Cómo generar y instalar un certificado en un S A

Contenido

[Introducción](#)
[prerrequisitos](#)
[Cómo generar y instalar un certificado en un S A](#)
[Cree y certificado de exportación de un ESA](#)
[Convierta el certificado exportado](#)
[Cree el certificado con el OpenSSL](#)
[Opción adcional, exportando un certificado de un ESA](#)
[Instale el certificado en el S A](#)
[Ejemplo:](#)
[Verifique el certificado importado y configurado en el S A](#)
[Información Relacionada](#)

Introducción

Este documento describe cómo generar y instalar un certificado para la configuración y el uso en un dispositivo de la Administración del Cisco Security (S A).

Prerequisites

Usted necesitará tener acceso para ejecutar el **openssl del** comando localmente.

Usted necesitará el acceso de la cuenta de administración a su dispositivo de seguridad del correo electrónico (ESA), y el acceso admin al CLI de su S A.

Usted debe tener estos elementos disponibles en el formato del .pem:

- Certificado X.509
- Clave privada que hace juego su certificado
- Cualquier Certificados intermedios proporcionados por su Certificate Authority (CA)

Cómo generar y instalar un certificado en un S A

> **Tip**: Se recomienda para hacer un certificado firmar por un CA de confianza Cisco no recomienda un CA específico dependiendo de CA que usted elige trabajar con, usted puede recibir detrás el certificado firmado, la clave privada, y el certificado intermedio (en caso pertinente) en los diversos formatos. Investigue o discuta por favor directamente con CA el formato del archivo que proporcionan a usted antes de instalar el certificado.

Actualmente, el S A no soporta la generación de un certificado localmente. En lugar, es posible generar un certificado autofirmado en el ESA. Esto se puede utilizar como solución alternativa para crear un certificado para el S A para ser importado y para ser configurado.

Cree y certificado de exportación de un ESA

1. Del ESA GUI, cree un certificado firmado del uno mismo del **certificado de la red > de los Certificados > Add**. Al crear el certificado autofirmado, es importante que el “Common Name (CN)” utilice el nombre de host del S A y no del ESA, para poder utilizar correctamente el certificado.
2. Someta y confíe los cambios.
3. Exporte el certificado creado de la **red > de los Certificados > de los Certificados de exportación**. Usted tiene dos opciones, (1) exportación y salvaguardia/uso como certificado autofirmado, o (2) pedido de firma de certificado de la descarga (si usted está necesitando hacer el certificado firmar externamente): Salve/uso como certificado autofirmado: Elija los **Certificados de exportación**Déle un nombre del archivo (e.g mycert.pfx) y el passphrase que sean utilizados al convertir el certificado.Esto le indicará automáticamente a que salve el archivo localmente.Proceda “a convertir el certificado exportado”.Descargue el pedido de firma de certificado **Red > Certificados**Haga clic en el nombre del certificado que usted creó.En la “firma publicada por” la sección, haga clic el **pedido de firma de certificado de la descarga…**Salve el archivo del .pem localmente y someta a CA.

Convierta el certificado exportado

El certificado creado y exportado del ESA estará en el formato del .pfx. El S A soporta solamente el formato del .pem para importar, así que este certificado necesitará ser convertido. Para convertir el certificado del formato del .pfx al formato del .pem, utilice por favor el comando example siguiente del **openssl**:

```
openssl pkcs12 -in mycert.pfx -out mycert.pem -nodes
```

Le indicarán para el passphrase usado mientras que crea el certificado del ESA. El archivo del .pem creado en el comando del openssl contendrá el certificado y la clave en el formato del .pem. El certificado está listo ahora para ser configurado en el S A. Procede por favor “instala la sección del certificado” de este artículo.

Cree el certificado con el OpenSSL

Alternativamente, si usted tiene Acceso local para ejecutar el **openssl de** su PC/workstation, usted puede publicar el siguiente comando de generar el certificado y de salvar el archivo y la clave privada necesarios del .pem en dos archivos distintos:

```
openssl req -newkey rsa:2048 -new -nodes -x509 -days 3650 -keyout sma_key.pem -out sma_cert.pem
```

El certificado está listo ahora para ser configurado en el S A. Procede por favor “instala la sección del certificado” de este artículo.

Opción adcional, exportando un certificado de un ESA

En vez de convertir el certificado del .pfx en el .pem, como se mencionó anteriormente, usted puede salvar un archivo de configuración sin el enmascarado de las contraseñas en el ESA. Abra el archivo de configuración y la búsqueda guardados del .xml ESA para la etiqueta del <certificate>. El certificado y la clave privada estarán ya en el formato del .pem. Copie el

certificado y la clave privada para importar lo mismo en el S A que describió “instala sección del certificado” abajo.

> **Note**: Si usted optó por #2 arriba, “descargue el pedido de firma de certificado”, y haga el certificado firmar por CA, usted necesitará importar el certificado firmado de nuevo al ESA que el certificado fue creado antes de guardar el archivo de configuración para hacer una copia del certificado y de la clave privada. La importación puede ser hecha haciendo clic en el nombre del certificado en ESA GUI y la opción “certificado firmado del uso de la carga”.

Instale el certificado en el S A

Un solo certificado se puede utilizar para todos los servicios, o un certificado individual se puede utilizar para cada uno de los cuatro servicios:

- TLS entrante
- TLS saliente
- HTTPS
- LDAPS

En el S A, registre en vía el CLI y complete los pasos siguientes:

1. Ejecute el **certconfig**.
2. Elija la opción de la **configuración**.
3. Usted necesitará elegir si utilizar el mismo certificado para todos los servicios, o utilizar los Certificados separados para cada servicio individual: ¿Cuando está presentado “lo haga usted quisieron utilizar una certificado/clave para recibir, la salida, el acceso de la administración de HTTPS, y LDAPS? ”, “Y de contestación” le requerirá solamente ingresar en el certificado y cerrar una vez, y después asignará ese certificado a todos los servicios.Si usted elige ingresar “N”, usted necesitará ingresar en el certificado, la clave, y el certificado intermedio (en caso pertinente) para cada servicio cuando está indicado: Entrante, saliente, HTTPS, y Administración
4. Cuando se le pregunte, pegue el certificado o ciérrelo.
5. Termine con '. 'en su propia línea para cada entrada para indicar que le hacen que pega el elemento actual. (Véase la sección del “ejemplo”.)
6. Si usted tiene un certificado intermedio, esté seguro de ingresarlo cuando está indicado para hacer tan.
7. Una vez que está completado, Presione ENTER para volver al prompt principal CLI del S A.
8. Ejecute el **cometer** para salvar la configuración.

> **Note**: No salga el comando del **certconfig** con el Ctrl+C puesto que esto cancela inmediatamente sus cambios.

Ejemplo:

```
mysma.local> certconfig

Currently using the demo certificate/key for receiving, delivery, HTTPS management access, and
LDAPS.
```

```
Choose the operation you want to perform:
- SETUP - Configure security certificates and keys.
[]> setup

Do you want to use one certificate/key for receiving, delivery, HTTPS management access, and
LDAPS? [Y]> y

paste cert in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAwIJAIXvIlkArow9MA0GCSqGSIb3DQEBBQUAMG4xCzAJBgNV
BAYTAlVTMRowGAYDVQQDDBF3dS5jYWxvLmNpc2NvLmNvbTEMMAoGA1UEBwwDUlRQ
MQ4wDAYDVQQKDAVDaXNjbzEXMBUGA1UECAwOTm9ydGggQ2Fyb2xpbmExDDAKBgNV
BAsMA1RBQzAeFw0xNzExMTAxNjA3MTRaFw0yNzExMDgxNjA3MTRaMG4xCzAJBgNV
BAYTAlVTMRowGAYDVQQDDBF3dS5jYWxvLmNpc2NvLmNvbTEMMAoGA1UEBwwDUlRQ
MQ4wDAYDVQQKDAVDaXNjbzEXMBUGA1UECAwOTm9ydGggQ2Fyb2xpbmExDDAKBgNV
BAsMA1RBQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKPz0perw3QA
ZH8xctOrvvjsnOPkItmSc+DUqtVKM6OOOkNHA2WY9XJ3+vESwkIdwexibj6VUQ85
K7NE6zOgRfpYdQsxmpIWhzYf9qCBOXuKsRw/9jonKk98DfHFM02J3BSmmgZ0MPp7
6EwA/sZAN+aqYB7IE1fgnqpEXek8xFlfcVnS2YTc7NXz78lNK0jvXOtCVBrWFu0z
lEmZVpAj0AKkz1nujvzfOqEzed+tjauZr7nDIaiTrzhLKte4pJUm3T61q/PhegvN
Iy/WHN1xojP+FzjRAUlmtmjMzHyM2///dmq8JivUlaLXX9vUfdK3VViIOIz4zngG
Rz85QXO7ivcCAwEAATANBgkqhkiG9w0BAQUFAAOCAQEAM10zCcOOtqV1LDBmoDqd
4G2IhVbBESsbvZ/QmB6kpikT4pe5clQucskHq4D/xg1EZyfuXu+4auMie4B9Dym8
8pjbMDDi9hJPZ7j85nWMd6SfWhQUOPankdazpCycN6gNVzRBgPdR8tLOvt90vtV4
KCPmDYbwi6kfOl8tvjWHMh/wYicfvFRy0vPMpemtbCVGyC3cpquv8nFDutB6exym
skotn5wixCqErKlnHdUa3Z+zhutIAm/Q0sVWQQlbZZ+MIxBegyJ0ucTmBqqQHhhJ
pSO7PbevxwanYVXvNR8o2feAWs5LYkrwqdGRxLJmHjFnMV3PbkwRPgFWQ6AD1g12
34==
-----END CERTIFICATE-----
.
paste key in PEM format (end with '.'):
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCj89KXq8N0AGR/
MXLTq7747Jzj5CLZknPg1KrVSjOjjjpDRwNlmPVyd/rxEsJCHcHsYm4+lVEPOSuz
ROszoEX6WHULMZqSFoc2H/aggTl7irEcP/Y6JypPfA3xxTNNidwUppoGdDD6e+hM
AP7GQDfmqmAeyBNX4J6qRF3pPMRZX3FZ0tmE3OzV8+/JTStI71zrQlQa1hbtM5RJ
mVaQI9ACpM9Z7o783zqhM3nfrY2rma+5wyGok684SyrXuKSVJt0+tavz4XoLzSMv
1hzdcaIz/hc40QFJZrZozMx8jNv//3ZqvCYr1JWi11/b1H3St1VYiDiM+M54Bkc/
OUFzu4r3AgMBAAECggEAB9EFjsaZHGwyXmAIpe/PvIVnW3QSd0YEsUjiViXh/V+4
BmIZ1tuqhAkVVS38RfOuPatZrzEmOrASlcro3b6751oVRnHYeTOKwblXZEKU739m
vz6Lai1Y1o5HCepJbl5uuCtTN5CNjzueERWRD/ma0Kv5xi3qwitK1TpKMeb8Q3h2
YABmpk0TyJQ5ixLw3ch9ru1nqiO5zQ91GvIuDckudUu/bBnao+jV7D362lIPyLG8
03GqNviNZ6c3wjD0yQWg619g+ZmjM8DTtDR16zmzBvQ4TgZi22sUWrSSILRa69jW
q8XszQVRydl+gt666iUeN/ozmEMt5J8pu3i9vf3G2QKBgQDHyfv55rjZbWyf0eAT
Ch5T1YsjjMgMOtC9ivi5mMQCunWyRiyZ6qqSBME9Tper/YdAA07PoNtTpVPYyuVX
DDmyuWGHE04baf5QEmSgvQjXOSUPN5TI9hc5/mtvD8QjDO6rebUWxV3NJoR7YNrz
OmfARMXxaF+/mEj+6blSjZuGaQKBgQDSFKvYownPL6qTFhIH7B3kOLwZHk6cJUau
Zoaj7vTw7LrVJv1B0iLPmttEXeJgxzlFYR8tzfn0kTxGQlnhQxXkQ1kdDeqaiLvm
0TtmHMDupjDNKCNH8yBPqB+BIA4cB+/vo23W1HMHpGgqYWRRX/qremL72XFZSRnM
B8nRwK4aXwKBgB+hkwtVxB5ofLIxAFEDYRnUzVqrh2CoTzQzNH3t+dqUut2mzpjv
1mGX7yBNuSW51hgEbg3hYdg0bLn+JaFKhjgNsas5Gzyr41+6CcSJKUUp/vwRyLSo
gbTk2w2SaXNDMOZlNo6MYPWCC6edBg1MSfDe8pft9nrXGXeCeZzgXqdBAoGAQ6Iq
DQ24O76h0Ma7OVe36+CkFgYe0sBheAZD9IUa0HG2WKc7w7QORv4Y93KuTe/1rTNu
YUW94hHb8Natrwr1Ak74YpU3YVcB/3Z/BAnfxzUz4ui4KxLH5T1AH0cdo8KeaW0Z
EJ/HBL/WVUaTkGsw/YHiWiiQCGmzZ29edyvsIUsCgYEAvJtx0ZBAJ443WeHajZWm
J2SLKy0KHeDxZOZ4CwF5sRGsmMofILbK0OuHjMirQ5U9HFLpcINt11VWwhOiZZ5l
k6o79mYhfrTMa4LlHOTyScvuxELqow82vdj6gqX0HVj4fUyrrZ28MiYOMcPw6Y12
34VjKaAsxgZIgN3LvoP7aXo=
-----END PRIVATE KEY-----
.
Do you want to add an intermediate certificate? [N]> n
```

```
Currently using one certificate/key for receiving, delivery, HTTPS management access, and LDAPS.


Choose the operation you want to perform:
- SETUP - Configure security certificates and keys.
- PRINT - Display configured certificates/keys.
- CLEAR - Clear configured certificates/keys.
[]>

mysma.local> commit

Please enter some comments describing your changes:
[]> Certificate installation

Changes committed: Fri Nov 10 11:46:07 2017 EST
```

Verifique el certificado importado y configurado en el S A

1. Conecte con el S A vía el GUI usando el HTTPS (IP de https:// <SMA u hostname>) y ingrese en sus credenciales del login.
2. Al lado del URL en la barra de dirección en su navegador, haga clic el icono o el icono de información del bloqueo para marcar la validez del certificado, del vencimiento, del etc. Dependiendo de qué navegador usted está utilizando, sus acciones y resultados pueden variar.
3. Haga clic en el trayecto de certificación para marcar el encadenamiento de los Certificados.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems