



## 証明書の管理

---

この章は、次の項で構成されています。

- [サーバ証明書の管理](#) (1 ページ)
- [証明書署名要求の生成](#) (1 ページ)
- [自己署名証明書の作成](#) (3 ページ)
- [サーバ証明書のアップロード](#) (5 ページ)

## サーバ証明書の管理

証明書署名要求 (CSR) を生成して新しい証明書を取得し、新しい証明書を CIMC にアップロードして現在のサーバ証明書と交換することができます。サーバ証明書は、Verisign のようなパブリック認証局 (CA)、または独自に使用している認証局のいずれかによって署名されます。

---

**ステップ1** CIMC から CSR を生成します。

**ステップ2** 証明書の発行と署名を行う認証局に CSR ファイルを送信します。組織で独自の自己署名証明書を生成している場合は、CSR ファイルを使用して自己署名証明書を生成できます。

**ステップ3** 新しい証明書を CIMC にアップロードします。

(注) アップロードされた証明書は、CIMC によって生成された CSR から作成される必要があります。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。

---

## 証明書署名要求の生成

始める前に

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。

## 手順の概要

1. Server# **scope certificate**
2. Server /certificate # **generate-csr**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope certificate</b>	証明書コマンドモードを開始します。
ステップ 2	Server /certificate # <b>generate-csr</b>	証明書署名要求 (CSR) の生成に関するダイアログを起動します。

証明書署名要求に関して、次の情報の入力を求めるプロンプトが表示されます。

Common Name (CN)	CIMC の完全修飾ホスト名
Organization Name (O)	証明書を要求している組織。
Organization Unit (OU)	組織ユニット
Locality (L)	証明書を要求している会社の本社が存在する市または町。
StateName (S)	証明書を要求している会社の本社が存在する州または行政区分。
Country Code (CC)	会社の本社が存在する国を示す 2 文字の ISO 国コード。
Email	会社の管理用電子メールの連絡先。

要求された情報を入力すると、証明書署名要求が生成され、コンソール出力に表示されます。CSR ファイルは作成されませんが、コンソール出力から CSR 情報をコピーして、テキストファイルに貼り付けることができます。

## 例

次に、証明書署名要求を生成する例を示します。

```
Server# scope certificate
Server /certificate # generate-csr
Common Name (CN): test.example.com
Organization Name (O): Example, Inc.
Organization Unit (OU): Test Department
Locality (L): San Jose
StateName (S): CA
Country Code (CC): US
Email: user@example.com
Continue to generate CSR?[y|N]y

-----BEGIN CERTIFICATE REQUEST-----
MIIB/zCCAQAwgZkxCzAJBgNVBAYTAlVMTQswCQYDVQQLIEwJJDQTEVMBGAlUE
```

```
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGx1IEluYy4xEzARBgNVBAst
ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBkgkqhkig
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivYCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAGMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzCl90306Mg51zqlzXcz75+VFj2I6rH9asckClD3mkOVx5gJU
Ptt5CVQpNgNLdvdDPSSXretysOhqHmp9+CLv8FDuy1CDYfuaLtv1WvfhevsKv0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE REQUEST-----
```

Copy everything from "-----BEGIN ..." to "END CERTIFICATE REQUEST-----",  
paste to a file, send to your chosen CA for signing,  
and finally upload the signed certificate via upload command.

---OR---

Continue to self sign CSR and overwrite the current certificate?  
All HTTPS and SSH sessions will be disconnected. [y|N]N

## 次のタスク

次のいずれかの作業を実行します。

- 公共の認証局から証明書を取得したくない場合に、組織が独自の認証局を運用していなければ、CSR から自己署名証明書を内部生成し、すぐにサーバにアップロードするよう、CIMC を設定できます。この処理を行うには、この例では最後のプロンプトの後に **y** と入力します。
- 組織が自己署名証明書を生成するための独自の証明書サーバを運用している場合は、「-----BEGIN ...」から「END CERTIFICATE REQUEST-----」までのコマンド出力をコピーして、`csr.txt` という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て、自己署名証明書を生成します。
- 公共の認証局から証明書を取得する場合は、「-----BEGIN ...」から「END CERTIFICATE REQUEST-----」までのコマンド出力をコピーして、`csr.txt` というファイルに貼り付けます。CSR ファイルを認証局に提出して、署名付き証明書を取得します。

CIMC によって自己署名証明書を内部生成し、アップロードする最初のオプションを使用しない場合は、証明書コマンドモードで **upload** コマンドを使用して新しい証明書を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

パブリック認証局 (CA) を使用してサーバ証明書の生成と署名を行う代わりに、独自の CA を運用して独自の証明書に署名することができます。このセクションでは、Linux で実行されている OpenSSL 証明書サーバを使用して CA を作成するコマンドおよびサーバ証明書を生成するコマンドについて説明します。OpenSSL の詳細については、<http://www.openssl.org> を参照してください。



(注) これらのコマンドは、CIMC CLIではなく、OpenSSL パッケージを使用している Linux サーバで入力します。

### 始める前に

組織内のサーバで、証明書サーバのソフトウェアパッケージを取得してインストールします。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>openssl genrsa -out CA_keyfilename keysize</b> 例： <pre># openssl genrsa -out ca.key 1024</pre>	このコマンドは、CA で使用される RSA 秘密キーを生成します。 (注) ユーザ入力なしでCAがキーにアクセスできるように、このコマンドに <b>-des3</b> オプションは使用しないでください。 指定されたファイル名には、指定されたサイズの RSA キーが含まれています。
ステップ 2	<b>openssl req -new -x509 -days numdays -key CA_keyfilename -out CA_certfilename</b> 例： <pre># openssl req -new -x509 -days 365 -key ca.key -out ca.crt</pre>	このコマンドは、指定されたキーを使用して、CA の自己署名証明書を新規に作成します。証明書は指定された期間有効になります。このコマンドは、ユーザに証明書の追加情報を求めるプロンプトを表示します。 証明書サーバは、アクティブな CA です。
ステップ 3	<b>echo "nsCertType = server" &gt; openssl.conf</b> 例： <pre># echo "nsCertType = server" &gt; openssl.conf</pre>	このコマンドは、証明書がサーバ限定の証明書であることを指定する行を OpenSSL 設定ファイルに追加します。この指定により、認証されたクライアントがサーバになりすます man-in-the-middle 攻撃を防御できます。 OpenSSL 設定ファイル openssl.conf には、"nsCertType = server" という文が含まれています。
ステップ 4	<b>openssl x509 -req -days numdays -in CSR_filename -CA CA_certfilename -set_serial 04 -CAkey CA_keyfilename -out server_certfilename -extfile openssl.conf</b> 例： <pre># openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf</pre>	このコマンドは、CA が CSR ファイルを使用してサーバ証明書を生成するように指示します。 サーバ証明書は、出力ファイルに含まれています。

## 例

この例は、CAの作成方法、および新規に作成されたCAが署名するサーバ証明書の生成方法を示します。これらのコマンドは、OpenSSLを実行しているLinuxサーバで入力します。

```
# /usr/bin/openssl genrsa -out ca.key 1024 Generating RSA private key, 1024
bit long modulus .....+++++ .....+++++ e is 65537 (0x10001) #
/usr/bin/openssl req -new -x509 -days 365 -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) [GB]:US State or Province Name (full
name) [Berkshire]:California Locality Name (eg, city) [Newbury]:San Jose
Organization Name (eg, company) [My Company Ltd]:Example Incorporated
Organizational Unit Name (eg, section) []:Unit A Common Name (eg, your name or
your server's hostname) []:example.com Email Address []:admin@example.com #
echo "nsCertType = server" > openssl.conf # /usr/bin/openssl x509 -req -days
365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt -extfile
openssl.conf Signature ok subject=/C=US/ST=California/L=San Jose/O=Example
Inc./OU=Unit A/CN=example.com/emailAddress=john@example.com Getting CA Private
Key #
```

## 次のタスク

新しい証明書を CIMC にアップロードします。

# サーバ証明書のアップロード

## 始める前に

証明書をアップロードするには、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。

アップロードする証明書は、読み取り可能テキストとして使用できる必要があります。アップロード手順で、証明書テキストをコピーして CLI に貼り付けます。



- 
- (注) 最初に、CIMC 証明書管理 CSR の生成手順を使用して CSR を生成し、その CSR を使用してアップロード用の証明書を取得する必要があります。この方法で取得されていない証明書はアップロードしないでください。
- 



- 
- (注) 新しいサーバ証明書がアップロードされると、現在の HTTPS および SSH セッションはすべて切断されます。
-

