CSM - GUIアクセスのためのサード・パーティ SSL 証明書をインストールする方法

目次

概要

Cisco Security Manager （CSM）はサード・パーティ証明書権限（CA）によって発行されるセキュリティ証明書を使用するためにオプションを提供します。 これらの証明書は組織ポリシーが CSM 自己署名証明書の使用から防ぐか、またはシステムを特定の CA から得られる証明書を使用するように要求するとき使用することができます。

TLS/SSL は CSM サーバとクライアント ブラウザ間のコミュニケーションのためにこれらの証明書を使用します。 この文書は CSM の証明書署名要求（CSR）を生成するためにステップを同じに識別およびルートCA 証明書をインストールする方法を記述したものです。

前提条件

要件

次の項目に関する知識が推奨されます。

- SSL 証明書アーキテクチャの知識。
- Cisco Security Manager の基本的な知識。

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くものです。

- Cisco Security Manager バージョン 4.11 および それ 以降。

ユーザインターフェイスからの CSR 作成

このセクションは CSR を生成する方法を記述します。

ステップ 1. Cisco Security Manager ホームページを実行し、**Administration > サーバ > Security > 単一サーバ管理 > 証明書設定を**『Server』 を選択 して下さい。

ステップ 2.この表に説明があるフィールドに必要な値を入力して下さい:

フィールド	使用方法に関する特記事項
国名	2 文字国別コード。
状態か地域	状態または地域の 2 文字状態または地域コードか完全な名前。
局所性	都市または町の 2 文字都市または町コードか完全な名前。
組織名	組織または省略形の名前を完了して下さい。
Organization Unit 名前	部門または省略形の名前を完了して下さい。
サーバ名	DNS名、コンピュータの 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のサーバ名を入力して下さい。 これは証明書に発行される自己署名またはサード パーティかどうか) 表示されます (。 ローカル ホス 127.0.0.1 は与えるべきではありません。
E メールアドレス	メールが送られなければならない E メールアドレス。

ステップ 3. CSR を作成するために『Apply』 をクリック して下さい。

プロセスは次のファイルを生成します:

- server.key —サーバのプライベートキー。
- server.crt —サーバの自己署名証明書。
- server.pk8 — PKCS#8 形式のサーバのプライベートキー。
- server.csr —証明書署名要求 (CSR) ファイル。

注: これは生成されるファイルのためのパスです。

~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、この情報を修正できません。

CSM サーバへの ID証明アップ ロード

このセクションは CA によって提供される CSM サーバに ID証明をアップ ロードする方法を記述します

ステップ 1 SSL ユーティリティ スクリプトをこの位置で利用可能見つけて下さい

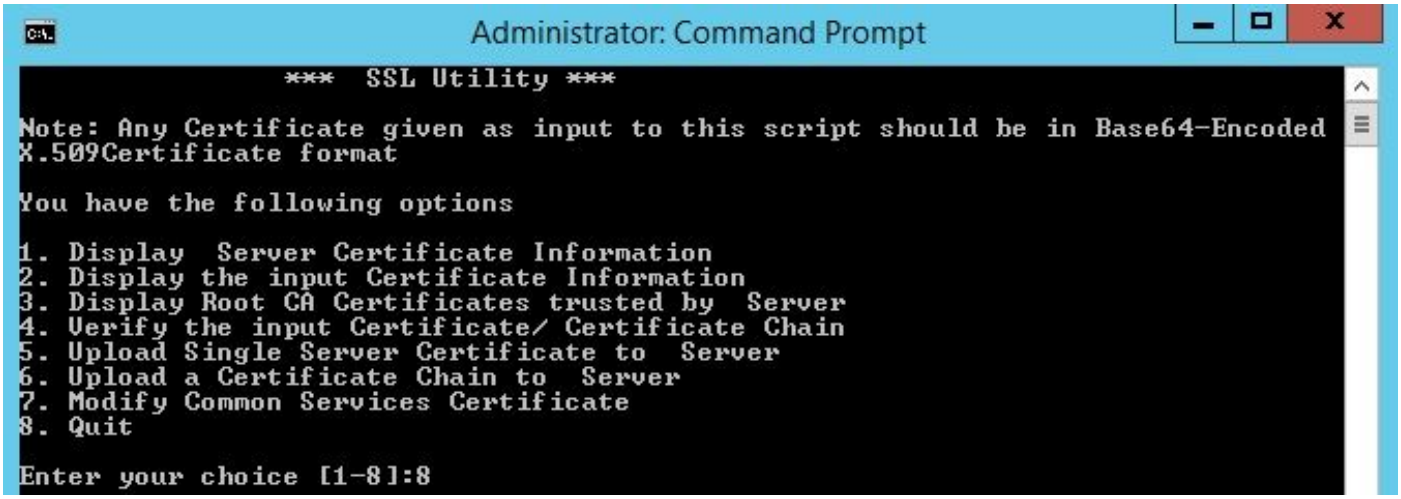
```
NMSROOT\MDC\Apache
```

注: NMSROOT は CSM がインストールされているディレクトリと取替える必要があります。

このユーティリティにこれらのオプションがあります。

number オプション		何をそれが…
1	サーバ証明情報を表示して下さい	• CSM サーバの証明書の詳細を表示します。 サード パーティ 発された認証に関しては、このオプションです。 • 証明書が有効であるかどうか確認します。
2	入力証明書情報を表示して下さい	このオプションは入力として証明書を受け入れ、: • 証明書が符号化された X.509 証明書フォーマットにあ • 証明書の主題および発行証明書の細部を表示します。 • 証明書がサーバで有効であるかどうか確かめます。
3	サーバによって信頼されるルートCA証明書を表示して下さい	すべてのルートCA 証明書のリストを作成します。
4	入力証明書か証明書 チェーンを確認して下さい	サード パーティ CA が発行するサーバ証明がアップ ロード このオプションを選択する時、ユーティリティ: • 証明書が Base64 によって符号化される X.509Certifica • 証明書がサーバで有効であるかどうか確認します • サーバ プライベートキーおよび入力サーバ証明が一致 • サーバ証明が署名した必須ルートCA認証にトレースす • 中間チェーンがまた与えられれば、組み立てチェーンが 確認が正常に完了した後、CSM サーバに証明書をアップ ロ ユーティリティは エラーを表示します: • 入力証明書が必要とされたフォーマットでなければ • 証明書日付が無効であるか、または証明書が既に切れて • サーバ証明がルートCA認証に確認されか、またはトレ • 中間証明書のうちのどれかが入力として与えられなか

		• サーバのプライベートキーが抜けているか、またはア した。 CSM に証明書をアップ ロードする前にこれらの問題を訂正 このオプションを選択する前にオプション 4 を使用して証 中間証明書がないし、顕著なルートCA認証によって署名す ルートCA が CSM によって信頼される 1 ではない場合この このような場合、CA からの証明書に署名するために使用さ して下さい。 このオプションを選択し、証明書の位置を提供する時、ユ
5	サーバへのアップ ロード単一サーバ証明書	• 証明書が Base64 によって符号化される X.509 証明書 • 証明書の主題および発行証明書の細部を表示します。 • 証明書がサーバで有効であるかどうか確かめます。 • サーバ プライベートキーおよび入力サーバ証明が一致 • 署名のために使用されたサーバ証明が必須ルートCA認 確認が正常に完了した後、ユーティリティは CiscoWorksサ ユーティリティはエラーを表示します: • 入力証明書が必要とされたフォーマットでなければ • 証明書日付が無効であるか、または証明書が既に切れて • サーバ証明がルートCA認証に確認されか、またはトレ • サーバのプライベートキーが抜けているか、またはア した。 CSM の証明書を再度アップ ロードする前にこれらの問題を このオプションを選択する前にオプション 4 を使用して証
6	サーバに証明書 チェーンをアップロードして下さい	証明書 チェーンをアップ ロードする場合、このオプション に証明書の 1 つとしてそれを含めて下さい。 このオプションを選択し、証明書の位置を提供する時、ユ • 証明書が Base64 によって符号化される X.509 証明書 • 証明書の主題および発行証明書の細部を表示します。 • 証明書がサーバで有効であるかどうか確かめます • サーバ プライベートキーおよびサーバ証明が一致する • 署名のために使用されたサーバ証明がルートCA認証に • 中間チェーンが与えられれば組み立て、チェーンが適 確認が正常に完了した後、サーバ証明は CiscoWorksサーバ すべての中間証明書およびルートCA認証は CSM TrustStor ユーティリティは工ラーを表示します:
		• 入力証明書が必要とされたフォーマットでなければ。 • 証明書日付が無効であるか、または証明書が既に切れて • サーバ証明がルートCA認証に確認されか、またはトレ • 中間証明書のうちのどれかが入力として与えられなか • サーバのプライベートキーが抜けているか、またはア した。 CiscoWorks の証明書を再度アップ ロードする前にこれらの
7	Common Services 証明書を修正して下さい	このオプションは Common Services 証明書のホスト名項目 既存のホスト名項目を変更したい場合代替ホスト名を入力



ステップ 2 現在の証明書のコピーを得、未来の参照用の保存するのに**オプション 1 を**使用して下さい。

ステップ 3 証明書アップ ロード プロセスを開始する前に Windows コマンド プロンプトのこのコマンドを使用している CSM デーモン 管理 プログラムを停止して下さい。

```
net stop crmdmgtd
```

> **注:** CSM サービスはこのコマンドの使用をたどって行きます。 この手順の間にアクティブな配備がないことを確かめて下さい。

ステップ 4 SSL ユーティリティをもう一度開いて下さい。 このユーティリティはコマンド プロンプトを使用して以前に述べられたパスへのナビゲートし、このコマンドを使用することによって開くことができます。

```
perl SSLUtil.pl
```

ステップ 5 4.を確認します入力認証証明書 チェーンを『Option』 を選択 して下さい**。**

ステップ 6 証明書口ケーションを入力して下さい（サーバ証明および中間物証明書）。

> **注:** スクリプトはサーバ証明が有効であるかどうか確認します。 確認が完了する後、ユーティリティはオプションを表示します。 検証および確認の間の Script レポート エラー、これらのエラーを訂正する SSL ユーティリティ展示教育。 それらの問題を訂正し、次に同じオプションをもう一度試みる手順に従って下さい。

ステップ 7 の次の 2 つのオプション選択して下さい。

アップ ロードするべき証明書が 1 つだけあったら **5 つを**それサーバ証明がルートCA認証によって署名する場合です『Option』 を選択 して下さい。

または

アップ ロードするべき証明書 チェーンがあったら **6 つを**それサーバ証明および中間物証明書がある場合です『Option』 を選択 して下さい。

注: CiscoWorks は CSM デーモン 管理 プログラムが停止しない場合アップロードを続行することを割り当てません。 ユーティリティはホスト名がある場合警告メッセージを表示します-アップ ロードされるサーバ証明で検出されるミスマッチしかしアップ ロードは続けることができます。

ステップ 8 これらの必須詳細を入力して下さい。

- 証明書の位置
- 中間証明書の位置、もしあれば。

SSL ユーティリティはすべての細部が正しく、証明書がセキュリティ証明書のための CSM 要件を満たせば場合証明書をアップ ロードします。

ステップ 9 実施され、CSM サービスを有効に するために新しい変更のための CSM デーモン 管理 プログラムを再起動して下さい。

```
net start crmdmgtd
```

注: CSM サービスすべてのための 10 分のオーバーオールのために再起動するべき待って下さい。

ステップ 10 CSM を使用していますインストールされる ID証明を確認して下さい。

注: からインストールすることを CSM への SSL 接続が stablished PC かサーバにルートおよび中間 CA 証明書を忘れないで下さい。