Managing Certificates

Managing the Server Certificate

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.

Procedure

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

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

Common Name (CN)	The fully qualified hostname of the CIMC.
Organization Name (O)	The organization requesting the certificate.
Organization Unit (OU)	The organizational unit.
Locality (L)	The city or town in which the company requesting the certificate is headquartered.
StateName (S)	The state or province in which the company requesting the certificate is headquartered.
Country Code (CC)	The two-letter ISO country code for the country in which the company is headquartered.
Email	The administrative 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 /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
[Supported Algorithms: sha1, sha256, sha384, sha512 (Default sha384)]
Signature Algorithm: sha384
Do you want to set Challenge Password ? [y|n] (Default y)n
String Encoding utf8only/nombstr/pkix/default (Enter to skip):
Do you want to enter Subject Alternative Name parameters?[y|n]n
Continue to generate CSR?[y|N]y
Do you want self sign CSR and overwrite the current certificate?
All HTTPS and SSH sessions will be disconnected. [y|N]y

Server /certificate # show detail
Certificate Information:
    Serial Number: 3FA8AF325A18359FAFB29C518838A542D945F0EB
    Subject Country Code (CC): US
    Subject State (S): CA
    Subject Locality (L): San Jose
    Subject Organization (O): "Example
    Subject Organizational Unit (OU): Test Department
    Subject Common Name (CN): test.example.com
    Issuer Country Code (CC): US
    Issuer State (S): CA
    Issuer Locality (L): San Jose
    Issuer Organization (O): "Example
    Issuer Organizational Unit (OU): Test Department
```

```
Issuer Common Name (CN): test.example.com
Valid From: Mar 24 04:32:34 2023 GMT
Valid To: Jun 26 04:32:34 2025 GMT
```

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
Step 1	**openssl genrsa -out** *CA_keyfilenamekeysize* **Example:** `# openssl genrsa -out ca.key 1024`	This command generates an RSA private key that is 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.

	Command or Action	Purpose
Step 2	**opensslreq-new -x509 -days** *numdays*-**key***CA_keyfilename*-**out***CA_certfilename* **Example:** `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	This command generates a new self-signed certificatefor the CA using the specified key. The certificate is valid for the specified period. The command prompts the user for additional certificate information. The certificate server is an active CA.
Step 3	**echo"nsCertType = server" > openssl.conf** **Example:** `# echo "nsCertType = server" > openssl.conf`	This command adds a line to the OpenSSL configuration fileto 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	**opensslx509-text -noout -in ca.crt** **Example:** `# openssl x509 -text -noout -in ca.crt`	This command displays the certificate.

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.

```
[root@localhost ~]# openssl genrsa -out ca.key 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
...........+++++
......+++++
e is 65537 (0x010001)
[root@localhost ~]# 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) [XX]:US
State or Province Name (full name) []:CA
Locality Name (eg, city) [Default City]:San Jose
Organization Name (eg, company) [Default Company Ltd]:Example
Organizational Unit Name (eg, section) []:Test Department
Common Name (eg, your name or your server's hostname) []:test.example.com
Email Address []:user@example.com
[root@localhost ~]#
[root@localhost ~]# echo "nsCertType = server" > openssl.conf
[root@localhost ~]# openssl x509 -text -noout -in ca.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            33:52:14:5a:12:8d:12:9c:c1:fa:77:13:a5:0c:eb:af:83:bd:6b:68
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = CA, L = San Jose, O = Example, OU = Test Department, CN =
test.example.com, emailAddress = user@example.com
```

```
        Validity
            Not Before: Mar 28 23:15:11 2023 GMT
            Not After : Mar 27 23:15:11 2024 GMT
        Subject: C = US, ST = CA, L = San Jose, O = Example, OU = Test Department, CN =
test.example.com, emailAddress = user@example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (1024 bit)
                Modulus:
                    00:b9:a6:16:7d:bf:74:d0:10:e2:61:af:56:55:ee:
                    60:e6:57:c0:74:bd:b0:0b:7d:64:54:75:74:d8:f8:
                    7b:3e:1a:5b:cf:d4:76:6d:fb:01:92:07:d0:3b:45:
                    9c:49:22:7d:22:55:75:05:d9:94:d2:f2:7d:4b:14:
                    96:5e:fc:26:12:30:6f:1f:54:a8:40:25:e2:1a:62:
                    f8:ec:f8:be:e2:b0:fc:85:21:9b:cb:78:f7:6d:0e:
                    00:01:50:a9:07:e8:de:c2:b5:44:c5:41:c1:3a:0b:
                    93:4f:e9:94:c6:82:df:76:15:de:42:1f:b3:86:de:
                    96:0c:52:27:10:25:25:75:8d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                71:84:61:C4:AF:E7:57:2C:B4:BB:19:22:D7:DC:7A:7F:80:E8:58:A3
            X509v3 Authority Key Identifier:
                keyid:71:84:61:C4:AF:E7:57:2C:B4:BB:19:22:D7:DC:7A:7F:80:E8:58:A3

            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         89:6d:7f:72:89:29:4e:8b:da:74:ec:8b:10:78:ca:86:68:be:
         88:c2:25:79:cd:a1:dc:7d:ac:32:18:be:7d:54:6e:12:c9:53:
         de:c3:dc:b3:e7:52:1e:14:c5:1c:10:95:3f:e3:df:04:82:27:
         19:56:55:c6:96:e1:0c:cc:0a:81:05:aa:3f:a3:29:52:b3:bb:
         66:78:55:2b:b0:c5:f9:f7:bc:fb:e4:fd:30:f2:16:73:65:88:
         38:ea:6f:dc:34:44:50:ef:3b:a8:ac:22:98:34:11:bb:e8:27:
         6d:da:5d:ff:18:b9:e4:4f:22:54:b9:ab:51:1f:41:51:00:4e:
         25:f6
[root@localhost ~]#
```

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
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
gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE-----
<CTRL+D>
```