Een certificaat op een SMA genereren en installeren

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Een certificaat op een SMA genereren en installeren](#)
[Certificaat maken en exporteren vanuit een ESA](#)
[Het geëxporteerde certificaat converteren](#)
[Certificaat met OpenSSL maken](#)
[Aanvullende optie: Een certificaat uitvoeren vanuit een ESA](#)
[Installeer het certificaat op de SMA](#)
[Voorbeeld](#)
[Controleer het geïmporteerde en ingestelde certificaat op de SMA](#)
[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u een certificaat voor configuratie en gebruik kunt genereren en installeren op een Cisco Security Management-applicatie (SMA).

Voorwaarden

U hebt toegang tot de opdracht **openssl** ter plaatse.

U hebt beheeraccount nodig voor toegang tot uw e-mail security applicatie (ESA) en beheertoegang tot de CLI van uw SDH.

U moet deze items in .pem-indeling beschikbaar hebben:

- X.509-certificaat
- Private-sleutel die overeenkomt met uw certificaat
- Alle intermediaire certificaten die door uw certificeringsinstantie worden geleverd (CA)

Een certificaat op een SMA genereren en installeren

> **Tip**: Aanbevolen wordt een certificaat te hebben ondertekend door een vertrouwde CA. Cisco adviseert geen specifieke CA. Afhankelijk van de CA waarmee u wilt werken, kunt u het ondertekende certificaat, de privé sleutel en het intermediaire certificaat (indien van toepassing) in verschillende formaten ontvangen. Onderzoek of bespreek rechtstreeks met de CA de bestandsindeling van het bestand dat zij aan u leveren voordat u het certificaat installeert.

Op dit moment ondersteunt de SMA niet het lokaal genereren van een certificaat. In plaats daarvan is het mogelijk een zichzelf ondertekend certificaat over de ESA op te stellen. Dit kan als tijdelijke oplossing worden gebruikt om een certificaat voor de SMA te creëren om te worden geïmporteerd en geconfigureerd.

Certificaat maken en exporteren vanuit een ESA

1. Maak vanuit de ESA GUI een zelf-ondertekend certificaat van **Netwerk > Certificaten > Certificaten toevoegen**. Bij het opstellen van het zelfgetekende certificaat is het belangrijk dat "Gemeenschappelijke Naam (GN)" de hostnaam van het SMA en niet van het ESA gebruikt, zodat het certificaat naar behoren kan worden gebruikt.
2. Breng veranderingen in en begaan.
3. Exporteren het certificaat dat is gemaakt via **Network > Certificaten > Exportcertificaten**. U hebt twee opties, (1) een eigen certificaat exporteren en opslaan/gebruiken, of (2) een downloadcertificaat dat een gebarentaal indient (indien u het certificaat extern wilt laten ondertekenen): Opslaan/gebruiken als een zelfondertekend certificaat: **Exportcertificaten** kiezenGeef het een bestandsnaam (bijv. mycert.pfx) en wachtwoord die gebruikt worden bij het converteren van het certificaat.U wordt hierdoor automatisch gevraagd het bestand lokaal op te slaan.Ga verder naar "Het geëxporteerde certificaat converteren".Aanvraag voor downloadoptie **Network > Certificaten**Klik op de certificaatnaam die u hebt gemaakt.Klik in het gedeelte "Handtekening afgegeven door" op **Aanvraag voor handtekening downloaden...**Sla het .pem-bestand lokaal op en dien het in bij de CA.

Het geëxporteerde certificaat converteren

Het certificaat dat is gemaakt en geëxporteerd uit het ESA, wordt in .pfx-formaat gesteld. De SMA ondersteunt alleen .pem-indeling voor het importeren, zodat dit certificaat moet worden geconverteerd. Als u een certificaat van .pfx-formaat naar .pem-formaat wilt converteren, gebruikt u het volgende opdrachtvoorbeeld **openssl**:

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

U wordt gevraagd het wachtwoord in te voeren dat wordt gebruikt bij het maken van het certificaat vanuit het ESA. Het .pem-bestand dat met de opdracht OpenSSL is gemaakt, bevat zowel het certificaat als de toets in .pem-indeling. Het certificaat is nu klaar om in de VS te worden ingesteld. Ga verder naar "Installeer het certificaatgedeelte" van dit artikel.

Certificaat met OpenSSL maken

Als u lokale toegang hebt om **openssl** uit te voeren vanaf uw pc/werkstation, kunt u ook de volgende opdracht geven om het certificaat te genereren en de benodigde .pem-bestand en privé-toets in twee afzonderlijke bestanden op te slaan:

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

Het certificaat is nu klaar om in de VS te worden ingesteld. Ga verder naar "Installeer het certificaatgedeelte" van dit artikel.

Aanvullende optie: Een certificaat uitvoeren vanuit een ESA

U kunt het certificaat niet van .pfx naar .pem converteren, zoals hierboven is aangegeven, maar u kunt een configuratiebestand opslaan zonder de wachtwoorden in het ESR te maskeren. Open het opgeslagen configuratiebestand in het ESR .xml en zoek de tag <certificaat>. De certificaat en de privé-toets bevinden zich al in .pem-formaat. Kopieer het certificaat en de privétoets om hetzelfde in het SMA te importeren zoals hieronder beschreven in "Installeer het certificaat".

> Opmerking: Deze optie is alleen geldig voor apparatuur die AsyncOS 11.1 en hoger heeft, waarbij het configuratiebestand kan worden opgeslagen met behulp van de optie 'gewoon wachtwoord'. Nieuwe versies van AsyncOS bieden alleen de optie om het wachtwoord te maskeren of het wachtwoord te versleutelen. Beide opties versleutelen de privé-toets, die nodig is voor de optie certificaatinvoer of -pasta.

> Opmerking: Indien u voor #2 hierboven heeft gekozen, "Download certificaataanvraag" en het certificaat laten ondertekenen door een CA, dan moet u het ondertekende certificaat terugimporteren naar de ESA. Het certificaat is gemaakt vanaf voordat u het configuratiebestand opslaat voor een kopie van het certificaat en de privétoets. U kunt dit importeren door op de certificaatnaam op de ESR-GUI te klikken en de optie "Upload Signed certificaatcertificaat" te gebruiken.

Installeer het certificaat op de SMA

Voor alle diensten kan één certificaat worden gebruikt, of voor elk van de vier diensten kan een afzonderlijk certificaat worden gebruikt:

- Ingebonden TLS
- Uitgaande TLS
- HTTPS
- LDAPS

In het SMA logt u in via de CLI en voert u de volgende stappen uit:

1. Start **certeconfig**.
2. Kies de optie **Instellingen**.
3. U dient te kiezen of u voor alle services hetzelfde certificaat wilt gebruiken of dat u voor elke afzonderlijke service afzonderlijke certificaten gebruikt: Als "Wilt u één certificaat/sleutel gebruiken voor ontvangst, levering, HTTPS-beheertoegang en LDAPS?" wordt voor het beantwoorden van "Y" alleen gevraagd om het certificaat en de toets eenmaal in te voeren, en zal dat certificaat dan aan alle diensten worden toegewezen.Als u "N" wilt invoeren, dient u voor elke service het certificaat, de sleutel en het tussentijdse certificaat (indien van toepassing) in te voeren. Inkomend, uitgaande, HTTPS en beheer
4. Plakt het certificaat of de toets wanneer dit wordt gevraagd.
5. Einde met ". op eigen regel voor elke vermelding om aan te geven dat het huidige item geplakt is. (Zie het gedeelte "Voorbeeld".)
6. Als u een tussentijds certificaat hebt, kunt u dit desgevraagd invoeren.
7. Druk na voltooiing **op** ENTER om naar de belangrijkste CLI-prompt van het SMA terug te

keren.

8. Ga de configuratie opslaan.

Opmerking: Sluit de opdracht **certfig** niet met Ctrl+C af omdat dit onmiddellijk uw wijzigingen opheft.

Voorbeeld

```
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
```

Controleer het geïmporteerde en ingestelde certificaat op de SMA

1. Sluit aan op het SMA via GUI met behulp van HTTPS (https://<SMA IP of hostname>) en voer uw inlogreferenties in.
2. Naast de URL in de adresbalk in uw browser, klik op het pictogram van het slot of op het informatiescherm om de geldigheid van het certificaat, de vervaldatum, enz. te controleren. Afhankelijk van welke browser u gebruikt, kunnen uw acties en resultaten variëren.
3. Klik op het certificeringspad om de keten van certificaten te controleren.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems