

# Поддержка SHA 256 UCCX

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Объявления от Microsoft и Mozilla](#)

[Пользовательский опыт](#)

[Факторы UCCX](#)

[Нотации, используемые в этом документе](#)

[UCCX 11.5](#)

[UCCX 11.0 \(1\)](#)

[UCCX 10.5 и 10.6](#)

[UCCX 10.0](#)

[Инструкции управления сертификатами](#)

[Подписанные сертификаты](#)

[Сертификаты доверенного корня](#)

[Подписанные сертификаты третьей стороны](#)

[Дополнительные примечания](#)

## 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.

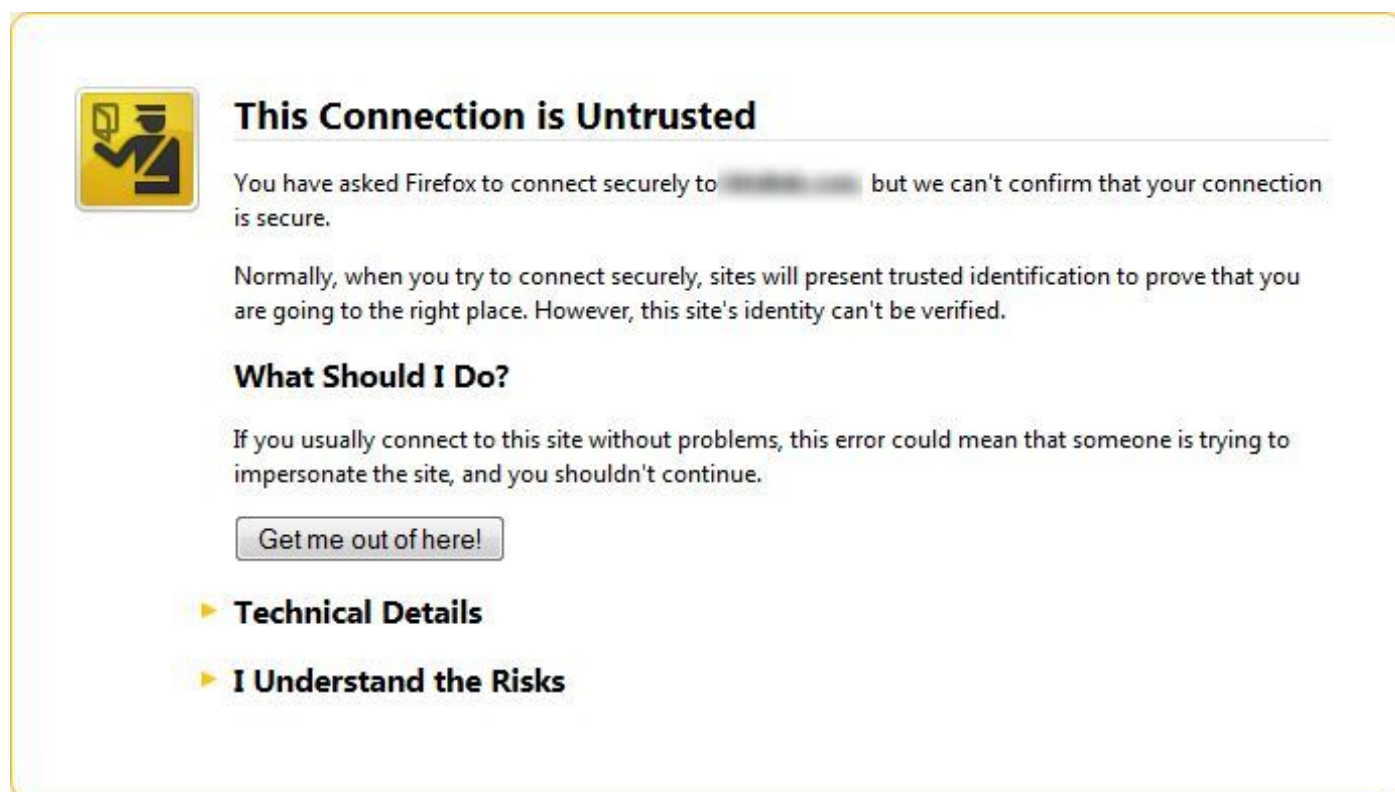
Кроме того, текущий план записи состоит в том, чтобы заблокировать веб-сайты, которые используют сертификаты SHA-1 после 1 января 2017 независимо от записи ValidFrom в сертификате. Однако с недавними атаками, которые предназначаются для сертификатов SHA-1, эти браузеры могли бы переместить эту шкалу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



**This Connection is Untrusted**

You have asked Firefox to connect securely to [redacted] but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

**What Should I Do?**

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)




- ▶ **Technical Details**
- ▶ **I Understand the Risks**

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 CUIС Оперативный Data#	Администрирование изящества Desktop#	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 (CUIС) 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 сервере исп серт SHA-1 Предст госуда Перед ОСТ шага рабо то серт восста U

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

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

## UCCX 11.0 (1)

	Администрирование UCCX	Администрирование CUIС оперативный Data#	Администрирование изящества Desktop#	Электронная почта агента и чат с SocialMiner**	Шаги RES

<b>Новая установка</b>	 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 V кото серт в к ост С ш ра с вос
<b>Обновление от предыдущей версии</b>	 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 уд 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 сценария 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. х.	 UCCX отклонил удаленный Web-сервер, который использует сертификаты SHA-1 в качестве остальных связей. ОСТАЛЬНЫЕ шагают, браться работа после того сертификаты восстановлены на UCCX.
	 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. х.	 UCCX отклонил удаленный Web-сервер, который использует сертификаты SHA-1 в качестве остальных связей. ОСТАЛЬНЫЕ шагают, браться работа после того сертификаты восстановлены на UCCX.

**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 CUIС. Сертификаты восстановлены только однажды на странице администрирования

платформы UCCX.

## UCCX 10.0

	Администрирование UCCX **	Администрирование CUIС оперативный Data#	Администрирование изящества Desktop#	Чат агента с SocialMiner*	Шаги сценария REST UC
Новая установка	 <p>Подписанный сертификат по умолчанию является SHA-1. Сертификат регенерации не предоставляет возможность для SHA 256.</p>	 <p>Подписанный сертификат по умолчанию является SHA-1. Сертификат регенерации не предоставляет возможность для SHA 256.</p>	 <p>Подписанный сертификат по умолчанию является SHA-1. Сертификат регенерации не предоставляет возможность для SHA 256.</p>	 <p>Поддержка SHA 256 чата агента доступна только в SM v11, и SM v11 не совместим с UCCX v10. x.</p>	 <p>UCCX не отклонит удаленный Web-сервис, который использует сертификат SHA-1 в качестве чата, остальные шаги не выполняются. ОСТАЛЬНЫЕ шаги выполняются, но работат после того, как сертификат восстановлен на UCCX.</p>
Обновление от предыдущей версии	 <p>Подписанный сертификат по умолчанию является SHA-1. Сертификат регенерации не предоставляет возможность для SHA 256.</p>	 <p>Подписанный сертификат по умолчанию является SHA-1. Сертификат регенерации не предоставляет возможность для SHA 256.</p>	 <p>Подписанный сертификат по умолчанию является SHA-1. Сертификат регенерации не предоставляет возможность для SHA 256.</p>	 <p>Поддержка SHA 256 чата агента доступна только в SM v11, и SM v11 не совместим с UCCX v10. x.</p>	 <p>UCCX не отклонит удаленный Web-сервис, который использует сертификат SHA-1 в качестве чата, остальные шаги не выполняются. ОСТАЛЬНЫЕ шаги выполняются, но работат после того, как сертификат восстановлен на UCCX.</p>

**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 CUIС. Сертификаты восстановлены только однажды на странице администрирования платформы UCCX.

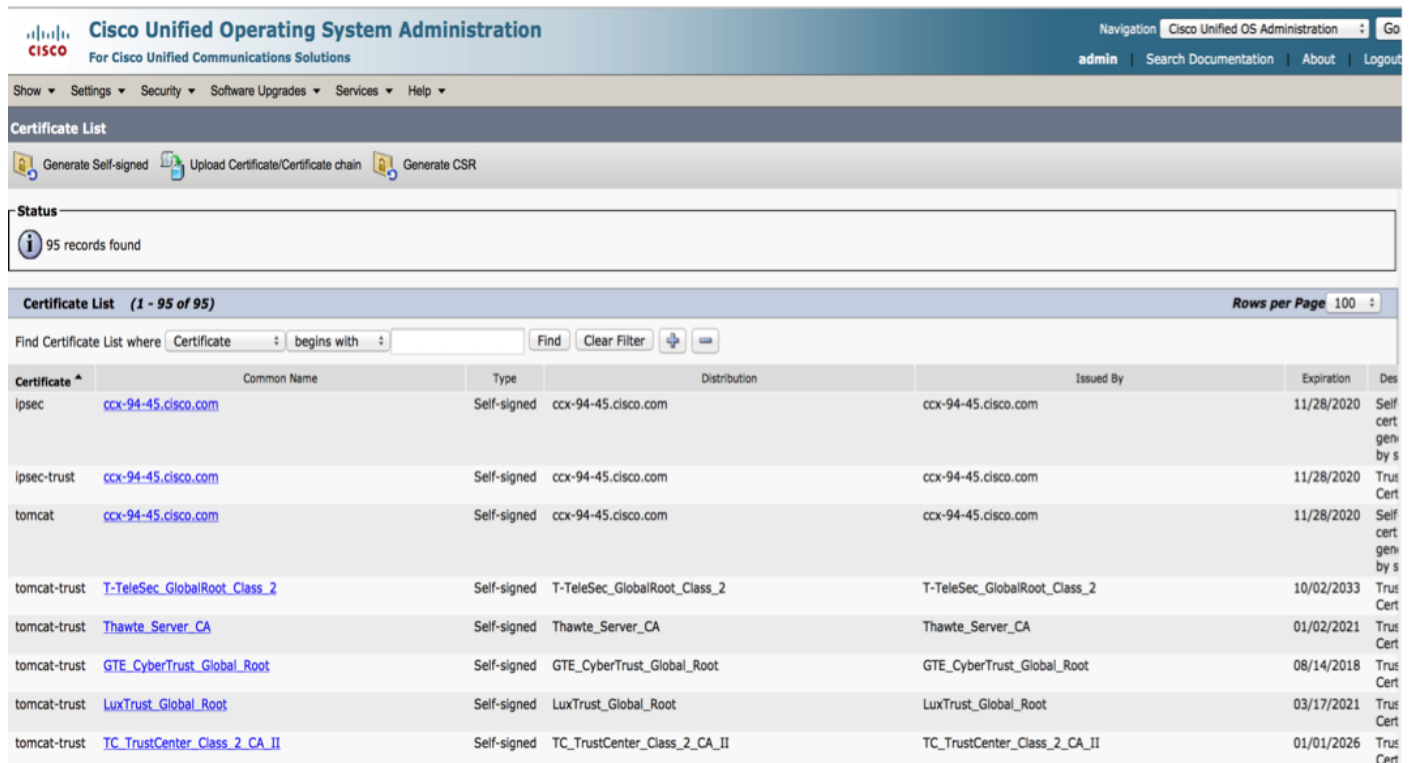
## Инструкции управления сертификатами

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".



The screenshot shows the Cisco Unified Operating System Administration interface. The main heading is "Certificate List" with a status of "95 records found". Below this is a search bar and a table of certificates. The table has the following columns: Certificate, Common Name, Type, Distribution, Issued By, Expiration, and Description. The table lists several certificates, including ipsec, ipsec-trust, tomcat, and tomcat-trust, with their respective details.

Certificate	Common Name	Type	Distribution	Issued By	Expiration	Description
ipsec	<a href="#">ccx-94-45.cisco.com</a>	Self-signed	ccx-94-45.cisco.com	ccx-94-45.cisco.com	11/28/2020	Self cert gen by s
ipsec-trust	<a href="#">ccx-94-45.cisco.com</a>	Self-signed	ccx-94-45.cisco.com	ccx-94-45.cisco.com	11/28/2020	Trus Cert
tomcat	<a href="#">ccx-94-45.cisco.com</a>	Self-signed	ccx-94-45.cisco.com	ccx-94-45.cisco.com	11/28/2020	Self cert gen by s
tomcat-trust	<a href="#">T-TeleSec_GlobalRoot_Class_2</a>	Self-signed	T-TeleSec_GlobalRoot_Class_2	T-TeleSec_GlobalRoot_Class_2	10/02/2033	Trus Cert
tomcat-trust	<a href="#">Thawte_Server_CA</a>	Self-signed	Thawte_Server_CA	Thawte_Server_CA	01/02/2021	Trus Cert
tomcat-trust	<a href="#">GTE_CyberTrust_Global_Root</a>	Self-signed	GTE_CyberTrust_Global_Root	GTE_CyberTrust_Global_Root	08/14/2018	Trus Cert
tomcat-trust	<a href="#">LuxTrust_Global_Root</a>	Self-signed	LuxTrust_Global_Root	LuxTrust_Global_Root	03/17/2021	Trus Cert
tomcat-trust	<a href="#">TC_TrustCenter_Class_2_CA_II</a>	Self-signed	TC_TrustCenter_Class_2_CA_II	TC_TrustCenter_Class_2_CA_II	01/01/2026	Trus Cert

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**.

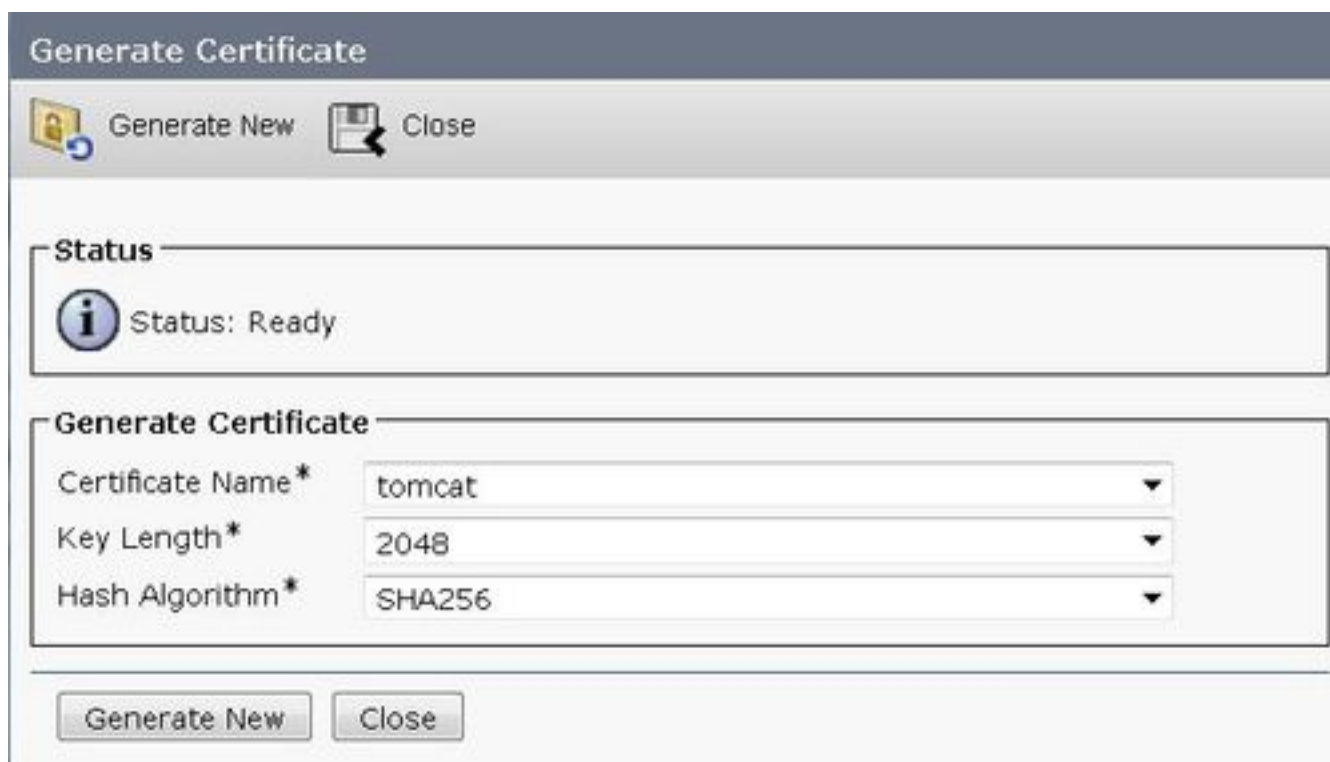
Шаг 3. Выберите алгоритм шифрования SHA 256.

Для версии 10.6 USSX 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](https://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 UCSX, должны запланировать обновить к последним поддерживаемым релизам для поддержания Cisco и поддержки обозревателя.