Содержание

Введение

Для использования HTTPS для безопасной связи между Изяществом, Cisco Unified Intelligence Center (CUIC) и Оперативными Серверами данных, настройка сертификатов безопасности необходима. По умолчанию эти серверы предоставляют самоподписанные certifcates, которые используются, или клиенты могут обеспечить и установить сертификат Центра сертификации (CA). Они CA certs могут быть получены или от Стороннего поставщика как VeriSign, Thawte, GeoTrust или могут быть произведены внутренне.

Этот документ стремится объяснять подробно шаги, включенные, чтобы получить и установить сертификат Центра сертификации (CA), генерируемый от стороннего поставщика для установления Подключения HTTPS между Изяществом, Cisco Unified Intelligence Center (CUIC) и Оперативными Серверами данных.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco Unified Contact Center Enterprise (UCCE)
- Данные Cisco live
- Cisco Unified Intelligence Center (CUIC)
- Изящество Cisco
- CA сертифицируемый

Используемые компоненты

Информация, используемая в документе, основывается на версии решения 11.0 (1) UCCE.

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, удостоверьтесь, что вы понимаете потенциальное воздействие любого шага.

Процедура

Устанавливая сертификат для Связи HTTPS в Изяществе, CUIC и Оперативные Серверы данных требуют следующих шагов

- Генерируйте и загрузите Запрос подписи сертификата (CSR).
- Получите Root, промежуточное звено (если применимо) и сертификат Приложения от Центра сертификации с помощью CSR.
- Сертификаты загрузки к серверам.

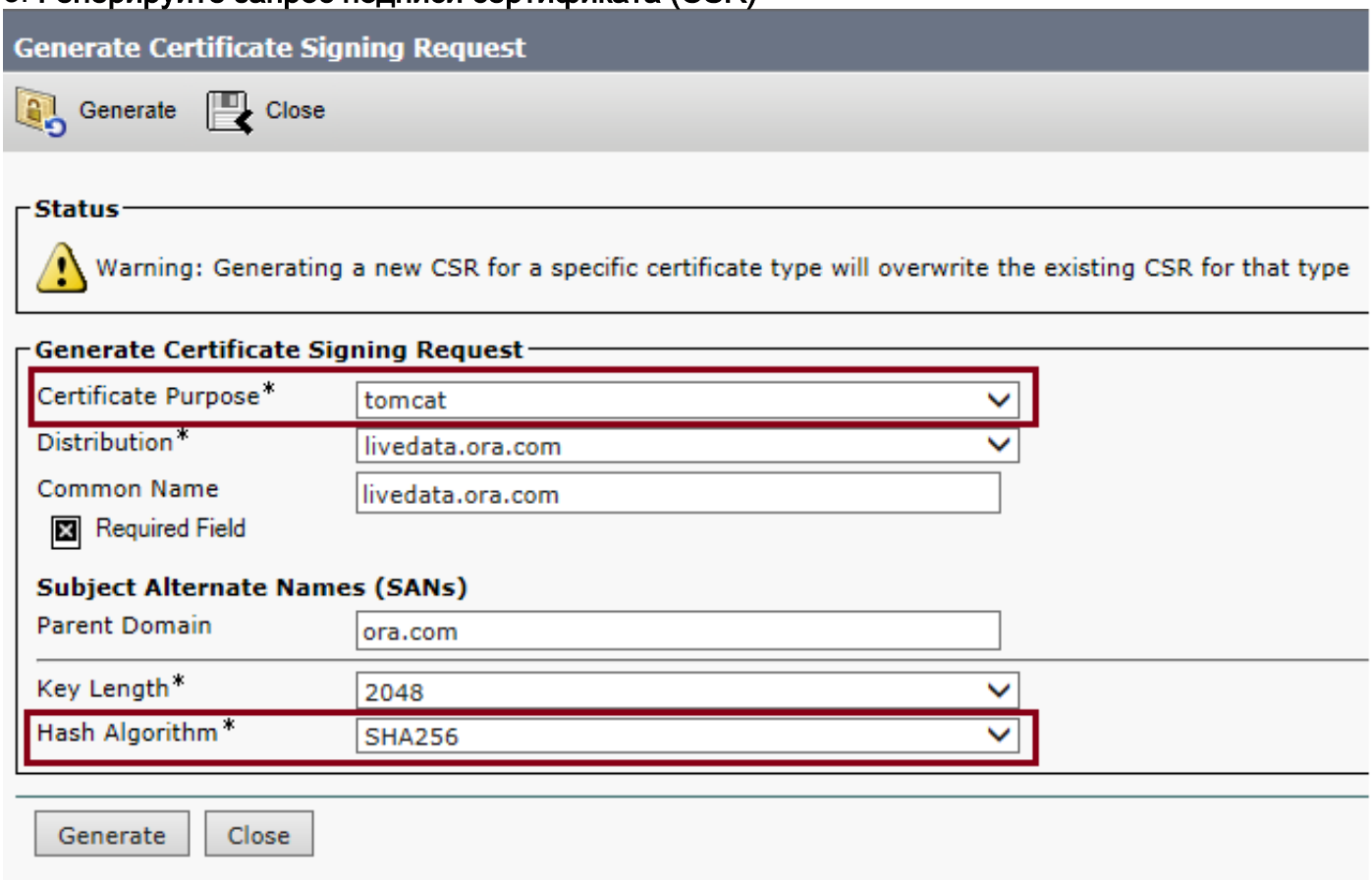
Шаг 1: Генерируйте и загрузите Запрос подписи сертификата (CSR)

---

1. Шаги, описанные ниже для генерации и загрузки CSR, являются тем же для Изящества, CUIC и Оперативные данные разъединяют.

2. Откройте Страницу администратора Операционной системы Унифицированной связи Cisco с помощью ниже установленного URL и регистрируйтесь с учетной записью администратора ОС, созданной во время установки provcess
https://имя хоста основного сервера/cmplatform

3. **Генерируйте запрос подписи сертификата (CSR)**

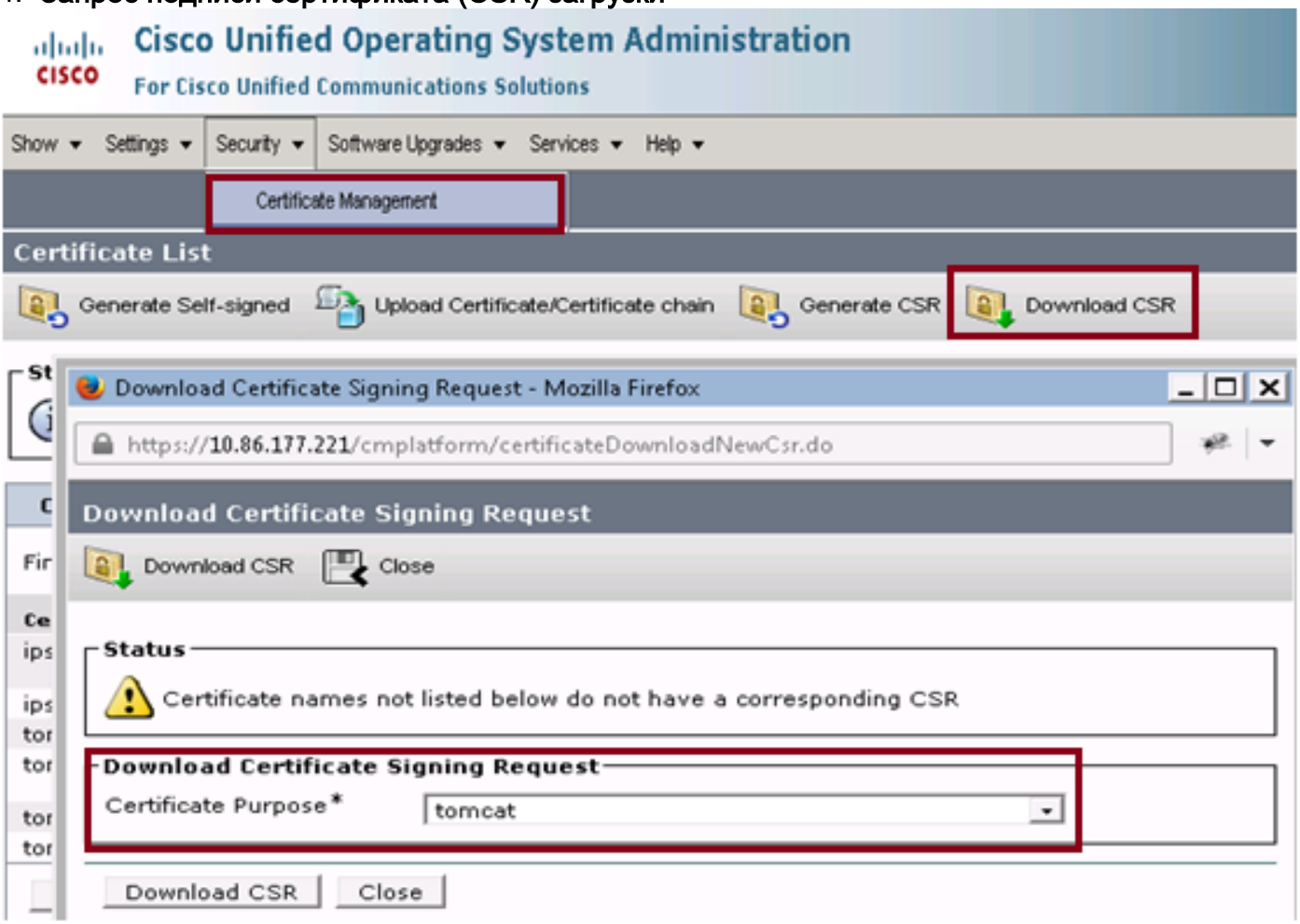


a) Выберите Security> Certificate Management> Generate CSR.

b) От выпадающего списка Названия Цели Сертификата выберите tomcat.

c) Выберите Hash Algorithm как SHA256
d) Нажмите Generate CSR.

4. **Запрос подписи сертификата (CSR) загрузки**



a) Выберите Security> Certificate Management> Download CSR.
b) От выпадающего списка Названия Сертификата выберите tomcat.
c) Нажмите Download CSR.

Примечание:

Выполните вышеупомянутые шаги в использование secondory сервера URL "https://имя хоста secondory server/cmplatform" для получения CSR для Центра сертификации.

Шаг 2: Получите Root, Промежуточное звено (если применимо) и сертификат Приложения от Центра сертификации

---

1. Предоставьте основную и secondory информацию о Запросе подписи сертификата (CSR) серверов Полномочиям Certifcate (CA) третьей стороны как VeriSign, Thawte, GeoTrust и т.д.

2. От Полномочий Certifcate (CA) нужно получить следующую цепочку сертификатов для

основных и secondory серверов.

- **Серверы изящества:** Root, Промежуточное звено и сертификат Приложения
- **Серверы CUIC:** Root и сертификат Приложения
- **Оперативные подачи данных:** Root и сертификат Приложения

Шаг 3: Сертификаты загрузки к серверам.

В этом разделе описываются о том, как загрузить цепочку сертификатов правильно на Изяществе, CUIC и Оперативных серверах данных.

Серверы изящества:

==========

1. Загрузите основной сертификат корневого каталога сервера изящества

a) На основном сервере Страница администратора Операционной системы Унифицированной связи Cisco выбрать

Безопасность> Управление сертификатами> Сертификат Загрузки.

b) От выпадающего списка Названия Сертификата выберите доверие tomcat.
c) В Поле файла Загрузки щелчок просматривает и переходит к файлу корневого сертификата.
d) Нажмите Upload File.

2. Загрузите основной fineese промежуточный сертификат сервера.

a) От выпадающего списка Названия Сертификата выберите доверие tomcat.
b) В поданном Корневом сертификате введите имя корневого сертификата, который вы загрузили в предыдущем шаге. Не включайте расширение (например, ТЕСТОВЫЙ Узел CA 2048).
c) В Поле файла Загрузки нажмите Browse и перейдите к промежуточному файлу сертификата.
d) Нажмите Upload File.

Примечание:
Поскольку база доверенных сертификатов Tomcat реплицирована между основными и secondory серверами, не необходимо загрузить основной корневой каталог сервера Изящества или Промежуточный сертификат к вторичному серверу Изящества.

3. Загрузите основной сертификат серверного приложения изящества.

a) От выпадающего списка Названия Сертификата выберите tomcat.

b) В поле Root Certificate введите имя промежуточного сертификата, который вы загрузили в предыдущем шаге. Включайте расширение .pem (например, TEST-SSL-CA.pem).

c) В Поле файла Загрузки нажмите Browse и перейдите к файлу сертификата приложения.
d) Нажмите Upload File.

4. Загрузите корневой каталог сервера Изящества Secondory и Промежуточный сертификат.

a) Выполните те же действия, как упомянуто выше в (1) и (2) на secondory сервере для его сертификатов

Примечание:
Поскольку база доверенных сертификатов Tomcat реплицирована между основными и secondory серверами, не необходимо загрузить корневой каталог сервера изящества secondory или Промежуточный сертификат к основному серверу изящества.

5. Загрузите secondory fineese сертификат серверного приложения.

a)

6. Серверы перезапуска

Обратитесь к CLI на основном и серверах Изящества secondory и введите команду "перезапуск системы utils" для перезапуска серверов.

Серверы CUIC:

==========

1. Загрузите cuic root основного сервера (общий) сертификат

a) На основном сервере Страница администратора Операционной системы Унифицированной связи Cisco выбрать

Безопасность> Управление сертификатами> Сертификат Загрузки.

b) От выпадающего списка Названия Сертификата выберите доверие tomcat.
c) В Поле файла Загрузки щелчок просматривает и переходит к файлу корневого сертификата.
d) Нажмите Upload File.

Примечание:
Поскольку база доверенных сертификатов Tomcat реплицирована между основными и secondory серверами, не необходимо загрузить основной сертификат корневого каталога сервера CUIC к вторичным серверам CUIC.

2. Загрузите cuic приложение основного сервера (основной) сертификат
a) От выпадающего списка Названия Сертификата выберите tomcat.
b) В поле Root Certificate введите имя корневого сертификата, который вы загрузили в предыдущем шаге. Включайте расширение .pem (например, TEST-SSL-CA.pem).
c) В Поле файла Загрузки нажмите Browse и просмотрите к приложению (основной) файл сертификата.
d) Нажмите Upload File

3. Загрузите cuic secondory корневой каталог сервера (общественность) сертификат

a) На secondory cuic сервер выполняют те же действия, как упомянуто в шаге (1) для его

корневого сертификата.

Примечание:
Поскольку база доверенных сертификатов Tomcat реплицирована между основными и secondory серверами, не необходимо загрузить secondory CUIc сертификат корневого каталога сервера к основному серверу CUIC.

4. Загрузите cuic secondory серверное приложение (основной) сертификат.
a) Придерживайтесь того же процесса, как сообщили в шаге (2) в secondory сервер для его собственного сертификата.

6. Серверы перезапуска

Обратитесь к CLI на основном и secondory CUIC серверы и введите команду "перезапуск системы utils" для перезапуска серверов.

Примечание:

Избегать исключения сертификата, предупреждающего вас, должно обратиться к серверам с помощью названия Полного доменного имени (FQDN).

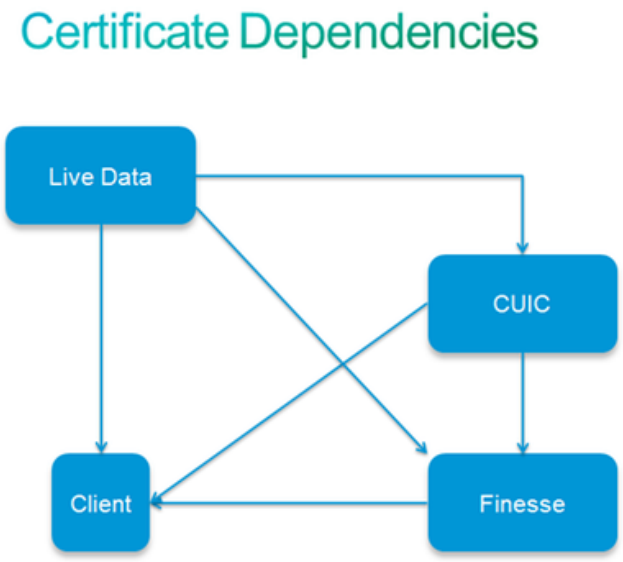
Оперативные серверы данных:

==========

1. Для загрузки оперативного root данных и certficate приложения выполняют те же действия, как выделено выше для серверов CUIC.

2. Поскольку оперативные серверы данных взаимодействуют с CUIC и серверами Изящества, нужно загрузить корневые сертификаты этих серверов также в следующем порядке для поддержания зависимостей от сертификата.

- Изящество **загрузки** root\intermediate и корневые сертификаты CUIC на оперативном сервере данных
- Корневой сертификат Оперативных серверов данных загрузки на основном сервере изящества
- Загрузите корневой сертификат серверов CUIC на основном сервере изящества
- Корневые сертификаты Оперативных данных загрузки на основном сервере CUIC
- Изящество загрузки root\intermediate сертификат на основном сервере CUIC



a) Изящество загрузки root\intermediate и корневые сертификаты CUIC на оперативном сервере данных

---

1. Загрузите основной корневой сертификат изящества

i) На основном Оперативном сервере данных в Странице администратора Операционной системы Унифицированной связи Cisco выбрать

Безопасность> Управление сертификатами> Сертификат Загрузки

ii) От выпадающего списка Названия Сертификата выберите доверие tomcat.
III) В Поле файла Загрузки нажмите Browse и перейдите к основному файлу корневого сертификата изящества.
iV), Нажимают Upload File.

2. Загрузите основной промежуточный сертификат изящества

i) От выпадающего списка Названия Сертификата выберите доверие tomcat.
ii) В поданном Корневом сертификате введите имя корневого сертификата, который вы загрузили в предыдущем шаге. Не включайте расширение (например, ТЕСТОВЫЙ Узел CA 2048).
iii) В Поле файла Загрузки нажмите Browse и перейдите к промежуточному файлу сертификата.
iv) Нажмите Upload File.

3. Загрузите Основной корневой сертификат CUIC
i) На основном Оперативном сервере данных в Странице администратора Операционной системы Унифицированной связи Cisco выбрать

Безопасность> Управление сертификатами> Сертификат Загрузки
ii) От выпадающего списка Названия Сертификата выберите доверие tomcat.
iii) В Поле файла Загрузки нажмите Browse и перейдите к основному файлу корневого сертификата CUIC.
iv) Нажмите Upload File.

4. Выполните те же шаги (1 и 2) для Изящества secondory root\intermediate и корневые

сертификаты CUIC на основном оперативном сервере данных.

Примечание:

Поскольку база доверенных сертификатов Tomcat реплицирована между основными и secondory серверами, не необходимо загрузить Изящество root/internediate и корневые сертификаты CUIC к secondory оперативный сервер данных.

5. Обратитесь к CLI на основном и secondory оперативные серверы данных и введите команду "перезапуск системы utils" для перезапуска серверов.

b)

---

1. На основном изяществе сервер открывают Страницу администратора Операционной системы Унифицированной связи Cisco с помощью ниже установленного URL и регистрируются с учетной записью администратора ОС, созданной во время установки provcess

https://имя хоста основного Изящества server/cmplatform

2. Загрузите Основной Оперативный корневой сертификат данных.
a) Выберите Security> Certificate Management> Upload Certificate.
b) От выпадающего списка Названия Сертификата выберите доверие tomcat.
c) В Поле файла Загрузки нажмите Browse и перейдите к файлу корневого сертификата.
d) Нажмите Upload File.

3. Загрузите Secondory Оперативный корневой сертификат данных.

a) Выберите Security> Certificate Management> Upload Certificate.
b) От выпадающего списка Названия Сертификата выберите доверие tomcat.
c) В Поле файла Загрузки нажмите Browse и перейдите к файлу корневого сертификата.
d) Нажмите Upload File.

Примечание:
Поскольку база доверенных сертификатов Tomcat реплицирована между основными и secondory серверами, не необходимо загрузить оперативный корневой сертификат данных к вторичному серверу изящества.

c)

---

1. На

https://имя хоста основного Изящества server/cmplatform

2. Загрузите Основной корневой сертификат CUIC.
a) Выберите Security> Certificate Management> Upload Certificate.

b) От выпадающего списка Названия Сертификата выберите доверие tomcat.
c) В Поле файла Загрузки нажмите Browse и перейдите к файлу корневого сертификата.
d) Нажмите Upload File.

3. Загрузите Secondory CUIC корневой сертификат.

a) Выберите Security> Certificate Management> Upload Certificate.
b) От выпадающего списка Названия Сертификата выберите доверие tomcat.
c) В Поле файла Загрузки нажмите Browse и перейдите к файлу корневого сертификата.
d) Нажмите Upload File.

Примечание:
Поскольку база доверенных сертификатов Tomcat реплицирована между основными и secondory серверами, не необходимо загрузить оперативный корневой сертификат данных к вторичному серверу изящества.

4. Обратитесь к CLI на основном и серверах изящества secondory и введите команду "перезапуск системы utils" для перезапуска серверов.

d) Корневые сертификаты Оперативных данных загрузки на основном сервере CUIC

---

1. На основном сервере CUIC открывают Страницу администратора Операционной системы Унифицированной связи Cisco с помощью ниже установленного URL и регистрируются с учетной записью администратора ОС, созданной во время установки provcess
https://имя хоста основного CUIC server/cmplatform

2. Загрузите Основной Оперативный корневой сертификат данных.
a) Выберите Security> Certificate Management> Upload Certificate.
b) От выпадающего списка Названия Сертификата выберите доверие tomcat.
c) В Поле файла Загрузки нажмите Browse и перейдите к файлу корневого сертификата.
d) Нажмите Upload File.

3. Загрузите Secondory Оперативный корневой сертификат данных.

a) Выберите Security> Certificate Management> Upload Certificate.
b) От выпадающего списка Названия Сертификата выберите доверие tomcat.
c) В Поле файла Загрузки нажмите Browse и перейдите к файлу корневого сертификата.
d) Нажмите Upload File.

Примечание:
Поскольку база доверенных сертификатов Tomcat реплицирована между основными и secondory серверами, не необходимо загрузить оперативный корневой сертификат данных к вторичным серверам CUIC.

e) Изящество загрузки root\intermediate сертификат на основном сервере CUIC

---

1. На основном сервере CUIC открывают Страницу администратора Операционной системы Унифицированной связи Cisco с помощью ниже установленного URL и регистрируются с учетной записью администратора ОС, созданной во время установки provcess
https://имя хоста основного CUIC server/cmplatform

2. Загрузите Основной корневой сертификат Изящества.
a) Выберите Security> Certificate Management> Upload Certificate.
b) От выпадающего списка Названия Сертификата выберите доверие tomcat.
c) В Поле файла Загрузки нажмите Browse и перейдите к файлу корневого сертификата.
d) Нажмите Upload File.

3. Загрузите основной промежуточный сертификат изящества

i) От выпадающего списка Названия Сертификата выберите доверие tomcat.
ii) В поданном Корневом сертификате введите имя корневого сертификата, который вы загрузили в предыдущем шаге.
iii) В Поле файла Загрузки нажмите Browse и перейдите к промежуточному файлу сертификата.
iv) Нажмите Upload File.

4. Выполните те же шаги (2, и 3) для secondory ловко обходят root\intermediate сертификаты на основном сервере CUIC.

Примечание:

Поскольку база доверенных сертификатов Tomcat реплицирована между основными и secondory серверами, не необходимо загрузить root изящества / промежуточный сертификат к вторичным серверам CUIC.

5. Обратитесь к CLI на основном и secondory CUIC серверы и введите команду "перезапуск системы utils" для перезапуска серверов.