# Generar y configurar certificados autofirmados para SSO SAML ESA/SMA

## Contenido



## Introducción

Este documento describe cómo crear certificados autofirmados para la configuración del proveedor de servicios (SP) del lenguaje de marcado de aserción de seguridad (SAML).

## Prerequisites

Utilice este documento para generar certificados autofirmados para la configuración del proveedor de servicios (SP) de inicio de sesión único (SSO) del lenguaje de marcado de aserción de seguridad (SAML) 2.0 en el dispositivo de seguridad Email Security Appliance (ESA) y el dispositivo de administración de seguridad (SMA).

### Requirements

Método 1 (ESA Web UI): Acceso administrativo ESA en la interfaz de usuario web y permiso para administrar certificados.

Método 2 (comando OpenSSL): OpenSSL instalado y disponible desde la línea de comandos.

Windows: Instale OpenSSL.

macOS, Linux o Unix: OpenSSL suele estar disponible de forma predeterminada o a través del administrador de paquetes del sistema operativo.

### Componentes Utilizados

No existen requisitos específicos de hardware y software.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

Este documento se aplica a las implementaciones de Email Security Appliance (ESA) y Security Management Appliance (SMA) que utilizan el inicio de sesión único (SSO) de Lenguaje de marcado de aserción de seguridad (SAML) 2.0. La configuración de SAML SP requiere certificados de Secure Sockets Layer (SSL) para la configuración del proveedor de servicios. Los certificados pueden proceder de herramientas de certificados internas, una entidad de certificación (CA) o un certificado autofirmado.

## Problema

Se requieren certificados autofirmados en algunas implementaciones de SAML SP para ESA y SMA. Este documento describe cómo crear el certificado y la clave privada, y opcionalmente cifrar la clave privada con una frase de contraseña.

## Resolución

- En Windows, instale OpenSSL para Windows. Hay tutoriales disponibles en línea con instrucciones sobre cómo hacerlo.
- En Unix, macOS y Linux, OpenSSL suele estar disponible de forma predeterminada.
- Utilice el método de interfaz de usuario web ESA cuando ESA ya administre el certificado y el certificado se debe exportar para el uso de SAML SP.
- Utilice el método de comando OpenSSL cuando se deba crear un certificado y un par de claves directamente desde la línea de comandos.

## Método 1: Crear y exportar un certificado autofirmado en la interfaz de usuario web de ESA

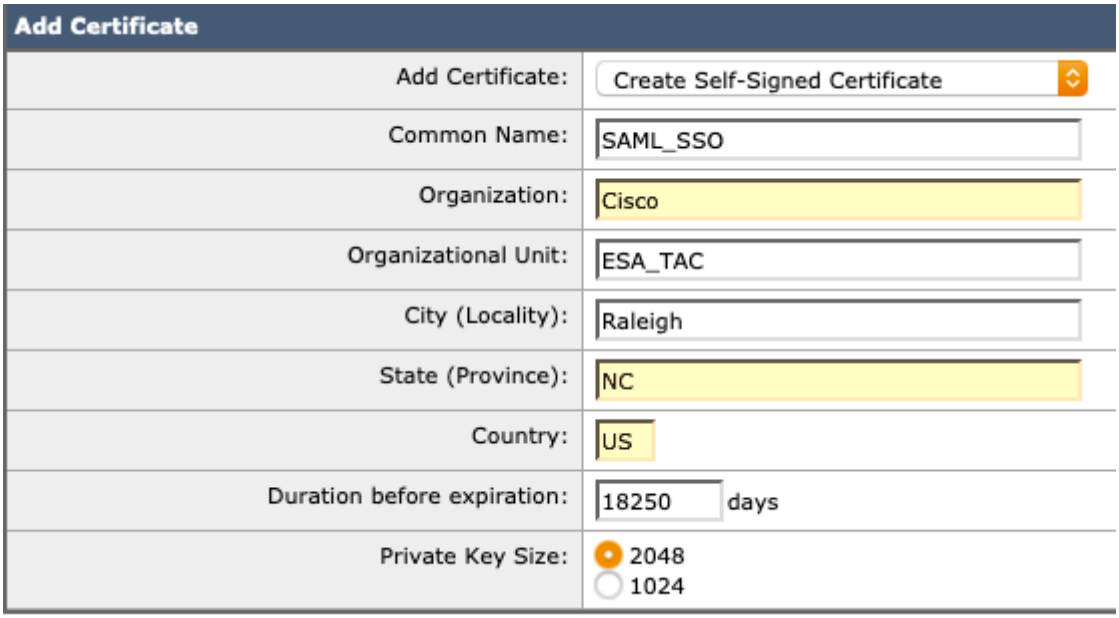
Utilice este método cuando el ESA ya administre el certificado y éste se deba exportar para el uso de SAML SP.

Cree el certificado.

1. En la interfaz de usuario web de ESA, navegue hasta Red > Certificados. Seleccione Agregar certificado y, a continuación, Seleccione Crear certificado autofirmado.

2. Introduzca los campos de plantilla: Nombre común, organización, unidad organizativa, ciudad, estado, país y duración (de 1 a 18250 días).

3. Establezca el tamaño de la clave privada en 2048.




Plantilla de certificado autofirmado completa

4. Ejecute el certificado, revise el resultado y seleccione Registrar Cambios.

| | |
|---|---|
| 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<br>Organization (O): Cisco<br>Organizational Unit (OU): ESA_TAC<br>Issued On: Sep 20 15:50:27 2019 GMT<br>Expires On: Sep 7 15:50:27 2069 GMT |

Ver tras configuración

Exporte el certificado.

1. En la interfaz de usuario web de ESA, navegue hasta Red > Certificados > Certificado de exportación.

2. Seleccione el certificado que desea exportar, cree una frase de paso, seleccione Exportar y guarde el archivo en un directorio.

---

Nota: SAML SSO for Administration puede importar certificados PKCS#12 (PFX). Si no se requiere el cifrado de clave privada, los pasos restantes de la conversión son opcionales.

---

Convertir el certificado.

El certificado exportado está en formato PKCS#12/PFX y requiere conversión a Privacy-Enhanced Mail (PEM).

Ejecute este comando OpenSSL para convertir el archivo PFX al formato PEM.

<#root>

**openssl**

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

<#root>

**openssl**

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

Edite el contenido y divida el resultado en dos archivos.

1. El archivo recién convertido requiere una edición menor.

2. Abra dos archivos en blanco en un editor de texto y denomínelos <name>.crt y <name>.key.

3. Copie la sección -----BEGIN CERTIFICATE----- a -----END CERTIFICATE----- del archivo convertido.

4. Pegue el contenido en el <name>.crt file y guárdelo.

5. Copie la sección -----BEGIN PRIVATE KEY----- a -----END PRIVATE KEY----- del archivo convertido.

6. Pegue el contenido en el archivo <name>.key y guárdelo.

7. El certificado y la clave se pueden cargar ahora en la parte SP de SAML de la configuración.

## Método 2: Utilice el comando OpenSSL para crear un certificado y un par de claves autofirmados

Utilice este método cuando se deba crear un certificado y un par de claves directamente desde la línea de comandos.

Cree el certificado y el par de claves.

Ejecute el comando OpenSSL en una interfaz de línea de comandos de Unix, Linux o macOS. Reemplace domain con el nombre requerido.

<#root>

**openssl**

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

Durante la creación, se muestran mensajes para los campos enumerados.

Se generan dos archivos en el directorio donde se ejecuta el comando: saml_ssl.crt y 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
```

Cifrar la clave privada (opcional; no es necesario para la configuración).

---

Nota: No reutilice frases de contraseña de ejemplo. Esta clave es solo para fines de ejemplo.

---

Este comando OpenSSL toma una clave privada no cifrada (unencryption.key) y genera una clave cifrada (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
```

El certificado y la clave están listos para la configuración de SAML SSO SP o Spam SSO SP.

## Información Relacionada

Dispositivo de seguridad Cisco Email Security Appliance: guías del usuario final

Cisco Content Security Management Appliance: Guías para el usuario final

Cisco Web Security: guías para el usuario final

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).