Как генерировать и установить сертификат на SMA

Содержание

Введение

Этот документ описывает, как генерировать и установить сертификат для конфигурации и использования на Устройстве менеджмента Cisco Security (SMA).

Предварительные условия

У вас должен будет быть доступ для выполнения команды **openssl** локально.

Вам будут нужны доступ учетной записи администратора к вашему Email Security Appliance (ESA) и доступ администратора к CLI вашего SMA.

Необходимо иметь эти элементы в наличии в формате .pem:

- X. 509
- Секретный ключ, который совпадает с вашим сертификатом
- Любые промежуточные сертификаты предоставлены вашим Центром сертификации (CA)

Как генерировать и установить сертификат на SMA

> **Совет:** Рекомендуется подписать сертификат доверяемым CA., которого Cisco не рекомендует определенному CA. В зависимости от CA, с которым вы принимаете решение работать, можно получить назад подписанный сертификат, секретный ключ и промежуточный сертификат (где применимый) в различных форматах. Исследование или обсуждает непосредственно с CA формат файла, который они предоставляют вам до установки сертификата.

В настоящее время SMA не поддерживает генерацию сертификата локально. Вместо этого возможно генерировать подписанный сертификат на ESA. Это может использоваться в качестве обходного пути для создания сертификата для SMA, чтобы быть импортированным и настроенным.

Создайте и экспортируйте сертификат от ESA

1. От GUI ESA создайте сам подписанный сертификат от **Сети>, Сертификаты> Добавляют Сертификат**. При создании подписанного сертификата для "Общего имени (CN)" важно использовать имя хоста SMA а не ESA, так, чтобы мог должным образом использоваться сертификат.
2. Отправьте и передайте изменения.
3. Экспортируйте сертификат, созданный от **Сети> Сертификаты> Сертификаты Экспорта**. Вы имеете две опции, (1) экспорт и сохраняете/используете как подписанный сертификат, или (2) запрос подписи сертификата загрузки (если необходимо было подписать сертификат внешне): Сохраняйте/Используйте как Подписанный сертификат: Выберите **Export Certificates**Дайте ему имя файла (например, mycert.pfx) и пароль, который будет использоваться при преобразовании сертификата.Это автоматически побудит вас сохранить файл локально.Продолжите "Преобразовывать экспортируемый сертификат".Запрос подписи сертификата загрузки **Сеть> Сертификаты**Щелкните по сертификату, называют вас созданными.В "Подписи, Выполненной" разделом, нажмите **Download Certificate Signing Request...**Сохраните файл .pem локально и подвергнитесь CA.

Преобразуйте экспортируемый сертификат

Сертификат, созданный и экспортируемый от ESA, будет в формате .pfx. SMA только поддерживает формат .pem для импорта, таким образом, должен будет быть преобразован этот сертификат. Для преобразования сертификата от формата .pfx до формата .pem используйте следующий **openssl** пример команды:

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

Вам предложат для пароля, используемого при создании сертификата от ESA. Файл .pem, созданный в openssl команде, будет содержать и сертификат и ключ в формате .pem. Сертификат теперь готов быть настроенным на SMA. Продолжите "Устанавливать Сертификат" раздел этой статьи.

Создайте сертификат с OpenSSL

Также, если у вас есть локальный доступ для выполнения **openssl** от ПК/рабочей станции, можно выполнить следующую команду, чтобы генерировать сертификат и сохранить необходимый файл .pem и секретный ключ в два отдельных файла:

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

Сертификат теперь готов быть настроенным на SMA. Продолжите "Устанавливать Сертификат" раздел этой статьи.

Дополнительный параметр, экспортируя сертификат от ESA

Вместо того, чтобы преобразовать сертификат из .pfx в .pem, как упомянуто выше, можно сохранить файл конфигурации, не маскируя пароли на ESA. Откройте сохраненный файл конфигурации .xml ESA и ищите <сертификат> метку. Сертификат и секретный ключ уже будут в формате .pem. Скопируйте сертификат, и секретный ключ для импорта того же в SMA, как описано "Устанавливают Сертификат" раздел ниже.

> **Примечание:** Если вы действительно выбирали #2 выше, "Запросу подписи сертификата Загрузки", и подписал сертификат CA, необходимо будет импортировать подписанный сертификат назад к ESA, от которого был создан сертификат до сохранения файла конфигурации для того, чтобы сделать копию сертификата и секретного ключа. Импорт может быть сделан путем щелчка по названию сертификата на GUI ESA и опции "Upload Signed Certificate" использования.

Установите сертификат на SMA

Одиночный сертификат может использоваться для всех сервисов, или отдельный сертификат может использоваться для каждого из этих четырех сервисов:

- Входящий TLS
- Исходящий TLS
- HTTPS
- LDAP

На SMA войдите через CLI и завершите следующие шаги:

1. Выполните **certconfig**.
2. Выберите **опцию настройки**.
3. Необходимо будет выбрать, использовать ли тот же сертификат для всех сервисов, или использовать отдельные сертификаты для каждого отдельного сервиса: Когда представлено "Вы хотите использовать один сертификат/ключ для получения, доставки, управляющего доступ HTTPS и LDAP?", ответ "Y" только потребует, чтобы вы вошли в сертификате и ключе однажды, и тогда назначит тот сертификат на все сервисы.Если вы примете решение ввести "N", то необходимо будет войти в сертификате, ключе и промежуточном сертификате (где применимый) для каждого сервиса, когда предложено: Входящий, Исходящий, HTTPS и менеджмент
4. Когда предложено, вставьте сертификат или ключ.
5. Конец с '.'on его собственная линия для каждой записи, чтобы указать, что вы сделаны, вставив текущий элемент. (См. раздел "В качестве примера".)
6. Если у вас есть промежуточный сертификат, несомненно, введут его, когда предложено сделать так.
7. После того, как завершенный, нажмите **Enter** для возврата к основному приглашению CLI SMA.
8. Выполните **передачу** для сохранения конфигурации.

> **Примечание:** Не выходите **из certconfig** команды с Ctrl+C, так как это сразу отменяет ваши изменения.

Пример

```
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
```

Проверьте импортированный и настроенный сертификат на SMA

1. Соединитесь с SMA через GUI с помощью HTTPS (https://<IP SMA или имя хоста>) и войдите в учетных данных входа в систему.
2. Рядом с URL в строке адреса на вашем браузере нажмите значок блокировки или информационный значок для проверки законности сертификата, истечения, и т.д. В зависимости от которого браузера вы используете, ваши действия и результаты могут варьироваться.
3. Щелкните по Пути сертификации для проверки цепочки сертификатов.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация