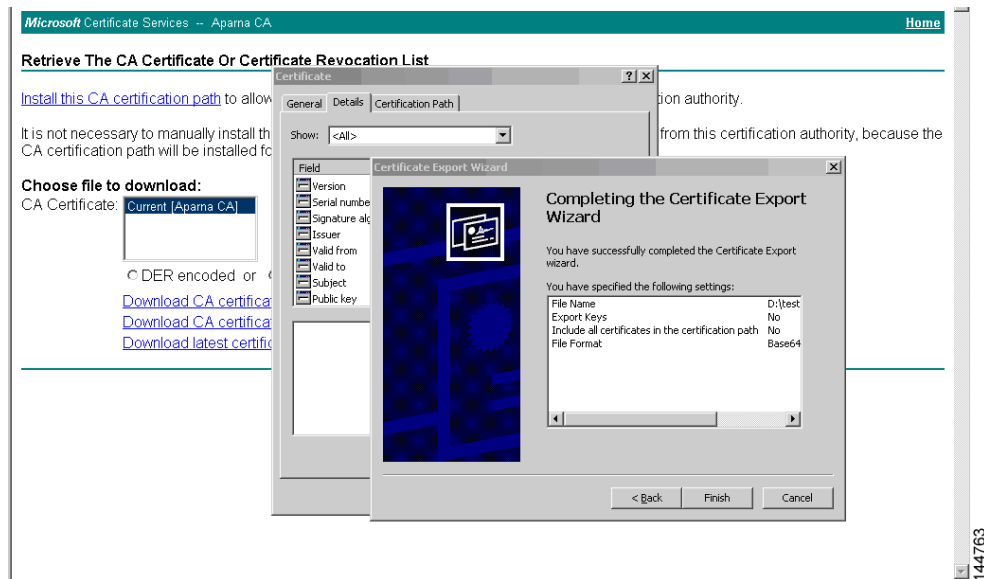


Step 5 Select the **Base-64 encoded X.509 (CER)** on the Certificate Export Wizard dialog box and click **Next**.

Send documentation comments to mdsfeedback-doc@cisco.com



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



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

Send documentation comments to mdsfeedback-doc@cisco.com

```

C:\WINNT\system32\cmd.exe
D:\testcerts>type aparnaCA.cer
-----BEGIN CERTIFICATE-----
MIIC4jCCAgYgAwIBAgIQBWDSiay0GZRP5RI1jK0Ze jANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmrRrZUBjaXNjb55jb20xCzAJBgNVBAYTAK1O
MRIwEAYDUQIETw1LXXJuYXRha2ExEjAQBgNVBAMTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ21zY28xZzAARBgNVBA5TCm5ldHN0b3JhZ2UxEjAQBgNVBAMTGFwYXJyYXN0
QTAeFw0wNTA1MDMwMjQ2MzdaFw0wNTA1MDMwMjQ2MzdaMIIMDAIwGQMSAwHgYJKoZI
hvcNAQkBFHhbbWZGc2l0Gmpe2NoLmNvbTElMAkGA1UEBhMCSU4xEjAQBgNVBAgT
CUchcm5hdGFrYTESMBAAGA1UEBxMJQmFuZ2Z2Fsb3JlM04wDAYDUQkEwUdaXNjbz
ETMBEQA1UECzMkbnU0c3RvcnFnZTESMBAAGA1UEAxMjQXhcm5hIENBMFw0DQYJKoZI
hvcNAQEBBQADSwAwSAJBAMw/7b3+DXJPANBSIHHzluNccNM87ypyzwuoSNZKOMpe
RXXIOzYBAQYXIT2ASFuU0wQ1iDM8r0/41jF8RxyYKvysCAwEAa0BuzCBvDALBg
NUHQ8EBAACAcywDwYDUR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyYyRoMbrCNMRU
20yRhQGgsWbHEwawYDUR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0
RW5yb2xsL0FwYXJyYXN0MENBLmNvbDAwC6gLIYgZmlsZTovL1xc3NLLTA4XEN1
cnRFBnJvbGxcQXhcm5hJTl0Q0EuY3JsMBAGCSsGAQQBgjcUAQQDAgEAMAA0GCS
qGSIb3DQEBBQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaQNgLh0AFcI0rEyuyt
/WYGPzksF9EaNBG7E0oN66zex0EOEfG1Us6mXp1/w==
-----END CERTIFICATE-----

D:\testcerts>

```

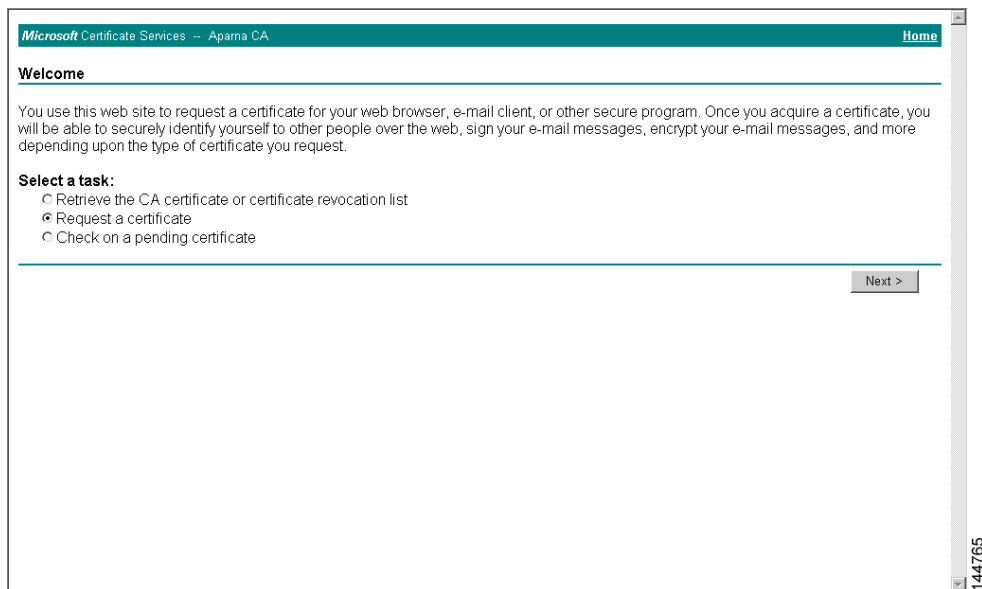
144764

Send documentation comments to mdsfeedback-doc@cisco.com

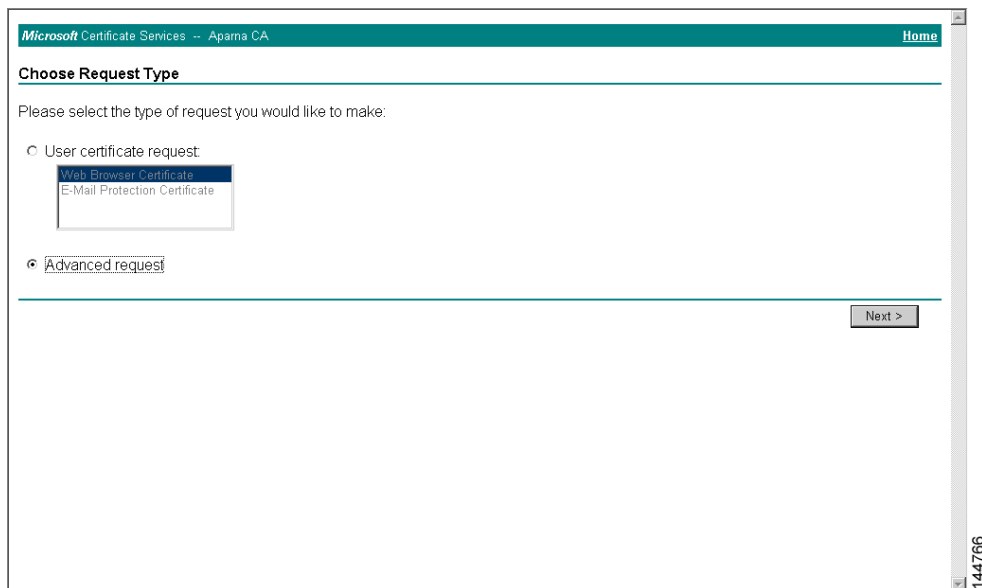
Requesting an Identity Certificate

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

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



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



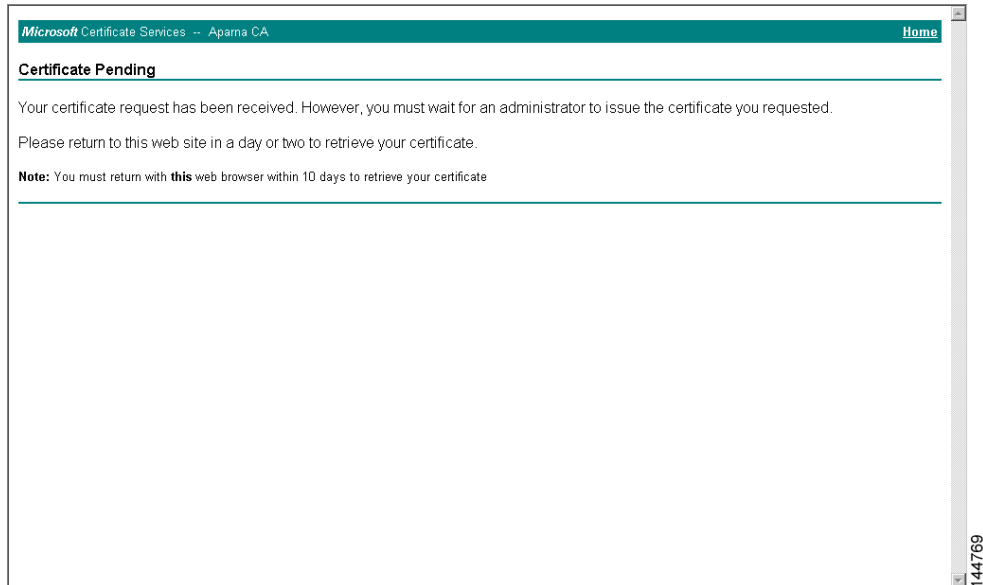
Send documentation comments to mdsfeedback-doc@cisco.com

- 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**.

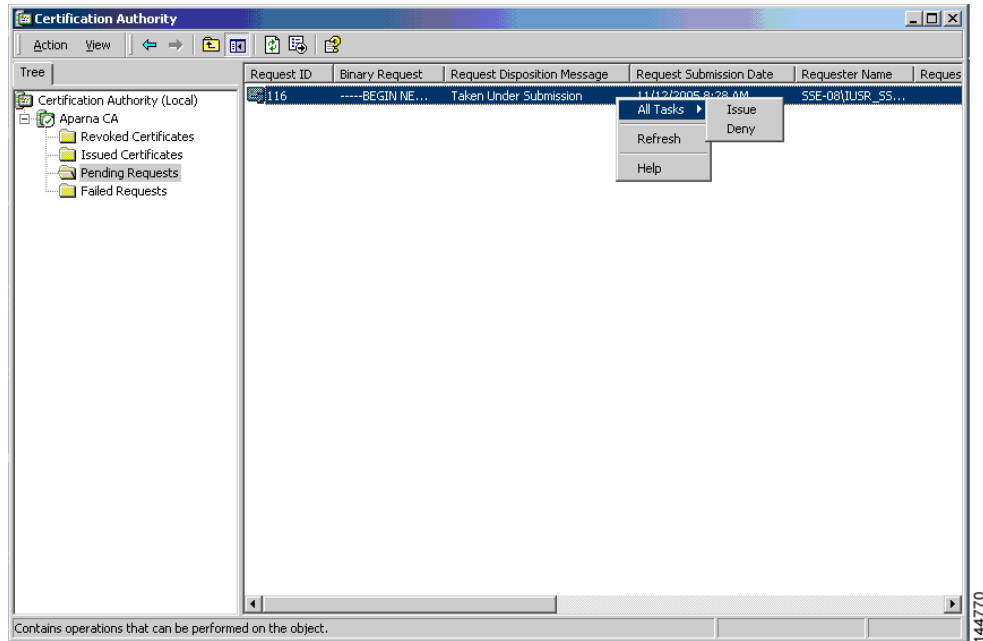
- Step 4** Paste the base64 PKCS#10 certificate request in the Saved Request text box and click **Next**. The certificate request is copied from the MDS switch console (see the “Generating Certificate Requests” section on page 34-10 and “Configuring Certificates on the MDS Switch” section on page 34-16)

Send documentation comments to mdsfeedback-doc@cisco.com

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



Step 6 The CA administrator approves the certificate request.



Send documentation comments to mdsfeedback-doc@cisco.com

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

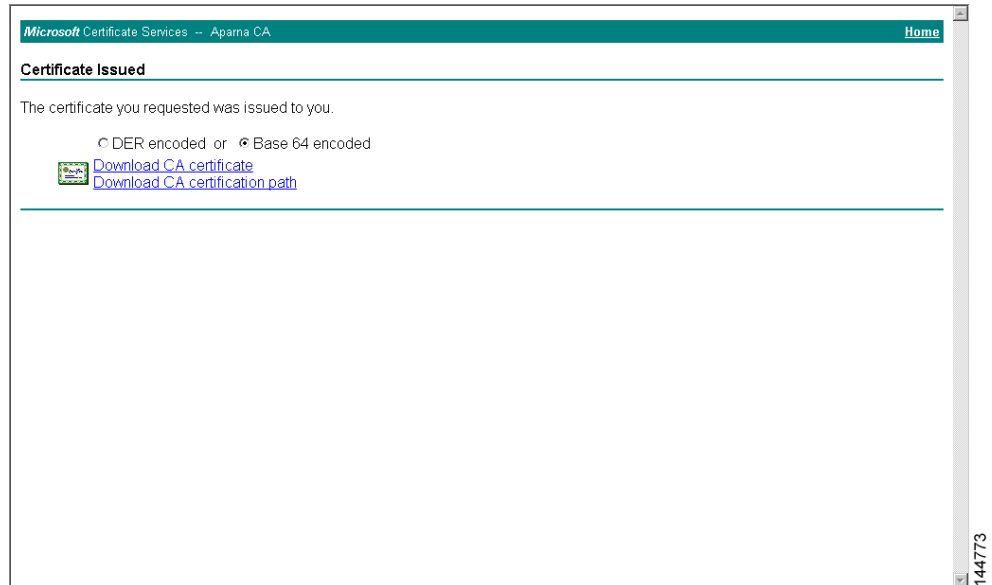
The screenshot shows the Microsoft Certificate Services web interface for the 'Apama CA'. The page title is 'Microsoft Certificate Services -- Apama CA' and there is a 'Home' link. The main heading is 'Welcome'. Below this, there is a paragraph explaining the site's purpose: 'You use this web site to 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.' Underneath, the 'Select a task:' section contains three radio button options: 'Retrieve the CA certificate or certificate revocation list', 'Request a certificate', and 'Check on a pending certificate'. The 'Check on a pending certificate' option is selected. A 'Next >' button is located at the bottom right of the form area. A vertical ID number '144771' is visible on the right side of the browser window.

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

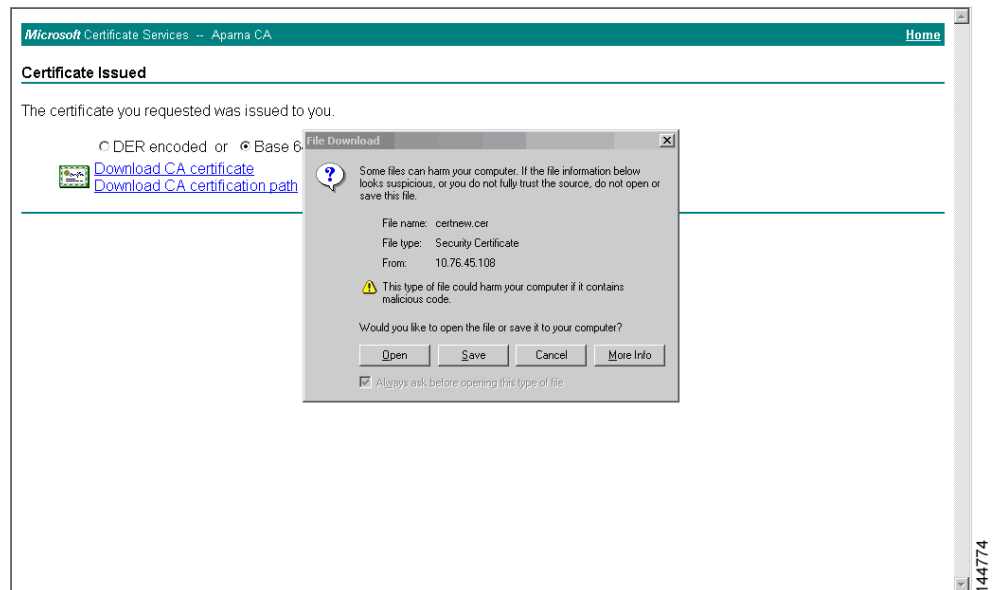
The screenshot shows the Microsoft Certificate Services web interface for the 'Apama CA' at the 'Check On A Pending Certificate Request' page. The page title is 'Microsoft Certificate Services -- Apama CA' and there is a 'Home' link. The main heading is 'Check On A Pending Certificate Request'. Below this, there is a prompt: 'Please select the certificate request you want to check'. A list box contains one entry: 'Saved-Request Certificate (12 November 2005 20:30:22)'. A 'Next >' button is located at the bottom right of the form area. A vertical ID number '144772' is visible on the right side of the browser window.

Send documentation comments to mdsfeedback-doc@cisco.com

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

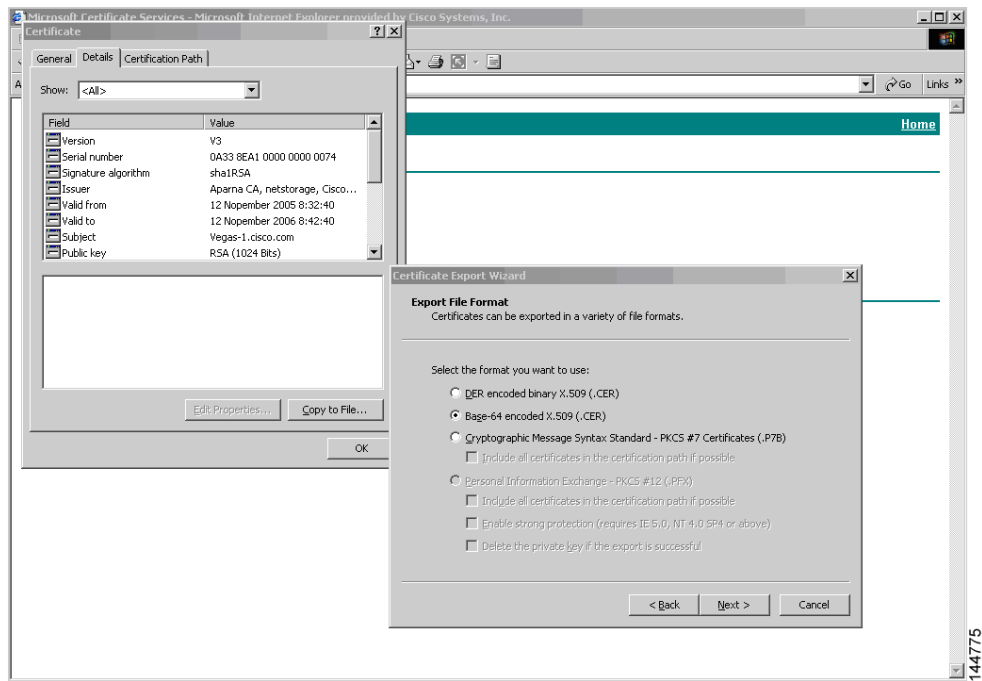


Step 10 Click **Open** on the File Download dialog box.

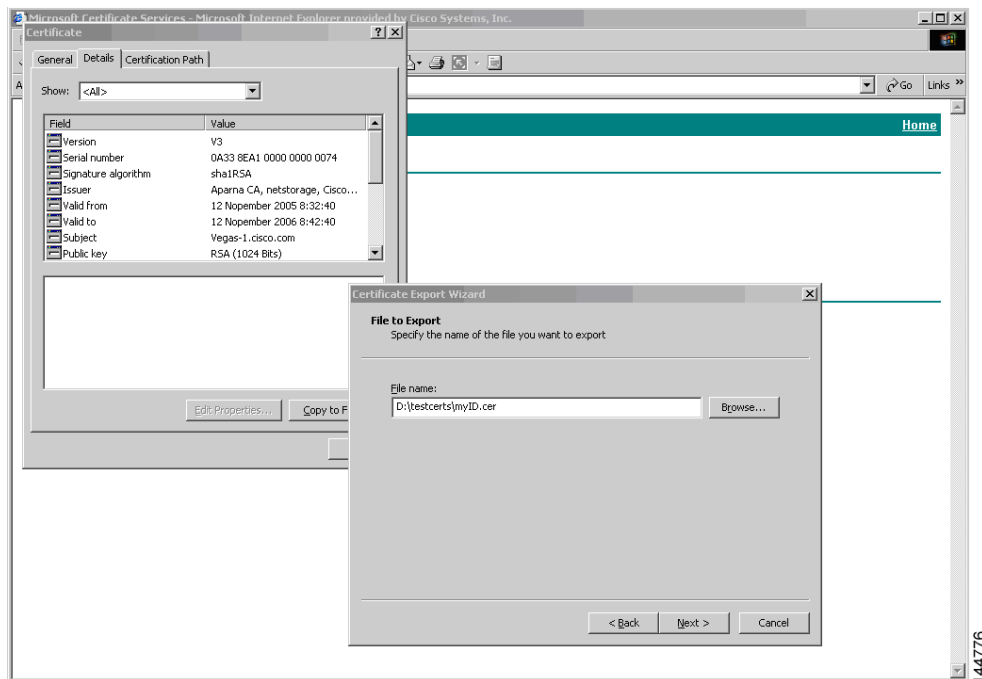


Send documentation comments to mdsfeedback-doc@cisco.com

- 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**.

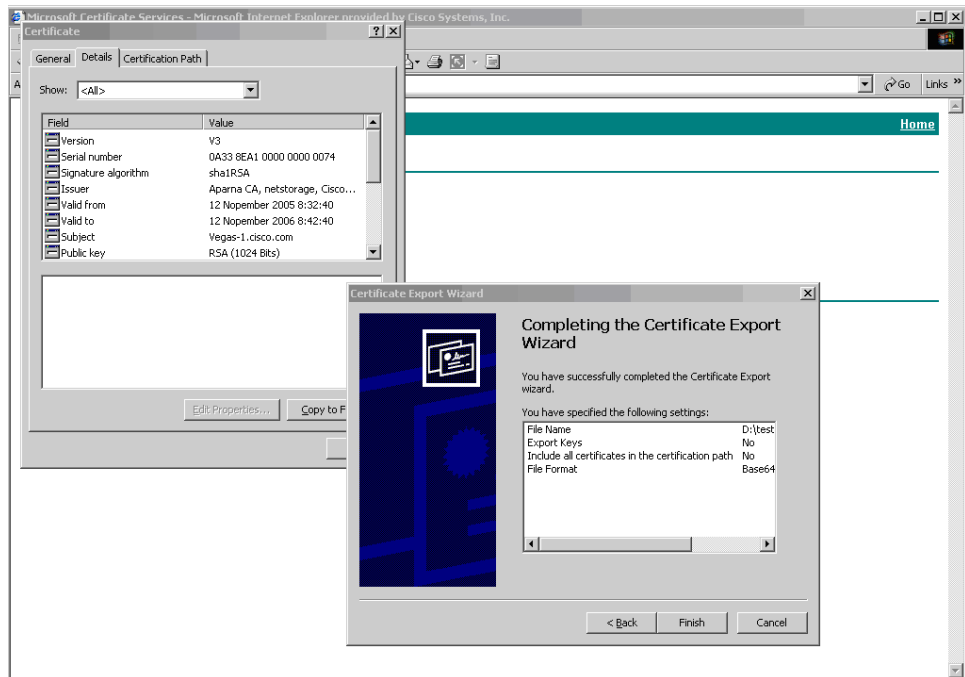


- Step 12** Enter the destination file name in the File name: text box on the Certificate Export Wizard dialog box, then click **Next**.

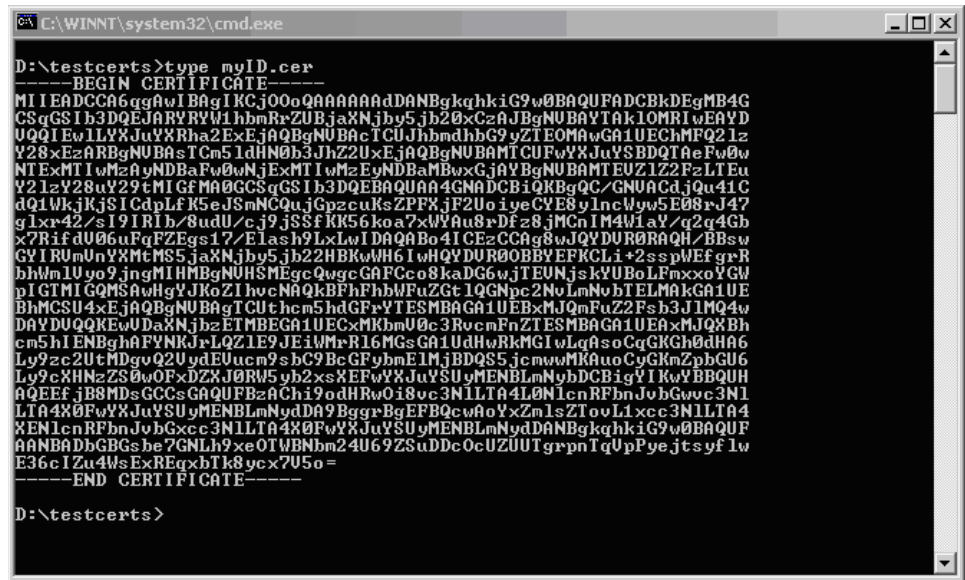


- Step 13** Click **Finish**.

Send documentation comments to mdsfeedback-doc@cisco.com



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

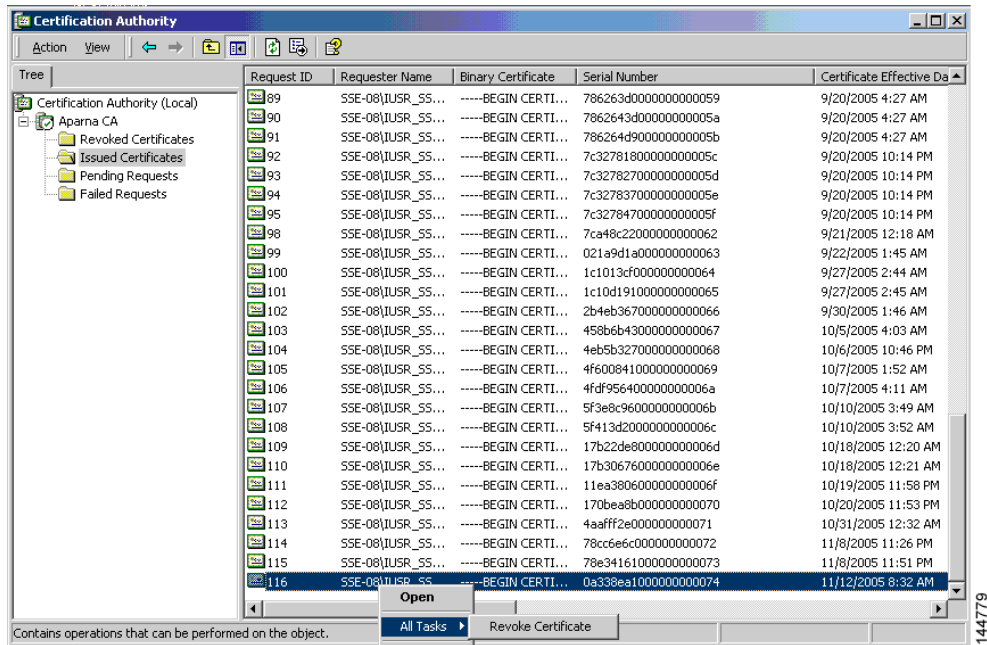


Revoking a Certificate

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

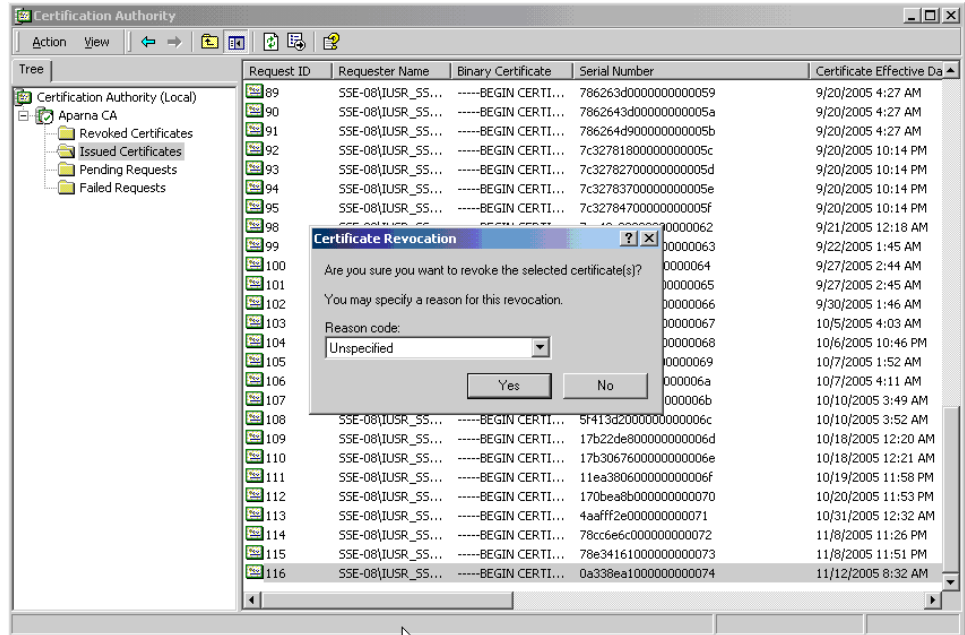
Send documentation comments to mdsfeedback-doc@cisco.com

- 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**.

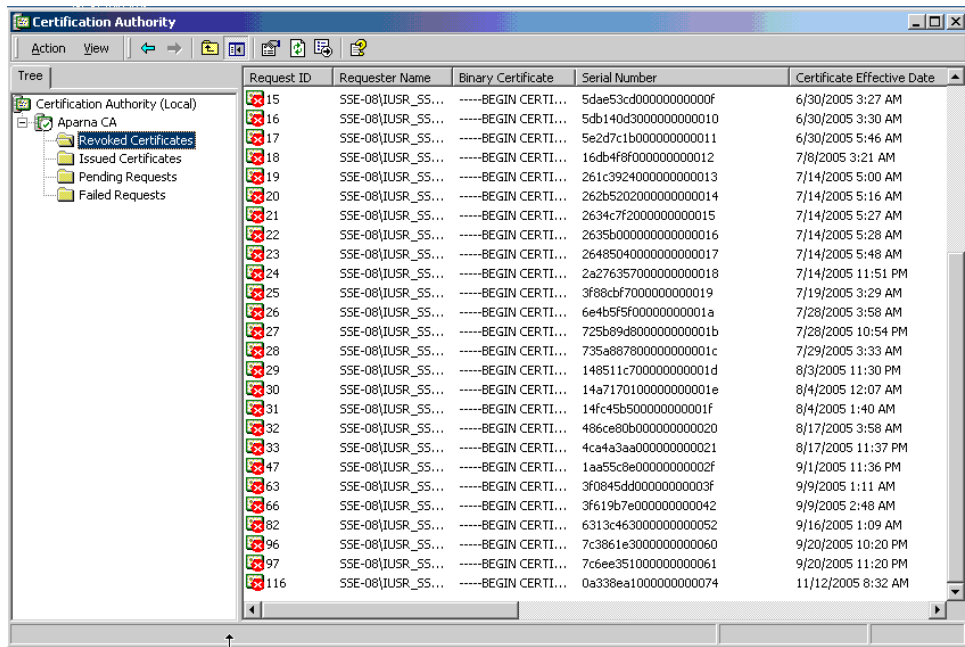


Send documentation comments to mdsfeedback-doc@cisco.com

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



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

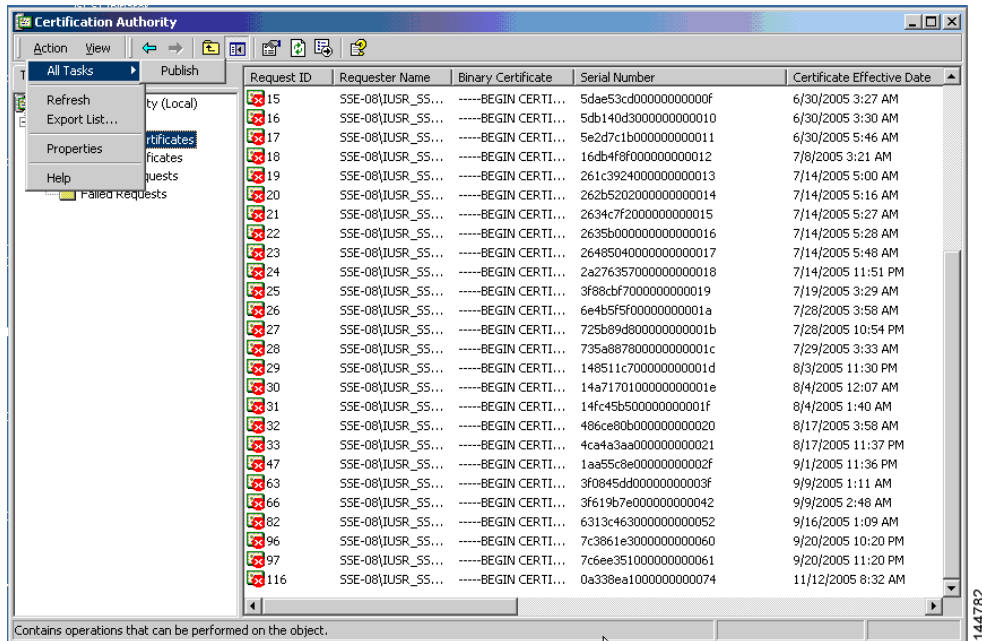


Send documentation comments to mdsfeedback-doc@cisco.com

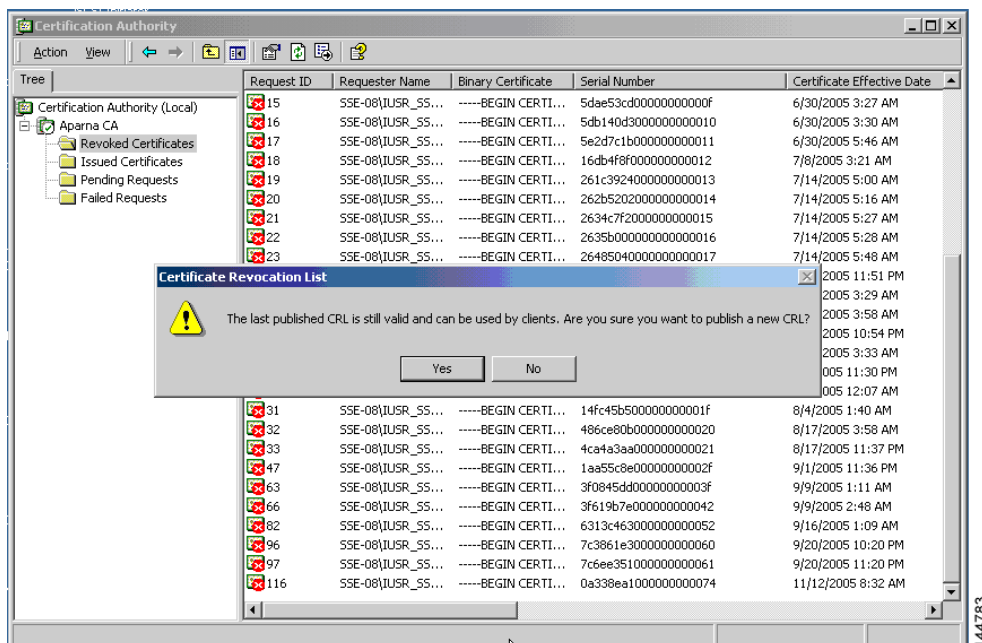
Generating and Publishing the CRL

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.



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

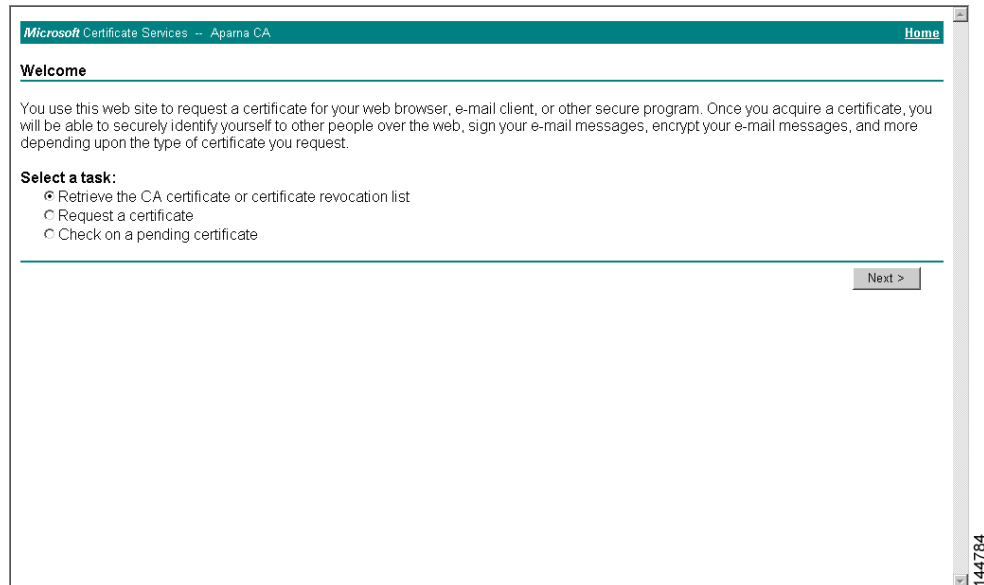


Send documentation comments to mdsfeedback-doc@cisco.com

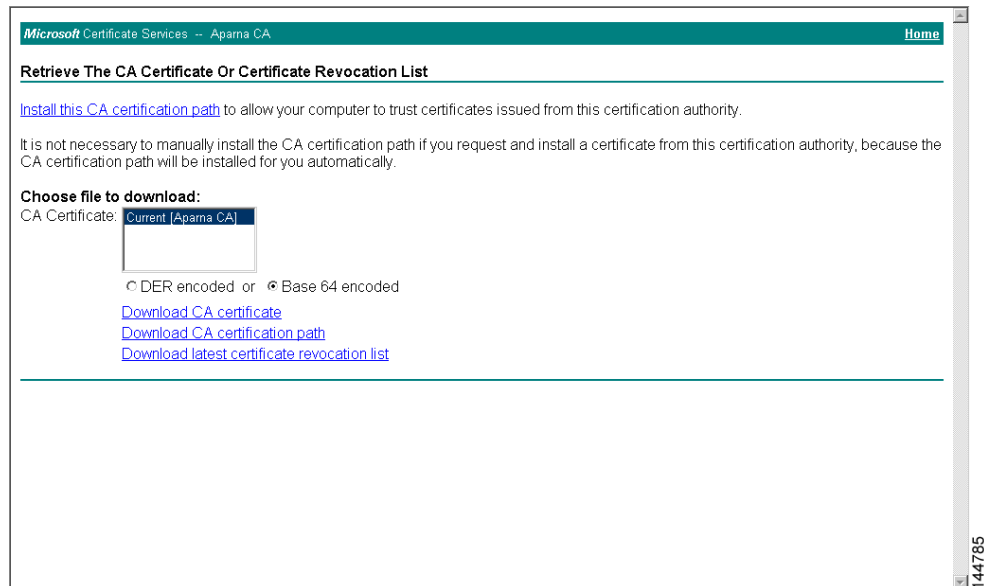
Downloading the CRL

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**.

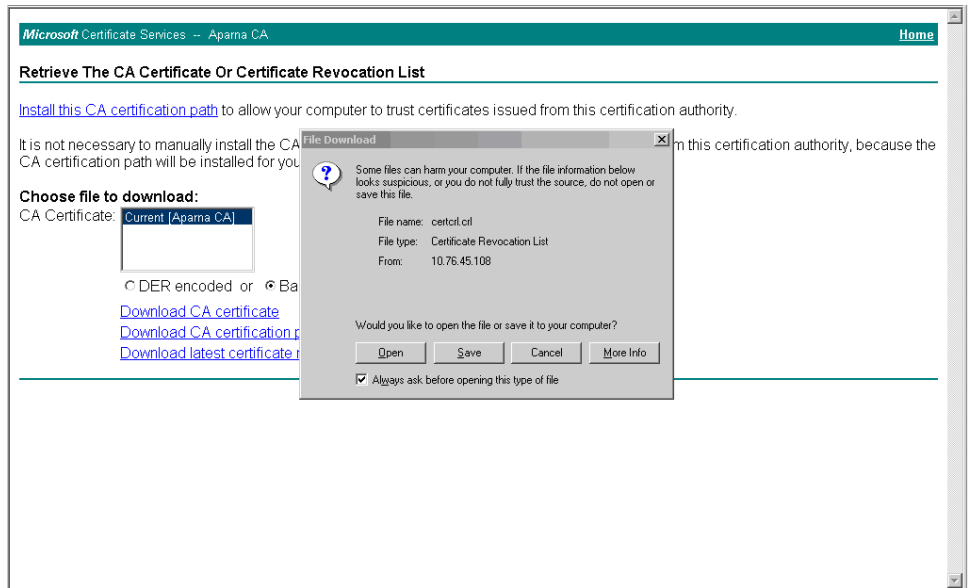


- Step 2** Click the **Download latest certificate revocation list** link.

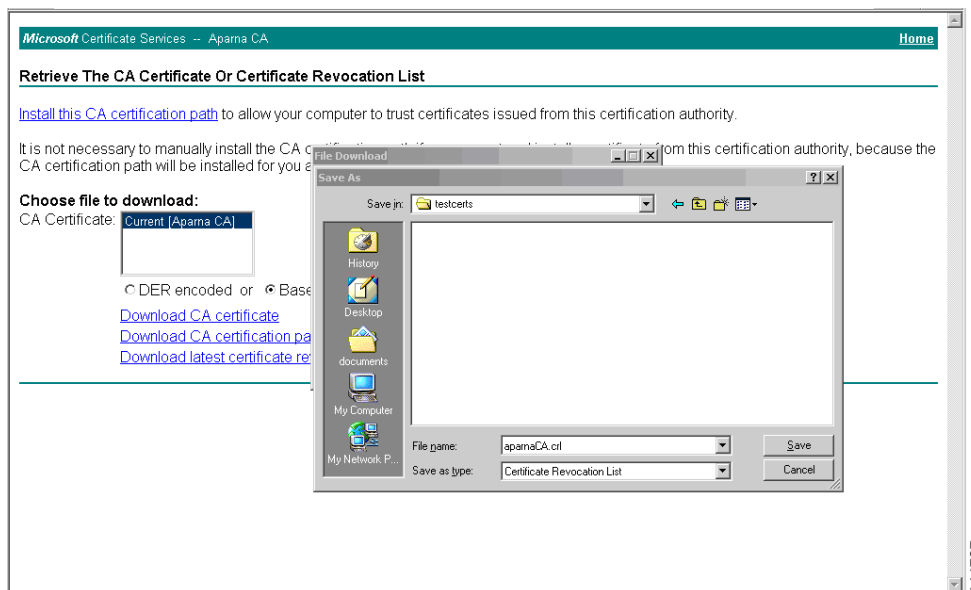


- Step 3** Click **Save** in the File Download dialog box.

Send documentation comments to mdsfeedback-doc@cisco.com



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



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

Send documentation comments to mdsfeedback-doc@cisco.com

```

C:\WINNT\system32\cmd.exe
D:\testcerts>type apranaCA.crl
-----BEGIN X509 CRL-----
MIIGBTCCBa8CAQEWdQYJKoZIhvcNAQEFBQAwwZANIDAEBgkqhkiG9w0BCQEWEWft
YU5ka2UAY21zY28uYy29tMQswCQYDUQGEwJITjESMBAGA1UECBMJS2FybmF0YVWt
hMRIwEAYDUQGEwJICyW5nVWxucmUxdjAMBgNUNBAoTBUnc2NvMRMwEQYDUQQLExpu
ZkZzdG9yYVtdIMR1wEAYDUQGEw1BcGFybWVzEgQ0EXDTA1MTExMjA0MzYwNFoXDTA1
MTExOTIzNTYwNFowggSxMBSCCmEbCaEAAAAAAAAIXDTA1MDgxnjI1xNTI1xOUowGwIK
TNSGTgAAAAAAAAxcNMDUwODE2MjE1MjE1WjAbaGppM/CtCAAAAAAAAAEFw0wNTA4MTYy
MTUyNDFAmBScCmXpnsIAAAAAAAAAUXDTA1MDgxnjI1xNTI1MlOwGwIKbM93AAAAAAAA
BhcNMDUwNjA4MDAxMjA0WjAbaGppwzE/AAAAAAAAAFw0wNTA4MTYyMTUzMTUaMBSc
Ck2bERYAAAAAAAAAgXDTA1MDgxnjI1xNTMxNUowKQIKUggCMAAAAAAAAAACRcNMDUwNjI3
MjM0NzA2WjAMMAoGA1UdFQDDCgECMCC1NjRUVVAAAAAAAAoXDTA1MDYyNzIzNDcy
MlOwDDAKBgNURUeAwoBAjAbaGppT0Rc8AAAAAAAAALFw0wNTA3MDQxODAwMDFAmAw
CgYDUROUBAMKAQYwGwIKWR56zgAAAAAAAAADbcNMDUwODE2MjE1MzE1WjAbaGppdP9Uu
AAAAAAAAANFw0wNTA2MjkyMjA3MjUaMAwwCgYDUROUBAMKAQEWGwIKKXat3EwAAAAA
AAdhcNMDUwNzE0MDAzMzU2WjAbaGppdR1PNAAAAAAAAAFw0wNTA4MTYyMTUzMTUaMBSc
C12xQNMAAAAAAAAABAxDTA1MDgxnjI1xNTMxNUowKQIKXii18GwAAAAAAAAERcNMDUwNzA2
MjExMjEwWjAMMAoGA1UdFQDDCgEFMBScCChbbT48AAAAAAAABIxDTA1MDgxnjI1xNTMx
NUowCwIKJhw5JAAAAAAAAEXcNMDUwODE2MjE1MzE1WjAbaGppMk1ICAAAAAAAAUFw0w
NTA3MTQwMDMzMTBaMBScC1Y0x/IAAAAAAAAABUxDTA1MDcxNDwzMTU0NUowGwIKJjW
AAAAAAAAAFhcNMDUwNzE0MDAzMTUxWjAbaGppMFBAAAAAAAAAFw0wNTA3MTQwMDM5
MjUaMBScCionY1cAAAAAAAAABgXDTA1MDgxnjI1xNTMxNUowGwIKP4jL9wAAAAAAAAGRcN
MDUwODE2MjE1MzE1WjAbaGppuS19fAAAAAAAAAFw0wNTA4MTYyMTUzMTUaMBScCnJb
idgAAAAAAAABsXDTA1MDgxnjI1xNTMxNUowGwIKc1q1eAAAAAAAAAHbcNMDUwODE2MjE1
MzE1WjAbaGppUhhHAAAAAAAAADFw0wNTA4MTYyMTUzMTUaMBScCChSnFwEAAAAAAAAAB4X
DTA1MDgxnjI1xNTMxNUowGwIKFPxFcQAAAAAAAAHxcNMDUwODE3MTgzMDQyWjAbaGppI
bOgLAAAAAAAAAgFw0wNTA4MTcxODMwNDNaMBScCkyko6oAAAAAAAAACEXDTA1MDgxnzE4
MzA0M1owGwIKGgUcJgAAAAAAAAALxcNMDUwOTA1MTcxNzA2WjAbaGpp/CEXAAAAAAAAAF
w0wNTA5MDgyMDI0MzJAMBSCCj9hm34AAAAAAAAEIXDTA1MDkwODI1xNDg00FowGwIK
YxPEYwAAAAAAAAhcnMDUwOTE5MTczNzE4WjAbaGpp8OGHjAAAAAAAABgFw0wNTA5MjA0
NzUyNTZAMBSCCnxu41EAAAAAAAAACEXDTA1MDkwMDE4NTIzMFowGwIKCj00oQAAAAAAAA
dBCNMDUxMTYgMDQzNDQyWgA1MDMwHwYDUROUjBBBwFoAUJyJyRoNhrCMRRU20yRhQ
GgsWbHEwEAYJKoYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEFBQAQDQALy91DCRhi
HoCUBm9GwzYjJJEjqeU168CuaacFP3rkM8YyZVyu1c32R/UvU6a5xgrAC/$bsEa
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
```

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

```

1.3.6.1.4.1.311.21.1:
...
Revoked Certificates:
 Serial Number: 611B09A1000000000002
 Revocation Date: Aug 16 21:52:19 2005 GMT
Serial Number: 4CDE464E000000000003
 Revocation Date: Aug 16 21:52:29 2005 GMT
 Serial Number: 4CFC2B42000000000004
 Revocation Date: Aug 16 21:52:41 2005 GMT
 Serial Number: 6C699EC2000000000005
 Revocation Date: Aug 16 21:52:52 2005 GMT
 Serial Number: 6CCF7DDC000000000006
 Revocation Date: Jun 8 00:12:04 2005 GMT
 Serial Number: 70CC4FFF000000000007
 Revocation Date: Aug 16 21:53:15 2005 GMT
 Serial Number: 4D9B1116000000000008
 Revocation Date: Aug 16 21:53:15 2005 GMT
 Serial Number: 52A80230000000000009
 Revocation Date: Jun 27 23:47:06 2005 GMT
 CRL entry extensions:
 X509v3 CRL Reason Code:
 CA Compromise
Serial Number: 5349AD46000000000000A
 Revocation Date: Jun 27 23:47:22 2005 GMT
 CRL entry extensions:
 X509v3 CRL Reason Code:
 CA Compromise
Serial Number: 53BD173C000000000000B
 Revocation Date: Jul 4 18:04:01 2005 GMT
 CRL entry extensions:
 X509v3 CRL Reason Code:
 Certificate Hold
Serial Number: 591E7ACE000000000000C
 Revocation Date: Aug 16 21:53:15 2005 GMT
 Serial Number: 5D3FD52E000000000000D
 Revocation Date: Jun 29 22:07:25 2005 GMT
 CRL entry extensions:
 X509v3 CRL Reason Code:
 Key Compromise
Serial Number: 5DAB7713000000000000E
 Revocation Date: Jul 14 00:33:56 2005 GMT
 Serial Number: 5DAE53CD000000000000F
 Revocation Date: Aug 16 21:53:15 2005 GMT
 Serial Number: 5DB140D30000000000010
 Revocation Date: Aug 16 21:53:15 2005 GMT
 Serial Number: 5E2D7C1B0000000000011
 Revocation Date: Jul 6 21:12:10 2005 GMT
 CRL entry extensions:
 X509v3 CRL Reason Code:
 Cessation Of Operation
Serial Number: 16DB4F8F0000000000012
 Revocation Date: Aug 16 21:53:15 2005 GMT
 Serial Number: 261C39240000000000013
 Revocation Date: Aug 16 21:53:15 2005 GMT
 Serial Number: 262B52020000000000014
 Revocation Date: Jul 14 00:33:10 2005 GMT
 Serial Number: 2634C7F20000000000015
 Revocation Date: Jul 14 00:32:45 2005 GMT
 Serial Number: 2635B0000000000000016
 Revocation Date: Jul 14 00:31:51 2005 GMT
 Serial Number: 264850400000000000017
 Revocation Date: Jul 14 00:32:25 2005 GMT
 Serial Number: 2A2763570000000000018

```

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

```

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

**Table 34-1** 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.           |

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

## Default Settings

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

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

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