



Managing Certificates and Server Security

This chapter includes the following sections:

- [Managing the Server Certificate, on page 1](#)
- [Generating a Certificate Signing Request, on page 2](#)
- [Creating a Self-Signed Certificate, on page 5](#)
- [Creating a Self-Signed Certificate Using Windows, on page 8](#)
- [Uploading a Server Certificate, on page 8](#)
- [Managing the External Certificate, on page 9](#)
- [SPDM Security - MCTP SPDM, on page 13](#)
- [Key Management Interoperability Protocol, on page 18](#)
- [FIPS 140-2 Compliance in Cisco IMC, on page 35](#)

Managing the Server Certificate

You can generate a certificate signing request (CSR) to obtain a new certificate, and you can upload the new certificate to the Cisco IMC to replace the current server certificate. The server certificate may be signed either by a public Certificate Authority (CA), such as Verisign, or by your own certificate authority. The generated certificate key length is 2048 bits.



Note Before performing any of the following tasks in this chapter, ensure that the Cisco IMC time is set to the current time.

Procedure

- Step 1** Generate the CSR from the Cisco IMC.
- Step 2** Submit the CSR file to a certificate authority that will issue and sign your certificate. If your organization generates its own self-signed certificates, you can use the CSR file to generate a self-signed certificate.
- Step 3** Upload the new certificate to the Cisco IMC.

Note The uploaded certificate must be created from a CSR generated by the Cisco IMC. Do not upload a certificate that was not created by this method.

Generating a Certificate Signing Request



Note Do not use special characters (For example ampersand (&)) in the **Common Name** and **Organization Unit** fields.

Before you begin

- You must log in as a user with admin privileges to configure certificates.
- Ensure that the Cisco IMC time is set to the current time.

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
- Step 2** In the **Admin** menu, click **Security Management**.
- Step 3** In the **Actions** area, click the **Generate New Certificate Signing Request** link.
The **Generate New Certificate Signing Request** dialog box appears.
- Step 4** In the **Generate New Certificate Signing Request** dialog box, update the following properties:

Name	Description
Common Name field	The fully qualified name of the Cisco IMC. By default the CN of the servers appears in CXXX-YYYYYY format, where XXX is the model number and YYYYYY is the serial number of the server. When you upgrade to latest version, CN is retained as is.

Name	Description
Subject Alternate Name (SAN)	<p>You can now provide additional input parameter for Subject Alternate Name. This allows various values to be associated using the subject field of the certificate.</p> <p>The various options of SAN includes:</p> <ul style="list-style-type: none"> • Email • DNS name • IP address • Uniform Resource Identifier (URI) <p>Note This field is optional. You can configure any number of SAN instances of each type, but all together the instances count must not exceed 10.</p>
Organization Name field	The organization requesting the certificate.
Organization Unit field	The organizational unit.
Locality field	The city or town in which the company requesting the certificate is headquartered.
State Name field	The state or province in which the company requesting the certificate is headquartered.
Country Code drop-down list	The country in which the company resides.
Email field	The email contact at the company.
Signature Algorithm	<p>Allows you to select the signature algorithm for generating certificate signing request. This can be one of the following:</p> <ul style="list-style-type: none"> • SHA1 • SHA256 • SHA384 • SHA512 • ECDSA • RSA <p>The default signature algorithm selected for generating certificate signing request is SHA384.</p> <p>Note The signature algorithms ECDSA and RSA are available in Cisco UCS C-series M7 servers only.</p>

Name	Description
Key Length drop-down list	<p>Note</p> <ul style="list-style-type: none"> This option is available in Cisco UCS C-series M7 servers only. <p>This option is available for all the Signature Algorithm except ECDSA.</p> <p>You may select from one of the following:</p> <ul style="list-style-type: none"> • 1024 • 2048 • 4096
Key Curve drop-down list	<p>Note</p> <ul style="list-style-type: none"> This option is available in Cisco UCS C-series M7 servers only. This option is available only for ECDSA Signature Algorithm. <p>You may select from one of the following:</p> <ul style="list-style-type: none"> • P256 • P384 • P512
Challenge Password check box	<p>A Challenge Password is to be embedded in the Certificate Signing Request (CSR) dialog box, which the issuer Certificate Authority (CA) uses to authenticate the certificate.</p> <p>If Challenge Password option is selected, then Challenge Password String will be populated for the user to enter the valid password string.</p> <p>Note The user has an option not to select the Challenge Password in which case the Challenge Password String is not populated. However, the user can proceed with generating the CSR successfully.</p>
Challenge Password String field	<p>This option is displayed only when Challenge Password String is selected. Enter a string.</p>

Name	Description
String Mask drop-down list	This sets a mask for permitted string types in Certificate Signing Request (CSR) dialog box. This option masks out the use of certain string types in certain fields. The string types are as follows: <ul style="list-style-type: none"> • Default: Uses PrintableString, T61String, BMPString. • pkix: Uses PrintableString, BMPString. • utf8only: Uses only UTF8Strings. • nombstr: Uses PrintableString, T61String (no BMPStrings or UTF8Strings).
Self Signed Certificate check box	Generates a Self Signed Certificate. <p>Warning After successful certificate generation, the Cisco IMC Web GUI restarts. Communication with the management controller may be lost momentarily and you will need to re-login.</p> <p>Note If enabled, CSR is generated, signed and uploaded automatically.</p>
Generate CSR button	Click to generate the certificate.
Reset Values button	Reset all values in the dialog box.

Note If Self-signed certificate is enabled, ignore steps 5 and 6.

Step 5 Click **Generate CSR**.
The **Opening csr.txt** dialog box appears.

Step 6 Perform any one of the following steps to manage the CSR file, csr.txt:

- a) Click **Open With** to view csr.txt.
- b) Click **Save File** and then click **OK** to save csr.txt to your local machine.

What to do next

- Submit the CSR file to a certificate authority that will issue and sign your certificate. If your organization generates its own self-signed certificates, you can use the CSR file to generate a self-signed certificate.
- Ensure that the certificate is of type **Server**.

Creating a Self-Signed Certificate

As an alternative to using a public Certificate Authority (CA) to generate and sign a server certificate, you can operate your own CA and sign your own certificates. This section shows commands for creating a CA

and generating a server certificate using the OpenSSL certificate server running on Linux. For detailed information about OpenSSL, see <http://www.openssl.org>.



Note These commands are to be entered on a Linux server with the OpenSSL package, not in the Cisco IMC.

Before you begin

- Obtain and install a certificate server software package on a server within your organization.
- Ensure that the Cisco IMC time is set to the current time.

Procedure

	Command or Action	Purpose
Step 1	openssl genrsa -out CA_keyfilename keysize Example: <pre># openssl genrsa -out ca.key 2048</pre>	This command generates an RSA private key that will be used by the CA. Note To allow the CA to access the key without user input, do not use the <code>-des3</code> option for this command. The specified file name contains an RSA key of the specified key size.
Step 2	openssl req -new -x509 -days numdays -key CA_keyfilename -out CA_certfilename Example: <pre># openssl req -new -x509 -days 365 -key ca.key -out ca.crt</pre>	This command generates a new self-signed certificate for the CA using the specified key. The certificate is valid for the specified period. The command prompts the user for additional certificate information. The certificate server is an active CA.
Step 3	echo "nsCertType = server" > openssl.conf Example: <pre># echo "nsCertType = server" > openssl.conf</pre>	This command adds a line to the OpenSSL configuration file to designate the certificate as a server-only certificate. This designation is a defense against a man-in-the-middle attack, in which an authorized client attempts to impersonate the server. The OpenSSL configuration file <code>openssl.conf</code> contains the statement <code>"nsCertType = server"</code> .
Step 4	openssl x509 -req -days numdays -in CSR_filename -CA CA_certfilename -set_serial 04 -CAkey CA_keyfilename -out server_certfilename -extfile openssl.conf Example: <pre># openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf</pre>	This command directs the CA to use your CSR file to generate a server certificate. Your server certificate is contained in the output file.

	Command or Action	Purpose
Step 5	<p>openssl x509 -noout -text -purpose -in <cert file></p> <p>Example:</p> <pre>openssl x509 -noout -text -purpose -in <cert file></pre>	<p>Verifies if the generated certificate is of type Server.</p> <p>Note If the values of the fields Server SSL and Netscape SSL server are not yes, ensure that openssl.conf is configured to generate certificates of type server.</p>
Step 6	<p>(Optional) If the generated certificate does not have the correct validity dates, ensure the Cisco IMC time is set to the current time, and regenerate the certificate by repeating steps 1 through 5.</p>	<p>Certificate with the correct validity dates is created.</p>

Example

This example shows how to create a CA and to generate a server certificate signed by the new CA. These commands are entered on a Linux server running OpenSSL.

```
# /usr/bin/openssl genrsa -out ca.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
# /usr/bin/openssl req -new -x509 -days 365 -key ca.key -out ca.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:San Jose
Organization Name (eg, company) [My Company Ltd]:Example Incorporated
Organizational Unit Name (eg, section) []:Unit A
Common Name (eg, your name or your server's hostname) []:example.com
Email Address []:admin@example.com
# echo "nsCertType = server" > openssl.conf
# /usr/bin/openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 01
-CAkey ca.key -out server.crt -extfile openssl.conf
Signature ok
subject=/C=US/ST=California/L=San Jose/O=Example Inc./OU=Unit
A/CN=example.com/emailAddress=john@example.com
Getting CA Private Key
#
```

What to do next

Upload the new certificate to the Cisco IMC.

Creating a Self-Signed Certificate Using Windows

Before you begin

- You must log in as a user with admin privileges to configure certificates.
- Ensure that the Cisco IMC time is set to the current time.

Procedure

- Step 1** Open **IIS Manager** and navigate to the level you want to manage.
- Step 2** In the **Features** area, double-click **Server Certificate**.
- Step 3** In the **Action** pane, click **Create Self-Signed Certificate**.
- Step 4** On the **Create Self-Signed Certificate** window, enter name for the certificate in the **Specify a friendly name for the certificate** field.
- Step 5** Click **Ok**.
- Step 6** (Optional) If the generated certificate does not have the correct validity dates, ensure the Cisco IMC time is set to the current time, and regenerate the certificate by repeating steps 1 through 5. Certificate with the correct validity dates is created.
-

Uploading a Server Certificate

You can either browse and select the certificate to be uploaded to the server or copy the entire content of the signed certificate and paste it in the **Paste certificate content** text field and upload it.

Before you begin

- You must log in as a user with admin privileges to upload a certificate.
- The certificate file to be uploaded must reside on a locally accessible file system.
- Ensure that the generated certificate is of type server.
- The following certificate formats are supported:
 - .crt
 - .cer
 - .pem



Note You must first generate a CSR using the Cisco IMC Certificate Management menu, and you must use that CSR to obtain the certificate for uploading. Do not upload a certificate that was not obtained by this method.

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
- Step 2** In the **Admin** menu, click **Certificate Management**.
- Step 3** In the **Actions** area, click **Upload Server Certificate**.
The **Upload Certificate** dialog box appears.
- Step 4** In the **Upload Certificate** dialog box, update the following properties:

Name	Description
Upload Certificate through browser client button	Allows you to upload the certificate.
File	The certificate file you want to upload.
Browse button	Opens a dialog box that allows you to navigate to the appropriate certificate file.
Paste Certificate content radio button	Opens a text box that allows you to copy the entire content of the signed certificate and paste it in the Paste certificate content text field. Note Ensure the certificate is signed before uploading.
Upload button	Click Upload to upload the certificate.

- Step 5** Click **Upload Certificate**.

Managing the External Certificate

Prior to the 4.1.2 release, you can generate a certificate signing request (CSR) and upload a new server certificate to Cisco IMC. Release 4.1.2 onwards, you can also upload a wildcard or an external certificate and an external private key, in addition to a server certificate. Unlike a server certificate, you could upload and use the same external certificate and key pair for *multiple* Cisco IMC servers.

1. Upload the external certificate and external private key to Cisco IMC.
2. Activate the uploaded certificate.

On activation, the new certificate and private key pair replaces the existing certificate and key pair in Cisco IMC.

Uploading an External Certificate

Before you begin

- You must log in as a user with admin privileges.

- The certificate file to be uploaded must reside on a locally accessible file system.
- The following certificate formats are supported:
 - .crt
 - .cer
 - .pem

**Note**

- Cisco IMC supports external private key size of 2048 bits, 4096 bits and 8192 bits in Cisco UCS C-Series servers.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Certificate Management**.

Step 3 In the **Actions** area, click **Upload External Certificate**.

The **Upload External Certificate** dialog box appears.

Step 4 In the **Upload External Certificate** dialog box, select the appropriate options and enter the relevant details:

- **Upload from remote location:** Select this radio button to upload an external certificate from a remote location.

Name	Description
Upload from remote location field	Select from one of the following protocols: <ul style="list-style-type: none"> • TFTP • FTP • SCP • SFTP • HTTP <p>Note If you select FTP, SCP or SFTP, you will be prompted to enter your username and password.</p>
Server IP/ Hostname button	Enter the remote server IP address or hostname.
Path and Filename	Enter the filepath on the remote server from where you want to upload the external certificate along with the filename. <p>Note The maximum file size supported for upload using this option is:</p> <ul style="list-style-type: none"> • Up to 8 KB in Cisco UCS C-Series servers

Name	Description
Username	Enter the user name for your remote server.
Password	Password for your remote server.

- **Upload through browser Client:** Select this radio button to upload an external certificate using a browser client.

Click **Browse** and navigate to the location from where you want to upload the external certificate.

Note The maximum file size supported for upload using this option is up to 5 KB in:

- Cisco UCS C-Series servers

- **Paste External Certificate Content:** Select this radio button to paste the external certificate details directly in the dialog box.

Note The maximum file size supported for upload using this option is:

- Up to 8 KB in Cisco UCS C-Series servers

Step 5 Click **Upload** to upload the external certificate.

What to do next

Upload the external private key and then activate the uploaded external certificate.



Important After you upload the external certificate and the external private key, the **Activate External Certificate** tab is enabled. Select **Activate External Certificate** to activate the uploaded external certificate.

Activating the uploaded certificate replaces the existing certificate and key pair, and disconnects any existing HTTPS and SSH sessions.

Uploading an External Private Key

Before you begin

- You must log in as a user with admin privileges to upload an external private key.
- Ensure that you have uploaded an external certificate.



Note • Cisco IMC supports external private key size of 2048 bits, 4096 bits and 8192 bits in Cisco UCS C-Series servers.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Certificate Management**.

Step 3 In the **Actions** area, click **Upload External Private Key**.

The **Upload External Private Key** dialog box appears.

Step 4 In the **Upload External Private Key** dialog box, select the appropriate options and enter the relevant details:

- **Upload from remote location:** Select this radio button to upload an external certificate from a remote location.

Name	Description
Upload from remote location field	Select from one of the following protocols: <ul style="list-style-type: none"> • SFTP • SCP
Server IP/ Hostname button	Enter the remote server IP address or hostname.
Path and Filename	Enter the filepath on the remote server from where you want to upload the external private key along with the filename. Note The maximum file size supported for upload using this option is: <ul style="list-style-type: none"> • Up to 8 KB in Cisco UCS C-Series servers
Username	Enter the user name for your remote server.
Password	Password for your remote server.

- **Upload through browser Client:** Select this radio button to upload an external private key using a browser client.

Click **Browse** and navigate to the location from where you want to upload the external private key.

- Note** The maximum file size supported for upload using this option is up to 5 KB in:
- Cisco UCS C-Series servers

- **Paste External Private Key Content:** Select this radio button to paste the external private key details directly in the dialog box.

- Note** The maximum file size supported for upload using this option is:
- Up to 8 KB in Cisco UCS C-Series servers

Step 5 Click **Upload** to upload the external private key.

What to do next

After uploading the external certificate and external private key, activate the uploaded external certificate.



Important After you upload the external certificate and the external private key, the **Activate External Certificate** tab is enabled. Select **Activate External Certificate** to activate the uploaded external certificate.

Activating the uploaded certificate replaces the existing certificate and key pair, and disconnects any existing HTTPS and SSH sessions.

Activating the External Certificate

Before you begin

- You must log in as a user with admin privileges to activate an external certificate.
- Ensure that you have uploaded the external certificate and external private key.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Certificate Management**.

After uploading the external certificate and the private key, the **Activate External Certificate** tab is enabled in the **Actions** area.

Step 3 Click **Activate External Certificate**.

Note Activating the external certificate overwrites any existing certificate and key pair, and disconnects any existing HTTPS and SSH sessions.

SPDM Security - MCTP SPDM

SPDM Security

Cisco M6 Servers might contain mutable components that could provide vectors for attack against a device itself or use of a device to attack another device within the system. To defend against these attacks, SPDM (Security Protocol and Data Model) specification defines messages, data objects, and sequences for performing message exchanges between devices over a variety of transport and physical media. It orchestrates message exchanges between management controllers and end-point devices over Management Component Transport Protocol (MCTP).

Message exchanges include authentication of hardware identities accessing the controller. The SPDM enables access to low-level security capabilities and operations by specifying a managed level for device authentication

and certificate management. This feature is supported on Cisco UCS C220 and 240 M6 Servers, in Cisco IMC, Release 4.2(1a).

Endpoint certificates and authorities (Root CA) certificates are listed on all user interfaces on the server. You can also upload the content of one or more external device certificates into Cisco IMC. Using a SPDM policy allows you to change or delete external Root CA certificate or settings as desired. You can also delete or replace the root CA certificate when no longer needed.

A SPDM security policy allows you to specify any one of the three security level settings, as listed below:

- **Full Security:**

This is the highest MCTP security setting. When you select this setting, a fault is generated when any endpoint authentication failure is detected. A fault will also be generated if any of the endpoints do not support endpoint authentication.

- **Partial Security:**

When you select this setting, a fault is generated when any endpoint authentication failure is detected. There will NOT be a fault generated when the endpoint doesn't support endpoint authentication. This is chosen as the default setting.

- **No Security**

When you select this setting, no fault will be generated for any failure (endpoint measurement).

Configuring and Viewing the MCTP SPDM Fault Alert Setting



Note This is available only on some C-Series servers.

You can view and change the fault alert setting by performing the following steps.

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
- Step 2** In the **Admin** menu, click **Security Management**.
- Step 3** In the **Security Management** tab > **MCTP SPDM** tab > **Actions** area, click the **Fault Alert Setting** drop-down.

This can be one of the following:

- **Full** - If you select this option, then a fault is generated when there is any endpoint authentication failure.
If you select this option, then a fault is generated when the endpoints do not support endpoint authentication.
- **Partial** - The default option. If you select this option, then a fault is generated when there is any endpoint authentication failure.
If you select this option, no fault is generated when the endpoints do not support endpoint authentication.

- **Disabled** - If you select this option, no fault is generated for endpoint authentication failure.

What to do next

When a fault is generated in case of device attestation failure, you can view the respective fault details in the **Faults and Logs** tab in the **Chassis** menu under the **Navigation** pane.

Viewing SPDM Authentication Status

You can view the SPDM authentication status and SPDM certificate chain by performing the following step.

Before you begin



Note This is available only on some C-Series servers.

Procedure

	Command or Action	Purpose
Step 1	In the Navigation pane, click the Admin menu.	
Step 2	In the Admin menu, click Security Management .	
Step 3	In the Security Management tab > MCTP SPDM tab > Actions area, you can view the following details:	<ul style="list-style-type: none"> • Certificate Upload Progress - Displays the certificate upload progress. • Certificate Upload Status - Displays the certificate upload status. • SPDM Status - Displays the overall SPDM authentication status.

Adding Authorities Certificate

Before you begin



Note This is available only on some C-Series servers.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Security Management**.

Step 3 In the **Security Management** tab > **Certificates** area, click **Authorities** tab.

Step 4 In the Authorities tab, click the **Add** icon.

The **Add Authorities Certificate** dialog box is displayed.

Step 5 Select any of the following options to add the authorities certificate:

- Select **Paste Authorities Certificate**.

Copy the authorities certificate from the host and paste the key in the text field.

- Select **Upload from local**.

Click **Browse** and navigate to the location of the authorities certificate file that you want to add.

- Select **Upload from remote location**.

Enter the following details to upload the authorities certificate file from the remote location.

Name	Description
Upload Authorities Certificate from drop-down list	<p>The remote server type. This can be one of the following:</p> <ul style="list-style-type: none"> • TFTP • FTP • SCP • SFTP • HTTP <p>Note If you choose FTP, SCP or SFTP, you will be prompted to enter your username and password.</p>
Server IP/Hostname field	The IP address or hostname of the server on which the authorities certificate file is available.
Path and Filename field	The path and filename of the authorities certificate file on the remote server.

Step 6 Click **Upload Authorities Certificate**.

You can view the upload progress and status from the following fields in MCTP SPDM tab.

- Certificate Upload Progress
- Certificate Upload Status

After the upload is complete and successful, the authorities certificate is uploaded and the details are displayed in the **Authorities** tab.

Viewing the List of Certificates and Certificate Details

Before you begin



Note This is available only on some C-Series servers.

Procedure

	Command or Action	Purpose
Step 1	In the Navigation pane, click the Admin menu.	
Step 2	In the Admin menu, click Security Management .	
Step 3	In the Security Management tab > MCTP SPDM tab > Certificates area, click the Endpoints tab.	<p>The list of endpoints are displayed with the following details:</p> <ul style="list-style-type: none"> • Common Name - Displays the endpoint's Root CA certificate common name. • Endpoint ID - Displays the PCIe Slot ID. • Status - Displays the endpoint's final SPDM handshake status.
Step 4	In the Security Management tab > MCTP SPDM tab > Certificates area, click the Authorities tab.	<p>The list of SPDM Root CA certificates that have been uploaded are displayed with the following details:</p> <ul style="list-style-type: none"> • Common Name - Displays the authorities certificate common name. • Issued By - Displays the details of who issued the authorities certificate. • Expires - Displays the validity of the authorities certificate. <p>Note A lock icon is displayed next to the certificates that are shipped from the factory. You cannot delete the certificates with the lock icon.</p>
Step 5	To view the details of a specific certificate, perform the following steps:	<ol style="list-style-type: none"> In the Authorities tab, select the check box on any row in the table. Click the View icon to view the endpoint certificate details.

	Command or Action	Purpose
		The following details of the authorities certificate are displayed in View Certificate dialog box.

Deleting Certificates

Before you begin



Note This is available only on some C-Series servers.

Procedure

	Command or Action	Purpose
Step 1	In the Navigation pane, click the Admin menu.	
Step 2	In the Admin menu, click Security Management .	
Step 3	In the Security Management tab > MCTP SPDM tab > Certificates area, click the Authorities tab.	
Step 4	In the Authorities tab, select the check box on any row in the table.	Note A lock icon is displayed next to the certificates that are shipped from the factory. You cannot delete the certificates with the lock icon.
Step 5	Click the Delete icon to delete the endpoint certificate.	The following message is displayed in a pop-window: The certificate has deleted successfully. CIMC will re-authenticate all devices.
Step 6	Click OK .	

Key Management Interoperability Protocol

Key Management Interoperability Protocol (KMIP) is a communication protocol that defines message formats to handle keys or classified data on a key management server. KMIP is an open standard and is supported by several vendors. Key management involves multiple interoperable implementations, so a KMIP client works effectively with any KMIP server.

Self-Encrypting Drives (SEDs) contain hardware that encrypts incoming data and decrypts outgoing data in realtime. A drive or media encryption key controls this function. However, the drives need to be locked in

order to maintain security. A security key identifier and a security key (key encryption key) help achieve this goal. The key identifier provides a unique ID to the drive.

Different keys have different usage requirements. Currently, the responsibility of managing and tracking local keys lies primarily with the user, which could result in human error. The user needs to remember the different keys and their functions, which could prove to be a challenge. KMIP addresses this area of concern to manage the keys effectively without human involvement.

Viewing Secure Key Management Settings

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
- Step 2** In the **Admin** menu, click **Security Management**.
- Step 3** In the **Security Management** pane, click **Secure Key Management**.
- Step 4** In the **Work** pane, review the following field:

Name	Description
Enable Secure Key Management check box	If checked, allows you to enable the secure key management feature.

- Step 5** In the **Actions** Area, review the following fields:

Name	Description
Download Root CA Certificate link	This allows you to download the root CA certificate to Cisco IMC.
Export Root CA Certificate link	This allows you to export the downloaded root CA certificate to a local file or remote server.
Delete Root CA Certificate link	This allows you to delete the root CA certificate.
Download Client Certificate link	This allows you to download the client certificate to Cisco IMC.
Export Client Certificate link	This allows you to export the downloaded client certificate to a local file or remote server.
Delete Client Certificate link	This allows you to delete the client certificate.
Download Client Private Key link	This allows you to download the client private key to Cisco IMC.
Export Client Private Key link	This allows you to export the downloaded root CA certificate to local file or remote server.
Delete Client Private Key link	This allows you to delete the root CA certificate.
Delete KMIP Login link	This allows you to delete the KMIP login details.

Step 6 In the **KMIP Servers** Area, review the following fields:

Name	Description
ID field	ID for the KMIP server configuration.
IP Address field	IP address of the KMIP server.
Port field	Communication port to the KMIP server.
Timeout field	Time period that Cisco IMC waits for a response from the KMIP server.
Delete button	Deletes the KMIP server configuration.
Test Connection button	Tests whether or not the KMIP connection was successful.

Step 7 In the **KMIP Root CA Certificate** Area, review the following fields:

Name	Description
Server Root CA Certificate field	Indicates the availability of the root CA certificate.
Download Status field	This field displays the status of the root CA certificate download.
Download Progress field	This field displays the progress of the root CA certificate download.
Export Status field	This field displays the status of the root CA certificate export.
Export Progress field	This field displays the progress of the root CA certificate export.

Step 8 In the **KMIP Client Certificate** Area, review the following fields:

Name	Description
Client Certificate field	Indicates the availability of the client certificate.
Download Status field	This field displays the status of the client certificate download.
Download Progress field	This field displays the progress of the client certificate download.
Export Status field	This field displays the status of the client certificate export.
Export Progress field	This field displays the progress of the client certificate export.

Step 9 In the **KMIP Login Details** Area, review the following fields:

Name	Description
Use KMIP Login check box	Allows you to choose whether or not to use KMIP login details.
Login name to KMIP Server field	User name of the KMIP server.
Password to KMIP Server field	Password of the KMIP server.
Change Password check box	Allows you to change the KMIP password.
New Password field	Allows you to enter the new password that you want to assign to the KMIP server. Note This option is only visible when you enable the Change Password check box.
Confirm Password field	Enter the new password again in this field. Note This option is only visible when you enable the Change Password check box.

Step 10

In the **KMIP Client Private Key** Area, review the following fields:

Name	Description
Client Private Key field	Indicates the availability of the client private key.
Download Status field	This field displays the status of the client private key download.
Download Progress field	This field displays the progress of the client private key download.
Export Status field	This field displays the status of the client private key export.
Export Progress field	This field displays the progress of the client private key export.

Creating a Client Private Key and Client Certificate for KMIP Configuration

As an alternative to using a public Certificate Authority (CA) to generate and sign a server certificate, you can operate your own CA and sign your own certificates. This section shows commands for creating a CA and generating a server certificate using the OpenSSL certificate server running on Linux. For detailed information about OpenSSL, see <http://www.openssl.org>.



Note These commands are to be entered on a Linux server with the OpenSSL package, not in the Cisco IMC.

Before you begin

- Obtain and install a certificate server software package on a server within your organization.
- Ensure that the Cisco IMC time is set to the current time.

Procedure

	Command or Action	Purpose
Step 1	<p>openssl genrsa -out <i>Client_Privatekeyfilename</i> <i>keysize</i></p> <p>Example:</p> <pre># openssl genrsa -out client_private.pem 2048</pre>	<p>This command generates a client private key that will be used to generate the client certificate.</p> <p>The specified file name contains an RSA key of the specified key size.</p>
Step 2	<p>openssl req -new -x509 -days <i>numdays</i> -key <i>Client_Privatekeyfilename</i> -out <i>Client_certfilename</i></p> <p>Example:</p> <pre># openssl req -new -x509 -key client_private.pem -out client.pem -days 365</pre>	<p>This command generates a new self-signed client certificate using the client private key obtained from the previous step. The certificate is valid for the specified period. The command prompts the user for additional certificate information.</p> <p>A new self-signed client certificate is created.</p>
Step 3	Obtain the KMIP root CA certificate from the KMIP server.	Refer to the KMIP vendor documentation for details on obtaining the root CA certificate.

What to do next

Upload the new certificate to the Cisco IMC.

Downloading a Client Certificate

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
- Step 2** In the **Admin** menu, click **Security Management**.
- Step 3** In the **Security Management** pane, click **Secure Key Management**.
- Step 4** In the **Actions** area of the **Secure Key Management** tab, click **Download Client Certificate**.
- Step 5** In the **Download Client Certificate** dialog box, complete these fields:

Name	Description
<p>Download From Remote Location radio button</p>	<p>Selecting this option allows you to choose the certificate from a remote location and download it. Enter the following details:</p> <ul style="list-style-type: none"> • TFTP Server • FTP Server • SFTP Server • SCP Server • HTTP Server <p>Note If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message <i>Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?</i>. Click Yes or No depending on the authenticity of the server fingerprint.</p> <p>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</p> <ul style="list-style-type: none"> • Server IP/Hostname field — The IP address or hostname of the server on which the client certificate file should be stored. Depending on the setting in the Download Certificate from drop-down list, the name of the field may vary. • Path and Filename field — The path and filename Cisco IMC should use when downloading the file to the remote server. • Username field — The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. • Password field — The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
<p>Download Through Browser Client radio button</p>	<p>Selecting this option allows you to navigate to the certificate stored on a drive that is local to the computer running the Cisco IMC GUI.</p> <p>When you select this option, Cisco IMC GUI displays a Browse button that lets you navigate to the file you want to import.</p>
<p>Paste Content radio button</p>	<p>Selecting this option allows you to copy the entire content of the signed certificate and paste it in the Paste Certificate Content text field.</p> <p>Note Ensure the certificate is signed before uploading.</p>

Exporting a Client Certificate

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
- Step 2** In the **Admin** menu, click **Security Management**.
- Step 3** In the **Security Management** pane, click **Secure Key Management**.
- Step 4** In the **Actions** area of the **Secure Key Management** tab, click **Export Client Certificate**.
- Step 5** In the **Export Client Certificate** dialog box, complete these fields:

Name	Description
<p>Export to Remote Location</p>	<p>Selecting this option allows you to choose the certificate from a remote location and export it. Enter the following details:</p> <ul style="list-style-type: none"> • TFTP Server • FTP Server • SFTP Server • SCP Server • HTTP Server <p>Note If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message <i>Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?</i>. Click Yes or No depending on the authenticity of the server fingerprint.</p> <p>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</p> <ul style="list-style-type: none"> • Server IP/Hostname field — The IP address or hostname of the server on which the certificate file should be exported. Depending on the setting in the Download Certificate from drop-down list, the name of the field may vary. • Path and Filename field — The path and filename Cisco IMC should use when downloading the certificate from the remote server. • Username field — The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. • Password field — The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Name	Description
Export to Local File	Selecting this option allows you to choose the certificate stored on a drive that is local to the computer and export it.

Deleting a Client Certificate

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
- Step 2** In the **Admin** menu, click **Security Management**.
- Step 3** In the **Security Management** pane, click **Secure Key Management**.
- Step 4** In the **Actions** area of the **Secure Key Management** tab, click **Delete Client Certificate**.
- Step 5** At the prompt, click **OK** to delete the client certificate, or **Cancel** to cancel the action.

Downloading a Root CA Certificate

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
- Step 2** In the **Admin** menu, click **Security Management**.
- Step 3** In the **Security Management** pane, click **Secure Key Management**.
- Step 4** In the **Actions** area of the **Secure Key Management** tab, click **Download Root CA Certificate**.
- Step 5** In the **Download Root CA Certificate** dialog box, complete these fields:

Name	Description
<p>Download From Remote Location radio button</p>	<p>Selecting this option allows you to choose the certificate from a remote location and download it. Enter the following details:</p> <ul style="list-style-type: none"> • TFTP Server • FTP Server • SFTP Server • SCP Server • HTTP Server <p>Note If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message <i>Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?</i>. Click Yes or No depending on the authenticity of the server fingerprint.</p> <p>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</p> <ul style="list-style-type: none"> • Server IP/Hostname field — The IP address or hostname of the server on which the root CA certificate file should be stored. Depending on the setting in the Download Certificate from drop-down list, the name of the field may vary. • Path and Filename field — The path and filename Cisco IMC should use when downloading the file to the remote server. • Username field — The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. • Password field — The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
<p>Download Through Browser Client radio button</p>	<p>Selecting this option allows you to navigate to the certificate stored on a drive that is local to the computer running the Cisco IMC GUI.</p> <p>When you select this option, Cisco IMC GUI displays a Browse button that lets you navigate to the file you want to import.</p>
<p>Paste Content radio button</p>	<p>Selecting this option allows you to copy the entire content of the signed certificate and paste it in the Paste Certificate Content text field.</p> <p>Note Ensure the certificate is signed before uploading.</p>

Exporting a Root CA Certificate

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
- Step 2** In the **Admin** menu, click **Security Management**.
- Step 3** In the **Security Management** pane, click **Secure Key Management**.
- Step 4** In the **Actions** area of the **Secure Key Management** tab, click **Export Root CA Certificate**.
- Step 5** In the **Export Root CA Certificate** dialog box, complete these fields:

Name	Description
<p>Export to Remote Location</p>	<p>Selecting this option allows you to choose the certificate from a remote location and export it. Enter the following details:</p> <ul style="list-style-type: none"> • TFTP Server • FTP Server • SFTP Server • SCP Server • HTTP Server <p>Note If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message <i>Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?</i>. Click Yes or No depending on the authenticity of the server fingerprint.</p> <p>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</p> <ul style="list-style-type: none"> • Server IP/Hostname field — The IP address or hostname of the server on which the certificate file should be exported. Depending on the setting in the Download Certificate from drop-down list, the name of the field may vary. • Path and Filename field — The path and filename Cisco IMC should use when downloading the certificate from the remote server. • Username field — The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. • Password field — The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Name	Description
Export to Local File	Selecting this option allows you to choose the certificate stored on a drive that is local to the computer and export it.

Deleting a Root CA Certificate

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
 - Step 2** In the **Admin** menu, click **Security Management**.
 - Step 3** In the **Security Management** pane, click **Secure Key Management**.
 - Step 4** In the **Actions** area of the **Secure Key Management** tab, click **Delete Root CA Certificate**.
 - Step 5** At the prompt, click **OK** or **Cancel** to delete the root CA certificate, or cancel the action.
-

Downloading a Client Private Key

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
- Step 2** In the **Admin** menu, click **Security Management**.
- Step 3** In the **Security Management** pane, click **Secure Key Management**.
- Step 4** In the **Actions** area of the **Secure Key Management** tab, click **Download Client Private Key**.
- Step 5** In the **Download Client Private Key** dialog box, complete these fields:

Name	Description
<p>Download From Remote Location radio button</p>	<p>Selecting this option allows you to choose the private key from a remote location and download it. Enter the following details:</p> <ul style="list-style-type: none"> • TFTP Server • FTP Server • SFTP Server • SCP Server • HTTP Server <p>Note If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message <i>Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?</i>. Click Yes or No depending on the authenticity of the server fingerprint.</p> <p>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</p> <ul style="list-style-type: none"> • Server IP/Hostname field — The IP address or hostname of the server on which the client private key should be stored. Depending on the setting in the Download Certificate From drop-down list, the name of the field may vary. • Path and Filename field — The path and filename Cisco IMC should use when downloading the file to the remote server. • Username field — The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. • Password field — The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
<p>Download Through Browser Client radio button</p>	<p>Selecting this option allows you to navigate to the private key stored on a drive that is local to the computer running the Cisco IMC GUI.</p> <p>When you select this option, Cisco IMC GUI displays a Browse button that lets you navigate to the file you want to import.</p>
<p>Paste Content radio button</p>	<p>Selecting this option allows you to copy the entire content of the signed private key and paste it in the Paste Private Key Content text field.</p>

What to do next

Exporting a Client Private Key

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
- Step 2** In the **Admin** menu, click **Security Management**.
- Step 3** In the **Security Management** pane, click **Secure Key Management**.
- Step 4** In the **Actions** area of the **Secure Key Management** tab, click **Export Client Private Key**.
- Step 5** In the **Export Client Private Key** dialog box, complete these fields:

Name	Description
<p>Export to Remote Location</p>	<p>Selecting this option allows you to choose the certificate from a remote location and export it. Enter the following details:</p> <ul style="list-style-type: none"> • TFTP Server • FTP Server • SFTP Server • SCP Server • HTTP Server <p>Note If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message <i>Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?</i>. Click Yes or No depending on the authenticity of the server fingerprint.</p> <p>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</p> <ul style="list-style-type: none"> • Server IP/Hostname field — The IP address or hostname of the server on which the certificate file should be exported. Depending on the setting in the Download Certificate from drop-down list, the name of the field may vary. • Path and Filename field — The path and filename Cisco IMC should use when downloading the certificate from the remote server. • Username field — The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. • Password field — The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Name	Description
Export to Local File	Selecting this option allows you to choose the certificate stored on a drive that is local to the computer and export it.

Deleting a Client Private Key

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
- Step 2** In the **Admin** menu, click **Security Management**.
- Step 3** In the **Security Management** pane, click **Secure Key Management**.
- Step 4** In the **Actions** area of the **Secure Key Management** pane, click **Delete Client Private Key**.
- Step 5** At the prompt, click **OK** or **Cancel** to delete the client private key, or cancel the action.

Testing the KMIP Server Connection

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
- Step 2** In the **Admin** menu, click **Security Management**.
- Step 3** In the **Security Management** pane, click **Secure Key Management**.
- Step 4** In the **KMIP Servers** area of the **Secure Key Management** tab, select a row by checking the check box and click **Test Connection**.
- Step 5** If the connection is successful, a success message is displayed.

Restoring the KMIP Server to Default Settings

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
- Step 2** In the **Admin** menu, click **Security Management**.
- Step 3** In the **Security Management** pane, click **Secure Key Management**.
- Step 4** In the **KMIP Servers** area of the **Secure Key Management** tab, select a row by checking the check box and click **Delete**.

- Step 5** At the prompt, click **OK**.
This restores the KMIP server to its default settings.
-

Deleting KMIP Login Details

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
- Step 2** In the **Admin** menu, click **Security Management**.
- Step 3** In the **Security Management** pane, click **Secure Key Management**.
- Step 4** In the **Actions** area of the **Secure Key Management** pane, click **Delete KMIP Login**.
- Step 5** At the prompt, click **OK** to delete the KMIP login details, or **Cancel** to cancel the action.
-

FIPS 140-2 Compliance in Cisco IMC

The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules. Prior to the 3.1(3) release, the Rack Cisco IMC is not FIPS compliant as per NIST guideline. It does not follow FIPS 140-2 approved cryptographic algorithms and modules. With this release, all CIMC services will use the Cisco FIPS Object Module (FOM), which provides the FIPS 140-2 compliant cryptographic module.

The Cisco FIPS Object Module is a software library that provides cryptographic services to a vast array of Cisco's networking and collaboration products. The module provides FIPS 140 validated cryptographic algorithms and KDF functionality for services such as IPSec (IKE), SRTP, SSH, TLS, and SNMP.

Enabling Security Configuration

Before you begin

You must log in with admin privileges to perform this task.

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
- Step 2** In the **Admin** menu, click **Security Management**.
- Step 3** In the **Security Management** pane, click **Security Configuration**.
- Step 4** In the **Federal Information Processing Standard Configuration (FIPS) and Common Criteria (CC) Configuration** pane, check the **Enable FIPS** check-box.

Table 1: Federal Information Processing Standard Configuration (FIPS) and Common Criteria (CC) Configuration

Name	Description
<p>Enable FIPS check box</p>	<p>If checked, allows you to enable the FIPS feature. By default, this option is disabled.</p> <p>When you enable FIPS, the following is an impact on the SNMP configuration:</p> <ul style="list-style-type: none"> • The community string configuration for the SNMPv2 protocols, and the SNMPv3 users configured with noAuthNoPriv or authNoPriv security-level option are disabled. • The traps configured for SNMPv2 or SNMPv3 users with the noAuthNoPriv security-level option are disabled. • The MD5 and DES Authentication type and Privacy type are disabled. <p>Note DES privacy type is not applicable for release 4.1(3b) or later. However, if DES was configured in an earlier release before you upgraded to release 4.1(3b) or later, then you may see DES privacy type, which is disabled if FIPS is enabled.</p> <p>Note Both MD5 and DES Authentication type and Privacy type are not supported in Cisco UCS M6 C-Series servers.</p> <ul style="list-style-type: none"> • It also ensures only FIPS-compliant ciphers in SSH, webserver, and vKVM connections. • Allows the Common Criteria (CC) to be enabled. • Disables TACACS+ Authentication.
<p>Enable CC check box</p>	<p>Note Enabling CC requires FIPS to be enabled.</p> <p>If checked, allows you to enable the CC feature. By default, this option is disabled.</p> <p>Note If Enable TLS v1.2 check under Communication Services is disabled, you cannot enable CC.</p>

Note When you switch the FIPS or CC mode, it restarts the SSH, KVM, SNMP, webserver, XMLAPI, and redfish services. You will be prompted to continue. If you wish to continue, click **OK** else click on **Cancel**.

Enabling Security Configuration (FIPS)

Before you begin

You must log in with admin privileges to perform this task.

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
- Step 2** In the **Admin** menu, click **Security Management**.
- Step 3** In the **Security Management** pane, click **Security Configuration**.
- Step 4** In the **Work** pane, check the **Enable FIPS** check-box.

Note When you switch the FIPS mode, it restarts the SSH, KVM, SNMP, webserver, XMLAPI, and redfish services.

- Step 5** You will be prompted to continue. If you wish to continue, click **OK** else click on **Cancel**.

Note When you enable FIPS, the following is an impact on the SNMP configuration:

- The community string configuration for the SNMPv2 protocols, and the SNMPv3 users configured with **noAuthNoPriv** or **authNoPriv** security-level option are disabled.
 - The traps configured for SNMPv2 or SNMPv3 users with the **noAuthNoPriv** security-level option are disabled.
 - The **MD5** and **DES** Authentication type and Privacy type are disabled.
 - It also ensures only FIPS-compliant ciphers in SSH, webserver, and KVM connections.
-

