Générer et configurer des certificats auto-signés pour ESA/SMA SAML SSO

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Problème

Résolution

- Méthode 1 : Créer et exporter un certificat auto-signé dans l'interface utilisateur Web de l'ESA
- Méthode 2 : Utiliser la commande OpenSSL pour créer une paire certificat/clé auto-signée

Informations connexes

Introduction

Ce document décrit comment créer des certificats auto-signés pour la configuration du fournisseur de services SAML (Security Assertion Markup Language).

Conditions préalables

Utilisez ce document pour générer des certificats auto-signés pour la configuration du fournisseur de services (SP) SSO (Single Sign-On) SAML (Security Assertion Markup Language) 2.0 sur l'appliance de sécurité de la messagerie (ESA) et l'appliance de gestion de la sécurité (SMA).

Exigences

Méthode 1 (interface utilisateur Web ESA) : Accès administratif ESA dans l'interface utilisateur Web et autorisation de gérer les certificats.

Méthode 2 (commande OpenSSL) : OpenSSL installé et disponible à partir de la ligne de commande.

Fenêtres: Installez OpenSSL.

macOS, Linux ou Unix : OpenSSL est généralement disponible par défaut ou via le gestionnaire de package du système d'exploitation.

Composants utilisés

Il n'existe pas de configuration matérielle ou logicielle spécifique.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Ce document s'applique aux déploiements d'appareils de sécurité de la messagerie électronique (ESA) et d'appareils de gestion de la sécurité (SMA) qui utilisent le langage SAML (Security Assertion Markup Language) 2.0 SSO (Single Sign-On). La configuration du fournisseur de services SAML nécessite des certificats SSL (Secure Sockets Layer) pour la configuration du fournisseur de services. Les certificats peuvent provenir d'outils de certificats internes, d'une autorité de certification (CA) ou d'un certificat auto-signé.

Problème

Des certificats auto-signés sont requis dans certains déploiements de SP SAML pour ESA et SMA. Ce document décrit comment créer le certificat et la clé privée, et éventuellement chiffrer la clé privée avec une phrase de passe.

Résolution

- Sous Windows, installez OpenSSL pour Windows. Des didacticiels sont disponibles en ligne avec des instructions sur la façon de le faire.
- Sous Unix, macOS et Linux, OpenSSL est généralement disponible par défaut.
- Utilisez la méthode d'interface utilisateur Web ESA lorsque ESA gère déjà le certificat et que le certificat doit être exporté pour une utilisation par le fournisseur de services SAML.
- Utilisez la méthode de commande OpenSSL lorsqu'un certificat et une paire de clés doivent être créés directement à partir de la ligne de commande.

Méthode 1 : Créer et exporter un certificat auto-signé dans l'interface utilisateur Web de l'ESA

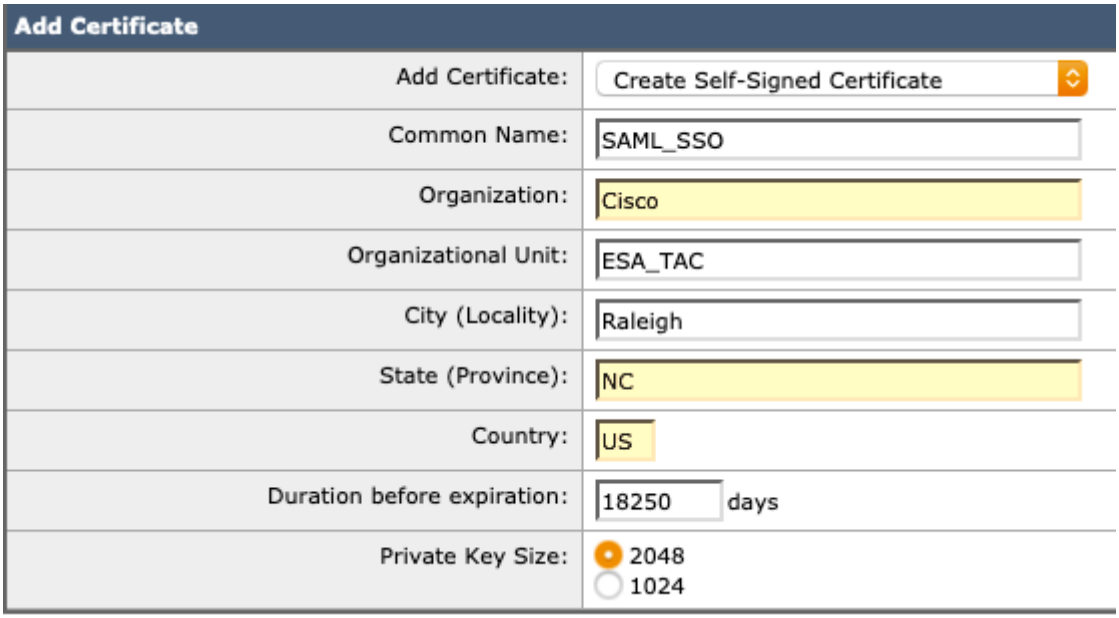
Utilisez cette méthode lorsque ESA gère déjà le certificat et que le certificat doit être exporté pour une utilisation SAML SP.

Créez le certificat.

1. Dans l'interface utilisateur Web ESA, accédez à Réseau > Certificats. Sélectionnez Ajouter un certificat, puis Créer un certificat auto-signé.

2. Renseignez les champs du modèle : Nom commun, organisation, unité organisationnelle, ville, état, pays et durée (1 à 18250 jours).

3. Définissez la taille de la clé privée sur 2048.



Modèle de certificat auto-signé complet

4. Soumettez le certificat, vérifiez le résultat et sélectionnez Valider les modifications.

Certificate Name:	SAML_SSO
Common Name:	SAML_SSO
Organization:	Cisco
Organization Unit:	ESA_TAC
City (Locality):	Raleigh
State (Province):	NC
Country:	US
Signature Issued By:	Common Name (CN): SAML_SSO Organization (O): Cisco Organizational Unit (OU): ESA_TAC Issued On: Sep 20 15:50:27 2019 GMT Expires On: Sep 7 15:50:27 2069 GMT

Affichage après configuration

Exportez le certificat.

1. Dans l'interface utilisateur Web ESA, accédez à Réseau > Certificats > Exporter le certificat.

2. Sélectionnez le certificat à exporter, créez une phrase de passe, sélectionnez Export, et enregistrez le fichier dans un répertoire.

Remarque : SAML SSO for Administration peut importer des certificats PKCS#12 (PFX). Si le chiffrement par clé privée n'est pas requis, les étapes de conversion restantes sont facultatives.

Convertissez le certificat.

Le certificat exporté est au format PKCS#12/PFX et doit être converti en PEM (Privacy-Enhanced Mail).

Exécutez cette commande OpenSSL pour convertir le fichier PFX au format PEM.

<#root>

openssl

```
 pkcs12 -in <certname>.pfx -nokeys -out cert.pem -nodes
```

<#root>

openssl

```
 pkcs12 -in SAML_SSO.pfx -out UNIX_FULL.pem -nodes
```

Modifiez le contenu et fractionnez le résultat en deux fichiers.

1. Le fichier nouvellement converti nécessite une modification mineure.

2. Ouvrez deux fichiers vides dans un éditeur de texte et nommez-les <name>.crt et <name>.key.

3. Copiez la section -----BEGIN CERTIFICATE----- à -----END CERTIFICATE----- du fichier converti.

4. Collez le contenu dans le <name>.crt et enregistrez-le.

5. Copiez la section -----BEGIN PRIVATE KEY----- à -----END PRIVATE KEY----- du fichier converti.

6. Collez le contenu dans le fichier <name>.key et enregistrez-le.

7. Le certificat et la clé peuvent maintenant être chargés dans la partie SP SAML de la configuration.

Méthode 2 : Utiliser la commande OpenSSL pour créer une paire certificat/clé auto-signée

Utilisez cette méthode lorsqu'un certificat et une paire de clés doivent être créés directement à partir de la ligne de commande.

Créez la paire certificat/clé.

Exécutez la commande OpenSSL dans une interface de ligne de commande Unix, Linux ou

macOS. Remplacez domain par le nom requis.

<#root>

openssl

```
 req -newkey rsa:2048 -nodes -keyout domain.key -x509 -days 1095 -out domain.crt
```

Lors de la création, des invites s'affichent pour les champs répertoriés.

Deux fichiers sont générés dans le répertoire d'exécution de la commande : saml_ssl.crt et saml_ssl.key.

```
$ openssl req -newkey rsa:2048 -nodes -keyout saml_sso.key -x509 -days 1095 -out saml_sso.crt
Generating a 2048 bit RSA private key
..........+++
.....................................................................................................
writing new private key to 'saml_sso.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:NC
Locality Name (for example, city) []:Raleigh
Organization Name (for example, company) []:Cisco
Organizational Unit Name (for example, section) []:ESA_TAC
Common Name (for example, fully qualified host name) []:SAML_SSO
Email Address []:user@example.com
```

Chiffrer la clé privée (facultatif ; non requis pour la configuration).

Remarque : Ne réutilisez pas les exemples de phrases de passe. Cette clé n'est utilisée qu'à titre d'exemple.

Cette commande OpenSSL prend une clé privée non chiffrée (unencryption.key) et génère une clé chiffrée (encryption.key) :

<#root>

```
openssl

 rsa -des3 -in unencrypted.key -out encrypted.key
```

<#root>

```
openssl

 rsa -des3 -in saml_sso.key -out saml_secure.key
```

```
$ openssl rsa -des3 -in saml_sso.key -out saml_secure.key
writing RSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:


$ ls

saml_sso.crt
saml_sso.key
saml_secure.key
```

Le certificat et la clé sont prêts pour la configuration de SAML SSO SP ou Spam SSO SP.

Informations connexes

[Appliance de sécurisation de la messagerie Cisco - Guides de l'utilisateur final]

[Cisco Content Security Management Appliance - Guides d'utilisation]

[Cisco Web Security - Guides d'utilisation]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.