Zelf ondertekende certificaten genereren en configureren voor ESA/SMA SAML SSO

Inhoud

Inleiding

In dit document wordt beschreven hoe u zelf ondertekende certificaten kunt maken voor de configuratie Security Assertion Markup Language (SAML) Service Provider (SP).

Voorwaarden

Gebruik dit document om zelf ondertekende certificaten te genereren voor de configuratie Security Assertion Markup Language (SAML) 2.0 Single Sign-On (SSO) Service Provider (SP) op de apparaten E-mail Security Appliance (ESA) en Security Management Appliance (SMA).

Vereisten

Methode 1 (ESA Web UI): administratieve toegang van ESA in de Web UI en toestemming om certificaten te beheren.

Methode 2 (OpenSSL-opdracht): OpenSSL geïnstalleerd en beschikbaar vanaf de opdrachtregel.

Windows: OpenSSL installeren.

macOS, Linux of Unix: OpenSSL is meestal standaard beschikbaar of via de pakketbeheerder van het besturingssysteem.

Gebruikte componenten

Er zijn geen specifieke hardware- en softwarevereisten.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document is van toepassing op implementaties van het Email Security Appliance (ESA) en het Security Management Appliance (SMA) die gebruikmaken van Security Assertion Markup Language (SAML) 2.0 Single Sign-On (SSO). Voor de configuratie van SAML SP zijn SSL-certificaten (Secure Sockets Layer) vereist voor de configuratie van de Serviceverlener. Certificaten kunnen afkomstig zijn van interne certificaattools, een certificeringsinstantie (CA) of een zelf ondertekend certificaat.

Probleem

In sommige SAML SP-implementaties voor ESA en SMA zijn zelfondertekende certificaten vereist. In dit document wordt beschreven hoe u het certificaat en de privésleutel kunt maken en de privésleutel optioneel kunt coderen met een wachtwoordgroep.

resolutie

- Installeer OpenSSL voor Windows. Er zijn online tutorials beschikbaar met instructies over hoe dit te doen.
- Op Unix, macOS en Linux is OpenSSL standaard beschikbaar.
- Gebruik de ESA Web UI-methode wanneer ESA het certificaat al beheert en het certificaat moet worden geëxporteerd voor gebruik met SAML SP.
- Gebruik de opdrachtregelmethode OpenSSL wanneer een certificaat en sleutelpaar rechtstreeks vanaf de opdrachtregel moeten worden gemaakt.

Methode 1: Een zelfondertekend certificaat maken en exporteren in de ESA Web UI

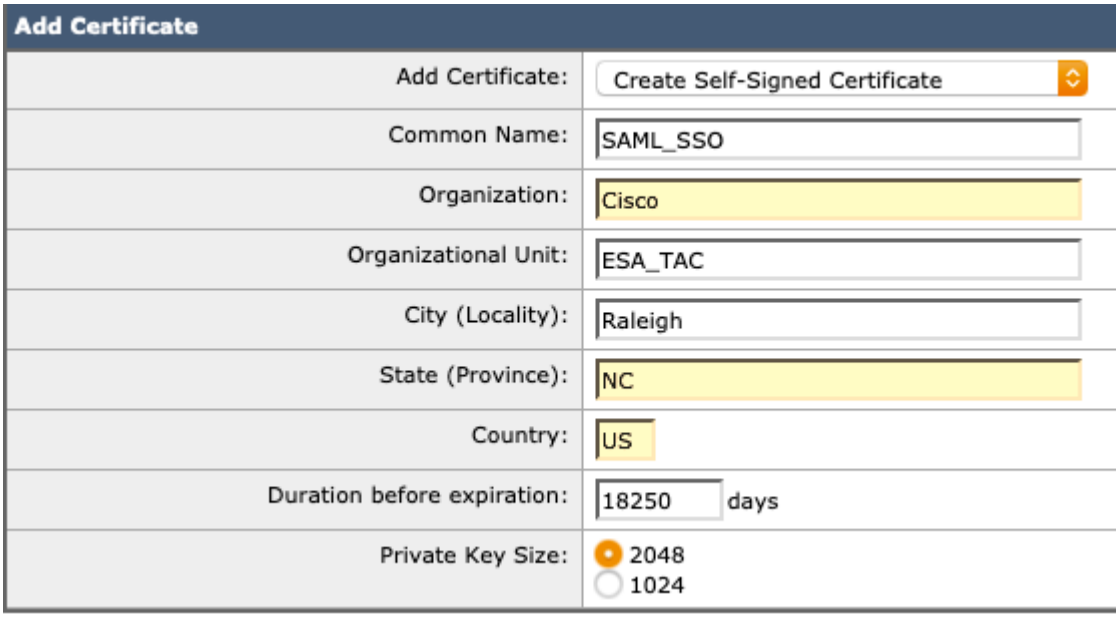
Gebruik deze methode wanneer ESA het certificaat al beheert en het certificaat moet worden geëxporteerd voor gebruik met SAML SP.

Maak het certificaat aan.

1. Ga in de ESA Web UI naar Netwerk > Certificaten. Selecteer Certificaat toevoegen en selecteer Zelf ondertekend certificaat maken.

2. Voer de velden in: Algemene naam, organisatie, organisatorische eenheid, stad, staat, land en duur (1-18250 dagen).

3. Stel de grootte van de privésleutel in op 2048.



Volledige zelf ondertekende certificaatsjabloon

4. Dien het certificaat in, bekijk het resultaat en selecteer Wijzigingen vastleggen.

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

Bekijken na configuratie

Exporteer het certificaat.

1. Navigeer in de ESA Web UI naar Netwerk > Certificaten > Exportcertificaat.

2. Selecteer het certificaat dat u wilt exporteren, maak een wachtwoordgroep, selecteer Exporteren en sla het bestand op in een directory.

Opmerking: SAML SSO for Administration kan PKCS#12 (PFX)-certificaten importeren. Als codering met een privésleutel niet vereist is, zijn de overige conversiestappen optioneel.

Converteer het certificaat.

Het geëxporteerde certificaat heeft de PKCS#12/PFX-indeling en moet worden omgezet naar Privacy-Enhanced Mail (PEM).

Voer deze OpenSSL-opdracht uit om het PFX-bestand naar PEM-indeling te converteren.

<#root>

openssl

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

<#root>

openssl

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

Bewerk de inhoud en verdeel de uitvoer in twee bestanden.

1. Voor het nieuw geconverteerde bestand zijn kleine bewerkingen nodig.

2. Open twee lege bestanden in een teksteditor en noem ze <name>.crt en <name>.key.

3. Kopieer de sectie -----BEGIN CERTIFICATE----- through ----END CERTIFICATE----- uit het geconverteerde bestand.

4. Plak de inhoud in het <name>.crt bestand en sla het op.

5. Kopieer de sectie -----BEGIN PRIVATE KEY----- through ----END PRIVATE KEY------ uit het geconverteerde bestand.

6. Plak de inhoud in het <name>.key bestand en sla het op.

7. Het certificaat en de sleutel kunnen nu worden geladen in het SAML SP-gedeelte van de configuratie.

Methode 2: Gebruik de opdracht OpenSSL om een zelf ondertekend certificaat en sleutelpaar te maken

Gebruik deze methode wanneer een certificaat en sleutelpaar rechtstreeks vanaf de opdrachtregel moeten worden gemaakt.

Maak het certificaat en het sleutelpaar.

Voer de opdracht OpenSSL uit in een Unix-, Linux- of macOS-opdrachtregelinterface. Vervang het

domein door de gewenste naam.

<#root>

openssl

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

Tijdens het maken worden vragen voor de vermelde velden weergegeven.

Er worden twee bestanden gegenereerd in de directory waarin de opdracht wordt uitgevoerd: saml_ssl.crt en 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
```

Codeer de persoonlijke sleutel (optioneel; niet vereist voor configuratie).

Opmerking: voorbeeldwachtwoordgroepen niet opnieuw gebruiken. Deze sleutel is alleen voor bijvoorbeeld doeleinden.

Deze OpenSSL-opdracht neemt een niet-gecodeerde privésleutel (unencrypted.key) en voert een gecodeerde sleutel (encrypted.key) uit:

<#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
```

Het certificaat en de sleutel zijn klaar voor de SAML SSO SP- of Spam SSO SP-installatie.

Gerelateerde informatie

Cisco e-mail security applicatie – eindgebruikershandleiding

Cisco Content Security Management Appliance - Handleidingen voor eindgebruikers

Cisco Web Security - Handleidingen voor eindgebruikers

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.