Como gerar e instalar um certificado em um SMA

Contents

[Introduction](#)
[Prerequisites](#)
[Como gerar e instalar um certificado em um SMA](#)
[Criar e exportar certificado de um ESA](#)
[Converter o certificado exportado](#)
[Criar certificado com OpenSSL](#)
[Opção adicional, exportando um certificado de um ESA](#)
[Instalar o certificado no SMA](#)
[Exemplo](#)
[Verifique o certificado importado e configurado no SMA](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve como gerar e instalar um certificado para configuração e uso em um Cisco Security Management Appliance (SMA).

Prerequisites

Você precisará ter acesso para executar o comando **openssl** localmente.

Você precisará de acesso de conta de administrador ao seu ESA (Email Security Appliance) e acesso de administrador ao CLI de seu SMA.

Você deve ter estes itens disponíveis no formato .pem:

- certificado X.509
- Chave privada que corresponde ao certificado
- Qualquer certificado intermediário fornecido pela autoridade de certificação (AC)

Como gerar e instalar um certificado em um SMA

> **Tip**: Recomenda-se que um certificado seja assinado por uma AC fidedigna. A Cisco não recomenda uma CA específica. Dependendo da CA com a qual você optar por trabalhar, você poderá receber de volta o certificado assinado, a chave privada e o certificado intermediário (quando aplicável) em vários formatos. Pesquise ou discuta diretamente com a autoridade de certificação o formato do arquivo fornecido antes de instalar o certificado.

Atualmente, o SMA não oferece suporte à geração de um certificado localmente. Em vez disso, é

possível gerar um certificado autoassinado no ESA. Isso pode ser usado como uma solução alternativa para criar um certificado para o SMA a fim de ser importado e configurado.

Criar e exportar certificado de um ESA

1. Na GUI do ESA, crie um certificado autoassinado em **Rede > Certificados > Adicionar Certificado**. Ao criar o certificado autoassinado, é importante que "Common Name (CN)" use o nome de host do SMA e não do ESA, para que o certificado possa ser usado corretamente.
2. Enviar e confirmar alterações.
3. Exporte o certificado criado em **Rede > Certificados > Exportar Certificados**. Você tem duas opções: (1) exportar e salvar/usar como certificado autoassinado ou (2) baixar solicitação de assinatura de certificado (se precisar ter o certificado assinado externamente): Salvar/usar como certificado autoassinado: Escolher **certificados de exportação**Forneça a ele um nome de arquivo (por exemplo, mycert.pfx) e uma senha que serão usados ao converter o certificado.Isso solicitará automaticamente que você salve o arquivo localmente.Vá para "Converter o certificado exportado".Baixar solicitação de assinatura de certificado **Rede > Certificados**Clique no nome do certificado criado.Na seção "Assinatura emitida por", clique em **Download do pedido de assinatura do certificado...**Salve o arquivo .pem localmente e envie para a CA.

Converter o certificado exportado

O certificado criado e exportado do ESA estará no formato .pfx. O SMA suporta apenas o formato .pem para importação, por isso este certificado terá de ser convertido. Para converter um certificado do formato .pfx para o formato .pem, use o seguinte exemplo de **comando openssl**:

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

Você será solicitado a inserir a senha usada ao criar o certificado do ESA. O arquivo .pem criado no comando OpenSSL conterá o certificado e a chave no formato .pem. O certificado agora está pronto para ser configurado no SMA. Prossiga para a seção "Instalar o certificado" deste artigo.

Criar certificado com OpenSSL

Como alternativa, se você tiver acesso local para executar **openssl** do seu PC/estação de trabalho, você poderá emitir o seguinte comando para gerar o certificado e salvar o arquivo .pem e a chave privada necessários em dois arquivos separados:

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

O certificado agora está pronto para ser configurado no SMA. Prossiga para a seção "Instalar o certificado" deste artigo.

Opção adicional, exportando um certificado de um ESA

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

formato .pem. Copie o certificado e a chave privada para importar o mesmo no SMA conforme descrito abaixo na seção "Instalar o certificado".

> **Note**: Esta opção só é válida para dispositivos que executam o AsyncOS 11.1 e versões anteriores, onde o arquivo de configuração pode ser salvo usando a opção "senha simples". As versões mais recentes do AsyncOS fornecem somente a opção de mascarar a senha ou criptografar a senha. Ambas as opções criptografam a chave privada, que é necessária para a opção de importação ou colar certificado.

> **Note**: Se você optou por #2 acima, "Download Certificate Signing Request" (Baixar solicitação de assinatura do certificado) e tiver o certificado assinado por uma CA, será necessário importar o certificado assinado de volta para o ESA do qual 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 na GUI do ESA e usando a opção "Carregar certificado assinado".

Instalar o certificado no SMA

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 saída
- HTTPS
- LDAPS

No SMA, faça login via CLI e execute as seguintes etapas:

1. Execute **certconfig**.
2. Escolha a opção **setup**.
3. Você precisará escolher se deseja usar o mesmo certificado para todos os serviços ou usar certificados separados para cada serviço individual: Quando apresentado "Deseja usar um certificado/chave para recebimento, entrega, acesso de gerenciamento HTTPS e LDAPS?", responder a "Y" exigirá que você insira o certificado e a chave apenas uma vez e, em seguida, atribuirá esse certificado a todos os serviços.Se você optar por inserir "N", precisará inserir o certificado, a chave e o certificado intermediário (quando aplicável) para cada serviço quando solicitado: Entrada, saída, HTTPS e gerenciamento
4. Quando solicitado, cole o certificado ou a chave.
5. Terminar com '.' em sua própria linha para cada entrada para indicar que você terminou de colar o item atual. (Consulte a seção "Exemplo".)
6. Se você tiver um certificado intermediário, insira-o quando for solicitado.
7. Depois de concluído, pressione **Enter** para retornar ao prompt CLI principal do SMA.
8. Execute **commit** para salvar a configuração.

> **Observação**: não saia do comando **certconfig** com Ctrl+C, pois isso cancela imediatamente

suas alterações.

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 SMA

1. Conecte-se ao SMA via GUI usando HTTPS (https://<SMA IP ou hostname>) e insira suas credenciais de login.
2. Ao lado da URL na barra de endereços do navegador, clique no ícone de cadeado ou ícone de informações para verificar a validade do certificado, a expiração, etc. Dependendo do navegador que você estiver usando, suas ações e resultados podem variar.
3. Clique no Caminho de certificação para verificar a cadeia de certificados.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems