Содержание

Введение

Этот документ предоставляет рекомендуемый, пошаговая процедура для регенерации сертификатов, используемых в Выпуске 8.x Cisco Unified Communications Manager (CUCM) и позже. Безопасность Функцией по умолчанию (ITL) и Смешанным Режимом (CTL) также быть покрытой во избежание любых нежелательных простоев. Например, как избежать проблем регистрации телефона или телефонов, которые не принимают изменения конфигурации или микропрограммные обеспечения.

> **Внимание:** Всегда рекомендуется завершить регенерацию сертификата в периоде технического обслуживания.

Обзор

Этот документ обсуждает процесс регенерации сертификата для этих сервисов:

- (диспетчер вызовов Call Manager)
- CAPF (функция прокси центра сертификации)
- IPsec
- Tomcat
- TVS (трастовый сервис проверки)

- ITLRecovery (только для CUCM 10. X и позже)
- телефонное доверие vpn
- phone-sast-trust
- телефонное доверие
- phone-ctl-trust

А также эти телефонные сертификаты:

- LSC (локально значительные сертификаты)
- MIC (изготовитель установленные сертификаты)

Используемые компоненты

Все выходные данные и снимки экрана, показанные в этом документе, основываются на Выпуске 9.1 (2) SU2a CUCM, однако представленная процедура может использоваться с Выпуском 8.x CUCM и позже. Различия, которые являются определенным выпуском, упомянуты в соответствующих разделах.

Сведения в этом документе основывались на устройствах в лабораторной среде, которая запустила с чистой (заданной по умолчанию) конфигурацией. Если ваша сеть является оперативной, удостоверьтесь, что вы понимаете потенциальное воздействие любой команды и принятых мер.

Когда восстановить сертификаты

Большинство сертификатов, используемых в CUCM после новой установки, является выполненными подписанными сертификатами, по умолчанию, в течение пяти лет. Обратите внимание на то, что пятилетний временной диапазон в настоящее время не может модифицироваться, чтобы быть меньшим диапазоном времени на CUCM. Однако Центр сертификации (CA) может выполнить сертификаты для почти любого диапазона времени.

Существуют также некоторые надежные сертификаты (такие как доверие CAPF и доверие CallManager), которые предварительно загружены и имеют более длинный период достоверности. Например, "Cisco, Производящая CA" сертификат, предоставлена на базах доверенных сертификатов CUCM определенным функциям и не истечет до 2029 года.

Сертификаты должны быть восстановлены, прежде чем они истекут. Когда сертификаты соберутся истечь, вы получите предупреждения в RTMT (Средство просмотра системного журнала), и электронное письмо с уведомлением будет послано, если настроено.

Пример уведомления окончания срока действия сертификата, которое детализирует сертификат "CUCM01.der", истечет на "понедельник 19 мая 14:46" на сервере, который CUCM02 на базе доверенных сертификатов "доверие tomcat" показывают здесь:

```
At Fri Sep 05 02:00:56 CEST 2014 on node 192.168.1.2, the following
```

```
SyslogSeverityMatchFound events generated:

SeverityMatch : Critical

MatchedEvent : Sep 5 02:00:06 CUCM02 local7 2 : 864: CUCM02.localdomain:
Sep 05 2014 00:00:06.433 UTC : %UC_CERT-2-CertValidfor7days:
%[Message=Certificate expiration Notification. Certificate name:CUCM01.der
Unit:tomcat-trust Type:own-cert Expiration:Mon May 19 14:46:]
[AppID=Cisco Certificate Monitor][ClusterID=][NodeID=CUCM02]:
Alarm to indicate that Certificate has Expired or Expires in less than seven days

AppID : Cisco Syslog Agent

ClusterID :

NodeID : CUCM02

TimeStamp : Fri Sep 05 02:00:16 CEST 2014
```

Если трудовые книжки (хранилища сертификата, которые не маркированы "-доверие") уже истекаются, все еще возможно восстановить их. Следует иметь в виду, что просроченные сертификаты могли бы оказать влияние на вашу функциональность CUCM, зависящую от конфигурации кластера. Факторы обсуждены в следующих разделах.

Сервисное влияние хранилищем сертификата

Важно для хорошей функциональности системы иметь все сертификаты, обновленные через кластер CUCM. Если ваши сертификаты истекаются или недопустимы, они могли бы значительно влиять на стандартную функциональность системы. Список потенциальных проблем, которые вы могли бы иметь, когда любой из определенных сертификатов недопустим или с истекшим сроком, показывают здесь. Влияние могло бы отличаться зависящее от вашей системной настройки.

(диспетчер вызовов Call Manager). pem

- Шифровал/аутентифицировал телефоны, не регистрируются.
- TFTP не доверял (телефоны не принимают подписанные файлы конфигурации и/или файлы ITL).
- На телефонные службы можно было бы влиять.
- Безопасные транки Протокола SIP или медиаресурсы (Мосты конференц-связи, Media Termination Point (MTP), Xcoders, и так далее) не будут регистрироваться или работать.
- Сбои запроса AXL.

Tomcat.pem

- Телефоны не в состоянии обратиться к сервисам HTTPs, размещенным на узле CUCM, таким как Корпоративный каталог.
- Веб-проблемы GUI CUCM, такой как неспособный к страницам службы доступа от других узлов в кластере.
- Функция Extension Mobility или проблемы Кластера Пересечения Функции Extension Mobility.

CAPF.pem

- Телефоны не аутентифицируются для Телефонной VPN, 802.1x или Телефонного Прокси.
- Не может выполнить сертификаты LSC для телефонов.

- Зашифрованные файлы конфигурации не работают.

IPSec.pem

- Система аварийного восстановления (DRS) / Платформа Восстановления после отказа (DRF) не могла бы функционировать должным образом.
- Туннели IPSec к шлюзу (GW) к другим кластерам CUCM не работают.

TVS (трастовый сервис проверки)

- Телефон не может аутентифицировать сервис HTTPS. Телефон не может аутентифицировать файлы конфигурации (это может влиять почти на все на CUCM).

телефонное доверие vpn

- Телефонная VPN не будет работать, потому что не может аутентифицироваться URL HTTPS VPN.

  Примечание: Если это не существует, не волнуются. Это только для определенных конфигураций.

phone-sast-trust

- Предыдущий CTL/eToken не будет в состоянии обновить или модифицировать CTL.

  Примечание: Если это не существует, не волнуются. Это только для определенных конфигураций.

телефонное доверие и phone-ctl-trust

- Визуальная голосовая почта с Unity или Unity Connection не будет работать.

  Примечание: Если это не существует, не волнуются. Это только для определенных конфигураций.

LSC и MIC

- Телефоны не регистрируются, телефон не аутентифицируется для Вызова по телефону VPN, Телефонному Прокси или 802.1x.

  Примечание: MIC находятся на большинстве моделей телефонов по умолчанию. LSC подписаны CAPF и длятся пять лет по умолчанию. Клиентским программным обеспечениям, таким как CIPC (IP-коммуникатор Cisco) и Jabber не установили MIC.

Создайте резервную копию DRS

Рекомендуется создать резервную копию DRS перед выполнением любых основных изменений как это. Резервные копии DRF CUCM выполнят резервное копирование все сертификаты в кластере. Вся резервная копия/процедуры восстановления DRS может быть найдена в Cisco "

Внимание: CSCtn50405, Резервная копия DRF CUCM не резервирует сертификаты

Определите, находится ли Кластер в Смешанном Режиме

Чтобы определить, выполняете ли вы кластер CTL/Secure/Mixed-Mode, выбираете **Cisco Unified CM Administration> System> Enterprise Parameters > Cluster Security Mode (0 == Незащищенный; 1 == Смешанный Режим)**.

Если Кластер находится в Смешанном Режиме

При выполнении кластера CUCM в Смешанном Режиме это означает, что файл CTL должен быть обновлен после всех изменений сертификата. Процедура о том, как сделать это, в рамках Документации Руководства по обеспечению безопасности Cisco. Однако убедитесь, что у вас есть по крайней мере один eToken от исходного инициирования функции Смешанного Режима, и пароль eToken известен.

> **Примечание:** Обновление CTL не происходит автоматически (как это делает в случае файла ITL). Это должно быть завершено вручную администратором или с Клиентом CTL или с командой CLI.

В CUCM 10. X и позже можно поместить кластер в Смешанный Режим двумя способами:

- Команда CLI - если этот метод используется тогда ваш файл CTL, подписана с сертификатом CallManager.pem Сервера публикаций. `admin:`**`show ctl`**

```
The checksum value of the CTL file:
0c05655de63fe2a042cf252d96c6d609(MD5)
8c92d1a569f7263cf4485812366e66e3b503a2f5(SHA1)

Length of CTL file: 4947
The CTL File was last modified on Fri Mar 06 19:45:13 CET 2015

[...]

CTL Record #:1
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1156
2 DNSNAME 16 cucm-1051-a-pub
3 SUBJECTNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
6 SERIALNUMBER 16 70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 694 E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D 21
A5 A3 8C 9C (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

- Клиент CTL - если этот метод используется тогда ваш файл CTL, подписан с одним из аппаратных eToken. `admin:`**`show ctl`**

```
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)
```

```
Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Примечание: Можно переместить между методом, используемым с CUCM Смешанный Режим с CTL Tokenless.

Зависящий от метода использовал защищать ваш кластер, соответствующая процедура обновления CTL должна использоваться. Или повторно выполните клиента CTL или введите **utils ctl** команда **CTLfile обновления** от CLI.

Проверьте безопасность по умолчанию на кластере

Предотвращение проблем ITL важно, потому что проблемы ITL могут заставить много функций отказывать, или телефон откажется соблюдать любые изменения к конфигурациям. Проблем ITL можно избежать этими двумя способами.

Используйте, "Готовят Кластер к Откату к пред 8.0" Функций

Эта функция "очищает" ваш ITL на всех серверах, таким образом, телефоны будут доверять любому серверу TFTP. Когда этот параметр будет установлен в True, телефонные службы (например, функция Extension Mobility) НЕ будут работать. Однако пользователи будут в состоянии продолжить делать и получать базовые телефонные вызовы.

Примечание: Изменение к этому параметру заставляет ALL PHONES ПЕРЕЗАГРУЖАТЬ.

Как только эта функция установлена, все серверы TFTP должны быть перезапущены (для предоставления нового ITL), и все телефоны должны быть перезагружены, чтобы вынудить их запросить новый "пустой" ITL. Как только изменения сертификата завершены, и все необходимые сервисы были перезапущены, эта функция может быть задержана ко "Лжи", Сервис TFTP, перезапущенный, и телефонный сброс (таким образом, телефон может получить допустимый файл ITL). Затем все функции продолжат работать, как они сделали ранее.

Восстановите сертификаты в определенном заказе

Эта процедура предоставляет серверу TFTP допустимый/обновленный файл ITL от доверяемого сервера TFTP, который доступен.

1. Остановите Сервис TFTP на Основном сервере TFTP.
2. Внесите изменения на сертификатах Основного сервера TFTP (по мере необходимости).
3. Перезагрузите телефоны (для получения нового файла ITL от Вторичного сервера TFTP) - зависящий, на который восстановлены сертификаты, это могло бы произойти автоматически.
4. Как только телефоны возвратились, запустите Сервис TFTP Основного сервера TFTP.
5. Внесите изменения сертификата на Вторичном сервере TFTP.
6. Перезагрузите телефоны (для получения нового файла ITL от Основного сервера TFTP).

> **Внимание:** Не редактируйте сертификаты на обоих серверах TFTP в то же время. Это не дает телефонам сервера TFTP для доверия и требует, чтобы локальный администратор вручную удалил ITL из всех телефонов.

Удалите и восстановите сертификаты в CUCM

Только трудовые книжки (хранилища сертификата, которые не маркированы "-доверие") могут быть восстановлены. Сертификаты в базах доверенных сертификатов (хранилища сертификата, которые маркированы "-доверие") должны быть удалены, поскольку они не могут быть восстановлены.

> **Внимание:** Знайте об идентификаторе ошибки Cisco CSCut58407 - Устройства не должны перезапускать, когда удален CAPF / CallManager / доверие TVS.

После всех модификаций сертификата соответствующий сервис должен быть перезапущен для принятия изменения. Это покрыто в После Регенерации/Удаления раздела Сертификатов.

> **Внимание:** Знайте об идентификаторе ошибки Cisco CSCto86463 - Удаленные сертификаты вновь появляются, неспособные удалить сертификаты из CUCM. Это - проблема, где удаленные сертификаты продолжают вновь появляться после удаления. Придерживайтесь обходного пути в дефекте.

Восстановите Сертификаты через CLI

> **Внимание:** Регенерации сертификатов инициируют автоматическое обновление файлов ITL в кластере, который инициирует общекластерный сброс программного телефона, чтобы позволить телефонам инициировать обновление своего локального ITL. Это фокусируется на CAPF и регенерациях сертификата CallManager, но может произойти с другими хранилищами сертификата в CUCM, такими как Tomcat.

Восстановите CAPF

После регенерации сертификат CAPF автоматически загружает себя к доверию CAPF и доверию CallManager. Кроме того, CAPF всегда имеет уникальный заголовок Имени субъекта, таким образом ранее используемые сертификаты CAPF будут сохраняться и использоваться для аутентификации.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

> **Примечание:** Если сертификат CAPF истечется, то телефоны, которые используют LSC, не будут в состоянии зарегистрироваться к CUCM, потому что CUCM отклоняет их сертификат. Однако можно все еще генерировать новый LSC для телефона с новым сертификатом CAPF. При перезагрузке телефона, он загружает конфигурацию и затем связывается с CAPF для обновления LSC. После того, как LSC обновлен, телефонные регистры, как он должен. Это работает, пока новый сертификат CAPF находится в файле ITL и загруженном телефоне и доверял сертификату, который подписал его (callmanager.pem).

Восстановите CallManager

После регенерации CallManager автоматически загружает себя к доверию CallManager.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
```

```
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Восстановите IPsec

После регенерации сертификат IPsec автоматически загружает себя к доверию ipsec.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Восстановите Tomcat

После регенерации сертификат Tomcat автоматически загружает себя к доверию tomcat.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
```

```
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Восстановите TVS

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Что ожидать

При регенерации сертификатов через CLI вас запрашивают проверить это изменение. Введите да и нажмите Enter.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Удалите Сертификаты через CLI

Удалите трастовые CAPF сертификаты

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Удалите трастовые CallManager сертификаты

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Удалите трастовые ipsec Сертификаты

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015
```

```
[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Удалите трастовые Tomcat сертификаты

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Удалите трастовые TVS сертификаты

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
```

```
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Восстановите Сертификаты через веб-GUI

Восстановите CAPF

После регенерации сертификат CAPF автоматически загружает себя к доверию CAPF и доверию CallManager. Кроме того, сертификат CAPF всегда имеет уникальный заголовок Имени субъекта, таким образом ранее используемые сертификаты CAPF сохраняются и используются для аутентификации.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Восстановите CallManager

После регенерации сертификат CAPF автоматически загружает себя к доверию CallManager.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
```

```
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Восстановите IPsec

После регенерации сертификат IPsec автоматически загружает себя к доверию ipsec.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Восстановите Tomcat

После регенерации сертификат Tomcat автоматически загружает себя к доверию tomcat.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
```

```
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Восстановите TVS

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Удалите Сертификаты через веб-GUI

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

После Регенерации/Удаления Сертификатов

После того, как вы удаляете или восстанавливаете сертификат от хранилища сертификата, соответствующий сервис должен быть перезапущен для принятия изменения.

Хранилище	Сервис для перезапуска	Как (C == CLI; W == веб-GUI)
Tomcat	Tomcat	C : сервис utils перезапускает Tomcat Cisco G: Cisco Унифицированное Удобство обслуживания> To
(диспетчер вызовов Call Manager)	(диспетчер вызовов Call Manager); TFTP	Control Center - Feature Services> (Выбирают Сервер)> выбирает "Cisco CallManager"> Restart И G: Cisco Унифицированное Удобство обслуживания> To Control Center - Feature Services> (Выбирают Сервер)> выбирает "Cisco Tftp"> Restart
CAPF	CAPF (Только на Издателе)	G: Cisco Унифицированное Удобство обслуживания> To Control Center - Feature Services> (Выбирают Сервер)> выбирает "Cisco Certificate Authority Proxy Function"> Res
TVS	Трастовый Сервис Проверки (на соответствующем сервере)	G: Cisco Унифицированное Удобство обслуживания> To Control Center - Сетевые сервисы> (Выбирают Сервер)> выбирает "Cisco Trust Verification Service"> Restart
ipsec	Локальный DRF Cisco (на всех узлах); Ведущее устройство DRF Cisco (на Издателе)	C : сервис utils перезапускает Локальный DRF Cisco И C : сервис utils перезапускает Ведущее устройство DRF

Установите/Обновите LSC по Телефону

Если сертификат CAPF был восстановлен, то сертификаты LSC для всех телефонов в кластерной потребности, которая будет обновлена с LSC, подписанным новым сертификатом CAPF.

1. Выберите **CUCM Serviceability> Service Activation**. Активируйте Поставщика CTL Cisco и Функцию прокси Центра сертификации Cisco на сервере публикаций.
2. От CCMAdmin CUCM выберите **Device> Phone.** Выберите IP-телефон, на котором вы хотите настроить LSC.
3. На странице Конфигурации устройства при Операции Сертификата выберите **Install / Обновление> Пустой строкой**.
4. Сохраните конфигурацию телефона в CCMAdmin и выберите **Apply Config**.

Если телефон испытывает затруднения из-за установки LSC, завершите эти действия с телефоном:

Когда телефон перезагружает, перейдите к обычному телефону и выберите **Settings> (6) Security Configuration> (4) LSC> **#** (эта операция разблокировала GUI и позволяет нам продолжать к следующему шагу)**,> Обновление** (обновление не будет видимо, пока вы не выполните, предыдущий шаг)> **Подвергаются**.

Не назначайте сертификаты на телефон, пока это не беспроводной телефон (7921/25). Беспроводные сети звонят Центрам сертификации (CA) третьей стороны использования для аутентификации себя.

Заключение

Если вы сталкиваетесь с проблемой или нуждаетесь в помощи с этой процедурой, свяжитесь с Центром технической поддержки Cisco (TAC) для помощи. В этом случае поддержите свою Резервную копию DRF доступной, поскольку она будет использоваться как

последнее прибежище для восстановления сервиса, если TAC неспособен сделать так через другие методы.