Руководство управления сертификатами решения UCCX

Содержание

Введение

Этот документ описывает, как настроить Cisco Unified Contact Center Express (UCCX) для использования самоподписанных и подписанных сертификатов.

Предварительные условия

Требования

Перед переходом действия настройки, которые описаны в этом документе, гарантируют, что у вас есть доступ к Странице администратора Операционной системы (OS) для этих приложений:

- UCCX
- SocialMiner
- MediaSense

У администратора должен также быть доступ к хранилищу сертификата на клиентских компьютерах супервизора и агенте.

FQDN, DNS и домены

Требуется, что все серверы в конфигурации UCCX установлены с серверами Системы доменных имен (DNS) и доменными именами. Также требуется, что агенты, супервизоры и администраторы обращаются к приложениям конфигурирования UCCX через Полное доменное имя (FQDN).

Версия UCCX 10.0 + требует, чтобы доменное имя и серверы DNS были заполнены на установку. Сертификаты, которые генерируются Версией UCCX 10.0 + установщик, содержат FQDN, как соответствующий. Добавьте серверы DNS и домен к кластеру UCCX перед обновлением к Версии UCCX 10.0 +.

Если домен изменяется или заполнен впервые, сертификаты должны быть восстановлены. После того, как вы добавите доменное имя к конфигурации сервера, восстановите все сертификаты Tomcat перед установкой их на других приложениях в клиентских браузерах, или после генерации Запроса подписи сертификата (CSR) для подписания.

Используемые компоненты

Информация, описанная в этом документе, основывается на этих компонентах программного и аппаратного обеспечения:

- Веб-сервисы UCCX
- Сервис уведомлений UCCX
- Tomcat платформы UCCX
- Tomcat изящества Cisco
- Tomcat Cisco Unified Intelligence Center (CUIC)
- SocialMiner Tomcat
- Веб-сервисы MediaSense

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить

потенциальное воздействие всех команд до их использования.

Общие сведения

С введением совместно расположенного Изящества и CUIC, интеграция между UCCX и SocialMiner для электронной почты и чата и использования MediaSense для записи, понимает и устанавливает сертификаты через Изящество, способность решить проблемы сертификата теперь критически важна.

Этот документ описывает использование и самоподписанного и подписанные сертификаты в среде конфигурации UCCX, которая покрывает:

- Сервисы уведомлений UCCX
- Веб-сервисы UCCX
- Сценарии UCCX
- Совместно расположенное изящество
- Совместно расположенный CUIC (оперативные данные и историческое создание отчетов)
- MediaSense (Основанная на изяществе запись и маркировка)
- SocialMiner (чат)

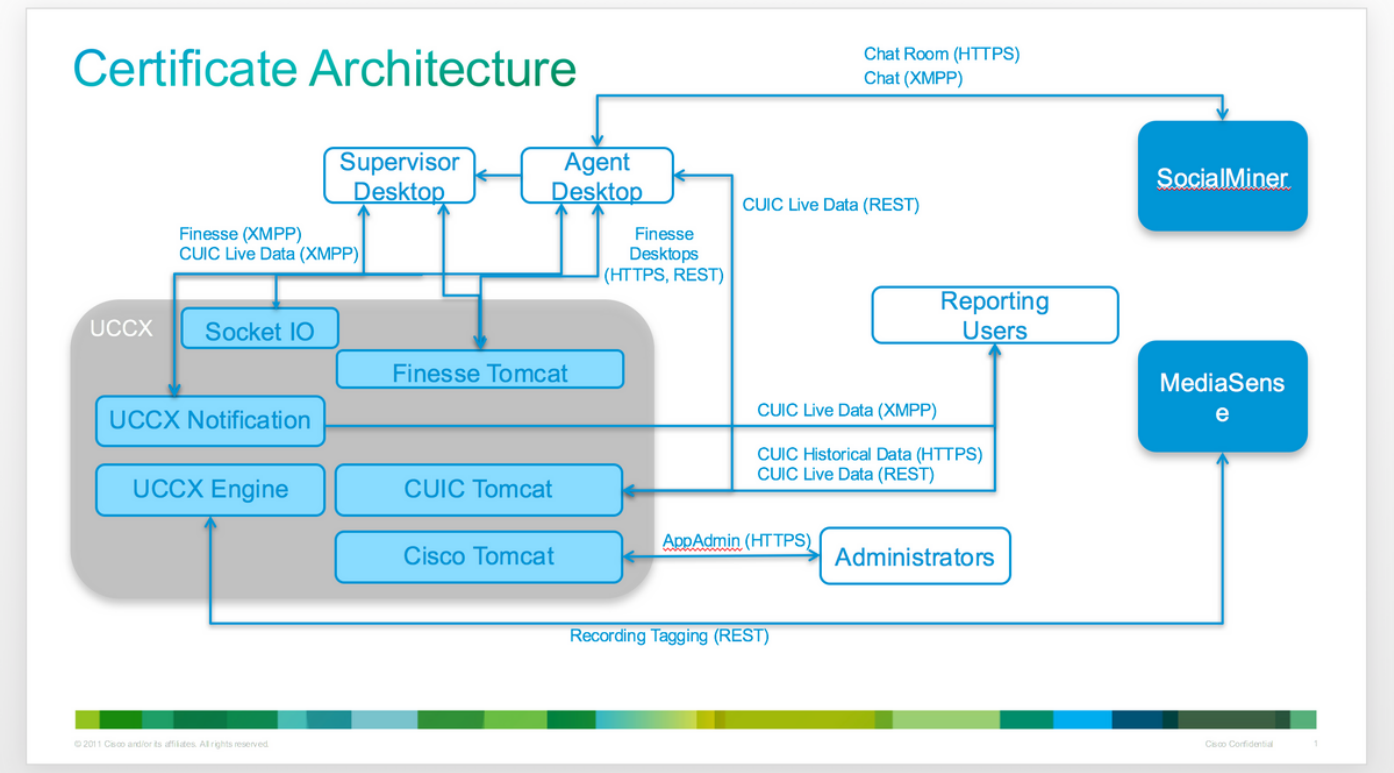
Сертификаты, или подписанные или самоподписанные, должны быть установлены и на приложениях (серверы) в конфигурации UCCX, а также агент и на компьютерах клиента супервизора.

В Операционной системе унифицированной связи (UCOS) 10.5, были добавлены мультисерверные сертификаты так, чтобы одиночный CSR мог генерироваться для кластера вместо того, чтобы иметь необходимость подписать отдельный сертификат для каждого узла в кластере. Этот тип сертификата является явно неподдерживаемым для UCCX, MediaSense и SocialMiner.

Настройка

В этом разделе описывается настроить UCCX для использования самоподписанных и подписанных сертификатов.

Схема конфигурации



Подписанные сертификаты

Рекомендуемый метод управления сертификатами для конфигурации UCCX должен усилить подписанные сертификаты. Эти сертификаты могут или быть подписаны внутренним Центром сертификации (CA) или известным сторонним CA.

В главных браузерах, таких как Mozilla Firefox и Internet Explorer, корневые сертификаты для известного независимого поставщика CAs установлены по умолчанию. Сертификатам для приложений конфигурирования UCCX, которые подписаны этими CAs, доверяют по умолчанию, поскольку их цепочка сертификатов заканчивается в корневом сертификате, который уже установлен в браузере.

Корневой сертификат внутреннего CA мог бы также быть предварительно установлен в клиентском браузере через Групповую политику или другую текущую конфигурацию.

Можно выбрать, иметь ли сертификаты приложения конфигурирования UCCX, подписанные известным независимым поставщиком CA или внутренним CA на основе доступности и предварительной установки корневого сертификата для CAs в клиентском браузере.

Установите сертификаты приложения Tomcat со знаком

Выполните эти шаги для каждого узла Издателя и подписчика UCCX, SocialMiner и Приложений администрирования Издателя и подписчика MediaSense:

1. Перейдите к **Странице администрирования операционной системы** и выберите **Security> Certificate Management**.
2. Нажмите **Generate CSR**.
3. От выпадающего списка **Списка Сертификата** выберите**, tomcat** как сертификат называют и нажимают **Generate CSR**.
4. Перейдите к **Безопасности> Управление сертификатами** и выберите **Download CSR**.

5. От всплывающего окна выберите **tomcat** из выпадающего списка и нажмите **Download CSR**.

Передайте новый CSR к независимому поставщику CA или подпишите его с внутренним CA, как ранее описано. Этот процесс должен произвести эти подписанные сертификаты:

- Корневой сертификат для CA
- Сертификат приложения издателя UCCX
- Сертификат приложения абонента UCCX
- Сертификат приложения SocialMiner
- Сертификат приложения издателя MediaSense
- Сертификат приложения абонента MediaSense

Примечание: Покиньте поле **Distribution** в CSR как FQDN сервера. Не изменяйте его на "Мультисервер (SAN)", поскольку мультисерверные сертификаты не поддерживаются с UCCX, MediaSense или SocialMiner.

Выполните эти шаги на каждом сервере приложений для загрузки корневого сертификата и сертификата приложения к узлам:

Примечание: При загрузке корневых и промежуточных сертификатов на издателе (UCCX или MediaSense), это должно автоматически быть реплицировано в абонента. Если все сертификаты приложения подписаны через ту же цепочку сертификатов, нет никакой потребности загрузить корневые или промежуточные сертификаты на другой, несерверы публикаций в конфигурации.

1. Перейдите к **Странице администрирования операционной системы** и выберите **Security> Certificate Management**.
2. Нажмите **Upload Certificate**.
3. Загрузите корневой сертификат и выберите **доверие tomcat** в качестве Типа сертификата.
4. **Щелкните Upload File (Загрузить файл).**
5. Нажмите **Upload Certificate**.
6. Загрузите сертификат приложения и выберите **tomcat** в качестве Типа сертификата.
7. **Щелкните Upload File (Загрузить файл). Примечание:** Если подчиненный CA подписывает сертификат, загрузите корневой сертификат подчиненного CA как *трастовый tomcat* сертификат вместо корневого сертификата. Если промежуточный сертификат выполнен, загрузите этот сертификат к *базе доверенных сертификатов tomcat* в дополнение к сертификату приложения.
8. Однажды завершенный, перезапустите эти приложения: Издатель и подписчик Cisco MediaSenseCisco SocialMinerCisco издатель и подписчик UCCX

Примечание: При использовании UCCX, MediaSense и SocialMiner 11.5 и позже, существует новый сертификат, названный tomcat-ECDSA. Когда вы загружаете сертификат tomcat-ECDSA со знаком к серверу, загружаете сертификат приложения как сертификат tomcat-ECDSA - не сертификат tomcat. Для получения дополнительной информации на ECDSA, обратитесь к Разделу связанных сведений для ссылки, чтобы понять и настроить сертификаты ECDSA.

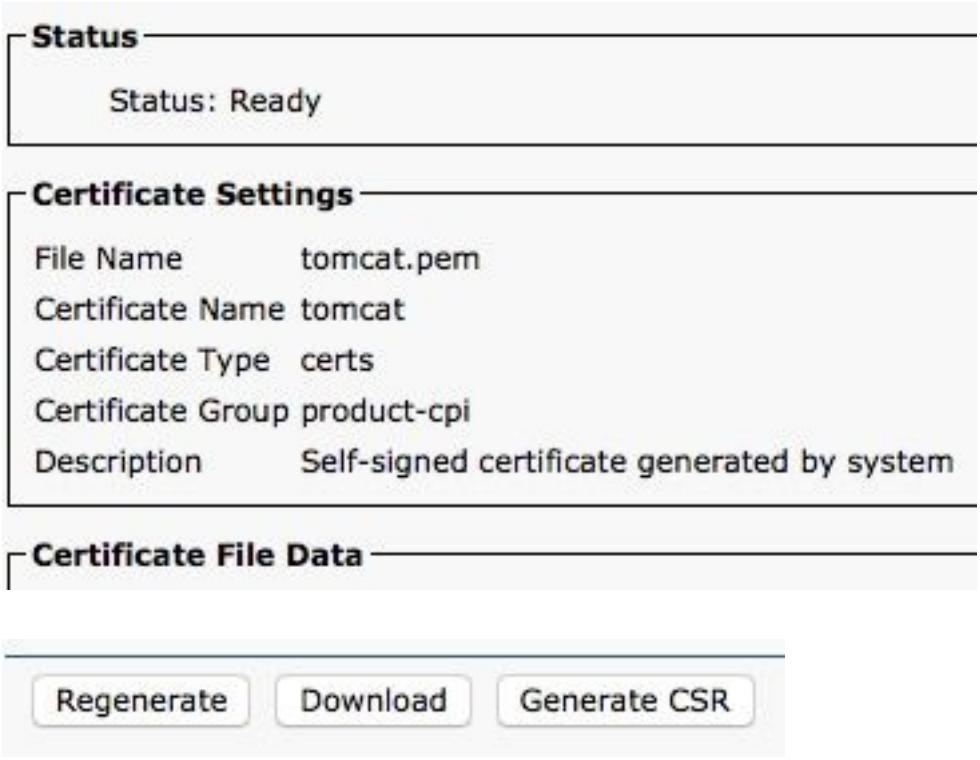
Подписанные сертификаты

Все сертификаты, которые используются в конфигурации UCCX, прибывают предварительно установленные в приложения конфигурирования и самоподписаны. Этим подписанным сертификатам не слепо доверяют, когда представлено или клиентскому браузеру или другому приложению конфигурирования. Несмотря на то, что рекомендуется подписать все сертификаты в конфигурации UCCX, можно использовать предварительно установленные подписанные сертификаты.

Для каждой взаимосвязи приложений необходимо загрузить соответствующий сертификат и загрузить его к приложению. Выполните эти шаги, чтобы получить и загрузить сертификаты:

1. Обратитесь к приложению **Страница администрирования операционной системы** и выберите **Security> Certificate Management**.

2. Нажмите соответствующий файл **.pem** сертификата и выберите **Download**:



3. Для загрузки сертификата на подходящем приложении перейдите к **Странице администрирования операционной системы** и выберите **Security> Certificate Management**.
4. Нажмите **Upload Certificate / Цепочка сертификатов:**

5. Однажды завершенный, перезапустите эти серверы:

   Издатель и подписчик Cisco MediaSenseCisco SocialMinerCisco издатель и подписчик UCCX

Для установки подписанных сертификатов на клиентском компьютере используйте групповую политику или диспетчер пакетов, или установите их индивидуально в браузере каждого ПК агента.

Для Internet Explorer установите клиентские подписанные сертификаты в хранилище **Доверенных корневых центров сертификации**.

Для Mozilla Firefox выполните эти шаги:

1. Перейдите к **Программным средствам> Опции**.
2. **Щелкните вкладку Advanced ("Дополнительно").**
3. Нажмите **View Certificates**.
4. Перейдите к вкладке **Servers**.
5. **Нажмите Add исключение**.

Интеграция и конфигурация клиента

UCCX-to-MediaSense

UCCX использует Прикладной программный интерфейс (API) REST веб-сервисов MediaSense в двух целях:

- Для подписки на уведомления о новых записях, которые вызваны на Cisco Unified Communications Manager (CUCM).
- Для маркировки записей агентов UCCX с информацией об Очереди обслуживания контакта (CSQ) и агентом.

UCCX использует остальных API на узлах администрирования MediaSense. Существует максимум два в любом кластере MediaSense. UCCX не подключает через остальных API к узлам расширения MediaSense. Оба узлы UCCX должны использовать MediaSense REST API, так устанавливают эти два сертификата MediaSense Tomcat на обоих из узлов UCCX.

Загрузите цепочку со знаком или цепочку подписанного сертификата серверов MediaSense к *доверию tomcat* UCCX keystore.

MediaSense к изяществу

MediaSense использует API REST веб-сервисов Изящества для аутентификации агентов для гаджета Поиска и Воспроизведения MediaSense на Изяществе.

Сервер MediaSense, настроенный на плане XML Изящества для гаджета Поиска и Воспроизведения, должен использовать API REST Изящества, так установите два сертификата Tomcat UCCX на том узле MediaSense.

Загрузите цепочку со знаком или цепочку подписанного сертификата серверов UCCX к *доверию tomcat* MediaSense keystore.

UCCX-to-SocialMiner

UCCX использует SocialMiner REST и API Уведомления для управления почтовыми контактами и конфигурацией. Оба из узлов UCCX должны использовать SocialMiner REST API и быть уведомлены сервисом уведомлений SocialMiner, так установите сертификат SocialMiner Tomcat на обоих из узлов UCCX.

Загрузите цепочку со знаком или цепочку подписанного сертификата сервера SocialMiner к

доверию tomcat UCCX keystore.

Сертификат клиента AppAdmin UCCX

Сертификат клиента AppAdmin UCCX используется для администрирования системы UCCX. Для установки сертификата AppAdmin UCCX для администраторов UCCX, на клиентском компьютере, перейдите к **https://<UCCX FQDN>/appadmin/main** для каждого из узлов UCCX и установите сертификат через браузер.

Сертификат клиента платформы UCCX

Веб-сервисы UCCX используются для доставки контактов чата к клиентским браузерам. Для установки сертификата Платформы UCCX для агентов UCCX, и супервизоры, на клиентском компьютере, перешли к **https://<UCCX FQDN>/appadmin/main** для каждого из узлов UCCX и устанавливают сертификат через браузер.

Сертификат клиента сервиса уведомлений

Сервис уведомлений CCX используется Изяществом, UCCX и CUIC для передачи поступающия в реальном времени данные к компьютеру клиента по Расширяемому Протоколу Обмена сообщениями и Присутствия (XMPP). Это используется для связи Изящества в реальном времени, а также CUIC Оперативные Данные.

Для установки сертификата клиента Сервиса уведомлений на ПК агентов и супервизоров или сообщающих пользователей, которые используют Оперативные Данные, перешли к **https://<UCCX FQDN>:7443/**для каждого из узлов UCCX и устанавливают сертификат через браузер.

Сертификат клиента изящества

Сертификат клиента Изящества используется рабочими столами Изящества для соединения с экземпляром Tomcat Изящества в целях связи API REST между рабочим столом и совместно расположенным сервером Изящества.

Для установки сертификата Изящества для агентов, и супервизоры, на клиентском компьютере, перешли к **https://<UCCX FQDN>:8445/**для каждого из узлов UCCX и устанавливают сертификат через приглашения браузера.

Для установки сертификата Изящества для администраторов Изящества, на клиентском компьютере, перейдите к **https://<UCCX FQDN>:8445/cfadmin** для каждого из узлов UCCX и установите сертификат через приглашения браузера.

Сертификат клиента SocialMiner

Сертификат SocialMiner Tomcat должен быть установлен на клиентском компьютере. Как только агент принимает запрос чата, гаджет Чата перенаправлен к URL, который представляет чат. Этот чат размещен сервером SocialMiner и содержит контакт чата или клиент.

Для установки сертификата SocialMiner в браузере, на клиентском компьютере, перейдите к

https://<SocialMiner FQDN> / и установите сертификат через приглашения браузера.

Сертификат клиента CUIC

Сертификат Tomcat CUIC должен быть установлен на клиентском компьютере для агентов, супервизоров и сообщающих пользователей, которые используют веб-интерфейс CUIC для отчетов предыстории, или Оперативные Данные сообщают или в веб-странице CUIC или в гаджетах в рабочем столе.

Для установки сертификата Tomcat CUIC в браузере, на клиентском компьютере, перейдите к **https://<UCCX FQDN>:8444/**и установите сертификат через приглашения браузера.

CUIC оперативный сертификат данных (так как 11. x

CUIC использует Сокетный Сервис IO для бэкэнда Оперативные данные. Этот сертификат должен быть установлен на клиентском компьютере для агентов, супервизоров и сообщающих пользователей, которые используют веб-интерфейс CUIC для Оперативных Данных или кто использует Оперативные гаджеты Данных в Изяществе.

Для установки Сокетного сертификата IO в браузере, на клиентском компьютере, перейдите к **https://<UCCX FQDN>:12015/**и установите сертификат через приглашения браузера.

Сторонние приложения, доступные из сценариев

Если сценарий UCCX разработан, чтобы обратиться к безопасному месту на стороннем сервере (например, *Получить* шаг *Документа URL* в URL HTTPS или *Выполнять Вызов Отдыха* к URL REST HTTPS), загрузите цепочку со знаком или цепочку подписанного сертификата услуги от стороннего поставщика к *доверию tomcat* UCCX keystore. Для получения этого сертификата обратитесь **к Странице администрирования операционной системы** UCCX и выберите **Upload Certificate**.

Механизм UCCX настроен для поиска Tomcat платформы keystore сторонние цепочки сертификатов, когда предоставлено эти сертификаты сторонними приложениями, когда они обращаются к безопасным местам через шаги сценария.

Вся цепочка сертификатов должна быть загружена к Tomcat платформы keystore, доступный через **Страницу администрирования операционной системы**, поскольку Tomcat keystore не содержит корневых сертификатов по умолчанию.

После того, как вы завершаете эти действия, перезапускаете Cisco Механизм UCCX.

Проверка

Чтобы проверить, что все сертификаты установлены правильно, можно протестировать функции, которые описаны в этом разделе. Если никакие ошибки сертификата не появляются, и все функции функционируют должным образом, сертификаты установлены правильно.

- Настройте Изящество так, чтобы оно автоматически сделало запись агента через поток операций. После того, как вызов обрабатывается агентом, используйте приложение

Поиска и Воспроизведения MediaSense для обнаружения вызова. Проверьте, что вызов имеет агента, CSQ и метки команды, подключенные к метаданным записи в MediaSense.
- Настройте веб-Чат Агента через SocialMiner. Введите контакт чата с помощью веб-формы. Проверьте, что агент получает баннер, чтобы признать, что чат связывается и также проверяет, что, как только контакт чата принят, форма чата загружается должным образом, и агент может и получить и передать сообщения чата.
- Попытка войти в агента через Изящество. Проверьте, что никакие предупреждения сертификата не появляются и что веб-страница не вызывает для установки сертификатов в браузер. Проверьте, что агент может изменить состояния должным образом, и новый вызов в UCCX правильно представлен агенту.
- После того, как вы настраиваете Оперативные гаджеты Данных в агенте и настольном плане Изящества супервизора, входите в агента, супервизор и сообщающего пользователя. Проверьте, что Оперативные гаджеты Данных загружаются должным образом, что исходные данные заполнены в гаджет, и что данные обновляют, когда изменяются базовые данные.
- Попытайтесь подключить от браузера до URL AppAdmin на обоих узлы UCCX. Проверьте, что никакие предупреждения сертификата не появляются, когда предложено со страницей входа.

Устранение неполадок

Проблема - ID/Пароль недействительного пользователя

Агенты Изящества UCCX неспособны войти с ошибкой "**в ID/Пароль Недействительного пользователя**".

Причины

Унифицированный CCX выдает исключение “SSLHandshakeException “и не в состоянии устанавливать соединение с Унифицированным CM.

Решение

- Проверьте, что не истекается Унифицированный сертификат Tomcat CM.
- Гарантируйте, что любой сертификат, который вы загрузили в Унифицированном CM, имеет любое из этих расширений, отмеченных как важное:
  Использование ключа X509v3 (OID - 2.5.29.15)
  Основные ограничения X509v3 (OID - 2.5.29.19)
  Если вы отмечаете какие-либо другие расширения как важные, связь отказывает между Унифицированным CCX и Унифицированным CM из-за сбоя Унифицированной Проверки сертификата CM.

Проблема - SAN CSR и SAN сертификата не совпадают

Загрузка подписанного сертификата CA отображает ошибку "SAN CSR, и SAN Сертификата не совпадает".

Причины

CA, возможно, добавил другой родительский домен в поле альтернативных имен субъекта (SAN) сертификата. По умолчанию CSR будет иметь эти SANs:

SubjectAltName [
  пример. com (dNSName)
  host name. пример. com (dNSName)
]

CAs мог бы возвратить сертификат с другим SAN, добавленным к сертификату: www. host name. пример. com. Сертификат будет иметь дополнительный SAN в этом случае:

SubjectAltName [
  пример. com (dNSName)
  host name. пример. com (dNSName)

  www. host name. пример. com (dNSName)
]

Это вызывает SAN ошибку несоответствия.

Решение

На 'Подчиненное Альтернативное название (SANs)' раздел страницы 'Generate Certificate Signing Request' UCCX, генерируйте CSR с пустым Родительским полем Domain. Таким образом, CSR не генерируется с SAN атрибутом, CA может отформатировать SANs, и не будет SAN несоответствия атрибута при загрузке сертификата к UCCX. Обратите внимание на то, что Родительские полевые Domain настройки по умолчанию к домену сервера UCCX, таким образом, значение должно явно быть удалено, в то время как настроены параметры настройки для CSR.

Проблема - СЕТЬ:: ERR_CERT_COMMON_NAME_INVALID

При доступе к любому UCCX, MediaSense или веб-странице SocialMiner, вы получаете сообщение об ошибках.

"Ваше соединение не является частным.

Атакующие могли бы пытаться украсть вашу информацию из <Server_FQDN> (например, пароли, сообщения или кредитные карты). СЕТЬ:: ERR_CERT_COMMON_NAME_INVALID

Этот сервер не мог доказать, что это <Server_FQDN>; его сертификат безопасности от [missing_subjectAltName]. Это может быть вызвано неверной конфигурацией или атакующим, перехватывающим ваше соединение."

Причины

Версия 58 Chrome представила новую характеристику безопасности, где она сообщает, что сертификат веб-сайта не безопасен, если его общее имя (CN) также не включено как SAN.

Решение

- Можно перейти к **Усовершенствованному>, Продолжаются к <Server_FQDN> (опасному)** , чтобы продолжить к узлу и принять ошибку сертификата.
- Можно избежать ошибки в целом с подписанными сертификатами CA. При генерации CSR FQDN сервера включен как SAN. CA может подписать CSR, и после загрузки подписанного сертификата назад к серверу сертификат сервера будет иметь FQDN в поле SAN так, чтобы не была представлена ошибка.

Дополнительные сведения

Посмотрите, что раздел "Удаляет поддержку commonName, совпадающего в сертификатах" в Осуждениях и Удалениях в Chrome 58.

Дефекты сертификата

- Идентификатор ошибки Cisco CSCvb46250 - UCCX: Tomcat влияние сертификата ECDSA на Изящество Оперативные Данные
- Идентификатор ошибки Cisco CSCvb58580 - Неспособный войти к SocialMiner и с tomcat и с tomcat-ECDSA, подписанным RSA CA
- Идентификатор ошибки Cisco CSCvd56174 - UCCX: Ошибка входа агента Изящества из-за SSLHandshakeException
- Идентификатор ошибки Cisco CSCuv89545 - Уязвимость Затора Изящества

Дополнительные сведения

- **Поймите сертификаты ECDSA в решении UCCX**
- **UCCX, со знаком и пример конфигурации подписанных сертификатов**
- **Cisco Systems – техническая поддержка и документация**