# Gerar e configurar certificados autoassinados para ESA/SMA SAML SSO

## Contents



## Introdução

Este documento descreve como criar certificados autoassinados para a configuração do provedor de serviços (SP) SAML (Security Assertion Markup Language).

## Pré-requisitos

Use este documento para gerar certificados autoassinados para a configuração do Provedor de Serviços (SP) do Security Assertion Markup Language (SAML) 2.0 Single Sign-On (SSO) no Email Security Appliance (ESA) e no Security Management Appliance (SMA).

### Requisitos

Método 1 (IU Web do ESA): Acesso administrativo do ESA na interface do usuário da Web e permissão para gerenciar certificados.

Método 2 (comando OpenSSL): OpenSSL instalado e disponível na linha de comando.

Windows: Instale o OpenSSL.

MacOS, Linux ou Unix: O OpenSSL geralmente está disponível por padrão ou através do gerenciador de pacotes do sistema operacional.

### Componentes Utilizados

Não há requisitos específicos de hardware e software.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

Este documento se aplica às implantações do Email Security Appliance (ESA) e do Security Management Appliance (SMA) que usam o Security Assertion Markup Language (SAML) 2.0 Single Sign-On (SSO). A configuração da controladora de armazenamento SAML requer certificados SSL (Secure Sockets Layer) para a instalação do Provedor de Serviços. Os certificados podem vir de ferramentas de certificado internas, uma CA (autoridade de certificação) ou um certificado autoassinado.

## Problema

Certificados autoassinados são necessários em algumas implantações de SAML SP para ESA e SMA. Este documento descreve como criar o certificado e a chave privada e, opcionalmente, criptografar a chave privada com uma senha.

## Resolução

- No Windows, instale o OpenSSL para Windows. Há tutoriais disponíveis on-line com instruções sobre como fazer isso.
- Em Unix, macOS e Linux, o OpenSSL normalmente está disponível por padrão.
- Use o método de interface do usuário da Web do ESA quando o ESA já gerenciar o certificado e este deve ser exportado para uso da controladora SAML.
- Use o método de comando OpenSSL quando um certificado e um par de chaves precisarem ser criados diretamente da linha de comando.

## Método 1: Criar e exportar um certificado autoassinado na interface de usuário da Web do ESA

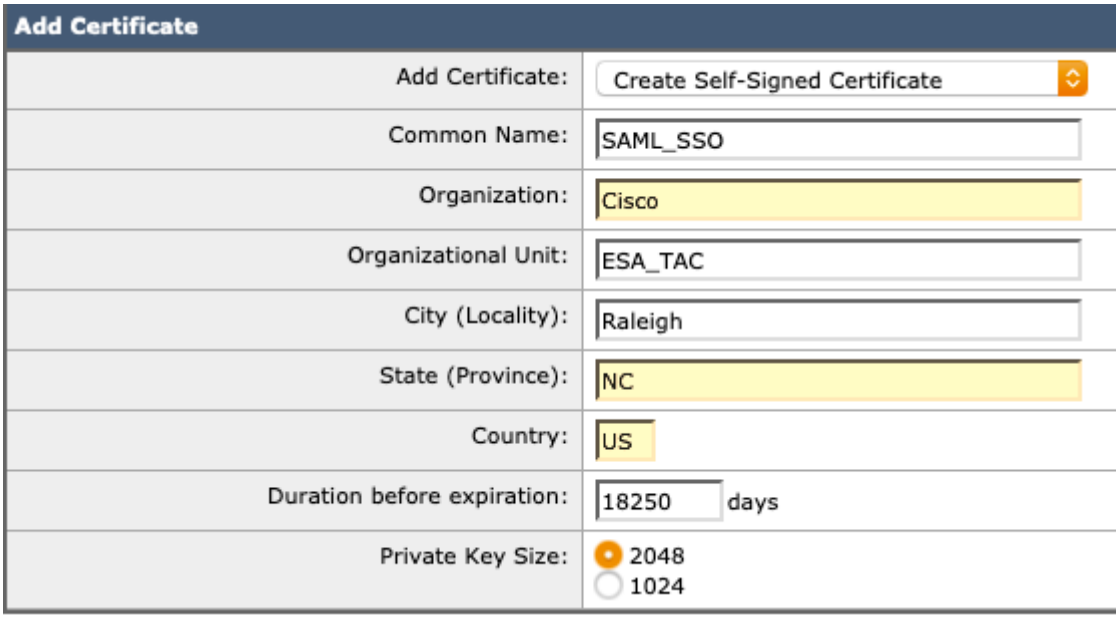
Use este método quando o ESA já gerenciar o certificado e o certificado precisar ser exportado para uso com a controladora SAML.

Crie o certificado.

1. Na IU da Web do ESA , navegue para Rede > Certificados. Selecione Adicionar certificado e, em seguida, selecione Criar certificado autoassinado.

2. Informe os campos de modelo: Nome comum, Organização, Unidade organizacional, Cidade, Estado, País e Duração (1 a 18250 dias).

3. Defina o Tamanho da Chave Privada como 2048.




Concluir Modelo de Certificado Autoassinado

4. Submeta o certificado, revise o resultado e Selecione Confirmar Alterações.

| | |
|---|---|
| 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 |

Visualizar após configuração

Exporte o certificado.

1. Na interface do usuário da Web do ESA, navegue para Network > Certificates > Export Certificate.

2. Selecione o certificado a ser exportado, crie uma senha, selecione Exportar e salve o arquivo em um diretório.

---

Note: O SAML SSO for Administration pode importar certificados PKCS#12 (PFX). Se a criptografia de chave privada não for necessária, as etapas de conversão restantes serão opcionais.

---

Converta o certificado.

O certificado exportado está no formato PKCS#12/PFX e requer conversão para Privacy-Enhanced Mail (PEM).

Execute este comando OpenSSL para converter o arquivo PFX para o 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 o conteúdo e divida a saída em dois arquivos.

1. O arquivo recém-convertido requer uma pequena edição.

2. Abra dois arquivos em branco em um editor de texto e nomeie-os como <nome>.crt e <nome>.key.

3. Copie a seção -----BEGIN CERTIFICATE----- por meio de -----END CERTIFICATE----- do arquivo convertido.

4. Cole o conteúdo no arquivo <name>.crt e salve-o.

5. Copie a seção -----BEGIN PRIVATE KEY----- por -----END PRIVATE KEY----- do arquivo convertido.

6. Cole o conteúdo no arquivo <name>.key e salve-o.

7. O certificado e a chave agora podem ser carregados na parte SAML SP da configuração.

## Método 2: Usar o comando OpenSSL para criar um certificado autoassinado e um par de chaves

Use este método quando um certificado e um par de chaves precisarem ser criados diretamente da linha de comando.

Crie o certificado e o par de chaves.

Execute o comando OpenSSL em uma interface de linha de comando Unix, Linux ou macOS.

Substitua domain pelo nome necessário.

<#root>

**openssl**

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

Durante a criação, serão exibidos prompts para os campos listados.

Dois arquivos são gerados no diretório em que o comando é executado: saml_ssl.crt e 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
```

Criptografe a chave privada (opcional; não é necessário para a configuração).

---

Note: Não reutilize frases secretas de exemplo. Essa chave é apenas para fins de exemplo.

---

Este comando OpenSSL usa uma chave privada não criptografada (unencrypted.key) e gera uma chave criptografada (encrypted.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
```

O certificado e a chave estão prontos para a configuração da controladora de armazenamento SSO SAML ou da controladora de armazenamento SSO Spam.

# Informações Relacionadas

Cisco Email Security Appliance – Guias do usuário final

Dispositivo de gerenciamento de segurança de conteúdo da Cisco - Guias do usuário final

Cisco Web Security - Guias do usuário final

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.