

# Генерируйте SHA 256 подписанных сертификатов для Cisco веб-сервисы UCCE

## Содержание

[Введение](#)

[Проблема](#)

[Решение](#)

[Решение для WebSetup и администрирования CCE](#)

[Решение для диагностического портала платформы](#)

[Проверка](#)

[Похожие статьи](#)

## Введение

Этот документ описывает процесс генерации подписанных сертификатов с помощью алгоритма сигнатуры SHA 256 сертификата для Cisco Unified Contact Center Enterprise (UCCE) веб-сервисы как веб-Настройка или администрирование CCE.

## Проблема

Cisco UCCE имеет несколько веб-сервисов, размещенных Microsoft Internet Information Services (IIS) сервер. Microsoft IIS в развертываниях UCCE по умолчанию использует подписанные сертификаты с алгоритмом сигнатуры сертификата SHA-1.

Алгоритм SHA-1 считает небезопасным большинство браузеров, поэтому в некоторый момент важные программные средства как администрирование CCE, используемое супервизорами для агента, обучающего новым навыкам, могут стать недоступными.

## Решение

Решение той проблемы состоит в том, чтобы генерировать SHA 256 сертификатов для сервера IIS для использования.

**% Warning:** Рекомендуется использовать подписанные сертификаты Центра сертификации. Так генерация подписанных сертификатов, описанных здесь, как должны полагать, как временный обходной путь восстанавливает сервис быстро.

**Примечание:** В случае, если Редактор Интернет-сценария ICM используется для удаленного управления сценария существует потребность использовать Утилиту Шифрования SSL для генерации сертификата для него.

## Решение для WebSetup и администрирования CCE

1. Запустите программное средство Windows PowerShell на сервере UCCE.

2. В PowerShell вводят команду

```
New-SelfSignedCertificate -DnsName "pgb.allevich.local" -CertStoreLocation  
"cert:\LocalMachine\My"
```

Где параметр после **DnsName** задаст общее имя (CN) сертификата. Замените параметр после DnsName к корректному для сервера. Сертификат будет генерироваться с законностью одного года.

**Примечание:** Общее имя в сертификате должно совпасть с Полным доменным именем (FQDN) сервера.

3. Открытое программное средство Консоли управления Microsoft (MMC). Выберите **File->, Add/Remove Snap - В...->** выбирает **Certificates**, выбирает **Учетную запись компьютера** и добавляет его к выбранному моментальному-снимку-ins. Нажмите ok, затем перейдите к **Корневым (сертификат) консолям-> Сертификаты (Локальный компьютер)-> Персональный-> Сертификаты**.

Гарантируйте, что недавно созданный сертификат присутствует здесь. Сертификату не настроят дружественное название, таким образом, это сможет быть распознано на основе его CN и дата окончания действия.

Дружественное название может быть назначено на сертификат путем выбора **свойств** сертификата и заполнения **Дружественного** текстового поля **названия** с соответствующим названием.

4. Запустите Менеджера информационных сервисов интернета (IIS). Выберите IIS Default Web Site, и на правой панели выбирают **Bindings**. Выберите **HTTPS->, Edit** и из списка сертификата SSL выбирает генерируемый сертификат самоподписанного SHA 256.

5. Перезапустите сервис "Сервиса веб-публикации".

## Решение для диагностического портика платформы

1. Повторите шаги 1-3.

Будет генерироваться новый подписанный сертификат. Для программного средства Портка существует другой способ связать сертификат.

2. Удалите текущую привязку сертификата для программного средства Портка.

```
cd c:\icm\serviceability\diagnostics\bin
```

```
DiagFwCertMgr /task:UnbindCert
```

3. Свяжите подписанный сертификат, генерируемый для Портка.

Откройте подписанный сертификат , генерируемый для программного средства Портка, и

выберите вкладку **Details**. Скопируйте значение Следы большого пальца текстовому редактору.

**Примечание:** В некоторых текстовых редакторах след большого пальца автоматически предварительно ожидается с вопросительным знаком. Удалите его.

Удалите все пробелы из следы большого пальца и используйте его в следующей команде.

```
DiagFwCertMgr /task:BindCertFromStore /certhash:<thumbprint-value>
```

4. Гарантируйте, что привязка сертификата была успешным использованием этой команды.

```
DiagFwCertMgr /task:ValidateCertBinding
```

Подобное сообщение должно быть отображено в выходных данных.

"Привязка сертификата ДОПУСТИМА"

5. Перезапустите Диагностический сервис Платформы.

```
sc stop "diagfwsvc"  
sc start "diagfwsvc"
```

## Проверка

Очистите кэш-память обозревателя и историю. Веб-страница Административной службы ССЕ доступа и вы должны получить предупреждение подписанного сертификата.

Просмотрите сведения о сертификате и гарантируйте, что сертификат имеет алгоритм сигнатуры SHA 256 сертификата.

## Похожие статьи

[Генерируйте подписанный сертификат CA для диагностического программного средства порта UCCE](#)

[Генерируйте подписанный сертификат CA для веб-настройки UCCE](#)

[Генерируйте подписанный сертификат CA для VOS базирующийся сервер Использование CLI](#)

[Генерируйте подписанный сертификат CA для CVP сервер OAMP](#)