

CSM:GUIアクセス用のサードパーティSSL証明書のインストール方法

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ユーザインターフェイスからのCSRの作成](#)

[CSMサーバへのID証明書のアップロード](#)

概要

Cisco Security Manager(CSM)には、サードパーティ認証局(CA)によって発行されたセキュリティ証明書を使用するオプションがあります。これらの証明書は、組織ポリシーがCSM自己署名証明書を使用できない場合や、特定のCAから取得した証明書を使用する場合に使用できます。

TLS/SSLは、CSMサーバとクライアントブラウザ間の通信にこれらの証明書を使用します。このドキュメントでは、CSMで証明書署名要求(CSR)を生成する手順と、同じID証明書とルートCA証明書をインストール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。

- SSL証明書アーキテクチャに関する知識。
- Cisco Security Managerの基礎知識。

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。

- Cisco Security Managerバージョン4.11以降

ユーザインターフェイスからのCSRの作成

この項では、CSRの生成方法について説明します。

ステップ1:Cisco Security Managerホームページを実行し、[Server Administration] > [Server] > [Security] > [Single-Server Management] > [Certificate Setup]を選択します。

ステップ2 : 次の表に記載されているフィールドに必要な値を入力します。

フィールド	使用方法に関する特記事項
国名	2文字の国番号。
都道府県	2文字の都道府県コードまたは都道府県の完全な名前。
地域	2文字の市区町村番号、または市区町村名の完全な名前。
組織名	組織の完全な名前または省略形。
組織単位名	部署名または省略形。
サーバ名	コンピュータのDNS名、IPアドレス、またはホスト名。 適切で解決可能なドメイン名を持つサーバ名を入力します。これは証明書に表示され、ローカルホストまたは127.0.0.1は指定しないでください。
電子メールアドレス	メールの送信先の電子メールアドレス。

Certificate Setup

Self Signed Certificate Setup

Country Name:

State or Province:

City (Eg : SJ):

Organization Name:

Organization Unit Name:

Server Name*:

Email Address:

Certificate Bit: 2048

Note:
Server Name (Hostname or IP Address or FQDN) is the mandatory field. This is required to create the certificate. Ensure that the server name is same as the peer hostname that is used for setting up peer relations. Entering other fields are optional. However, it is desirable to provide all input fields for certificate regeneration.

ステップ3:[Apply]をクリックしてCSRを作成します。

このプロセスでは、次のファイルが生成されます。

- server.key : サーバの秘密キー。
- server.crt : サーバの自己署名証明書。
- server.pk8:PKCS#8形式のサーバの秘密キー。
- server.csr : 証明書署名要求(CSR)ファイル。

注 : これは、生成されたファイルのパスです。

- ~ CSCOpX\MDC\Apache\conf\ssl\chain.cer
- ~ CSCOpX\MDC\Apache\conf\ssl\server.crt
- ~ CSCOpX\MDC\Apache\conf\ssl\server.csr
- ~ CSCOpX\MDC\Apache\conf\ssl\server.pk8

~ CSCOpX\MDC\Apache\conf\ssl\server.key

注：証明書が自己署名証明書である場合、この情報は変更できません。

CSMサーバへのID証明書のアップロード

このセクションでは、CAから提供されたID証明書をCSMサーバにアップロードする方法について説明します

ステップ1この場所で利用可能なSSLユーティリティスクリプトを検索する

NMSROOT\MDC\Apache

注:NMSROOTは、CSMがインストールされているディレクトリに置き換える必要があります。

このユーティリティには、次のオプションがあります。

番号 オプション

- 1 サーバ証明書情報の表示
- 0 入力証明書情報を表示します
- 3 サーバによって信頼されたルートCA証明書を表示する
- 4 入力証明書または証明書チェーンを確認します
- 5 単一のサーバ証明書のサーバへのアップロード

機能

- CSMサーバの証明書の詳細を表示します。サードパーティが発行した証明書の場合、このオプションでは、証明書が有効かどうかを確認します。
 - 証明書が有効かどうかを確認します。このオプションでは、証明書を入力として受入れます。
 - 証明書がエンコードされたX.509証明書であることを確認します。
 - 証明書のサブジェクトと発行証明書の詳細を確認します。
 - 証明書がサーバで有効かどうかを確認します。
 - 証明書のリストを生成し、サーバによって発行されたすべてのルートCA証明書のリストを生成し、サードパーティCAによって発行されたサーバ証明書を確認します。
 - このオプションを選択すると、ユーティリティは、証明書がBase64 Encoded X.509Certificateであることを確認します。
 - 証明書がサーバで有効かどうかを確認します。
 - サーバの秘密キーと入力サーバ証明書を確認します。
 - サーバ証明書が、署名された必要なルートCA証明書であることを確認します。
 - 中間チェーンも指定されている場合は証明書チェーンを確認します。
 - 証明書が正常に完了すると、CSMサーバに証明書がアップロードされます。
 - ユーティリティに次のエラーが表示されます。
 - 入力証明書の形式が必須でない場合
 - 証明書の日付が無効であるか、証明書の有効期限が満了しているか
 - サーバ証明書を検証できなかつたり、ルートCA証明書が信頼されていない場合
 - 中間証明書のいずれかが入力として指定されていない場合
 - サーバの秘密キーが見つからない場合
- 証明書がCSMにアップロードする前に、証明書チェーンを確認してください。このオプションを選択する前に、オプションで指定されたルートCA証明書が中間証明書がなく、目立つルートCA証明書であることを確認してください。ルートCAがCSMによって信頼されていない場合、このような場合、証明書の署名に使用する

このオプションを選択し、証明書場所を指定する。

- 証明書がBase64 Encoded X.509証明書形式であるか、証明書のサブジェクトと発行証明書のサブジェクトが一致しているかを確認する。
- 証明書がサーバで有効かどうかを確認する。
- サーバの秘密キーと入力サーバ証明書が一致しているかを確認する。
- サーバ証明書が、署名に使用された必要十分な秘密キーを持っているかを確認する。

検証が正常に完了すると、ユーティリティは入力された証明書とサーバ証明書を比較し、ユーティリティに次のエラーが表示されません。

- 入力証明書の形式が必須でない場合
- 証明書の日付が無効であるか、証明書のサブジェクトと発行証明書のサブジェクトが一致していない場合
- サーバ証明書を検証できなかつたり、サーバの秘密キーが見つからない場合

証明書をCSMに再度アップロードする前に、このオプションを選択する前に、オプション1を使用して証明書チェーンをアップロードする場合は、このオプションを選択し、証明書場所を指定する。

- 証明書がBase64 Encoded X.509 Certificate形式であるか、証明書のサブジェクトと発行証明書のサブジェクトが一致しているかを確認する。
- 証明書がサーバで有効かどうかを確認する。
- サーバ秘密キーとサーバ証明書が一致しているかを確認する。
- サーバ証明書が、署名に使用された十分な秘密キーを持っているかを確認する。
- 中間チェーンが指定されている場合は、中間チェーンのいずれかが入力として指定されているかを確認する。

検証が正常に完了すると、サーバ証明書がCSMにアップロードされ、すべての中間証明書とルートCA証明書がアップロードされ、ユーティリティに次のエラーが表示されません。

- 入力証明書の形式が必須でない場合。
- 証明書の日付が無効であるか、証明書のサブジェクトと発行証明書のサブジェクトが一致していない場合
- サーバ証明書を検証できなかつたり、サーバの秘密キーが見つからない場合

証明書をCiscoWorksに再度アップロードする前に、このオプションを使用すると、Common Servicesの既存のホスト名エントリを変更する場合は、

6 サーバへの証明書チェーンのアップロード

7 Common Services証明書の変更

```

Administrator: Command Prompt

*** SSL Utility ***

Note: Any Certificate given as input to this script should be in Base64-Encoded X.509Certificate format

You have the following options

1. Display Server Certificate Information
2. Display the input Certificate Information
3. Display Root CA Certificates trusted by Server
4. Verify the input Certificate/ Certificate Chain
5. Upload Single Server Certificate to Server
6. Upload a Certificate Chain to Server
7. Modify Common Services Certificate
8. Quit

Enter your choice [1-8]:8

```

ステップ2オプション1を使用して、現在の証明書のコピーを取得し、将来の参照用に保存します

。

ステップ3 Windowsコマンドプロンプトでこのコマンドを使用してCSMデーモンマネージャを停止してから、証明書のアップロードプロセスを開始します。

```
net stop crmdmgt
```

注：このコマンドを使用すると、CSMサービスがダウンします。この手順でアクティブな配置がないことを確認します。

ステップ4 SSLユーティリティをもう一度開きます。このユーティリティを開くには、前述のパスに移動し、このコマンドを使用します。

```
perl SSLUtil.pl
```

ステップ5 オプション4を選択します。入力した証明書/証明書チェーンを確認します。

ステップ6 証明書の場所 (サーバ証明書と中間証明書) を入力します。

注:スクリプトは、サーバ証明書が有効かどうかを確認します。検証が完了すると、ユーティリティにオプションが表示されます。検証および検証時にスクリプトがエラーを報告すると、SSLユーティリティはこれらのエラーを修正する手順を表示します。手順に従ってこれらの問題を修正し、もう一度同じオプションを試してください。

ステップ7 次の2つのオプションのいずれかを選択します。

アップロードする証明書が1つしかない場合は、オプション5を選択します。これは、サーバ証明書がルートCA証明書によって署名されている場合です。

または

アップロードする証明書チェーンがある場合は[オプション6]を選択します。サーバ証明書と中間証明書がある場合は、

注:CSM Daemon Managerが停止していない場合、CiscoWorksはアップロードを続行できません。サーバ証明書のアップロード中にホスト名の不一致が検出された場合、ユーティリティは警告メッセージを表示しますが、アップロードは続行できます。

ステップ8:必要な詳細情報を入力します。

- 証明書の場所
- 中間証明書がある場合、その場所。

すべての詳細が正しく、証明書がセキュリティ証明書のCSM要件を満たしている場合、SSLユーティリティは証明書をアップロードします。

ステップ9 CSMデーモンマネージャを再起動して、新しい変更を有効にし、CSMサービスを有効にします。

```
net start crmdmgt
```

注：すべてのCSMサービスが再起動するまで、全体で10分待ちます。

ステップ10 CSMがインストールされているID証明書を使用していることを確認します。

注:SSL接続がCSMに確立されるPCまたはサーバに、ルートおよび中間CA証明書をインストールすることを忘れないでください。