



## Managing Certificates

---

This chapter includes the following sections:

- [Managing the Server Certificate, page 1](#)
- [Generating a Certificate Signing Request, page 1](#)
- [Creating a Self-Signed Certificate, page 3](#)
- [Uploading a Server Certificate, page 5](#)

## Managing the Server Certificate

You can generate a certificate signing request (CSR) to obtain a new certificate, and you can upload the new certificate to the CIMC 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.

### Procedure

---

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

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

---

## Generating a Certificate Signing Request

### Before You Begin

You must log in as a user with admin privileges to configure certificates.



```
gYEAG61CaJoJaVMhzCl90306Mg51zq1zXcz75+VFj2I6rH9asckClD3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtv1WvfhevskV0j6
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 the CIMC 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.

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

## Creating a Self-Signed Certificate

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



#### Note

These commands are to be entered on a Linux server with the OpenSSL package, not in the CIMC CLI.

### Before You Begin

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

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<pre>openssl genrsa -out CA_keyfilename keysize</pre> <p><b>Example:</b> # openssl genrsa -out ca.key 1024</p>	<p>This command generates an RSA private key that will be used by the CA.</p> <p><b>Note</b> To allow the CA to access the key without user input, do not use the <code>-des3</code> option for this command.</p> <p>The specified file name contains an RSA key of the specified key size.</p>
<b>Step 2</b>	<pre>openssl req -new -x509 -days numdays -key CA_keyfilename -out CA_certfilename</pre> <p><b>Example:</b> # openssl req -new -x509 -days 365 -key ca.key -out ca.crt</p>	<p>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.</p> <p>The certificate server is an active CA.</p>
<b>Step 3</b>	<pre>echo "nsCertType = server" &gt; openssl.conf</pre> <p><b>Example:</b> # echo "nsCertType = server" &gt; openssl.conf</p>	<p>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.</p> <p>The OpenSSL configuration file <code>openssl.conf</code> contains the statement <code>"nsCertType = server"</code>.</p>
<b>Step 4</b>	<pre>openssl x509 -req -days numdays -in CSR_filename -CA CA_certfilename -set_serial 04 -CAkey CA_keyfilename -out server_certfilename -extfile openssl.conf</pre> <p><b>Example:</b> # openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf</p>	<p>This command directs the CA to use your CSR file to generate a server certificate.</p> <p>Your server certificate is contained in the output file.</p>

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 1024
Generating RSA private key, 1024 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 CIMC.

# 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.



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



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

**Procedure**

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

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

This example uploads a new certificate to the server:

```
Server# scope certificate
Server /certificate # upload
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGx1IEluYy4xEzARBgNVBAst
C1Rlc3QgR3JvdXAxEWVzAG56ZmSHRMQeOGHemdh66u2/XAoLx7YCCyU
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCCyU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBKOND1
GMbkPayVlQjbG4MD2dx2+H8EH3LmtdZrgKvPxPTE+bf5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzC190306Mg51zq1zXcz75+VFj2I6rH9ascClD3mkOVx5gJU
Ptt5CVQpNgNldvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvLWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L4317IPN1HhOi3oha4=
-----END CERTIFICATE-----
<CTRL+D>
```