This section introduces the basic concepts, methodology, and general troubleshooting guidelines for problems that may occur when configuring and using digital certificates in Cisco MDS 9000 Family of multilayer directors and fabric switches.

Contents

Troubleshooting Digital Certificates

This chapter describes how to troubleshoot digital certificates created and maintained in the Cisco MDS 9000 Family. It includes the following sections:

- Overview
- Initial Troubleshooting Checklist
- Digital Certificate Issues

Overview

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

Digital Certificates

Digital signatures, based on public key cryptography, digitally authenticate devices and individual users. In public key cryptography, each device or user has a key pair containing both a private key and a public key. Digital certificates link the digital signature to the remote device. 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 certificate authority (CA), a third party that is explicitly trusted by the receiver to validate identities and to create digital certificates.

Certificate Authorities

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

RSA Key Pairs and Identity Certificates

You can generate one or more RSA key pairs and associate each RSA key pair with a trusted 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.

Peer Certificate Verification

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.

CRLs and OCSP Support

Two methods are supported for verifying that the peer certificate has not been revoked: certificate revocation list (CRL) and Online Certificate Status Protocol (OCSP). The switch uses one or both of these methods to verify that the peer certificate has not been revoked.

CRLs are maintained by CAs to give information of prematurely revoked certificates, and the CRLs are published in a repository.

Cisco MDS SAN-OS allows the manual configuration of pre-downloaded CRLs for the trusted CAs, 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.

OCSP facilitates online certificate revocation checking. You can specify an OCSP URL for each trusted CA.

Import and Export Support for Certificates and Associated Key Pairs

As part of the CA authentication and enrollment process, the CA certificate (or the entire chain in the case of a subordinate CA) and the 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. The information in a PKCS#12 file consists of the RSA key pair, the identity certificate, and the CA certificate (or chain).

PKI Enrollment Support

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

1. Create a trust point and authenticate the CA to it.

2. Generate an RSA private and public key pair on the switch.

3. Associate the RSA key pair to the trust point.

4. Generate a certificate request in standard format and forward it to the CA.

5. Might require manual intervention at the CA server by the CA administrator to approve the enrollment request when it is received by the CA.

6. Receive the issued certificate back from the CA, signed with the CA's private key.

7. Write the certificate into a nonvolatile storage area on the switch (bootflash).

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 (using a console, Telnet, or SSH connection) 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.

Maximum Limits

Table 24-1 lists the maximum limits for CAs and digital certificate parameters.

Table 24-1 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

Initial Troubleshooting Checklist

Begin troubleshooting digital certificates issues by checking the following issues first:

Checklist	**Check off**
Verify that the fully qualified domain name (FQDN) has been configured on the switch.	
Verify that all the CA certificates in a CA chain for a trusted CA are added to the switch if the CA is not self-signed.	
Verify that you have installed your identity certificates.	
Verify that you have revoked your identity certificates if you delete the associated RSA key pairs.	

Common Troubleshooting Tools in Fabric Manager

Choose **Switches > Security > PKI** to access digital certificates.

Common Troubleshooting Commands in the CLI

The following commands may be useful in troubleshooting digital certificate issues:

- **show crypto ca certificates**
- **show crypto key**
- **show crypto ca crl**
- **show crypto ca trustpoint**

Digital Certificate Issues

This section describes troubleshooting digital certificates and includes the following topics:

- CA Will Not Generate Identity Certificate
- Cannot Export Identity Certificate in PKCS#12 Format
- Certificate Fails at Peer
- PKI Fails After Reboot
- Cannot Import Certificate and RSA Key Pairs from Backup

CA Will Not Generate Identity Certificate

Symptom CA will not generate an identity certificate.

Table 24-2 CA Will Not Generate Identity Certificate

Symptom	Possible Cause	Solution
CA will not generate an identity certificate.	FQDN is not configured.	Configure the host name and the IP domain name. Choose **Switches** in Fabric Manager and set the LogicalName field to the host name. Choose **Switches > Interfaces > Management > DNS** and set the DefaultDomainName field. You can also use the **hostname** and th**e ip domain-name** CLI commands.
	Empty challenge password is specified.	Specify a non-empty challenge password during enrollment. Create exportable RSA keys. Choose **Switches > Security > PKI** in Fabric Manager and click the **Trustpoint Action** tab. Select **certreq** from the Command drop-down menu, fill in the URL field and enter the challenge password in the Password field. Click **Apply Changes**. You can also use the **crypto ca enroll** CLI command and enter a challenge password during enrollment.

Cannot Export Identity Certificate in PKCS#12 Format

Symptom Cannot export identity certificate in PKCS#12 format.

Table 24-3 Cannot Export Identity Certificate in PKCS#12 Format

Symptom	Possible Cause	Solution
Cannot export identity certificate in PKCS#12 format.	RSA keys not exportable.	Create exportable RSA keys. **Choose Switches > Security > PKI** in Fabric Manager and click **Create Row**. Check the **Exportable** check box and create an RSA key pair. Or use the **crypto key generate rsa exportable** CLI command.

Certificate Fails at Peer

Symptom Certificate fails at peer.

Table 24-4 Certificate Fails at Peer

Symptom	Possible Cause	Solution
Certificate fails at peer.	FQDN changed after certificate was issued.	Revoke certificate and re-create. See the "Configuring Certificates on the MDS Switch Using Fabric Manager" section or the "Configuring Certificates on the MDS Switch Using the CLI" section.
	Local and remote clocks are not synchronized.	If the clocks are not synchronized, the certificate may appear to be expired. Validate the clocks on the local and peer device.
	Peer does not recognize CA issuing the certificate.	Create a certificate for the CAs known to the peer device. See the "Configuring Certificates on the MDS Switch Using Fabric Manager" section or the "Configuring Certificates on the MDS Switch Using the CLI" section.

Configuring Certificates on the MDS Switch Using Fabric Manager

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

---

1. Choose **Switches** and set the LogicalName field to configure the switch host name.

2. Choose **Switches > Interfaces > Management > DNS** and set the DefaultDomainName field to configure the DNS domain name for the switch.

3. Create an RSA key pair for the switch by following these steps:

    a. Choose **Switches > Security > PKI** and select the **RSA Key-Pair** tab.

    b. Click **Create Row** and set the name and size field.

    c. Check the **Exportable** check box and click **Create**.

4. Create a trust point and associate the RSA key pairs with it by following these steps:

    a. Choose S**witches > Security > PKI** and select the **Trust Point** tab.

    b. Click **Create Row** and set the TrustPointName field.

    c. Select the RSA key pairs from the KeyPairName drop-down menu.

    d. Select the certificates revocation method from the RevokeCheckMethods drop-down menu.

    e. Click **Create**.

5. Choose **Switches > Copy Configuration** and click **Apply Changes** to copy the running-config to startup-config and save the trust point and key pair.

6. Download the CA certificate from the CA that you want to add as the trustpoint CA.

7. Authenticate the CA that you want to enroll to the trust point by following these steps:

   a. In Device Manager, choose **Admin > Flash Files** and select **Copy** and then select **tftp** from the Protocols radio button to copy the CA certificate to bootflash.

   b. In Fabric Manager, choose **Switches > Security > PKI** and click the **TrustPoint Actions** tab.

   c. Select **cauth** from the Command drop-down menu.

   d. Click**...** in the URL field and select the CA certificate from bootflash.

   e. Click **Apply Changes** to authenticate the CA that you want to enroll to the trust point.

   f. Click the **Trust Point Actions** tab in the Information Pane.

   g. Make a note of the CA certificate fingerprint displayed in the IssuerCert FingerPrint column for the trust point row in question. Compare the CA certificate fingerprint with the fingerprint already communicated by the CA (obtained from the CA web site). If the fingerprints match exactly, accept the CA by selecting the **certconfirm** trust point action. Otherwise, reject the CA by selecting the **certnoconfirm** trust point action.

   h. If you selected **certconfirm** in step g, click the **Trust Point Actions** tab, select **certconfirm** from the Command drop-down menu, and then click **Apply Changes**.

   i. If you selected **certnoconfirm** in Step g, click the **Trust Point Actions** tab, select **certnoconfirm** from the Command drop-down menu, and then click **Apply Changes**.

8. Generate a certificate request for enrolling with that trust point by following these steps:

   a. Click the **Trust Point Actions** tab in the Information pane.

   b. Select **certreq** from the Command drop-down menu. This generates a PKCS#10 certificate signing request (CSR) needed for an identity certificate from the CA corresponding to this trust point entry.

   c. Enter the output file name for storing the generated certificate request. It should be specified in the bootflash:filename format and will be used to store the CSR generated in PEM format.

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

   e. Click **Apply Changes** to save the changes.

9. Request an identity certificate from the CA.

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

---

10. Import the identity certificate by following these steps:

a. In Device Manager, choose **Admin > Flash Files** and select **Copy,** then select **tftp** from the Protocol radio buttons to tftp copy the CA certificate to bootflash.

b. In Fabric Manager, choose **Switches > Security > PKI** and click the **TrustPoint Actions** tab.

c. Select the **certimport** option from the Command drop-down menu to import an identity certificate in this trust point.

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

d. Enter the name of the certificate file that was copied to bootflash in the URL field in the bootflash:filename format.

e. Click **Apply Changes** to save your changes.

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

Configuring Certificates on the MDS Switch Using the CLI

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

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)#
```

2. Configure the DNS domain name for the switch.

```
Vegas-1(config)# ip domain-name cisco.com
Vegas-1(config)#
```

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)#
```

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)#
```

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)#
```

6. Use the **copy running-config startup-config** command to save the trust point and key pair.

7. Download the CA certificate from the CA that you want to add as the trust point CA.

8. 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-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO
MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
-----END CERTIFICATE-----
 END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
Do you accept this certificate? [yes/no]:y
Vegas-1(config)#
Vegas-1(config)# do show crypto ca certificates
Trustpoint: myCA
CA certificate 0:
subject= /emailAddress=amandke@cisco.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/O
U=netstorage/CN=Aparna CA
issuer= /emailAddress=amandke@cisco.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/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
Vegas-1(config)#
```

9. Generate a certificate request for enrolling with that 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:172.22.31.162
 The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----
Vegas-1(config)#
```

10. Request an identity certificate from the CA.

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

11. Import the identity certificate.

```
Vegas-1(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD
VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz
Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w
NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu
Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6
Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4
XENlcnRFbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
Vegas-1(config)#
Vegas-1(config)# do show crypto ca certificates
Trustpoint: myCA
certificate:
subject= /CN=Vegas-1.cisco.com
issuer= /emailAddress=amandke@cisco.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/OU
=netstorage/CN=Aparna CA
serial=0A338EA1000000000074
```

```
notBefore=Nov 12 03:02:40 2005 GMT
notAfter=Nov 12 03:12:40 2006 GMT
MD5 Fingerprint=3D:33:62:3D:B4:D0:87:A0:70:DE:A3:87:B3:4E:24:BF
purposes: sslserver sslclient ike
CA certificate 0:
subject= /emailAddress=amandke@cisco.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/O
U=netstorage/CN=Aparna CA
issuer= /emailAddress=amandke@cisco.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/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
```

PKI Fails After Reboot

Symptom PKI fails after reboot.

Table 24-5 PKI Fails After Reboot

Symptom	Possible Cause	Solution
PKI fails after a reboot.	Certificates not saved to NVRAM.	Save the running-config to startup-config to save the trust point to startup. Then reimport the certificates. See the "Configuring Certificates on the MDS Switch Using Fabric Manager" section or the "Configuring Certificates on the MDS Switch Using the CLI" section.

Cannot Import Certificate and RSA Key Pairs from Backup

Symptom Cannot import certificate and RSA key pairs from backup.

Table 24-6 Cannot Import Certificate and RSA Key Pairs from Backup

Symptom	Possible Cause	Solution
Cannot import certificate and RSA key pairs from backup.	Configured trust point is not empty.	Delete the identity certificate, the CRL, and CA certificates, and then disassociate the RSA key pair from the trust point in that order. See the "Importing Certificate and RSA Key Pairs from Backup Using Fabric Manager" section or the "Importing Certificate and RSA Key Pairs from Backup Using the CLI" section.
	An RSA key pair exists with the same name as the trust point that the import failed for.	Delete the RSA key pair. Choose **Switches > Security > PKI** in Fabric Manager. Right-click the RSA key pair that you want to delete and click **Delete Row**.

	You can also use the no **crypto key zeroize rsa** CLI command.

Importing Certificate and RSA Key Pairs from Backup Using Fabric Manager

To import certificates and RSA key pairs from a PKCS#12 backup file using Fabric Manager, follow these steps:

1. Choose **Switches > Security > PKI** and select the **TrustPointDetails** tab to verify that the trust point is empty.

2. (Optional)Empty the trust point by following these steps:

    a. Choose **Switches > Security > PKI** and click the **TrustPoint** tab.

    b. Delete the RSA key pair from the Key Pair Name field and click **Apply Changes**.

    c. Choose **Switches > Security > PKI** and click the **TrustPoint Actions** tab.

    d. Select **cadelete** from the Command drop-down menu and click **Apply Changes** to delete the CA certificate.

    e. Select **forcecertdelete** from the Command drop-down menu and click **Apply Changes** to delete the identity certificates.

3. In Device Manager, choose **Admin > Flash Files** and select **Copy** to copy the PKCS#12 format file to the switch bootflash.

4. In Fabric Manager, choose **Switches > Security > PKI** and click the **TrustPoint Actions** tab.

5. Select the **pkcs12import** option from the Command drop-down menu to import the key pair, identity certificate, and the CA certificate or certificate chain in PKCS#12 format to the selected trust point.

6. Enter the input in bootflash:filename format, for the PKCS#12 file.

7. Enter the required password. The password is set for decoding the PKCS#12 data. On completion, the imported data is available in bootflash in the specified file.

8. Click **Apply Changes** to save the changes.

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

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

Importing Certificate and RSA Key Pairs from Backup Using the CLI

To import certificates and RSA key pairs from a PKCS#12 backup file using the CLI, follow these steps:

1. Use the **show crypto ca trustpoints** command to verify that the trust point is empty.

2. (Optional) Use the **delete ca-certificate** command in trust point config submode to remove the CA certificate from the trust point.

```
switch(config)# crypto ca trustpoint myCA

switch(config-trustpoint)# delete ca-certificate
```

3. (Optional) Use the **delete certificate force** command in trust point config submode to remove the certificates from the trust point.

```
switch(config)# crypto ca trustpoint myCA

switch(config-trustpoint)# delete certificate force
```

4. (Optional) Use the **no rsakeypair** command in the trust point config submode to remove the RSA key pairs from the trust point.

```
switch(config)# crypto ca trustpoint myCA

switch(config-trustpoint)# no rsakeypair SwitchA
```

5. Use the **copy tftp** command to copy the PKCS#12 format file to the switch.

```
switch# copy tftp:adminid.p12 bootflash:adminid.p12
```

6. Use the **crypto ca import** command to import the certificates and RSA key pairs to the trust point.

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

Back to Main Page: Cisco MDS SAN-OS Troubleshooting Guide