Cómo Generar e Instalar un Certificado en un SMA

Contenido

[Introducción](#)
[Prerequisites](#)
[Cómo Generar e Instalar un Certificado en un SMA](#)
[Crear y exportar certificado desde un ESA](#)
[Convertir el certificado exportado](#)
[Crear certificado con OpenSSL](#)
[Opción adicional, exportación de un certificado desde un ESA](#)
[Instalación del certificado en el SMA](#)
[Ejemplo:](#)
[Verifique el certificado importado y configurado en el SMA](#)
[Información Relacionada](#)

Introducción

Este documento describe cómo generar e instalar un certificado para su configuración y uso en un dispositivo de administración de seguridad (SMA) de Cisco.

Prerequisites

Deberá tener acceso para ejecutar el comando **openssl** localmente.

Necesitará acceso de cuenta de administrador a su dispositivo de seguridad Email Security Appliance (ESA) y acceso de administrador a la CLI de su SMA.

Debe tener estos elementos disponibles en formato .pem:

- certificado X.509
- Clave privada que coincide con el certificado
- Cualquier certificado intermedio proporcionado por su Autoridad de Certificación (CA)

Cómo Generar e Instalar un Certificado en un SMA

> **Consejo:** Se recomienda que una CA de confianza firme un certificado. Cisco no recomienda una CA específica. Dependiendo de la CA con la que elija trabajar, puede recibir de nuevo el certificado firmado, la clave privada y el certificado intermedio (si procede) en diversos formatos. Investigue o hable directamente con la CA el formato del archivo que le proporcione antes de instalar el certificado.

Actualmente, el SMA no admite la generación de un certificado localmente. En su lugar, es

posible generar un certificado autofirmado en el ESA. Esto se puede utilizar como solución alternativa para crear un certificado para el SMA para ser importado y configurado.

Crear y exportar certificado desde un ESA

1. Desde la GUI de ESA, cree un certificado autofirmado desde **Network > Certificates > Add Certificate**. Al crear el certificado autofirmado, es importante que "Common Name (CN)" utilice el nombre de host del SMA y no del ESA, de modo que el certificado pueda utilizarse correctamente.
2. Enviar y registrar cambios.
3. Exportar el certificado creado desde **Red > Certificados > Exportar certificados**. Tiene dos opciones: (1) exportar y guardar/utilizar como certificado autofirmado o (2) descargar solicitud de firma de certificado (si necesita que el certificado se firme externamente): Guardar/Utilizar como certificado firmado automáticamente: Elija **Exportar certificados**Proporcione un nombre de archivo (por ejemplo, mycert.pfx) y una frase de paso que se utilizarán al convertir el certificado.Esto le solicitará automáticamente que guarde el archivo localmente.Vaya a "Convertir el certificado exportado".Descargar solicitud de firma de certificado **Network > Certificates**Haga clic en el nombre del certificado que creó.En la sección "Firma emitida por", haga clic en **Descargar solicitud de firma de certificado...**Guarde el archivo .pem localmente y envíelo a la CA.

Convertir el certificado exportado

El certificado creado y exportado desde el ESA estará en formato .pfx. El SMA sólo admite el formato .pem para la importación, por lo que este certificado deberá convertirse. Para convertir un certificado del formato .pfx al formato .pem, utilice el siguiente ejemplo de comando **openssl**:

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

Se le solicitará la frase de paso utilizada mientras se crea el certificado desde el ESA. El archivo .pem creado en el comando OpenSSL contendrá tanto el certificado como la clave en formato .pem. El certificado ya está listo para configurarse en el SMA. Vaya a la sección "Instalación del certificado" de este artículo.

Crear certificado con OpenSSL

Alternativamente, si tiene acceso local para ejecutar **openssl** desde su PC/estación de trabajo, puede ejecutar el siguiente comando para generar el certificado y guardar el archivo .pem y la clave privada necesarios en dos archivos independientes:

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

El certificado ya está listo para configurarse en el SMA. Vaya a la sección "Instalación del certificado" de este artículo.

Opción adicional, exportación de un certificado desde un ESA

En lugar de convertir el certificado de .pfx en .pem, como se mencionó anteriormente, puede guardar un archivo de configuración sin enmascarar las contraseñas en el ESA. Abra el archivo

de configuración ESA .xml guardado y busque la etiqueta <certificate>. El certificado y la clave privada ya estarán en formato .pem. Copie el certificado y la clave privada para importar el mismo en el SMA como se describe a continuación en la sección "Instalación del certificado".

> **Nota:** Esta opción sólo es válida para los dispositivos que ejecutan AsyncOS 11.1 y versiones anteriores, donde el archivo de configuración se puede guardar mediante la opción "frase de paso simple". Las versiones más recientes de AsyncOS proporcionan sólo la opción de enmascarar la frase de paso o cifrar la frase de paso. Ambas opciones cifran la clave privada, que es necesaria para la opción de importación o pegado del certificado.

> **Nota:** Si optó por el nº 2 anterior, "Descargar solicitud de firma de certificado", y tiene el certificado firmado por una CA, deberá importar el certificado firmado de vuelta al ESA desde el que se creó el certificado antes de guardar el archivo de configuración para hacer una copia del certificado y la clave privada. Para realizar la importación, haga clic en el nombre del certificado en la GUI de ESA y utilice la opción "Cargar certificado firmado".

Instalación del certificado en el SMA

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

- TLS entrante
- TLS saliente
- HTTPS
- LDAPS

En el SMA, inicie sesión a través de la CLI y realice los siguientes pasos:

1. Ejecute **certconfig**.
2. Elija la opción **setup**.
3. Deberá elegir entre utilizar el mismo certificado para todos los servicios o utilizar certificados independientes para cada servicio individual: Cuando se presenta "¿Desea utilizar un certificado/clave para recibir, entregar, acceso de administración HTTPS y LDAPS?", la respuesta "Y" sólo le obligará a introducir el certificado y la clave una vez y, a continuación, asignará ese certificado a todos los servicios.Si decide introducir "N", deberá introducir el certificado, la clave y el certificado intermedio (si procede) para cada servicio cuando se le solicite: Entrantes, Salientes, HTTPS y Gestión
4. Cuando se le solicite, pegue el certificado o la clave.
5. Finalizar con '.' en su propia línea para cada entrada para indicar que ha terminado de pegar el elemento actual. (Consulte la sección "Ejemplo".)
6. Si tiene un certificado intermedio, asegúrese de introducirlo cuando se le solicite.
7. Una vez completada, presione **Enter** para volver a la indicación CLI principal del SMA.
8. Ejecute **commit** para guardar la configuración.

> **Nota**: No salga del comando **certconfig** con Ctrl+C porque esto cancelará inmediatamente

los 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 SMA

1. Conéctese al SMA a través de la GUI mediante HTTPS (https://<SMA IP o nombre de host>) e introduzca sus credenciales de inicio de sesión.
2. Junto a la URL de la barra de direcciones del explorador, haga clic en el icono de bloqueo o en el icono de información para comprobar la validez del certificado, la caducidad, etc. Dependiendo del navegador que utilice, sus acciones y resultados pueden variar.
3. Haga clic en la ruta de certificación para comprobar la cadena de certificados.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems