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

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 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。

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	機能
1	サーバ証明書情報の表示	• 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 • 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
0	入力証明書情報を表示します	• 証明書がエンコードされたX.509証明書 • 証明書のサブジェクトと発行証明書の詳 • 証明書がサーバで有効かどうかを確認し
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	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 このオプションを選択すると、ユーティリテ
4	入力証明書または証明書チェーンを確認します	• 証明書がBase64 Encoded X.509Certific • 証明書がサーバで有効かどうかを確認し • サーバーの秘密キーと入力サーバー証明 • サーバ証明書が、署名された必要なルー • 中間チェーンも指定されている場合は証 検証が正常に完了すると、CSMサーバに証明 ユーティリティに次のエラーが表示されます
5	単一のサーバ証明書のサーバへのアップロード	• 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 • サーバ証明書を検証できなかったり、ル • 中間証明書のいずれかが入力として指定 • サーバーの秘密キーが見つからない場合 証明書をCSMにアップロードする前に、証明 このオプションを選択する前に、オプション 中間証明書がなく、目立つルートCA証明書 ルートCAがCSMによって信頼されていない このような場合、証明書の署名に使用するル

	このオプションを選択し、証明書の場所を指 • 証明書がBase64 Encoded X.509証明書 • 証明書のサブジェクトと発行証明書の詳 • 証明書がサーバで有効かどうかを確認し • サーバーの秘密キーと入力サーバー証明 • サーバ証明書が、署名に使用された必要 検証が正常に完了すると、ユーティリティは 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 • サーバ証明書を検証できなかったり、小 • サーバー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 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、証明書の場所を指 • 証明書がBase64 Encoded X.509 Certific • 証明書のサブジェクトと発行証明書の詳 • 証明書がサーバで有効かどうかを確認し • サーバー秘密キーとサーバー証明書がー • サーバ証明書が、署名に使用されたルー • 中間チェーンが指定されている場合は証 検証が正常に完了すると、サーバ証明書がC すべての中間証明書とルートCA証明書がア 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 • サーバ証明書を検証できなかったり、小 • 中間証明書のいずれかが入力として指定 • サーバー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 このオプションを使用すると、Common Se 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

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 crmdmgtd
```

> **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 crmdmgtd
```

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。