Как я сертифицирую Подключения HTTPS к своему MCU Codian?

Содержание

Введение

Эта статья касается Cisco TelePresence MCU 4203, Cisco TelePresence MCU MSE 8420, Cisco TelePresence MCU 4505, Cisco TelePresence MCU MSE 8510 и Cisco TelePresence Усовершенствованный Медиашлюз 3610 продуктов.

Вопрос. . Как я сертифицирую Подключения HTTPS к своему MCU Codian?

O. От версии 2.3 MCU Codian и далее, если у вас есть Безопасное управление (HTTPS) или установленный ключ Функции шифрования, поддержки MCU безопасные соединения HTTP (HTTPS) для веб-интерфейса. В то время как это позволяет всему трафику между пользователем и MCU быть зашифрованным, администраторы, включающие, это должно заменить предоставленный сертификат и секретный ключ с их собственным, чтобы позволить идентичности MCU аутентифицироваться. Обратите внимание на то, что у вас может только быть один сертификат на MCU.

Для создания секретного ключа и пары сертификата, с помощью OpenSSL (например):

1. Если необходимая установка Безопасное управление (HTTPS) или ключ Функции шифрования.
2. Перейдите **к Сетевому> Services** и откройте порты.
3. Соединитесь с MCU с помощью HTTPS, принимающего temprary сертификат, выполненный нами.
4. На вашем компьютере устанавливают OpenSSL*. Это доступно по умолчанию на многих Unix/системы Linux и может быть загружено для Windows от (во время записи): http://www.slproweb.com/products/Win32OpenSSL.html
5. В окне командной строки перейдите к каталогу, в котором OpenSSL был установлен, например C:\OpenSSL\bin.
6. Генерируйте закрытый ключ RSA с помощью команды ниже. Эта команда генерирует файл, названный 'privkey.pem', который является вашим секретным ключом. TANDBERG рекомендует, чтобы этот ключ был по крайней мере 2048 битов длиной. Если этот секретный ключ будет сохранен где-нибудь кроме на MCU, он должен быть защищен паролем: вам предлагают ввести этот пароль дважды.> openssl genrsa-des3 - privkey.pem 2048

7. Создайте сертификат на основе этого секретного ключа с помощью одной из команд ниже. Для тестирования и внутреннего пользования, может быть самоподписан этот сертификат, но для максимальной безопасности это должно быть подписано центром сертификации. Создать подписанный сертификат (файл, названный cert.pem) использование:> openssl req - новый-x509 - ключ privkey.pem - cert.pem - дни 1000 Или для запроса сертификата, который будет передаваться использованию центра сертификации:> openssl req - новый - ключ privkey.pem - cert.csr Обе из этих команд вызывают для многих атрибутов. Общее имя должно совпасть с именем хоста или IP-адресом MCU, на котором это будет установлено.
8. При использовании объединенных в цепочку сертификатов цепочечные сертификаты, в формате pem, должны быть добавлены до конца сертификата модуля. Это может быть сделано двумя способами: путем копирования и вставки в текстовом редакторе или использования чего-то, таком как команда Unix кошки (например, кошка cert.pem authority.pem> chained.pem). Затем загрузите созданный файл.
9. На MCU переходят **к Сети> сертификаты SSL**.
10. Для Сертификатов нажмите **Browse** и найдите сертификат, который вы создали (это находится в каталоге, который вы использовали ранее). При создании подписанного сертификата сертификат называют cert.pem. Для одного со знаком центром сертификации выберите подписанный сертификат, который они предоставили.
11. Для Секретного ключа выберите privkey.pem файл.
12. Для пароля Шифрования с помощью закрытого ключа введите пароль, используемый при генерации секретного ключа (если таковые имеются).
13. Нажмите **сертификат Upload и ключ**. Если загрузка имеет успех, локальная информация о сертификате обновлена к тому из нового сертификата, и предупреждение, кажется, на заголовке веб-интерфейса побуждает вас перезапускать MCU.
14. Перейдите **к Параметрам настройки> Завершение** и перезапустите MCU.
15. После того, как это перезапустило, подключение к веб-интерфейсу с помощью HTTPS. При использовании подписанного сертификата проигнорируйте предупреждающие сообщения.
16. Подтвердите, что используется корректный сертификат. Для этого выполните следующие действия: - В Firefox: щелкните правой кнопкой мыши на странице, выберите **View Page Info**. Щелкните **по Вкладке Безопасность** и нажмите **View**. - В Internet Explorer: щелкните правой кнопкой мыши на странице, выберите **Properties**. Щелкните **по Certificates**.

* TANDBERG не ответственен за содержание веб-сайтов третьей стороны

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация