如何在SMA上生成和安裝證書

目錄

簡介

本檔案介紹如何產生和安裝用於思科安全管理裝置(SMA)配置及使用的憑證。

必要條件

您需要具有本地運行命令**openssl**。

您需要管理員帳戶訪問您的郵件安全裝置(ESA)，並且需要管理員訪問SMA的CLI。

您必須以.pem格式提供以下專案：

- X.509憑證
- 與證書匹配的私鑰
- 由證書頒發機構(CA)提供的任何中間證書

如何在SMA上生成和安裝證書

> **提示**：建議使用受信任CA簽名的證書。思科不建議使用特定的CA。 根據您選擇使用的CA，您可能會收到各種格式的已簽名證書、私鑰和中間證書（如果適用）。 安裝證書之前，請研究或直接與CA討論他們提供給您的檔案的格式。

目前，SMA不支援在本地生成證書。 相反，可以在ESA上生成自簽名證書。這可以用作一種解決方法，為要匯入和配置的SMA建立證書。

從ESA建立和匯出證書

1. 在ESA GUI中，從**Network > Certificates > Add Certificate**建立自簽名證書。 建立自簽名證書

時，「公用名(CN)」必須使用SMA的主機名而不是ESA的主機名，這樣才能正確使用證書。
2. 提交和提交更改。
3. 匯出從**Network > Certificates > Export Certificates創建的證書。** 有兩個選項：(1)匯出並儲存/用作自簽名證書，或(2)下載證書簽名請求（如果需要從外部簽名證書）： 儲存/用作自簽名證書： 選擇**匯出證書**為其指定檔名（例如mycert.pfx）和轉換證書時使用的密碼短語。這將自動提示您本地儲存檔案。繼續操作「轉換匯出的證書」。下載證書簽名請求 **Network > Certificates**按一下您建立的憑證名稱。在「Signature Issued By」部分，按一下**Download Certificate Signing Request...**將.pem檔案儲存，然後提交給CA。

轉換匯出的證書

從ESA建立和匯出的證書將採用.pfx格式。SMA僅支援.pem格式進行匯入，因此需要轉換此證書。若要將憑證從.pfx格式轉換為.pem格式，請使用以下**openssl**命令範例：

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

系統將提示您輸入從ESA建立證書時使用的密碼。 在OpenSSL指令中建立的.pem檔案將包含.pem格式的憑證和金鑰。 證書現在準備在SMA上配置。 請繼續參閱本文的「安裝證書」一節。

使用OpenSSL建立憑證

或者，如果您擁有從PC/工作站運行**openssl**的本地訪問許可權，則可以發出以下命令來生成證書並將所需的.pem檔案和私鑰儲存到兩個不同的檔案中：

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

證書現在準備在SMA上配置。 請繼續參閱本文的「安裝證書」一節。

其他選項，從ESA匯出證書

您可以儲存配置檔案，而不用像上述那樣將證書從.pfx轉換為.pem，而不用掩蔽ESA上的密碼。開啟儲存的ESA .xml配置檔案，並搜尋<certificate>標籤。證書和私鑰已經採用.pem格式。複製證書和私鑰，將其匯入SMA，如下面的「安裝證書」一節所述。

附註：此選項只對運行AsyncOS 11.1及更早版本的裝置有效，其中配置檔案可以使用「普通密碼」選項儲存。 較新版本的AsyncOS僅提供遮蔽密碼或加密密碼的選項。 兩個選項都會加密私鑰，這是憑證匯入或貼上選項所需的私鑰。

附註：如果您選擇上述選項「下載證書簽名請求」，並且證書由CA簽署，則您需要將已簽名的證書匯入回ESA，之前建立證書的配置檔案用於複製證書和私鑰#2。可通過按一下ESA GUI上的證書名稱並使用選項「上傳簽名證書」完成匯入。

在SMA上安裝證書

單個證書可用於所有服務，或者單個證書可用於以下四個服務中的每個：

- 入站TLS
- 出站TLS
- HTTPS
- LDAPS

在SMA上，通過CLI登入並完成以下步驟：

1. 執行**certconfig**。
2. 選擇設**置**選項。
3. 您需要選擇是否對所有服務使用相同的證書，還是對每個單獨的服務使用單獨的證書： 如果顯示「您想使用一個證書/金鑰來接收、傳遞、HTTPS管理訪問和LDAPS嗎？」，回答「Y」將僅要求您輸入一次證書和金鑰，然後將該證書分配給所有服務。如果您選擇輸入「N」，則當系統提示時，您需要輸入每個服務的證書、金鑰和中間證書（如果適用）：傳入、傳出、HTTPS和管理
4. 出現提示時，貼上證書或金鑰。
5. 以「。」結尾 每個條目在其自己的行上，以指示您已完成貼上當前專案。 （請參閱「示例」部分。）
6. 如果您有中間證書，請務必在系統提示時輸入。
7. 完成後，按**Enter**返回到SMA的主要CLI提示。
8. 運行**commit**以儲存配置。

注意：不要使用Ctrl+C退出**certconfig命令，因為此操作會立即取消更改。**

範例

```
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+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
```

驗證SMA上匯入和配置的證書

1. 使用HTTPS(https://<SMA IP或主機名>)通過GUI連線到SMA，然後輸入您的登入憑證。
2. 在瀏覽器位址列中的URL旁邊，按一下鎖定圖示或資訊圖示檢查證書的有效性、到期等。 根據您使用的瀏覽器，您的操作和結果可能會有所不同。

3. 按一下證書路徑檢查證書鏈。

相關資訊

- 技術支援與文件 - Cisco Systems