CIMC에 UCS 서버 인증서 구성

목차

소개

이 문서에서는 새 인증서를 가져오기 위해 CSR(Certificate Signing Request)을 생성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 인증서를 구성하려면 관리자 권한이 있는 사용자로 로그인해야 합니다.
- CIMC 시간이 현재 시간으로 설정되어 있는지 확인합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CIMC 1.0 이상
- Openssl

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

현재 서버 인증서를 대체하기 위해 CIMC(Cisco Integrated Management Controller)에 인증서를 업로드할 수 있습니다. 서버 인증서는 Verisign과 같은 공용 CA(Certificate Authority)에서 서명하거나 자체 인증 기관에서 서명할 수 있습니다. 생성된 인증서 키 길이는 2048비트입니다.

구성

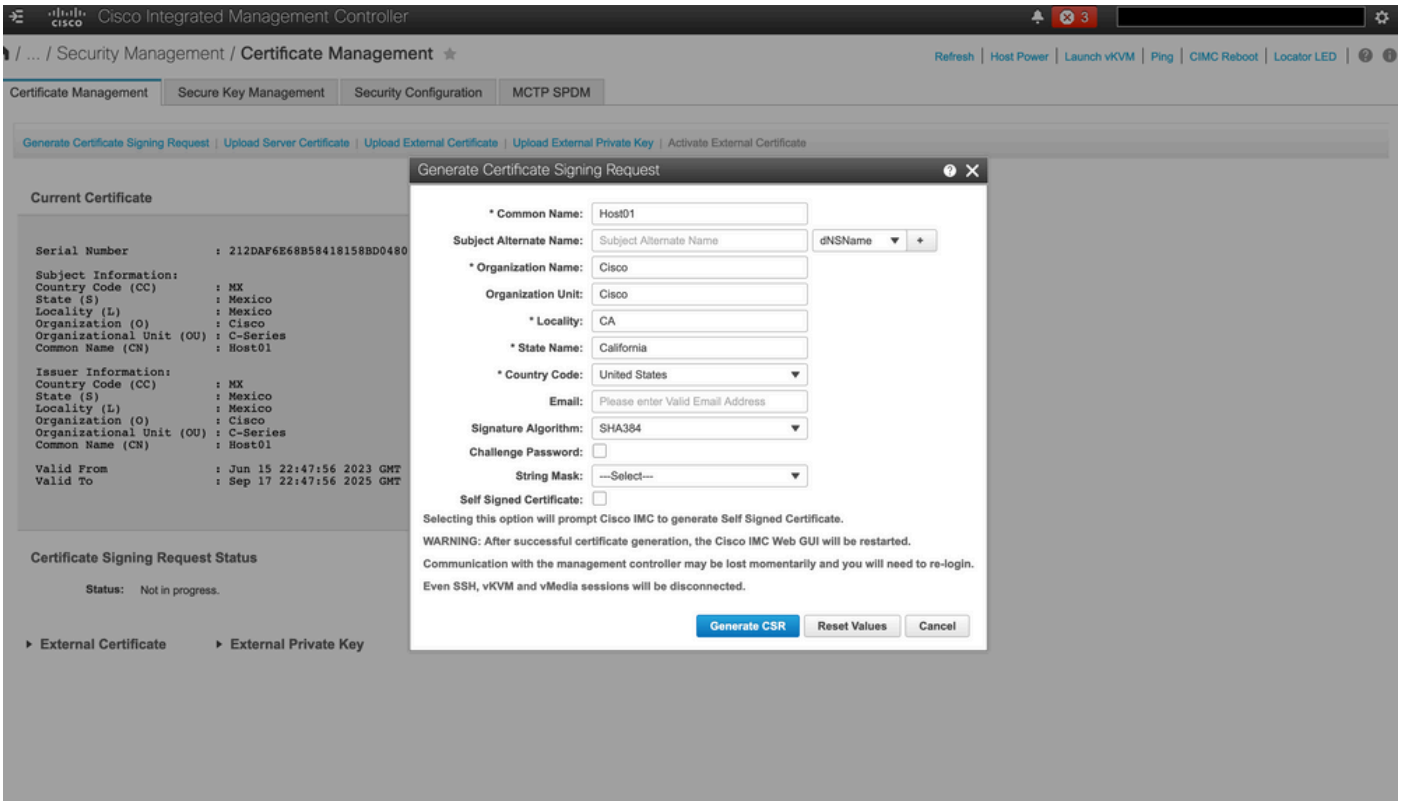
1단계.	CIMC에서 CSR을 생성합니다.
2단계.	CSR 파일을 CA에 제출하여 인증서를 서명합니다. 조직에서 자체 서명 인증서를 생성하는 경우 CSR 파일을 사용하여 자체 서명 인증서를 생성할 수 있습니다.
3단계.	CIMC에 새 인증서를 업로드합니다.

참고: 업로드된 인증서는 CIMC에서 생성한 CSR에서 생성해야 합니다. 이 방법으로 만들지 않은 인증서는 업로드하지 마십시오.

CSR 생성

Admin(관리) 탭 > Security Management(보안 관리) > Certificate Management(인증서 관리) > Generate Certificate Signing Request(CSR)(CSR(Certificate Signing Request))로 이동하여 *로 표시된 세부사항을 입력합니다.

또한 Generating a Certificate Signing Request(인증서 서명 요청 생성)를 참조하십시오.



⚠ 주의: Subject Alternate Name(주체 대체 이름)을 사용하여 이 서버에 대한 추가 호스트 이름을 지정합니다. dNSName을 구성하지 않거나 업로드된 인증서에서 제외하면 브라우저에서 Cisco IMC 인터페이스에 대한 액세스를 차단할 수 있습니다.

다음 작업

다음 작업을 수행합니다.

- 공용 인증 기관으로부터 인증서를 취득하지 않으려는 경우, 그리고 조직에서 자체 인증 기관을 운영하지 않는 경우, CIMC가 내부적으로 CSR로부터 자체 서명 인증서를 생성하고 이를 서버에 즉시 업로드하도록 허용할 수 있습니다. 이 작업을 수행하려면 자체 서명 인증서 확인란을 선택합니다.
- 조직에서 자체 서명 인증서를 운영하는 경우 -----BEGIN ...에서 END CERTIFICATE REQUEST-----으로 명령 출력을 복사하고 csr.txt라는 파일에 붙여넣습니다. 자체 서명 인증서를 생성하려면 인증서 서버에 CSR 파일을 입력합니다.
- 공용 인증 기관에서 인증서를 가져오는 경우 -----BEGIN ... 의 명령 출력을 END CERTIFICATE REQUEST-----으로 복사하고 csr.txt라는 파일에 붙여넣습니다. CSR 파일을 인증 기관에 제출하여 서명된 인증서를 얻습니다. 인증서가 서버 유형인지 확인합니다.

✎ 참고: 인증서를 성공적으로 생성하면 Cisco IMC 웹 GUI가 다시 시작됩니다. 관리 컨트롤러와의 통신이 잠시 중단될 수 있으며 다시 로그인해야 합니다.

CIMC가 내부적으로 자체 서명 인증서를 생성하고 업로드하는 첫 번째 옵션을 사용하지 않은 경우, 새 자체 서명 인증서를 생성하여 CIMC에 업로드해야 합니다.

자체 서명 인증서 생성

공용 CA 대신 서버 인증서를 서명하고 고유한 CA를 운영하고 고유한 인증서를 서명합니다. 이 섹션에서는 CA를 생성하고 OpenSSL 서버 인증서를 사용하여 서버 인증서를 생성하는 명령을 보여줍니다. OpenSSL에 대한 자세한 내용은 OpenSSL을 참조하십시오.

1단계. 이미지에 표시된 대로 RSA 개인 키를 생성합니다.

<#root>

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

openssl genrsa -out ca.key 1024

2단계. 이미지에 표시된 대로 새 자체 서명 인증서를 생성합니다.

<#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 ~]#
```

3단계. 이미지에 표시된 대로 인증서 유형이 서버인지 확인합니다.

<#root>

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

echo "nsCertType = server" > openssl.conf

4단계. 이미지에 표시된 대로 CSR 파일을 사용하여 서버 인증서를 생성하도록 CA에 지시합니다.

<#root>

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

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

5단계. 생성된 인증서가 이미지에 표시된 것처럼 Server 유형인지 확인합니다.

<#root>

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

openssl x509 -in server.crt -purpose

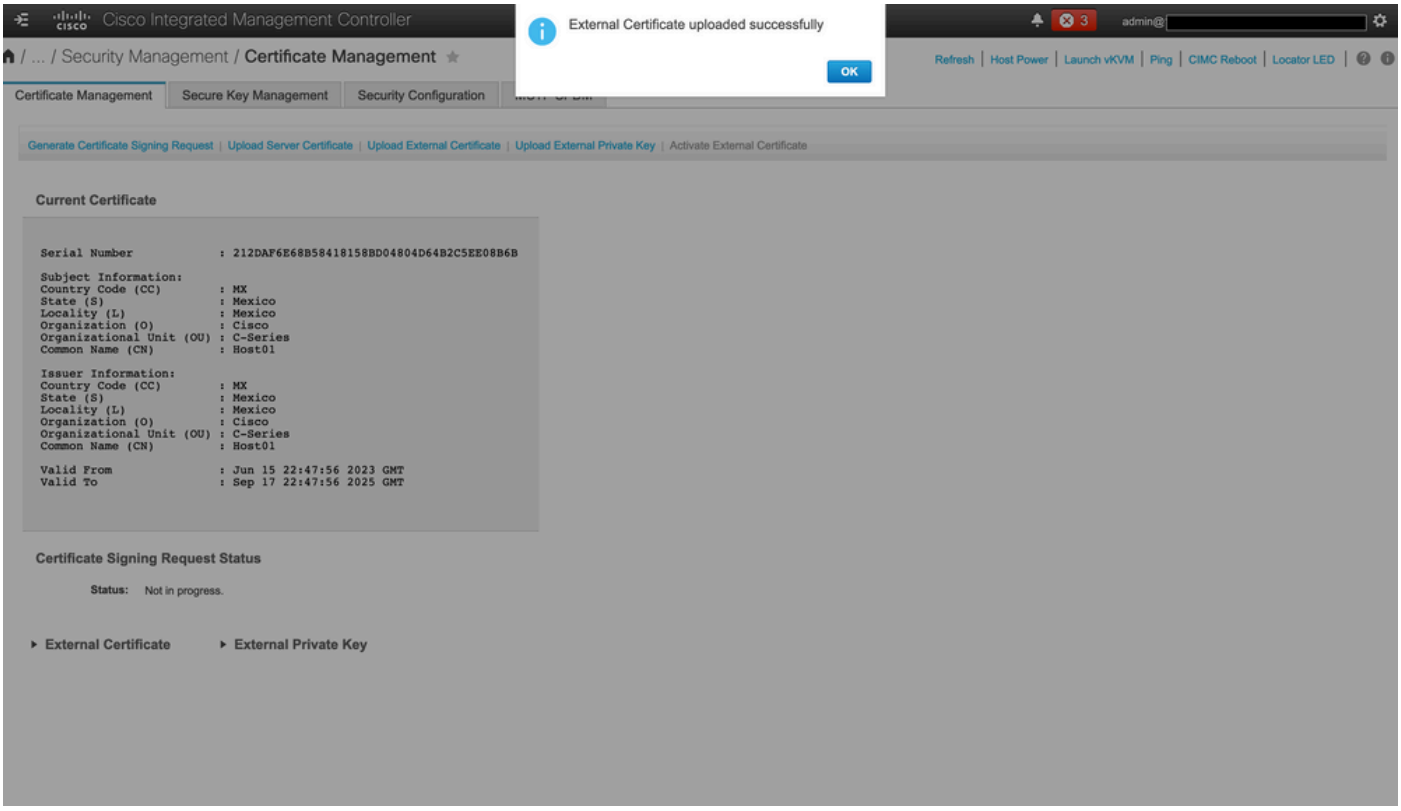
```
Certificate purposes:
SSL client : No
SSL client CA : No
SSL server :
```

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
NgzaeoCDLOBn+Zl0800/eciSCsGIJKxYD/FYlQIDAQABo1UwUzARBglghkgBhvhC
AQEEBAMCBkAwHQYDVR0OBBYEFEJ2OTeuP27jyCJRiAKKfflNcOhbMB8GA1UdIwQY
MBaAFA4QR965FinE4GrhkiwRV62ziPj/MA0GCSqGSIb3DQEBCwUAA4GBAJuL/Bej
DxenfCt6pBA7O9GtkltWUS/rEtpQX190hdlahjwbfG/67MYIpIEbidL1BCw55dal
LI7sgu1dnItnIGsJIlL7h6IeFBu/coCvBtopOYUanaBJ1BgxBWhT2FAnmB9wIvYJ
5rMx95vWZXt3KGE8QlP+eGkmAHWA8M0yhwHa
-----END CERTIFICATE-----
[root@redhat ~]#
```

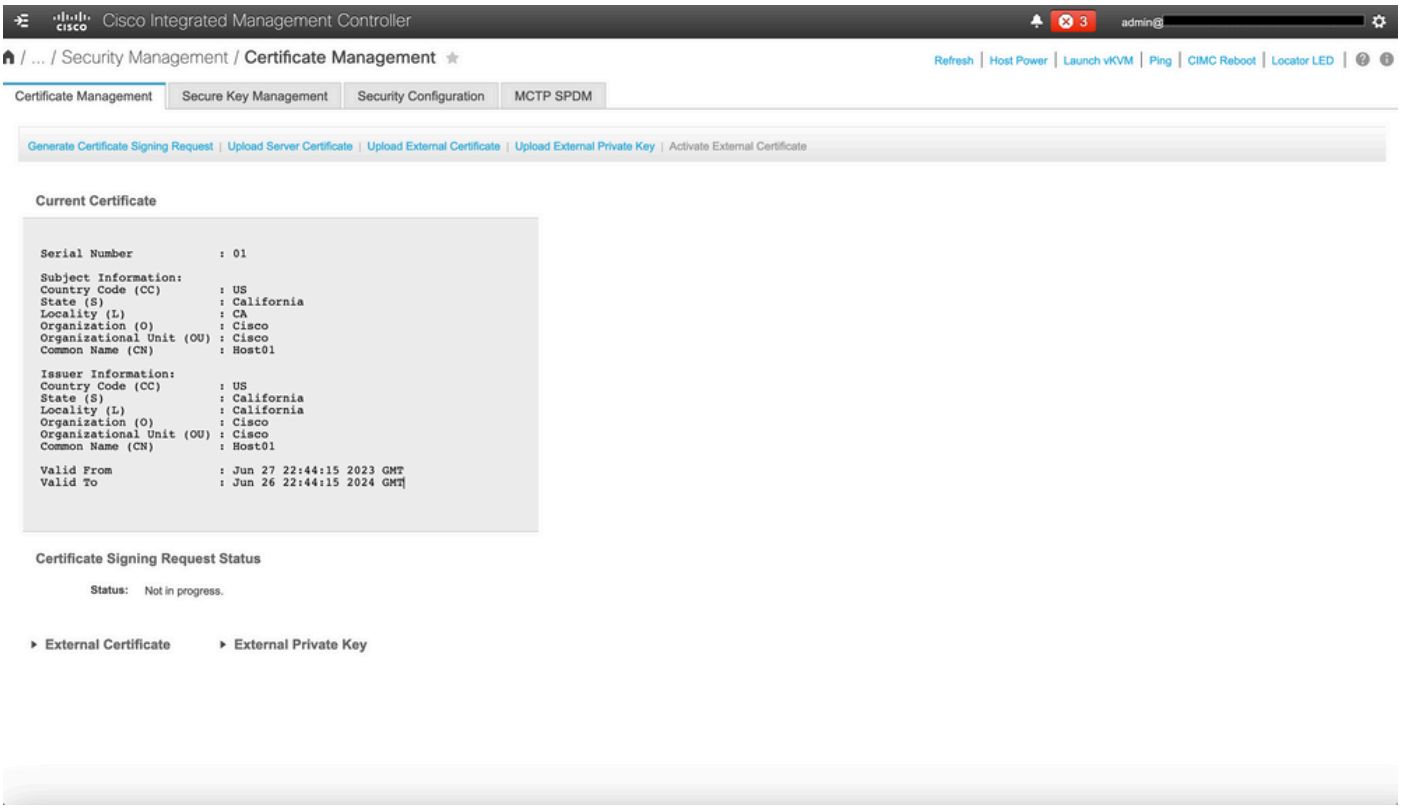
6단계. 그림과 같이 서버 인증서를 업로드합니다.



다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

Admin(관리) > Certificate Management(인증서 관리)로 이동하고 이미지에 표시된 대로 현재 인증서를 확인합니다.



문제 해결

현재 이 구성의 문제를 해결하는 데 사용할 수 있는 특정 정보가 없습니다.

관련 정보

- Cisco 버그 ID CSCup26248 - 서드파티 CA SSL 인증서를 CIMC 2.0에 업로드할 수 없습니다 .(1a)
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.