Configuring Certificate Authorities and Digital Certificates

This chapter includes the following sections:
- About CAs and Digital Certificates, page 6-131
- Configuring CAs and Digital Certificates, page 6-135
- Example Configurations, page 6-145
- Maximum Limits, page 6-167
- Default Settings, page 6-168

About CAs and Digital Certificates

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

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

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

This section provides information about certificate authorities (CAs) and digital certificates, and includes the following topics:
- Purpose of CAs and Digital Certificates, page 6-132
- Trust Model, Trust Points, and Identity CAs, page 6-132
- RSA Key-Pairs and Identity Certificates, page 6-133
- Multiple Trusted CA Support, page 6-133
- PKI Enrollment Support, page 6-134
Purpose of CAs and Digital Certificates

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

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

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

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

Trust Model, Trust Points, and Identity CAs

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

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

The MDS switch can also enroll with a trust point to obtain an identity certificate (for example, for IPsec/IKE). This trust point is called an identity CA.
RSA Key-Pairs and Identity Certificates

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

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

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

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

Multiple Trusted CA Support

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

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

PKI Enrollment Support

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

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

Manual Enrollment Using Cut-and-Paste Method

Cisco MDS NX-OS supports certificate retrieval and enrollment using a manual cut-and-paste method. Cut-and-paste enrollment literally means you must cut and paste the certificate requests and resulting certificates between the switch and the CA, as follows:
1. Create an enrollment certificate request, which is displayed in base64-encoded text form.
2. Cut and paste the encoded certificate request text in an e-mail message or in a web form and send it to the CA.
3. Receive the issued certificate (in base64-encoded text form) from the CA in an e-mail message or in a web browser download.
4. Cut and paste the issued certificate to the switch using the certificate import facility.

Multiple RSA Key-Pair and Identity CA Support

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

The multiple RSA key-pair support feature allows the switch to maintain a distinct key pair for each CA with which it is enrolled. Thus, it can match policy requirements for each CA without conflicting with the requirements specified by the other CAs, such as key length. The switch can generate multiple RSA key-pairs and associate each key-pair with a distinct trust point. Thereafter, when enrolling with a trust point, the associated key-pair is used to construct the certificate request.
Peer Certificate Verification

The PKI support on an MDS switch provides the means to verify peer certificates. The switch verifies certificates presented by peers during security exchanges pertaining to applications, such as IPsec/IKE and SSH. The applications verify the validity of the peer certificates presented to them. The peer certificate verification process involves the following steps:

• Verifies that the peer certificate is issued by one of the locally trusted CAs.
• Verifies that the peer certificate is valid (not expired) with respect to current time.
• Verifies that the peer certificate is not yet revoked by the issuing CA.

For revocation checking use certificate revocation list (CRL). A trust point uses this method to verify that the peer certificate has not been revoked.

CRL Downloading, Caching, and Checking Support

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

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

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 6-136
• Generating an RSA Key-Pair, page 6-136
• Creating a Trust Point CA Association, page 6-138
• Authenticating the CA, page 6-138
• Configuring Certificate Revocation Checking Methods, page 6-139


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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;switch# config terminal&lt;br&gt;switch(config)#</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;switch(config)# hostname SwitchA</td>
<td>Configures the host name (SwitchA) of the switch.</td>
</tr>
<tr>
<td><strong>Step 3</strong>&lt;br&gt;SwitchA(config)# ip domain-name example.com</td>
<td>Configures the IP domain name (example.com) of the switch.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 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.  
Note | Only exportable key-pairs can be exported in PKCS#12 format. |
|         | 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. |
|         | |
Creating a Trust Point CA Association

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# crypto ca trustpoint admin-ca</td>
<td>Declares a trust point CA that the switch should trust and enters trust point configuration submode.</td>
</tr>
<tr>
<td>switch(config-trustpoint)#</td>
<td></td>
</tr>
<tr>
<td>switch(config)# no crypto ca trustpoint admin-ca</td>
<td>Removes the trust point CA.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-trustpoint)# enroll terminal</td>
<td>Specifies manual cut-and-paste certificate enrollment (default).</td>
</tr>
<tr>
<td></td>
<td>Note Manual cut-and-paste certificate enrollment is the only method supported for enrollment.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-trustpoint)# rsakeypair SwitchA</td>
<td>Specifies the label of the RSA key-pair to be associated to this trust point for the purpose of enrollment. It was generated earlier in the “Generating an RSA Key-Pair” section on page 6-136. Only one RSA key-pair can be specified per CA.</td>
</tr>
<tr>
<td>switch(config-trustpoint)# no rsakeypair SwitchA</td>
<td>Disassociates the RSA key-pair from the trust point (default).</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-trustpoint)# end</td>
<td>Exits trust point configuration submode.</td>
</tr>
<tr>
<td>switch#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>switch# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration to ensure the configuration is persistent across reboots.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 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-----  
MIIC4jCCojgAwIBAgIQZPSRl1jK02ejANBgkqhkiG9w0BAQUFADBw  
kDMgMB4GCSqGSGiG2IjQJARYWR1Y1hmRz2UBjxANjy5jb20x7jAzBgNVBAAYTAklO  
MR1wEAYDVQQIIBwIYXRhV2h5d3NlcnRha2EYQgIBAgIBAQBcMB0GA1UdDgQGCSqGSIb3DQEBCwUAA4M  
CAcYwDQYJKoZIhvcNAQEBBQADSwAwSDA0BQAoBgNVHQ4EFgQUJyjyRoMbrCNMNU2sGyysCAwEAAaOBvzCBvDALBgNVHQ8E  
BAMCAcYwDwYDVQQTAQhhBBAwDQYJKoZIhvcNAQEBBQADSwAwSDA0BQAoBgNVHQ4EFgQUJyjyRoMbrCNMNU2sGyysCAwEAAaOBvzCBvDALBgNVHQ8E  
BAMCAcYwDwYDVQQTAQhhBBAwDQYJKoZIhvcNAQEBBQADSwAwSDA0BQAoBgNVHQ4EFgQUJyjyRoMbrCNMNU2sGyysCAwEAAaOBvzCBvDALBgNVHQ8E  
BAMCAcYwDwYDVQQTAQhhBBAwDQYJKoZIhvcNAQEBBQADSwAwSDA0BQAoBgNVHQ4EFgQUJyjyRoMbrCNMNU2sGyysCAwEAAaOBvzCBvDALBgNVHQ8E  
BAMCAcYwDwYDVQQTAQhhBBAwDQYJKoZIhvcNAQEBBQADSwAwSDA0BQAoBgNVHQ4EFgQUJyjyRoMbrCNMNU2sGyysCAwEAAaOBvzCBvDALBgNVHQ8E  
BAMCAcYwDwYDVQQTAQhhBBAwDQYJKoZIhvcNAQEBBQADSwAwSDA0BQAoBgNVHQ4EFgQUJyjyRoMbrCNMNU2sGyysCAwEAAaOBvzCBvDALBgNVHQ8E  
-----END CERTIFICATE-----  
END OF INPUT  
Fingerprint(s): MD5  
Do you accept this certificate? [yes/no]: y |

**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 revocation status checking.

You can use the CRL method for checking revoked sender certificates. You can configure the switch to check the CRL downloaded from the CA (see the “Configuring a CRL” section on page 6-143). Downloading the CRL 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. Using local CRL checking provides the 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# crypto ca trustpoint admin-ca</code></td>
<td>Declares a trust point CA that the switch should trust and enters trust point configuration submode.</td>
</tr>
<tr>
<td><code>switch(config-trustpoint)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-trustpoint)# revocation-check crl</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>switch(config-trustpoint)# revocation-check none</code></td>
<td>Does not check for revoked certificates.</td>
</tr>
<tr>
<td><code>switch(config-trustpoint)# no revocation-check</code></td>
<td>Reverts to default method.</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch# config terminal</code></td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# crypto ca enroll admin-ca</code></td>
<td>Generates a certificate request for an authenticated CA.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td><code>Create the certificate request ..</code></td>
<td></td>
</tr>
<tr>
<td><code>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</code></td>
<td></td>
</tr>
<tr>
<td>The subject name in the certificate will be: <em>Vegas-1.cisco.com</em> 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`</td>
<td></td>
</tr>
<tr>
<td>The certificate request will be displayed...</td>
<td></td>
</tr>
<tr>
<td>-----BEGIN CERTIFICATE REQUEST-----</td>
<td></td>
</tr>
<tr>
<td>MIIBqzCCARQCAwHDrRAmBqGA1UEAxMRVnVNVXMTMS5jaXNjby5jb20wZ8wDQYJ K0Z1hvcNAEQBBQADgY0AMIGJAOGBAL8Y1UAJ2NC7jUlDvaSMqN1gJ2k8:8141K Y0JCG6ManNy4pkkVeMXZSliL4JgTzKwUbdLkTTSysnuuCXGVjbb+wj0hA/Ev/y51T9y P2NJS8cognqShrFZgC7ysN/Fy9wKcghvbVp+j+argZvHtGJ91X7q4WvKSz7Czhv88 VqyH0EvAgMBAAGqTzAVBgkqhkiG9w0BCQcsxVBGkqhkiG9w0BCQcxDiJan7MTIz MDYGCQGs1b3DQBJ DijEpcCcwYQDVR0AQI/iBsswGHRMVnXMTMS5jaXNjby5jb22HBKwW6IwDQYJ K0Z1hvcNAEQBBQADgY0AEEBQwIcBAHmJ2MzIwMTkwMDIwMDkmdWFYb3JpZ2luYW5jZSJs</td>
<td></td>
</tr>
<tr>
<td>-----END CERTIFICATE REQUEST-----</td>
<td></td>
</tr>
</tbody>
</table>
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 by e-mail or through a web browser, follow these steps:

Saving Your Configuration

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

Ensuring Trust Point Configurations Persist Across Reboots

The trust point configuration is a normal Cisco NX-OS configuration that persists across system reboots only if you copy it explicitly to the startup configuration. The certificates, key-pairs, and CRL associated with a trust point are automatically persistent if you have already copied the trust point configuration in the startup configuration. Conversely, if the trust point configuration is not copied to the startup configuration, the certificates, key-pairs, and CRL associated with it are not persistent since they require the corresponding trust point configuration after a reboot. Always copy the running configuration to the startup configuration to ensure that the configured certificates, key-pairs, and CRLs are persistent. Also, save the running configuration after deleting a certificate or key-pair to ensure that the deletions are permanent.
The certificates and CRL associated with a trust point automatically become persistent when imported (that is, without an explicitly copying to the startup configuration) if the specific trust point is already saved in startup configuration.

We also recommend that you create a password-protected backup of the identity certificates and save it to an external server (see the “Exporting and Importing Identity Information in PKCS#12 Format” section on page 6-142).

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

### Configuring CAs and Digital Certificates

Monitoring and Maintaining CA and Certificates Configuration

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

- Exporting and Importing Identity Information in PKCS#12 Format, page 6-142
- Configuring a CRL, page 6-143
- Deleting Certificates from the CA Configuration, page 6-143
- Deleting RSA Key-Pairs from Your Switch, page 6-144
- Displaying Key-Pair and CA Information, page 6-145

#### Exporting and Importing Identity Information in PKCS#12 Format

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

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>switch# copy tftp:adminid.p12 bootflash:adminid.p12</td>
</tr>
<tr>
<td>Step 2</td>
<td>switch# config terminal switch(config)#</td>
</tr>
<tr>
<td>Step 3</td>
<td>switch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>switch# copy tftp:adminca.crl bootflash:adminca.crl</td>
</tr>
<tr>
<td>Step 2</td>
<td>switch# config terminal switch(config)#</td>
</tr>
<tr>
<td>Step 3</td>
<td>switch(config)# crypto ca crl request admin-ca bootflash:adminca.crl</td>
</tr>
</tbody>
</table>

**Deleting Certificates from the CA Configuration**

You can delete the identity certificates and CA certificates that are configured in a trust point. You must first delete the identity certificate, followed by the CA certificates. After deleting the identity certificate, you can disassociate the RSA key-pair from a trust point. The certificate deletion is necessary to remove expired or revoked certificates, certificates whose key-pairs are compromised (or suspected to be compromised) or CAs that are no longer trusted.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>switch# config t switch(config)#</td>
</tr>
<tr>
<td>Step 2</td>
<td>switch(config)# crypto ca trustpoint myCA</td>
</tr>
<tr>
<td>Step 3</td>
<td>switch(config-trustpoint)# delete ca-certificate</td>
</tr>
</tbody>
</table>
## 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switch(config-trustpoint)# delete certificate</code></td>
<td>Deletes the identity certificate.</td>
</tr>
<tr>
<td><code>switch(config-trustpoint)# delete certificate force</code></td>
<td>Forces the deletion of the identity certificate. <strong>Note</strong> If the identity certificate being deleted is the last-most or only identity certificate in the device, you must use the <code>force</code> 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.</td>
</tr>
<tr>
<td><code>switch(config-trustpoint)# end</code></td>
<td>Returns to EXEC mode.</td>
</tr>
<tr>
<td><code>switch# copy running-config startup-config</code></td>
<td>Copies the running configuration to the startup configuration to ensure the configuration is persistent across reboots.</td>
</tr>
</tbody>
</table>

**Note** After you delete RSA key-pairs from a switch, ask the CA administrator to revoke your switch’s certificates at the CA. You must supply the challenge password you created when you originally requested the certificates. See “Generating Certificate Requests” section on page 6-140.
Displaying Key-Pair and CA Information

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch# show crypto key mypubkey rsa</td>
<td>Displays information about the switch’s RSA public keys.</td>
</tr>
<tr>
<td>switch# show crypto ca certificates</td>
<td>Displays information on CA and identity certificates.</td>
</tr>
<tr>
<td>switch# show crypto ca crl</td>
<td>Displays information about CA CRLs.</td>
</tr>
<tr>
<td>switch# show crypto ca trustpoints</td>
<td>Displays information about CA trust points.</td>
</tr>
</tbody>
</table>

Example Configurations

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

This section includes the following topics:

• Configuring Certificates on the MDS Switch, page 6-145
• Downloading a CA Certificate, page 6-148
• Requesting an Identity Certificate, page 6-152
• Revoking a Certificate, page 6-159
• Generating and Publishing the CRL, page 6-161
• Downloading the CRL, page 6-162
• Importing the CRL, page 6-165

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)#
```
### Example Configurations

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

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

| key label: myKey |
| key size: 1024 |
| exportable: yes |

Vegas-1(config)#

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

Vegas-1(config)# crypto ca trustpoint myCA
Vegas-1(config-trustpoint)# rsakeypair myKey
Vegas-1(config-trustpoint)# exit
Vegas-1(config)# do show crypto ca trustpoints

| trustpoint: myCA; key: myKey |
| revokation methods: crl |

Vegas-1(config)#

#### Step 6  Download the CA certificate from the Microsoft Certificate Service web interface (see the “Downloading a CA Certificate” section on page 6-148)

#### 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-----
MIIC4jCCAzogAwIBAgIQGZRPSRI1jK0ZejJABgkqhkiG9w0BAQUFADCB
hDBgMBAGC5ggDIhQhDQJARYYWhbmR0SUBjajXJyj5b3oCAjBgNVYTAf
MR1wDQYJK2VYa2VQIEQfQH4v3YXxyHDx2bAEXjAQBgNVBAcTUCUIhmdmhyb
9yeZTEOMaBjGEliasMiHgG1Ue0jCiAOARH2uWJ1M4Q0DA4DYVQQKED
5h5dGFrYTVSMBAGA1UEaXJvYXJ0cmFmZHV4dGV4cyMBAAEgCAYm9er
AQKfBhFhFbHWFVuG0t1QUNpc2NvLiNvRhELdMaA1UEBhxMCU4x8jAQBgNB
AVhCcm5hI0NBMFwwDQYJKoZIhvcn
AQREFQQDASwEwSAJAM%/7b3+DXJPMN8sIHs1uWccNM/71Wt/8w2s2oS
mX2OemXXlRMrXXO5JByAgT2ASUFuU0wQ1lDM8r0/41j8R0xvXKvysCAwEAa
BvzCBbDLbGnPQH8EB
BMACaywDwYDV0T0AQX/BAUAWxEB2/ADBGmVQQ4EFQGUJyjRoMbrCNMRU20
RQQgswfH0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0
L0wPwXJUXyYUDMEMBnYmBnGw2CD9Y2LqmsIZoTVVVlxxccM11T2m6N
KtFlhF3nJv56h701WjTlwjQ0y3JnJMAVOICEsGAQQBrgcVQQDAGENAMAOGCSG
J79123DQEB
BQUAoGAEHv6QQ+8iE99tTtwuKa5gQ0ONJ3aqNgL0AFCt0zEyyt/WIGPzeaF9E
aMB07B0n66exOBOEFOGIv96mEpj1/w==

-----END CERTIFICATE-----

END OF INPUT


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/OU=Aparna CA |
| issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Yourcompany/O |
| U=netstorage/OU=Aparna CA |
| serial=0560D289AC419944F12258CDA97A |
| notBefore=May 3 22:46:37 2005 GMT |
| notAfter=May 3 22:55:17 2007 GMT |
**Step 8** Generate a request certificate to use to enroll with a trust point.

```bash
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-----
MIIBqzCCARQCAQWHDaeEBaOBgkqbi9g9w0BAQUFADBkXGZ8wDQYJKoZIhvcNAQEB
BQADggY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVAkSMqNIG2ktt8r14lKYOC6CmMnN4y
Q4zkn8V8EXMS1Ly4jZgTesKwdbbLDkTTYtsnuCXGvb+wjz08EHv/yS1T9yP2NjNj0r
b5hrVgVfG7y7mN/PMy/MwqcnzVbVj+rarg2VhcG91X7q4XOrvKczVx8S
VqygH0vLyvMgSAAGAGtyZ2VhKghk19gW0BCQxxCBMG8BmJ2MTi2MDYGCgSGS1b3DJ
DjBBpcmGc2X7VR0RAqK/HBawEyVRhXYMxM5JajXJnbj5zbz2HKBW8H16W6QYJU
VzXhAcemGqAsgvTcA6C7jJIVd5vGx7Y7U7gN/IJCIZGqC6Ur2Yaj6k7bn/1kn
8a233DnqM9xBkXw saddenedVLEGUZEFqBjIgPNTdZaszCUC628QCMetbKykU=-----
```

---BEGIN CERTIFICATE REQUEST-----

```
-----END CERTIFICATE REQUEST-----
```

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

**Step 9** Request an identity certificate from the Microsoft Certificate Service web interface (see the “Requesting an Identity Certificate” section on page 6-152).

**Step 10** Import the identity certificate.

```bash
Vegas-1(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
```

```
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCjGOoAAAAADAnBgMQAwIBAgIGA1UEBxMCTDREMCwwGAYD
VQQIEwpDcmVhdGVyMRMwEQYDVQQIKwZcMjEQMA4GA1UEAwwfZm9vcmV0LmNvbDAg
BgNVBAsTVEFwYXJuYSBDaXNzc3RvcHMwJAYDVQQKEwMMDQgMA0GA1UEChMDS2Fz
LTEuY2lzY28wDQYJKoZIhvcNAQEFBQADgYEAMA9GCIwggB0AgEBABoIBAQQgMQAwIB
AgIKCjGOoAAAAADAnBgMTAwIBAgIGA1UEBxQCTDREMCwwGAYDVQQIKwZcMjEQMA4G
AQIBAgYIKwYBBQUHMRYW0wDQYJKoZIhvcNAQEFBQADgYEAMA9GCIwggB0AgEBABoI
BAQQgMQAwIBAgIKCjGOoAAAAADAnBgMTAwIBAgIGA1UEBxQCTDREMCwwGAYDVQQI
```

---END CERTIFICATE-----

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

---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
  purposes: sslserver sslclient ike

CA certificate 0:
  subject= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Yourcompany/OU=netstorage/CN=Aparna CA
  issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Yourcompany/OU=netstorage/CN=Aparna CA
  serial=0560D289ACB419944F4912258CAD197A
  notBefore=May  3 22:46:37 2005 GMT
  notAfter=May  3 22:55:17 2007 GMT
  purposes: sslserver sslclient ike

Step 12  Save the certificate configuration to the startup configuration.

Vegas-1# **copy running-config startup-config**

**Downloading a CA Certificate**

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

---

**Step 1**  Click the **Retrieve the CA certificate or certificate revocation task** radio button in the Microsoft Certificate Services web interface and click the **Next button**.
Step 2  Select the CA certificate file to download from the displayed list. Click the **Base 64 encoded** radio button, and choose the **Download CA certificate** link.

Step 3  Click the **Open** button in the File Download dialog box.
Step 4  Click the Copy to File button in the Certificate dialog box and click OK.

Step 5  Select the Base-64 encoded X.509 (CER) on the Certificate Export Wizard dialog box and click Next.
Step 6  Enter the destination file name in the File name: text box on the Certificate Export Wizard dialog box and click **Next**.

Step 7  Click the **Finish** button on the Certificate Export Wizard dialog box.
Step 8  Display the CA certificate stored in Base-64 (PEM) format using the Microsoft Windows `type` command.

---

**Requesting an Identity Certificate**

To request an identify certificate from a Microsoft Certificate server using a PKCS#10 certificate signing request (CRS), follow these steps:
Step 1  Click the **Request a certificate** radio button on the Microsoft Certificate Services web interface and click **Next**.

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

Step 3  Click the **Submit a certificate request using a base64 encoded PKCS#10 file or a renewal request using a base64 encoded PKCS#7 file** radio button and click **Next**.
Step 4  Paste the base64 PKCS#10 certificate request in the Saved Request text box and click **Next**.

The certificate request is copied from the MDS switch console (see the “Generating Certificate Requests” section on page 6-140 and “Configuring Certificates on the MDS Switch” section on page 6-145).

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.

Step 7  Click the **Check on a pending certificate** radio button on the Microsoft Certificate Services web interface and click **Next**.
Step 8  Select the certificate request you want to check and click **Next**.

Step 9  Select **Base 64 encoded** and click the **Download CA certificate** link.
Step 10  Click Open on the File Download dialog box.

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

Chapter 6  Configuring Certificate Authorities and Digital Certificates

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.

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.
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.
Example Configurations

Chapter 6 Configuring Certificate Authorities and Digital Certificates

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

Downloading the CRL

To download the CRL from the Microsoft CA website, follow these steps:
Step 1  Click **Request the CA certificate or certificate revocation list** radio button on the Microsoft Certificate Services web interface and click **Next**.

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

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

Chapter 6 Configuring Certificate Authorities and Digital Certificates

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:aparnaCA.crl bootflash:aparnaCA.crl
```

Step 2 Configure the CRL.

```
Vegas-1# config terminal
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)# show 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:
```
Example Configurations

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: 4CFCC2B4200000000004
Revocation Date: Aug 16 21:52:41 2005 GMT

Serial Number: 6C699EC2000000000005
Revocation Date: Aug 16 21:52:52 2005 GMT

Serial Number: 6CCF7DCC000000000006
Revocation Date: Jun 8 00:12:04 2005 GMT

Serial Number: 70CC4FF000000000007
Revocation Date: Aug 16 21:53:15 2005 GMT

Serial Number: 4D9B1116000000000008
Revocation Date: Aug 16 21:53:15 2005 GMT

Serial Number: 52A8023000000000009
Revocation Date: Jun 27 23:47:06 2005 GMT

CRL entry extensions:
X509v3 CRL Reason Code:
CA Compromise

Serial Number: 5349AD4600000000000A
Revocation Date: Jun 27 23:47:22 2005 GMT

CRL entry extensions:
X509v3 CRL Reason Code:
CA Compromise

Serial Number: 53BD177C00000000000B
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: 5DF3DF5200000000000D
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: 5DAB53CD0000000000F
Revocation Date: Aug 16 21:53:15 2005 GMT

Serial Number: 5DB140D300000000010
Revocation Date: Aug 16 21:53:15 2005 GMT

Serial Number: 5ED77C1B00000000011
Revocation Date: Jun 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: 261C392400000000013
Revocation Date: Aug 16 21:53:15 2005 GMT

Serial Number: 262B520200000000014
Revocation Date: Jul 14 00:33:10 2005 GMT

Serial Number: 263C670200000000015
Revocation Date: Jul 14 00:32:45 2005 GMT

Serial Number: 263580000000000016
Revocation Date: Jul 14 00:31:51 2005 GMT

Serial Number: 264850400000000017
Revocation Date: Jul 14 00:12:25 2005 GMT

Serial Number: 2A2763570000000018
Maximum Limits

Note

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

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

**Table 6-1 Maximum Limits for CA and Digital Certificate**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Maximum Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust points declared on a switch</td>
<td>16</td>
</tr>
<tr>
<td>RSA key-pairs generated on a switch</td>
<td>16</td>
</tr>
<tr>
<td>Identity certificates configured on a switch</td>
<td>16</td>
</tr>
<tr>
<td>Certificates in a CA certificate chain</td>
<td>10</td>
</tr>
<tr>
<td>Trust points authenticated to a specific CA</td>
<td>10</td>
</tr>
</tbody>
</table>
Table 6-2 lists the default settings for CAs and digital certificate parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust point</td>
<td>None</td>
</tr>
<tr>
<td>RSA key-pair</td>
<td>None</td>
</tr>
<tr>
<td>RSA key-pair label</td>
<td>Switch FQDN</td>
</tr>
<tr>
<td>RSA key-pair modulus</td>
<td>512</td>
</tr>
<tr>
<td>RSA key-pair exportable</td>
<td>Yes</td>
</tr>
<tr>
<td>Revocation check method of trust point</td>
<td>CRL</td>
</tr>
</tbody>
</table>