如何在SMA上生成和安装证书

目录

简介

本文档介绍如何生成和安装证书以在思科安全管理设备(SMA)上进行配置和使用。

先决条件

您需要具有本地运行命令**openssl**的权限。

您需要对邮件安全设备(ESA)的管理员帐户访问权限，以及对SMA的CLI的管理员访问权限。

您必须以.pem格式提供以下项目：

- X.509 证书
- 与证书匹配的私钥
- 证书颁发机构(CA)提供的任何中间证书

如何在SMA上生成和安装证书

> **提示：**建议由受信任CA签名证书。思科不推荐特定CA。 根据您选择使用的CA，您可能会以各种格式收回签名的证书、私钥和中间证书（如果适用）。 请在安装证书之前直接与CA研究或讨论他们提供给您的文件的格式。

目前，SMA不支持在本地生成证书。 相反，可以在ESA上生成自签名证书。这可用作为SMA创建证书以便导入和配置的解决方法。

从ESA创建和导出证书

1. 从ESA GUI中，从Network > Certificates > Add Certificate**创建自签名证书**。 创建自签名证书

时，“公用名(CN)”必须使用SMA的主机名，而不是ESA的主机名，以便正确使用证书。
2. 提交并提交更改。
3. 导出从Network > Certificates > Export Certificates**创建的证书**。 您有两个选项：(1)导出和另存为自签名证书或(2)下载证书签名请求（如果您需要外部签名证书）： 保存/用作自签名证书： 选择**导出证书**为其提供转换证书时将使用的文件名（例如mycert.pfx）和密码短语。这将自动提示您在本地保存文件。继续“转换导出的证书”。下载证书签名请求 **网络>证书**点击您创建的证书名称。在“Signature Issued By”（签名颁发者）部分，单击**Download Certificate Signing Request...**将.pem文件保存到本地并提交到CA。

转换导出的证书

从ESA创建和导出的证书将采用.pfx格式。SMA仅支持.pem格式进行导入，因此需要转换此证书。要将证书从.pfx格式转换为.pem格式，请使用以下**openssl**命令示例：

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

系统将提示您输入从ESA创建证书时使用的密码。 在OpenSSL命令中创建的.pem文件将同时包含证书和.pem格式的密钥。 证书现在已准备好在SMA上配置。 请继续阅读本文的“安装证书”部分。

使用OpenSSL创建证书

或者，如果您具有从PC/工作站运行**openssl**的本地访问权限，则可以发出以下命令来生成证书，并将所需的.pem文件和私钥保存到两个单独的文件中：

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

证书现在已准备好在SMA上配置。 请继续阅读本文的“安装证书”部分。

其他选项，从ESA导出证书

如上所述，您无需将证书从.pfx转换为.pem，而是可以保存配置文件，而无需屏蔽ESA上的密码。打开保存的ESA .xml配置文件并搜索<certificate>标记。证书和私钥将已采用.pem格式。将证书和私钥复制到SMA中，如下面的“安装证书”部分所述。

> **注意：**此选项仅对运行AsyncOS 11.1及更旧版本的设备有效，其中可使用“plain passphrase”选项保存配置文件。 较新版本的AsyncOS仅提供用于屏蔽密码短语或加密密码短语的选项。 两个选项都加密私钥，这是证书导入或粘贴选项所需的私钥。

> **注意：**如果您选择了#2，“下载证书签名请求”，并且证书由CA签名，则您需要在保存配置文件以复制证书和私钥之前将签名证书导入ESA。通过点击ESA GUI上的证书名称并使用选项“上传签名证书”(Upload Signed Certificate)，可以完成导入。

在SMA上安装证书

单个证书可用于所有服务，或单个证书可用于以下四项服务中的每一项：

- 入站TLS
- 出站TLS
- HTTPS
- LDAPS

在SMA上，通过CLI登录并完成以下步骤：

1. 运行**certconfig**。
2. 选择设**置选**项。
3. 您需要选择是对所有服务使用同一证书还是对每项服务使用单独的证书： 当出现“Do you want to use one certificate/key for receiving， delivery， HTTPS management access， and LDAPS？”时，回答“Y”只需输入一次证书和密钥，然后将该证书分配给所有服务。如果选择输入“N”，则在出现以下提示时，您需要为每个服务输入证书、密钥和中间证书（如果适用）：入站、出站、HTTPS和管理
4. 出现提示时，粘贴证书或密钥。
5. 以“。”结尾 在其自己的行上，以指示您已完成粘贴当前项目。 （请参阅“示例”部分。）
6. 如果您有中间证书，请务必在系统提示时输入。
7. 完成后，按**Enter**返回SMA的主CLI提示符。
8. 运行**commit**以保存配置。

注意：不要用Ctrl+C**退**出certconfig命令，因为这会立即取消更改。

示例

```
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+aqYB7IE1fgnqpEXek8xF1fcVnS2YTc7NXz78lNK0jvXOtCVBrWFu0z
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
```

验证SMA上的已导入和已配置证书

1. 使用HTTPS(https://<SMA IP或主机名>)通过GUI连接到SMA，并输入您的登录凭证。
2. 在浏览器地址栏中的URL旁，点击锁图标或信息图标以检查证书、到期等的有效性。 根据您使用的浏览器，您的操作和结果可能有所不同。
3. 点击Certification Path检查证书链。

相关信息

- 技术支持和文档 - Cisco Systems