CUCM смешанный режим с CTL Tokenless

Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Общие сведения](#)
[От незащищенного режима до смешанного режима (CTL Tokenless)](#)
[От Аппаратных eToken до Решения Tokenless](#)
[От Токенлесса Солушна к Аппаратным eToken](#)
[Регенерация сертификата для решения для CTL Tokenless](#)

Введение

Этот документ описывает различие между безопасностью Cisco Unified Communications Manager (CUCM) с и без использования аппаратных eToken USB. Этот документ также описывает сценарии базового внедрения, которые включают Список надежных сертификатов (CTL) Tokenless и процесс, который используется, чтобы гарантировать что системные функции должным образом после изменений.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с Версией 10.0 (1) CUCM или позже. Кроме того, гарантируйте что:

- У вас есть Административный доступ к Интерфейсу командной строки (CLI) узла Издателя CUCM.
- У вас есть доступ к аппаратным eToken USB и что Плагин Клиента CTL установлен на вашем ПК для сценариев, которые требуют, чтобы вы мигрировали назад на использование аппаратных eToken.
- Существует полное подключение между всеми узлами CUCM в кластере. Это очень важно, потому что файл CTL скопирован ко всем узлам в кластере через Протокол передачи файлов SSH (SFTP).

- База данных (DB), Репликация в кластере работает должным образом и что серверы реплицируют данные в режиме реального времени.

- Устройства в ваших развертываниях поддерживают Безопасность по умолчанию (TVS). Можно использовать *Унифицированный Список Телефонной функции CM* от Cisco Унифицированная веб-страница Создания отчетов (https://<IP CUCM или FQDN>/cucreports/) для определения устройств та Безопасность поддержки по умолчанию. **Примечание:** Cisco Jabber и многие Cisco TelePresence или IP-телефоны Серии Cisco 7940/7960 в настоящее время не поддерживают Безопасность по умолчанию. Если вы развернете CTL Tokenless с устройствами, которые не поддерживают Безопасность по умолчанию, то любое обновление вашей системы, которая изменяет сертификат CallManager на издателе, будет препятствовать тому, чтобы те устройства регистрировались в системе, пока не будет вручную удален их CTL.

Используемые компоненты

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

- Версия 10.5.1.10000-7 CUCM (кластер двух узлов)

- Cisco IP-телефоны серии 7975 зарегистрировалась через Skinny Client Control Protocol (SCCP) в Версии микропрограммы SCCP75.9-3-1SR4-1S

- Два Cisco Security Маркеры, которые используются для установки кластера в Смешанный режим с использованием Клиентского программного обеспечения CTL

Общие сведения

CTL Tokenless является новой характеристикой в Версиях CUCM 10.0 (1) и позже который позволяет шифрование передачи вызовов и сред для IP-телефонов без потребности использовать аппаратные eToken USB и плагин Клиента CTL, который был требованием в предыдущих версиях CUCM.

Когда кластер размещен в Смешанный режим с использованием команды CLI, файл CTL подписан с CCM+TFTP (сервер) сертификат узла Издателя, и в файле CTL нет никакого подарка сертификатов eToken.

> **Примечание:** При регенерации CallManager (CCM+TFTP) сертификат на издателе это изменяет подписывающее лицо файла. Телефоны и устройства, которые не поддерживают Безопасность по умолчанию, не примут новый файл CTL, пока файлы CTL не будут **вручную удалены из каждого устройства**. См. последнее требование, которое перечислено раздел Требований этого документа для получения дополнительной информации.

От незащищенного режима до смешанного режима (CTL

Tokenless)

В этом разделе описываются процесс, который используется для перемещения безопасности кластера CUCM в Смешанный режим через CLI.

До этого сценария CUCM был в Незащищенном режиме, что означает, что не было никакого подарка файла CTL ни на одном из узлов и что зарегистрированные IP-телефоны имели только установленный файл Идентификационного списка доверия (ITL), как показано в этих выходных данных:

```
admin:show ctl
Length of CTL file: 0
CTL File not found. Please run CTLClient plugin or run the CLI - utils ctl.. to
generate the CTL file.
Error parsing the CTL File.
admin:
```

Для перемещения безопасности кластера CUCM в Смешанный режим с использованием новой функции CTL Tokenless выполните эти шаги:

1. Получите Административный доступ к CLI узла Издателя CUCM.

2. Введите **utils ctl кластерный набором смешанный командный режим** в CLI:
   ```
   admin:utils ctl set-cluster mixed-mode
   This operation will set the cluster to Mixed mode. Do you want to continue? (y/n):y

   Moving Cluster to Mixed Mode
   Cluster set to Mixed Mode
   Please Restart the TFTP and Cisco CallManager services on all nodes in the cluster
   that run these services
   admin:
   ```
3. Перейдите к **Странице администратора CUCM> Система> Параметры предприятия** и проверьте, был ли кластер установлен в Смешанный режим (значение **1** указывает на Смешанный режим):

4. Перезапустите TFTP и Сервисы Cisco CallManager на всех узлах в кластере, которые выполняют эти сервисы.

5. Перезапустите все IP-телефоны так, чтобы они могли получить файл CTL из Сервиса TFTP CUCM.

6. Для проверки содержания файла CTL введите **показ ctl** команда в CLI. В файле CTL вы видите, что CCM+TFTP (сервер), сертификат для узла Издателя CUCM используется для подписания файла CTL (этот файл является тем же на всех серверах в кластере). Ниже приведен пример выходных данных:
   ```
   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.
CTL Record #:2
----
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 CCM+TFTP
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

[...]

The CTL file was verified successfully.
```

7. На стороне IP-телефона можно проверить, что после того, как сервис перезапущен, это загружает файл CTL, который теперь присутствует на сервере TFTP (соответствия контрольной суммы MD5 когда по сравнению с выходными данными от CUCM):

   Примечание: При проверке контрольной суммы по телефону вы видите или **MD5** или **SHA1**, зависящий от типа телефона.

От Аппаратных eToken до Решения Tokenless

В этом разделе описывается переместить безопасность кластера CUCM от аппаратных eToken до использования нового решения Tokenless.

В некоторых ситуациях Смешанный режим уже настроен на CUCM с использованием Клиента CTL и файлах CTL использования IP-телефонов, которые содержат сертификаты от аппаратных eToken USB. С этим сценарием файл CTL подписан сертификатом от одного из eToken USB и установлен на IP-телефонах. Здесь в примере:

```
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.

The CTL file was verified successfully.
```

Выполните эти шаги для перемещения безопасности кластера CUCM в использование CTL Tokenless:

1. Получите Административный доступ к CLI узла Издателя CUCM.

2. Войдите **utils ctl обновляют** команду CLI **CTLFile**:
   ```
   admin:utils ctl update CTLFile
   This operation will update the CTLFile. Do you want to continue? (y/n):y

   Updating CTL file
   CTL file Updated
   Please Restart the TFTP and Cisco CallManager services on all nodes in
   the cluster that run these services
   ```
3. Перезапустите TFTP и Сервисы CallManager на всех узлах в кластере, которые выполняют эти сервисы.

4. Перезапустите все IP-телефоны так, чтобы они могли получить файл CTL из Сервиса TFTP CUCM.

5. Введите **показ ctl** команда в CLI для проверки содержания файла CTL. В файле CTL вы видите, что CCM+TFTP (сервер), сертификат узла Издателя CUCM используется для подписания файла CTL вместо сертификата от аппаратных eToken USB. Еще одно важное различие в этом случае - то, что сертификаты от всех аппаратных eToken USB удалены из файла CTL. Ниже приведен пример выходных данных:
   ```
   admin:show ctl
   The checksum value of the CTL file:
   1d97d9089dd558a062cccfcb1dc4c57f(MD5)
   3b452f9ec9d6543df80e50f8b850cddc92fcf847(SHA1)

   Length of CTL file: 4947
   The CTL File was last modified on Fri Mar 06 21:56:07 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.

CTL Record #:2
----
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 CCM+TFTP
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

[...]

The CTL file was verified successfully.
```

6. На стороне IP-телефона можно проверить, что после того, как IP-телефоны были перезапущены, они загрузили обновленную версию файла CTL (соответствия контрольной суммы MD5 когда по сравнению с выходными данными от CUCM):

От Токенлесса Солушна к Аппаратным eToken

В этом разделе описывается переместить безопасность кластера CUCM далеко от нового решения Tokenless и назад к использованию аппаратных eToken.

Когда безопасность кластера CUCM установлена в Смешанный режим с использованием команд CLI, и файл CTL подписан с CCM+TFTP (сервер) сертификат для узла Издателя CUCM, нет никаких сертификатов от аппаратного подарка eToken USB в файле CTL. Поэтому при выполнении Клиента CTL для обновления файла CTL (попятитесь к использованию аппаратных eToken), это сообщение об ошибках появляется:

```
The Security Token you have inserted does not exist in the CTL File
```

```
Please remove any Security Tokens already inserted and insert another
Security Token. Click Ok when done.
```

Это особенно важно в сценариях, которые включают переход на более ранние версии (когда версия коммутирована назад) системы к pre-10.x версии, которая не включает **utils ctl** команды. Предыдущий файл CTL перемещен (без изменений в его содержании) в процессе обновления или Linux к обновлению Linux (L2), и это не содержит сертификаты eToken, как ранее упомянуто. Ниже приведен пример выходных данных:

```
admin:show ctl
The checksum value of the CTL file:
1d97d9089dd558a062cccfcb1dc4c57f(MD5)
3b452f9ec9d6543df80e50f8b850cddc92fcf847(SHA1)

Length of CTL file: 4947
The CTL File was last modified on Fri Mar 06 21:56:07 CET 2015

Parse CTL File
----------------

Version: 1.2
HeaderLength: 336 (BYTES)

BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
3 SIGNERID 2 149
4 SIGNERNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
5 SERIALNUMBER 16 70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB
6 CANAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
7 SIGNATUREINFO 2 15
8 DIGESTALGORTITHM 1
9 SIGNATUREALGOINFO 2 8
10 SIGNATUREALGORTITHM 1
11 SIGNATUREMODULUS 1
12 SIGNATURE 128
65 ba 26 b4 ba de 2b 13
b8 18 2 4a 2b 6c 2d 20
7d e7 2f bd 6d b3 84 c5
bf 5 f2 74 cb f2 59 bc
b5 c1 9f cd 4d 97 3a dd
6e 7c 75 19 a2 59 66 49
b7 64 e8 9a 25 7f 5a c8
56 bb ed 6f 96 95 c3 b3
72 7 91 10 6b f1 12 f4
d5 72 e 8f 30 21 fa 80
bc 5d f6 c5 fb 6a 82 ec
f1 6d 40 17 1b 7d 63 7b
52 f7 7a 39 67 e1 1d 45
b6 fe 82 0 62 e3 db 57
8c 31 2 56 66 c8 91 c8
d8 10 cb 5e c3 1f ef a
14 FILENAME 12
15 TIMESTAMP 4

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.

CTL Record #:2

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 **CCM+TFTP**
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

CTL Record #:3

BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1138
2 DNSNAME 16 cucm-1051-a-pub
3 SUBJECTNAME 60 CN=CAPF-e41e7d87;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
4 FUNCTION 2 CAPF
5 ISSUERNAME 60 CN=CAPF-e41e7d87;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
6 SERIALNUMBER 16 74:4B:49:99:77:04:96:E7:99:E9:1E:81:D3:C8:10:9B
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 680 46 EE 5A 97 24 65 B0 17 7E 5F 7E 44 F7 6C 0A
F3 63 35 4F A7 (SHA1 Hash HEX)
10 IPADDRESS 4

CTL Record #:4

BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1161
2 DNSNAME 17 cucm-1051-a-sub1
3 SUBJECTNAME 63 CN=cucm-1051-a-sub1;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
4 FUNCTION 2 CCM+TFTP
5 ISSUERNAME 63 CN=cucm-1051-a-sub1;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
6 SERIALNUMBER 16 6B:EB:FD:CD:CD:8C:A2:77:CB:2F:D1:D1:83:A6:0E:72
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 696 21 7F 23 DE AF FF 04 85 76 72 70 BF B1 BA 44
DB 5E 90 ED 66 (SHA1 Hash HEX)

```
10 IPADDRESS 4

The CTL file was verified successfully.

admin:
```

Для этого сценария выполните эти шаги для безопасного обновления файлов CTL без потребности использовать процедуру для потерянных eToken, которая заканчивается в ручном удалении файла CTL от всех IP-телефонов:

1. Получите Административный доступ к CLI узла Издателя CUCM.

2. Войдите **файл удаляют** команду **CTLFile.tlv tftp** в CLI узла Издателя для удаления файла CTL:
   ```
   admin:file delete tftp CTLFile.tlv
   Delete the File CTLFile.tlv?
   Enter "y" followed by return to continue: y
   files: found = 1, deleted = 1
   ```
3. Откройте **Клиента аутентификации Safenet** на машине Microsoft Windows, которая имеет установленного Клиента CTL (она установлена автоматически с Клиентом CTL):

4. В Клиенте аутентификации Safenet перейдите к *Усовершенствованному Представлению*:

5. Вставьте первый аппаратный eToken USB.

6. Выберите сертификат под папкой *Сертификатов пользователя* и экспортируйте его в папку на ПК. Когда предложено для пароля, используйте пароль по умолчанию **Cisco123**:

7. Повторите эти шаги для второго аппаратного eToken USB так, чтобы оба сертификата были экспортированы в ПК:

8. Войдите в Cisco Унифицированное администрирование Операционной системы (OS) и перейдите к **Безопасности> Управление сертификатами> Сертификат Загрузки**:

9. Страница Upload Certificate тогда появляется. Выберите **Phone-SAST-trust** из выпадающего меню Цели Сертификата и выберите сертификат, который вы экспортировали от первого eToken:

10. Выполните предыдущие шаги для загрузки сертификата, который вы экспортировали от второго eToken:

11. Выполните Клиента CTL, предоставьте IP-адрес / имя хоста узла Издателя CUCM и введите Учетные данные администратора CCM:

12. Так как кластер уже находится в Смешанном режиме, но никакой файл CTL не существует на узле Издателя, это предупреждающее сообщение появляется (нажмите **OK** для игнорирования его):
```
No CTL File exists on the server but the Call Manager Cluster Security Mode
is in Secure Mode.
For the system to function, you must create the CTL File and set Call Manager
Cluster the Secure Mode.
```
13. От Клиента CTL нажмите кнопку с зависимой фиксацией **Update CTL File**, и затем нажмите **Next**:

14. Вставьте первый маркер безопасности и нажмите **OK**:

15. После того, как подробные данные маркера безопасности отображены, **нажмите Add**:

16. Как только содержание файла CTL появляется, **нажмите Add Маркеры** для добавления второго eToken USB:

17. После того, как подробные данные маркера безопасности появляются, **нажмите Add**:

18. После того, как содержание файла CTL появляется, нажмите **Finish**. Когда предложено для пароля, введите **Cisco123**:

19. Когда список Серверов CUCM, на которых существует файл CTL, появляется, нажмите **Done**:

20. Перезапустите TFTP и Сервисы CallManager на всех узлах в кластере, которые выполняют эти сервисы.

21. Перезапустите все IP-телефоны так, чтобы они могли получить новую версию файла CTL от Сервиса TFTP CUCM.

22. Для проверки содержания файла CTL введите **показ ctl** команда в CLI. В файле CTL вы видите сертификаты от обоих из eToken USB (один из них используется для подписания файла CTL). Ниже приведен пример выходных данных:

```
admin:show ctl
The checksum value of the CTL file:
2e7a6113eadbdae67ffa918d81376902(MD5)
d0f3511f10eef775cc91cce3fa6840c2640f11b8(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 22:53:33 CET 2015

[...]

CTL Record #:1
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN0054f509 ";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 3C:F9:27:00:00:00:AF:A2:DA:45
7 PUBLICKEY 140
9 CERTIFICATE 902 19 8F 07 C4 99 20 13 51 C5 AE BF 95 03 93 9F F2
CC 6D 93 90 (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was not used to sign the CTL file.

[...]

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.

The CTL file was verified successfully.
```

23. На стороне IP-телефона можно проверить, что после того, как IP-телефоны были перезапущены, они загрузили обновленную версию файла CTL (соответствия контрольной суммы MD5 когда по сравнению с выходными данными от CUCM):

Это изменение возможно, потому что вы ранее экспортировали и загрузили сертификаты eToken к Базе доверенных сертификатов Сертификата CUCM, и IP-телефоны в состоянии проверить этот неизвестный сертификат, который использовался для подписания файла CTL против службы проверки доверия (TVS), которая работает на CUCM. Этот регистрационный фрагмент иллюстрирует, как IP-телефон связывается с TVS CUCM с запросом проверить неизвестный сертификат eToken, который загружают как **Телефонное доверие SAST** и доверяют:

```
//In the Phone Console Logs we can see a request sent to TVS server to verify unknown
certificate
8074: NOT 23:00:22.335499 SECD: setupSocketToTvsProxy: Connected to TVS proxy server
8075: NOT 23:00:22.336918 SECD: tvsReqFlushTvsCertCache: Sent Request to TVS proxy,
len: 3708

//In the TVS logs on CUCM we can see the request coming from an IP Phone which is being
successfully verified
23:00:22.052 | debug tvsHandleQueryCertReq
23:00:22.052 | debug tvsHandleQueryCertReq : Subject Name is: cn="SAST-ADN008580ef
";ou=IPCBU;o="Cisco Systems
23:00:22.052 | debug tvsHandleQueryCertReq : Issuer Name is: cn=Cisco Manufacturing
CA;o=Cisco Systems
23:00:22.052 | debug tvsHandleQueryCertReq :subjectName and issuerName matches for
eToken certificate
23:00:22.052 | debug tvsHandleQueryCertReq : SAST Issuer Name is: cn=Cisco
Manufacturing CA;o=Cisco Systems
23:00:22.052 | debug tvsHandleQueryCertReq : This is SAST eToken cert
23:00:22.052 | debug tvsHandleQueryCertReq : Serial Number is: 83E9080000005545AF31
23:00:22.052 | debug CertificateDBCache::getCertificateInformation - Looking up the
certificate cache using Unique MAP ID : 83E9080000005545AF31cn=Cisco Manufacturing
CA;o=Cisco Systems
23:00:22.052 | debug ERROR:CertificateDBCache::getCertificateInformation - Cannot find
the certificate in the cache
23:00:22.052 | debug CertificateCTLCache::getCertificateInformation - Looking up the
certificate cache using Unique MAP ID : 83E9080000005545AF31cn=Cisco Manufacturing
CA;o=Cisco Systems, len : 61
23:00:22.052 | debug CertificateCTLCache::getCertificateInformation - Found entry
{rolecount : 1}
23:00:22.052 | debug CertificateCTLCache::getCertificateInformation - {role : 0}
23:00:22.052 | debug convertX509ToDER -x509cert : 0xa3ea6f8
23:00:22.053 | debug tvsHandleQueryCertReq: Timer started from tvsHandleNewPhConnection

//In the Phone Console Logs we can see reply from TVS server to trust the new certificate
(eToken Certificate which was used to sign the CTL file)
8089: NOT 23:00:22.601218 SECD: clpTvsInit: Client message received on TVS proxy socket
8090: NOT 23:00:22.602785 SECD: processTvsClntReq: Success reading the client TVS
request, len : 3708
8091: NOT 23:00:22.603901 SECD: processTvsClntReq: TVS Certificate cache flush
request received
8092: NOT 23:00:22.605720 SECD: tvsFlushCertCache: Completed TVS Certificate cache
flush request
```

Регенерация сертификата для решения для CTL Tokenless

В этом разделе описывается восстановить сертификат безопасности кластера CUCM, когда используется решение для CTL Tokenless.

В процессе обслуживания CUCM, иногда изменения сертификата CallManager узла Издателя CUCM. Сценарии, в которых это может произойти, включают изменение имени хоста, изменение домена, или просто регенерацию сертификата (должный закрыть дату

окончания срока действия сертификата).

После того, как файл CTL обновлен, он подписан с другим сертификатом, чем те, которые существуют в файле CTL, который установлен на IP-телефонах. Обычно, этот новый файл CTL не принят; однако, после того, как IP-телефон находит неизвестный сертификат, который используется для подписания файла CTL, это связывается с сервисом TVS на CUCM.

> **Примечание:** Список серверов TVS находится в файле Настройки IP-телефона и сопоставлен в серверах CUCM от **Аппаратного пула** IP-телефона**> Группа CallManager**.

После успешной проверки против сервера TVS IP-телефон обновляет свой файл CTL с новой версией. Эти события имеют место в таком сценарии:

1. Файл CTL существует на CUCM и на IP-телефоне. CCM+TFT (сервер), сертификат для узла Издателя CUCM используется для подписания файла CTL:

```
admin:show ctl
The checksum value of the CTL file:
7b7c10c4a7fa6de651d9b694b74db25f(MD5)
819841c6e767a59ecf2f87649064d8e073b0fe87(SHA1)

Length of CTL file: 4947
The CTL File was last modified on Mon Mar 09 16:59:43 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.

CTL Record #:2
----
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 CCM+TFTP
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

[...]

The CTL file was verified successfully.
```

2. Файл **CallManager.pem** (сертификат CCM+TFTP) восстановлен, и вы видите, что изменяется серийный номер сертификата:

3. **Utils ctl** команда **CTLFile обновления** введен в CLI для обновления файла CTL:

```
admin:utils ctl update CTLFile
This operation will update the CTLFile. Do you want to continue? (y/n):y

Updating CTL file
CTL file Updated
Please Restart the TFTP and Cisco CallManager services on all nodes in
the cluster that run these services
admin:
```

4. Сервис TVS обновляет свой кэш сертификата с новыми подробными данными файла CTL:

```
17:10:35.825 | debug CertificateCache::localCTLCacheMonitor - CTLFile.tlv has been
modified. Recaching CTL Certificate Cache
17:10:35.826 | debug updateLocalCTLCache : Refreshing the local CTL certificate cache
17:10:35.827 | debug tvs_sql_get_all_CTL_certificate - Unique Key used for Caching ::
6B1D357B6841740B078FEE4A1813D5D6CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL, length : 93
17:10:35.827 | debug tvs_sql_get_all_CTL_certificate - Unique Key used for Caching ::
6B1D357B6841740B078FEE4A1813D5D6CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL, length : 93
17:10:35.827 | debug tvs_sql_get_all_CTL_certificate - Unique Key used for Caching ::
744B5199770516E799E91E81D3C8109BCN=CAPF-e41e7d87;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL, length : 91
17:10:35.827 | debug tvs_sql_get_all_CTL_certificate - Unique Key used for Caching ::
6BEBFDCDCD8CA277CB2FD1D183A60E72CN=cucm-1051-a-sub1;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL, length : 94
```

5. При просмотре содержимого файла CTL вы видите, что файл подписан с новым сертификатом Сервера CallManager для узла Издателя:

```
admin:show ctl
The checksum value of the CTL file:
ebc649598280a4477bb3e453345c8c9d(MD5)
ef5c006b6182cad66197fac6e6530f15d009319d(SHA1)

Length of CTL file: 6113
The CTL File was last modified on Mon Mar 09 17:07:52 CET 2015

[..]

CTL Record #:1
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1675
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 6B:1D:35:7B:68:41:74:0B:07:8F:EE:4A:18:13:D5:D6
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 955 5C AF 7D 23 FE 82 DB 87 2B 6F 4D B7 F0 9D D5
86 EE E0 8B FC (SHA1 Hash HEX)
10 IPADDRESS 4

This etoken was used to sign the CTL file.

CTL Record #:2
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1675
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 CCM+TFTP
5 ISSUERNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
6 SERIALNUMBER 16 6B:1D:35:7B:68:41:74:0B:07:8F:EE:4A:18:13:D5:D6
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 955 5C AF 7D 23 FE 82 DB 87 2B 6F 4D B7 F0 9D D5
86 EE E0 8B FC (SHA1 Hash HEX)
10 IPADDRESS 4

[...]

The CTL file was verified successfully.
```

6. От Унифицированной страницы Serviceability TFTP и Сервисы Cisco CallManager перезапущены на всех узлах в кластере, которые выполняют эти сервисы.

7. IP-телефоны перезапущены, и они связываются с сервером TVS для проверки неизвестного сертификата, который теперь используется для подписания новой версии файла CTL:

```
// In the Phone Console Logs we can see a request sent to TVS server to verify
unknown certificate
2782: NOT 17:21:51.794615 SECD: setupSocketToTvsProxy: Connected to TVS proxy server
2783: NOT 17:21:51.796021 SECD: tvsReqFlushTvsCertCache: Sent Request to TVS
proxy, len: 3708

// In the TVS logs on CUCM we can see the request coming from an IP Phone which is
being successfully verified
17:21:51.831 | debug tvsHandleQueryCertReq
17:21:51.832 | debug tvsHandleQueryCertReq : Subject Name is: CN=cucm-1051-a-pub;
OU=TAC;O=Cisco;L=Krakow;ST=Malopolska
17:21:51.832 | debug tvsHandleQueryCertReq : Issuer Name is: CN=cucm-1051-a-pub;
OU=TAC;O=Cisco;L=Krakow;ST=Malopolska;
17:21:51.832 | debug tvsHandleQueryCertReq : Serial Number is:
6B1D357B6841740B078FEE4A1813D5D6
17:21:51.832 | debug CertificateDBCache::getCertificateInformation - Looking up the
certificate cache using Unique MAPco;L=Krakow;ST=Malopolska;C=PL
17:21:51.832 | debug CertificateDBCache::getCertificateInformation - Found entry
{rolecount : 2}
17:21:51.832 | debug CertificateDBCache::getCertificateInformation - {role : 0}
17:21:51.832 | debug CertificateDBCache::getCertificateInformation - {role : 2}
17:21:51.832 | debug convertX509ToDER -x509cert : 0xf6099df8
17:21:51.832 | debug tvsHandleQueryCertReq: Timer started from
```

```
tvsHandleNewPhConnection

// In the Phone Console Logs we can see reply from TVS server to trust the new
certificate (new CCM Server Certificate which was used to sign the CTL file)
2797: NOT 17:21:52.057442 SECD: clpTvsInit: Client message received on TVS
proxy socket
2798: NOT 17:21:52.058874 SECD: processTvsClntReq: Success reading the client TVS
request, len : 3708
2799: NOT 17:21:52.059987 SECD: processTvsClntReq: TVS Certificate cache flush
request received
2800: NOT 17:21:52.062873 SECD: tvsFlushCertCache: Completed TVS Certificate
cache flush request
```

8. Наконец, на IP-телефонах, можно проверить, что файл CTL обновлен с новой версией и что контрольная сумма MD5 нового файла CTL совпадает с тем из CUCM: