Содержание

[Введение](#)
[Требования](#)
[Используемые компоненты](#)
[Настройка](#)
[Генерация запроса подписи сертификата (CSR):](#)
[Пример CSR сертификата индивидуального сервера:](#)
[Пример CSR подстановочного знака:](#)
[Импорт новой Цепочки сертификатов:](#)
[Проверка](#)
[Устранение неполадок](#)
[Соискатель не доверяет сертификату локального сервера ISE во время аутентификации dot1x.](#)
[Цепочка сертификатов ISE корректна, но Оконечная точка отклоняет ISE? s Серверный сертификат во время аутентификации.](#)
[Ссылки](#)
[Связанные обсуждения Сообщества Cisco Support](#)

Введение

Этот документ описывает установку третьей стороны CA подписанный сертификат в платформе Cisco Identity Services Engine.

Процесс является тем же независимо от заключительной роли сертификата (Аутентификация eap, Портал, Admin и pxGrid).

Требования

Основное знание Инфраструктуры открытых ключей.

Используемые компоненты

Сведения в этом документе основываются на следующих версиях программного и аппаратного обеспечения:

- Механизм Cisco Identity Services (ISE) Выпуск 2.0. Одинаковая конфигурация применяется к версиям 1.3 и 1.4.

Настройка

Генерация запроса подписи сертификата (CSR):

Для генерации CSR переходят к администрированию> Сертификаты> Запросы подписи сертификата и выбирают Generate Certificate Signing Requests (CSR).

- При Использовании раздел выбирают роль, которая будет использоваться из выпадающего меню. Если сертификат будет использоваться для множественных ролей , можно выбрать Multi-Use. Как только сертификат генерируется, роли могут быть изменены при необходимости.
- Выберите узел, для которого будет генерироваться сертификат.
- Заполните информацию по мере необходимости (Подразделение, Организация, Город, Состояние и Страна).

Примечание: Под Common Name (CN) ISE поля будет автоматический заполнять узел? s Полное доменное имя (FQDN).

Подстановочные знаки:

- Если цель состоит в том, чтобы генерировать проверку сертификата подстановочного знака? Позволить

Сертификаты Подстановочного знака? коробка.

- Если сертификат будет использоваться для Аутентификаций eap? *? символ не должен быть в поле Subject CN , поскольку соискатели Windows отклонят серверный сертификат.
- Даже когда? Проверить Идентичность Сервера? отключен на соискателе, подтверждение связи SSL может отказать когда? *? находится в поле CN.
- Вместо этого FQDN общего назначения может использоваться в поле CN, и затем? *.domain.com? может использоваться на поле имени DNS альтернативного имени субъекта (SAN).

Примечание: Некоторые Центры сертификации (CA) могут добавить подстановочный знак (*) в CN сертификата автоматически, даже если это не представляет в CSR. В этом сценарии для специального запроса будет нужно мне сделанный предотвратить это действие.

Пример CSR сертификата индивидуального сервера:

Пример CSR подстановочного знака:

Примечание: Каждый узел (узлы) развертываний? когда вы обращаетесь к серверу через IP-адрес, s IP-адрес может быть добавлен к полю SAN для предотвращения сертификата, предупреждающего..

Как только CSR был создан, ISE отобразит раскрывающееся окно с опцией для экспортирования его. После того, как экспортируемый, этот файл должен быть передан CA для подписания.

Импорт новой Цепочки сертификатов:

Центр сертификации возвратит серверный сертификат со знаком наряду с полной цепочкой подписания (Root/Промежуточное звено). После того, как полученный, выполните действия ниже для импорта сертификатов в сервер ISE.

1. Импортируйте любой Root и (или) Промежуточные сертификаты, предоставленные CA, перейдя к администрированию> Сертификаты> Надежные сертификаты.
2. Импортируйте Серверный сертификат, перейдя к администрированию>> Сертификаты>> Запросы подписи сертификата.
3. Выберите созданный на предыдущем этапе CSR и щелкните по Bind Certificate.
4. Выберите новое местоположение сертификата, и ISE свяжет сертификат с секретным ключом, созданным и сохраненным в базе данных.

Примечание: Если Роль Admin была выбрана для этого сертификата, ISE перезапустит сервисы.

Проверка

Если роль admin была выбрана во время импорта сертификата , можно проверить, что новый сертификат существует путем загрузки страницы администратора в браузере. Браузер должен доверять новому сертификату admin, пока цепочка была создана правильно и если цепочке сертификатов доверяет браузер.

Поскольку дополнительная проверка выбирает символ блокировки в браузере, и под путем сертификата проверяют, что полная цепочка присутствует и доверяется машиной. Это не прямой индикатор, что полная цепочка была передана правильно сервером, но индикатором браузера, который в состоянии доверять серверному сертификату на основе его локальной базы доверенных сертификатов.

Устранение неполадок

Соискатель не доверяет сертификату локального сервера ISE во время аутентификации dot1x.

Проверьте, что ISE передает полную цепочку сертификатов во время процесса подтверждения связи SSL.

При использовании методов EAP, которые требуют серверного сертификата (т.е. PEAP) и? Проверить Идентичность Сервера? выбран, соискатель проверит цепочку сертификатов с помощью сертификатов, которые она имеет в ее локальной базе доверенных сертификатов как часть процесса проверки подлинности. Поскольку часть ISE процесса подтверждения связи SSL представит свой сертификат и также любой Root и (или) промежуточный подарок сертификатов в его цепочке. Соискатель победил? t быть в состоянии проверить идентичность сервера, если цепочка является неполной. Проверить цепочку сертификатов пасуется назад вашему клиенту, можно выполнить следующие шаги:

1. Возьмите перехват от ISE (TCPDump) во время аутентификации. Найденный при Операциях> Программные средства Diagostic> Общие средства> Дамп TCP
2. Загрузить/Открыть перехват и применить фильтр? ssl.handshake.certificates? в Wireshark и находят проблему доступа.
3. После того, как Выбранный, Разверните Протокол RADIUS> Пары значений атрибутов> сообщение EAP Последний сегмент> Расширяемый протокол аутентификации> Уровень защищенных сокетов> Сертификат > Сертификаты

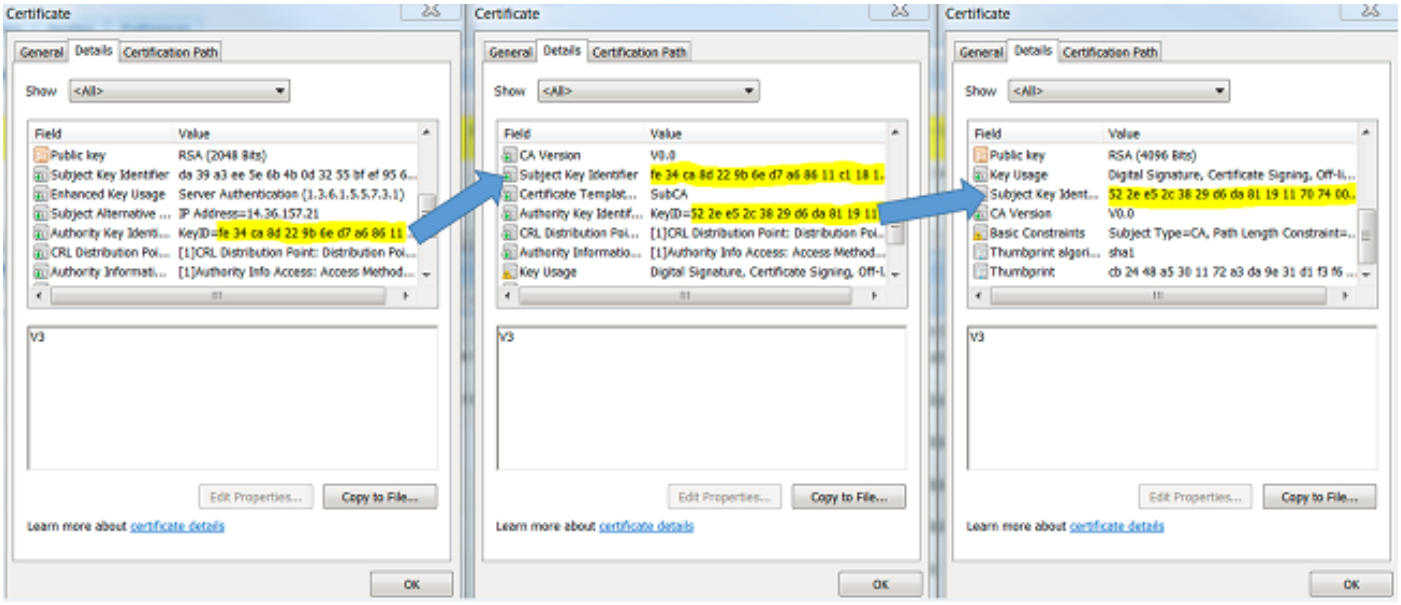
Цепочка сертификатов в перехвате.

Если цепочка не завершена, необходимо перейти к администрированию ISE> Сертификаты> Надежные сертификаты и проверять, что присутствует Root и (или) Промежуточные сертификаты. Если цепочку сертификатов передают успешно, сама цепочка должна быть проверена как

допустимая при помощи метода, выделенного ниже.

Откройте каждый сертификат (сервер, промежуточное звено и root) и проверьте цепочку доверия путем соответствия с Подчиненным ключевым идентификатором (SKI) каждого сертификата к Идентификатору ключа полномочий (AKI) следующего сертификата в цепочке.

Пример цепочки сертификатов.

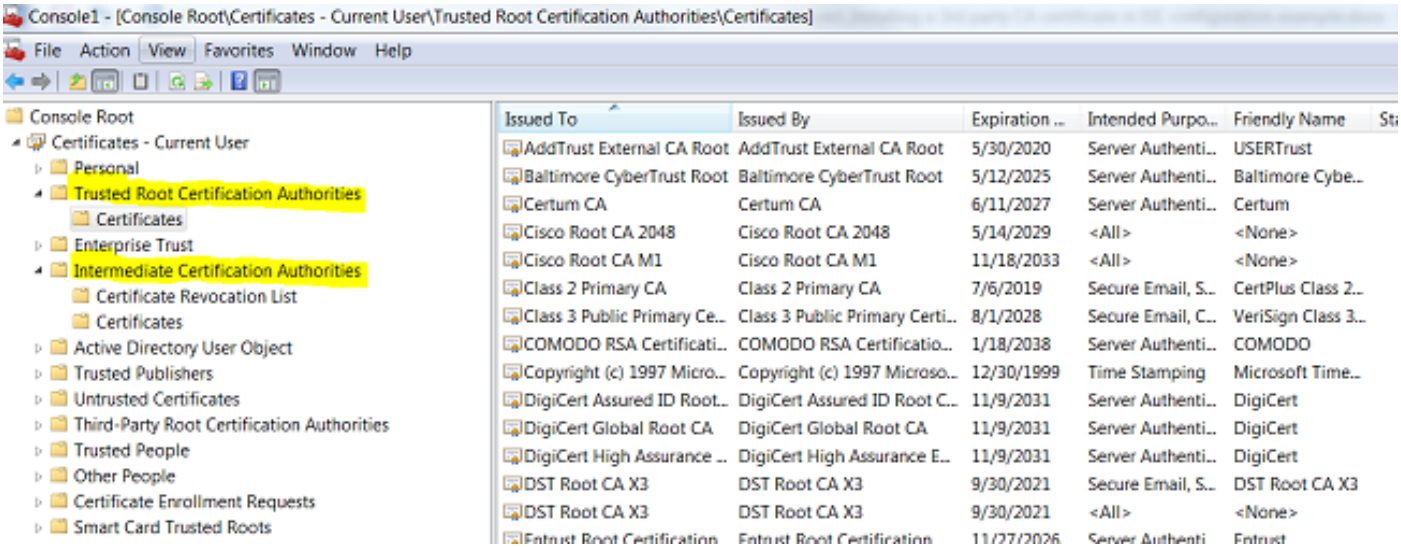


Цепочка сертификатов ISE корректна, но Оконечная точка отклоняет ISE? s Серверный сертификат во время аутентификации.

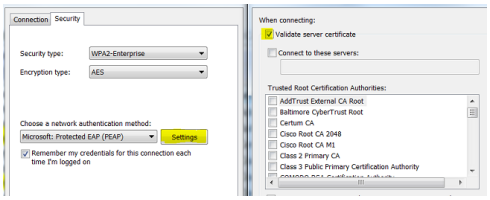
Если ISE представляет свою полную цепочку сертификатов во время подтверждения связи SSL, и соискатель все еще отклоняет цепочку сертификатов; следующий шаг должен проверить, что Root и (или) Промежуточные сертификаты находится в клиентской Локальной Базе доверенных сертификатов.

Для проверки это от устройства Windows открывается, mmc.exe Файл> Добавляют - Удаляют Моментальный снимок - в> От Доступной поспешной колонки Ins, выбирают сертификаты>, Добавляют>, выбирают также? Моя учетная запись пользователя? или? учетная запись компьютера? в зависимости от типа проверки подлинности в использовании (Пользователь или Машина). > OK

Под консольным обзорным выбором? Доверенные корневые центры сертификации? и? Промежуточные Центры сертификации? проверить присутствие Корневого и Промежуточного сертификата в локальной базе доверенных сертификатов.



Простой способ, чтобы проверить, что это - проблема Установления личности Сервера, снимите флажок? Проверить Серверный сертификат? под настройкой профиля соискателя и тестом это снова.



Примечание: ISE в настоящее время не поддерживает сертификаты обработки с помощью RSASSA-PSS в качестве алгоритма сигнатуры. Это

включает серверный сертификат, Root, Промежуточное звено или сертификат клиента (т.е. EAP-TLS, PEAP (TLS), и т.д.). См. дефект CSCug22137.

Ссылки

- Руководство администратора платформы Cisco Identity Services Engine, выпуск 2.0