

将UCS服务器证书配置为CIMC

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[生成 CSR](#)

[创建自签名证书](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何生成证书签名请求(CSR)以获取新证书。

先决条件

要求

Cisco 建议您了解以下主题：

- 您必须以具有管理员权限的用户身份登录才能配置证书。
- 确保CIMC时间设置为当前时间。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CIMC 1.0或更高版本
- Openssl

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

可将证书上传到思科集成管理控制器(CIMC)以替换当前服务器证书。服务器证书可以由公共证书颁发机构(CA)（例如Verisign）签署，也可以由您自己的证书颁发机构签署。生成的证书密钥长度为

2048位。

配置

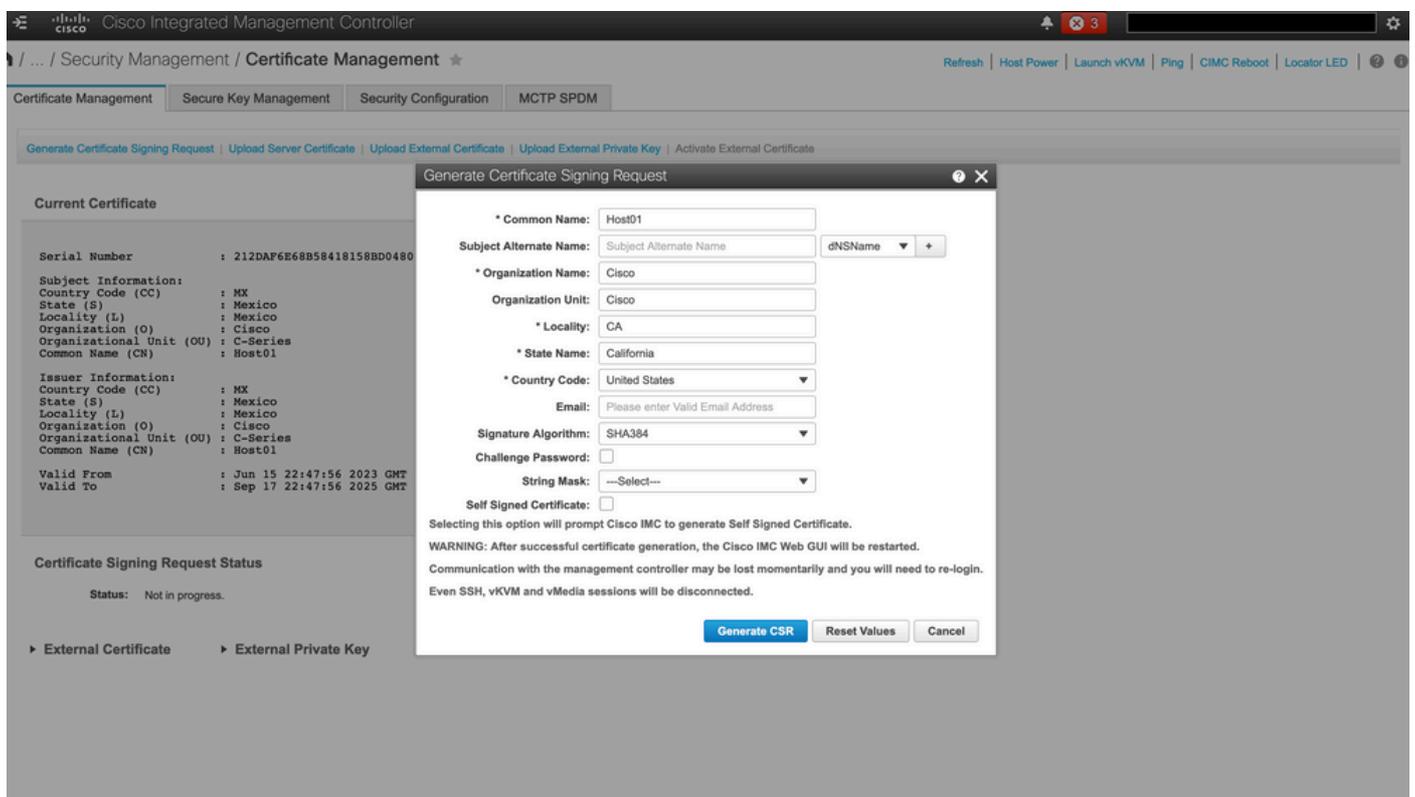
步骤1:	从CIMC生成CSR。
步骤 2	将CSR文件提交到CA以签署证书。如果您的组织生成自己的自签名证书，您可以使用CSR文件生成自签名证书。
第 3 步 :	将新证书上传到CIMC。

 注意：上传的证书必须从CIMC生成的CSR中创建。请勿上传不是由此方法创建的证书。

生成 CSR

导航到管理员选项卡> 安全管理 > 证书管理 > 生成证书签名请求 (CSR)并填写带有*标记的详细信息。

此外，请参阅[生成证书签名请求指南](#)。



The screenshot shows the Cisco Integrated Management Controller (IMC) interface for Certificate Management. The main window displays the 'Generate Certificate Signing Request' dialog box. The dialog box contains the following fields and options:

- * Common Name:** Host01
- Subject Alternate Name:** Subject Alternate Name (with a dropdown menu set to dNSName and a plus sign)
- * Organization Name:** Cisco
- Organization Unit:** Cisco
- * Locality:** CA
- * State Name:** California
- * Country Code:** United States (dropdown menu)
- Email:** Please enter Valid Email Address
- Signature Algorithm:** SHA384 (dropdown menu)
- Challenge Password:** (empty field)
- String Mask:** ---Select---
- Self Signed Certificate:** (checkbox, currently unchecked)

Below the fields, 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".

 注意：使用主题备用名可为此服务器指定其他主机名。不配置dNSName或者将其从上传的证书中排除，可能会导致浏览器阻止对思科IMC接口的访问。

下一步要做什么？

执行以下任务：

- 如果您不想从公共证书颁发机构获取证书，并且您的组织不运行自己的证书颁发机构，则可以允许CIMC从CSR内部生成自签名证书，并立即将其上传到服务器。选中Self Signed Certificate框以执行此任务。
- 如果您的组织运行自己的自签名证书，请将命令输出从-----BEGIN ... 复制到END CERTIFICATE REQUEST-----并粘贴到名为csr.txt的文件中。将CSR文件输入到证书服务器以生成自签名证书。
- 如果从公共证书颁发机构获取证书，请将-----BEGIN ... to END CERTIFICATE REQUEST-----的命令输出复制到名为csr.txt的文件中。将CSR文件提交到证书颁发机构以获取签名证书。确保证书类型为Server。

 注意：成功生成证书后，思科IMC Web GUI将重新启动。与管理控制器的通信可能会暂时中断，需要重新登录。

如果您没有使用第一个选项(在该选项中，CIMC在内部生成并上传自签名证书)，则必须创建新的自签名证书并将其上传到CIMC。

创建自签名证书

作为公共CA的替代方案并签署服务器证书，请运行您自己的CA并签署您自己的证书。本部分显示用于创建CA并使用OpenSSL服务器证书生成服务器证书的命令。有关OpenSSL的详细信息，请参阅[OpenSSL](#)。

步骤1:生成RSA私钥（如图所示）。

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

第二步：生成新的自签名证书，如图所示。

```
<#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 ~]#

第三步：确保证书类型为服务器，如图所示。

```
<#root>
```

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

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

第四步：指示CA使用您的CSR文件生成服务器证书，如图所示。

```
<#root>
```

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

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

第五步：验证生成的证书是否为Server类型（如图所示）。

<#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

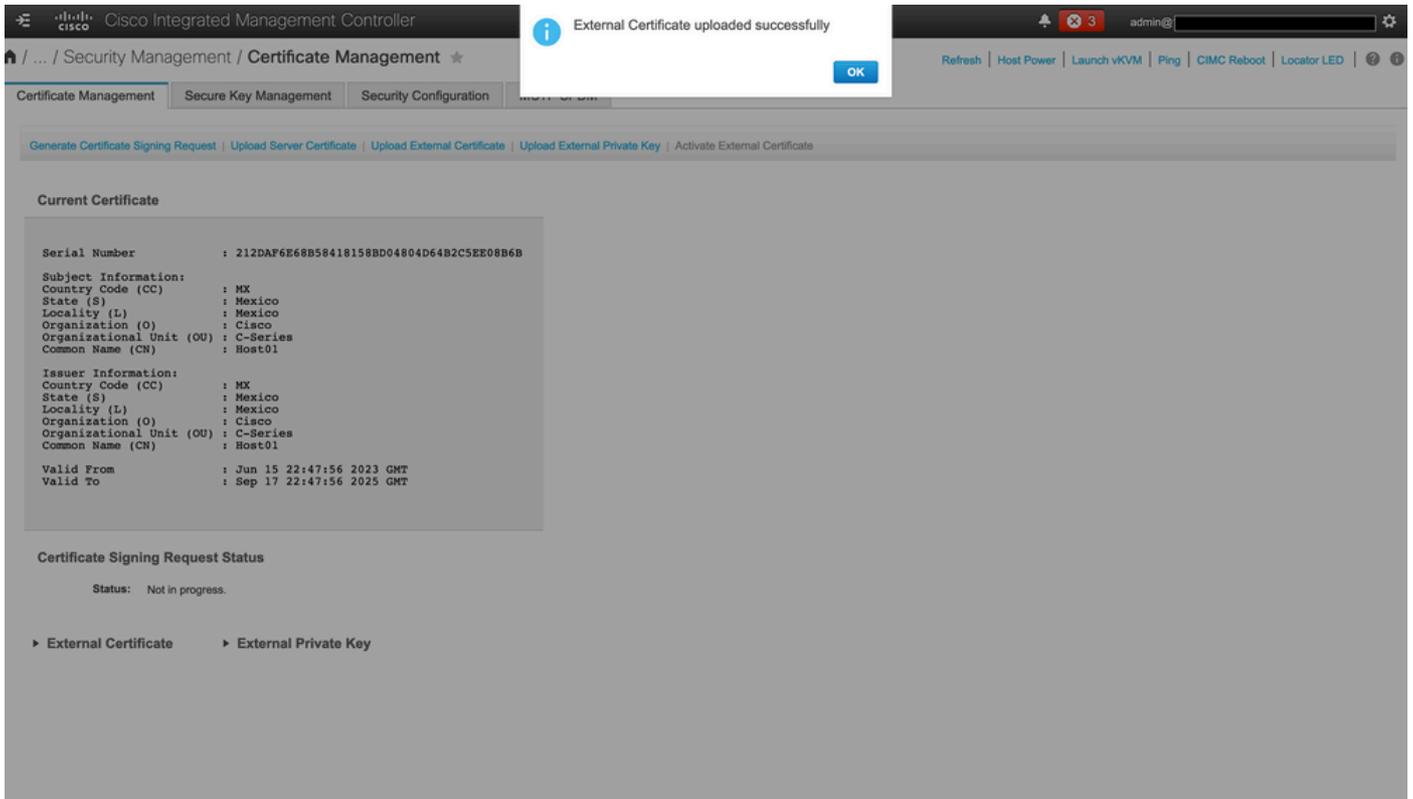
-----BEGIN CERTIFICATE-----

```
MIIDFzCCAoCgAwIBAgIBATANBgkqhkiG9w0BAQsFADBoMQswCQYDVQQGEwJVUzET
MBEGA1UECAwKQ2FsaWZvcn5pYTETMBEGA1UEBwwKQ2FsaWZvcn5pYTEOMAwGA1UE
CgwFQ2IzY28xDjAMBGNVBA5MBUNpc2NvMQ8wDQYDVQQDDAIZb3NOMDEwHhcNMjMw
NjI3MjI0NDU1WjBGMQswCQYDVQQGEwJVUzETMBEGA1UE
CAwKQ2FsaWZvcn5pYTELMakGA1UEBwwCQ0ExDjAMBGNVBAoMBUNpc2NvMQ4wDAYD
VQQLDAVDAxNjBzEPMAOGA1UEAwwGSG9zdDAxMIIBIjANBgkqhkiG9w0BAQEFAAOCC
AQ8AMIIBCgKCAQEAuhJ50V004MZNv3dgQw0Mns9sgzZwjJS8LvOtHt+GA4uzNf1Z
WKNyZbzD/yLoXiv8ZFgawJbqEe2yijVzEcguZQTGFRkAWmDecKM9Fieob03B5Fnt
pC8M9Dfb3YmkIx29abrZKFEIrybabbG4gQyFzgoB6D9CK1WuoEzsE7zH0oJX4Bcy
ISE0RsOd9bsXvxyLk2cauS/zvI9hvrwW9P/Og8nF3Y+PGtm/bnfodEnNFWPLtvF
dGuG5/wBmmMbEb/GbrH9uVcy0z+3HReDcQ+kJde7PoFK3d6Z0dkh7Mmtjpvk5ucQ
NgzaeoCDL0Bn+Zl0800/eciScsGIJKxYD/FYlQIDAQABo1UwUzARBglghkgBhvhC
AQEEBAMCBkAwHQYDVRO0BBYEFJ20TeuP27jyCJRiAKKfflNc0hbMB8GA1UdIwQY
MBaAFA4QR965FinE4GrhkiwRV62ziPj/MA0GCSqGSIb3DQEBwUAA4GBAJuL/Bej
DxenfCt6pBA709GtkltwUS/rEtpQX190hdlahjwbfG/67MYIpIEbidL1BCw55da1
LI7sgu1dnItnIGsJI1L7h6IEFBu/coCvBtopOYUanaBJ1BgxBWhT2FAnmB9wIvYJ
5rMx95vWZxt3KGE8Q1P+eGkmAHWA8M0yhwHa
```

-----END CERTIFICATE-----

[root@redhat ~]#

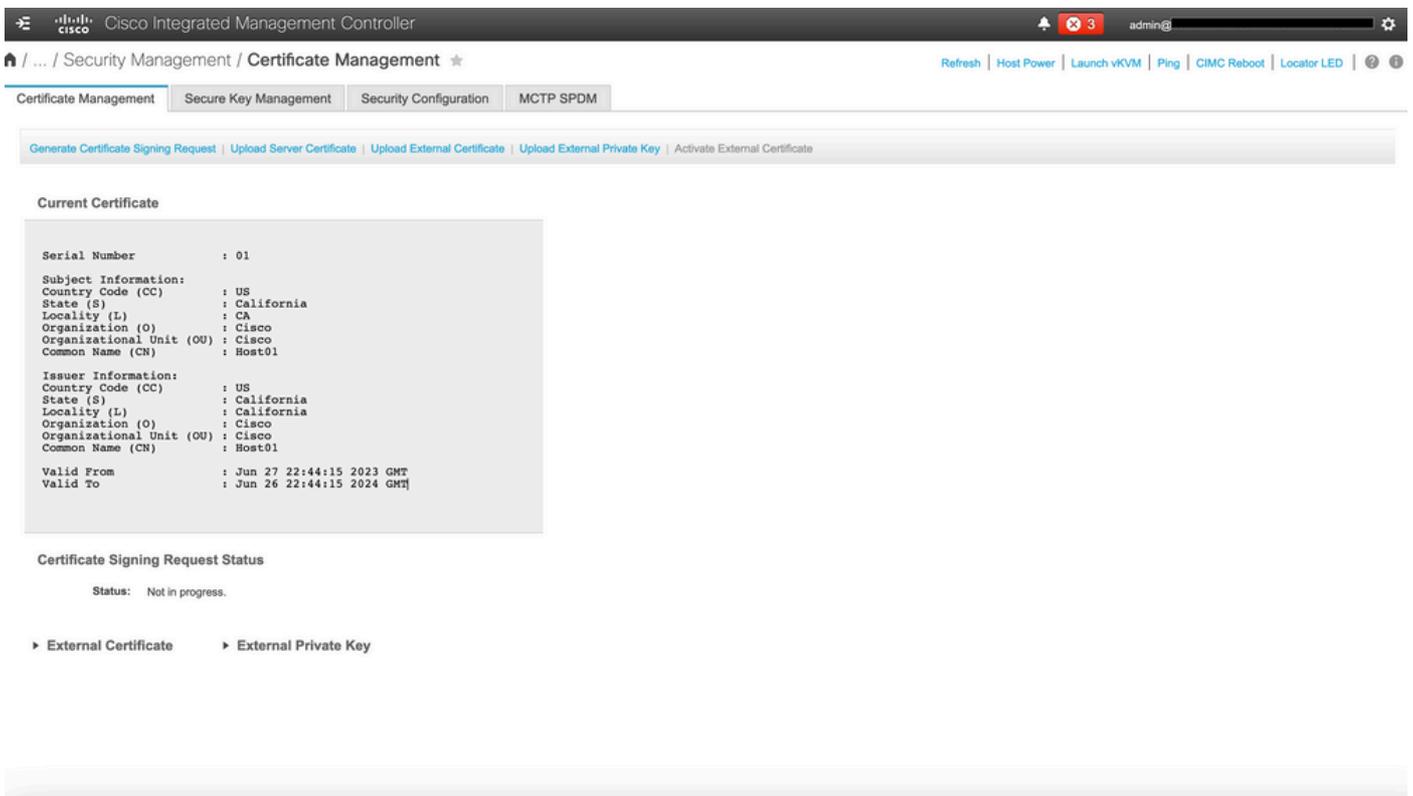
第六步：上传服务器证书（如图所示）。



验证

使用本部分可确认配置能否正常运行。

导航到管理>证书管理，验证当前证书（如图所示）。



故障排除

当前没有故障排除此配置的特定可用资料。

相关信息

- [思科漏洞ID CSCup26248](#) -无法将第三方CA SSL证书上传到CIMC 2.0。(1a)
- [技术支持和文档 - Cisco Systems](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。