

# Configuración del certificado del servidor UCS en CIMC

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Generar CSR](#)

[Crear certificado con firma automática](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe cómo generar una Solicitud de firma de certificado (CSR) para obtener un nuevo certificado.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Debe iniciar sesión como usuario con privilegios de administrador para configurar certificados.
- Asegúrese de que la hora CIMC está establecida en la hora actual.

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CIMC 1.0 o posterior
- Openssl

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en


funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

El certificado se puede cargar en Cisco Integrated Management Controller (CIMC) para sustituir el certificado de servidor actual. El certificado de servidor puede estar firmado por una entidad emisora de certificados (CA) pública, como Verisign, o por su propia entidad emisora de certificados. La longitud de la clave del certificado generado es de 2048 bits.

## Configurar

Paso 1.	Genere la CSR desde el CIMC.
Paso 2.	Envíe el archivo CSR a una CA para firmar el certificado. Si su organización genera sus propios certificados autofirmados, puede utilizar el archivo CSR para generar un certificado autofirmado.
Paso 3.	Cargue el nuevo certificado en el CIMC.

 Nota: El certificado cargado debe crearse a partir de una CSR generada por el CIMC. No cargue un certificado que no haya sido creado por este método.

## Generar CSR


Vaya a la pestaña Admin > Security Management > Certificate Management > Generate Certificate Signing Request (CSR) y rellene los detalles marcados con un \*.

Además, consulte la guía [Generación de una Solicitud de Firma de Certificado](#).

The screenshot shows the Cisco IMC web interface with the 'Generate Certificate Signing Request' dialog box open. The dialog box contains the following fields and options:

- \* Common Name: Host01
- Subject Alternate Name: Subject Alternate Name (dropdown), dNSName (dropdown)
- \* Organization Name: Cisco
- Organization Unit: Cisco
- \* Locality: CA
- \* State Name: California
- \* Country Code: United States (dropdown)
- Email: Please enter Valid Email Address
- Signature Algorithm: SHA384 (dropdown)
- Challenge Password:
- String Mask: ---Select---
- Self Signed Certificate:


Below the dialog box, there is a warning message: "WARNING: After successful certificate generation, the Cisco IMC Web GUI will be restarted. Communication with the management controller may be lost momentarily and you will need to re-login. Even SSH, vKVM and vMedia sessions will be disconnected." At the bottom of the dialog box, there are three buttons: "Generate CSR", "Reset Values", and "Cancel".

 **Precaución:** utilice el nombre alternativo del sujeto para especificar nombres de host adicionales para este servidor. Si no se configura dNSName o se excluye del certificado cargado, los navegadores pueden bloquear el acceso a la interfaz de Cisco IMC.

## Pasos Sigüientes?

Realice estas tareas:

- Si no desea obtener un certificado de una autoridad de certificación pública y si su organización no tiene su propia autoridad de certificación, puede permitir que CIMC genere internamente un certificado autofirmado de la CSR y lo cargue inmediatamente en el servidor. Marque la casilla Certificado autofirmado para realizar esta tarea.
- Si su organización utiliza sus propios certificados autofirmados, copie el resultado del comando de -----BEGIN ...to END CERTIFICATE REQUEST----- y péguelo en un archivo denominado csr.txt. Introduzca el archivo CSR en el servidor de certificados para generar un certificado autofirmado.
- Si obtiene un certificado de una autoridad de certificación pública, copie el resultado del comando de -----BEGIN ... a END CERTIFICATE REQUEST----- y péguelo en un archivo denominado csr.txt. Envíe el archivo CSR a la autoridad de certificación para obtener un certificado firmado. Asegúrese de que el certificado es del tipo Servidor.

 **Nota:** tras generar correctamente el certificado, se reinicia la GUI web de Cisco IMC. La comunicación con el controlador de administración se puede perder momentáneamente y es necesario volver a iniciar sesión.

Si no utilizó la primera opción, en la que CIMC genera y carga internamente un certificado autofirmado, debe crear un nuevo certificado autofirmado y cargarlo en CIMC.

## Crear certificado con firma automática

Como alternativa a una CA pública y firmar un certificado de servidor, utilice su propia CA y firme sus propios certificados. Esta sección muestra comandos para crear una CA y generar un certificado de servidor con el certificado de servidor OpenSSL. Para obtener información detallada sobre OpenSSL, vea [OpenSSL](#).

Paso 1. Genere la clave privada RSA como se muestra en la imagen.

```
<#root>
```

```
[root@redhat ~]#  
openssl genrsa -out ca.key 1024
```

Paso 2. Genere un nuevo certificado autofirmado como se muestra en la imagen.

```
<#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 ~]#

Paso 3. Asegúrese de que el tipo de certificado sea servidor, como se muestra en la imagen.

<#root>

[root@redhat ~]#

```
echo "nsCertType = server" > openssl.conf
```

Paso 4. Indica a la CA que utilice el archivo CSR para generar un certificado de servidor, como se muestra en la imagen.

<#root>

[root@redhat ~]#

```
openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt -extfile
```

Paso 5. Verifique si el certificado generado es del tipo Servidor como se muestra en la imagen.

<#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

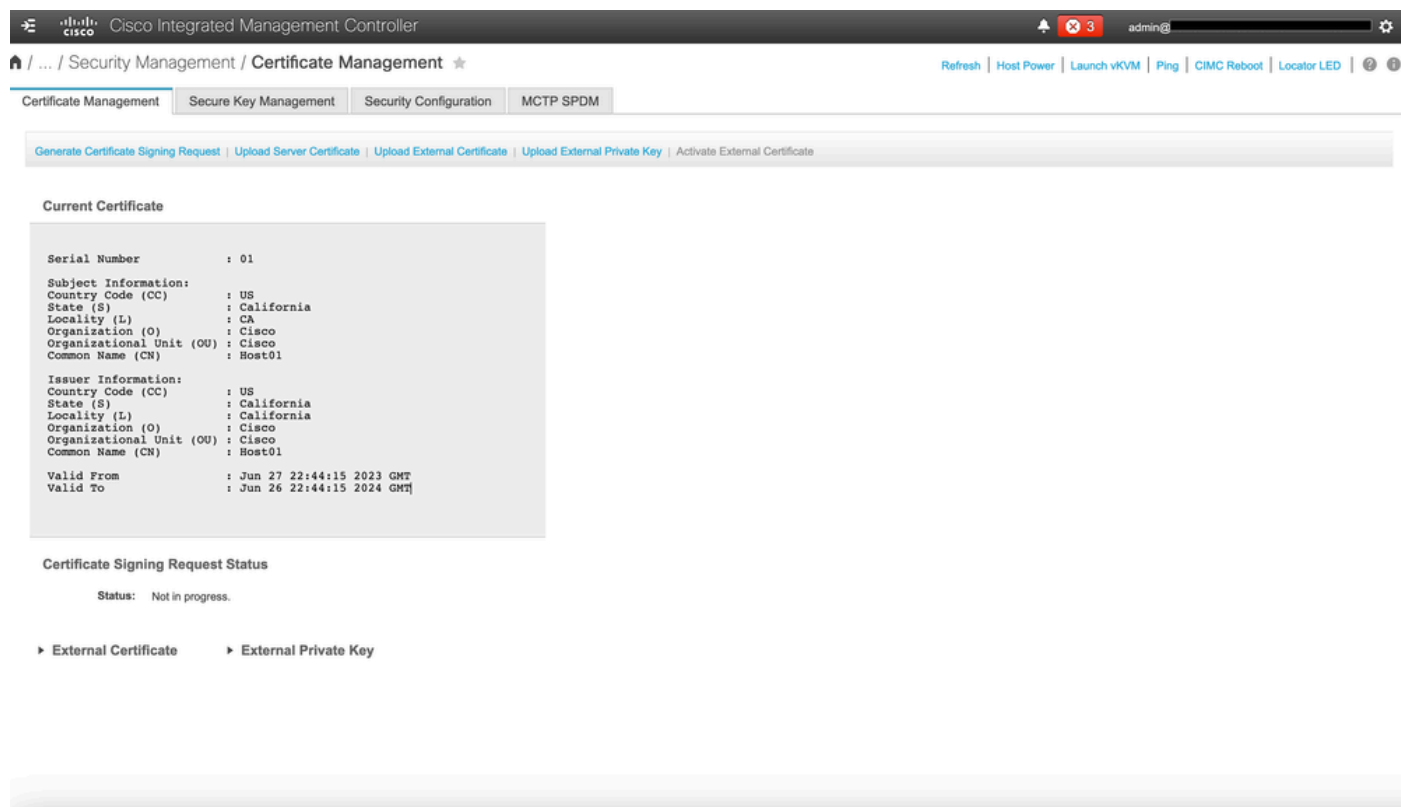
S/MIME encryption : No



# Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Navegue hasta Admin > Certificate Management y verifique el Certificado actual como se muestra en la imagen.



Cisco Integrated Management Controller

admin@

... / Security Management / Certificate Management

Refresh | Host Power | Launch vKVM | Ping | CIMC Reboot | Locator LED

Certificate Management | Secure Key Management | Security Configuration | MCTP SPDM

Generate Certificate Signing Request | Upload Server Certificate | Upload External Certificate | Upload External Private Key | Activate External Certificate

Current Certificate

```
Serial Number          : 01
Subject Information:
Country Code (CC)     : US
State (S)              : California
Locality (L)          : CA
Organization (O)      : Cisco
Organizational Unit (OU) : Cisco
Common Name (CN)      : Host01
Issuer Information:
Country Code (CC)     : US
State (S)              : California
Locality (L)          : California
Organization (O)      : Cisco
Organizational Unit (OU) : Cisco
Common Name (CN)      : Host01
Valid From             : Jun 27 22:44:15 2023 GMT
Valid To               : Jun 26 22:44:15 2024 GMT
```

Certificate Signing Request Status

Status: Not in progress.

External Certificate   External Private Key

# Troubleshoot

Actualmente, no hay información específica disponible sobre cómo solucionar los problemas de esta configuración.

# Información Relacionada

- Id. de error de Cisco [CSCup26248](#): no se puede cargar el certificado SSL de CA de terceros en CIMC 2.0.(1a)
- [Soporte Técnico y Documentación - Cisco Systems](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).