

Настройте Подписанный сертификат CA через CLI в голосовой операционной системе (VOS) Cisco

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Генерируйте подписанный сертификат CA](#)

[Сводка команд](#)

[Проверьте корректную информацию о сертификате](#)

[Генерируйте Запрос знака сертификата \(CSR\)](#)

[Генерируйте серверный сертификат Tomcat](#)

[Сертификат Tomcat импорта к Cisco сервер VOS](#)

[Сертификат CA импорта](#)

[Сертификат Tomcat импорта](#)

[Перезапустите службу](#)

[Проверка](#)

[Устранение неполадок](#)

[Отступите план](#)

[Похожие статьи](#)

Введение

Этот документ описывает действия настройки о том, как загрузить подписанный сертификат Центра сертификации (CA) третьей стороны на основанном сервере совместной работы голосовой операционной системы (VOS) любой Cisco при помощи интерфейса командной строки (CLI).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Основное понимание Инфраструктуры открытых ключей (PKI) и ее реализации на Cisco серверы VOS и Microsoft CA
- Инфраструктура DNS предварительно сконфигурирована

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Сервер VOS: версия 9.1.2 Cisco Unified Communications Manager (CUCM)
- CA: Windows 2012 Server
- Клиентский браузер: версия 47.0.1 Mozilla Firefox

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Во всей Cisco Унифицированный Communications VOS продукты существует по крайней мере два учетных типа: приложение как (ccsadmin, ccmservice, suadmin, cfadmin, cuic) и платформа VOS (cmplatform, drf, cli).

В некоторых определенных сценариях очень удобно управлять приложениями через веб-страницу и выполнить, платформа отнеслась действия через командную строку. Ниже вас может найти процедуру о том, как импортировать подписанный сертификат ^{третьей стороны} исключительно через CLI. В данном примере загружен сертификат Tomcat. Для CallManager или любого другого приложения это выглядит одинаково.

Генерируйте подписанный сертификат CA

Сводка команд

Список команд используется в статье.

```
show cert list own
show cert own tomcat
```

```
set csr gen CallManager
show csr list own
show csr own CallManager
```

```
show cert list trust
set cert import trust CallManager
set cert import own CallManager CallManager-trust/allevich-DC12-CA.pem
```

Проверьте корректную информацию о сертификате

Перечислите все загруженные надежные сертификаты.

```
admin:show cert list own
```

```
tomcat/tomcat.pem: Self-signed certificate generated by system
ipsec/ipsec.pem: Self-signed certificate generated by system
CallManager/CallManager.pem: Certificate Signed by allevich-DC12-CA
CAPF/CAPF.pem: Self-signed certificate generated by system
TVS/TVS.pem: Self-signed certificate generated by system
```


Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

Загрузите корневой сертификат CA. Выберите **Download a CA certificate, цепочку сертификатов или меню CRL**. В следующем меню выбирают надлежащий CA из списка. Способ кодирования должен быть **Ядром 64**. Загрузите сертификат ЦС и сохраните его к операционной системе с названием **ca.cer**.

Нажмите **Request a Certificate** и затем **Усовершенствованный Запрос сертификата. Шаблон сертификата** набора на Web-сервер и вставку содержание CSR от текстового файла **tac_tomcat.csr** как показано.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
PiJkCvzWTeEo6v9qG0nnaI53e15+RPpWxpEgAIPP
ak/tTuWmZbfyk2iqNFy0YgYTeBkG3AqPwWUCNodu
gCzhIHfsV5DzYp3IR5C13hEa5fDgpD2ubQWja2LI
7ZKa6fKnpACehrtVqEn02jOi+sanfQKGQqH8VYMF
StV2Eh0afxPEq/1rQP3/rzq4NMYlJ7glyNFGPUVP
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

Совет: Если операция сделана в лабораторной работе (или Cisco, сервер VOS и CA находятся под тем же административным доменом) сэкономить копию времени и вставить CSR от буфера памяти.

Нажмите **Submit**. Выберите **закодированную** опцию **Base 64** и загрузите сертификат для сервиса Tomcat.

Примечание: Если генерация сертификата выполнена, оптом убеждаются для изменения названия сертификата к meaningful один.

Сертификат Tomcat импорта к Cisco сервер VOS

Сертификат CA импорта

Откройте сертификат CA, который был сохранен названием **ca.cer**. Это должно быть

импортированный сначала.



Скопируйте его содержание к буферу и введите следующую команду в CLI CUCM:

```
admin:set cert import trust tomcat
```

Paste the Certificate and Hit Enter

Приглашение для вставки сертификата CA будет отображено. Вставьте его как показано ниже.

```
admin:set cert import trust tomcat
```

Paste the Certificate and Hit Enter

В случае, если трастовая загрузка сертификата успешна, эти выходные данные будут отображены.

```
admin:set cert import trust tomcat
```

Paste the Certificate and Hit Enter

Проверьте, что сертификат CA успешно импортирован как трастовый Tomcat.

```
admin:show cert list trust
```

```
tomcat-trust/ucml-1.pem: Trust Certificate
tomcat-trust/allevich-win-CA.pem: w2008r2 139
<output omitted for brevity>
```

Сертификат Tomcat импорта

Следующий шаг должен импортировать Tomcat CA подписанный сертификат. Операция выглядит одинаково как с трастовым tomcat свидетельством, просто команда является другой.

```
set cert import own tomcat tomcat-trust/allevich-DC12-CA.pem
```

Перезапустите службу

И наконец сервис Tomcat перезапуска.

```
utils service restart Cisco Tomcat
```

Внимание. : Следует иметь в виду, что это разрушает использование подчиненных сервисов Web-сервера, как Функция Extension Mobility, Пропущенные вызовы, Корпоративный каталог и другие.

Проверка

Проверьте сертификат, который генерировался.

```
admin:show cert own tomcat
```

```
[
  Version: V3
  Serial Number: 2765292404730765620225406600715421425487314965
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: CN=allevich-DC12-CA, DC=allevich, DC=local
  Validity From: Sun Jul 31 12:17:46 CEST 2016
                 To: Tue Jul 31 12:17:46 CEST 2018
  Subject Name: CN=ucm1-1.allevich.local, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL
  Key: RSA (1.2.840.113549.1.1.1)
  Key value: 3082010a028201010095a
```

Гарантируйте, что имя запрашивающей стороны принадлежит СА, который создал тот сертификат.

Вход в систему к веб-странице путем ввода FQDN сервера в браузере и никаком сертификате, предупреждающем, будет отображен.

Устранение неполадок

Цель этой статьи состоит в том, чтобы дать процедуру с синтаксисом команды о том, как загрузить сертификат через CLI, для не выделения логики Infrastructure с открытым ключом (PKI). Это не покрывает SAN сертификат, Подчиненный СА, 4096 длин ключа сертификата и много других сценариев.

В некоторых редких случаях при загрузке сертификата Web-сервера через CLI операция отказывает с сообщением об ошибках, "Неспособным считать сертификат СА". Обходной путь для этого должен установить сертификат с помощью веб-страницы.

Нестандартная конфигурация Центра сертификации может привести к проблеме с установкой сертификатов. Попробуйте генерировать и установить сертификат от другого СА с основной конфигурацией по умолчанию.

Отступите план

В случае, если будет потребность генерировать подписанный сертификат, она может также

быть сделана в CLI.

Введите команду ниже, и сертификат Tomcat будет восстановлен к самоподписанному.

```
admin:set cert regen tomcat
```

```
WARNING: This operation will overwrite any CA signed certificate previously imported for tomcat
```

```
Proceed with regeneration (yes|no)? yes  
Successfully Regenerated Certificate for tomcat.
```

```
You must restart services related to tomcat for the regenerated certificates to become active.
```

Применять новый сервис Tomcat сертификата должно быть перезапущено.

```
admin:utils service restart Cisco Tomcat
```

```
Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted  
Properly, execute the same Command Again
```

```
Service Manager is running  
Cisco Tomcat[STOPPING]  
Cisco Tomcat[STOPPING]  
Commanded Out of Service  
Cisco Tomcat[NOTRUNNING]  
Service Manager is running  
Cisco Tomcat[STARTING]  
Cisco Tomcat[STARTING]  
Cisco Tomcat[STARTED]
```

Похожие статьи

[Сертификат загрузки через веб-страницу](#)

[Процедура, чтобы получить и загрузить Windows Server Self-Signed или Центр сертификации \(CA\)...](#)