Managing Certificates and Server Security

This chapter includes the following sections:

Managing the Server Certificate

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 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.

SUMMARY STEPS

1. Generate the CSR from Cisco IMC.
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.
3. Upload the new certificate to Cisco IMC.

DETAILED STEPS

Step 1 Generate the CSR from 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 Cisco IMC.

Note The uploaded certificate must be created from a CSR generated by 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 time is set to the current time.

SUMMARY STEPS

1. Server# **scope certificate**
2. Server /certificate # **generate-csr**

DETAILED STEPS

	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 . 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.

Name	Description
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/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 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 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 .

Before you begin

- Obtain and install a certificate server software package on a server within your organization.
- Ensure that the 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:**	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.

	Command or Action	Purpose
	`# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	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**
	Example:
	`# openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04`
	`-CAkey ca.key -out myserver05.crt -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.

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	(Optional) If the generated certificate does not have the correct validity dates, ensure the 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 .

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**.
- The following certificate formats are supported:
    - .crt
    - .cer
    - .pem

Note You must first generate a CSR using the 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.

SUMMARY STEPS

1. Server# **scope certificate**
2. Server /certificate # **upload**

DETAILED STEPS

	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/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzCl90306Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE-----
<CTRL+D>
```

Managing the External Certificate

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

Step 1 Server# **scope certificate**

Enters Cisco IMC certificate command mode.

Step 2 Server /certificate # **upload-remote-external-certificate** *remote-protocol server_address path certificate_filename*

Specify the protocol to connect to the remote server. It can be of the following types:

- TFTP
- FTP
- SFTP
- SCP
- HTTP

Note If you enter the protocol as FTP, SCP or SFTP, you will be prompted to enter your username and password.

Along with the remote protocol, enter the filepath from where you want to upload the external certificate. After validating your remote server username and password, uploads the external certificate from the remote server.

Step 3 (Optional) Server /certificate #**upload-paste-external-certificate**

This is an additional option to upload the external certificate.

At the prompt, paste the content of the certificate and press `CTRL+D`.

Example

- This example uploads an external certificate from a remote server:

```
Server # scope certificate
Server /certificate # upload-remote-external-certificate scp 10.10.10.10
/home/user-xyz/ext-certif.cert
Server (RSA) key fingerprint is dd:b5:2b:07:ad:c0:30:b2:d5:6a:6a:78:80:85:93:b0
Do you wish to continue? [y/N]y
Username: user-xyz
Password:
External Certificate uploaded successfully
Server /certificate #
```

- This example uploads an external certificate using paste option:

```
Server # scope certificate
Server /certificate # upload-paste-external-certificate
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIID8zCCAtugAwIBAgIBBDANBgkqhkiG9w0BAQwFADCBsDELMAkGA1UEBhMCSU4x
EjAQBgNVBAgMCUthcm5hdGFrYTESMBAGA1UEBwwJQmFuZ2Fsb3JlMSQwIgYDVQQK
DBtDaXNjbyBTeXN0ZW1zIEluZGlhIFB2dCBMdGQxGDAWBgNVBAsMD1VDUy1SYWNr
LVNlcnZlcjEWMBQGA1UEAwwNQ2lzY28gU3lzdGVtczEhMB8GCSqGSIb3DQEJARYS
c3JpdmF0c3NAY2lzY28uY29tMB4XDTIwMDExMzA4MTM1NVoXDTIxMDExMjA4MTM1
NVowgbExCzAJBgNVBAYTAklOMRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcT
CUJlbmdhbHVydTEkMCIGA1UEChMbQ2lzY28gU3lzdGVtcyBJbmRpYSBQdnQgTHRk
MRgwFgYDVQQLEw9VQ1MtUmFjay1TZXJ2ZXIxFjAUBgNVBAMTDUNpc2NvIFN5YXRl
bXMxIjAgBgkqhkiG9w0BCQEWE3NyaXZhdHNzQGNpc2NvLmNvbm0wggEiMA0GCSqG
```

```
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC6fcG9QISg6t1fi6U3+czmek2LvfhAxSGd
r2g7uMssgdTrBh59TEgZl5azal5zWaZm/1iO69D6/iabyoli8+MiQAtANnKxqWM3
STeih+3U2jOf39lIlZrAMpd4Ag/OtK5OcUtwUHM52ixm/UU61geVPZ5mJpPkzq3T
JNcv6TR90K8v0nEILm1lgoA96y64I9YN3ufSE4gm9VOS/sFughmAyYErsgvgoJpn
SQZUYxwdueBm4XV48QY7Mc7neUVYCNo7TcfBX7DC/N0BHv3hlKhGCCQ+5if63uOh
ja8ahdBoIPJqI0h70a92yBK5lv4dxSHexccw2D40kar4CzfVSqx9AgMBAAGjFTAT
MBEGCWCGSAGG+EIBAQQEAwIGQDANBgkqhkiG9w0BAQwFAAOCAQEAXdVTJevqNyI9
DEVibfjGXiKnJ2gEuYr8MdhpDeff/WrsLk7lxhOomVrDZ3iyCX99tNoCIvtOMgNs
jOu9OEjNtBulOlgwdQ9ugwp/JToohbD+2JHRK/MgrFpZmewH1oKKDNpOdayR6u9m
SNfvMNBgvxg+cMcbkif0pJU3XHlniPF6UVgj/LJDyBSGrULpnyDwTOq2UEF6g9Dc
6gOgRGYNHn7MRzigPJtyjbJsbxgPQ9C46I3Me9N2sJNaSLSVQhOxW7KonPI6USRs
e2iEAYaaCvThGE4HTwOMF9dJ24inU+SKTci1AFq2+V4I3P9v+aH5ao1H9T/p/AUP
ho6MuZ+wWg==
-----END CERTIFICATE-----
External Certificate pasted successfully.
Server /certificate #
```

What to do next

You must upload an external private key and then activate the external certificate.

Uploading an External Private Key

Before you begin

- You must log in as a user with admin privileges to upload an external private key.

Note

- Cisco IMC supports external private key size of 2048 bits, 4096 bits and 8192 bits in Cisco UCS S-Series M5 servers.

Step 1 Server# **scope certificate**

Enters Cisco IMC certificate command mode.

Step 2 Server /certificate # **upload-remote-external-private-key** *remote-protocol server_address path key_filename*

Specify the protocol to connect to the remote server. It can be one of the following:

- SFTP
- SCP

Along with the remote protocol, enter the filepath from where you want to upload the private key. After validating your remote server username and password, uploads the private key from the remote server.

Step 3 (Optional) Server /certificate #**upload-paste-external-private-key**

This is an additional option to upload the private key.

At the prompt, paste the content of the private key and press `CTRL+D`.

Note The maximum file size supported for upload:

- Up to 8 KB in Cisco UCS S-Series M5 servers

Example

- This example uploads an external private key from a remote server:

```
Server # scope certificate
Server /certificate # upload-remote-external-private-key scp 10.10.10.10
/home/user-xyz/ext-pvt-key.pem
Server (RSA) key fingerprint is dd:b5:2b:07:ad:c0:30:b2:d5:6a:6a:78:80:85:93:b0
Do you wish to continue? [y/N]y
Username: user-xyz
Password:
External Private Key uploaded successfully
Server /certificate #
```

- This example uploads an external private key using paste option:

```
Server # scope certificate
Server /certificate # upload-paste-external-private-key
Please paste your private key here, when finished, press CTRL+D.
-----BEGIN RSA PRIVATE KEY-----
MIIEoQIBAAKCAQEAun3BvUCEoOrdX4ulN/nM5npNi734QMUhna9oO7jLLIHU6wYe
fUxIGZeWs2pec1mmZv9YjuvQ+v4mm8qJYvPjIkALQDZysaljN0k3ooft1Nozn9/Z
SJWawDKXeAIPzrSuTnFLcFBzOdosZv1FOtYHlT2eZiaT5M6t0yTXL+k0fdCvL9Jx
CC5tZYKAPesuuCPWDd7n0hOIJvVTkv7BboIZgMmBK7IL4KCaZ0kGVGMcHbngZuF1
ePEGOzHO53lFWAjaO03HwV+wwvzdAR794ZSoRggkPuYn+t7joY2vGoXQaCDyaiNI
e9GvdsgSuZb+HcUh3sXHMNg+NJGq+As31UqsfQIDAQABAoH/MSv3aW8ZiVRkCk1H
wvqajCqzR6VPT8SqmGknkpem+pVBDrcOUvtKB3Vwxt3FCaUZuw6YyxZig8t/YpSE
pRKpUN6SGNxCYZXIE0u635/3lafy9LSRFhJcO1EbnwjsIhSB4Sz+Nx7/QsHD82PU
XS8R0MfufACv/iSAsKuGEZvru0BWexD1ycojGTDRhGqWZGzsN6ncsbhQ0kItC0Pv
Ycx+9NeKfGwO+P9NwyWwaKW9M4nOyx3/MviMx9QRbNjgxjrdTj+A0aBUEzgdeZOf
WCJ/LlSbHmJ46HYZOILL4KDBbow/c7a1c2JcFWn01m33qNCRWdkb5H+1UZA+el7g
XnxDAoGBALzBdW26GGIZjj42Ayr9PAXFsO8n0MonqVHRlRTvxeuLOvHYdD9HzgkH
CFXA0IGmNk/1RuwEArx6U6ezSP6z7za9B63MskE7t3Vs28/OJg14KptRftGKUIbZ
NRf1o3J7VUf9mYk9u3pc/PJ8oVweFoml/SwRTDvZyUn5WRLq7zJ3AoGBAPztx24M
qj0Gcbqa7U5pUM+9bD9eGPxrGranFlDp79eobG+9kva286clp0Yr5XrNsQpx42Q6
RJLBVEwrB03D7X9UIOaAgyiaDbDMbIeAcRqOC9qpLDUXrpMVrdvVhtcPrKS8VAp4
hOle6zYKMShMXDExhH3EHaQ7aVOQRpt5GoGrAoGBAKBX1uE3TK9I9kRyrY4/QFXG
8d62++4+ct9GIlZ+uKq2w4PeVCHNZYDVsIboHDeGcmzJ901WutxRLe8vpbp4L6VY
PsWtNV+k0tu1daS5gim/ArKeMBTgYjerHCcWS5pcmr1k+KBVCIWRqG504L3X8V1M
3BwrNY9CGnP0lW40lK1RAoGASikuIIZ2JA6Pqjdi/WrD1yWjZ7EfgmOlIYk8cd0m
BgXMRbdAMDbUml3f/iNA1hEZqAZctjafhKhLH0o+if641GzGeM+VpYIGIaDO8awn
fbHIqASSgb6/4UCqCZtCPizKYkMWITvVPNgn/2BdqYM6RPJP9tBaIJ2K9IWJLm0D
6KECgYB9rmj/8YW7Rz1Isfg7JhK32p7LC+5xSSbpxQc8s/3PftZ5uQnsXXHoZJ0H
cfA4mbj4nttyFwX+kuUpQdG/ZhoJ/SDqE5lvzVM4stMRKFEJq8ksld+KGGzLFEkj
OotvpQor5dHHU46IIu9tv5ctrJImMjSM7wro26kW2EE3UzZMYw==
-----END RSA PRIVATE KEY-----
External Private Key pasted successfully.
Server /certificate #
```

What to do next

You must activate the external certificate.

Activating the External Certificate

- You must log in as a user with admin privileges.
- You can activate the external certificate only after the certificate and private key are uploaded.
- Activating the external certificate replaces the existing certificate and disconnects any active HTTPS or SSH sessions.

Step 1 Server# **scope certificate**

Enters Cisco IMC certificate command mode.

Step 2 Server /certificate # **activate-external-certificate**

Activates the uploaded external certificate.

Example

This example activates the uploaded certificate:

```
Server # scope certificate
Server /certificate # activate-external-certificate
This operation will overwrite the current certificate with the uploaded external certificate.
All HTTPS and SSH sessions will be disconnected.
Continue?[y|N]y
A system reboot has been initiated.
Server /certificate #
```

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.

SUMMARY STEPS

1. Server# **scope kmip**
2. Server/kmip# **set enabled** {**yes** | **no**}
3. Server/kmip*# **commit**
4. (Optional) Server/kmip # **show detail**

DETAILED STEPS

	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	(Optional) Server/kmip # **show detail**	Displays the KMIP status.

Example

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 .

Before you begin

- Obtain and install a certificate server software package on a server within your organization.

- Ensure that the time is set to the current time.

SUMMARY STEPS

1. **openssl genrsa -out** *Client_Privatekeyfilename keysize*
2. **openssl req -new -x509 -days** *numdays* **-key** *Client_Privatekeyfilename* **-out** *Client_certfilename*
3. Obtain the KMIP root CA certificate from the KMIP server.

DETAILED STEPS

	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 .

Downloading a KMIP Client Certificate

Before you begin

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

SUMMARY STEPS

1. Server# **scope kmip**
2. Server/kmip # **set enabled yes**
3. Server/kmip*# **commit**
4. Server/kmip # **scope kmip-client-certificate**
5. Server /kmip/kmip-client-certificate # **download-client-certificate** *remote-protocol IP Address KMIP client certificate file*
6. At the confirmation prompt, enter **y**.
7. (Optional) Server /kmip/kmip-client-certificate # **paste-client-certificate**

DETAILED STEPS

	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	(Optional) Server /kmip/kmip-client-certificate # **paste-client-certificate**	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.

Example

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
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 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.

SUMMARY STEPS

1. Server# **scope kmip**

2. Server /kmip # **scope kmip-client-certificate**
3. Server /kmip/kmip-client-certificate # **export-client-certificate** *remote-protocol IP Adderss KMIP root CA Certificate file*
4. (Optional) Server /kmip/kmip-client-certificate # **show detail**

DETAILED STEPS

	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 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	(Optional) Server /kmip/kmip-client-certificate # **show detail**	Displays the status of the certificate export.

Example

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.

SUMMARY STEPS

1. Server# **scope kmip**
2. Server# /kmip **scope kmip-client-certificate**
3. Server /kmip/kmip-client-certificate # **delete-client-certificate**
4. At the confirmation prompt, enter **y**.

DETAILED STEPS

	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.

Example

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.

SUMMARY STEPS

1. Server# **scope kmip**
2. Server/kmip # **set enabled yes**
3. Server/kmip * # **commit**
4. Server /kmip # **scope kmip-root-ca-certificate**
5. Server /kmip/kmip-root-ca-certificate # **download-root-ca-certificate** *remote-protocol IP Address KMIP CA Certificate file*
6. At the confirmation prompt, enter **y**.
7. (Optional) Server /kmip/kmip-root-ca-certificate # **paste-root-ca-certificate**

DETAILED STEPS

	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** *remote-protocol IP Address KMIP 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.
Step 6	At the confirmation prompt, enter **y**.	This begins the download of the KMIP root CA certificate.
Step 7	(Optional) Server /kmip/kmip-root-ca-certificate # **paste-root-ca-certificate**	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.

Example

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
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 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.

SUMMARY STEPS

1. Server # **scope kmip**
2. Server /kmip # **scope kmip-root-ca-certificate**
3. Server /kmip/kmip-root-ca-certificate # **export-root-ca-certificate** *remote-protocol IP Adderss KMIP root CA Certificate file*
4. (Optional) Server /kmip/kmip-root-ca-certificate # **show detail**

DETAILED STEPS

	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

	Command or Action	Purpose
		• 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	(Optional) Server /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 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.

SUMMARY STEPS

1. Server# **scope kmip**
2. Server# /kmip **scope kmip-root-ca-certificate**
3. Server /kmip/kmip-root-ca-certificate # **delete-root-ca-certificate**

4. At the confirmation prompt, enter **y**.

DETAILED STEPS

	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.
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.

Example

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.

SUMMARY STEPS

1. Server# **scope kmip**
2. Server/kmip# **set enabled yes**
3. Server/kmip*# **commit**
4. Server/kmip # **scope kmip-client-private-key**
5. Server /kmip/kmip-client-private-key # **download-client-pvt-key** *remote-protocol IP Address KMIP client private key file*
6. At the confirmation prompt, enter **y**.
7. (Optional) Server /kmip/kmip-client-private-key # **paste-client-pvt-key**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope kmip**	Enters the KMIP command mode.
Step 2	Server/kmip# **set enabled yes**	Enables KMIP.

	Command or Action	Purpose
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 **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	(Optional) Server /kmip/kmip-client-private-key # **paste-client-pvt-key**	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.

Example

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.

SUMMARY STEPS

1. Server# **scope kmip**
2. Server /kmip # **scope kmip-client-private-key**
3. Server /kmip/kmip-client-private-key # **export-client-pvt-key** *remote-protocol IP Adderss KMIP root CA Certificate file*
4. (Optional) Server /kmip/kmip-client-private-key # **show detail**

DETAILED STEPS

	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 **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	(Optional) Server /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 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.

SUMMARY STEPS

1. Server# **scope kmip**
2. Server# /kmip **scope kmip-client-private-key**
3. Server /kmip/kmip-client-private-key # **delete-client-pvt-key**
4. At the confirmation prompt, enter **y**.

DETAILED STEPS

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

Example

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.

SUMMARY STEPS

1. Server# **scope kmip**
2. Server /kmip # **scope kmip-login**
3. Server/kmip/kmip-login # **set login** *username*
4. Server/kmip/kmip-login * # **set password**
5. Server/kmip/kmip-login * # **set use-kmip-cred** {**yes** | **no**}
6. Server/kmip/kmip-login * # **commit**
7. (Optional) Server/kmip/kmip-login # **restore**

DETAILED STEPS

	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	(Optional) Server/kmip/kmip-login # **restore**	Restores the KMIP settings to defaults.

Example

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	(Optional) Server /kmip/kmip-server # **show detail**	Displays the KMIP server details.

Example

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 #
```

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.

SUMMARY STEPS

1. Server # **scope server** {**1** | **2**}
2. Server /server # **scope bmc**
3. Server /server/bmc # **scope kmip**
4. Server /server/bmc/kmip # **set enabled** {**yes** | **no**}
5. Server /server/bmc/kmip *# **commit**
6. (Optional) Server /server/bmc/kmip # **show detail**

DETAILED STEPS

	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.
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.

SUMMARY STEPS

1. Server # **scope server** {**1** | **2**}
2. Server /server # **scope bmc**
3. Server /server/bmc # **scope kmip**
4. Server /server/bmc/kmip # **scope kmip-login**
5. Server /server/bmc/kmip/kmip-login # **set login** *username*
6. Server /server/bmc/kmip/kmip-login * # **set password**
7. Server /server/bmc/kmip/kmip-login * # **set use-kmip-cred** {**yes** | **no**}
8. Server /server/bmc/kmip/kmip-login * # **commit**
9. (Optional) Server /server/bmc/kmip/kmip-login # **restore**

DETAILED STEPS

	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** *username*	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.

	Command or Action	Purpose
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.
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 preforming 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 .

Before you begin

- Obtain and install a certificate server software package on a server within your organization.

- Ensure that the time is set to the current time.

SUMMARY STEPS

1. **openssl genrsa -out** *Client_Privatekeyfilename keysize*
2. **openssl req -new -x509 -days** *numdays* **-key** *Client_Privatekeyfilename* **-out** *Client_certfilename*
3. Obtain the KMIP root CA certificate from the KMIP server.

DETAILED STEPS

	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 .

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** *server ID*	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** *server ID*	Enters the chosen KMIP server command mode.
Step 5	Server /server/bmc/kmip/kmip-server # **set** *kmip-port*	Sets the KMIP port.
Step 6	Server /server/bmc/kmip/kmip-server *# **set** *kmip-server*	Sets the KMIP server ID.
Step 7	Server /server/bmc/kmip/kmip-server # **set** *kmip-timeout*	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.

SUMMARY STEPS

1. Server # **scope server** {**1** | **2**}
2. Server /server # **scope bmc**
3. Server /server/bmc # **scope kmip**
4. Server /server/bmc/kmip # **set enabled yes**
5. Server /server/bmc/kmip *# **commit**
6. Server /server/bmc/kmip # **scope kmip-client-certificate**
7. Server /server/bmc/kmip/kmip-client-certificate # **download-client-certificate** *remote-protocol IP Address KMIP client certificate file*
8. At the confirmation prompt, enter **y**.
9. (Optional) Server /server/bmc/kmip/kmip-client-certificate # **paste-client-certificate**

DETAILED STEPS

	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** *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

	Command or Action	Purpose
		• 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 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**	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.

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
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 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.

SUMMARY STEPS

1. Server # **scope server** {**1** | **2**}
2. Server /server # **scope bmc**
3. Server /server/bmc # **scope kmip**
4. Server /server/bmc/kmip # **scope kmip-client-certificate**
5. Server /server/bmc/kmip/kmip-client-certificate # **export-client-certificate** *remote-protocol IP Adderss KMIP root CA Certificate file*
6. (Optional) Server /server/bmc/kmip/kmip-client-certificate # **show detail**

DETAILED STEPS

	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 # **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 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 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.

SUMMARY STEPS

1. Server # **scope server** {**1** | **2**}
2. Server /server # **scope bmc**
3. Server /server/bmc # **scope kmip**
4. Server /server/bmc/kmip # **scope kmip-client-certificate**
5. Server /server/bmc/kmip/kmip-client-certificate # **delete-client-certificate**
6. At the confirmation prompt, enter **y**.

DETAILED STEPS

	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.

SUMMARY STEPS

1. Server # **scope server** {**1** | **2**}
2. Server /server # **scope bmc**
3. Server /server/bmc # **scope kmip**
4. Server /server/bmc/kmip # **set enabled yes**
5. Server /server/bmc/kmip *# **commit**
6. Server /server/bmc/kmip # **scope kmip-client-private-key**
7. Server /server/bmc/kmip/kmip-client-private-key # **download-client-pvt-key** *remote-protocol IP Address KMIP client private key file*
8. At the confirmation prompt, enter **y**.
9. (Optional) Server /server/bmc/kmip/kmip-client-private-key # **paste-client-pvt-key**

DETAILED STEPS

	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-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 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 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**	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.

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
```

```
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 /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.

SUMMARY STEPS

1. Server # **scope server** {**1** | **2**}
2. Server /server # **scope bmc**
3. Server /server/bmc # **scope kmip**
4. Server /server/bmc/kmip # **scope kmip-client-private-key**
5. Server /server/bmc/kmip/kmip-client-private-key # **export-client-pvt-key** *remote-protocol IP Adderss KMIP root CA Certificate file*
6. (Optional) Server /server/bmc/kmip/kmip-client-private-key # **show detail**

DETAILED STEPS

	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.

	Command or Action	Purpose
Step 5	Server /server/bmc/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 **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 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
KmipCertificates
/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.

SUMMARY STEPS

1. Server # **scope server** {**1** | **2**}
2. Server /server # **scope bmc**
3. Server /server/bmc # **scope kmip**
4. Server /server/bmc/kmip # **scope kmip-client-private-key**
5. Server /server/bmc//kmip/kmip-client-private-key # **delete-client-pvt-key**
6. At the confirmation prompt, enter **y**.

DETAILED STEPS

	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.

SUMMARY STEPS

1. Server # **scope server** {**1** | **2**}
2. Server /server # **scope bmc**
3. Server /server/bmc # **scope kmip**
4. Server /server/bmc/kmip # **set enabled yes**
5. Server /server/bmc/kmip * # **commit**
6. Server server/bmc/kmip # **scope kmip-root-ca-certificate**
7. Server server/bmc/kmip/kmip-root-ca-certificate # **download-root-ca-certificate** *remote-protocol IP Address KMIP CA Certificate file*
8. At the confirmation prompt, enter **y**.
9. (Optional) Server server/bmc/kmip/kmip-root-ca-certificate # **paste-root-ca-certificate**

DETAILED STEPS

	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** *remote-protocol IP Address KMIP 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.
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**	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.

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-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 /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
```

```
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 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.

SUMMARY STEPS

1. Server # **scope server** {**1** | **2**}
2. Server /server # **scope bmc**
3. Server /server/bmc # **scope kmip**
4. Server /server/bmc/kmip # **scope kmip-root-ca-certificate**
5. Server /server/bmc/kmip/kmip-root-ca-certificate # **export-root-ca-certificate** *remote-protocol IP Adderss KMIP root CA Certificate file*
6. (Optional) Server /server/bmc/kmip/kmip-root-ca-certificate # **show detail**

DETAILED STEPS

	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.

	Command or Action	Purpose
Step 5	Server /server/bmc/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 **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 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.

SUMMARY STEPS

1. Server # **scope server** {**1** | **2**}
2. Server /server # **scope bmc**
3. Server /server/bmc # **scope kmip**
4. Server /server/bmc/kmip # **scope kmip-root-ca-certificate**
5. Server /server/bmc/kmip/kmip-root-ca-certificate # **delete-root-ca-certificate**
6. At the confirmation prompt, enter **y**.

DETAILED STEPS

	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.
```

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.

SUMMARY STEPS

1. Server # **scope cimc**
2. Server /cimc # **scope security-configuration**
3. Server /chassis/security-configuration # **set fips enabled** or **disabled**
4. Server /chassis/security-configuration* # **commit**
5. Server /chassis/security-configuration # **set cc enabled** or **disabled**
6. Server /chassis/security-configuration* # **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope security-configuration**	Enters the security configuration command mode.
Step 3	Server /chassis/security-configuration # **set fips enabled** or **disabled**	If you choose enabled, it enables FIPS.
Step 4	Server /chassis/security-configuration* # **commit**	Enter **y** at the warning prompt to enable FIPS and commit the transaction to the system. **Note** When you switch the FIPS mode, it restarts the SSH, KVM, SNMP, webserver, XMLAPI, and redfish services.

	Command or Action	Purpose
		Note When you enable FIPS, or both FIPS and CC, the following SNMP configuration changes occur: • 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.
Step 5	Server /chassis/security-configuration # **set cc enabled** or **disabled**	**Note** FIPS must be in enabled state to enable CC. If you choose enabled, it enables CC.
Step 6	Server /chassis/security-configuration* # **commit**	Enter **y** at the warning prompt to enable FIPS and commit the transaction to the system. **Note** When you switch the FIPS mode, it restarts the SSH, KVM, SNMP, webserver, XMLAPI, and redfish services. **Note** When you enable FIPS, or both FIPS and CC, the following SNMP configuration changes occur: • 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.

Example

This example shows how to view the controller information:

```
Server# scope cimc
Server /cimc # scope security-configuration
Server /cimc/security-configuration # set fips enabled
Enabling FIPS would
1. Disables support for SNMP V2 and V3 with No 'Auth/Priv' security level.
2. Disables support for 'MD5/DES' crypto algorithms in SNMP 'Auth/Priv' keys.
3. Ensures use of only FIPS-compliant ciphers in SSH, webserver and KVM connections.
Server /cimc/security-configuration* # commit
Server/cimc/security-configuration # set cc enabled
Enabling Common Criteria
Server /cimc/security-configuration* # commit
Warning: changing "fips" or "CC" will restart SSH, KVM, SNMP, webserver, XMLAPI and redfish
 services.
Do you wish to continue? [y/N] y
Server /cimc/security-configuration #
```