CIMCへのUCSサーバ証明書の設定

内容

はじめに

このドキュメントでは、新しい証明書を取得するために証明書署名要求(CSR)を生成する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 証明書を設定するには、admin権限を持つユーザとしてログインする必要があります。
- CIMCの時刻が現在時刻に設定されていることを確認します。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CIMC 1.0以降
- OpenSSL

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

証明書をCisco Integrated Management Controller(CIMC)にアップロードして、現在のサーバ証明書を置き換えることができます。 サーバ証明書は、Verisignなどのパブリックな認証局(CA)または独自の認証局によって署名できます。生成される証明書キーの長さは2048ビットです。

設定

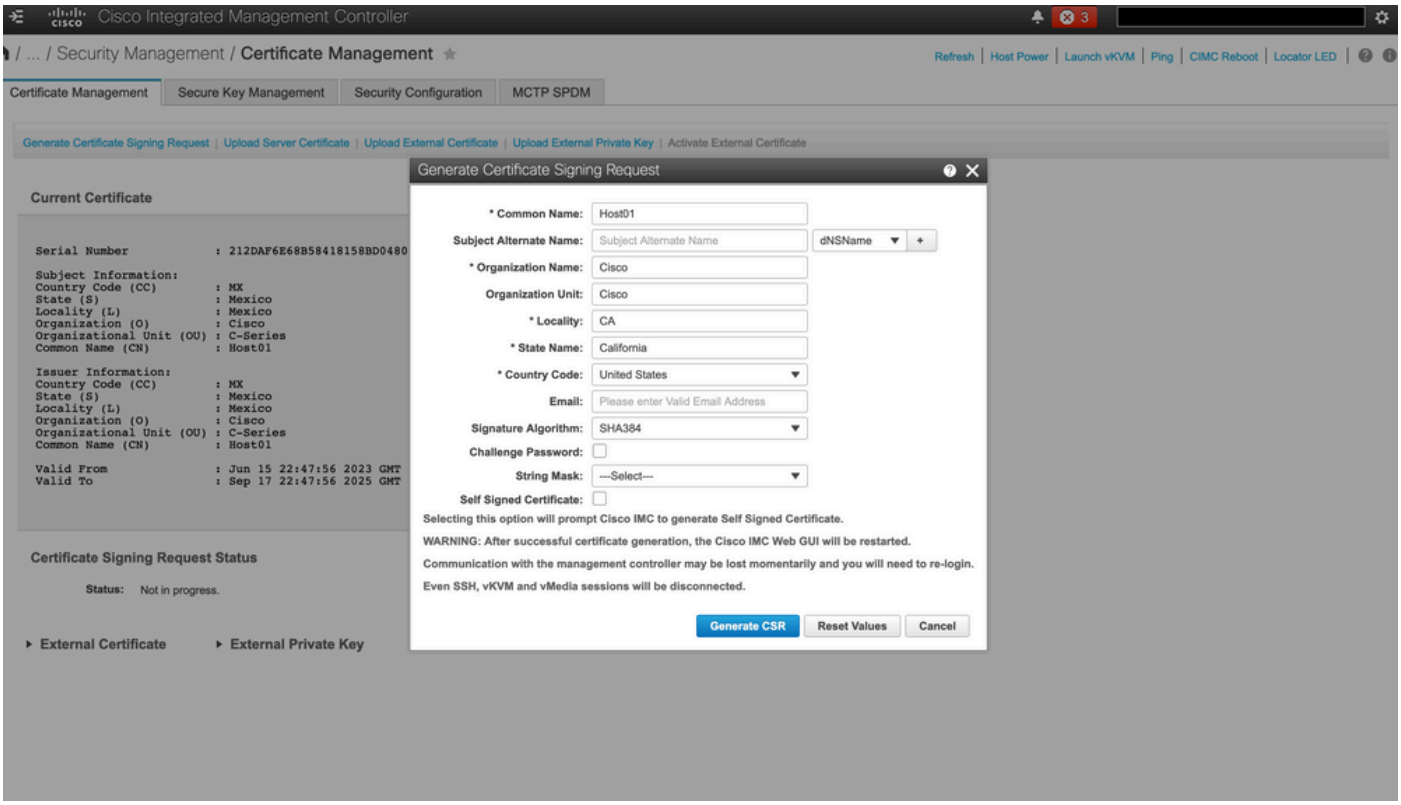
ステップ1：	CIMCからCSRを生成します。
ステップ2.	CSRファイルをCAに送信し、証明書に署名します。組織が独自の自己署名証明書を生成する場合は、CSRファイルを使用して自己署名証明書を生成できます。
手順3：	新しい証明書をCIMCにアップロードします。

注：アップロードする証明書は、CIMCによって生成されたCSRから作成する必要があります。この方法で作成されていない証明書はアップロードしないでください。

CSR の生成

Adminタブ> Security Management > Certificate Management > Generate Certificate Signing Request (CSR)の順に移動し、*でマークされた詳細情報を入力します。

また、「証明書署名要求の生成」も参照してください。



⚠ 注意:サブジェクトの別名を使用して、このサーバの追加のホスト名を指定してください。dNSNameを設定したり、アップロードされた証明書から除外したりすると、ブラウザがCisco IMCインターフェイスへのアクセスをブロックする可能性があります。

次の作業?

次のタスクを実行します。

- 公開されている認証局から証明書を取得する必要がなく、組織が独自の認証局を運用していない場合は、CSRから自己署名証明書を内部で生成し、即座にサーバにアップロードすることができます。このタスクを実行するには、Self Signed Certificateボックスにチェックマークを付けます。
- 組織が独自の自己署名証明書を運用している場合は、-----BEGIN ...からEND CERTIFICATE REQUESTへのコマンド出力をコピーし-----csr.txtという名前のファイルに貼り付けます。CSRファイルを証明書サーバに入力し、自己署名証明書を生成します。
- 公開されている認証局から証明書を取得する場合は、-----BEGIN ... to END CERTIFICATE REQUEST-----のコマンド出力をコピーし、csr.txtという名前のファイルに貼り付けます。署名付き証明書を取得するには、CSRファイルを認証局(CA)に送信します。証明書のタイプがサーバであることを確認します。

✎ 注：証明書が正常に生成されると、Cisco IMC Web GUIが再起動されます。管理コントローラとの通信が一時的に失われ、再ログインが必要になる場合があります。

CIMCが自己署名証明書を内部的に生成してアップロードする最初のオプションを使用しなかった

場合は、新しい自己署名証明書を作成してCIMCにアップロードする必要があります。

自己署名証明書の作成

パブリックCAの代わりにサーバー証明書に署名するには、独自のCAを使用して独自の証明書に署名します。このセクションでは、CAを作成し、OpenSSLサーバ証明書を使用してサーバ証明書を生成するコマンドを示します。OpenSSLの詳細については、「OpenSSL」を参照してください。

ステップ 1：図に示すように、RSA秘密キーを生成します。

<#root>

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

openssl genrsa -out ca.key 1024

ステップ 2：図に示すように、新しい自己署名証明書を生成します。

<#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 ~]#
```

ステップ 3：図に示すように、証明書タイプがサーバであることを確認します。

```
<#root>

[root@redhat ~]#

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

ステップ 4：図に示すように、CSRファイルを使用してサーバ証明書を生成するようにCAに指示します。

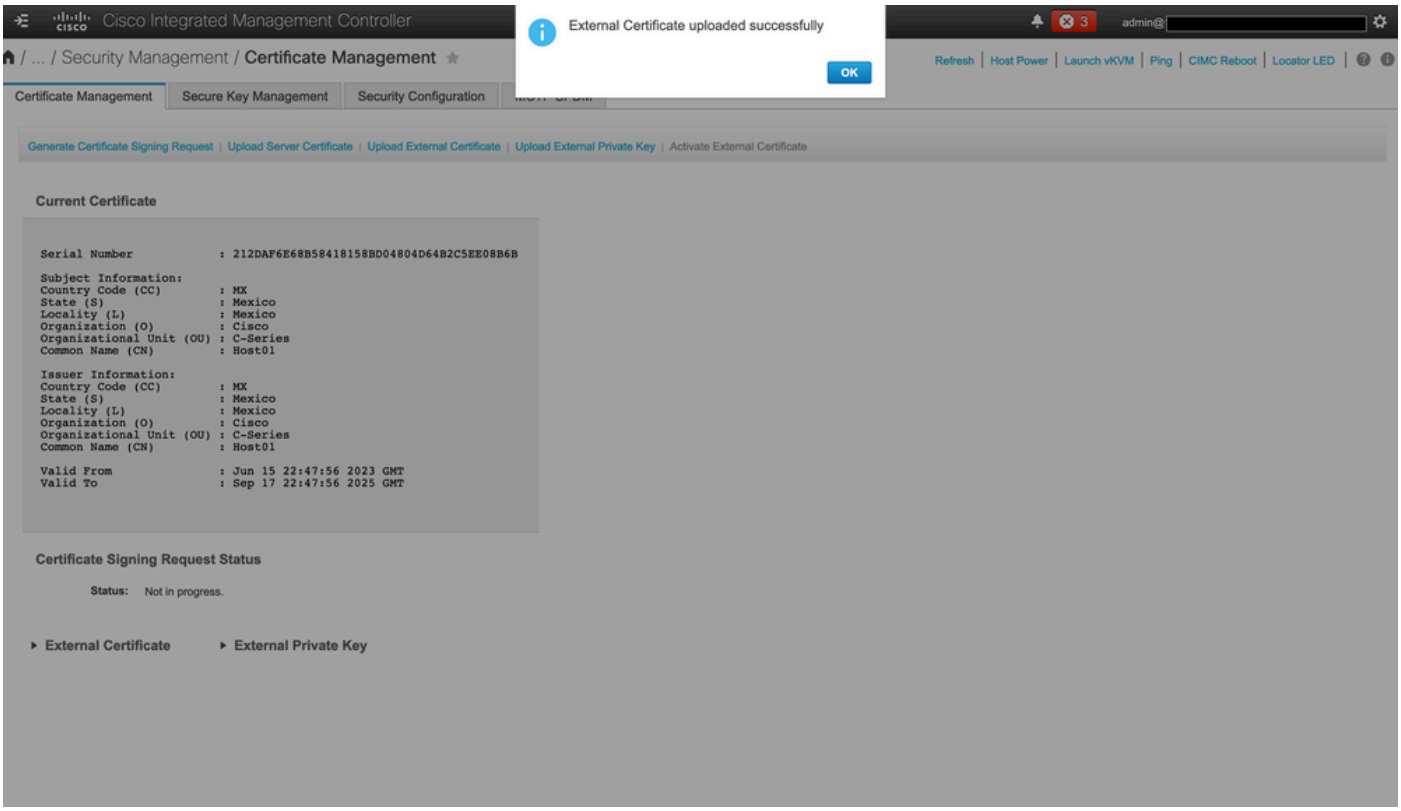
```
<#root>

[root@redhat ~]#

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

ステップ 5：図に示すように、生成された証明書がサーバタイプであるかどうかを確認します。

```
<#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
pC8M9Dfb3YMkIx29abrZKFEIrYbabbG4gQyfzgOB6D9CK1WuoezsE7zH0oJX4Bcy
ISE0RsOd9bsXvxyLk2cauS/zvI9hvrWW9P/Og8nF3Y+PGtm/bnfodEnNWFWPLtvF
dGuG5/wBmmMbEb/GbrH9uVcyOz+3HReDcQ+kJde7PoFK3d6ZOdkh7Mmtjpvk5ucQ
NgzaeoCDL0Bn+Zl0800/eciSCsGIJKxYD/FYlQIDAQABo1UwUzARBglghkgBhvhC
AQEEBAMCBkAwHQYDVR0OBBYEFEJ2OTeuP27jyCJRiAKKfflNcOhbMB8GA1UdIwQY
MBaAFA4QR965FinE4GrhkiwRV62ziPj/MA0GCSqGSIb3DQEBCwUAA4GBAJuL/Bej
DxenfCt6pBA7O9GtkltWUS/rEtpQX19Ohdlahjwbf G/67MYIpIEbidL1BCw55dal
LI7sgu1dnItnIGsJIlL7h6IeFBu/coCvBtopOYUanaBJ1BgxBWhT2FAnmB9wIvYJ
5rMx95vWZXt3KGE8QlP+eGkmAHWA8M0yhwHa
-----END CERTIFICATE-----
[root@redhat ~]#
```

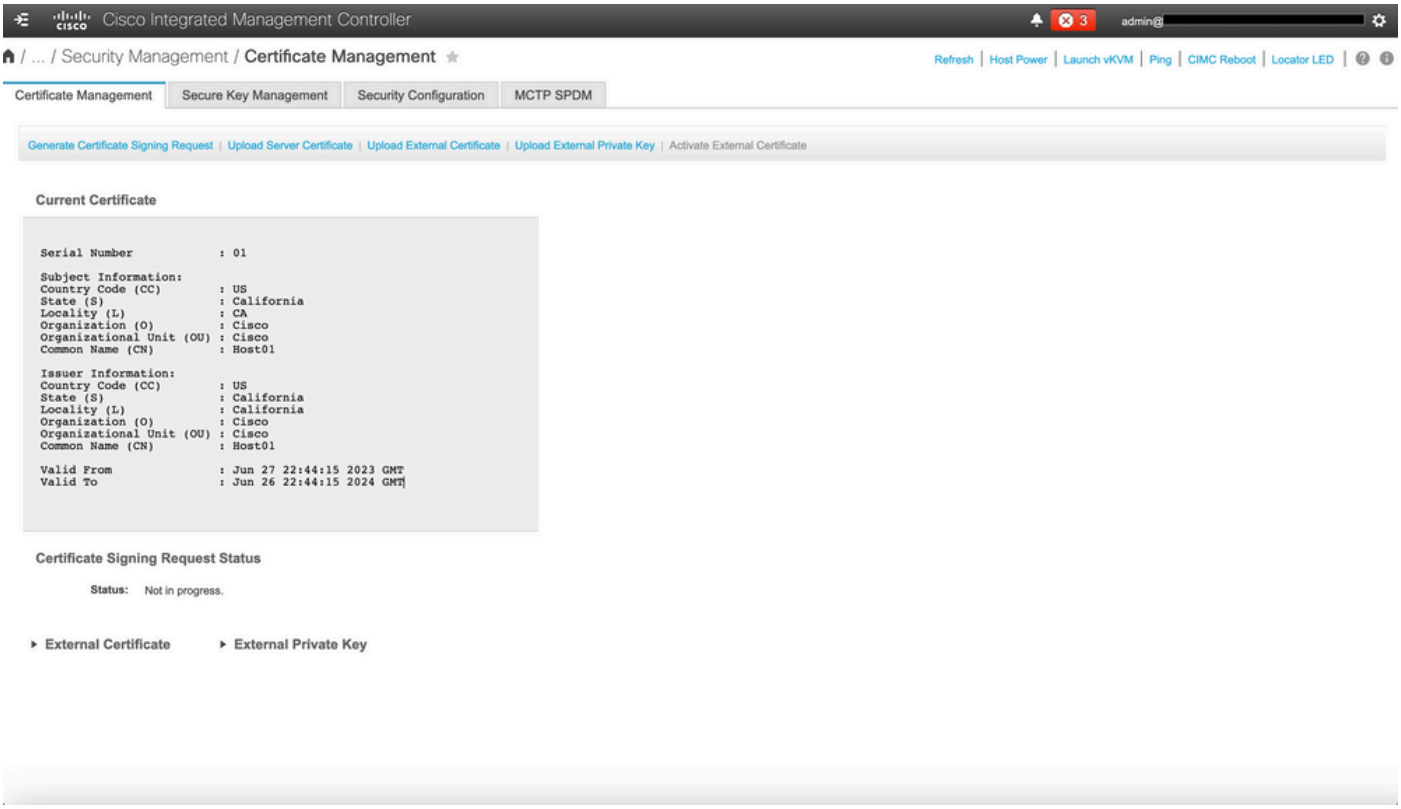
手順 6：図に示すように、サーバ証明書をアップロードします。



確認

ここでは、設定が正常に機能しているかどうかを確認します。

Admin > Certificate Managementの順に移動し、図に示すようにCurrent Certificateを確認します。



トラブルシュート

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco Bug ID CSCup26248：サードパーティのCA SSL証明書をCIMC 2.0.(1a)にアップロードできない
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。