Поймите сертификаты ECDSA в Решении UCCX

Содержание

Введение

Этот документ описывает, как настроить Cisco Unified Contact Center Express (UCCX) решение для использования Сертификатов Эллиптического алгоритма цифровой подписи кривой (ECDSA).

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
- Cisco Unified Communications Manager (CUCM)
- Конфигурация Сертификата Решения UCCX - [http://www. cisco . com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html](#)

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

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, гарантируйте понимание потенциального воздействия любой команды.

Общие сведения

Как часть сертификации Общих критериев (CC), Cisco Unified Communications Manager добавил сертификаты ECDSA в версии 11.0. Это влияет на все продукты голосовой операционной системы (VOS), такие как UCCX, SocialMiner, MediaSense, и т.д. от версии 11.5.

Больше подробных данных об **Алгоритме цифровой подписи Эллиптической кривой** может быть найдено здесь: https://www.maximintegrated.com/en/app-notes/index.mvp/id/5767

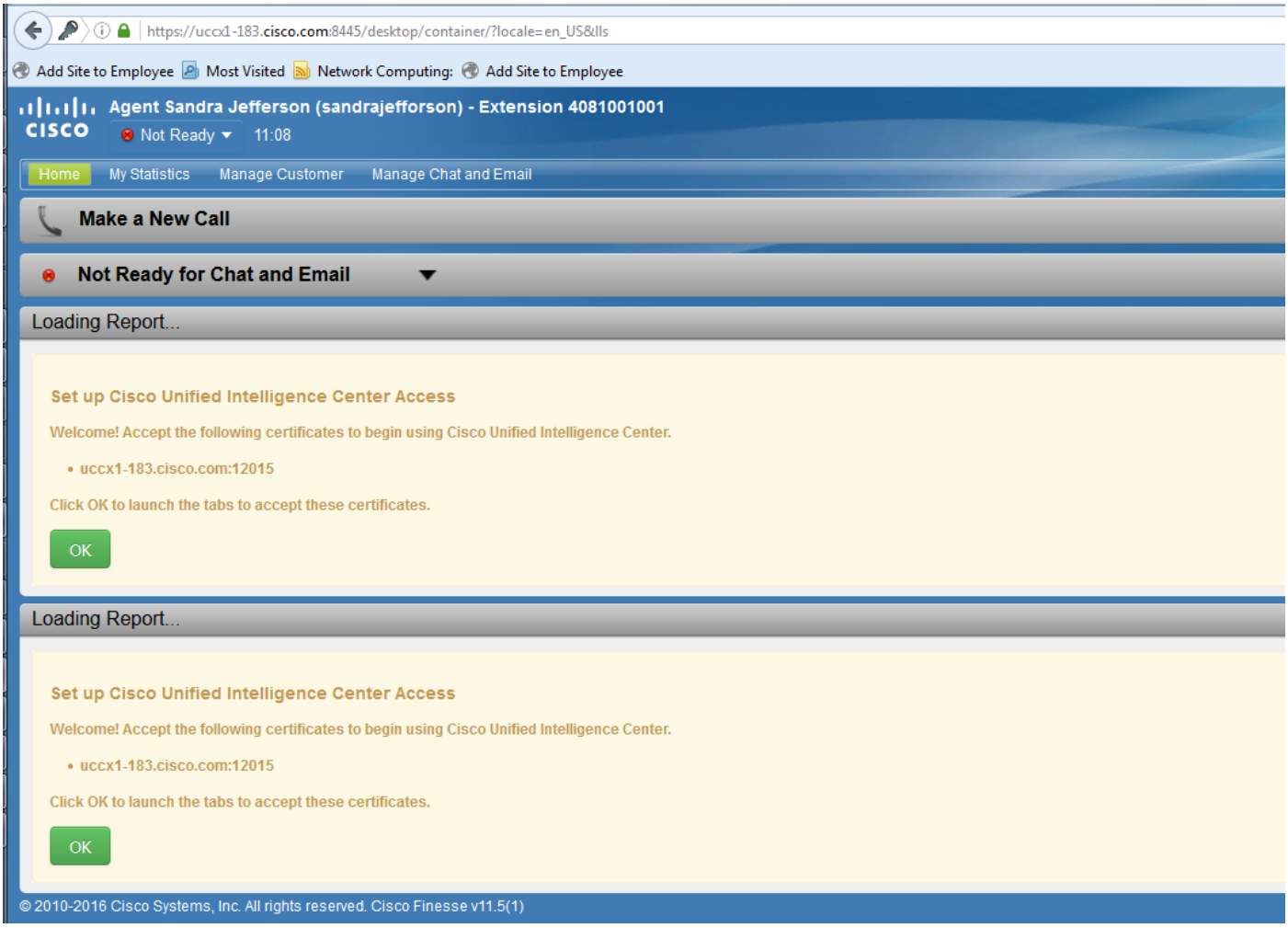
Относительно решения UCCX, когда вы обновляете к 11.5, вам предлагают дополнительный сертификат, который не присутствовал ранее. Это - сертификат Tomcat-ECDSA.

Это было также задокументировано в связь предварительного релиза: https://www. cisco . com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200651-UCCX-Version-11-5-Prerelease-Field-Commu .html? cachemode=refresh

Опыт агента

После обновления к 11.5, агента можно было бы попросить принять сертификаты на рабочем столе Изящества на основе того, самоподписан ли сертификат, или Центр сертификации (CA) подписан.

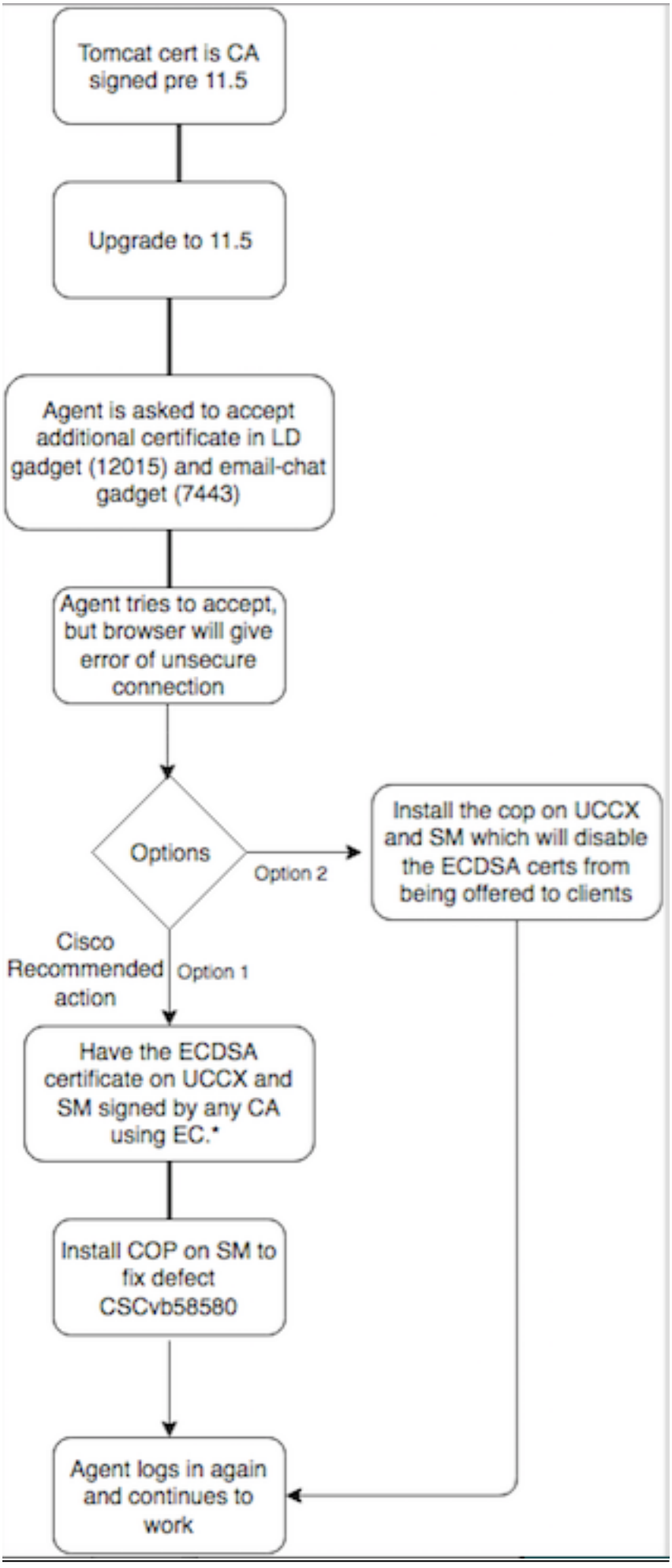
Пользовательский опыт переносит обновление к 11.5



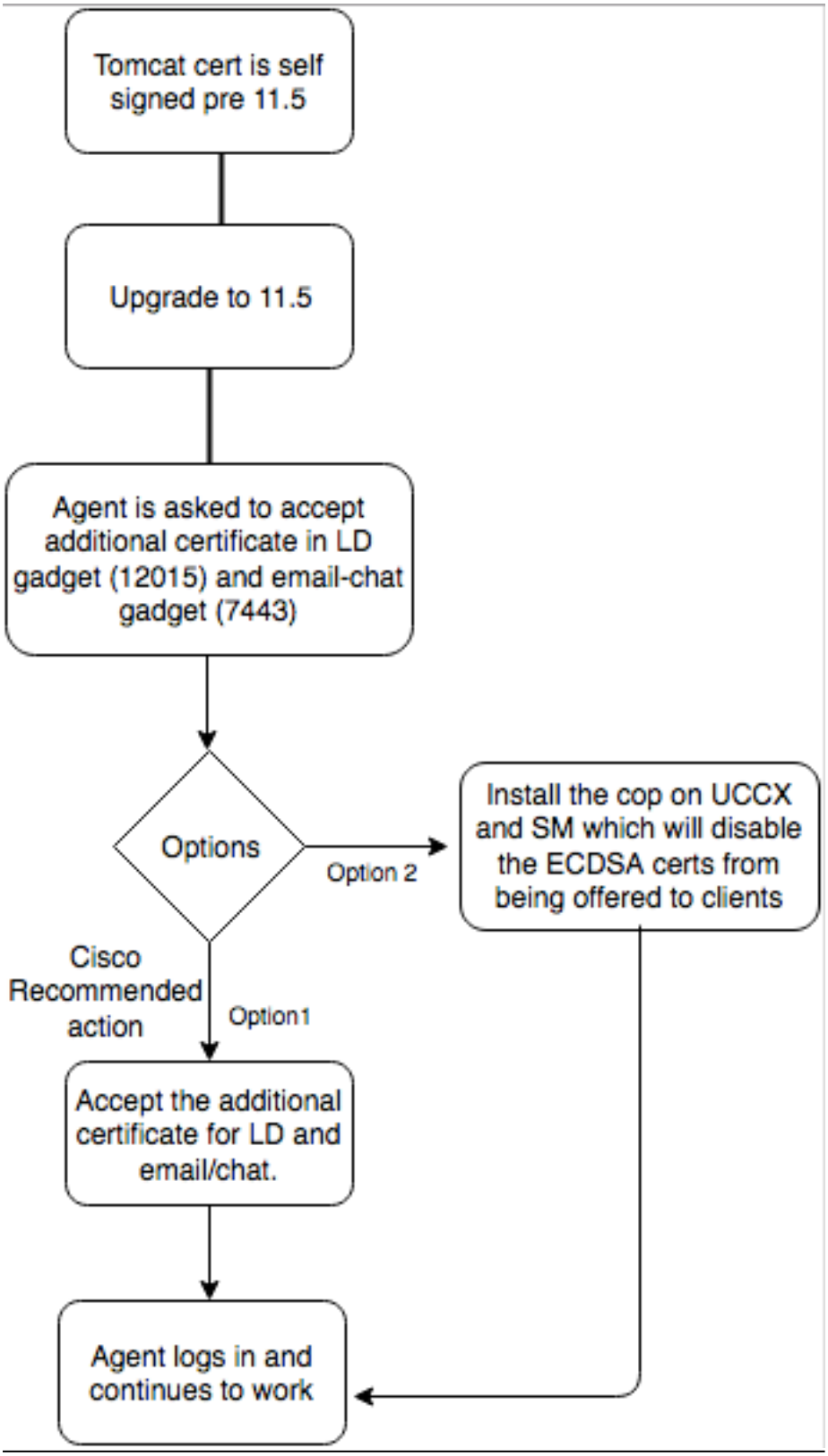
Это вызвано тем, что рабочему столу Изящества теперь предлагают сертификат ECDSA, который не предлагался ранее.

Процедура

CA предобновление подписанных сертификатов


Tomcat cert is CA signed pre 11.5
Upgrade to 11.5
Agent is asked to accept additional certificate in LD gadget (12015) and email-chat gadget (7443)
Agent tries to accept, but browser will give error of unsecure connection
Options
Option 2
Install the cop on UCCX and SM which will disable the ECDSA certs from being offered to clients
Cisco Recommended action
Option 1
Have the ECDSA certificate on UCCX and SM signed by any CA using EC.*
Install COP on SM to fix defect CSCvb58580
Agent logs in again and continues to work

Предобновление подписанных сертификатов



Настройка

Оптимальный метод рекомендован для этого сертификата

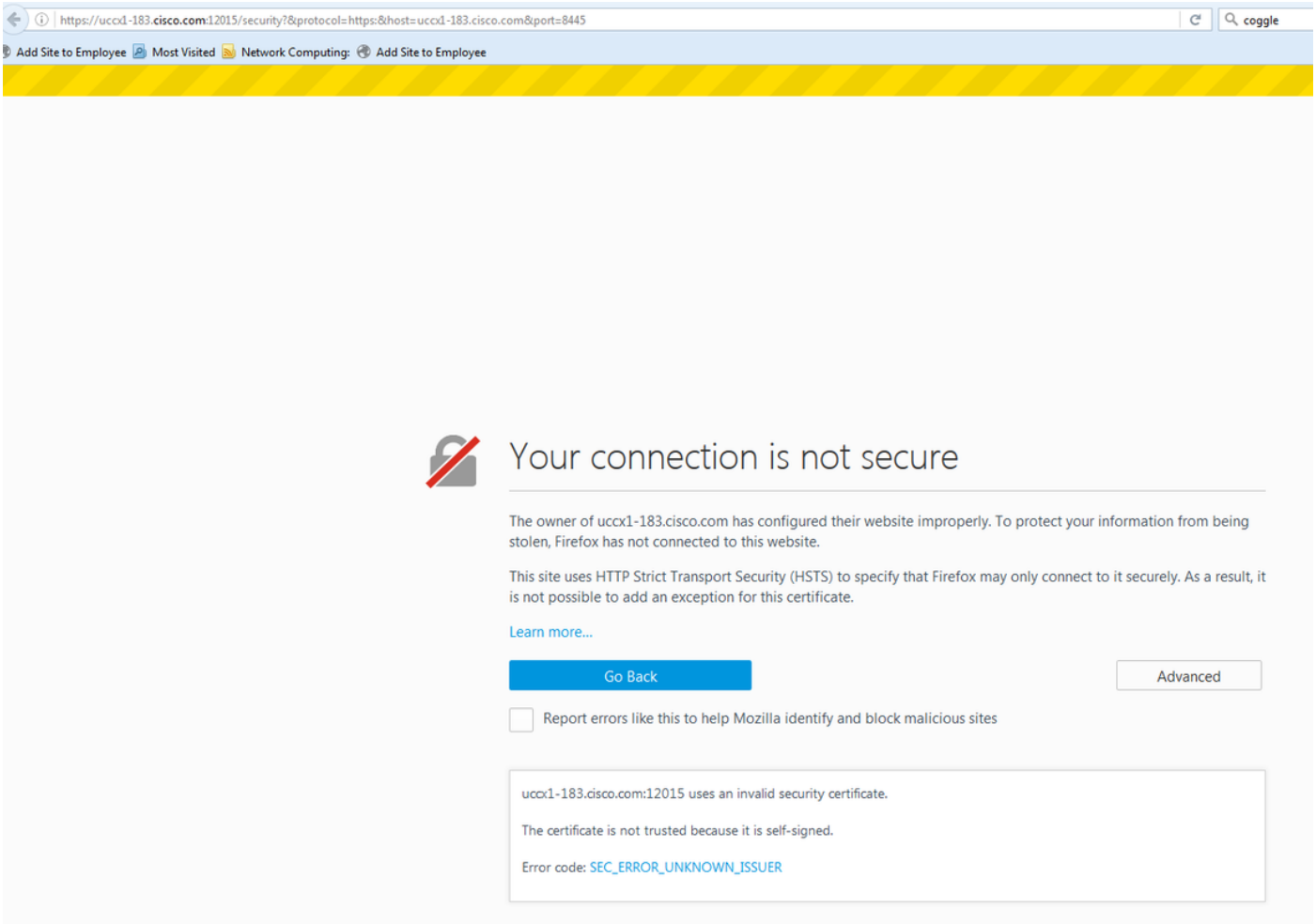
Подписанные сертификаты для UCCX и SocialMiner

При использовании подписанных сертификатов CA этот сертификат ECDSA должен быть подписан Центром сертификации (CA) наряду с другими сертификатами

> **Примечание:** Если бы CA подписывает этот сертификат ECDSA с RSA, этот certifictate не был бы представлен клиенту. Для усиленной безопасности сертификаты ECDSA, предлагаемые клиенту, являются рекомендуемым оптимальным методом.

> **Примечание:** Если сертификат ECDSA на SocialMiner подписан CA с RSA, это вызывает проблемы с электронной почтой и чатом. Это задокументировано в дефектный CSCvb58580, и файл полицейского доступен. Этот COP гарантирует, что сертификаты ECDSA не предлагаются клиентам. Если у вас есть CA, который способен для подписания сертификатов ECDSA с RSA только, не используйте этот сертификат. Используйте полицейского так, чтобы сертификат ECDSA не был предложен, и у вас есть RSA только среда.

При использовании подписанных сертификатов CA и после обновления, вам не подписали сертификат ECDSA и загруженный, агенты испытывают сообщение для принятия дополнительного сертификата. Когда они щелкают **по OK,** они перенаправлены к веб-сайту. Однако этот сбой из-за осуществления безопасности со стороны браузера начиная с сертификата ECDSA сам подписан, и ваши другие веб-сертификаты CA подписаны. Эта связь воспринята как риск securiry.



Выполните эти шаги на каждом узле Издателя и подписчика UCCX и SocialMiner после обновления к UCCX и SocialMiner на версии 11.5:

1. Перейдите к **Странице администрирования операционной системы** и выберите **Security> Certificate Management**.

2. Нажмите **Generate CSR**.

3. От выпадающего списка **Списка Сертификата** выберите **, tomcat-ECDSA** как сертификат называют и нажимают **Generate CSR**.

4. Перейдите к **Безопасности> Управление сертификатами** и выберите **Download CSR**.

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

Передайте новый CSR к независимому поставщику CA или подпишите его с внутренним CA, кто подписывает сертификаты EC. Это произвело бы эти подписанные сертификаты:

- Корневой сертификат для CA (При использовании того же CA для Сертификатов Приложения и сертификатов EC можно пропустить этот шаг),
- Издатель UCCX подписанный сертификат ECDSA
- Абонент UCCX подписанный сертификат ECDSA
- Подписанный сертификат SocialMiner ECDSA

Примечание: При загрузке корневых и промежуточных сертификатов на издателе (UCCX) он был бы автоматически реплицирован 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. Также можно пропустить эту загрузку корневого сертификата, если тот же CA подписывает сертификат EC, и вы уже сделали это при настройке сертификатов приложения UCCX.

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

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-ECDSA** 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. Также можно пропустить эту загрузку корневого сертификата, если тот же CA подписывает сертификат EC, и вы уже сделали это при настройке сертификатов приложения UCCX.

8. Однажды завершенный, перезапустите эти приложения:

   Cisco SocialMinerCisco издатель и подписчик UCCX

Подписанные сертификаты для UCCX и SocialMiner

Если UCCX или подписанные сертификаты использования SocialMiner, агентам нужно рекомендовать принять сертификат, предупреждающий, что им предлагают в почтовом чатом гаджете и Оперативных гаджетах Данных.

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**.

1. **Примечание:** Можно также добавить исключение безопасности для установки сертификата, который эквивалентен вышеупомянутому процессу. Это - одна конфигурация времени на клиенте.

Часто задаваемые вопросы (FAQ)

Мы имеем подписанные сертификаты CA и хотим использовать сертификат ECDSA, который должен быть подписан CA. EC, В то время как мы ждем подписанного сертификата CA, чтобы быть доступными, мы должны иметь, Соответствуют Данным. Какие действия следует предпринять?

Мы не хотим подписать этот дополнительный сертификат или сделать, чтобы агенты

приняли этот дополнительный сертификат. Какие действия следует предпринять?

Несмотря на то, что рекомендация состоит в том, чтобы иметь сертификаты ECDSA быть представленной браузерам, существует опция для отключения ее. Можно установить файл полицейского на UCCX и SocialMiner , который гарантирует, что только сертификаты RSA представлены клиенту. Сертификат ECDSA все еще остается в keystore, но не был бы предложен клиентам.

Если я использую этого полицейского для отключения сертификатов ECDSA, предлагаемых клиентам, я могу включить его назад?

Да, существует предоставленный полицейский отката. Как только это применено, можно было подписать этот сертификат и загруженный к серверу (серверам).

Все сертификаты были бы сделаны ECDSA?

В настоящее время не, но дальнейшие обновления системы защиты на платформе VOS в будущем.

Когда вы устанавливаете COP UCCX?

- Когда вы используете подписанные сертификаты и не хотите, чтобы агенты приняли дополнительные сертификаты
- Когда вы не могли подписать дополнительный сертификат CA

Когда вы устанавливаете COP SM?

- Когда вы используете подписанные сертификаты и не хотите, чтобы агенты приняли дополнительные сертификаты
- Когда вы не могли подписать дополнительный сертификат CA
- Когда у вас есть CA, который способен для подписания сертификатов ECDSA с RSA только

Каковы сертификаты, которые предлагаются другими экземплярами Web-сервера по умолчанию?

Комбинация/Web-сервер сертификата	Опыт Агента по умолчанию после обновления к 11.5 (без любого полицейского)	Tomcat UCCX	UCCX Openfire (Cisco унифицированный сервис уведомлений CCX)	UCCX SocketI
Сам подписанный Tomcat, Сам подписал Tomcat-ECDSA	Агентов попросили бы принять сертификат в Оперативном гаджете Данных и почтовом чатом гаджете	Самоподписанный	Самоподписанный	Самоподписанн
RSA CA подписал Tomcat, RSA CA подписал Tomcat-ECDSA	Агенты могут использовать Изящество и Оперативные Данные, но гаджет	RSA	RSA	RSA

RSA CA подписал Tomcat, EC CA подписало Tomcat-ECDSA	почтового чата не загрузится, и веб-страница SocialMiner не загружается.* Агенты могут использовать Изящество и с Оперативными Данными и с электронной почтой чата*	RSA	RSA	ECDSA
RSA CA подписал Tomcat, сам подписанный Tomcat-ECDSA	Агентов попросили бы принять дополнительный сертификат в Оперативных Данных и гаджете почтового чата. Примите сертификат от Оперативных сбоев гаджета Данных, признайте, что сертификат от гаджета почтового чата был бы успешен.*	RSA	RSA	Самоподписанн (Агенты не могу принять из-за браузера, принудил измерения безопасности. С снимок экрана выше. Необходимо было подписать сертификат EC CA или установить полицейского на UCCX для отключения сертификатов ECDSA, предлагаемых клиентам.)

Дополнительные сведения

- UCCX ECDSA COP - https://программное обеспечение. cisco . com/download/release.html? mdfid=286309734&softwareid=280840578&release=11.5 (1) &flowid=80822
- SocialMiner ECDSA COP - https://программное обеспечение. cisco . com/download/release.html? mdfid=283613136&flowid=73189&release=11.5 (1) &softwareid=283812550&sortparam =
- Информация о Сертификате UCCX - http://www. cisco . com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html