

# Générez les Certificats Auto-signés par SHA-256 pour des services Web de Cisco UCCE

## Contenu

[Introduction](#)

[Problème](#)

[Solution](#)

[Solution pour WebSetup et gestion CCE](#)

[Solution pour le portique diagnostique de cadre](#)

[Vérification](#)

[Articles relatifs](#)

## Introduction

Ce document décrit un processus de générer les Certificats auto-signés utilisant l'algorithme de signature du certificat SHA-256 pour des services Web du Cisco Unified Contact Center Enterprise (UCCE) comme l'installation de Web ou la gestion CCE.

## Problème

Cisco UCCE a plusieurs services Web hébergés par le serveur de l'Internet Information Services de Microsoft (IIS). Microsoft IIS dans le déploiement UCCE par défaut utilise les Certificats auto-signés avec l'algorithme de signature du certificat SHA-1.

L'algorithme SHA-1 est considéré unsecure par la plupart des navigateurs, donc à certains les outils essentiels de point comme la gestion CCE utilisée par des superviseurs pour la formation d'agent peuvent devenir indisponibles.

## Solution

La solution à ce problème est de générer les Certificats SHA-256 pour que le serveur IIS l'utilise.

**Avertissement** : Il est recommandé pour utiliser les Certificats signés d'autorité de certification. Générer ainsi les Certificats auto-signés décrits ici devrait être considéré comme comme contournement provisoire pour restaurer le service rapidement.

## Solution pour WebSetup et gestion CCE

1. Outil de Windows PowerShell de début sur le serveur UCCE.
2. En type de PowerShell la commande

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

Là où le paramètre après que **DnsName** spécifie le nom commun de certificat (NC). Remplacez le paramètre après DnsName au correct pour le serveur. Le certificat sera généré avec une validité d'un an.

Remarque: Le nom commun dans le certificat doit apparier le nom de domaine complet (FQDN) du serveur.

3. Ouvrez l'outil de Microsoft Management Console (MMC). Sélectionnez le **fichier** - > **ajout/suppression SNAP-dans...** - > les **Certificats** choisis, choisissez le **compte d'ordinateur** et **l'ajoutent au SNAP**-Institut central des statistiques sélectionné. Appuyez sur correct, puis naviguez **pour consoler la racine** - > **délivre un certificat (ordinateur local)** - > **personnel** - > des **Certificats**.

Assurez-vous que le certificat de création récente est présent ici. Le certificat n'aura pas le nom amical configuré, ainsi il peut identifier a basé sa NC et date d'expiration.

Le nom amical peut être assigné au certificat en sélectionnant les **propriétés de** certificat et en remplissant zone de texte **amicale de nom de** nom approprié.

4. Gestionnaire de l'Internet Information Services de début (IIS). Le site Web choisi de par défaut IIS et sur le volet de droite choisissent des **attaches**. **HTTPS** choisi - > **éditez** et du certificat généré par SHA-256 auto-signé choisi de liste de certificat ssl.

5. Service de « service d'édition de World Wide Web » de reprise.

Remarque: Il n'y a aucun besoin de défaire ou lier le certificat dans l'outil d'utilitaire de ssl encryption.

## Solution pour le portique diagnostique de cadre

1. Répétez les étapes 1-3.

Un nouveau certificat auto-signé sera généré. Pour l'outil de portique il y a une autre manière de lier le certificat.

2. Retirez le certificat valable liant pour l'outil de portique.

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

```
DiagFwCertMgr /task:UnbindCert
```

3. Liez le certificat auto-signé généré pour le portique.

Ouvrez le certificat auto-signé généré pour l'outil de portique et la copie choisie de tableau de **détails** la valeur de Thumbprint à l'éditeur de texte.

Remarque: Dans quelques éditeurs de texte le thumbprint est automatiquement ajouté au début avec un point d'interrogation. Retirez-le.

Enlevez tous les caractères espace du thumbprint et utilisez-les dans la commande suivante.

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

4. Assurez-vous que l'attache de certificat était réussie utilisant cette commande.

```
DiagFwCertMgr /task:ValidateCertBinding
```

Le message semblable devrait être affiché dans la sortie.

« L'attache de certificat est VALIDE »

5. Redémarrez le service diagnostique de cadre.

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

## Vérification

Effacez le cache du navigateur et l'historique. La page Web et vous de service de gestion d'Access CCE devriez obtenir un avertissement auto-signé de certificat.

Visualisez les détails de certificat et assurez-vous que le certificat a l'algorithme de signature du certificat SHA-256.

## Articles relatifs

[Générez le certificat signé CA pour l'outil diagnostique de portique UCCE](#)

[Générez le certificat signé CA pour l'installation de Web UCCE](#)

[Générez le certificat signé CA pour le serveur basé par VOS utilisant le CLI](#)

[Générez le certificat signé CA pour le serveur CVP OAMP](#)