CSM - Comment installer des certificats SSL tiers pour l'accès à l'interface utilisateur graphique

Contenu

Introduction

Cisco Security Manager (CSM) permet d'utiliser les certificats de sécurité émis par des autorités de certification tierces. Ces certificats peuvent être utilisés lorsque la stratégie d'organisation empêche l'utilisation de certificats auto-signés CSM ou exige que les systèmes utilisent un certificat obtenu d'une autorité de certification particulière.

TLS/SSL utilise ces certificats pour la communication entre CSM Server et le navigateur client. Ce document décrit les étapes pour générer une demande de signature de certificat (CSR) dans CSM et comment installer les certificats d'identité et d'autorité de certification racine dans le même.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de l'architecture des certificats SSL.
- Connaissances de base de Cisco Security Manager.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Security Manager versions 4.11 et ultérieures.

Création CSR à partir de l'interface utilisateur

Cette section décrit comment générer un CSR.

Étape 1. Exécutez la page d'accueil de Cisco Security Manager et sélectionnez **Server Administration > Server > Security > Single-Server Management > Certificate Setup.**

Étape 2. Entrez les valeurs requises pour les champs décrits dans ce tableau :

Champ	Notes d'utilisation
Nom du pays	Code pays à deux caractères.
État ou province	Code d'état ou de province à deux caractères ou nom complet de l'état ou de la province.
Localité	Code de ville à deux caractères ou nom complet de la ville ou de la ville.
Nom de l'organisation	Nom complet de votre organisation ou abréviation.
Nom de l'unité d e l'organisation	Nom complet de votre service ou abréviation.
	Nom DNS, adresse IP ou nom d'hôte de l'ordinateur.
Nom de serveur	Entrez le nom du serveur avec un nom de domaine approprié et résolvable. Ceci est affic votre certificat (qu'il soit autosigné ou émis par un tiers). L'hôte local ou 127.0.0.1 ne do être fourni.
Adresse e-mail	Adresse électronique à laquelle le courrier doit être envoyé.

Étape 3. Cliquez sur **Apply** pour créer le CSR.

Le processus génère les fichiers suivants :

- server.key : clé privée du serveur.
- server.crt : certificat auto-signé du serveur.
- server.pk8 : clé privée du serveur au format PKCS#8.
- server.csr : fichier CSR (Certificate Signing Request).

Remarque : il s'agit du chemin d'accès des fichiers générés.
~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

Remarque : si le certificat est un certificat auto-signé, vous ne pouvez pas modifier ces informations.

Téléchargement du certificat d'identité dans CSM Server

Cette section décrit comment télécharger le certificat d'identité fourni par l'autorité de certification sur le serveur CSM

Étape 1 Recherchez le script de l'utilitaire SSL disponible à cet emplacement

`NMSROOT\MDC\Apache`

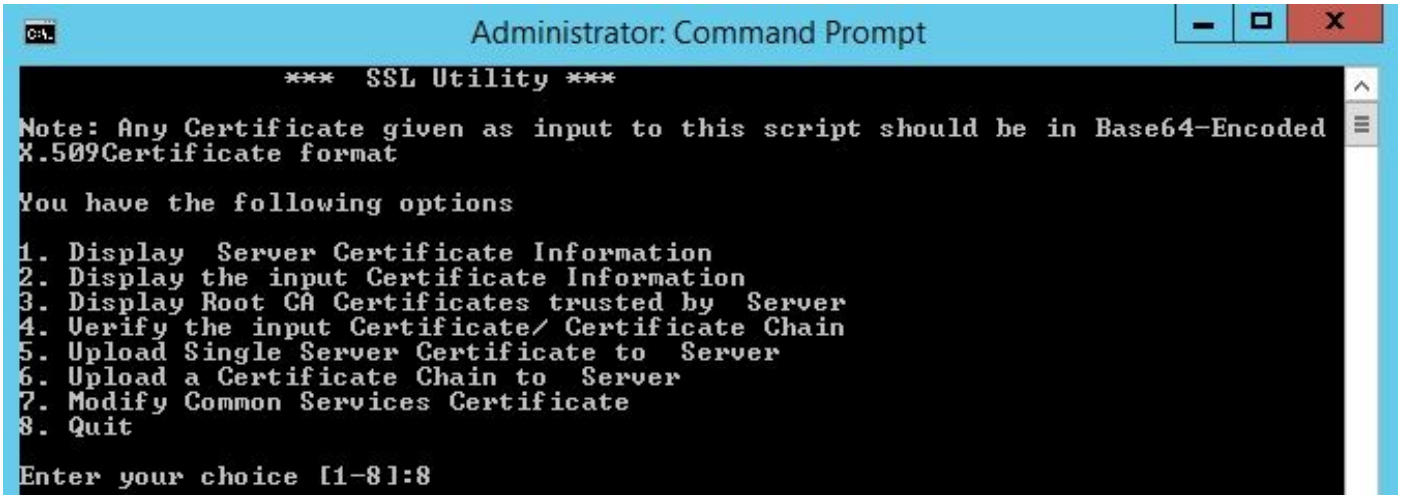
Remarque : NMSROOT doit être remplacé par le répertoire dans lequel CSM est installé.

Cet utilitaire propose ces options.

Nombre	Option	Ce que ça fait...
1	Afficher les informations de certificat du serveur	• Affiche les détails du certificat du serveur CSM. Pour les certificats émis par des tiers, cette option affiche les détail certificat serveur, des certificats intermédiaires, le cas échéant, et c certificat d'autorité de certification racine.
2	Afficher les informations de certificat d'entrée	• Vérifie si le certificat est valide. Cette option accepte un certificat comme entrée et : • Vérifie si le certificat est au format de certificat X.509 codé. • Affiche l'objet du certificat et les détails du certificat émetteur. • Vérifie si le certificat est valide sur le serveur.
3	Afficher les certificats d'autorité de certification racine approuvés par le serveur	Génère une liste de tous les certificats d'autorité de certification rac
4	Vérifier le certificat d'entrée ou la chaîne de certificats	Vérifie si le certificat de serveur émis par des autorités de certificat tierces peut être téléchargé. Lorsque vous choisissez cette option, l'utilitaire : • Vérifie si le certificat est au format de certificat X.509codé Bas • Vérifie si le certificat est valide sur le serveur

		• Vérifie si la clé privée du serveur et le certificat du serveur d'en correspondent. • Vérifie si le certificat du serveur peut être suivi au certificat d'au de certification racine requis à l'aide duquel il a été signé. • Construit la chaîne de certificats, si les chaînes intermédiaires également fournies, et vérifie si la chaîne se termine par le cer d'autorité de certification racine approprié. Une fois la vérification terminée, vous êtes invité à télécharger les certificats vers CSM Server. L'utilitaire affiche une erreur : • Si les certificats d'entrée ne sont pas au format requis • Si la date du certificat n'est pas valide ou si le certificat a déjà expiré. • Si le certificat du serveur n'a pas pu être vérifié ou associé à u certificat de l'autorité de certification racine. • Si l'un des certificats intermédiaires n'a pas été fourni en entré • Si la clé privée du serveur est manquante ou si le certificat du serveur en cours de téléchargement n'a pas pu être vérifié ave clé privée du serveur. Vous devez contacter l'autorité de certification qui a émis les certifi pour corriger ces problèmes avant de télécharger les certificats ver CSM.
5	Télécharger un certificat de serveur unique sur le serveur	Vous devez vérifier les certificats à l'aide de l'option 4 avant de sélectionner cette option. Sélectionnez cette option, uniquement s'il n'y a pas de certificats intermédiaires et que seul le certificat de serveur est signé par un certificat d'autorité de certification racine important. Si l'autorité de certification racine n'est pas approuvée par CSM, ne sélectionnez pas cette option. Dans de tels cas, vous devez obtenir un certificat d'autorité de certification racine utilisé pour signer le certificat de l'autorité de certification et télécharger les deux certificats à l'aide de l'option 6. Lorsque vous sélectionnez cette option et que vous indiquez l'emplacement du certificat, l'utilitaire : • Vérifie si le certificat est au format de certificat X.509 codé Bas • Affiche l'objet du certificat et les détails du certificat émetteur. • Vérifie si le certificat est valide sur le serveur. • Vérifie si la clé privée du serveur et le certificat du serveur d'en correspondent. • Vérifie si le certificat du serveur peut être suivi du certificat d'au de certification racine requis qui a été utilisé pour la signature. Une fois la vérification terminée, l'utilitaire télécharge le certificat ve CiscoWorks Server. L'utilitaire affiche une erreur : • Si les certificats d'entrée ne sont pas au format requis • Si la date du certificat n'est pas valide ou si le certificat a déjà expiré. • Si le certificat du serveur n'a pas pu être vérifié ou associé à u certificat de l'autorité de certification racine. • Si la clé privée du serveur est manquante ou si le certificat du

		serveur en cours de téléchargement n'a pas pu être vérifié ave clé privée du serveur. Vous devez contacter l'autorité de certification qui a émis les certifi pour corriger ces problèmes avant de télécharger à nouveau les certificats dans CSM.
6	Télécharger une chaîne de certificats sur le serveur	Vous devez vérifier les certificats à l'aide de l'option 4 avant de sélectionner cette option. Sélectionnez cette option si vous téléchargez une chaîne de certifi Si vous téléchargez également le certificat de l'autorité de certificat racine, vous devez l'inclure comme l'un des certificats de la chaîne Lorsque vous sélectionnez cette option et indiquez l'emplacement certificats, l'utilitaire : • Vérifie si le certificat est au format de certificat X.509 codé Bas • Affiche l'objet du certificat et les détails du certificat émetteur. • Vérifie si le certificat est valide sur le serveur • Vérifie si la clé privée du serveur et le certificat du serveur correspondent. • Vérifie si le certificat du serveur peut être retracé vers le certifi l'autorité de certification racine utilisé pour la signature. • Construit la chaîne de certificats, si des chaînes intermédiaires fournies et vérifie si la chaîne se termine par le certificat d'auto de certification racine approprié. Une fois la vérification terminée, le certificat du serveur est télécha vers CiscoWorks Server. Tous les certificats intermédiaires et le certificat de l'autorité de certification racine sont téléchargés et copiés dans CSM TrustStore L'utilitaire affiche une erreur : • Si le format des certificats d'entrée n'est pas requis. • Si la date du certificat n'est pas valide ou si le certificat a déjà expiré. • Si le certificat du serveur n'a pas pu être vérifié ou associé à u certificat de l'autorité de certification racine. • Si l'un des certificats intermédiaires n'a pas été donné en entré • Si la clé privée du serveur est manquante ou si le certificat du serveur en cours de téléchargement n'a pas pu être vérifié ave clé privée du serveur. Vous devez contacter l'autorité de certification qui a émis les certifi pour corriger ces problèmes avant de télécharger à nouveau les certificats dans CiscoWorks.
7	Modifier le certificat Common Services	Cette option vous permet de modifier l'entrée Nom d'hôte dans le certificat Common Services. Vous pouvez entrer un autre nom d'hôte si vous souhaitez modifier l'entrée de nom d'hôte existante.



Étape 2 Utilisez **l'option 1** pour obtenir une copie du certificat actuel et l'enregistrer pour référence future.

Étape 3 Arrêtez le Gestionnaire de démons CSM à l'aide de cette commande sur l'invite de commandes Windows avant de démarrer le processus de téléchargement de certificat.

```
net stop crmdmgtd
```

> **Remarque** : les services CSM tombent en panne à l'aide de cette commande. Assurez-vous qu'aucun déploiement n'est actif au cours de cette procédure.

Étape 4 Ouvrez l'utilitaire SSL une fois de plus. Cet utilitaire peut être ouvert à l'aide de l'invite de commandes en accédant au chemin mentionné précédemment et en utilisant cette commande.

```
perl SSLUtil.pl
```

Étape 5 Sélectionnez **Option 4**. **Vérifiez le certificat/la chaîne de certificats d'entrée.**

Étape 6 Entrez l'emplacement des certificats (certificat de serveur et certificat intermédiaire).

> **Remarque** : le script vérifie si le certificat du serveur est valide. Une fois la vérification terminée, l'utilitaire affiche les options. Si le script signale des erreurs lors de la validation et de la vérification, l'utilitaire SSL affiche des instructions pour corriger ces erreurs. Suivez les instructions pour corriger ces problèmes, puis essayez la même option une fois de plus.

Étape 7 Sélectionnez l'une des deux options suivantes.

Sélectionnez **Option 5** s'il n'y a qu'un seul certificat à télécharger, c'est-à-dire si le certificat du serveur est signé par un certificat d'autorité de certification racine.

OU

Sélectionnez **Option 6** s'il existe une chaîne de certificats à télécharger, c'est-à-dire s'il existe un certificat de serveur et un certificat intermédiaire.

Remarque : CiscoWorks ne permet pas de poursuivre le téléchargement si CSM Daemon Manager n'a pas été arrêté. L'utilitaire affiche un message d'avertissement si des incohérences de nom d'hôte sont détectées dans le certificat du serveur en cours de téléchargement, mais le téléchargement peut être poursuivi.

Étape 8 Entrez les détails requis.

- Emplacement du certificat
- Emplacement des certificats intermédiaires, le cas échéant.

L'utilitaire SSL télécharge les certificats si tous les détails sont corrects et que les certificats répondent aux exigences CSM pour les certificats de sécurité.

Étape 9 Redémarrez le gestionnaire de démon CSM pour que la nouvelle modification prenne effet et activez les services CSM.

```
net start crmdmgtd
```

Remarque : attendez une durée totale de 10 minutes pour redémarrer tous les services CSM.

Étape 10 Vérifiez que le CSM utilise le certificat d'identité installé.

Remarque : N'oubliez pas d'installer les certificats CA racine et intermédiaire sur le PC ou le serveur à partir duquel la connexion SSL est établie vers le CSM.