



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 an Untrusted CA-Signed Certificate, on page 4](#)
- [Uploading a Server Certificate, on page 6](#)
- [KMIP, on page 7](#)

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.

Example

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/zCCAwgCAQAwZkxCzAJBgNVBAYTA1VTMQswCQYDVQQIEwJDQTEVMBMGAlUE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAst
ClRlc3QgR3JvdXAuGTAXBgNVBAMTEHRlc3QuZXRhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCCYU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAGMBAAGgJTAjBgkq
hkiG9w0BCQcxPhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG6lCaJoJaVMhzCl90306Mg51zqlzXcz75+VFj2I6rH9asckClD3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtlvLWvfhevskV0j6
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 <i>CA_keyfilename</i> <i>keysize</i> 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 <i>numdays</i> -key <i>CA_keyfilename</i> -out <i>CA_certfilename</i> 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 <i>numdays</i> -in <i>CSR_filename</i> -CA <i>CA_certfilename</i> -set_serial	This command directs the CA to use your CSR file to generate a server certificate.

	Command or Action	Purpose
	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>	Your server certificate is contained in the output file.
Step 5	openssl x509 -noout -text -purpose -in <cert file> Example: <pre>openssl x509 -noout -text -purpose -in <cert file></pre>	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	(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.

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.

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.

Example

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/zCCAwgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGAlUE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAst
```

```

C1R1c3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wqZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCCyU
ZgAMivYCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBKOND1
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAGMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzC1903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtv1WvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE-----
<CTRL+D>

```

KMIP

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.

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 server {1 2}	Enters server command mode of server 1 or 2.
Step 2	Server /server # scope bmc	Enters bmc command mode.
Step 3	Server /server/bmc # scope kmip	Enters the KMIP command mode.
Step 4	Server /server/bmc/kmip # set enabled {yes no}	Enables or disables KMIP.

	Command or Action	Purpose
Step 5	Server /server/bmc/kmip *# commit	Commits the transaction to the system configuration.
Step 6	(Optional) Server /server/bmc/kmip # show detail	Displays the KMIP status.

Example

This example enables KMIP:

```
Server # scope server 1
Server /server # scope bmc
Server /server/bmc # scope kmip
Server /server/bmc/kmip # set enabled yes
Server /server/bmc/kmip *# commit
Server /server/bmc/kmip # show detail
    Enabled: yes
Server /server/bmc/kmip #
```

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 server {1 2}	Enters server command mode of server 1 or 2.
Step 2	Server /server # scope bmc	Enters bmc command mode.
Step 3	Server /server/bmc # scope kmip	Enters the KMIP command mode.
Step 4	Server /server/bmc/kmip # scope kmip-login	Enters the KMIP login command mode.
Step 5	Server /server/bmc/kmip/kmip-login # set login <i>username</i>	Sets the KMIP server user name.
Step 6	Server /server/bmc/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 7	Server /server/bmc/kmip/kmip-login * # set use-kmip-cred {yes no}	Decides whether the KMIP server login credentials should be mandatory for message authentication.

	Command or Action	Purpose
Step 8	Server /server/bmc/kmip/kmip-login * # commit	Commits the transaction to the system configuration.
Step 9	(Optional) Server /server/bmc/kmip/kmip-login # restore	Restores the KMIP settings to defaults.

Example

This example shows how to configure the KMIP server credentials:

```
Server # scope server 1
Server /server # scope bmc
Server /server/bmc # scope kmip
Server /server/bmc/kmip # scope kmip-login
Server /server/bmc/kmip/kmip-login # set login username
Server /server/bmc/kmip/kmip-login *# set password
Please enter password:
Please confirm password:
Server /server/bmc/kmip/kmip-login *# set use-kmip-cred yes
Server /server/bmc/kmip/kmip-login *# commit
Server /server/bmc/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 performing the following step:

```
Server /server/bmc/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 /server/bmc/kmip/kmip-login # show detail
    Use KMIP Login: no
    Login name to KMIP server:
    Password to KMIP server: *****
Server /server/bmc/kmip/kmip-login #
```

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 <i>Client_Privatekeyfilename</i> <i>keysize</i> Example: <pre># openssl genrsa -out client_private.pem 2048</pre>	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 <i>numdays</i> -key <i>Client_Privatekeyfilename</i> -out <i>Client_certfilename</i> Example: <pre># openssl req -new -x509 -key client_private.pem -out client.pem -days 365</pre>	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.

Testing the KMIP Server Connection

Procedure

	Command or Action	Purpose
Step 1	Server # scope server {1 2}	Enters server command mode of server 1 or 2.
Step 2	Server /server # scope bmc	Enters bmc command mode.
Step 3	Server /server/bmc # scope kmip	Enters the KMIP command mode.
Step 4	Server /server/bmc/kmip # scope kmip-server <i>server ID</i>	Enters the chosen KMIP server command mode.
Step 5	Server /server/bmc/kmip/kmip-server # test-connectivity	Verifies the connection of the KMIP server.

Example

This example tests the KMIP server connection:

```
Server # scope server 1
Server /server # scope bmc
```

```

Server /server/bmc # scope kmip
Server /server/bmc/kmip # scope kmip-server 1
Server /server/bmc/kmip/kmip-server # test-connectivity
Able to connect to KMIP server.
Server /server/bmc/kmip/kmip-server #

```

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 server {1 2}	Enters server command mode of server 1 or 2.
Step 2	Server /server # scope bmc	Enters bmc command mode.
Step 3	Server /server/bmc # scope kmip	Enters the KMIP command mode.
Step 4	Server /server/bmc/kmip # scope kmip-server <i>server ID</i>	Enters the chosen KMIP server command mode.
Step 5	Server /server/bmc/kmip/kmip-server # set <i>kmip-port</i>	Sets the KMIP port.
Step 6	Server /server/bmc/kmip/kmip-server *# set <i>kmip-server</i>	Sets the KMIP server ID.
Step 7	Server /server/bmc/kmip/kmip-server # set <i>kmip-timeout</i>	Sets the KMIP server timeout.
Step 8	Server /server/bmc/kmip/kmip-server # commit	Commits the transaction to system configuration.
Step 9	(Optional) Server /server/bmc/kmip/kmip-server # show detail	Displays the KMIP server details.

Example

This example tests the KMIP server connection:

```

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

```

```

Port: 5696
Timeout: 10
Server /server/bmc/kmip/kmip-server #

```

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 server {1 2}	Enters server command mode of server 1 or 2.
Step 2	Server /server # scope bmc	Enters bmc command mode.
Step 3	Server /server/bmc # scope kmip	Enters the KMIP command mode.
Step 4	Server /server/bmc/kmip # set enabled yes	Enables KMIP.
Step 5	Server /server/bmc/kmip *# commit	Commits the transaction to the system configuration.
Step 6	Server /server/bmc/kmip # scope kmip-client-certificate	Enters the KMIP client certificate command mode.
Step 7	Server /server/bmc/kmip/kmip-client-certificate # download-client-certificate <i>remote-protocol IP Address KMIP client certificate file</i>	Specifies the protocol to connect to the remote server. It can be of the following types: <ul style="list-style-type: none"> • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
		<p>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.</p> <p>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.</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>
Step 8	At the confirmation prompt, enter y .	This begins the download of the KMIP client certificate.
Step 9	(Optional) Server /server/bmc/kmip/kmip-client-certificate # paste-client-certificate	<p>At the prompt, paste the content of the signed certificate and press CTRL+D.</p> <p>Note You can either use the remote server method from the previous steps or use the paste option to download the client certificate.</p>

Example

This example downloads the KMIP client certificate:

```

Server # scope server 1
Server /server # scope bmc
Server /server/bmc # scope kmip
Server /server/bmc/kmip # set enabled yes
Server /server/bmc/kmip *# commit
Server /server/bmc/kmip # scope kmip-client-certificate
Server /server/bmc/kmip/kmip-client-certificate # show detail
    KMIP client certificate Available: 1
    Download client certificate Status: COMPLETED
    Export client certificate Status: NONE
Server /server/bmc/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 /server/bmc/kmip/kmip-client-certificate # paste-client-certificate
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIDTzCCAjegAwIBAgIQXuWpDbByTb5M7/FT8aAjZTANBgkqhkiG9w0BAQUFADA6
MRMwEQYKCZImiZPyLQBGRYDY29tMRMwEQYKCZImiZPyLQBGRYDbmV3MQ4wDAYD
VQQDEwVuzXkdQTAEFw0xNTAzMTIxMTM5MTZaFw0yMDAzMTIxMTQ5MTVaMDoxEzAR
BgoJkiaJk/IsZAEZFgNjb20xEzARBgoJkiaJk/IsZAEZFgNuZXcxZjAMBGNVBAMT
BW5ld0NBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuPSAwHtk0IbM
Cd5tYdCa498bfX5Nfdgnq5zE+cGIOqv0dAkucofC/Y0+m7hne9H12aQ9SqtOK1+L
5IT3PVCczhasI7L7jAa+Oe5AOYw7Nsugw5Bd23n42BTVMmp7xsgr1mVfFoHXbBkQ
wiT9DieyImSyGiq5n0/8Iooc0iN5WPMVcHO2ys76jR8p07xRqgYNC16cbKAHwfZ
oYIwJhpZv0+sxES8sEJZKDUhWIfOIpnDL7MoZYgl/kymgs/0hsW4L338jy303c7T
TwnG2/7BOMK0YFkEhqcjlkamGP7MKB2T9e/Cug6VkvFSkkim8M1eHx1gEnQxRtAG
YGp1n55iHQIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAd
BgNVHQ4EFgQU12F3U7cggzCuvRWliZWg91n5lccwEAYJKwYBBAGCNxUBBAMCAQAw
DQYJKoZIhvcNAQEFBQADggEBAJXoJJDDb3QH0q8VY8G/oC1SkAwYOE1dH0NdxFES
tNqQMTARb2Sb2L/ZzAtfIaZ0Xab9Ig4MqNIMBbHDCw1zhD5gX42GPYWhA/GjRj3O
Q5KcRaEFomxp+twRrJ25ScVSczKJaRonWqKDVL9TwoSuDar3ObiS9ZC0KuBBf0vu
dzrJEYY/1zz7WVPZVYevhba3VSt4LW75URTqOKBSuKO+fvGyyNHwvMPFEIEnJAKt
7Qmh02fiWhD8CxaPFIBYqkvrJ96no6oBxdEcjm9n1MttF/UJcpypSPH+46mRn5Az
SzgCBftYNjBPLcwbZGJkF/GpPwjD0Tc1MM08UOdqiTxR7Ts=
-----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 /server/bmc/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 server {1 2}	Enters server command mode of server 1 or 2.
Step 2	Server /server # scope bmc	Enters bmc command mode.
Step 3	Server /server/bmc # scope kmip	Enters the KMIP command mode.
Step 4	Server /server/bmc/kmip # scope kmip-client-certificate	Enters the KMIP client certificate command mode.
Step 5	Server /server/bmc/kmip/kmip-client-certificate # export-client-certificate remote-protocol IP Addresss KMIP root CA Certificate file	Specifies the protocol to connect to the remote server. It can be of the following types: <ul style="list-style-type: none"> TFTP

	Command or Action	Purpose
		<ul style="list-style-type: none"> • FTP • SFTP • SCP • HTTP <p>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.</p> <p>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.</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> <p>Initiates the export of the certificate.</p>
Step 6	(Optional) Server /server/bmc/kmip/kmip-client-certificate # show detail	Displays the status of the certificate export.

Example

This example exports the KMIP client certificate:

```

Server # scope server 1
Server /server # scope bmc
Server /server/bmc # scope kmip
Server /server/bmc/kmip # scope kmip-client-certificate
Server /server/bmc/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 /server/bmc/kmip/kmip-client-certificate # show detail
    KMIP Client Certificate Available: 1
    Download KMIP Client Certificate Status: COMPLETED
    Export KMIP Client Certificate Status: COMPLETED
Server /server/bmc/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 server {1 2}	Enters server command mode of server 1 or 2.
Step 2	Server /server # scope bmc	Enters bmc command mode.
Step 3	Server /server/bmc # scope kmip	Enters the KMIP command mode.
Step 4	Server /server/bmc/kmip # scope kmip-client-certificate	Enters the KMIP client certificate binding command mode.
Step 5	Server /server/bmc/kmip/kmip-client-certificate # delete-client-certificate	Confirmation prompt appears.
Step 6	At the confirmation prompt, enter y .	This deletes the KMIP client certificate.

Example

This example deletes the KMIP client certificate:

```
Server # scope server 1
Server /server # scope bmc
Server /server/bmc # scope kmip
Server /server/bmc/kmip # scope kmip-client-certificate
Server /server/bmc/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 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 server {1 2}	Enters server command mode of server 1 or 2.
Step 2	Server /server # scope bmc	Enters bmc command mode.
Step 3	Server /server/bmc # scope kmip	Enters the KMIP command mode.

	Command or Action	Purpose
Step 4	Server /server/bmc/kmip # set enabled yes	Enables KMIP.
Step 5	Server /server/bmc/kmip *# commit	Commits the transaction to the system configuration.
Step 6	Server /server/bmc/kmip # scope kmip-client-private-key	Enters the KMIP client private key command mode.
Step 7	Server /server/bmc/kmip/kmip-client-private-key # download-client-pvt-key remote-protocol IP <i>Address KMIP client private key file</i>	<p>Specifies the protocol to connect to the remote server. It can be of the following types:</p> <ul style="list-style-type: none"> • TFTP • FTP • SFTP • SCP • HTTP <p>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.</p> <p>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.</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>
Step 8	At the confirmation prompt, enter y .	This begins the download of the KMIP client private key.
Step 9	(Optional) Server /server/bmc/kmip/kmip-client-private-key # paste-client-pvt-key	<p>At the prompt, paste the content of the private key and press CTRL+D.</p> <p>Note You can either use the remote server method from the previous steps or use the paste option to download the client private key.</p>

Example

This example downloads the KMIP client private key:

```
Server # scope server 1
Server /server # scope bmc
Server /server/bmc # scope kmip
Server /server/bmc/kmip # set enabled yes
Server /server/bmc/kmip *# commit
Server /server/bmc/kmip # scope kmip-client-private-key
Server /server/bmc/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 /server/bmc/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 /server/bmc/kmip/kmip-client-private-key # paste-client-pvt-key
Please paste your client private here, when finished, press CTRL+D.
----BEGIN CERTIFICATE-----
MIIDTzCCAjegAwIBAgIQXuWpDbByTb5M7/FT8aAjZTANBgkqhkiG9w0BAQUFADA6
MRMwEQYKCZImiZPyLQGGRYDY29tMRMwEQYKCZImiZPyLQGGRYDbmV3MQ4wDAYD
VQQDEwVuZXZkdQTAeFw0xNTAzMTIxMTM5MTZaFw0yMDAzMTIxMTQ5MTVaMDoxEzAR
BgoJkiaJk/IsZAEZFgNjb20xZzARBgoJkiaJk/IsZAEZFgNuZXcxZjAMBGNVBAMT
BW5ld0NBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuPSAwHtk0IbM
Cd5tYdCa498bfX5Nfdgnq5zE+cGIOqv0dAkucofC/Y0+m7hne9H12aQ9SqtOK1+L
5IT3PVCczhasI7L7jAa+Oe5AOYw7Nsugw5Bd23n42BTVMmp7xsgrlmVfFoHXbBkQ
wiT9DieyImSyGiq5n0/8Iooc0iN5WPMVcHO2ys76jR8p07xRqgYNC16cbKAHwFZ
oYIwhjpZv0+SXEs8sEJZKDUDHwif0IpnDL7MoZYgl/kymgs/0hsW4L338jy303c7T
TwnG2/7BOMK0YfKEhqcjlkamGP7MKB2T9e/Cug6VkvFSkkim8M1eHx1gEnQxRtAG
YGpln55iHQIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAd
BgNVHQ4EFgQU12F3U7cggzCuvRWliZWg91n51ccwEAYJKwYBBAGCNxUBBAMCAQAw
DQYJKoZIhvcNAQEFBQADggEBAJXoJJDDB3QH0q8VY8G/oC1SkAwYOE1dH0NdxFES
tNqQMTaRB2Sb2L/ZzAtfIaZ0Xab9Ig4MqNIMBbHDCw1zhD5gX42GPYWhA/GjRj30
Q5KcRaEFomxp+twRrJ25ScVSczKJaRonWqKDVL9TwoSuDar3Obis9ZC0KuBBf0vu
dzrJEYY/1zz7WVPZVyeVhba3VSt4LW75URTqOKBSuKO+fvGyyNHwvMPFEIEnJAKt
7QmhO2fiWhD8CxaPFIBYqkvrJ96no6oBxdEcjm9n1MtTF/UJcypSPH+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 /server/bmc/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 server {1 2}	Enters server command mode of server 1 or 2.
Step 2	Server /server # scope bmc	Enters bmc command mode.
Step 3	Server /server/bmc # scope kmip	Enters the KMIP command mode.
Step 4	Server /server/bmc/kmip # scope kmip-client-private-key	Enters the KMIP client private key command mode.
Step 5	Server /server/bmc/kmip/kmip-client-private-key # export-client-pvt-key remote-protocol IP <i>Adderss KMIP root CA Certificate file</i>	<p>Specifies the protocol to connect to the remote server. It can be of the following types:</p> <ul style="list-style-type: none"> • TFTP • FTP • SFTP • SCP • HTTP <p>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.</p> <p>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.</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> <p>Initiates the export of the certificate.</p>
Step 6	(Optional) Server /server/bmc/kmip/kmip-client-private-key # show detail	Displays the status of the certificate export.

Example

This example exports the KMIP client private key:

```
Server # scope server 1
Server /server # scope bmc
Server /server/bmc # scope kmip
Server /server/bmc/kmip # scope kmip-client-private-key
Server /server/bmc/kmip/kmip-client-private-key # export-client-pvt-key tftp 10.10.10.10
KmpCertificates
/svbu-xx-blr-dn1-13_ClientPvtKey.pem_exported_tftp
KMIP Client Private Key exported successfully
Server /server/bmc/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 /server/bmc/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 server {1 2}	Enters server command mode of server 1 or 2.
Step 2	Server /server # scope bmc	Enters bmc command mode.
Step 3	Server /server/bmc # scope kmip	Enters the KMIP command mode.
Step 4	Server /server/bmc/kmip # scope kmip-client-private-key	Enters the KMIP client private key binding command mode.
Step 5	Server /server/bmc//kmip/kmip-client-private-key # delete-client-pvt-key	Confirmation prompt appears.
Step 6	At the confirmation prompt, enter y .	This deletes the KMIP client private key.

Example

This example deletes the KMIP client private key:

```
Server # scope server 1
Server /server # scope bmc
Server /server/bmc # scope kmip
Server /server/bmc/kmip # scope kmip-client-private-key
Server /server/bmc/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.
```

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 server {1 2}	Enters server command mode of server 1 or 2.
Step 2	Server /server # scope bmc	Enters bmc command mode.
Step 3	Server /server/bmc # scope kmip	Enters the KMIP command mode.
Step 4	Server /server/bmc/kmip # set enabled yes	Enables KMIP.
Step 5	Server /server/bmc/kmip * # commit	Commits the transaction to the system configuration.
Step 6	Server server/bmc/kmip # scope kmip-root-ca-certificate	Enters the KMIP root CA certificate command mode.
Step 7	Server server/bmc/kmip/kmip-root-ca-certificate # download-root-ca-certificate <i>remote-protocol IP Address KMIP CA Certificate file</i>	Specifies the protocol to connect to the remote server. It can be of the following types: <ul style="list-style-type: none"> • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
		<p>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.</p> <p>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.</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>
Step 8	At the confirmation prompt, enter y .	This begins the download of the KMIP root CA certificate.
Step 9	(Optional) Server server/bmc/kmip/kmip-root-ca-certificate # paste-root-ca-certificate	<p>At the prompt, paste the content of the root CA certificate and press CTRL+D.</p> <p>Note You can either use the remote server method from the previous steps or use the paste option to download the root CA certificate.</p>

Example

This example downloads the KMIP root CA certificate:

```

Server # scope server 1
Server /server # scope bmc
Server /server/bmc # scope kmip
Server /server/bmc/kmip # set enabled yes
Server /server/bmc/kmip *# commit
Server /server/bmc/kmip # scope kmip-root-ca-certificate
Server /server/bmc/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 /server/bmc/kmip/kmip-root-ca-certificate # download-root-ca-certificate tftp
10.10.10.10 KmipCertificates/
svbu-xx-blr-dnl-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 /server/bmc/kmip/kmip-root-ca-certificate # paste-root-ca-certificate
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIDTzCCAjegAwIBAgIQXuWpDbByTb5M7/FT8aAjZTANBgkqhkiG9w0BAQUFADA6
MRMwEQYKCZImiZPyLGBGRYDY29tMRMwEQYKCZImiZPyLGBGRYDhmV3MQ4wDAYD
VQQDEwVuzXddQTAeFw0xNTAzMTIxMTM5MTZaFw0yMDAzMTIxMTQ5MTVaMDoxZAR
BgoJkiaJk/IsZAEZFgNjb20xEzARBgoJkiaJk/IsZAEZFgNuZXcxZjAMBGNVBAMT
BW5ld0NBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEaUPSAwHtk0IbM
Cd5tYdCa498bfX5Nfdgnq5zE+cGIOqv0dAkucofC/Y0+m7hne9H12aQ9SqtOK1+L
5IT3PVCczhasI7L7jAa+Oe5AOYw7Nsugw5Bd23n42BTVMmp7xsgrlmVfFoHXbBkQ
wiT9DieyImSyGiQ5n0/8Iooc0iN5WPMVcHO2ys76jR8p07xRqgYNC16cbKAHwFZ
oYIwJhpZv0+SXEs8sEJZKDUhWifoIpnDL7MoZYgl/kymgs/0hsW4L338jy303c7T
TwnG2/7BOMK0YFkEhqcjlkamGP7MKB2T9e/Cug6VkvFSkkim8M1eHxlgEnQxRtAG
YGp1n55iHQIDAQABo1EwTzALBGNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAd
BgNVHQ4EFgQU12F3U7cggzCuvRWLiZWg91n5lccwEAYJKwYBBAGCNxUBBAMCAQAw
DQYJKoZIhvcNAQEFBQADggEBAJXoJJDDb3QH0q8VY8G/oC1SkAwYOE1dH0NdxFES
tNqQMTaRB2Sb2L/ZzAtfIaZ0Xab9Ig4MqNIMBbHDCwLzhD5gX42GPYWhA/GjRj30
Q5KcRaEfomxp+twRrJ25ScVSczKJaRonWqKDVl9TwoSuDar3Obis9ZC0KuBBf0vu
dzrJEYY/1zz7WVPZVYevhba3Vst4LW75URTqOKBSuKO+fvGyyNHwvMPFEIEnJAKt
7Qmh02fiWhD8CxaPFIBYqkvrJ96no6oBxdEcjm9n1MttF/UJcypSPH+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 /server/bmc/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 server {1 2}	Enters server command mode of server 1 or 2.
Step 2	Server /server # scope bmc	Enters bmc command mode.
Step 3	Server /server/bmc # scope kmip	Enters the KMIP command mode.
Step 4	Server /server/bmc/kmip # scope kmip-root-ca-certificate	Enters the KMIP root CA certificate command mode.
Step 5	Server /server/bmc/kmip/kmip-root-ca-certificate # export-root-ca-certificate remote-protocol IP <i>Adderss KMIP root CA Certificate file</i>	Specifies the protocol to connect to the remote server. It can be of the following types: <ul style="list-style-type: none"> • TFTP

	Command or Action	Purpose
		<ul style="list-style-type: none"> • FTP • SFTP • SCP • HTTP <p>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.</p> <p>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.</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> <p>Initiates the export of the certificate.</p>
Step 6	(Optional) Server /server/bmc/kmip/kmip-root-ca-certificate # show detail	Displays the status of the certificate export.

Example

This example exports the KMIP root CA certificate:

```

Server # scope server 1
Server /server # scope bmc
Server /server/bmc # scope kmip
Server /server/bmc/kmip # scope kmip-root-ca-certificate
Server /server/bmc/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 /server/bmc/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 /server/bmc/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 server {1 2}	Enters server command mode of server 1 or 2.
Step 2	Server /server # scope bmc	Enters bmc command mode.
Step 3	Server /server/bmc # scope kmip	Enters the KMIP command mode.
Step 4	Server /server/bmc/kmip # scope kmip-root-ca-certificate	Enters the KMIP root CA certificate binding command mode.
Step 5	Server /server/bmc/kmip/kmip-root-ca-certificate # delete-root-ca-certificate	Confirmation prompt appears.
Step 6	At the confirmation prompt, enter y .	This deletes the KMIP root CA certificate.

Example

This example deletes the KMIP root CA certificate:

```
Server # scope server 1
Server /server # scope bmc
Server /server/bmc # 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.
```

