Вопрос. Для СЕРТИФИКАТОВ PHONE CUCM (LSC/MIC)

Содержание

Введение

Этот документ покрывает некоторые вопросы и ответы для Сертификатов Телефона Cisco Unified Communications Manager (CUCM). Вот быстрое представление Телефонных Сертификатов.

Изготовитель установленный сертификат (MIC):

Как название указывает, телефоны предварительно установлены с MIC, и это не может

быть удалено / модифицируемый администраторами. Сертификаты Центра сертификации (CA) CAP-RTP-001, CAP-RTP-002, Cisco_Manufacturing_CA и Cisco Производственный CA SHA2 предварительно установлены в CUCM для доверия MIC. MIC может? t использоваться , как только законность истекается как MIC CA наклон быть генерируемым ре,

Логически значимый сертификат (LSC):

LSC обладает открытым ключом для Cisco IP Phone, который подписан секретным ключом функции представительства сертифицирующей организации (CAPF) Cisco Unified Communications Manager. Это не установлено по телефону по умолчанию. Администратор имеет полный контроль над LSC. Сертификат CA CAPF может быть восстановлен, в свою очередь может выполнить новый LSC к телефонам каждый раз, когда требуется.

Каково общее использование для Телефонных Сертификатов?

Вот некоторое общее использование для Телефонных Сертификатов

Между CAPF и Телефоном для Установки/обновления, удаления или устранения проблем

Телефон устанавливает соединение с CAPF, чтобы Установить/обновить, удалить, или устранить неполадки сертификата по Телефону. Когда Режим аутентификации под информацией о Функции прокси центра сертификации (CAPF) установил в Существующим сертификатом (Приоритеты к LSC) или Существующим сертификатом (Приоритеты к MIC), телефонный Certficate используется для установления соединения с CAPF.

Существующим сертификатом (Приоритеты к LSC): Телефон использует LSC для аутентификации с CAPF. Если LSC не будет установлен, это будет использовать MIC. Если существуют проблемы с используемым сертификатом, установка отказывает с причиной "недопустимый LSC". Пример, CA со знаком для LSC не доступен в Доверии CAPF. Обновите режим аутентификации с помощью другого метода сертификата или пустой строкой для таких случаев возникновения отказов.

Существующим сертификатом (Приоритеты к MIC): Телефон использует MIC для аутентификации с CAPF.

Между CallManager и телефоном для соединения Безопасности уровня Trasnsport (TLS)

Телефон использует LSC или MIC для установления TLS подключение с CallManager. CallManager Проверит Certficate, представленный Телефоном путем проверки доверия CallManager. Соответствующий Сертификат CAPF должен быть доступен в доверии CallManager для LSC и Изготовления Cisco CA? s для MIC.

Между Телефоном и Сервером проверки подлинности для Аутентификации 802.1x

CAPF/Производство CA certs загружен к Серверам проверки подлинности как сервер Cisco Secure Access Control Server (ACS) или платформа Identity Services Engine (ISE). Сервер проверки подлинности использует загруженные сертификаты для аутентификации Телефона, когда это представляет свой сертификат (LSC или MIC).

Поскольку Сертификат базировал аутентификацию между Телефоном и устройством адаптивной защиты Cisco (ASA) для VPN

CAPF/Изготовление CA certs загружен в ASA, когда телефон представляет LIC/MIC, ASA проверяет его путем проверки, что это доверяет.

То, когда LSC и MIC присутствуют, является там каким-либо способом выбрать LSC или MIC явно для соединений?

Никакая опция для выбора или LSC или MIC для соединений. Если LSC установлен, Телефонный LSC использования. Если LSC не установлен, телефон использует MIC.

Консольная запись, когда не присутствует LSC:

SECD:-PXY_NO_LSC: Никакой LSC для [SCCP], попробует MIC

Консольная запись, когда присутствует LSC:

SECD:-PXY_CERT_CIPHER: [SCCP], [TLSv1], свидетельство [LSC]

Выбор LSC или MIC возможен только между CAPF и Телефонной установкой/обновлением, удалением или устранением проблем.

Что причина является установленными телефонами LSC с защищенным профилем, не становятся зарегистрированными при перемещении в новый кластер?

Это может произойти для телефонов те, которые уже имеют LSC от Кластера OLD. Когда и MIC и LSC присутствуют, LSC используется для установления TLS подключение. TLS не может быть установлен начиная с нового CUCM doesn? t имеют CA для этого LSC в его CallManager - доверие.

Console log показывают, какой сертификат используется для установления TLS. Ниже записи показывает, что используется LSC.

3469 НЕ 0:01:31.935298 SECD:-PXY_CERT_CIPHER: [SCCP], [TLSv1], свидетельство [LSC], шифр [AES256-SHA:AES128-SHA]

SSL3_Alert c? неизвестный CA? для таких отказавших случаев в console log:-

3486 0:01:31 ERR.938954 SECD:-STATE_SSL3_ALERT: предупреждение SSL3 [чтение]: [фатальный]: [неизвестный CA

Один из способов решить этот вопрос, получите телефон, зарегистрированный с помощью non? защитите профиль, тогда удаляют существующий LSC. Установите LSC от нового кластера, тогда регистрируют телефон с помощью защищенного профиля. Также возможно иметь телефон с защищенным профилем, зарегистрированным с помощью MIC, не устанавливая LSC.

Требуется, чтобы он, LSC установил для Телефонов для получения зарегистрированное использование Аутентифицируемый или Зашифрованный защищенный профиль?

Нет. Если LSC не установлен, Телефонный MIC использования для установления TLS подключение к CUCM.

4878 15:47:34 WRN.756063 SECD:-PXY_NO_LSC: Никакой LSC для [SCCP], MIC попыток.

Действительно ли это является обязательным, что режим безопасности устройства в Профиле безопасности соответствующего устройства, который будет Аутентифицироваться, или Зашифрованным для установки LSC?

Это не является обязательным, это может быть сделано с помощью стандарта по умолчанию Незащищенный Профиль также, где в Режиме безопасности устройства безопасный non.

Действительно ли это является обязательным Кластер, чтобы быть в Смешанном Режиме для установки LSC в Телефоне?

Это не является обязательным. LSC устанавливает/Удаляет, может быть сделан даже когда кластерный режим безопасности в незащищенном.

Если существует проблема с LSC, используемым Телефоном, как протестировать быстро?

Удалите LSC в одном из телефона, перейдя к Телефонной Странице администратора. Это вынуждает Телефон использовать MIC. Если весь штраф с MIC тогда продолжает устранение проблем LSC.

Как получить Телефонные Сертификаты для Устранения проблем?

Заставьте Операцию Сертификата Устранять неполадки под Устройством/Телефоном. Соответствие Сохраняет, тогда Применяют Config. Ждите для наблюдения Состояния работы Сертификата для **Устранения проблем Успеха**. Соберите Журналы **Функции прокси Центра сертификации Cisco** от инструмента контроля в реальном времени (RTMT). Это содержит сертификаты с Телефона.

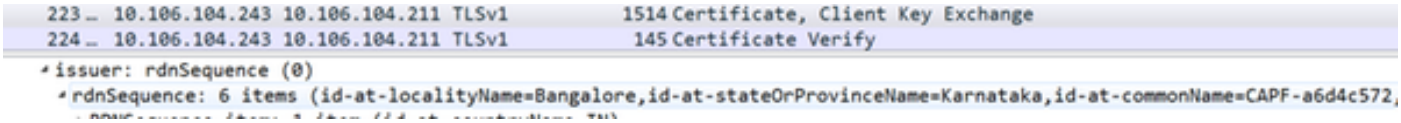
Если LSC или MIC Телефона используются для установления TLS подключение с CallManager, как проверить от захватов пакета?

Соберите Захваты пакета, покрывающие Телефонный перезапуск.

Проверьте Сертификат, Клиентское сообщение обмена ключами. Проверьте Сертификат, передаваемый от IP-телефона.

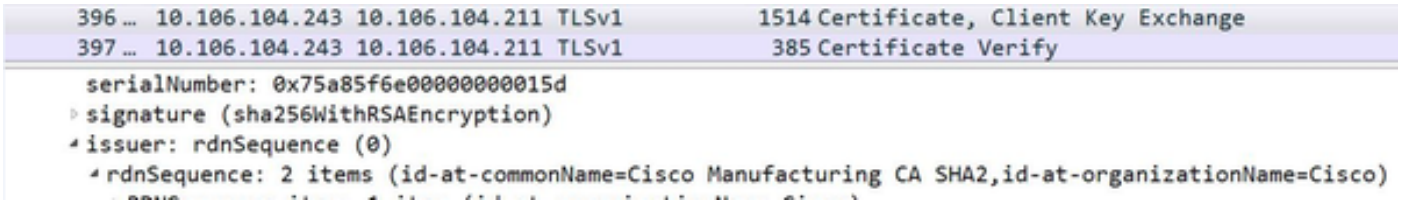
LSC в качестве примера:

Для LSC CN CAPF замечен в поле отправителя. Соответствующий root CAPF должен присутствовать в доверии CallManager.



MIC в качестве примера:

Для MIC, Cisco, Производящая CA в поле отправителя. Соответствующий Узел CA должен присутствовать в доверии CallManager.



Каково значение Режима аутентификации под информацией о Функции прокси центра сертификации (CAPF)? Значение для TLS подключение между CUCM и Телефоном?

Это - только метод аутентификации между Телефоном и CAPF для операций установки/обновления/удаления и устранения проблем. Это doesn? t имеют любое значение для TLS подключение между CUCM и Телефоном.

Каковы основные операции LSC для телефонов для рассмотрения после того, как Сертификат CAPF восстановил?

Этот раздел покрывает простаивающий сценарий, где никакой офлайновый CA не используется для запуска LSC.

TLS подключение с CallManager

Убедитесь для установки нового LSC по телефону прежде, чем удалить предыдущий Сертификат CAPF из доверия CallManager. Удаление предыдущего Сертификата CAPF, придерживавшегося перезапуском Сервиса CallManager, вызывает регистрационные проблемы к Телефонам, тем выполнил LSC этот Сертификат CAPF.

Операции LSC с доверием CAPF

Убедитесь для установки нового LSC по телефону прежде, чем удалить предыдущий Сертификат CAPF из доверия CAPF. Операциям LSC нравится, устанавливают/удаляют режим аутентификации использования **Существующим сертификатом (Приоритеты к LSC)** сбои с ошибкой **Недопустимый LSC** для Телефонов, тем выполнил LSC этот Сертификат CAPF.

Между Телефоном и Сервером проверки подлинности для Аутентификации 802.1x

Убедитесь для не удаления предыдущего сертификата CAPF из Сервера проверки подлинности, пока новый сертификат CAPF не загрузил, и Телефон выполнил LSC новым CAPF.

Между ASA и телефоном

Убедитесь для не удаления предыдущего сертификата CAPF из ASA, пока телефон не получит новый LSC и загрузит новый сертификат CA CAPF к ASA.

См. Регенерацию Сертификата для шагов, которые будут придерживаться для регенерации Сертификата CAPF.

Дополнительные сведения

- Сертификаты Cisco IP Phone и безопасная связь
- IP-телефония для руководства по дизайну 802.1X
- Руководство по обеспечению безопасности Cisco Unified Communications Manager