Generieren und Konfigurieren von selbstsignierten Zertifikaten für ESA/SMA SAML SSO

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie selbstsignierte Zertifikate für die Konfiguration eines SAML (Security Assertion Markup Language)-Service Providers (SP) erstellt werden.

Voraussetzungen

Verwenden Sie dieses Dokument, um selbstsignierte Zertifikate für die Konfiguration von Security Assertion Markup Language (SAML) 2.0 Single Sign-On (SSO) Service Provider (SP) auf Email Security Appliance (ESA) und Security Management Appliance (SMA) zu generieren.

Anforderungen

Methode 1 (ESA Web UI): Administratorzugriff der ESA auf die Webbenutzeroberfläche und Berechtigung zum Verwalten von Zertifikaten.

Methode 2 (OpenSSL-Befehl): OpenSSL ist installiert und über die Befehlszeile verfügbar.

Windows: OpenSSL installieren

macOS, Linux oder Unix: OpenSSL ist normalerweise standardmäßig oder über den Paketmanager des Betriebssystems verfügbar.

Verwendete Komponenten

Spezifische Hardware- und Softwareanforderungen bestehen nicht.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Dieses Dokument gilt für Bereitstellungen von E-Mail Security Appliances (ESAs) und Security Management Appliances (SMAs), die SAML 2.0 Single Sign-On (SSO) verwenden. Für die SAML-SP-Konfiguration sind SSL-Zertifikate (Secure Sockets Layer) für die Dienstanbieter-Konfiguration erforderlich. Zertifikate können aus internen Zertifikatstools, einer Zertifizierungsstelle (Certificate Authority, CA) oder einem selbstsignierten Zertifikat stammen.

Problem

In einigen SAML-SP-Bereitstellungen für die ESA und SMA sind selbstsignierte Zertifikate erforderlich. In diesem Dokument wird beschrieben, wie Sie das Zertifikat und den privaten Schlüssel erstellen und optional den privaten Schlüssel mit einer Passphrase verschlüsseln.

Auflösung

- Installieren Sie unter Windows OpenSSL für Windows. Online stehen Tutorials mit Anleitungen zur Verfügung.
- Unter Unix, macOS und Linux ist OpenSSL in der Regel standardmäßig verfügbar.
- Verwenden Sie die ESA-Webbenutzeroberflächenmethode, wenn die ESA das Zertifikat bereits verwaltet und das Zertifikat für die Verwendung durch SAML SP exportiert werden muss.

- Verwenden Sie die OpenSSL-Befehlsmethode, wenn ein Zertifikat und ein Schlüsselpaar direkt über die Befehlszeile erstellt werden müssen.

Methode 1: Erstellen und Exportieren eines selbstsignierten Zertifikats in der ESA-Weboberfläche

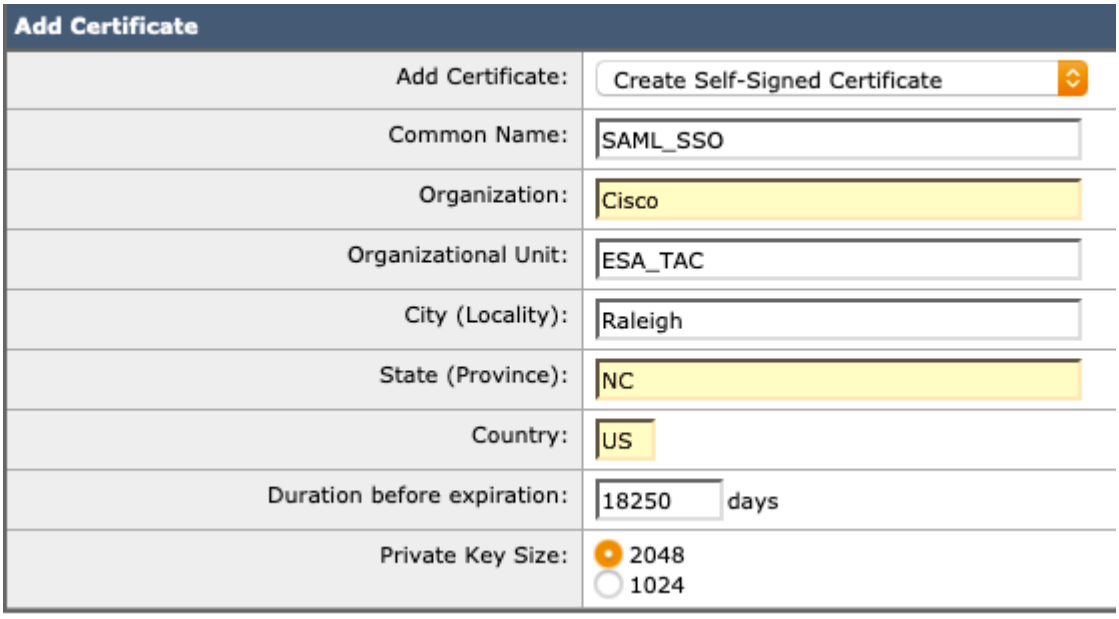
Verwenden Sie diese Methode, wenn die ESA das Zertifikat bereits verwaltet und das Zertifikat für die Verwendung durch SAML SP exportiert werden muss.

Zertifikat erstellen.

1. Navigieren Sie in der ESA Web UI zu Network > Certificates (Netzwerk > Zertifikate). Wählen Sie Zertifikat hinzufügen und anschließend Selbst signiertes Zertifikat erstellen aus.

2. Geben Sie die Vorlagenfelder ein: Common Name, Organization, Organizational Unit, City, State, Country, and Duration (1-18250 Tage).

3. Legen Sie die Größe des privaten Schlüssels auf 2048 fest.



Vollständige selbstsignierte Zertifikatvorlage

4. Senden Sie das Zertifikat, überprüfen Sie das Ergebnis, und wählen Sie Änderungen

bestätigen.

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

Nach Konfiguration anzeigen

Exportieren Sie das Zertifikat.

1. Navigieren Sie in der ESA-Webbenutzeroberfläche zu Netzwerk > Zertifikate > Zertifikat exportieren.

2. Wählen Sie das zu exportierende Zertifikat, erstellen Sie eine Passphrase, wählen Sie Exportieren aus, und speichern Sie die Datei in einem Verzeichnis.

Anmerkung: SAML SSO for Administration kann PKCS#12 (PFX)-Zertifikate importieren. Wenn keine Verschlüsselung mit privatem Schlüssel erforderlich ist, sind die übrigen Konvertierungsschritte optional.

Konvertieren Sie das Zertifikat.

Das exportierte Zertifikat ist im PKCS#12/PFX-Format und muss in Privacy-Enhanced Mail (PEM) konvertiert werden.

Führen Sie diesen OpenSSL-Befehl aus, um die PFX-Datei in das PEM-Format zu konvertieren.

<#root>

openssl

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

<#root>

openssl

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

Bearbeiten Sie den Inhalt, und teilen Sie die Ausgabe in zwei Dateien.

1. Die neu konvertierte Datei muss nur geringfügig bearbeitet werden.

2. Öffnen Sie zwei leere Dateien in einem Texteditor, und nennen Sie sie <name>.crt und <name>.key.

3. Kopieren Sie den Abschnitt -----BEGIN CERTIFICATE----- bis -----END CERTIFICATE----- aus der konvertierten Datei.

4. Fügen Sie den Inhalt in die <name>.crt-Datei ein, und speichern Sie sie.

5. Kopieren Sie den Abschnitt -----BEGIN PRIVATE KEY----- bis -----END PRIVATE KEY----- aus der konvertierten Datei.

6. Fügen Sie den Inhalt in die <name>.key-Datei ein und speichern Sie sie.

7. Das Zertifikat und der Schlüssel können nun in den SAML-SP-Teil der Konfiguration geladen werden.

Methode 2: Verwenden Sie den OpenSSL-Befehl, um ein selbstsigniertes Zertifikat und ein Schlüsselpaar zu erstellen.

Verwenden Sie diese Methode, wenn ein Zertifikat- und Schlüsselpaar direkt über die Befehlszeile erstellt werden muss.

Erstellen Sie das Zertifikat- und Schlüsselpaar.

Führen Sie den OpenSSL-Befehl in einer Unix-, Linux- oder macOS-Befehlszeilenschnittstelle aus. Ersetzen Sie die Domäne durch den erforderlichen Namen.

<#root>

openssl

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

Während der Erstellung werden Eingabeaufforderungen für die aufgeführten Felder angezeigt.

In dem Verzeichnis, in dem der Befehl ausgeführt wird, werden zwei Dateien generiert: saml_ssl.crt und 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
```

Verschlüsseln des privaten Schlüssels (optional; für die Konfiguration nicht erforderlich).

Anmerkung: Verwenden Sie keine Beispiel-Passphrasen erneut. Dieser Schlüssel dient nur als Beispiel.

Dieser OpenSSL-Befehl verwendet einen unverschlüsselten privaten Schlüssel (unencrypted.key)

und gibt einen verschlüsselten Schlüssel (encrypted.key) aus:

<#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
```

Zertifikat und Schlüssel sind bereit für die Einrichtung von SAML SSO SP oder Spam SSO SP.

Zugehörige Informationen

Cisco Email Security Appliance – Endbenutzerhandbücher

Cisco Content Security Management Appliance - Benutzerhandbücher

Cisco Web Security - Benutzerhandbücher

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.