

Contenu

[Introduction](#)

[Comment générer et installer un certificat numérique sur SMA ?](#)

[Fond](#)

[Créez et certificat d'exportation sur l'ESA](#)

[Convertissez le certificat exporté](#)

[Certificat d'importation à SMA - Option 1](#)

[Certificat d'importation à SMA - Option 2](#)

[Vérifiez le certificat importé](#)

[Informations connexes](#)

[Cisco relatif prennent en charge des discussions de la Communauté](#)

Introduction

Ce document décrit comment générer un certificat sur l'appliance de sécurité du courrier électronique (ESA) qui peut être utilisée sur l'appliance de Gestion de la sécurité (SMA).

Comment générer et installer un certificat numérique sur SMA ?

Fond

Le SMA ne prend en charge pas générer les Certificats sur l'appliance lui-même. Au lieu de cela il est possible de générer un certificat signé d'individu sur l'ESA. Ceci peut être utilisé comme contournement pour créer un certificat pour que le SMA soit importé et utilisé.

Créez et certificat d'exportation sur l'ESA

1. Créez un certificat signé d'individu sous le **GUI : Le réseau > les Certificats > ajoutent le certificat**. Il est important, en créant un certificat signé d'individu, pour le nom commun (NC) pour utiliser l'adresse Internet du SMA et pas de l'ESA, de sorte que le certificat puisse être correctement utilisé. Soumettez et commettez les modifications.
2. **GUI d'utilisation : Le réseau > délivre un certificat > des Certificats d'exportation** au certificat d'exportation. Donnez-lui un nom du fichier (par exemple mycert) et le mot de passe qui seront utilisés quand convertissant le certificat.

Convertissez le certificat exporté

Le certificat exporté sera dans le format **.pfx**. Le SMA prend en charge seulement le format **.pem** pour importer, ainsi les besoins de ce certificat d'être converti. Pour convertir le certificat du format **.pfx** en format **.pem**, utilisez s'il vous plaît la syntaxe suivante d'OpenSSL.

Après conversion du certificat en format correct, le certificat et la clé privée correspondante dans le format **.pem** devraient être présents. Il est important d'avoir le certificate **et la** clé privée

disponibles. Seulement le certificate sans clé privée ne peut pas être importé dans SMA. Il est recommandé pour signer le certificat d'une autorité de confiance de certification (CA). Cisco ne recommande pas une particularité CA. Pour signer « **la demande de signature de certificat de téléchargement** » choisie sur le GUI de l'ESA et soumettez-le au CA de confiance du choix.

Certificat d'importation à SMA - Option 1

Le certificat signé CA ou le certificat signé d'individu et la clé privée dans .pem formatent, peuvent être importés maintenant dans le SMA. Pour apprendre comment le faire, lisez s'il vous plaît TechNote « comment j'installe des Certificats sur un SMA ? » comme référé ci-dessous.

Certificat d'importation à SMA - Option 2

Au lieu de convertir le certificat de .pfx en .pem vous pouvez simplement sauvegarder un wihtout de fichier de configuration masquant les mots de passe sur l'ESA. Ouvrez le fichier XML et recherchez la balise de <certificate>. Vous trouverez le certificat et la clé privée déjà dans le format PEM. Copiez le certificat et la clé privée pour importer la même chose dans le SMA comme décrit dans TechNote « comment j'installe des Certificats sur un SMA ? » comme référé ci-dessous.

Remarque: Si vous allez chercher l'option 2 et si vous faites signer le certificat par un CA vous le premier besoin d'importer le certificat signé de nouveau à l'ESA avant d'enregistrer le fichier de configuration pour tirer une copie du certificat et de la clé privée. L'importation peut être faite en cliquant sur sur le nom de certificat en GUI et option « certificat signé ESA d'utilisation de téléchargement ».

Vérifiez le certificat importé

1. Accédez au GUI SMA par l'intermédiaire de HTTPS (IP de https:// <SMA ou hostname>) et mettez en vos qualifications
2. À côté de l'URL dans la barre d'adresses sur votre navigateur, cliquez sur la validité d'icône et de contrôle de verrouillage du certificat, de l'échéance, etc.
3. Cliquez sur en fonction le chemin de certification pour vérifier la chaîne des Certificats

[Informations connexes](#)

- [Comment est-ce que j'installe des Certificats sur un SMA ?](#)
- [Convertisseur en ligne SSL](#)