証明書の管理

この章は、次の内容で構成されています。

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 Certificate Authority（CA; 認証局）、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。

手順

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

はじめる前に

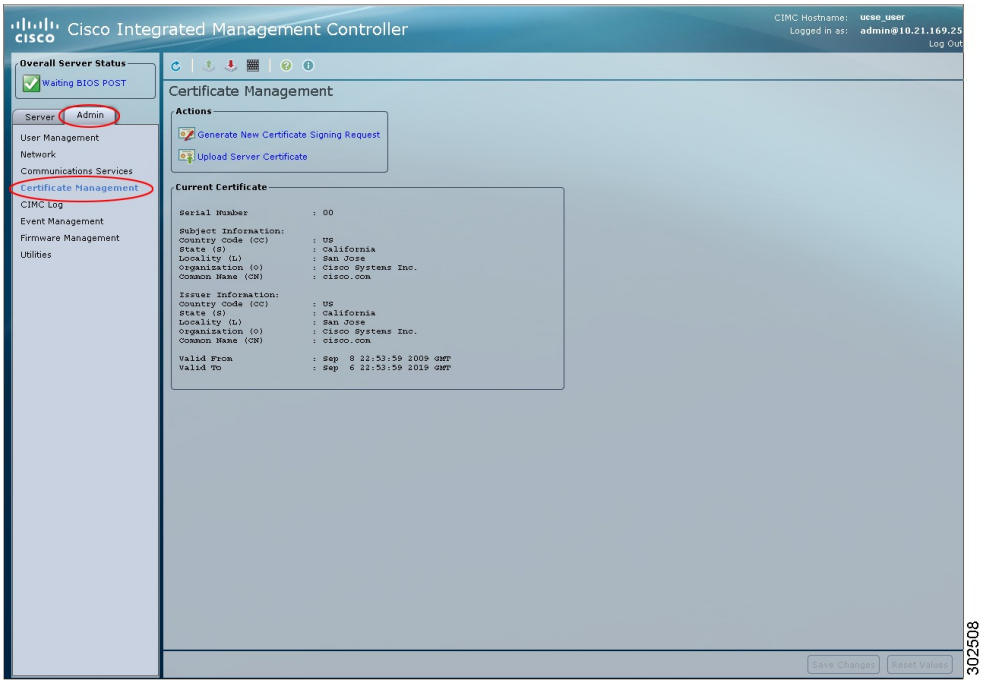
証明書を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Certificate Management] をクリックします。

図 *1*：*Certificate Management*



ステップ 3 [Actions] 領域で、[Generate New Certificate Signing Request] リンクをクリックします。
[Generate New Certificate Signing Request] ダイアログボックスが表示されます。

ステップ 4 [Generate New Certificate Signing Request] ダイアログボックスで、次のプロパティを更新します。

名前	説明
[Common Name] フィールド	CIMC の完全修飾ホスト名
[Organization Name] フィールド	証明書を要求している組織。
[Organization Unit] フィールド	組織ユニット

名前	説明
[Locality] フィールド	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。
[State Name] フィールド	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] ドロップダウンリスト	会社が存在する国。
[Email] フィールド	会社の電子メールによる連絡先。

ステップ 5 [Generate CSR] をクリックします。
[Opening csr.txt] ダイアログボックスが表示されます。

ステップ 6 CSR ファイル csr.txt を管理するには、次のいずれかの手順を実行します。

a) [Open With] をクリックして csr.txt を表示します。

b) [Save File] をクリックしてから [OK] をクリックし、ローカル マシンに csr.txt を保存します。

次の作業

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。

自己署名証明書の作成

パブリック Certificate Authority（CA; 認証局）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。

はじめる前に

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	**openssl genrsa -out** *CA_keyfilename keysize* 例： `# openssl genrsa -out ca.key 1024`	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 -des3 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	**openssl req -new -x509 -days** *numdays* **-key** *CA_keyfilename* **-out** *CA_certfilename* 例： `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	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	**echo "nsCertType = server" > openssl.conf** 例： `# echo "nsCertType = server" > openssl.conf`	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	**openssl x509 -req -days** *numdays* **-in** *CSR_filename* **-CA** *CA_certfilename* **-set_serial 04 -CAkey** *CA_keyfilename* **-out** *server_certfilename* **-extfile openssl.conf**
	
	例：
	`# openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04`
	`-CAkey ca.key -out myserver05.crt -extfile openssl.conf`
		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。

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
#
```

次の作業

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

はじめる前に

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ファイルは、ローカルにアクセスできるファイル システムに配置されている必要があります。

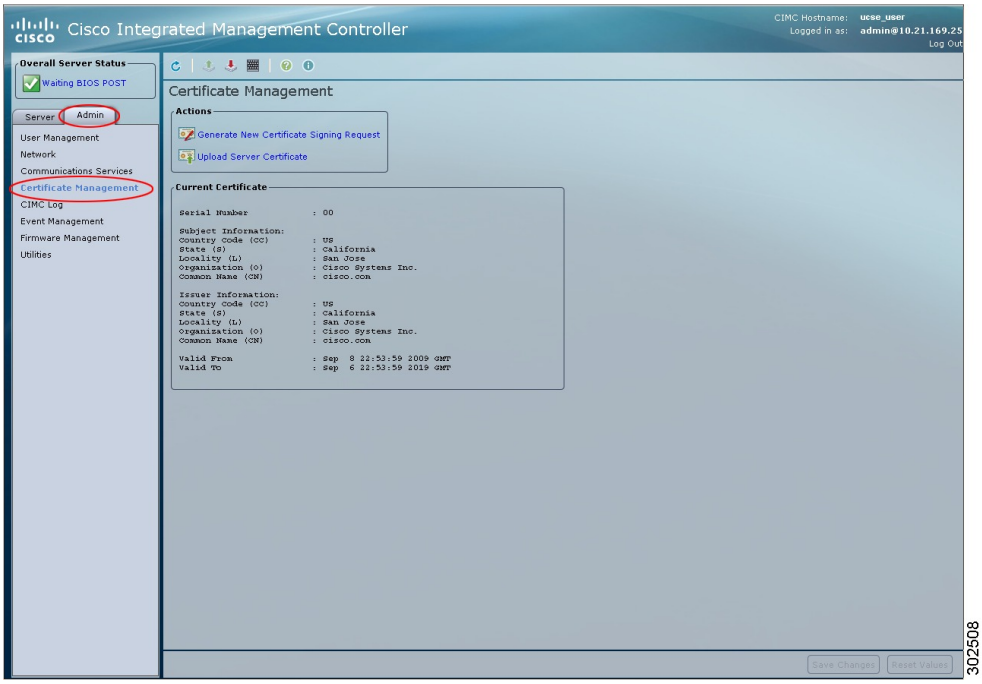
（注） [CIMC Certificate Management] メニューを使用して最初に CSR を生成してから、その CSR を使用してアップロードする証明書を取得する必要があります。 この方法で取得されていない証明書はアップロードしないでください。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Certificate Management] をクリックします。

図 2：***Certificate Management***



ステップ 3 [Actions] 領域で、[Upload Server Certificate] をクリックします。
[Upload Certificate] ダイアログボックスが表示されます。

ステップ 4 [Upload Certificate] ダイアログボックスで、次のプロパティを更新します。

名前	説明
[File] フィールド	アップロードする証明書ファイル。
[Browse] ボタン	適切な証明書ファイルに移動できるダイアログボックスが表示されます。 **注意** [Browse] ボタンを使用して証明書ファイルを選択した後は、キーボードの Backspace ボタンを使用して証明書ファイル名を編集しないでください。 編集すると、CIMC からログアウトされます。

ステップ 5 [Upload Certificate] をクリックします。