Поддержка SHA 256 UCCX

Содержание

Введение

Этот документ описывает поддержку SHA 256 Cisco Unified Contact Center Express (UCCX). Шифрование SHA-1 будет скоро осуждено, и все поддерживаемые web-браузеры для UCCX начнут блокировать веб-страницы от серверов, которые предлагают сертификаты с шифрованием SHA-1.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco Unified Contact Center Express (UCCX)
- Управление сертификатами

Объявления от Microsoft и Mozilla

[Обновление осуждения SHA-1](#)

[Продолжение постепенно сократить сертификаты SHA-1](#)

В этих предупреждениях изготовители браузера сообщили, что браузеры покажут, что bypassable предупреждения для сертификатов SHA-1 встретились, которые выполнены с

датами ValidFrom после 1 января 2016.

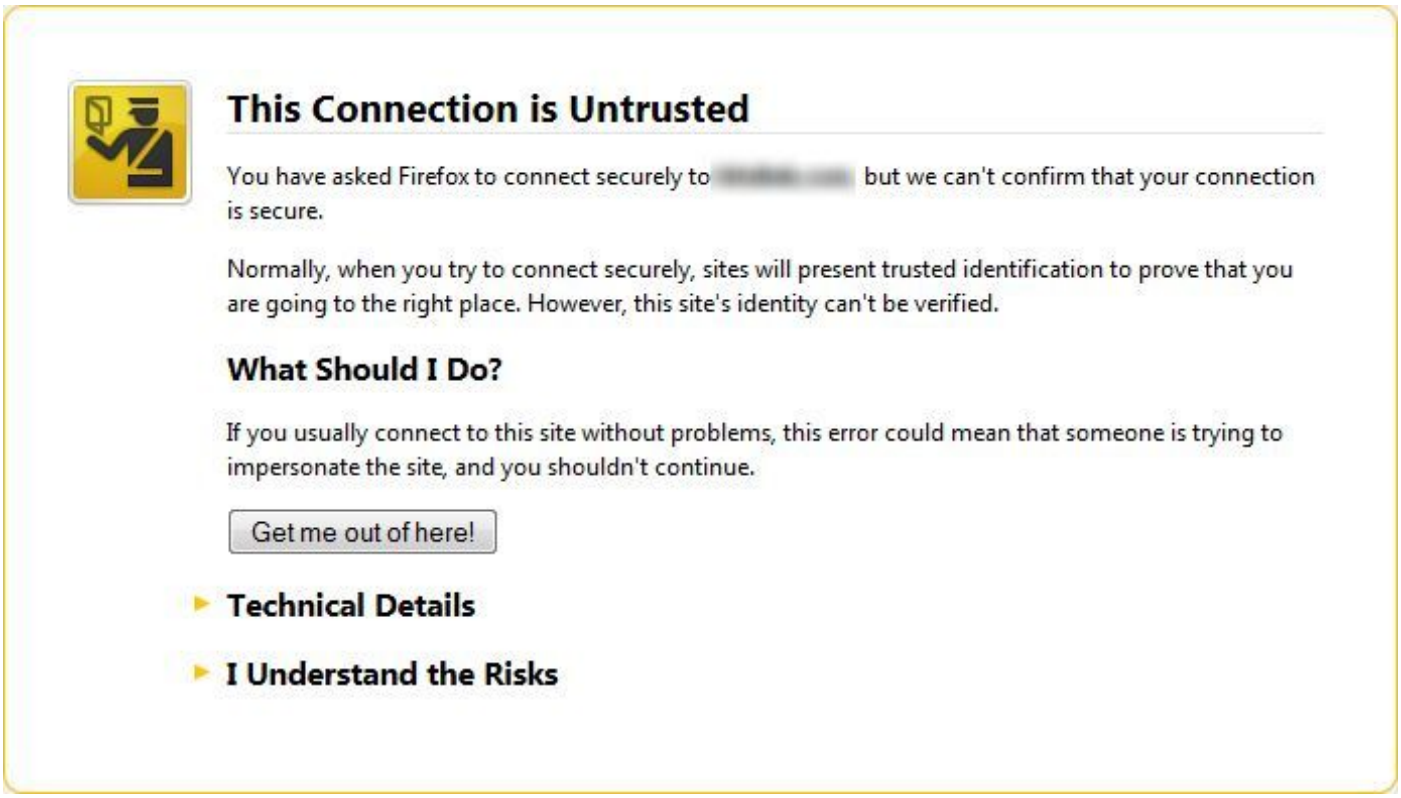
Кроме того, текущий план записи состоит в том, чтобы заблокировать веб-сайты, которые используют сертификаты SHA-1 после 1 января 2017 независимо от записи ValidFrom в сертификате. Однако с недавними атаками, которые предназначаются для сертификатов SHA-1, эти браузеры могли бы переместить эту шкалу времени вверх и заблокировать веб-сайты, которые используют сертификаты SHA-1 после 1 января 2017 независимо от даты выпуска сертификата.

Cisco советует клиентам читать объявления подробно и оставаться актуальными на дальнейших объявлениях от Microsoft и Mozilla по этой теме.

Некоторые версии UCCX генерируют сертификаты SHA-1. Если вы обращаетесь к веб-страницам UCCX, защищенным сертификатами SHA-1, они могли бы генерировать предупреждение или заблокированы в соответствии с датами и правилами, на которые обращают внимание ранее.

Пользовательский опыт

Когда сертификат SHA-1 обнаружен, зависит от даты ValidFrom и ранее перечисленных правил, пользователь мог бы видеть сообщение, подобное этому:



Зависящий от принятых решений, пользователь мог бы или не мог бы быть в состоянии обойти это предупреждение.

Факторы UCCX

Эти таблицы описывают влияние сертификата SHA-1 и стратегии смягчения каждой версии UCCX в настоящее время при обслуживании программного обеспечения.

Нотации, используемые в этом документе

Нотация	Описание
✅	Уже поддерживаемый. Никакие дальнейшие действия не требуются.
⚠	Поддержка доступна, но необходима регенерация сертификатов.
⛔	Поддержка не доступна.

UCCX 11.5

	Администрирование UCCX	Администрирование CUIC Оперативный Data#	Администрирование Desktop# изящества	Электронная почта агента и чат с SocialMiner*	Шаги RES
Новая установка	✅	✅	✅	✅	
Обновление от предыдущей версии	⚠ Сертификаты UCCX сохраняют алгоритм от более старых версий. Если генерируется с ключом SHA 11 в более старых версиях, подписанные сертификаты являются основанным SHA-1 и должны быть восстановлены.	⚠ Сертификаты Cisco Unified Intelligence Center (CUIC) UCCX сохраняют алгоритм от более старых версий. Если генерируется с ключом SHA 11 в более старых версиях, подписанные сертификаты являются основанным SHA-1 и должны быть восстановлены.	⚠ Сертификаты Изящества UCCX сохраняют алгоритм от более старых версий. Если генерируется с ключом SHA 11 в более старых версиях, подписанные сертификаты являются основанным SHA-1 и должны быть восстановлены.	⚠ SocialMiner и сертификаты UCCX сохраняют алгоритм от более старых версий. Если генерируется с ключом SHA 11 в более старых версиях, подписанные сертификаты являются основанным SHA-1 и должны быть восстановлены.	UCCX удале серве исп серт SHA-1 Предст госуда Перед ОСТ шага работ то серт восста

Примечание: *Восстановленный сертификат (сертификаты) MediaSense и SocialMiner должен быть повторно импортирован в UCCX.

Примечание: #No отдельные действия необходимы для Изящества и CUIC. Сертификаты восстановлены только однажды на странице администрирования платформы UCCX.

UCCX 11.0 (1)

	Администрирование UCCX	Администрирование CUIC оперативный Data#	Администрирование Desktop# изящества	Электронная почта агента и чат с SocialMiner **	Ша

Новая установка	По умолчанию все самоподписанные новые сертификаты установки являются сертификатами SHA-1 и должны быть восстановлены.	По умолчанию все самоподписанные новые сертификаты установки являются сертификатами SHA-1 и должны быть восстановлены.	По умолчанию все самоподписанные новые сертификаты установки являются сертификатами SHA-1 и должны быть восстановлены.	По умолчанию все самоподписанные новые сертификаты установки являются сертификатами SHA-1 и должны быть восстановлены.	откл кото серт в к ост С ш ра с вос
Обновление от предыдущей версии	Сертификаты UCCX сохраняют алгоритм от более старых версий. Если генерируется с ключом SHA 11 в более старых версиях, подписанные сертификаты являются основанным SHA-1 и должны быть восстановлены.	UCCX CUIC сертификаты сохраняют алгоритм от более старых версий. Если генерируется с ключом SHA 11 в более старых версиях, подписанные сертификаты являются основанным SHA-1 и должны быть восстановлены.	Сертификаты Изящества UCCX сохраняют алгоритм от более старых версий. Если генерируется с ключом SHA 11 в более старых версиях, подписанные сертификаты являются основанным SHA-1 и должны быть восстановлены.	SocialMiner и сертификаты UCCX сохраняют алгоритм от более старых версий. Если генерируется с ключом SHA 11 в более старых версиях, подписанные сертификаты являются основанным SHA-1 и должны быть восстановлены.	UC уда се серт в к ост С ш ра с вос

Примечание: *Engineering Special (ES) будет освобожден, чтобы позволить MediaSense 10.5 и 11.0 генерировать и принимать SHA 256 сертификатов.

Примечание: ** Восстановленный сертификат (сертификаты) MediaSense и SocialMiner должен быть повторно импортирован в UCCX.

Примечание: #No отдельные действия необходимы для Изящества и CUIC. Сертификаты восстановлены только однажды на странице администрирования платформы UCCX.

UCCX 10.5 и 10.6

Администрирование UCCX	Администрирование CUIC оперативный Data#	Администрирование изящества Desktop#	Электронная почта агента и чат с SocialMiner*	Шаги сценар REST U

Новая установка	По умолчанию все самоподписанные новые сертификаты установки являются сертификатами SHA-1 и должны быть восстановлены.	По умолчанию все самоподписанные новые сертификаты установки являются сертификатами SHA-1 и должны быть восстановлены.	По умолчанию все самоподписанные новые сертификаты установки являются сертификатами SHA-1 и должны быть восстановлены.	Поддержка SHA 256 электронной почты агента и чата доступна только в SocialMiner (SM) v11, и SM v11 не совместим с UCCX v10.x.	UCCX отклон удален Web-сер котор использ сертифи SHA-1 качестве остальн связь ОСТАЛЬ шагает, б работа после тог сертифи восстанов на UC
Обновление от предыдущей версии	Сертификаты сохраняют алгоритм от более старых версий. Если генерируется с ключом SHA 11 в более старых версиях, подписанные сертификаты являются основанным SHA-1 и должны быть восстановлены.	Сертификаты сохраняют алгоритм от более старых версий. Если генерируется с ключом SHA 11 в более старых версиях, подписанные сертификаты являются основанным SHA-1 и должны быть восстановлены.	Сертификаты сохраняют алгоритм от более старых версий. Если генерируется с ключом SHA 11 в более старых версиях, подписанные сертификаты являются основанным SHA-1 и должны быть восстановлены.	Поддержка SHA 256 электронной почты агента и чата доступна только в SM v11, и SM v11 не совместим с UCCX v10.x.	UCCX отклон удален Web-сер котор использ сертифи SHA-1 качестве остальн связь ОСТАЛЬ шагает, б работа после тог сертифи восстанов на UC

Примечание: *Техническое Специальное предложение будет освобождено, чтобы позволить SocialMiner 10.6 генерировать и принимать SHA 256 сертификатов.

Примечание: ** Engineering Special (ES) будет освобожден, чтобы позволить MediaSense 10.0 и 10.5 генерировать и принимать SHA 256 сертификатов.

Примечание: *** восстановленный сертификат (сертификаты) MediaSense и SocialMiner должен быть повторно импортирован в UCCX.

Примечание: #No отдельные действия необходимы для Изящества и CUIC. Сертификаты восстановлены только однажды на странице администрирования

платформы UCCX.

UCCX 10.0

	Администрирование UCCX **	Администрирование CUIC оперативный Data#	Администрирование Desktop# изящества	Чат агента с SocialMiner*	Шаги сценари REST UC
Новая установка	Подписанный сертификат по умолчанию является SHA-1. Сертификат регенерации не предоставляет возможность для SHA 256.	Подписанный сертификат по умолчанию является SHA-1. Сертификат регенерации не предоставляет возможность для SHA 256.	Подписанный сертификат по умолчанию является SHA-1. Сертификат регенерации не предоставляет возможность для SHA 256.	Поддержка SHA 256 чата агента доступна только в SM v11, и SM v11 не совместим с UCCX v10. x.	UCCX н отклони удаленн Web-серв которы использу сертифик SHA-1 качестве ч остальн связь. ОСТАЛЬН шагает, бу работат после того сертифик восстанов на UCC
Обновление от предыдущей версии	Подписанный сертификат по умолчанию является SHA-1. Сертификат регенерации не предоставляет возможность для SHA 256.	Подписанный сертификат по умолчанию является SHA-1. Сертификат регенерации не предоставляет возможность для SHA 256.	Подписанный сертификат по умолчанию является SHA-1. Сертификат регенерации не предоставляет возможность для SHA 256.	Поддержка SHA 256 чата агента доступна только в SM v11, и SM v11 не совместим с UCCX v10. x.	UCCX н отклони удаленн Web-серв которы использу сертифик SHA-1 качестве ч остальн связь. ОСТАЛЬН шагает, бу работат после того сертифик восстанов на UCC

Примечание: *Техническое Специальное предложение будет освобождено, чтобы позволить SocialMiner 10.6 генерировать и принимать SHA 256 сертификатов.

Примечание: ** Engineering Special (ES) будет освобожден, чтобы позволить MediaSense 10.0 генерировать и принимать SHA 256 сертификатов.

Примечание: *** восстановленный сертификат (сертификаты) MediaSense и SocialMiner должен быть повторно импортирован в UCCX.

Примечание: #No отдельные действия необходимы для Изящества и CUIC. Сертификаты восстановлены только однажды на странице администрирования платформы UCCX.

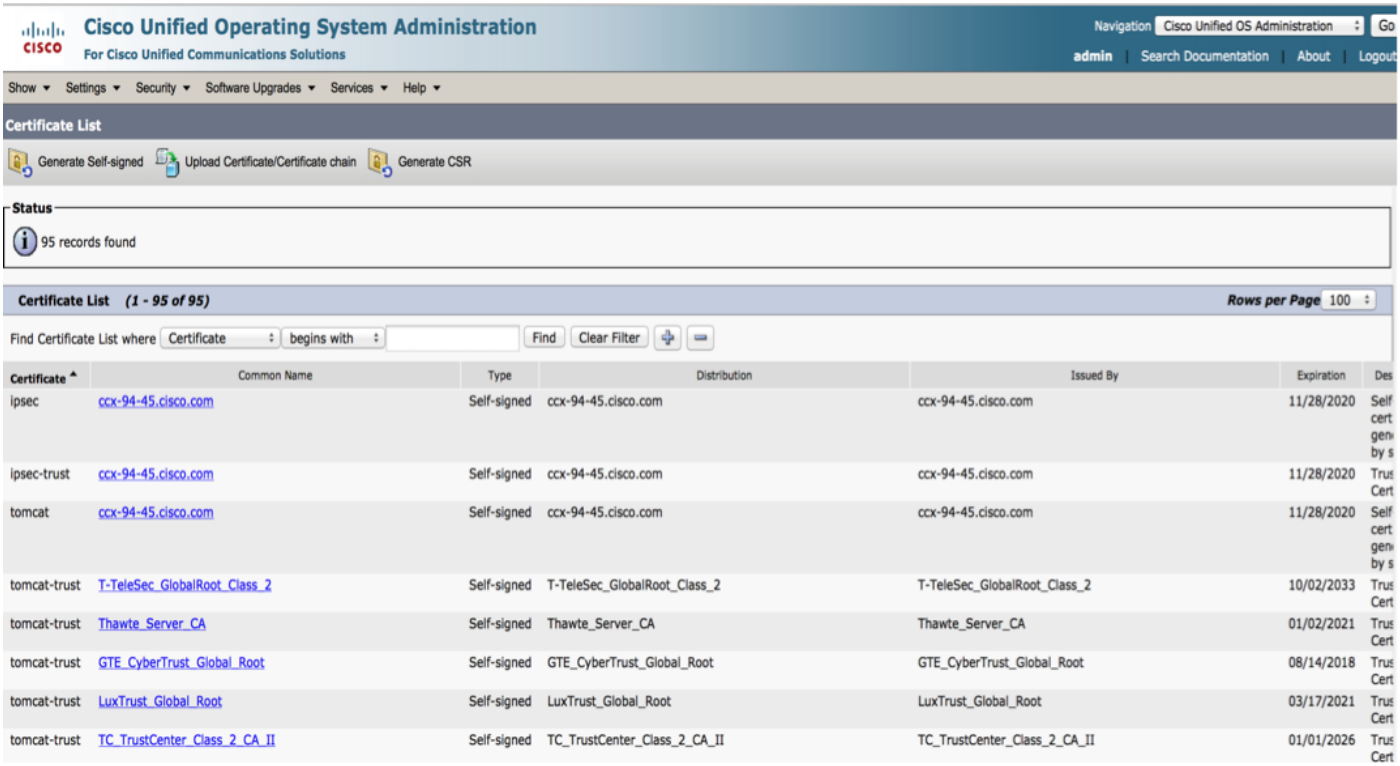
Инструкции управления сертификатами

Существует три типа сертификатов, которые должны быть проверены и потенциально восстановлены:

- Сам подписанные сертификаты
- Сертификаты доверенного корня
- Подписанные сертификаты третьей стороны

Подписанные сертификаты

Перейдите к Странице администрирования операционной системы. Выберите **Security> Navigate to Certificate management**. **Нажмите кнопку "Найти".**



Заметьте четыре категории сертификата:

- iPSec
- доверие ipsec
- tomcat
- доверие tomcat

Сертификаты под **tomcat** категории и **Самоподписанным** типом являются теми, которые

требуют регенерации. В предыдущем образе третий сертификат является тем, который требует регенерации.

Выполните эти шаги для регенерации сертификатов:

Шаг 1. Нажмите Common Name сертификата.

Шаг 2. От всплывающего окна нажмите **Regenerate**.

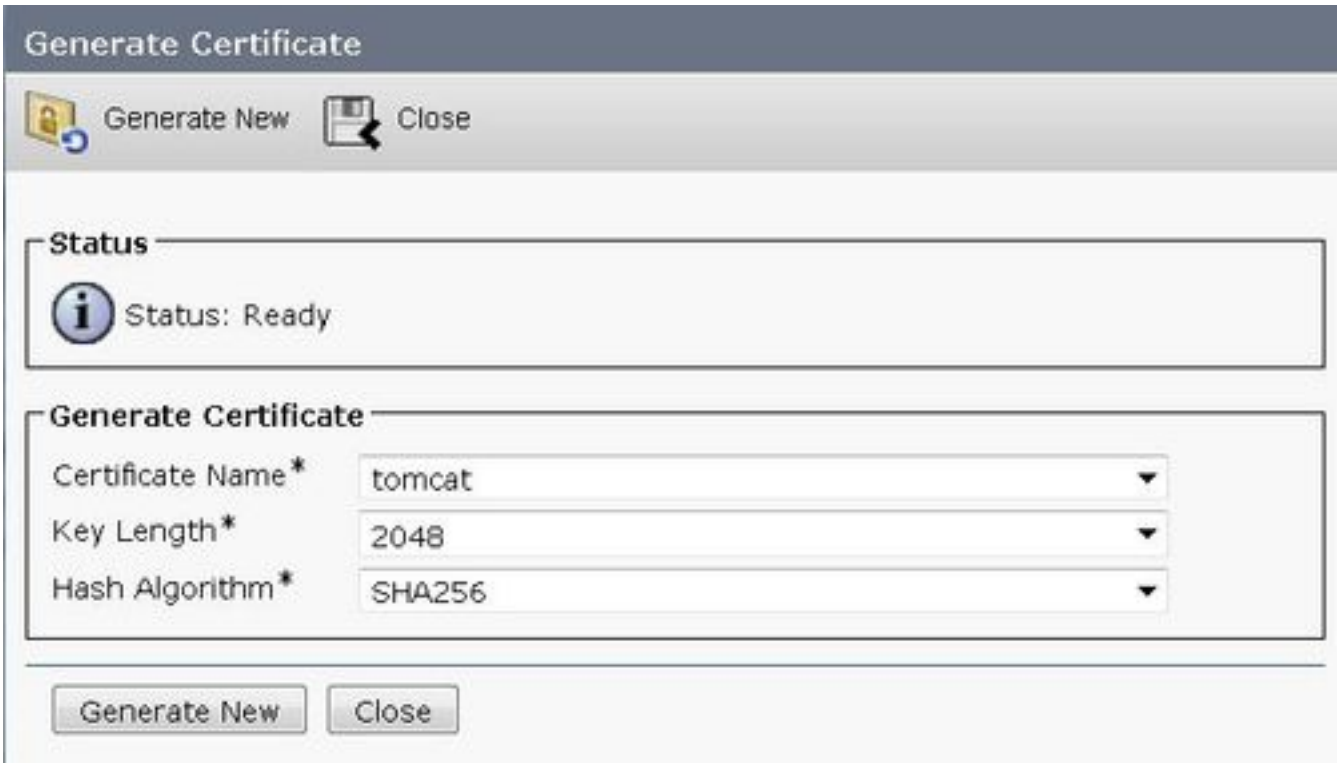
Шаг 3. Выберите алгоритм шифрования SHA 256.

Для версии 10.6 UCCX выполните эти шаги для регенерации сертификатов:

Шаг 1. Щелкните **по Generate New**.

Шаг 2. Выберите *Certificate Name* как **tomcat**, *Длина ключа* как **2048** и *Алгоритм хэширования* как **SHA256.**

Шаг 3. Нажмите **Generate New.**



Сертификаты доверенного корня

Это сертификаты, которые предоставлены платформой. SHA-1 базировался, подписи для этих сертификатов не являются проблемой, потому что этим сертификатам доверяют клиенты Transport Layer Security (TLS) на основе их идентичности, а не подпись их хэша.

Подписанные сертификаты третьей стороны

Сертификаты, подписанные Центром сертификации третьей стороны с алгоритмом SHA-1, должны быть повторно импортированы с SHA 256 подписанных сертификатов. Все сертификаты в цепочке сертификатов должны быть оставлены с SHA 256.

Дополнительные примечания

Последние Инженерные настройки зарегистрированы на cisco.com, когда доступно. Проверяйте соответствующие страницы продукта регулярно для Технических Специальных загрузок.

- Для любой помощи на регенерации сертификата или привязанных проблемах, откройте Обращение в Центр технической поддержки Cisco (TAC).
- Клиенты, которые работают на версиях 8.x или 9.x UCCX, должны запланировать обновить к последним поддерживаемым релизам для поддержания Cisco и поддержки обозревателя.