Configure UCS Server Certificate to CIMC

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

Generate CSR

Create Self-Signed Certificate

Verify

Troubleshoot

Related Information

Introduction

This document describes how to generate a Certificate Signing Request (CSR) to obtain a new certificate.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- You must log in as a user with admin privileges to configure certificates.
- Ensure that the CIMC time is set to the current time.

Components Used

The information in this document is based on these software and hardware versions:

- CIMC 1.0 or later
- Openssl

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The certificate can be uploaded to the Cisco Integrated Management Controller (CIMC) in order to replace the current server certificate. The server certificate can 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.

Configure

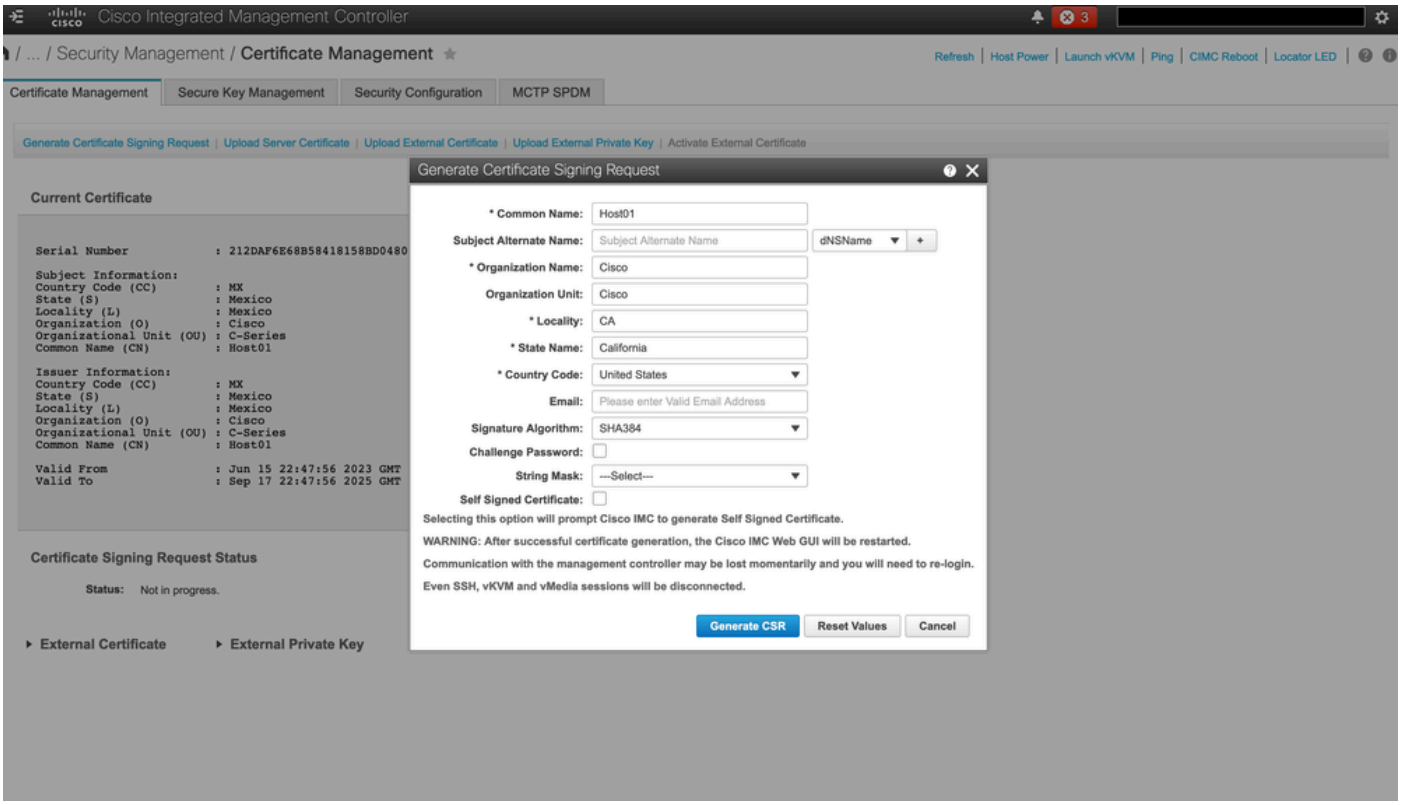
Step 1.	Generate the CSR from the CIMC.
Step 2.	Submit the CSR file to a CA to sign the certificate. If your organization generates its own self-signed certificates, you can use the CSR file to generate a self-signed certificate.
Step 3.	Upload the new certificate to the CIMC.

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.

Generate CSR

Navigate to **Admin tab > Security Management > Certificate Management > Generate Certificate Signing Request** (CSR) and fill the details marked with an *.

Also, refer to the guide Generating a Certificate Signing Request.



Caution: Use the Subject Alternate Name to specify additional host names for this Server. Not configuring dNSName or excluding it from the uploaded certificate can result in browsers blocking access to the Cisco IMC interface.

What to Do Next?

Perform these 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 CIMC to internally generate a self-signed certificate from the CSR and upload it immediately to the server. Check the **Self Signed Certificate** box to perform this task.
- If your organization operates its own 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 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.

Note: After successful certificate generation, the Cisco IMC Web GUI is restarted. Communication with the management controller can be lost momentarily and re-login is required.

If you did not use the first option, in which CIMC internally generates and uploads a self-signed certificate, you must create a new self-signed certificate and upload it to the CIMC.

Create Self-Signed Certificate

As an alternative to a public CA and sign a server certificate, operate your own CA and sign your own certificates. This section shows commands to create a CA and generate a server certificate with the OpenSSL server certificate. For detailed information about OpenSSL, see OpenSSL.

Step 1. Generate **RSA private key** as shown in the image.

<#root>

```
[root@redhat ~]#
```

openssl genrsa -out ca.key 1024

Step 2. Generate new **self-signed certificate** as shown in the image.

<#root>

```
[root@redhat ~]#
```

openssl req -new -x509 -days 1095 -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) []:
```

California

```
Locality Name (eg, city) [Default City]:
```

California

```
Organization Name (eg, company) [Default Company Ltd]:
Cisco

Organizational Unit Name (eg, section) []:
Cisco

Common Name (eg, your name or your server's hostname) []:
Host01

Email Address []:
[root@redhat ~]#
```

Step 3. Ensure that the certificate type is **server** as shown in the image.

```
<#root>
[root@redhat ~]#
echo "nsCertType = server" > openssl.conf
```

Step 4. Directs the CA to use your CSR file to generate a server certificate as shown in the image.

```
<#root>
[root@redhat ~]#
openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt -extfile
```

Step 5. Verify if the generated certificate is of type Server as shown in the image.

```
<#root>
[root@redhat ~]#
openssl x509 -in server.crt -purpose

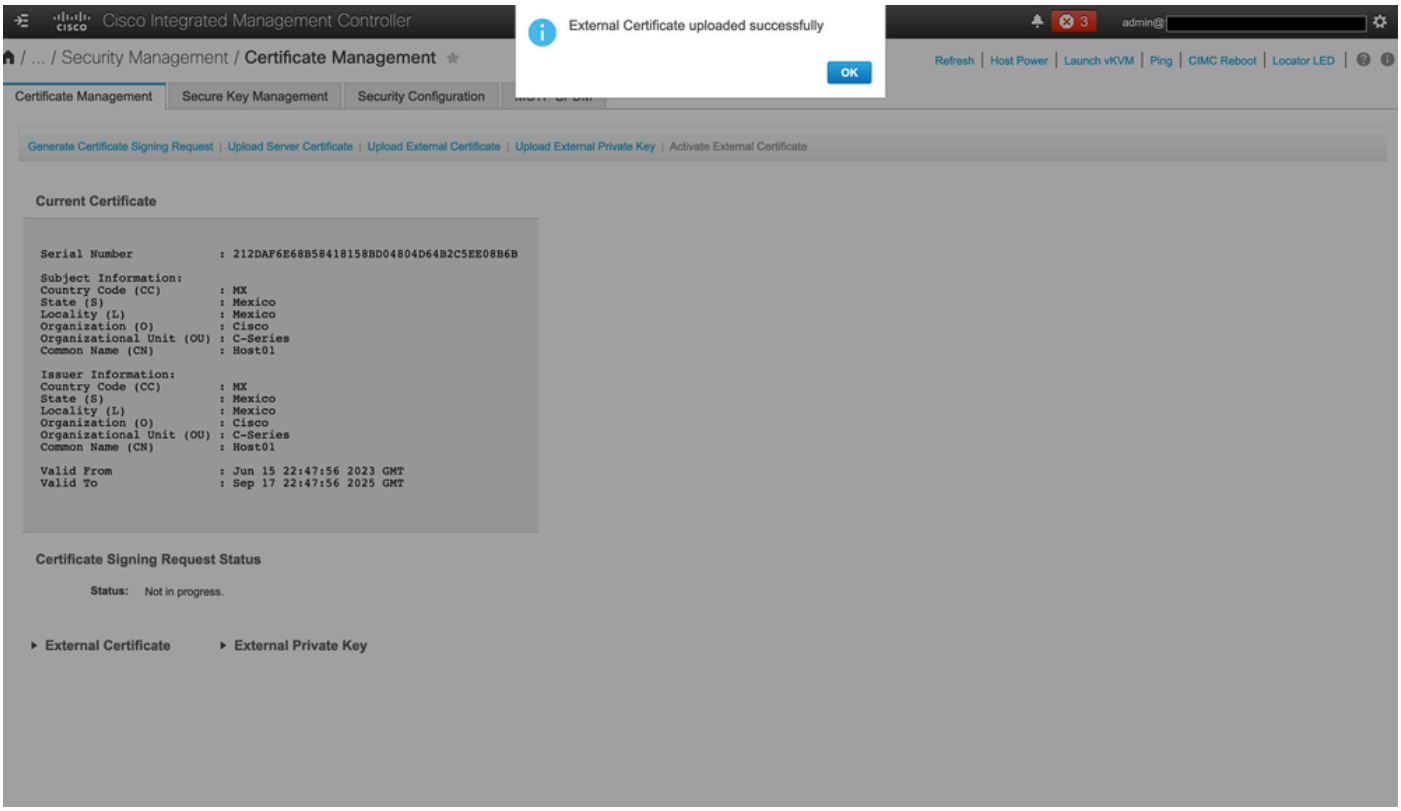
Certificate purposes:
SSL client : No
```

```
SSL client CA : No
SSL server :

Yes


SSL server CA : No
Netscape SSL server : Yes
Netscape SSL server CA : No
S/MIME signing : No
S/MIME signing CA : No
S/MIME encryption : No
S/MIME encryption CA : No
CRL signing : Yes
CRL signing CA : No
Any Purpose : Yes
Any Purpose CA : Yes
OCSP helper : Yes
OCSP helper CA : No
Time Stamp signing : No
Time Stamp signing CA : No
-----BEGIN CERTIFICATE-----
MIIDFzCCAoCgAwIBAgIBATANBgkqhkiG9w0BAQsFADBoMQswCQYDVQQGEwJVUzET
MBEGA1UECAwKQ2FsaWZvcm5pYTETMBEGA1UEBwwKQ2FsaWZvcm5pYTEOMAwGA1UE
CgwFQ2lzY28xDjAMBgNVBAsMBUNpc2NvMQ8wDQYDVQQDDAZIb3N0MDEwHhcNMjMw
NjI3MjI0NDE1WhcNMjQwNjI2MjI0NDE1WjBgMQswCQYDVQQGEwJVUzETMBEGA1UE
CAwKQ2FsaWZvcm5pYTELMAkGA1UEBwwCQ0ExDjAMBgNVBAoMBUNpc2NvMQ4wDAYD
VQQLDAVDaXNjbzEPMA0GA1UEAwwGSG9zdDAxMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAuhJ5OVOO4MZNV3dgQwOMns9sgzZwjJS8LvOtHt+GA4uzNf1Z
WKNyZbzD/yLoXiv8ZFgaWJbqEe2yijVzEcguZQTGFRkAWmDecKM9Fieob03B5FNt
pC8M9Dfb3YMkIx29abrZKFEIrYbabbG4gQyfzgOB6D9CK1WuoezsE7zHOoJX4Bcy
ISE0RsOd9bsXvxyLk2cauS/zvI9hvrWW9P/Og8nF3Y+PGtm/bnfodEnNWFWPLtvF
dGuG5/wBmmMbEb/GbrH9uVcyOz+3HReDcQ+kJde7PoFK3d6ZOdkh7Mmtjpvk5ucQ
NgzaeoCDL0Bn+Zl08O0/eciSCsGIJKxYD/FYlQIDAQABo1UwUzARBglghkgBhvhC
AQEEBAMCBkAwHQYDVR0OBBYEFEJ2OTeuP27jyCJRiAKKfflNcOhbMB8GA1UdIwQY
MBaAFA4QR965FinE4GrhkiwRV62ziPj/MA0GCSqGSIb3DQEBCwUAA4GBAJuL/Bej
DxenfCt6pBA7O9GtkltWUS/rEtpQX19Ohdlahjwbf G/67MYIpIEbidL1BCw55dal
LI7sgu1dnItnIGsJIlL7h6IeFBu/coCvBtopOYUanaBJ1BgxBWhT2FAnmB9wIvYJ
5rMx95vWZXt3KGE8QlP+eGkmAHWA8M0yhwHa
-----END CERTIFICATE-----
[root@redhat ~]#
```

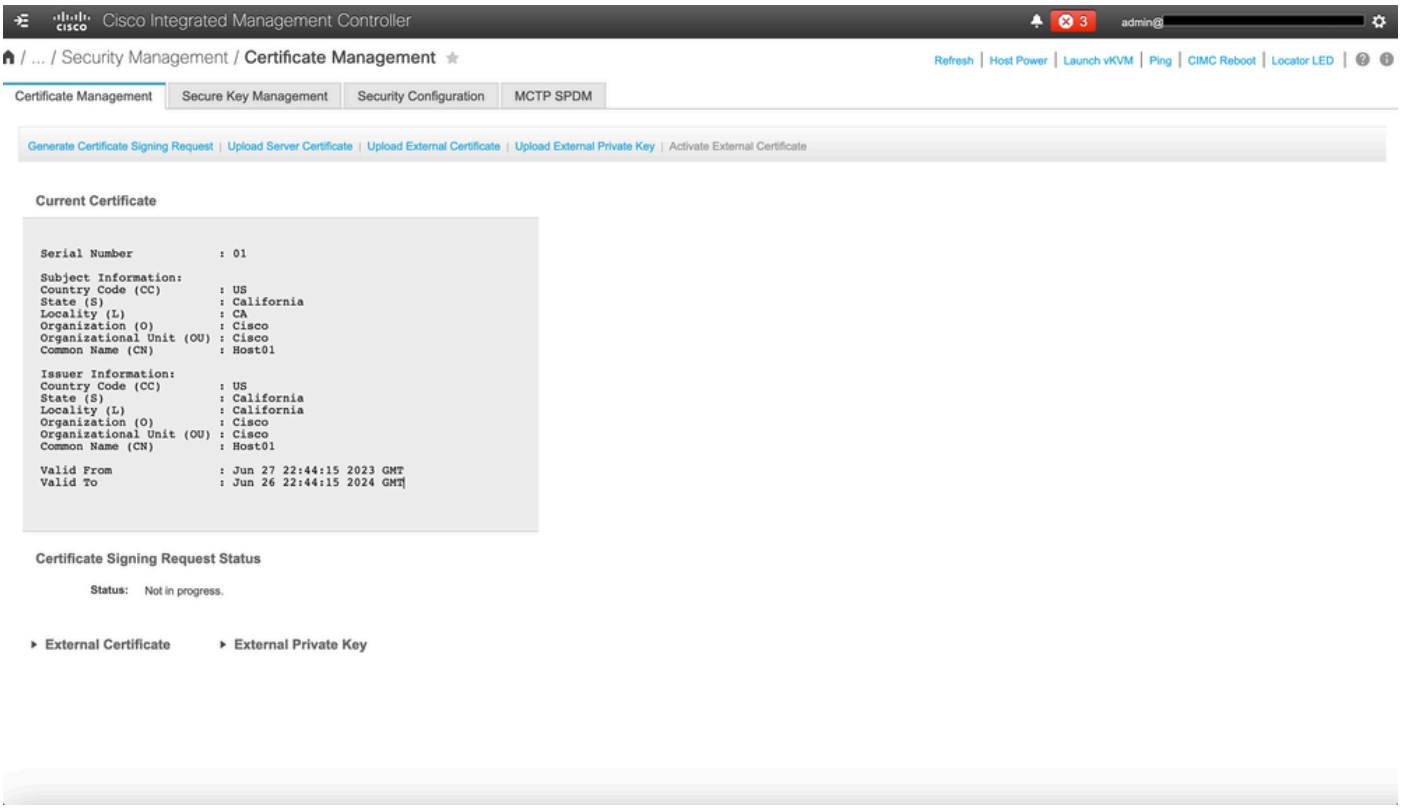
Step 6. Upload **Server Certificate** as shown in the image.



Verify

Use this section in order to confirm that your configuration works properly.

Navigate to **Admin > Certificate Management** and verify the **Current Certificate** as shown in the image.



Troubleshoot

There is currently no specific information available to troubleshoot this configuration.

Related Information

- Cisco bug ID CSCup26248 - Unable to upload 3rd party CA SSL certificate to CIMC 2.0.(1a)
- Technical Support & Documentation - Cisco Systems