Como gerar e instalar um certificado em um S A

Índice

[Introdução](#)
[Pré-requisitos](#)
[Como gerar e instalar um certificado em um S A](#)
[Crie e certificado de exportação de um ESA](#)
[Converta o certificado exportado](#)
[Crie o certificado com o OpenSSL](#)
[Opção adicional, exportando um certificado de um ESA](#)
[Instale o certificado no S A](#)
[Exemplo](#)
[Verifique o certificado importado e configurado no S A](#)
[Informações Relacionadas](#)

Introdução

Este documento descreve como gerar e instalar um certificado para a configuração e o uso em um dispositivo do Gerenciamento do Cisco Security (S A).

Pré-requisitos

Você precisará de ter o acesso para executar localmente o **OpenSSL do** comando.

Você precisará o acesso da conta admin a sua ferramenta de segurança do email (ESA), e o acesso admin ao CLI de seu S A.

Você deve ter estes artigos disponíveis no formato do .pem:

- Certificado X.509
- Chave privada que combina seu certificado
- Alguns Certificados intermediários fornecidos por seu Certificate Authority (CA)

Como gerar e instalar um certificado em um S A

> **Tip**: Recomenda-se ter um certificado assinado por um CA confiado Cisco não recomenda um CA específico segundo CA que você escolhe trabalhar com, você pode receber para trás o certificado assinado, a chave privada, e o certificado intermediário (onde aplicável) em vários formatos. Por favor pesquise ou discuta diretamente com CA o formato do arquivo que lhe fornecem antes de instalar o certificado.

Atualmente, o S A não apoia a geração de um certificado localmente. Em lugar de, é possível gerar um certificado auto-assinado no ESA. Isto pode ser usado como uma ação alternativa para criar um certificado para o S à fim ser importado e configurado.

Crie e certificado de exportação de um ESA

1. Do ESA GUI, crie um certificado assinado do self **certificado do > Add da rede > dos Certificados**. Ao criar o certificado auto-assinado, é importante para o “Common Name (CN)” usar o hostname do S A e não do ESA, de modo que o certificado possa corretamente ser usado.
2. Submeta e comprometa mudanças.
3. Exporte o certificado criado da **rede > dos Certificados > dos Certificados de exportação**. Você tem duas opções, (1) exportação e salvaguarda/uso como o certificado auto-assinado, ou (2) solicitação de assinatura de certificado da transferência (se você está precisando de ter o certificado assinado externamente): Salvar/uso como o certificado auto-assinado: Escolha **Certificados de exportação**Dê-lhe um nome de arquivo (por exemplo mycert.pfx) e a frase de passagem que sejam usados ao converter o certificado.Isto alertá-lo-á automaticamente salvar localmente o arquivo.Continue “converter o certificado exportado”.Transfira a solicitação de assinatura de certificado **Rede > Certificados**Clique sobre o nome que do certificado você criou.Na “assinatura emitida” pela seção, clique a **solicitação de assinatura de certificado da transferência…**Salvar o arquivo do .pem localmente e submeta-o a CA.

Converta o certificado exportado

O certificado criado e exportado do ESA estará no formato do .pfx. O S A apoia somente o formato do .pem para importar, assim que este certificado deverá ser convertido. A fim converter o certificado do formato do .pfx ao formato do .pem, use por favor o seguinte comando example do **OpenSSL**:

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

Você será alertado para a frase de passagem usada ao criar o certificado do ESA. O arquivo do .pem criado no comando do OpenSSL conterá o certificado e a chave no formato do .pem. O certificado está agora pronto para ser configurado no S A. Continua por favor “instala a seção do certificado” deste artigo.

Crie o certificado com o OpenSSL

Alternativamente, se você tem o acesso local para executar o **OpenSSL de** seu PC/workstation, você pode emitir o comando seguinte gerar o certificado e salvar o arquivo e a chave privada necessários do .pem em dois arquivos separados:

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

O certificado está agora pronto para ser configurado no S A. Continua por favor “instala a seção do certificado” deste artigo.

Opção adicional, exportando um certificado de um ESA

Em vez de converter o certificado do .pfx no .pem, como mencionado acima, você pode salvar um arquivo de configuração sem mascarar as senhas no ESA. Abra o arquivo de configuração e a busca salvar do .xml ESA para a etiqueta do <certificate>. O certificado e a chave privada estarão

já no formato do .pem. Copie o certificado e a chave privada para importar o mesmos no S A como descreveu “instala seção do certificado” abaixo.

> **Note**: Se você optou para #2 acima, “transfira a solicitação de assinatura de certificado”, e tenha o certificado assinado por CA, você precisará de importar o certificado assinado de volta ao ESA que o certificado foi criado antes de salvar o arquivo de configuração para fazer uma cópia do certificado e da chave privada. A importação pode ser feita clicando no nome do certificado em ESA GUI e em opção da “certificado assinado do uso transferência de arquivo pela rede”.

Instale o certificado no S A

Um único certificado pode ser usado para todos os serviços, ou um certificado individual pode ser usado para cada um dos quatro serviços:

- TLS de entrada
- TLS de partida
- HTTPS
- LDAP

No S A, o log através do CLI e termina as seguintes etapas:

1. Execute o **certconfig**.
2. Escolha a opção da **instalação**.
3. Você precisará de escolher se usar o mesmo certificado para todos os serviços, ou usar Certificados separados para cada serviço individual: Quando apresentado “faça você querem usar uns certificado/chave para a recepção, a entrega, o acesso do gerenciamento HTTPS, e os LDAP? ”, “Y de resposta” exigi-lo-á somente entrar no certificado e fechar uma vez, e atribui-lo-á então esse certificado a todos os serviços.Se você escolhe incorporar “N”, você precisará de entrar no certificado, na chave, e no certificado intermediário (onde aplicável) para cada serviço quando alertado: De entrada, de partida, HTTPS, e Gerenciamento
4. Quando alertado, cole o certificado ou feche-o.
5. Termine com '. 'em sua própria linha para cada entrada a fim indicar que você está feito que cola o artigo atual. (Veja a seção do “exemplo”.)
6. Se você tem um certificado intermediário, seja certo entrar n quando alertado para fazer assim.
7. Uma vez que terminado, pressione **entram** para retornar à alerta principal CLI do S A.
8. Seja executado **comprometem** para salvar a configuração.

> **Note**: Não retire o comando do **certconfig** com Ctrl+C desde que isto cancela imediatamente suas mudanças.

Exemplo

```
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 o certificado importado e configurado no S A

1. Conecte ao S A através do GUI usando o HTTPS (IP de https:// <SMA ou hostname>) e entre em suas credenciais do início de uma sessão.
2. Ao lado da URL na barra de endereços em seu navegador, clique o ícone ou o ícone de informação do fechamento para verificar a validez do certificado, da expiração, etc. Segundo que navegador você está usando, seus ações e resultados podem variar.
3. Clique sobre o caminho de certificação para verificar a corrente dos Certificados.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems