Managing Certificates and Server Security

This chapter includes the following sections:

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

You can either generate a self-signed certificate manually using the **generate-csr** command, or automatically when you change the hostname. For information on changing the hostname and auto generation of the self-signed certificate, see the **Configuring Common Properties** section.

To manually generate a certificate signing request, follow these steps:

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

	Command or Action	Purpose
Step 1	Server# **scope certificate**	Enters the certificate command mode.
Step 2	Server /certificate # **generate-csr**	Launches a dialog for the generation of a certificate signing request (CSR).

You will be prompted to enter the following information for the certificate signing request:

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.
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.

After you have entered the requested information, the system will generate and display a certificate signing request in the console output. A CSR file will not be created, but you can copy the CSR information from the console output and paste the information into a text file.

This example generates a certificate signing request:

```
Server# scope certificate
Server /certificate # generate-csr
Common Name (CN): test.example.com
Organization Name (O): Example, Inc.
Organization Unit (OU): Test Department
Locality (L): San Jose
StateName (S): CA
Country Code (CC): US
Email: user@example.com
Continue to generate CSR?[y|N]y


-----BEGIN CERTIFICATE REQUEST-----
MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE REQUEST-----

Copy everything from "-----BEGIN ..."  to "END CERTIFICATE REQUEST-----",
paste to a file, send to your chosen CA for signing,
and finally upload the signed certificate via upload command.
              ---OR---
Continue to self sign CSR and overwrite the current certificate?
All HTTPS and SSH sessions will be disconnected. [y|N]N
```

What to Do Next

Perform one of the following tasks:

- If you do not want to obtain a certificate from a public certificate authority, and if your organization does not operate its own certificate authority, you can allow Cisco IMC to internally generate a self-signed certificate from the CSR and upload it immediately to the server. Type **y** after the final prompt in the example to perform this action.
- If your organization operates its own certificate server for generating self-signed certificates, copy the command output from "-----BEGIN ..." to "END CERTIFICATE REQUEST-----" and paste to a file named csr.txt. Input the CSR file to your certificate server to generate a self-signed certificate.
- If you will obtain a certificate from a public certificate authority, copy the command output from "-----BEGIN ..." to "END CERTIFICATE REQUEST-----" and paste to a file named csr.txt. Submit the CSR file to the certificate authority to obtain a signed certificate.
- Ensure that the certificate is of type **Server**.

If you did not use the first option, in which Cisco IMC internally generates and uploads a self-signed certificate, you must upload the new certificate using the **upload** command in certificate command mode.

Creating an Untrusted CA-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:** `# openssl genrsa -out ca.key 2048`	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 -des3 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:** `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	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:** `# echo "nsCertType = server" > openssl.conf`	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 openssl.conf contains the statement "nsCertType = server".
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**	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
	Example: `# openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf`	
Step 5	**openssl x509 -noout -text -purpose -in <cert file>** **Example:** `openssl x509 -noout -text -purpose -in <cert file>`	Verifies if the generated certificate is of type **Server**. **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.
Step 6	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.	(Optional) Certificate with the correct validity dates is created.

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.

Uploading a Server Certificate

Before You Begin

- You must log in as a user with admin privileges to upload a certificate.
- The certificate to be uploaded must be available as readable text. During the upload procedure, you will copy the certificate text and paste it into the CLI.
- Ensure that the generated certificate is of type **Server**.

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

Note All current HTTPS and SSH sessions are disconnected when the new server certificate is uploaded.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope certificate**	Enters the certificate command mode.
Step 2	Server /certificate # **upload**	Launches a dialog for entering and uploading the new server certificate.

Copy the certificate text, paste it into the console when prompted, and type CTRL+D to upload the certificate.

This example uploads a new certificate to the server:

```
Server# scope certificate
Server /certificate # upload
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE-----
```

```
<CTRL+D>
```

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.

Note The KMIP feature is supported only on the C220 M4, C240 M4 and S3260 M4 servers.

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.

Enabling or Disabling KMIP

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope kmip**	Enters the KMIP command mode.
Step 2	Server/kmip# **set enabled** {**yes** | **no**}	Enables or disables KMIP.
Step 3	Server/kmip*# **commit**	Commits the transaction to the system configuration.
Step 4	Server/kmip # **show detail**	(Optional) Displays the KMIP status.

This example enables KMIP:

```
Server # scope kmip
Server /kmip # set enabled yes
Server /kmip *# commit
Server /kmip # show detail
  Enabled: yes
Server /kmip #
```

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	**openssl genrsa -out** *Client_Privatekeyfilename keysize* **Example:** `# openssl genrsa –out client_private.pem 2048`	This command generates a client private key that will be used to generate the client certificate. The specified file name contains an RSA key of the specified key size.
Step 2	**openssl req -new -x509 -days** *numdays* **-key** *Client_Privatekeyfilename* **-out** *Client_certfilename* **Example:** `# openssl req -new -x509 -key client_private.pem -out client.pem -days 365`	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. A new self-signed client certificate is created.
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 KMIP Client Certificate

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope kmip**	Enters the KMIP command mode.
Step 2	Server/kmip # **set enabled yes**	Enables KMIP.
Step 3	Server/kmip*# **commit**	Commits the transaction to the system configuration.
Step 4	Server/kmip # **scope kmip-client-certificate**	Enters the KMIP client certificate command mode.
Step 5	Server /kmip/kmip-client-certificate # **download-client-certificate** *remote-protocol IP Address KMIP client certificate file*	Specifies the protocol to connect to the remote server. It can be of the following types: • TFTP • FTP • SFTP • SCP • HTTP **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 6	At the confirmation prompt, enter **y**.	This begins the download of the KMIP client certificate.
Step 7	Server /kmip/kmip-client-certificate # **paste-client-certificate**	(Optional) At the prompt, paste the content of the signed certificate and press CTRL+D. **Note** You can either use the remote server method from the previous steps or use the paste option to download the client certificate.

This example downloads the KMIP client certificate:

```
Server # scope kmip
Server /kmip # set enabled yes
Server /kmip *# commit
Server /kmip # scope kmip-client-certificate
Server /kmip/kmip-client-certificate # show detail
    KMIP client certificate Available: 1
    Download client certificate Status: COMPLETED
    Export client certificate Status: NONE
Server /kmip/kmip-client-certificate #  download-client-certificate tftp 10.10.10.10
KmipCertificates/
svbu-xx-blr-dn1-13_ClientCert.pem
  You are going to overwrite the KMIP client certificate.
  Are you sure you want to proceed and overwrite the KMIP client certificate? [y|N]y
KMIP client certificate downloaded successfully

You can  either use the remote server method from the previous steps or use the paste option
 to download the client certificate.

Server /kmip/kmip-client-certificate # paste-client-certificate
Please paste your certificate here, when finished, press CTRL+D.
----BEGIN CERTIFICATE-----
MIIDTzCCAjegAwIBAgIQXuWPdBbyTb5M7/FT8aAjZTANBgkqhkiG9w0BAQUFADA6
MRMwEQYKCZImiZPyLGQBGRYDY29tMRMwEQYKCZImiZPyLGQBGRYDbmV3MQ4wDAYD
VQQDEwVuZXdDQTAeFw0xNTAzMTIxMTM5MTZaFw0yMDAzMTIxMTQ5MTVaMDoxEzAR
BgoJkiaJk/IsZAEZFgNjb20xEzARBgoJkiaJk/IsZAEZFgNuZXcxDjAMBgNVBAMT
BW5ld0NBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuPSAwHtk0IbM
Cd5tYdCa498bfX5Nfdgnq5zE+cGIOqv0dAkucofC/Y0+m7hne9H12aQ9SqTOK1+L
5IT3PVCczhasI7L7jAa+Oe5AOYw7Nsugw5Bd23n42BTVMMp7xsgr1mVfFoHXbBkQ
wiT9DieyImSyGiq5n0/8Iooc0iN5WPMVcHO2ysz76jR8p07xRqgYNCl6cbKAhWfZ
oYIwjhpZv0+SXEs8sEJZKDUhWIfOIpnDL7MoZYgl/kymgs/0hsW4L338jy303c7T
TwnG2/7BOMK0YFkEhqcjlkamGP7MKB2T9e/Cug6VkvFSkkim8M1eHx1gEnQxRtAG
YGp1n55iHQIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAd
BgNVHQ4EFgQUl2F3U7cggzCuvRWliZWg91n51ccwEAYJKwYBBAGCNxUBBAMCAQAw
DQYJKoZIhvcNAQEFBQADggEBAJXoJJDDB3QH0q8VY8G/oC1SkAwyOE1dH0NdxFES
tNqQMTaRB2Sb2L/ZzAtfIaZ0Xab9Ig4MqNIMBbHDCwlzhD5gX42GPYWhA/GjRj3O
Q5KcRaEFomxp+twRrJ25ScVSczKJaRonWqKDVL9TwoSuDar3ObiS9ZC0KuBBf0vu
dzrJEYY/1zz7WVPZVyevhba3VSt4LW75URTqOKBSuKO+fvGyyNHWvMPFEIEnJAKt
7QmhO2fiWhD8CxaPFIByqkvrJ96no6oBxdEcjm9n1MttF/UJcpypSPH+46mRn5Az
SzgCBftYNjBPLcwbZGJkF/GpPwjd0TclMM08UOdqiTxR7Ts=
-----END CERTIFICATE-----
  You are going to overwrite the KMIP Client Certificate.
  Are you sure you want to proceed and overwrite the KMIP Client Certificate? [y|N]
y
Server /kmip/kmip-client-certificate #
```

Exporting a KMIP Client Certificate

Before You Begin

- You must log in as a user with admin privileges to perform this task.
- You should have downloaded KMIP client certificate before you can export it.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope kmip**	Enters the KMIP command mode.

	Command or Action	Purpose
Step 2	Server /kmip # **scope kmip-client-certificate**	Enters the KMIP client certificate command mode.
Step 3	Server /kmip/kmip-client-certificate # **export-client-certificate** *remote-protocol IP Adderss KMIP root CA Certificate file*	Specifies the protocol to connect to the remote server. It can be of the following types: • TFTP • FTP • SFTP • SCP • HTTP **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. Initiates the export of the certificate.
Step 4	Server /kmip/kmip-client-certificate # **show detail**	(Optional) Displays the status of the certificate export.

This example exports the KMIP client certificate:

```
Server # scope kmip
Server /kmip # scope kmip-client-certificate
Server /kmip/kmip-client-certificate #  export-client-certificate ftp 10.10.10.10
/TFTP_DIR/KmipCertificates
/svbu-xx-blr-dn1-13_ClientCert.pem_exported_ftp
Username: username
Password:
KMIP Client Certificate exported successfully
Server /kmip/kmip-client-certificate # show detail
    KMIP Client Certificate Available: 1
    Download KMIP Client Certificate Status: COMPLETED
    Export KMIP Client Certificate Status: COMPLETED
Server /kmip/kmip-client-certificate #
```

Deleting a KMIP Client Certificate

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope kmip**	Enters the KMIP command mode.
Step 2	Server# /kmip **scope kmip-client-certificate**	Enters the KMIP client certificate binding command mode.
Step 3	Server /kmip/kmip-client-certificate # **delete-client-certificate**	Confirmation prompt appears.
Step 4	At the confirmation prompt, enter **y**.	This deletes the KMIP client certificate.

This example deletes the KMIP client certificate:

```
Server # scope kmip
Server /kmip # scope kmip-client-certificate
Server /kmip/kmip-client-certificate # delete-client-certificate
  You are going to delete the KMIP Client Certificate.
  Are you sure you want to proceed and delete the KMIP Client Certificate? [y|N]y
 KMIP Client Certificate deleted successfully.
```

Downloading a KMIP Root CA Certificate

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope kmip**	Enters the KMIP command mode.
Step 2	Server/kmip # **set enabled yes**	Enables KMIP.
Step 3	Server/kmip * # **commit**	Commits the transaction to the system configuration.
Step 4	Server /kmip # **scope kmip-root-ca-certificate**	Enters the KMIP root CA certificate command mode.
Step 5	Server /kmip/kmip-root-ca-certificate # **download-root-ca-certificate**	Specifies the protocol to connect to the remote server. It can be of the following types: • TFTP

	Command or Action	Purpose
	remote-protocol IP Address KMIP CA Certificate file	• FTP • SFTP • SCP • HTTP **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 6	At the confirmation prompt, enter **y**.	This begins the download of the KMIP root CA certificate.
Step 7	Server /kmip/kmip-root-ca-certificate # **paste-root-ca-certificate**	(Optional) At the prompt, paste the content of the root CA certificate and press CTRL+D. **Note** You can either use the remote server method from the previous steps or use the paste option to download the root CA certificate.

This example downloads the KMIP root CA certificate:

```
Server # scope kmip
Server /kmip # set enabled yes
Server /kmip *# commit
Server /kmip # scope kmip-root-ca-certificate
Server /kmip/kmip-root-ca-certificate # show detail
    KMIP Root CA Certificate Available: 1
    Download Root CA Certificate Status: COMPLETED
    Export Root CA Certificate Status: NONE
Server /kmip/kmip-root-ca-certificate # download-root-ca-certificate tftp 10.10.10.10
KmipCertificates/
svbu-xx-blr-dn1-13_ServerCert.pem
  You are going to overwrite the KMIP Root CA Certificate.
  Are you sure you want to proceed and overwrite the KMIP Root CA Certificate? [y|N]y
KMIP Root CA Certificate downloaded successfully

You can  either use the remote server method from the previous steps or use the paste option
 to download the client certificate.

Server /kmip/kmip-root-ca-certificate # paste-root-ca-certificate
Please paste your certificate here, when finished, press CTRL+D.
```

```
----BEGIN CERTIFICATE-----
MIIDTzCCAjegAwIBAgIQXuWPdBbyTb5M7/FT8aAjZTANBgkqhkiG9w0BAQUFADA6
MRMwEQYKCZImiZPyLGQBGRYDY29tMRMwEQYKCZImiZPyLGQBGRYDbmV3MQ4wDAYD
VQQDEwVuZXdDQTAeFw0xNTAzMTIxMTM5MTZaFw0yMDAzMTIxMTQ5MTVaMDoxEzAR
BgoJkiaJk/IsZAEZFgNjb20xEzARBgoJkiaJk/IsZAEZFgNuZXcxDjAMBgNVBAMT
BW51d0NBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuPSAwHtk0IbM
Cd5tYdCa498bfX5Nfdgnq5zE+cGIOqv0dAkucofC/Y0+m7hne9H12aQ9SqTOK1+L
5IT3PVCczhasI7L7jAa+Oe5AOYw7Nsugw5Bd23n42BTVMMp7xsgr1mVfFoHXbBkQ
wiT9DieyImSyGiq5n0/8Iooc0iN5WPMVcHO2ysz76jR8p07xRqgYNCl6cbKAhWfZ
oYIwjhpZv0+SXEs8sEJZKDUhWIfOIpnDL7MoZYgl/kymgs/0hsW4L338jy303c7T
TwnG2/7BOMK0YFkEhqcjlkamGP7MKB2T9e/Cug6VkvFSkkim8M1eHx1gEnQxRtAG
YGp1n55iHQIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAd
BgNVHQ4EFgQUl2F3U7cggzCuvRWliZWg91n5lccwEAYJKwYBBAGCNxUBBAMCAQAw
DQYJKoZIhvcNAQEFBQADggEBAJXoJJDDB3QH0q8VY8G/oC1SkAwyOE1dH0NdxFES
tNqQMTaRB2Sb2L/ZzAtfIaZ0Xab9Ig4MqNIMBbHDCwlzhD5gX42GPYWhA/GjRj3O
Q5KcRaEFomxp+twRrJ25ScVSczKJaRonWqKDVL9TwoSuDar3ObiS9ZC0KuBBf0vu
dzrJEYY/1zz7WVPZVyevhba3VSt4LW75URTqOKBSuKO+fvGyyNHWvMPFEIEnJAKt
7QmhO2fiWhD8CxaPFIByqkvrJ96no6oBxdEcjm9n1MttF/UJcpypSPH+46mRn5Az
SzgCBftYNjBPLcwbZGJkF/GpPwjd0TclMM08UOdqiTxR7Ts=
-----END CERTIFICATE-----
  You are going to overwrite the KMIP Root CA Certificate.
  Are you sure you want to proceed and overwrite the KMIP Root CA Certificate? [y|N]
y
Server /kmip/kmip-root-ca-certificate #
```

Exporting a KMIP Root CA Certificate

Before You Begin

- You must log in as a user with admin privileges to perform this task.
- You should have downloaded KMIP root CA certificate before you can export it.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope kmip**	Enters the KMIP command mode.
Step 2	Server /kmip # **scope kmip-root-ca-certificate**	Enters the KMIP root CA certificate command mode.
Step 3	Server /kmip/kmip-root-ca-certificate # **export-root-ca-certificate** *remote-protocol IP Adderss KMIP root CA Certificate file*	Specifies the protocol to connect to the remote server. It can be of the following types: • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
		Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. Initiates the export of the certificate.
Step 4	Server /kmip/kmip-root-ca-certificate # **show detail**	(Optional) Displays the status of the certificate export.

This example exports the KMIP root CA certificate:

```
Server # scope kmip
Server /kmip # scope kmip-root-ca-certificate
Server /kmip/kmip-root-ca-certificate #  export-root-ca-certificate tftp 10.10.10.10
KmipCertificates/
svbu-xx-blr-dn1-13_ServerCert.pem_exported_tftp
KMIP Root CA Certificate exported successfully
Server /kmip/kmip-root-ca-certificate # show detail
    KMIP Root CA Certificate Available: 1
    Download Root CA Certificate Status: COMPLETED
    Export Root CA Certificate Status: COMPLETED
Server /kmip/kmip-root-ca-certificate #
```

Deleting a KMIP Root CA Certificate

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope kmip**	Enters the KMIP command mode.
Step 2	Server# /kmip **scope kmip-root-ca-certificate**	Enters the KMIP root CA certificate binding command mode.

	Command or Action	Purpose
Step 3	Server /kmip/kmip-root-ca-certificate # **delete-root-ca-certificate**	Confirmation prompt appears.
Step 4	At the confirmation prompt, enter **y**.	This deletes the KMIP root CA certificate.

This example deletes the KMIP root CA certificate:

```
Server # scope kmip
Server /kmip # scope kmip-root-ca-certificate
Server /kmip/kmip-root-ca-certificate # delete-root-ca-certificate
  You are going to delete the KMIP root CA certificate.
  Are you sure you want to proceed and delete the KMIP root CA certificate? [y|N]y
 KMIP root CA certificate deleted successfully.
```

Downloading a KMIP Client Private Key

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope kmip**	Enters the KMIP command mode.
Step 2	Server/kmip# **set enabled yes**	Enables KMIP.
Step 3	Server/kmip*# **commit**	Commits the transaction to the system configuration.
Step 4	Server/kmip # **scope kmip-client-private-key**	Enters the KMIP client private key command mode.
Step 5	Server /kmip/kmip-client-private-key # **download-client-pvt-key** *remote-protocol IP Address KMIP client private key file*	Specifies the protocol to connect to the remote server. It can be of the following types: • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
		Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 6	At the confirmation prompt, enter **y**.	This begins the download of the KMIP client private key.
Step 7	Server /kmip/kmip-client-private-key # **paste-client-pvt-key**	(Optional) At the prompt, paste the content of the private key and press CTRL+D. **Note** You can either use the remote server method from the previous steps or use the paste option to download the client private key.

This example downloads the KMIP client private key:

```
Server # scope kmip
Server /kmip # set enabled yes
Server /kmip *# commit
Server /kmip # scope kmip-client-private-key
Server /kmip/kmip-client-private-key # show detail
    KMIP Client Private Key Available: 1
    Download Client Private Key Status: COMPLETED
    Export Client Private Key Status: NONE
Server /kmip/kmip-client-private-key #  download-client-pvt-key tftp 10.10.10.10
KmipCertificates/
svbu-xx-blr-dn1-13_ClientPvtKey.pem
  You are going to overwrite the KMIP Client Private Key.
  Are you sure you want to proceed and overwrite the KMIP Client Private Key? [y|N]y
KMIP Client Private Key downloaded successfully

You can  either use the remote server method from the previous steps or use the paste option
 to download the client certificate.

Server /kmip/kmip-client-private-key # paste-client-pvt-key
Please paste your client private here, when finished, press CTRL+D.
----BEGIN CERTIFICATE-----
MIIDTzCCAjegAwIBAgIQXuWPdBbyTb5M7/FT8aAjZTANBgkqhkiG9w0BAQUFADA6
MRMwEQYKCZImiZPyLGQBGRYDY29tMRMwEQYKCZImiZPyLGQBGRYDbmV3MQ4wDAYD
VQQDEwVuZXdDQTAeFw0xNTAzMTIxMTM5MTZaFw0yMDAzMTIxMTQ5MTVaMDoxEzAR
BgoJkiaJk/IsZAEZFgNjb20xEzARBgoJkiaJk/IsZAEZFgNuZXcxDjAMBgNVBAMT
BW5ld0NBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuPSAwHtk0IbM
Cd5tYdCa498bfX5Nfdgnq5zE+cGIOqv0dAkucofC/Y0+m7hne9H12aQ9SqTOK1+L
5IT3PVCczhasI7L7jAa+Oe5AOYw7Nsugw5Bd23n42BTVMMp7xsgr1mVfFoHXbBkQ
wiT9DieyImSyGiq5n0/8Iooc0iN5WPMVcHO2ysz76jR8p07xRqgYNCl6cbKAhWfZ
```

```
oYIwjhpZv0+SXEs8sEJZKDUhWIfOIpnDL7MoZYgl/kymgs/0hsW4L338jy303c7T
TwnG2/7BOMK0YFkEhqcjlkamGP7MKB2T9e/Cug6VkvFSkkim8M1eHx1gEnQxRtAG
YGp1n55iHQIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAd
BgNVHQ4EFgQUl2F3U7cggzCuvRWliZWg91n5lccwEAYJKwYBBAGCNxUBBAMCAQAw
DQYJKoZIhvcNAQEFBQADggEBAJXoJJDDB3QH0q8VY8G/oC1SkAwyOE1dH0NdxFES
tNqQMTaRB2Sb2L/ZzAtfIaZ0Xab9Ig4MqNIMBbHDCwlzhD5gX42GPYWhA/GjRj3O
Q5KcRaEFomxp+twRrJ25ScVSczKJaRonWqKDVL9TwoSuDar3ObiS9ZC0KuBBf0vu
dzrJEYY/1zz7WVPZVyevhba3VSt4LW75URTqOKBSuKO+fvGyyNHWvMPFEIEnJAKt
7QmhO2fiWhD8CxaPFIByqkvrJ96no6oBxdEcjm9n1MttF/UJcpypSPH+46mRn5Az
SzgCBftYNjBPLcwbZGJkF/GpPwjd0TclMM08UOdqiTxR7Ts=
-----END CERTIFICATE-----
  You are going to overwrite the KMIP client private key.
  Are you sure you want to proceed and overwrite the KMIP Client Private Key? [y|N]
y
Server /kmip/kmip-client-private-key #
```

Exporting KMIP Client Private Key

Before You Begin

- You must log in as a user with admin privileges to perform this task.
- You should have downloaded KMIP client private key before you can export it.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope kmip**	Enters the KMIP command mode.
Step 2	Server /kmip # **scope kmip-client-private-key**	Enters the KMIP client private key command mode.
Step 3	Server /kmip/kmip-client-private-key # **export-client-pvt-key** *remote-protocol IP Adderss KMIP root CA Certificate file*	Specifies the protocol to connect to the remote server. It can be of the following types: • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
		Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. Initiates the export of the certificate.
Step 4	Server /kmip/kmip-client-private-key # **show detail**	(Optional) Displays the status of the certificate export.

This example exports the KMIP client private key:

```
Server # scope kmip
Server /kmip # scope kmip-client-private-key
Server /kmip/kmip-client-private-key #  export-client-pvt-key tftp 10.10.10.10
KmipCertificates
/svbu-xx-blr-dn1-13_ClientPvtKey.pem_exported_tftp
KMIP Client Private Key exported successfully
Server /kmip/kmip-client-private-key # show detail
    KMIP Client Private Key Available: 1
    Download Client Private Key Status: COMPLETED
    Export Client Private Key Status: COMPLETED
Server /kmip/kmip-client-private-key #
```

Deleting a KMIP Client Private Key

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope kmip**	Enters the KMIP command mode.
Step 2	Server# /kmip **scope kmip-client-private-key**	Enters the KMIP client private key binding command mode.
Step 3	Server /kmip/kmip-client-private-key # **delete-client-pvt-key**	Confirmation prompt appears.

	Command or Action	Purpose
Step 4	At the confirmation prompt, enter **y**.	This deletes the KMIP client private key.

This example deletes the KMIP client private key:

```
Server # scope kmip
Server /kmip # scope kmip-client-private-key
Server /kmip/kmip-client-private-key # delete-client-pvt-key
  You are going to delete the KMIP client private key.
  Are you sure you want to proceed and delete the KMIP client private key? [y|N]y
 KMIP client private key deleted successfully.
```

Configuring KMIP Server Login Credentials

This procedure shows you how to configure the login credentials for the KMIP server and make the KMIP server login credentials mandatory for message authentication.

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope kmip**	Enters the KMIP command mode.
Step 2	Server /kmip # **scope kmip-login**	Enters the KMIP login command mode.
Step 3	Server/kmip/kmip-login # **set login** *username*	Sets the KMIP server user name.
Step 4	Server/kmip/kmip-login * # **set password**	Enter the password at the prompt and enter the same password again at the confirm password prompt. This sets the KMIP server password.
Step 5	Server/kmip/kmip-login * # **set use-kmip-cred** {**yes** | **no**}	Decides whether the KMIP server login credentials should be mandatory for message authentication.
Step 6	Server/kmip/kmip-login * # **commit**	Commits the transaction to the system configuration.
Step 7	Server/kmip/kmip-login # **restore**	(Optional) Restores the KMIP settings to defaults.

This example shows how to configure the KMIP server credentials:

```
Server /kmip # scope kmip-login
Server /kmip/kmip-login # set login username
Server /kmip/kmip-login *# set password
Please enter password:
Please confirm password:
```

```
Server /kmip/kmip-login *# set use-kmip-cred yes
Server /kmip/kmip-login *# commit
Server /kmip/kmip-login # show detail
    Use KMIP Login: yes
    Login name to KMIP server: username
    Password to KMIP server: ******
```

You can restore the KMIP server credentials to default settings by preforming the following step:

```
Server /kmip/kmip-login # restore
Are you sure you want to restore KMIP settings to defaults?
Please enter 'yes' to confirm: yes
Restored factory-default configuration.
Server /kmip/kmip-login # show detail
    Use KMIP Login: no
    Login name to KMIP server:
    Password to KMIP server: ******
Server /kmip/kmip-login #
```

Configuring KMIP Server Properties

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server # **scope kmip**	Enters the KMIP command mode.
Step 2	Server /kmip # **scope kmip-server** *server ID*	Enters the chosen KMIP server command mode.
Step 3	Server /kmip/kmip-server # **set** *kmip-port*	Sets the KMIP port.
Step 4	Server /kmip/kmip-server *# **set** *kmip-server*	Sets the KMIP server ID.
Step 5	Server /kmip/kmip-server # **set** *kmip-timeout*	Sets the KMIP server timeout.
Step 6	Server /kmip/kmip-server # **commit**	Commits the transaction to system configuration.
Step 7	Server /kmip/kmip-server # **show detail**	(Optional) Displays the KMIP server details.

This example tests the KMIP server connection:

```
Server # scope kmip
Server /kmip # scope kmip-server 1
Server /kmip/kmip-server # set kmip-port  5696
Server /kmip/kmip-server * # set kmip-server  kmipserver.com
Server /kmip/kmip-server * # set kmip-timeout  10
Server /kmip/kmip-server * # commit
Server /kmip/kmip-server # show detail
Server number 1:
    Server domain name or IP address: kmipserver.com
    Port: 5696
```

```
    Timeout: 10
Server /kmip/kmip-server #
```