

# Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Процедура](#)

[Шаг 1: Генерируйте и загрузите Запрос подписи сертификата \(CSR\)](#)

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

[Шаг 3: Сертификаты загрузки к серверам](#)

[Серверы изящества:](#)

[Серверы CUIС:](#)

[а\) Загрузите корневой сертификат серверов CUIС на основном сервере изящества](#)

[б\) Изящество загрузки root\intermediate сертификат на основном сервере CUIС](#)

[Связанные обсуждения Сообщества Cisco Support](#)

## Введение

Для использования HTTPS для безопасной связи между Изяществом и серверами Cisco Unified Intelligence Center (CUIС), настройка сертификатов безопасности необходима. По умолчанию эти серверы предоставляют самоподписанные certificates, которые используются, или клиенты могут обеспечить и установить сертификаты 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 серверами Cisco Unified Intelligence Center (CUIС) и Изяществом.

## Предварительные условия

### Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Предприятие Contact Center пакета (PCCE) Cisco
- Cisco Unified Intelligence Center (CUIС)
- Изящество Cisco
- Сертификаты CA

### Используемые компоненты

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

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

Устанавливание сертификатов для Связи HTTPS в Изяществе и

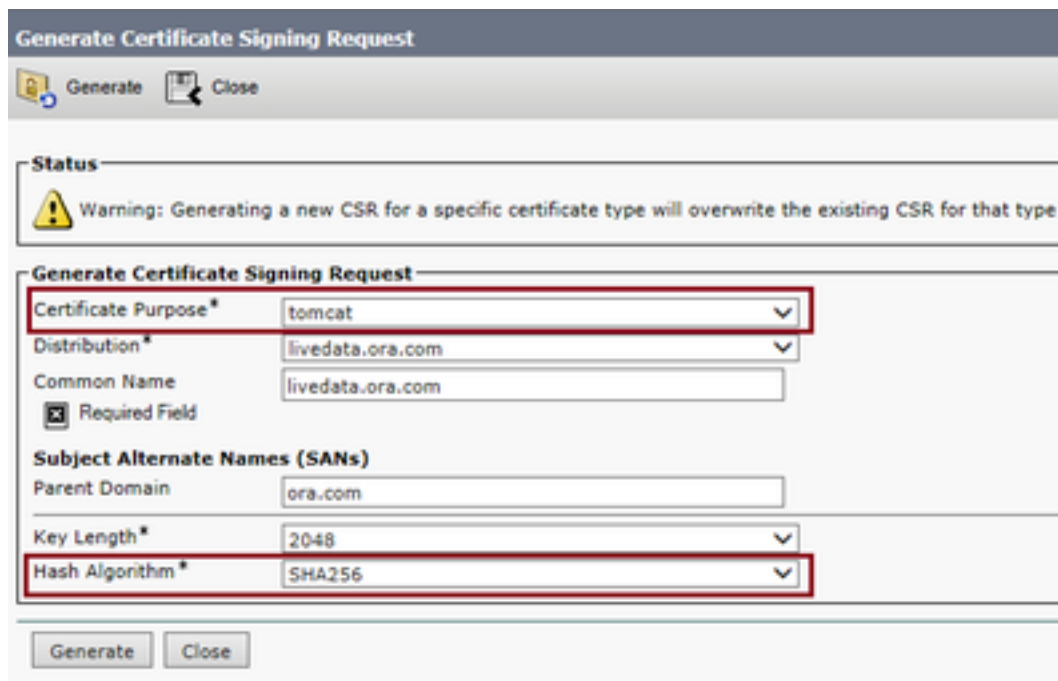
- Генерируйте и загрузите Запрос подписи сертификата (CSR).
- Получите root, промежуточное звено (если применимо) и сертификат приложения от Центра сертификации с помощью CSR.
- Сертификаты загрузки к серверам.

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

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

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

3. Генерируйте запрос подписи сертификата (CSR)



**Generate Certificate Signing Request**

Generate Close

**Status**

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

**Generate Certificate Signing Request**

Certificate Purpose\* tomcat

Distribution\* livedata.ora.com

Common Name livedata.ora.com

Required Field

**Subject Alternate Names (SANs)**

Parent Domain ora.com

Key Length\* 2048

Hash Algorithm\* SHA256

Generate Close

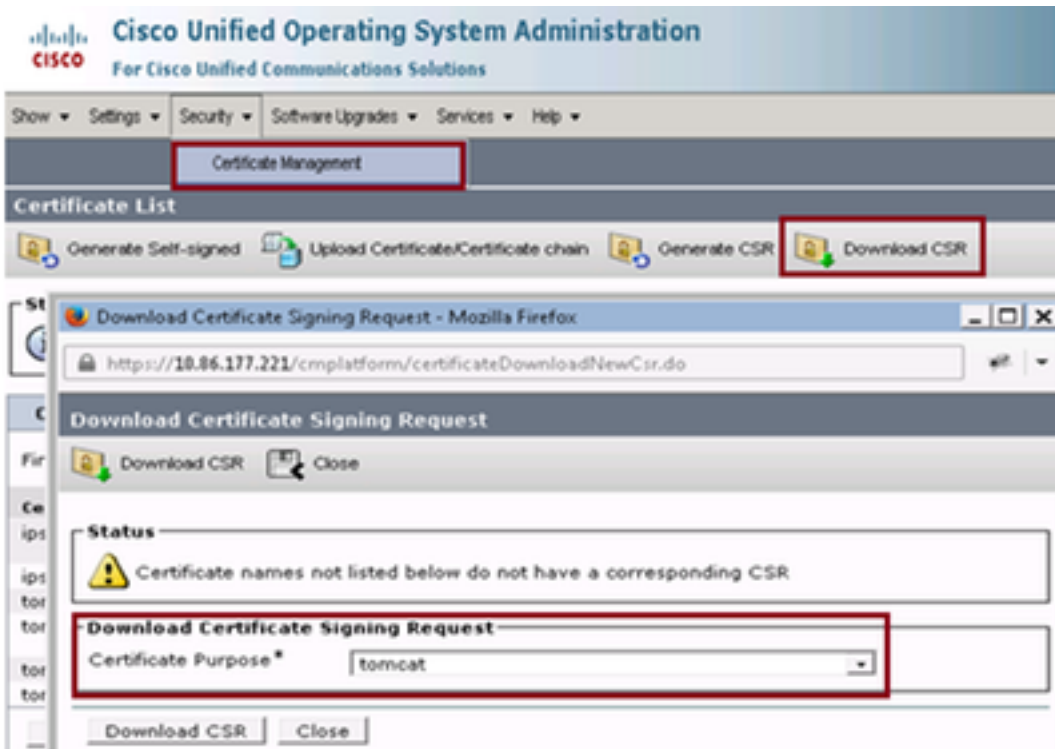
a) Выберите Security> Certificate Management> Generate CSR.

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 secondary сервера URL "https://имя хоста secondary 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 secondary информацию о Запросе подписи сертификата (CSR) серверов Полномочиям Certificate (CA) третьей стороны как VeriSign, Thawte, GeoTrust и т.д.

2. От Полномочий Certificate (CA) нужно получить следующую цепочку сертификатов для основных и secondary серверов.

- Серверы изящества: Root, Промежуточное звено и сертификат Приложения
- Серверы CUIС: Root и сертификат Приложения

### **Шаг 3: Сертификаты загрузки к серверам**

В этом разделе описываются о том, как загрузить цепочку сертификатов правильно на серверах Cisco Unified Intelligence Center (CUIC) и Изяществе.

Серверы изящества:

=====

### 1. Загрузите основной сертификат корневого каталога сервера изящества

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

Безопасность> Управление сертификатами> Сертификат Загрузки.

- б) От выпадающего списка Названия Сертификата выберите доверие tomcat.
- с) В Поле файла Загрузки щелчок просматривает и переходит к файлу корневого сертификата.
- д) Нажмите Upload File.

### 2. Загрузите основной промежуточный сертификат сервера изящества.

- а) От выпадающего списка Названия Сертификата выберите доверие tomcat.
- б) В поданном Корневом сертификате введите имя корневого сертификата, который вы загрузили в предыдущем шаге.

Это - файл .pem, который генерируется, когда был установлен корневой/общий сертификат. Для просмотра этого файла Перешли управлению сертификатами> ClickFind

- с) В Поле файла Загрузки нажмите Browse и перейдите к промежуточному файлу сертификата.
- д) Нажмите Upload File.

#### **Примечание:**

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

### 3. Загрузите основной сертификат серверного приложения изящества.

- а) От выпадающего списка Названия Сертификата выберите tomcat.
- б) В поле Root Certificate введите имя промежуточного сертификата, который вы загрузили в предыдущем шаге. Включайте расширение .pem (например, TEST-SSL-CA.pem).
- с) В Поле файла Загрузки нажмите Browse и перейдите к файлу сертификата приложения.
- д) Нажмите Upload File.

### 4. Загрузите корневой каталог сервера изящества secondary и Промежуточный сертификат.

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

#### **Примечание:**

*Поскольку база доверенных сертификатов Tomcat реплицирована между основными и secondary серверами, не необходимо загрузить корневой каталог сервера изящества*

*secondary или Промежуточный сертификат к основному серверу изящества.*

## 5. Загрузите сертификат серверного приложения изящества secondary.

a)

## 6. Серверы перезапуска

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

Серверы CUIС:

=====

### 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 secondary серверами, не необходимо загрузить основной сертификат корневого каталога сервера CUIС к вторичным серверам CUIС.*

### 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.

Это - файл .pem, который генерируется, когда был установлен корневой/общий сертификат. Для просмотра этого файла Перешли управлению сертификатами> ClickFind Включайте то 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 secondary корневого каталог сервера (общественность) сертификат

a) На secondary 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 secondary серверами, не необходимо загрузить secondary CUIс сертификат корневого*

каталога сервера к основному серверу CUIС.

#### 4. Загрузите cuic secondary серверное приложение (основной) сертификат.

а) Придерживайтесь того же процесса, как сообщили в шаге (2) в secondary сервер для его собственного сертификата.

#### 6. Серверы перезапуска

Обратитесь к CLI на основном и secondary CUIС 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).

#### Зависимости от сертификата:

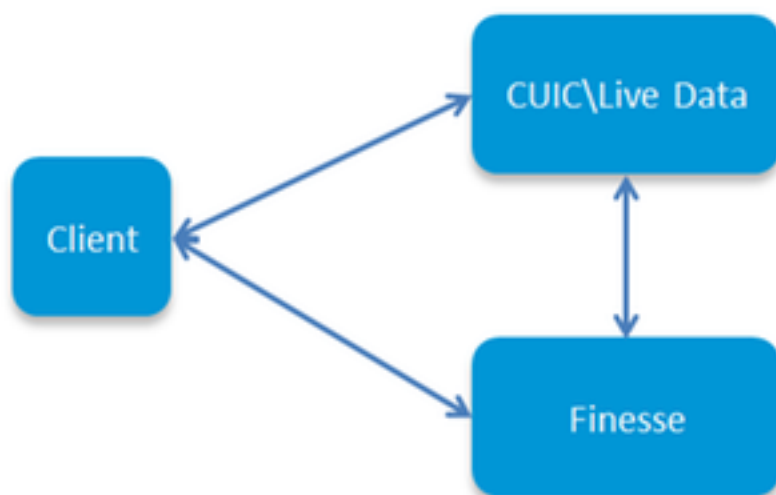
=====

Как

Ловко обойдите агентов, и супервизоры используют гаджеты CUIС для создания отчетов о целях

- Загрузите корневой сертификат серверов CUIС на изяществе основная подача
- Изящество загрузки root\intermediate сертификат на основном сервере CUIС

## Certificate Dependencies



а) Загрузите корневой сертификат серверов CUIС на основном сервере изящества

1. На

<https://имя хоста основного Изящества server/cmplatform>

## **2. Загрузите Основной корневой сертификат CUIС.**

- 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 Secondary CUIС 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 secondary серверами, не необходимо загрузить корневые сертификаты CUIС к вторичному серверу изящества.*

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

b) Изящество загрузки root\intermediate сертификат на основном сервере CUIС

---

1. На основном сервере CUIС 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 CUIС 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 Изящества secondary root\intermediate сертификаты на основном оперативном сервере данных.

### ***Примечание:***

*Поскольку база доверенных сертификатов Tomcat реплицирована между основными и*

*secondary серверами, не необходимо загрузить root Изящества / промежуточный сертификат к вторичным серверам CUIС.*

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