Кластер CUCM, измененный от смешанного режима до незащищенного примера конфигурации режима

Содержание

Введение

Документ описывает шаги, требуемые для изменения Режима безопасности Cisco Unified Communications Manager (CUCM) от Смешанного режима до Незащищенного режима. Это также показывает, как содержание файла Списка надежных сертификатов (CTL) изменено, когда завершено это перемещение.

Существует три главных части для изменения Режима безопасности CUCM:

1a. Выполните клиента CTL и выберите желаемый вариант Режима безопасности.
1b. Введите команду CLI для выбора желаемого варианта Режима безопасности.
2. Перезапустите Cisco CallManager и Сервисы TFTP Cisco на всех серверах CUCM, которые выполняют эти сервисы.
3. Перезапустите все IP-телефоны так, чтобы они могли загрузить обновленную версию файла CTL.

> **Примечание:** Если кластерный режим безопасности изменен от Смешанного режима до Незащищенного режима, файл CTL все еще существует на сервере (серверах) и по телефонам, но файл CTL не содержит CCM+TFTP (сервер) сертификаты. Начиная с

CCM+TFTP (сервер) сертификаты не существуют в файле CTL, это вынуждает телефон зарегистрироваться как Незащищенное в CUCM.

Предварительные условия

Требования

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

- Сервис Поставщика CTL подключен и работает на всех активных серверах TFTP в кластере. По умолчанию сервис работает на порте TCP 2444, но это может модифицироваться в конфигурации Параметра сервиса CUCM.
- Сервисы функции представительства сертифицирующей организации (CAPF) подключены и работают на узле Издателя.
- База данных (DB), Репликация в кластере работает правильно и серверы, реплицирует данные в режиме реального времени.

Используемые компоненты

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

- Кластер Выпуска 10.0.1.11900-2 CUCM двух узлов
- IP-телефон Cisco 7975 (зарегистрированный в Протоколе SCCP, версии микропрограммы SCCP75.9-3-1SR3-1S)
- Два Cisco Security Маркеры необходимы для установки кластера в Смешанный режим
- Один из Маркеров безопасности, перечисленных ранее, необходим для установки кластера в Незащищенный режим

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

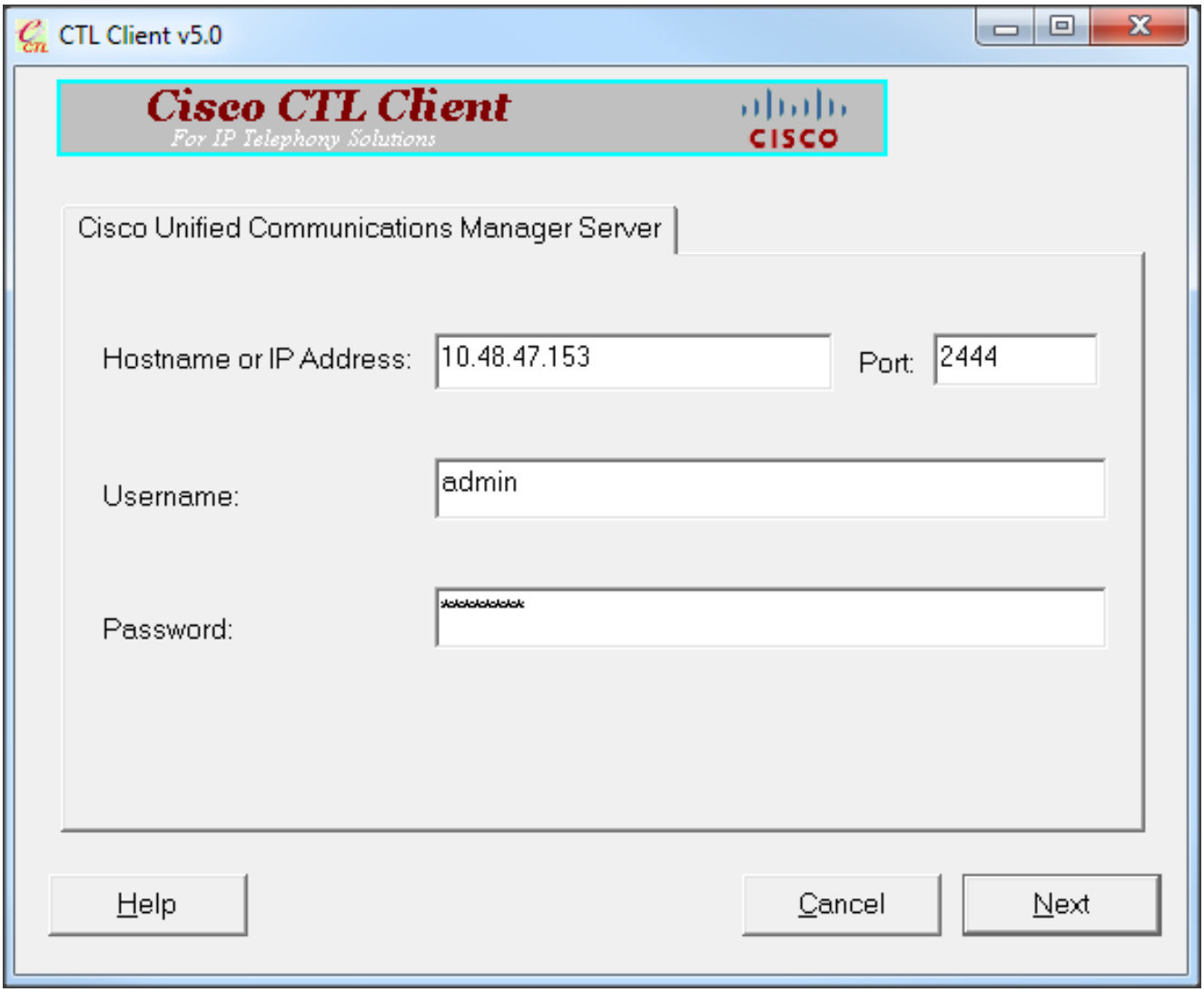
Для выполнения плагина Клиента CTL, он требуется, чтобы иметь доступ по крайней мере к одному маркеру безопасности, который был вставлен, чтобы создать или обновить последний файл CTL, существует на Сервере публикаций CUCM. Другими словами, по крайней мере один из сертификатов eToken, который существует в текущем файле CTL на CUCM, должен быть на маркере безопасности, который используется для изменения Режима безопасности.

Настройка

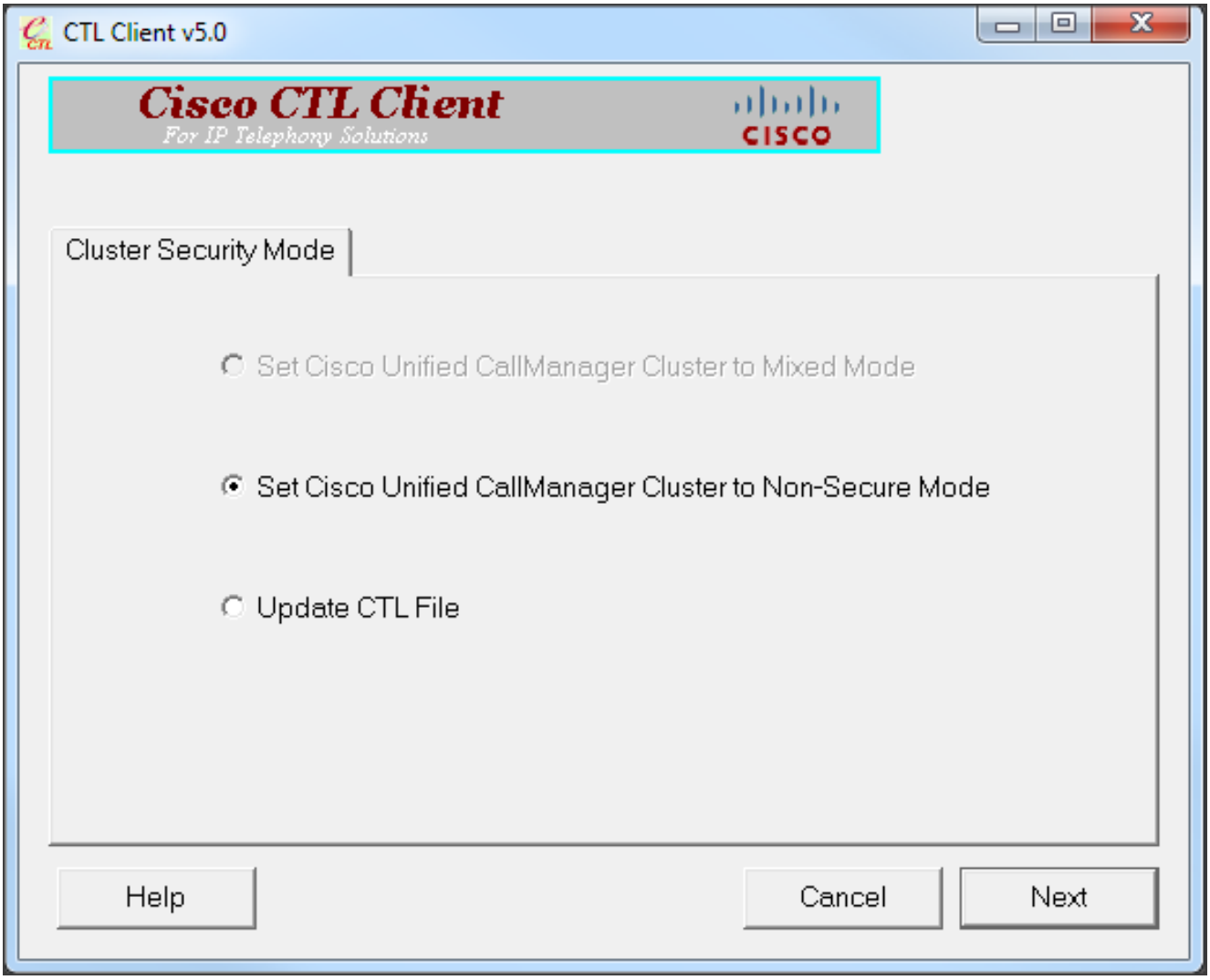
Измените безопасность кластера CUCM от смешанного режима до незащищенного режима с клиентом CTL

Выполните эти шаги для изменения безопасности кластера CUCM от Смешанного режима до Незащищенного режима с клиентом CTL:

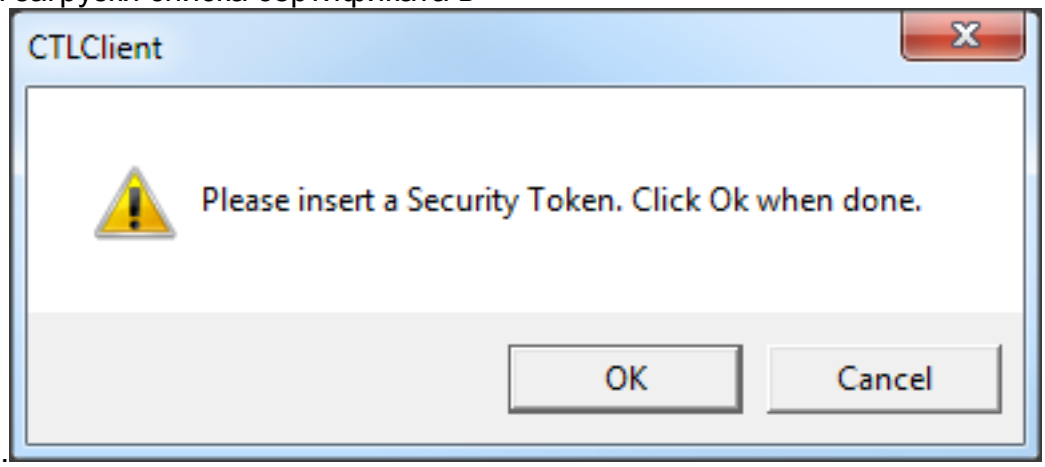
1. Получите один маркер безопасности, который вы вставили для настройки последнего файла CTL.
2. Выполните клиента CTL. Предоставьте имя хоста/адрес IP Паба CUCM и Учетных данных администратора CCM. **Нажмите кнопку Next.**



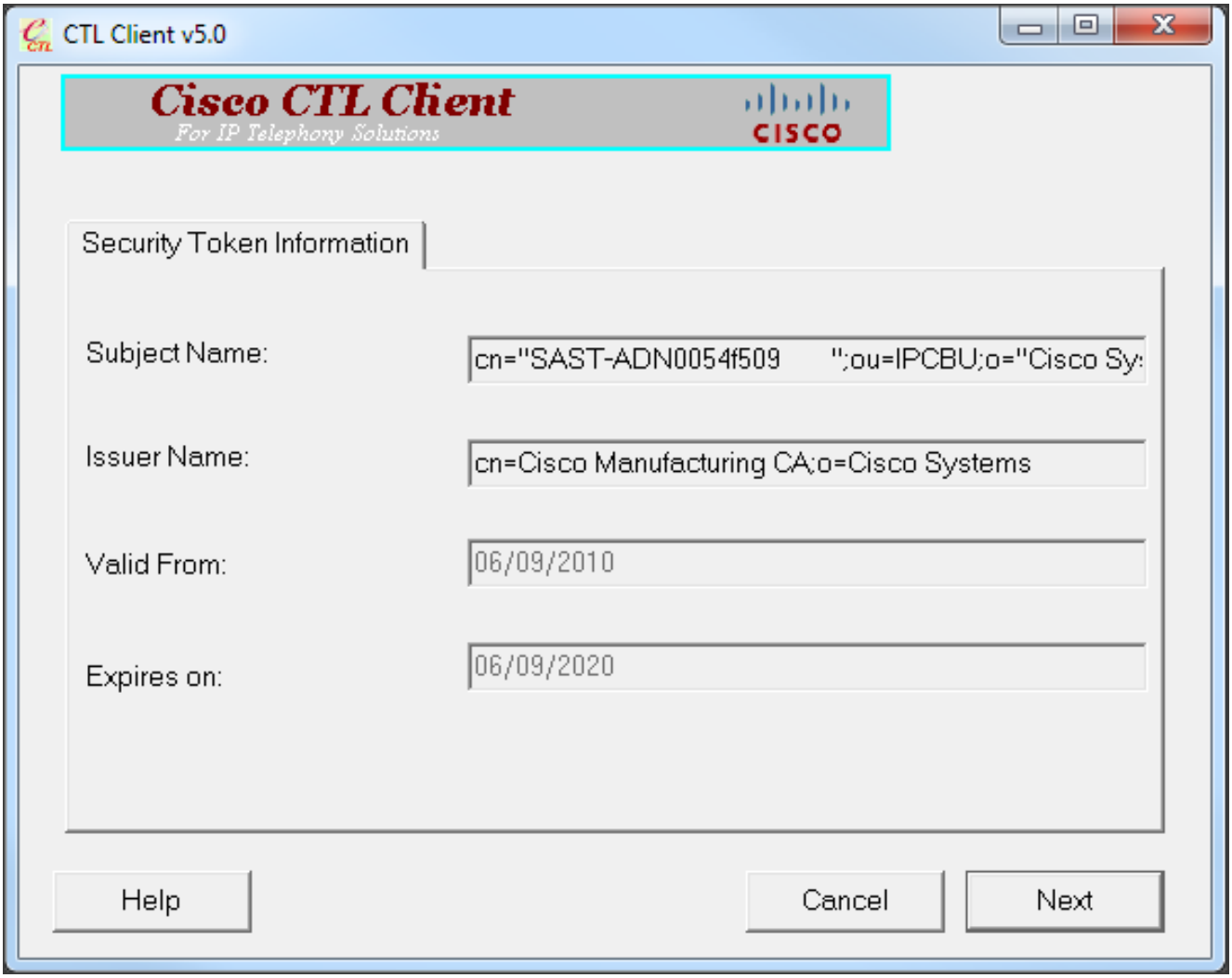
3. Нажмите **Кластер Cisco Unified CallManager Набора к Незащищенной кнопке с зависимой фиксацией Mode. Нажмите кнопку Next.**



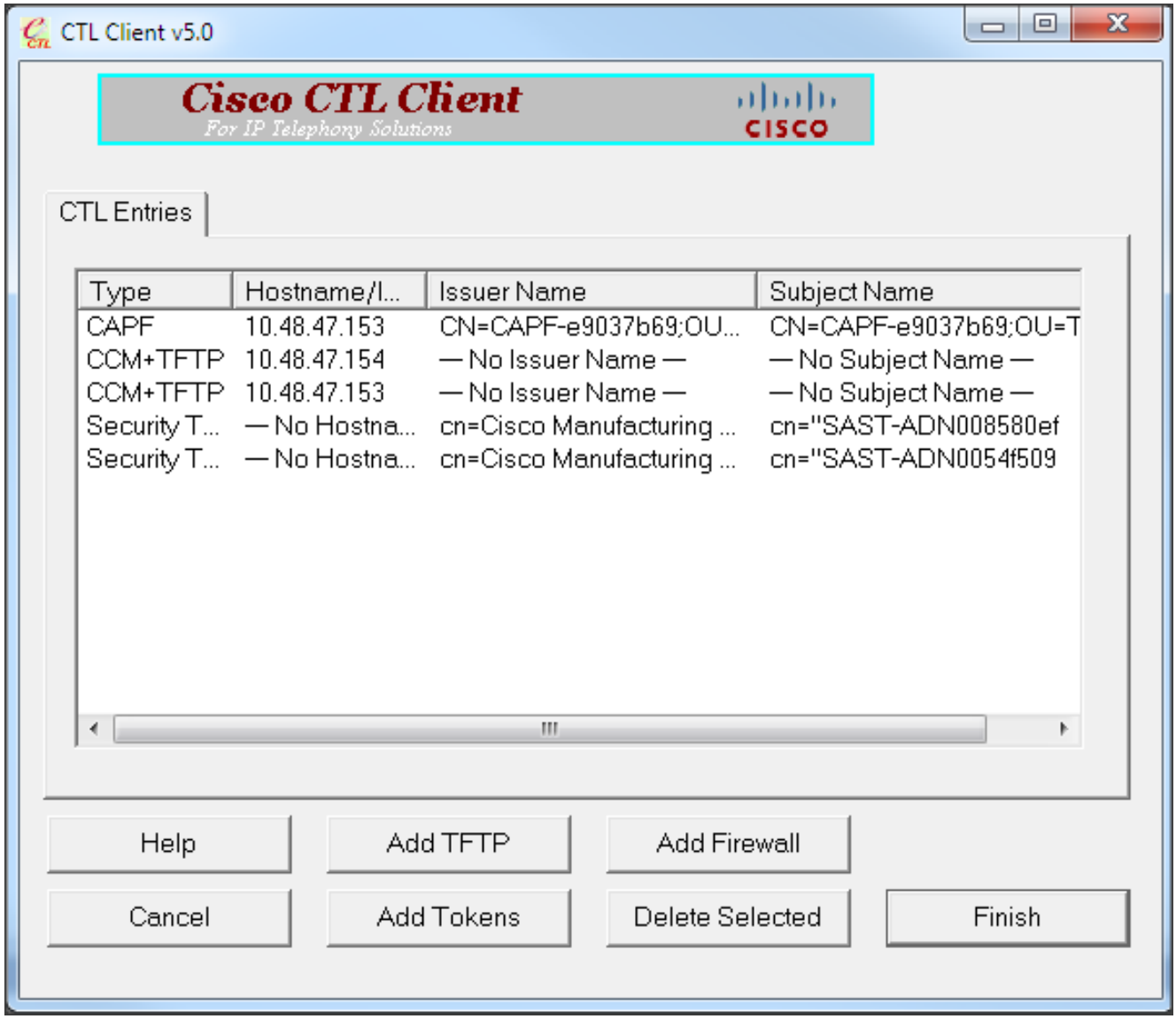
4. Вставьте один маркер безопасности, который был вставлен, чтобы настроить последний файл CTL и нажать **OK**. Это - один из маркеров, который использовался для начальной загрузки списка сертификата в CTLFile.tlv.



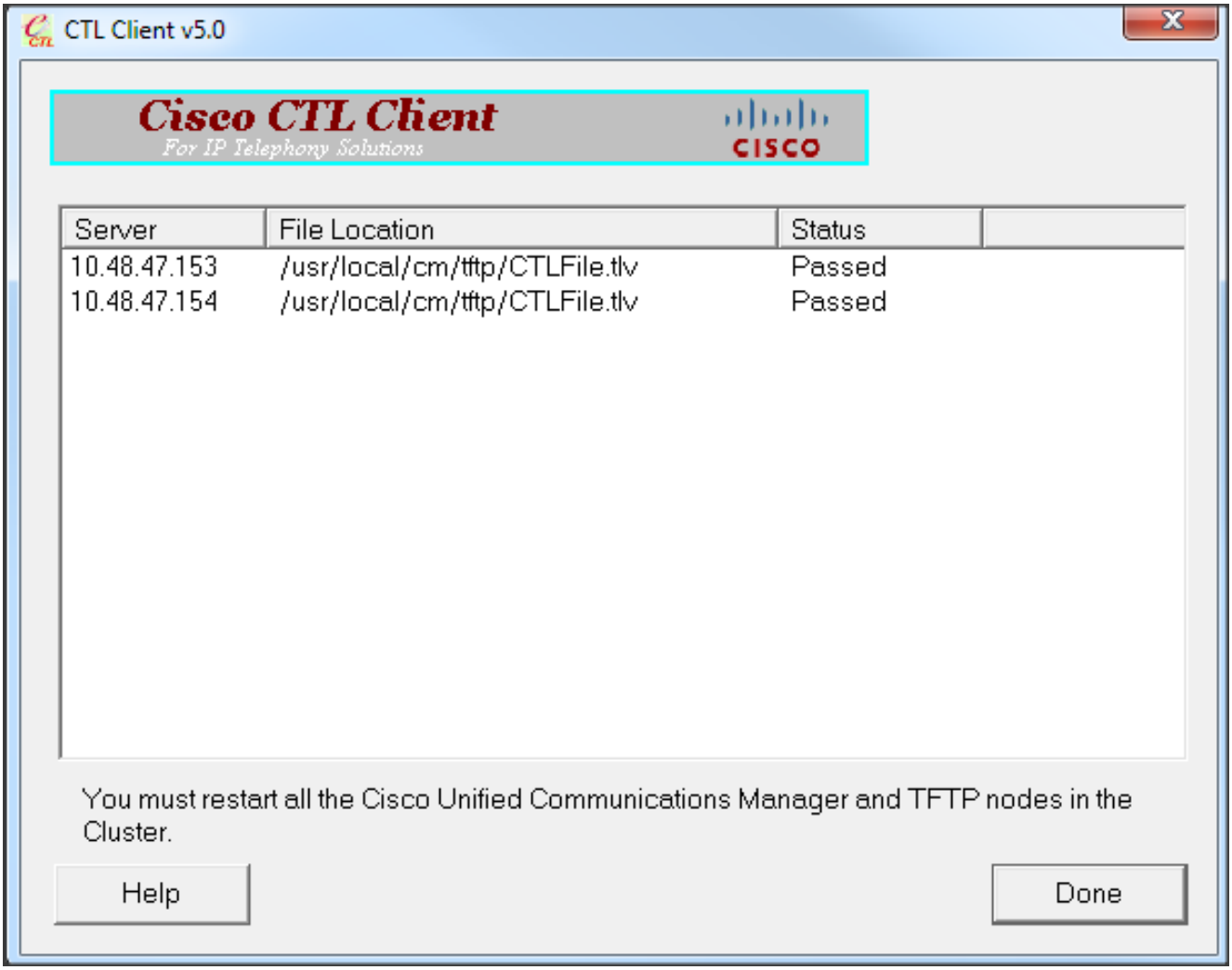
5. Подробные данные Маркера безопасности отображены. **Нажмите кнопку Next.**



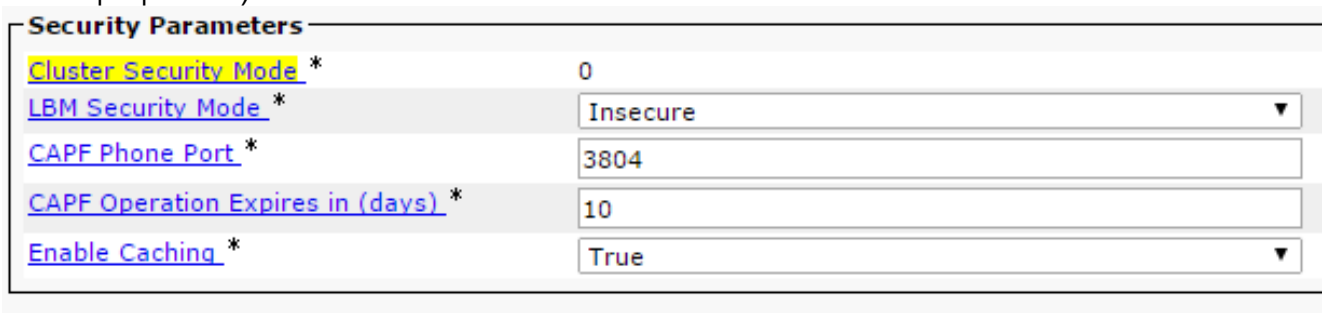
6. Содержание файла CTL отображено. **Нажмите кнопку Finish. По запросу введите пароль**
cisco123.



7. Список Серверов CUCM, на которых существует файл CTL, отображен. **Нажмите "Готово".**



8. Выберите **CUCM Admin Page> System> Enterprise Parameters** и проверьте, что кластер был установлен в Незащищенный Режим ("0", указывает Незащищенный).



9. Перезапустите TFTP и Сервисы Cisco CallManager на всех узлах в кластере, которые выполняют эти сервисы.
10. Перезапустите все IP-телефоны так, чтобы они могли получить новую версию файла CTL от TFTP CUCM.

Измените безопасность кластера CUCM от смешанного режима до незащищенного режима с CLI

Эта конфигурация только для Выпуска 10. X CUCM и позже. Для установки Режима безопасности Кластера CUCM в Незащищенный введите **utils ctl кластер набора non-secure-**

mode команда на CLI Издателя. После того, как это завершено, перезапустите TFTP и Сервисы Cisco CallManager на всех узлах в кластере, которые выполняют эти сервисы.

Вот типовые выходные данные CLI, которые показывают использование команды.

```
admin:utils ctl set-cluster non-secure-mode
This operation will set the cluster to non secure mode. Do you want to continue? (y/n):

Moving Cluster to Non Secure Mode
Cluster set to Non Secure Mode
Please Restart the TFTP and Cisco CallManager services on all nodes in the cluster that
run these services
admin:
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Для проверки CTLFIle.tlv можно использовать один из двух методов:

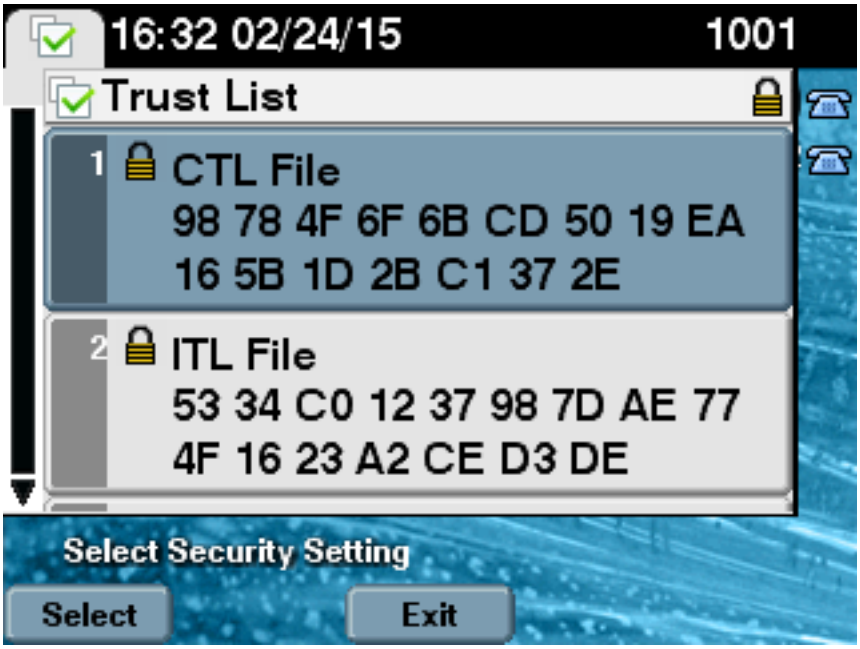
- Для проверки содержания и контрольной суммы MD5 подарка CTLFIle.tlv на стороне TFTP CUCM, введите **показ ctl** команда на CLI CUCM. Файл CTLFIle.tlv должен быть тем же на всех узлах CUCM.
- Для проверки контрольной суммы MD5 на 7975 IP-телефонах выберите**> Security Settings Конфигурация> Трастовый Список> Файл CTL**.

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

Набор кластера CUCM к режиму безопасности - контрольная сумма файла CTL

```
admin:show ctl
The checksum value of the CTL file:
98784f6f6bcd5019ea165b1d2bc1372e(MD5)
9c0aa839e5a84b18a43caf9f9ff23d8ebce90419(SHA1)
[...]
```

На стороне IP-телефона вы видите, что она имеет тот же установленный файл CTL (соответствия контрольной суммы MD5 когда по сравнению с выходными данными от CUCM).



Набор кластера CUCM к незащищенному режиму - содержимое файла CTL

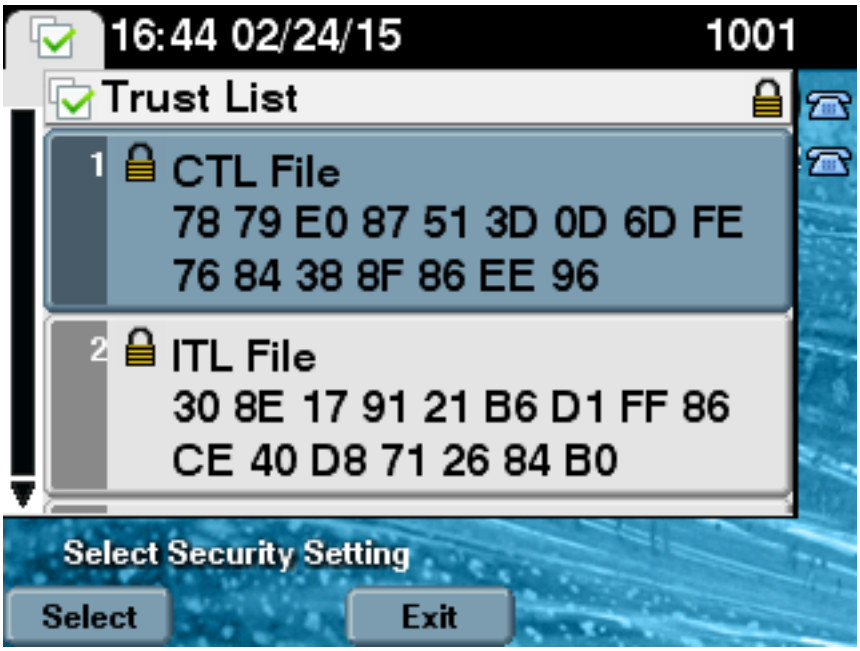
Вот пример файла CTL от набора кластера CUCM до Незащищенного режима. Вы видите, что сертификаты CCM+TFTP пусты и не содержат содержания. Остаток сертификатов в файлах CTL не изменен и является точно тем же как тогда, когда CUCM был установлен в Смешанный режим.

```
admin:show ctl
The checksum value of the CTL file:
7879e087513d0d6dfe7684388f86ee96(MD5)
be50e5f3e28e6a8f5b0a5fa90364c839fcc8a3a0(SHA1)


Length of CTL file: 3746
The CTL File was last modified on Tue Feb 24 16:37:45 CET 2015

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

Version: 1.2
HeaderLength: 304 (BYTES)

BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
3 SIGNERID 2 117
4 SIGNERNAME 56 cn="SAST-ADN0054f509 ";ou=IPCBU;o="Cisco Systems
5 SERIALNUMBER 10 3C:F9:27:00:00:00:AF:A2:DA:45
6 CANAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
7 SIGNATUREINFO 2 15
8 DIGESTALGORTITHM 1
9 SIGNATUREALGOINFO 2 8
10 SIGNATUREALGORTITHM 1
11 SIGNATUREMODULUS 1
12 SIGNATURE 128
45 ec 5 c 9e 68 6d e6
5d 4b d3 91 c2 26 cf c1
ee 8c b9 6 95 46 67 9e
19 aa b1 e9 65 af b4 67
36 7e e5 ee 60 10 b 1b
58 c1 6 64 40 cf e2 57
```

```
aa 86 73 14 ec 11 b a
3b 98 91 e2 e4 6e 4 50
ba ac 3e 53 33 1 3e a6
b7 30 0 18 ae 68 3 39
d1 41 d6 e3 af 97 55 e0
5b 90 f6 a5 79 3e 23 97
fb b8 b4 ad a8 b8 29 7c
1b 4f 61 6a 67 4d 56 d2
5f 7f 32 66 5c b2 d7 55
d9 ab 7a ba 6d b2 20 6
14 FILENAME 12
15 TIMESTAMP 4

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 used to sign the CTL file.

CTL Record #:2
----
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 not used to sign the CTL file.

CTL Record #:3
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 33
2 DNSNAME 13 10.48.47.153
4 FUNCTION 2 CCM+TFTP
10 IPADDRESS 4

CTL Record #:4
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1004
2 DNSNAME 13 10.48.47.153
3 SUBJECTNAME 60 CN=CAPF-e9037b69;OU=TAC;O=Cisco;L=Krakow;ST=Malopolska;C=PL
4 FUNCTION 2 CAPF
5 ISSUERNAME 60 CN=CAPF-e9037b69;OU=TAC;O=Cisco;L=Krakow;ST=Malopolska;C=PL
6 SERIALNUMBER 16 79:59:16:C1:54:AF:31:0C:0F:AE:EA:97:2E:08:1B:31
7 PUBLICKEY 140
9 CERTIFICATE 680 A0 A6 FC F5 FE 86 16 C1 DD D5 B7 57 38 9A 03 1C F7 7E FC 07 (SHA1 Hash HEX)
```

```
10 IPADDRESS 4

CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 33
2 DNSNAME 13 10.48.47.154
4 FUNCTION 2 CCM+TFTP
10 IPADDRESS 4

The CTL file was verified successfully.

admin:
```

На стороне IP-телефона, после того, как это было перезапущено и загрузило обновленную версию файла CTL, вы видите, что контрольная сумма MD5 совпадает когда по сравнению с выходными данными от CUCM.



Поместите безопасность кластера CUCM от смешанного режима до незащищенного режима, когда будут потеряны маркеры USB

Маркеры безопасности для защищенных кластеров могли быть потеряны. В той ситуации необходимо рассмотреть эти два сценария:

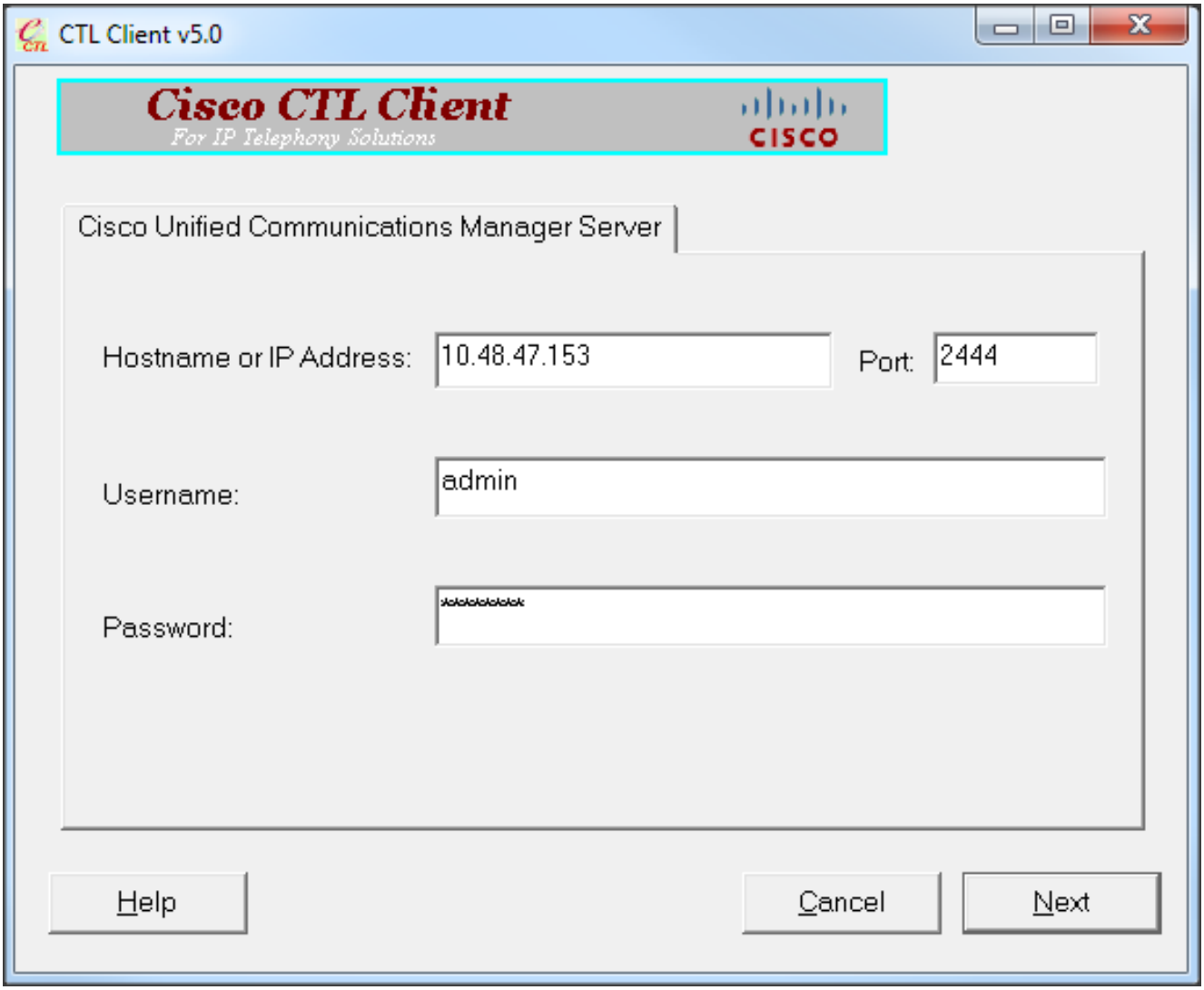
- Версия 10.0.1 cluster run или позже
- Cluster run версия ранее, чем 10. x

В первом сценарии завершите процедуру, описанную в Изменении Безопасность Кластера CUCM от Смешанного Режима до Незащищенного Режима с разделом CLI для восстановления с проблемы. Так как та команда CLI не требует маркера CTL, она могла использоваться, даже если бы кластер был помещен в Смешанный режим с клиентом CTL.

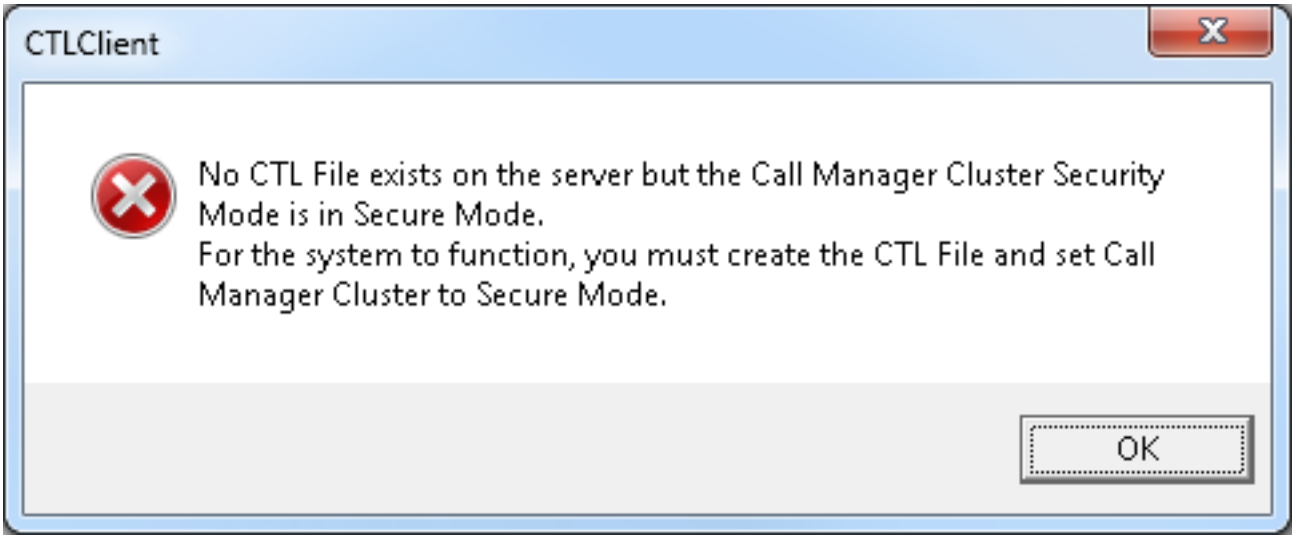
Когда версия ранее, чем 10.x CUCM используется, ситуация становится более сложной. Если вы теряете или забываете пароль одного из маркеров, можно все еще использовать

другой для выполнения клиента CTL с текущими файлами CTL. Это настоятельно рекомендовано, чтобы получить другой eToken и добавить его к файлу CTL как можно скорее ради резервирования. Если вы теряете или забываете пароли для всех eToken, перечисленных в вашем файле CTL, необходимо получить новую пару eToken и выполнить ручную процедуру, как объяснено сюда.

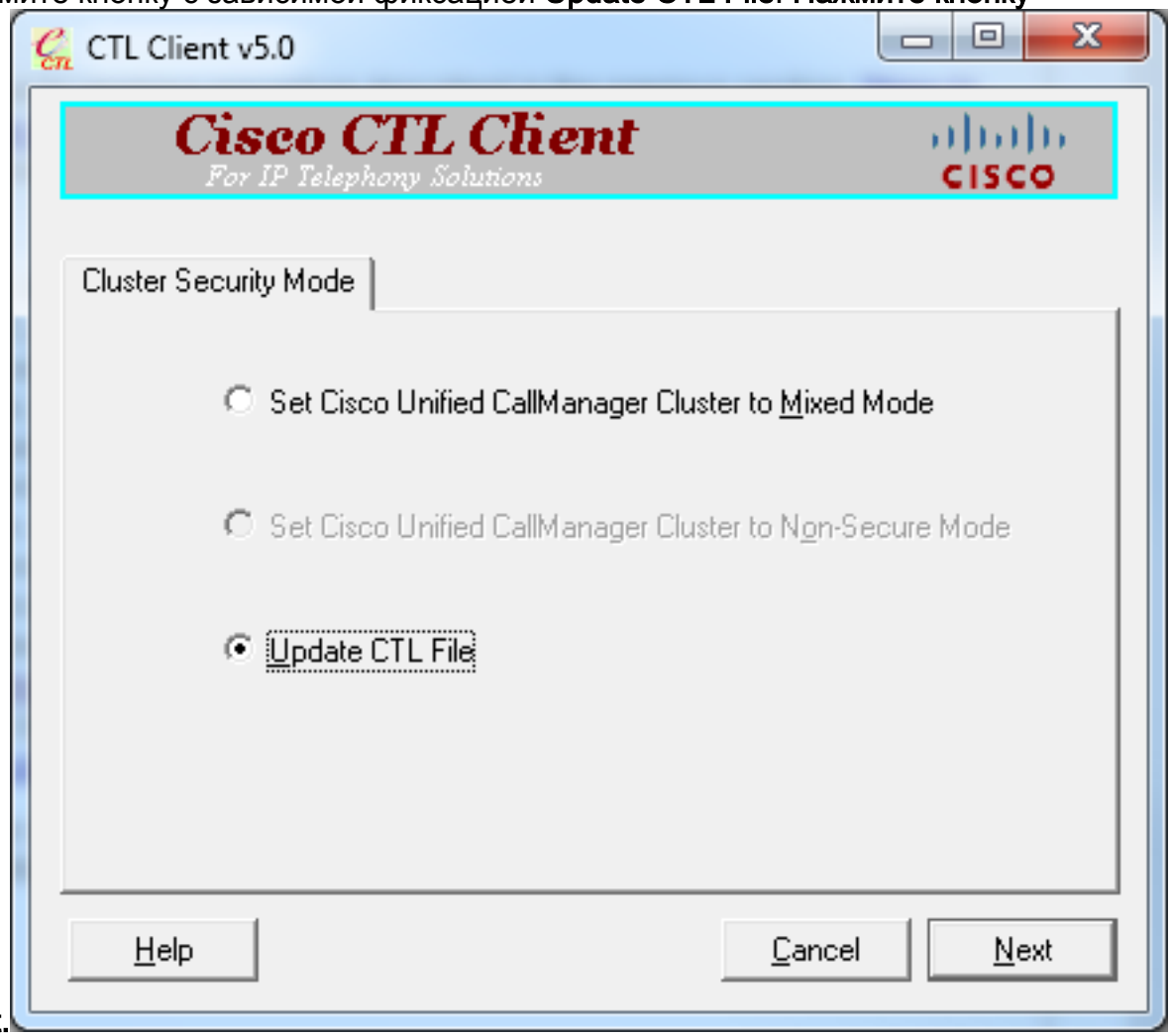
1. Войдите **файл удаляют** команду **CTLFile.tlv tftp** для удаления файла CTL из всех серверов TFTP.
```
admin:file delete tftp CTLFile.tlv
Delete the File CTLFile.tlv?
Enter "y" followed by return to continue: y
files: found = 1, deleted = 1

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.
```
2. Выполните клиента CTL. Введите имя хоста/адрес IP Паба CUCM и Учетных данных администратора CCM. **Нажмите кнопку Next.**



3. Так как кластер находится в Смешанном режиме, однако никакой файл CTL не существует на Издателе, это предупреждение отображено. Нажмите **OK**, чтобы проигнорировать его и продолжиться вперед.

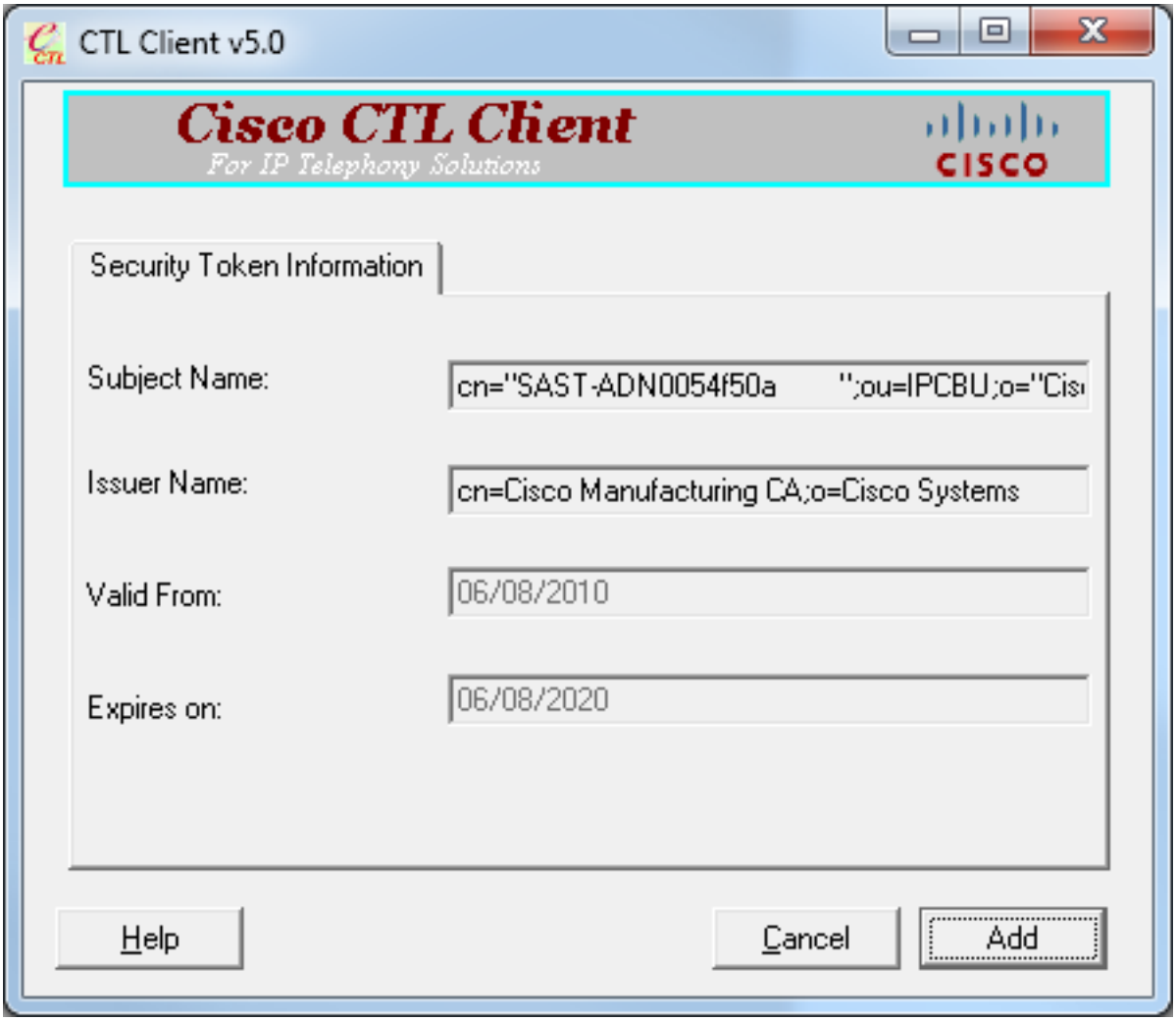


4. Нажмите кнопку с зависимой фиксацией **Update CTL File**. **Нажмите кнопку**

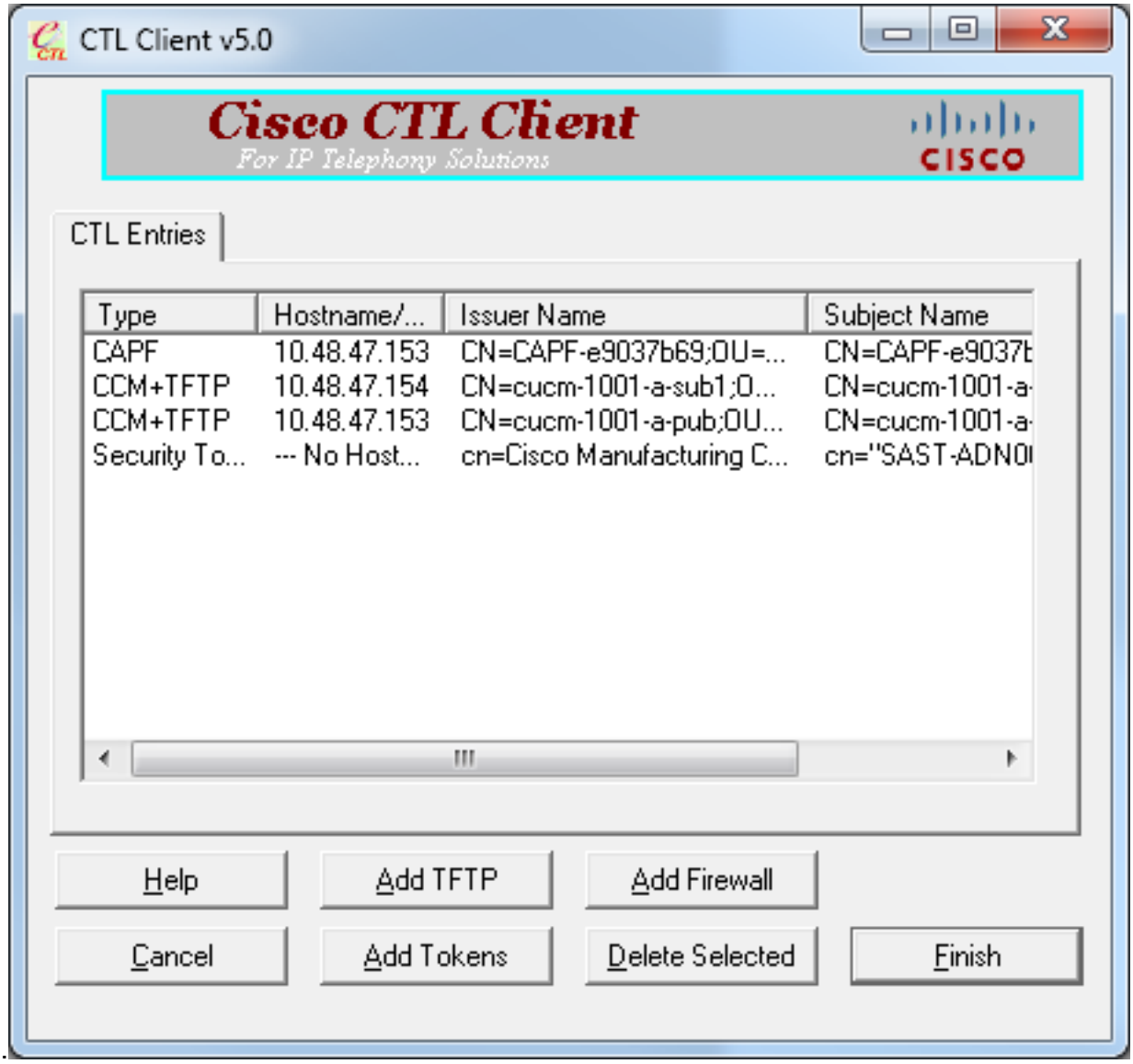


Next.

5. Клиент CTL просит добавлять Маркер безопасности. **Нажмите Add** для перехода.

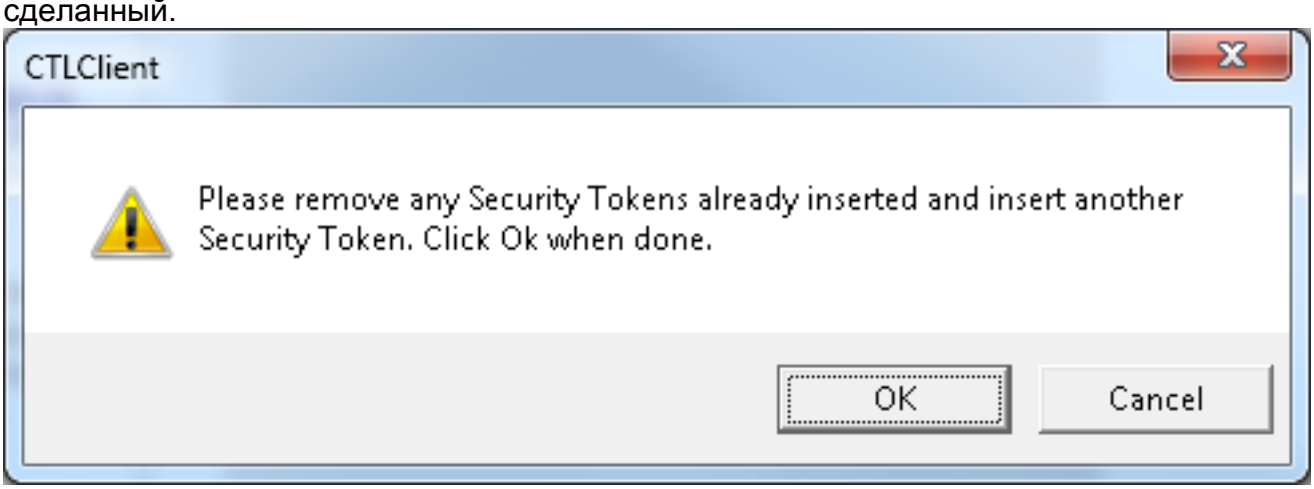


6. Изображения на экране все записи в новом CTL. **Нажмите Add Маркеры** для добавления второго маркера от новой

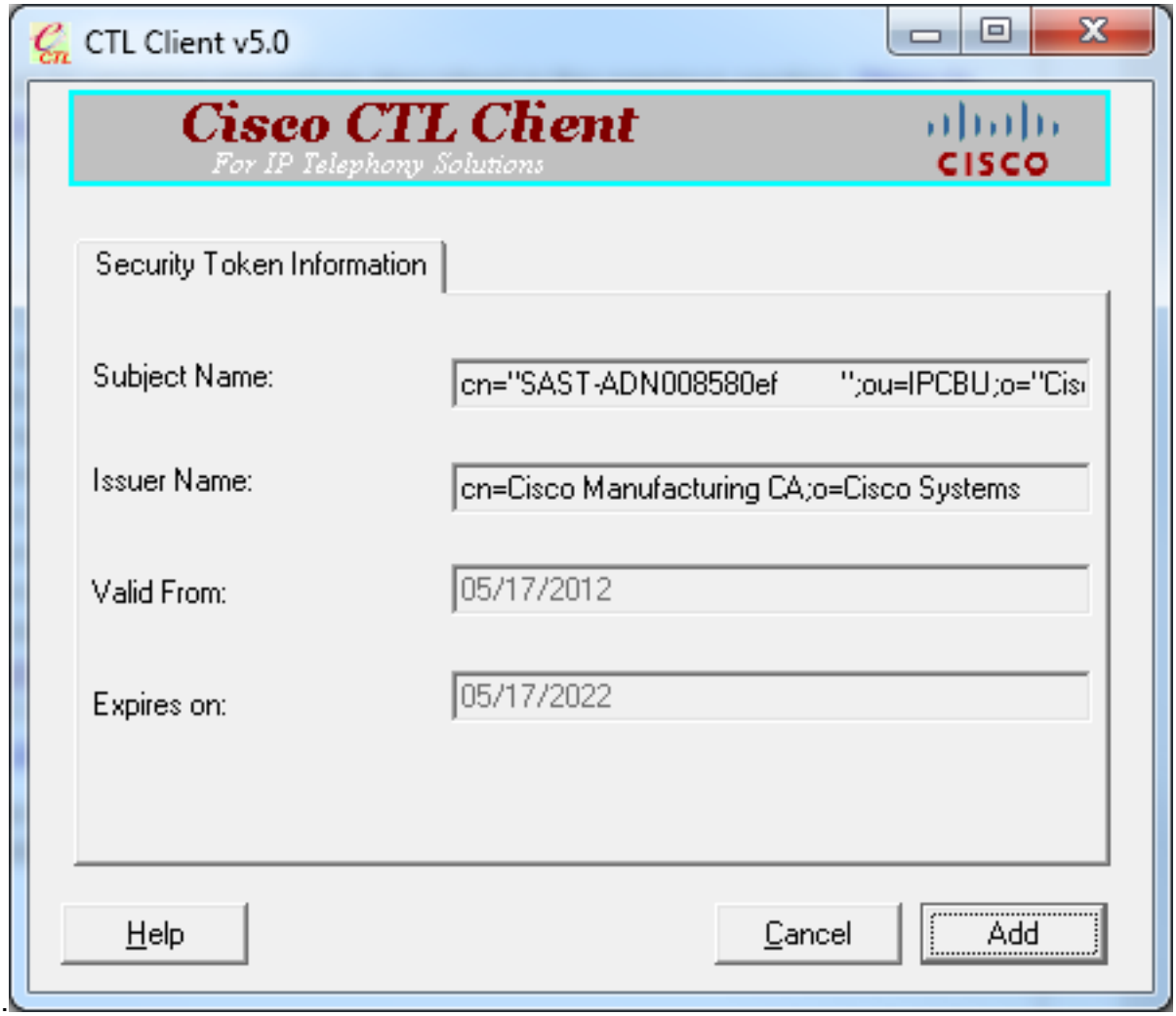


пары.

7. Вам предложат удалить текущий маркер и вставить новый. Нажмите **OK**, однажды сделанный.

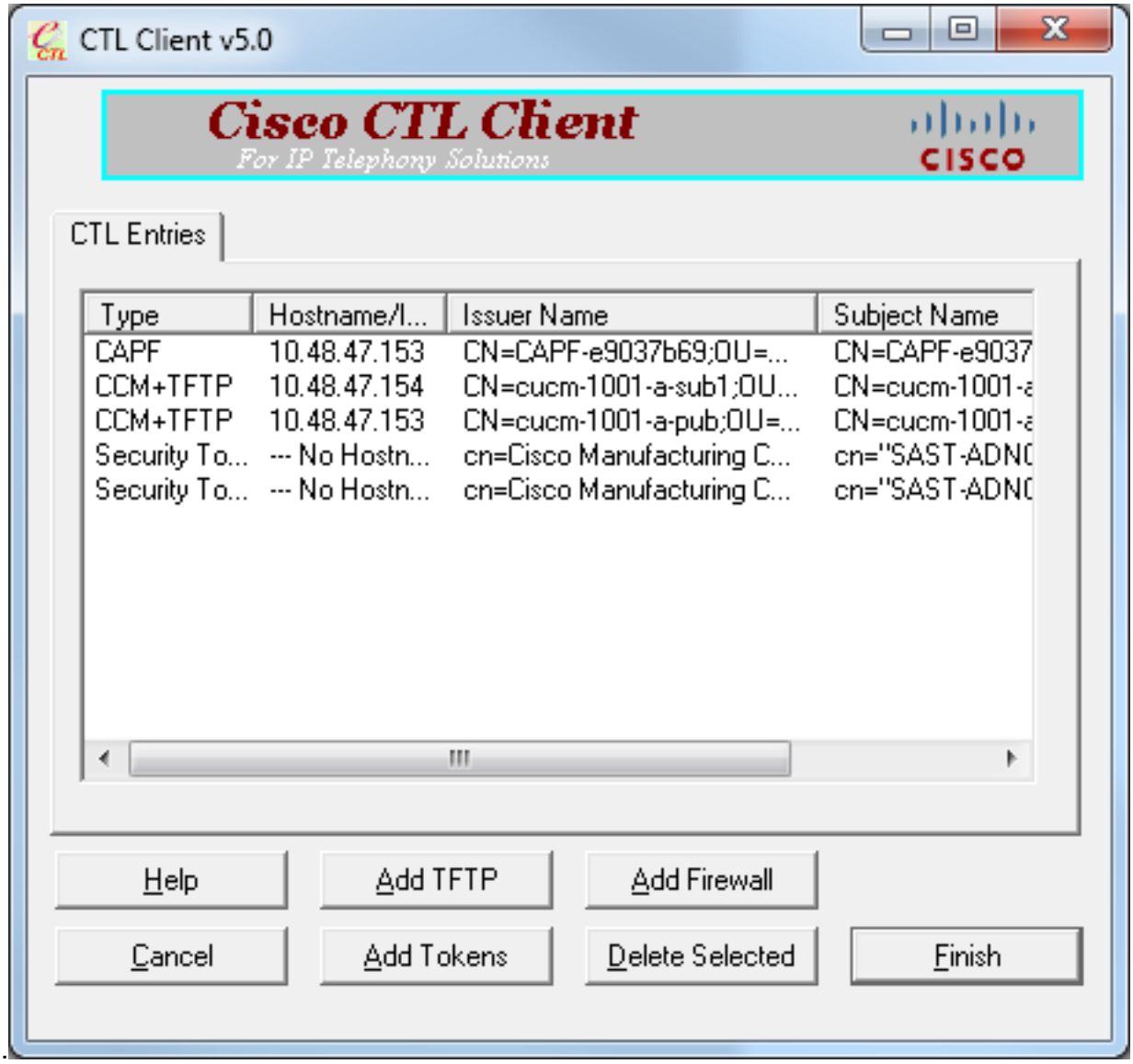


8. Отображен экран, который показывает подробные данные нового маркера. **Нажмите Add**, чтобы подтвердить их и добавить этот



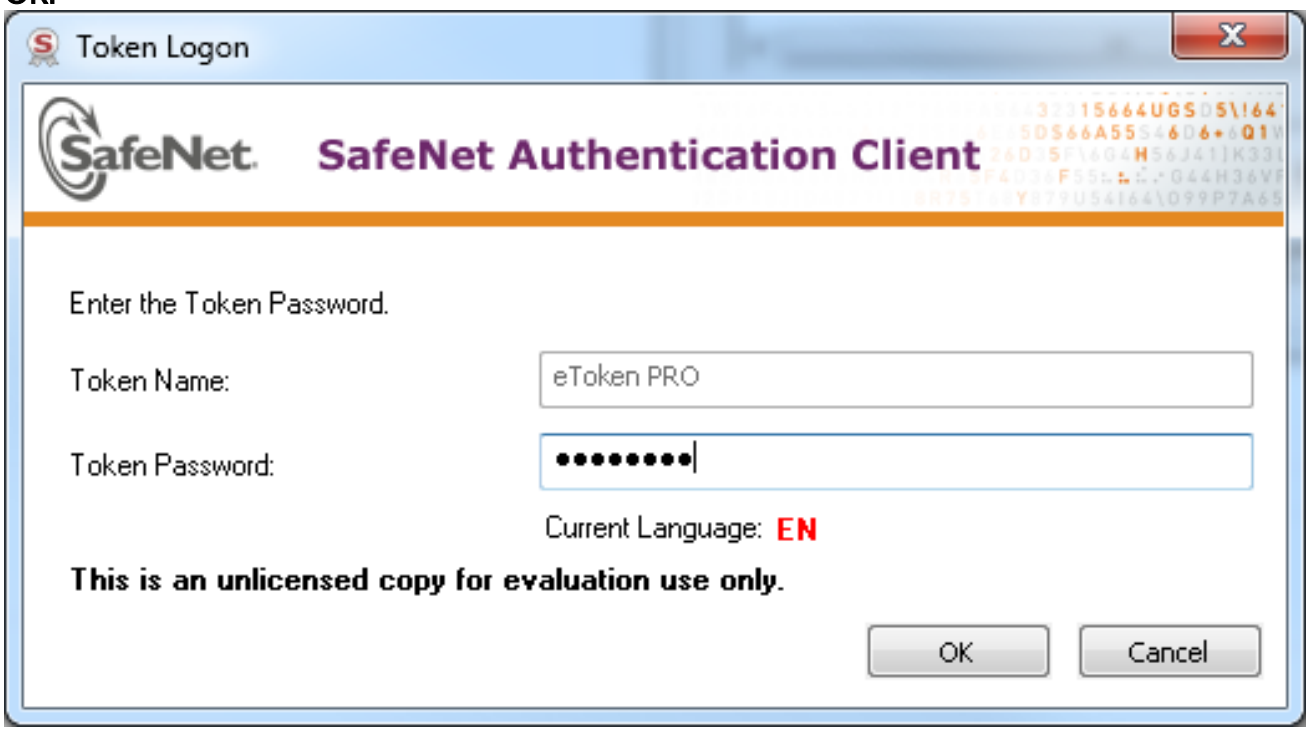
маркер.

9. Вам предоставят новый список записей CTL, которые показывают оба добавленных Маркера. Нажмите **Finish** для генерации новых файлов

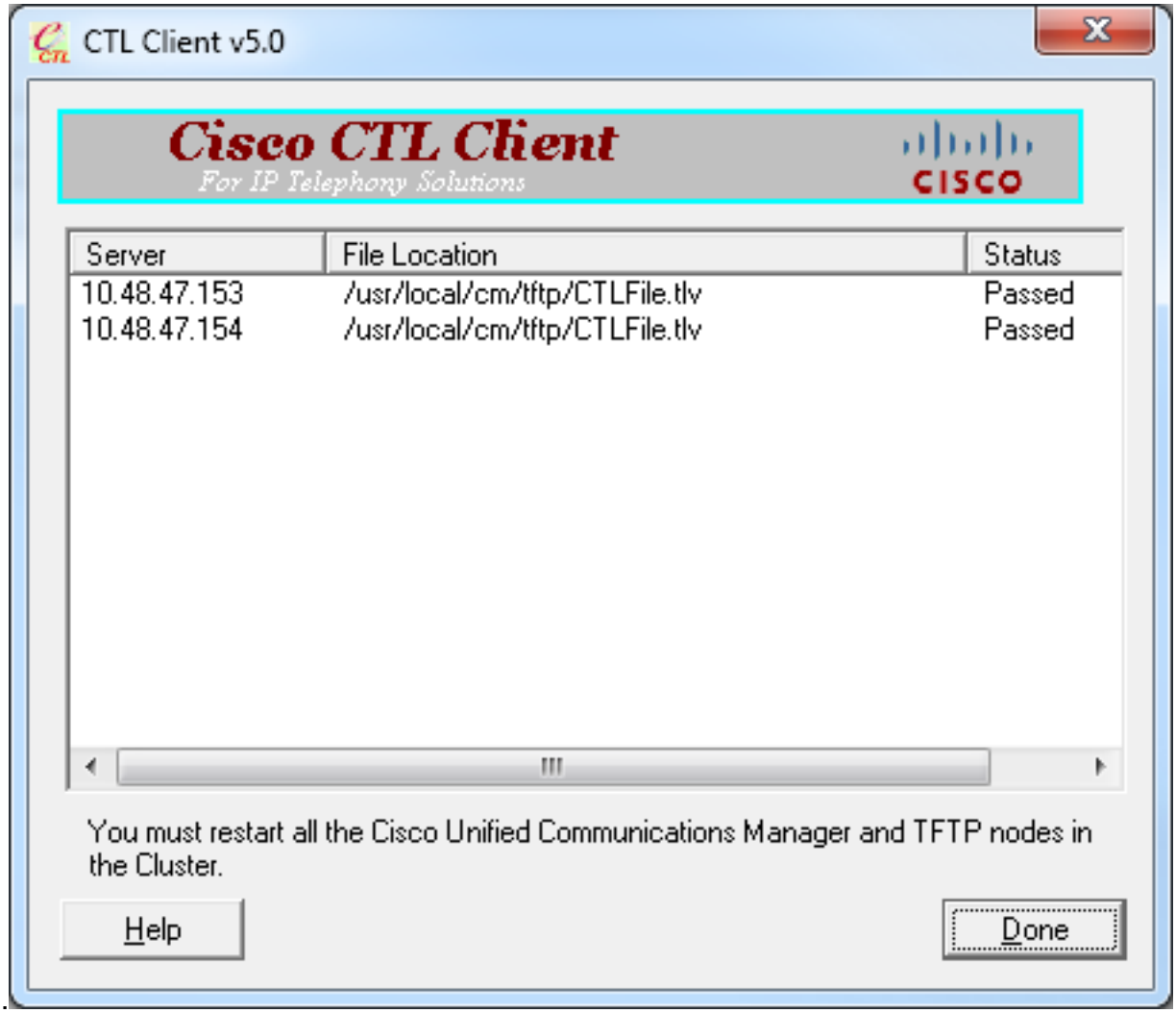


CTL.

10. В поле Token Password введите **Cisco123**. **Нажмите кнопку OK.**



11. Вы будете видеть подтверждение, что процесс был успешен. Нажмите **Done**, чтобы подтвердить и выйти из клиента



CTL.

12. Перезапустите TFTP Cisco, придерживавшийся Сервисом CallManager (Cisco Унифицированное Удобство обслуживания> Tools> Control Center - Feature Services). Новый файл CTL должен генерироваться. Введите **показ ctl** команда для проверки.

```
admin:show ctl
The checksum value of the CTL file:
68a954fba070bbcc3ff036e18716e351(MD5)
4f7a02b60bb5083baac46110f0c61eac2dceb0f7(SHA1)


Length of CTL file: 5728
The CTL File was last modified on Mon Mar 09 11:38:50 CET 2015
```

13. Удалите файл CTL из каждого телефона в кластере (эта процедура могла варьироваться на основе типа телефона - консультируйтесь с документацией для подробных данных, таких как IP-телефон Cisco Unified 8961, 9951, и 9971 Руководство по администрированию).**Примечание:** Телефоны могли бы все еще быть в состоянии зарегистрироваться (зависящий от параметров безопасности по телефону) и работать без продолжения шага 13. Однако у них будет старый файл CTL установленным. Это могло вызвать проблемы, если сертификаты восстановлены, другой сервер добавлен к кластеру, или оборудование сервера заменено. Не рекомендуется оставить кластер в этом статусе.
14. Переместите кластер в Незащищенный. Посмотрите Изменение Безопасность Кластера CUCM от Смешанного Режима до Незащищенного Режима с разделом Клиента CTL для подробных данных.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.