CSM - Comment installer de tiers Certificats SSL pour l'accès GUI

Contenu

Introduction

Le Cisco Security Manager (CSM) fournit une option d'utiliser des Certificats de Sécurité délivrés par les tiers autorités de certification (CAs). Ces Certificats peuvent être utilisés quand la stratégie organisationnelle empêche d'utiliser les Certificats auto-signés par CSM ou exige des systèmes d'utiliser un certificat obtenu d'un CA particulier.

TLS/SSL utilise ces Certificats pour la transmission entre le serveur CSM et le navigateur de client. Ce document décrit les étapes pour générer une demande de signature de certificat (CSR) dans le CSM et comment installer les Certificats CA d'identité et de racine dans la même chose.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance du SSL délivre un certificat l'architecture.
- Connaissance de base de Cisco Security Manager.

Composants utilisés

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

- Version 4.11 et ultérieures de Cisco Security Manager.

Création CSR de l'interface utilisateur

Cette section décrit comment générer un CSR.

Étape 1. Installation exécutez la page d'accueil de Cisco Security Manager et l'**administration de serveur** choisie **> le serveur > la Sécurité > de serveur unique Gestion > certificat.**

Étape 2. Écrivez les valeurs requises pour les champs décrits dans cette table :

Champ	Notes sur l'utilisation
Nom du pays	Code de pays de deux caractères.
État ou province	Code d'état ou de province de deux caractères ou le nom complet de l'état ou de la province.
Localité	Code de ville ou de ville de deux caractères ou le nom complet de ville ou de ville.
Nom d'organisation	Terminez-vous le nom de votre organisation ou d'une abréviation.
Nom d'unité d'organisation	Terminez-vous le nom de votre service ou d'une abréviation.
Nom de serveur	Nom DNS, adresse IP ou adresse Internet de l'ordinateur. Écrivez le nom du serveur avec un nom de domaine approprié et résoluble. Ceci est affiché sur votre certificat (si auto-signé ou tiers émis). L'hôte local ou le 127.0.0.1 ne devrait pas être donné.
Adresse e-mail	Adresse électronique à laquelle la messagerie doit être envoyée.

Étape 3. Cliquez sur Apply pour créer le CSR.

Le processus génère les fichiers suivants :

- server.key — La clé privée du serveur.
- server.crt — Le certificat signé auto- du serveur.
- server.pk8 — La clé privée du serveur dans le format PKCS#8.

- server.csr — Fichier de la demande de signature de certificat (CSR).

Note: C'est le chemin pour les 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

Note: Si le certificat est un certificat auto-signé, alors vous ne pouvez pas modifier ces informations.

Téléchargement de certificat d'identité dans le serveur CSM

Cette section décrit comment télécharger le certificat d'identité fourni par le CA au serveur CSM

Étape 1 Trouvez le script de service SSL disponible à cet emplacement

```
NMSROOT\MDC\Apache
```

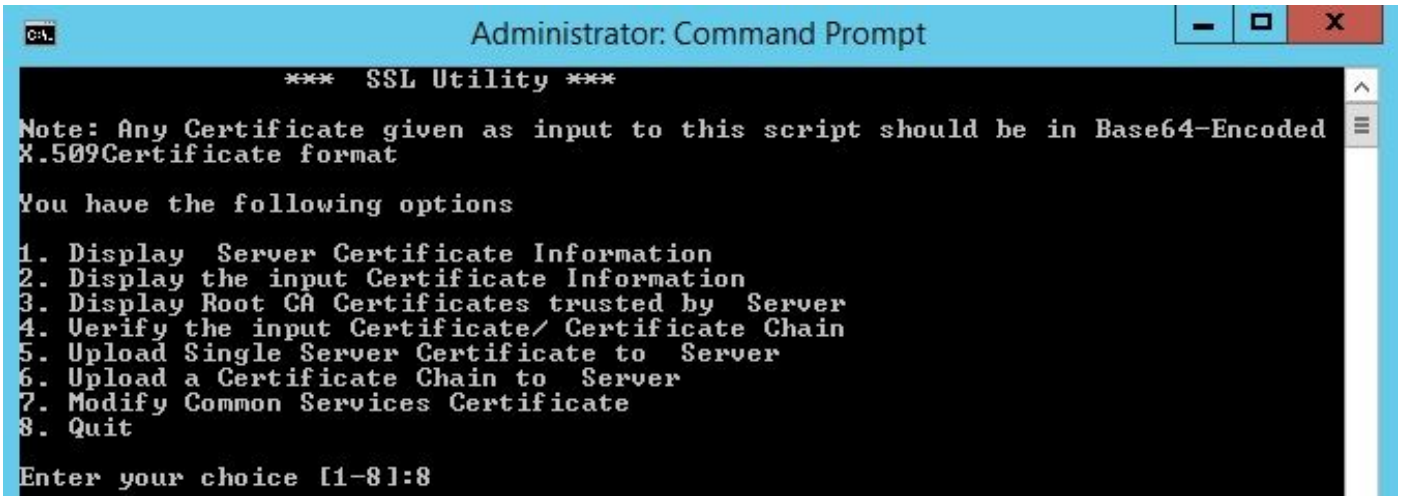
Note: NMSROOT doit être remplacé par le répertoire où le CSM est installé.

Cet utilitaire a ces options.

Nombre	Option	Ce qu'il fait…
1	Les informations de certificat de serveur d'affichage	• Affiche les coordonnées de certificat du serveur CSM. Pour le tiers émis les Certificats, cette option affichent les détails du ce de serveur, des Certificats intermédiaires, le cas échéant, et du certific CA de racine.
2	Affichez les informations de certificat d'entrée	• Vérifie si le certificat est valide. Cette option reçoit un certificat comme entrée et : • Vérifie si le certificat est dans le format encodé du certificat X.509. • Affiche le sujet du certificat et les petits groupes du certificat émett • Vérifie si le certificat est valide sur le serveur.
3	Certificats CA de racine d'affichage faits confiance par le serveur	Génère une liste de tous les Certificats CA de racine.
4	Vérifiez le certificat d'entrée ou la chaîne de certificat	Vérifie si le certificat de serveur délivré par le tiers CAs, peut être téléchargé. Quand vous choisissez cette option, l'utilitaire : • Vérifie si le certificat est dans le format X.509Certificate encodé pa Base64. • Vérifie si le certificat est valide sur le serveur • Vérifie si le certificat de serveur de clé privée et d'entrée de serveu s'assortissent. • Vérifie si le certificat de serveur peut être tracé au certificat de CA de racine utilisant lequel il a été signé.

		• Construit la chaîne de certificat, si les chaînes intermédiaires sont également données, et la vérifie si la chaîne finit avec le certificat approprié de racine. Après que la vérification soit avec succès terminée, vous êtes incité à télécharger les Certificats au serveur CSM. L'utilitaire affiche une erreur : • Si les Certificats d'entrée ne sont pas format dedans exigé • Si la date de certificat est non valide ou si le certificat a déjà expiré • Si le certificat de serveur ne pourrait pas être vérifié ou tracé à un certificat de CA de racine. • Si l'un des des Certificats intermédiaires n'ont pas été donnés com entrée. • Si la clé privée du serveur manque ou si le certificat de serveur qu téléchargé ne pourrait pas être vérifié avec la clé privée du serveu Vous devez entrer en contact avec le CA qui a délivré les Certificats po corriger ces problèmes avant que vous téléchargiez les Certificats au C
5	Certificat de serveur unique de téléchargement au serveur	Vous devez vérifier les Certificats utilisant l'option 4 avant que vous sélectionniez cette option. Sélectionnez cette option, seulement s'il n'y a aucun Certificats d'intermédiaire et il y a seulement le certificat de serveur signé par un certificat de CA important de racine. Si la racine CA n'est pas un fait confiance par CSM, ne sélectionnez pa cette option. En pareil cas, vous devez obtenir un certificat de CA de racine utilisé p signer le certificat du CA et télécharger les les deux les Certificats utilis l'option 6. Quand vous sélectionnez cette option, et fournissez l'emplacement du certificat, l'utilitaire : • Vérifie si le certificat est dans le format du certificat X.509 encodé Base64. • Affiche le sujet du certificat et les petits groupes du certificat émett • Vérifie si le certificat est valide sur le serveur. • Vérifie si le certificat de serveur de clé privée et d'entrée de serveu s'assortissent. • Vérifie si le certificat de serveur peut être tracé au certificat de CA de racine qui a été utilisé pour la signature. Après que la vérification soit avec succès terminée, l'utilitaire télécharg certificat au serveur de CiscoWorks. L'utilitaire affiche une erreur : • Si les Certificats d'entrée ne sont pas format dedans exigé • Si la date de certificat est non valide ou si le certificat a déjà expiré • Si le certificat de serveur ne pourrait pas être vérifié ou tracé à un certificat de CA de racine. • Si la clé privée du serveur manque ou si le certificat de serveur qu téléchargé ne pourrait pas être vérifié avec la clé privée du serveu Vous devez entrer en contact avec le CA qui a délivré les Certificats po corriger ces problèmes avant que vous téléchargiez les Certificats dan CSM de nouveau.
6	Téléchargez une chaîne de certificat au serveur	Vous devez vérifier les Certificats utilisant l'option 4 avant que vous sélectionniez cette option.

		Sélectionnez cette option, si vous téléchargez une chaîne de certificat. vous téléchargez également le certificat de CA de racine également, v devez l'inclure en tant qu'un des Certificats dans la chaîne. Quand vous sélectionnez cette option et fournissez l'emplacement des Certificats, l'utilitaire : • Vérifie si le certificat est dans le format du certificat X.509 encodé Base64. • Affiche le sujet du certificat et les petits groupes du certificat émett • Vérifie si le certificat est valide sur le serveur • Vérifie si la clé privée de serveur et le certificat de serveur s'assortissent. • Vérifie si le certificat de serveur peut être tracé au certificat de CA racine qui a été utilisé pour la signature. • Construit la chaîne de certificat, si des chaînes intermédiaires sont données et la vérifie si la chaîne finit avec le certificat de CA appro de racine. Après que la vérification soit avec succès terminée, le certificat de serv est téléchargé au serveur de CiscoWorks. Tous les Certificats d'intermédiaire et certificat de CA de racine sont téléchargés et copiés sur le CSM TrustStore. L'utilitaire affiche une erreur : • Si les Certificats d'entrée ne sont pas format dedans exigé. • Si la date de certificat est non valide ou si le certificat a déjà expiré • Si le certificat de serveur ne pourrait pas être vérifié ou tracé à un certificat de CA de racine. • Si l'un des des Certificats intermédiaires n'ont pas été donnés com entrée. • Si la clé privée du serveur manque ou si le certificat de serveur qu téléchargé ne pourrait pas être vérifié avec la clé privée du serveu Vous devez entrer en contact avec le CA qui a délivré les Certificats po corriger ces problèmes avant que vous téléchargiez les Certificats dan CiscoWorks de nouveau.
7	Modifiez le certificat commun de services	Cette option te permet pour modifier l'entrée de nom d'hôte dans le cer commun de services. Vous pouvez entrer dans une adresse Internet alternative si vous souh changer l'entrée existante de nom d'hôte.



Étape 2 Utilisez l'**Option 1** d'obtenir une copie du certificat valable et de la sauvegarder pour la référence ultérieure.

Étape 3 Arrêtez le gestionnaire de démon CSM utilisant cette commande sur la demande de commande Windows avant de commencer le processus de téléchargement de certificat.

```
net stop crmdmgtd
```

> **Note**: Les services CSM descendent utiliser cette commande. Assurez-vous qu'il n'y a aucun déploiement actif pendant cette procédure.

Étape 4 Ouvrez l'utilitaire SSL une fois de plus. Cet utilitaire peut être ouvert utilisant l'invite de commande en naviguant vers le chemin précédemment mentionné et en utilisant cette commande.

```
perl SSLUtil.pl
```

Étape 5 L'option choisie **4. vérifient la chaîne de certificat de certificat d'entrée.**

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

> **Note**: Le script vérifie si le certificat de serveur est valide. Après que la vérification soit complète, l'utilitaire présente les options. Si le script signale des erreurs pendant la validation et la vérification, les commandes d'affichages de service SSL de corriger ces erreurs. Suivez les instructions de corriger ces problèmes et puis d'essayer la même option une fois de plus.

Étape 7 Ensuite deux options l'unes des choisies.

Sélectionnez l'**option 5** s'il y a seulement un certificat au télécharger, cela est si le certificat de serveur est signé par un certificat de CA de racine.

OU

Sélectionnez l'**option 6** s'il y a une chaîne de certificat à la télécharger, cela est s'il y a un certificat de serveur et certificat intermédiaire.

> **Note**: Les CiscoWorks ne laissent pas se poursuivre par le téléchargement si le gestionnaire de démon CSM n'a pas été arrêté. L'utilitaire affiche un message d'avertissement s'il y a des non-concordances d'adresse Internet détectées dans le certificat de serveur étant téléchargé, mais le téléchargement peut être continué.

Étape 8 Écrivez ces détails requis.

- Emplacement du certificat
- Emplacement des Certificats intermédiaires éventuels.

L'utilitaire SSL télécharge les Certificats si tous les détails sont corrects et les Certificats répondent à des exigences CSM pour des Certificats de Sécurité.

Étape 9 Redémarrez le gestionnaire de démon CSM pour la nouvelle modification pour prendre effet et activer des services CSM.

```
net start crmdmgtd
```

> **Note**: Attendez pour une combinaison de 10 minutes pour que tous les services CSM soient redémarrés.

Étape 10 Confirmez le CSM utilise le certificat d'identité installé.

> **Note**: N'oubliez pas d'installer la racine et les Certificats CA intermédiaires dans le PC ou le serveur d'où la connexion SSL stablished au CSM.