

# Cisco UCCE Web サービスのための生成する SHA-256 自己署名証明書

## 目次

[概要](#)

[問題](#)

[解決策](#)

[WebSetup および CCE 管理のためのソリューション](#)

[診断フレームワーク柱廊玄関のためのソリューション](#)

[確認](#)

[関連記事](#)

## 概要

この資料は Web セットアップまたは CCE 管理のような Cisco Unified Contact Center Enterprise ( UCCE ) Web サービスのための SHA-256 認証 シグニチャ アルゴリズムを使用して自己署名証明書の生成のプロセスを説明したものです。

## 問題

Cisco UCCE に Microsoft Internet Information Services ( IIS ) サーバによってホストされる何人か Web サービスがあります。 UCCE 配備の Microsoft IIS は SHA-1 認証署名アルゴリズムとデフォルトで自己署名証明書を使用しています。

SHA-1 アルゴリズムはブラウザのほとんど安全でないと考慮されます、従ってある時点でエージェント reskilling にスーパーバイザによって使用する CCE 管理のような重要なツールは利用できなくなるかもしれません。

## 解決策

その問題へのソリューションは使用するために IIS サーバのための SHA-256 認証を生成することです。

**警告：** 署名入り認証を認証局 ( CA ) 使用するために推奨します。従ってここに記述されている自己署名証明書を生成することは一時的な次善策としてサービスをすぐに再開すると考慮する必要があります。

**注:** ICM インターネット スクリプト エディタ アプリケーションがリモート スクリプト管理のために使用されればそれのための認証を生成するのに SSL 暗号化ユーティリティを使用する必要があります。

[WebSetup および CCE 管理のためのソリューション](#)

1. UCCE サーバの Start ウィンドウ PowerShell ツール。

2. PowerShell 型コマンド

```
New-SelfSignedCertificate -DnsName "pgb.allevich.local" -CertStoreLocation  
"cert:\LocalMachine\My"
```

**DnsName** の後のパラメータが認証 Common Name ( CN ) を規定 するところ。サーバのための正しいものに DnsName の後でパラメータを取り替えて下さい。認証は 1 年の有効性と生成されます。

注: 認証の Common Name はサーバの完全修飾ドメイン名 ( FQDN ) を一致するなりません。

3. Microsoft Management Console ( MMC ) ツールを開いて下さい。『File』を選択して下さい-> Add は/取除きますスナップインを... -> 認証を選択し、指定スナップ ins にそれを『Computer Account』を選択し、追加して下さい。『OK』を押し、そして Console Root > Certificates ( Local Computer ) > Personal > Certificates にナビゲートして下さい。

新しく作成された認証がここにあることを確認して下さい。認証に設定された表示名がありません従ってそれは CN および有効期限に基づいて認識することができます。

表示名は認証に認証プロパティを選択し、適切な名前が表示名テキストボックスを一杯にすることによって割り当てることができます。

4. Internet Information Services ( IIS ) マネージャを開始して下さい。右のペインの選定された IIS デフォルトの Web サイトは『Bindings』を選択し。選定された **HTTPS は- SSL 認証リスト** 選定された自己署名 SHA-256 からの > Edit 認証を生成し。

5. 再始動「ワールドワイドウェブパブリッシングサービス」サービス。

## 診断フレームワーク柱廊玄関のためのソリューション

1. ステップを 1-3 繰り返して下さい。

新しい自己署名証明書は生成されます。柱廊玄関ツールに関しては認証を結合 するもう一つの方法があります。

2. 柱廊玄関ツールのための現在の認証 バインディングを取除いて下さい。

```
cd c:\icm\serviceability\diagnostics\bin
```

```
DiagFwCertMgr /task:UnbindCert
```

3. 柱廊玄関のために生成される自己署名証明書を結合 して下さい。

柱廊玄関ツールのために生成される自己署名証明書を開き、タブを『Details』を選択して下さい。テキストエディタに拇印値をコピーして下さい。

注: いくつかのテキストエディタで拇印は疑問符と自動的に付加されます。それを取除いて下さい。

すべての空白文字を拇印から削除し、次のコマンドでそれを使用して下さい。

```
DiagFwCertMgr /task:BindCertFromStore /certhash:<thumbprint-value>
```

4. 認証 バインディングがこのコマンドを使用して正常だったことを確認して下さい。

```
DiagFwCertMgr /task:ValidateCertBinding
```

同じようなメッセージは出力で表示する必要があります。

「認証 バインディングです有効」は

5. 診断フレームワーク サービスを再開して下さい。

```
sc stop "diagfwsvc"  
sc start "diagfwsvc"
```

## 確認

ブラウザキャッシュおよび履歴をクリアして下さい。CCE 管理サービス Web ページにアクセスすれば自己署名証明書警告を得る必要があります。

証明書の詳細を表示し、認証に SHA-256 認証 シグニチャ アルゴリズムがあることを確認して下さい。

## 関連記事

[UCCE 診断柱廊玄関ツールのための生成する CA 署名入り認証](#)

[UCCE Web セットアップ用の生成する CA 署名入り認証](#)

[VOS のための生成する CA 署名入り認証は CLI を使用してサーバを基づかせていました](#)

[CVP OAMP サーバのための生成する CA 署名入り認証](#)