تم تغيير مجموعة CUCM من الوضع المختلط إلى مثال تكوين الوضع غير الآمن

المحتويات

المقدمة

يصف المستند الخطوات المطلوبة لتغيير وضع أمان Cisco Unified Communications Manager (CUCM) من الوضع المختلط إلى الوضع غير الآمن. كما تظهر كيفية تغيير محتوى ملف قائمة الشهادات الموثوق بها (CTL) عند اكتمال عملية النقل هذه.

هناك ثلاثة أجزاء رئيسية لتغيير وضع أمان CUCM:

1 أ. قم بتشغيل عميل CTL وحدد المتغير المرغوب في وضع الأمان.
1 مليا. دخلت ال CLI أمر in order to حددت ال مرغوب مختلف من أمن أسلوب.
2. إعادة تشغيل خدمات Cisco CallManager و Cisco TFTP على جميع خوادم CUCM التي تشغل هذه الخدمات.
3. قم بإعادة تشغيل كافة هواتف IP حتى تتمكن من تنزيل الإصدار المحدث من ملف CTL.

ملاحظة: إذا تم تغيير وضع أمان نظام المجموعة من الوضع المختلط إلى الوضع غير الآمن، يظل ملف CTL موجودا على الخادم (الخوادم) وعلى الهواتف، ولكن ملف CTL لا يحتوي على أية شهادات CCM+TFTP (الخادم). بما أن شهادات CCM+TFTP (الخادم) غير موجودة في ملف CTL، فإن هذا يفرض على الهاتف التسجيل على أنه غير آمن باستخدام CUCM.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من CUCM صيغة 10.0(1) أو فيما بعد. بالإضافة إلى ذلك، تأكد من:

- خدمة "موفر CTL" قيد التشغيل على كافة خوادم TFTP النشطة في نظام المجموعة. تعمل الخدمة بشكل افتراضي على منفذ TCP 2444، ولكن يمكن تعديل هذا في تكوين معلمة خدمة CUCM.
- خدمات "وظيفة وكيل المرجع المصدق" (CAPF) قيد التشغيل على عقدة Publisher.
- يعمل النسخ المتماثل لقاعدة البيانات (DB) في نظام المجموعة بشكل صحيح، كما تقوم الخوادم بنسخ البيانات في الوقت الفعلي.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- مجموعة الإصدار 10.0.1.11900-2 من عقدتين
- هاتف بروتوكول الإنترنت Cisco 7975 IP Phone (مسجل مع بروتوكول التحكم في المكالمات Skinny Call Control Protocol (SCCP)، إصدار البرنامج الثابت SCCP75.9-3-1SR3-1S)
- يلزم وجود علامتي أمان من Cisco لتعيين نظام المجموعة على الوضع المختلط
- من الضروري وجود إحدى رموز الأمان المدرجة سابقا لتعيين نظام المجموعة على الوضع غير الآمن

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

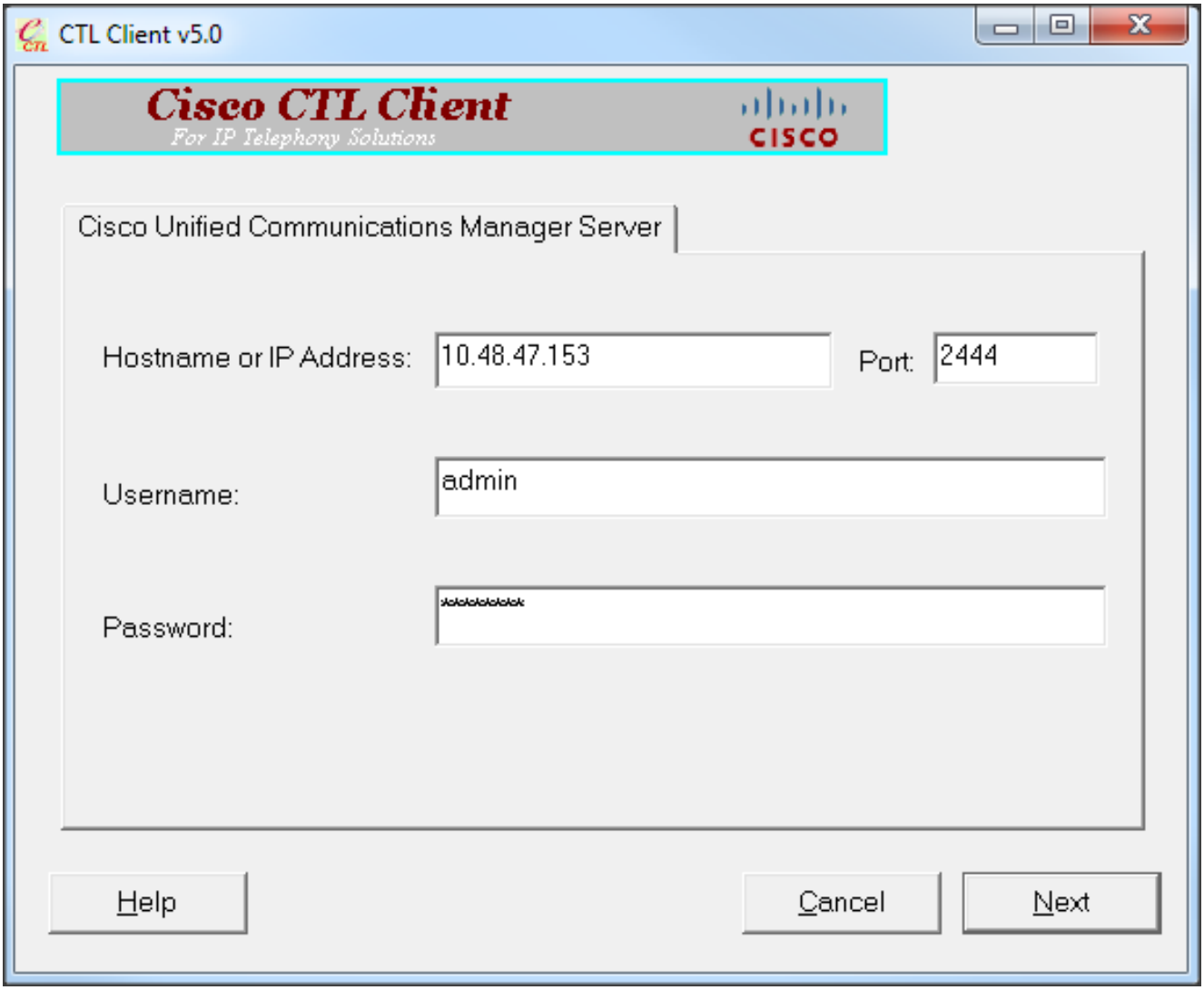
لتشغيل المكون الإضافي لعميل CTL، يلزم توفر وصول إلى رمز أمان واحد على الأقل تم إدخاله لإنشاء أحدث ملف CTL أو تحديثه على خادم CUCM Publisher. بمعنى آخر، يجب أن تكون شهادة واحدة على الأقل من شهادات eToken الموجودة في ملف CTL الحالي على CUCM على الرمز المميز للأمان الذي يتم إستخدامه لتغيير وضع الأمان.

التكوين

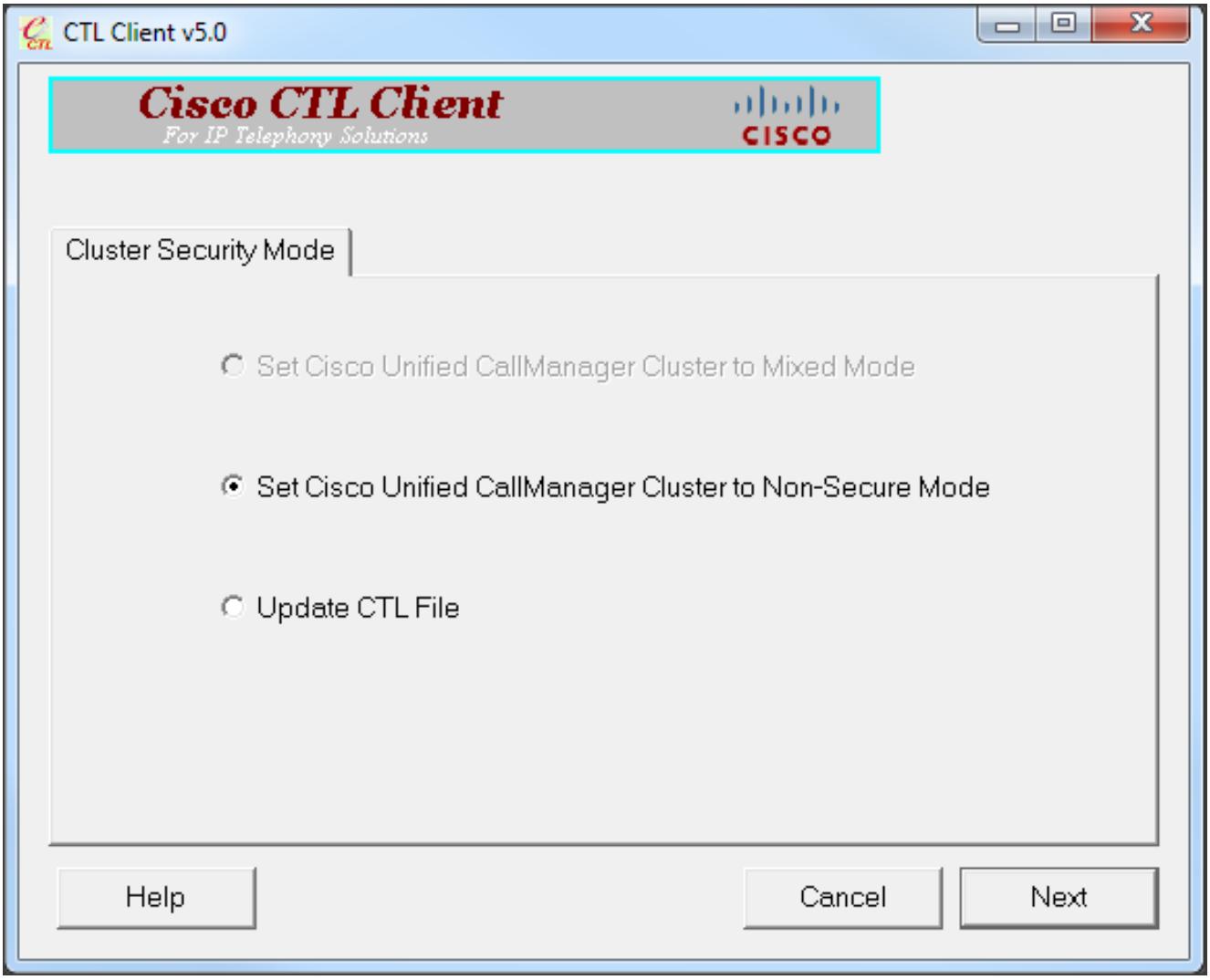
تغيير أمان مجموعة CUCM من الوضع المختلط إلى الوضع غير الآمن باستخدام عميل CTL

أكمل الخطوات التالية لتغيير أمان مجموعة CUCM من الوضع المختلط إلى الوضع غير الآمن باستخدام عميل CTL:

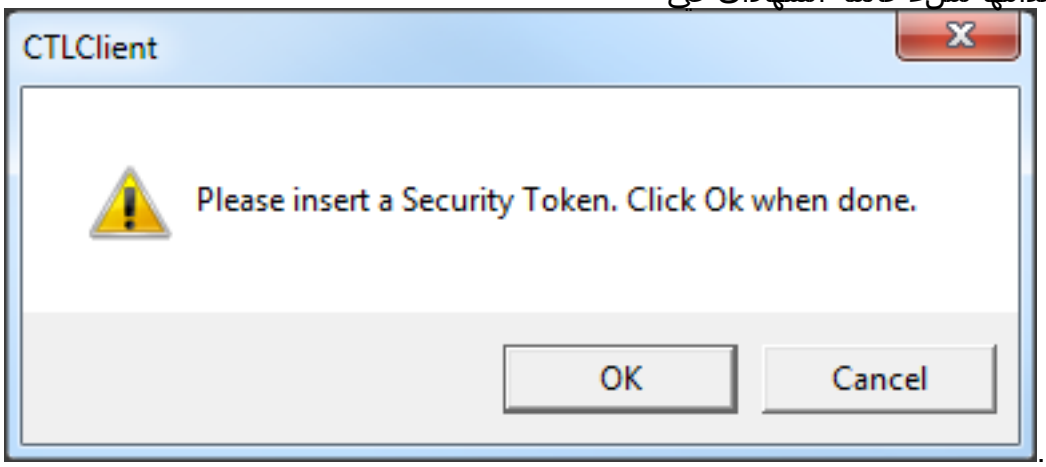
1. احصل على رمز أمان واحد قمت بإدراجه لتكوين أحدث ملف CTL.
2. قم بتشغيل عميل CTL. قم بتوفير اسم/عنوان IP الخاص ب CUCM PUB وبيانات اعتماد مسؤول CCM. انقر فوق **Next (التالي)**.



3. انقر على الزر **تعيين مجموعة Cisco Unified CallManager على** لاسلكي **وضع غير آمن**. انقر فوق **Next (التالي)**.

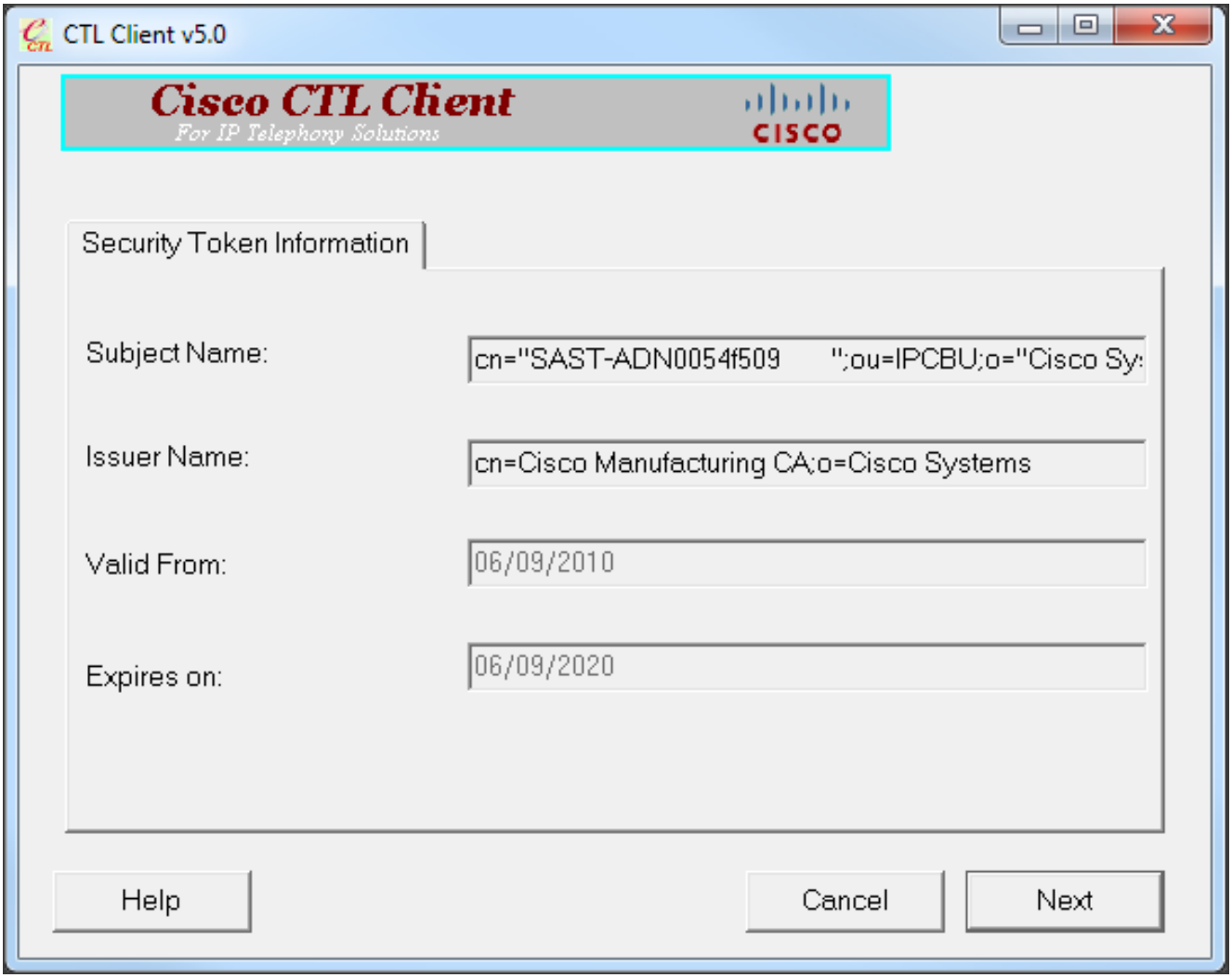


4. قم بإدراج رمز مميز واحد للأمان تم إدراجه لتكوين أحدث ملف CTL وانقر فوق **موافق**. هذا أحد الرموز المميزة التي تم إستخدامها لملء قائمة الشهادات في

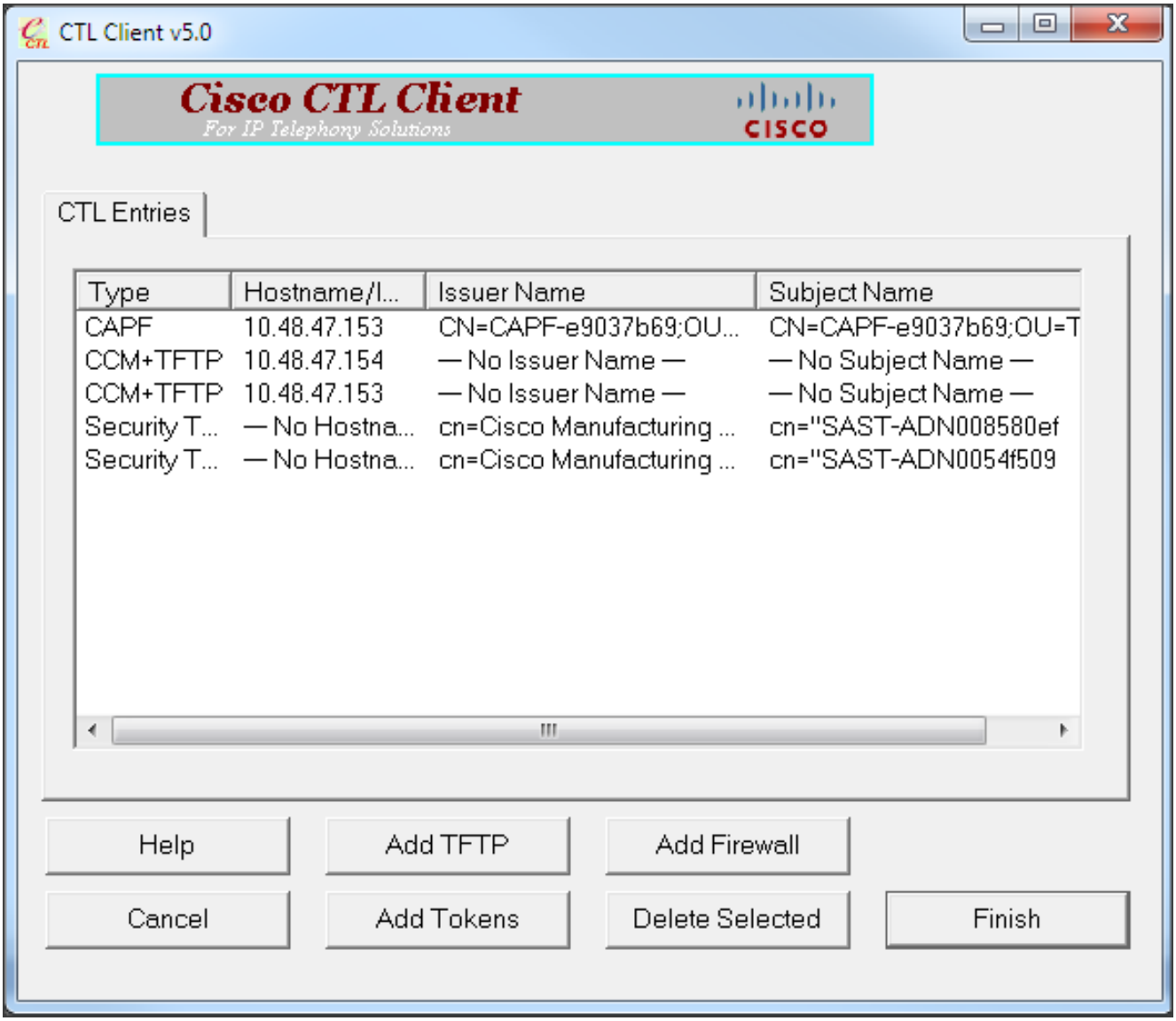


.CTLFile.tlv

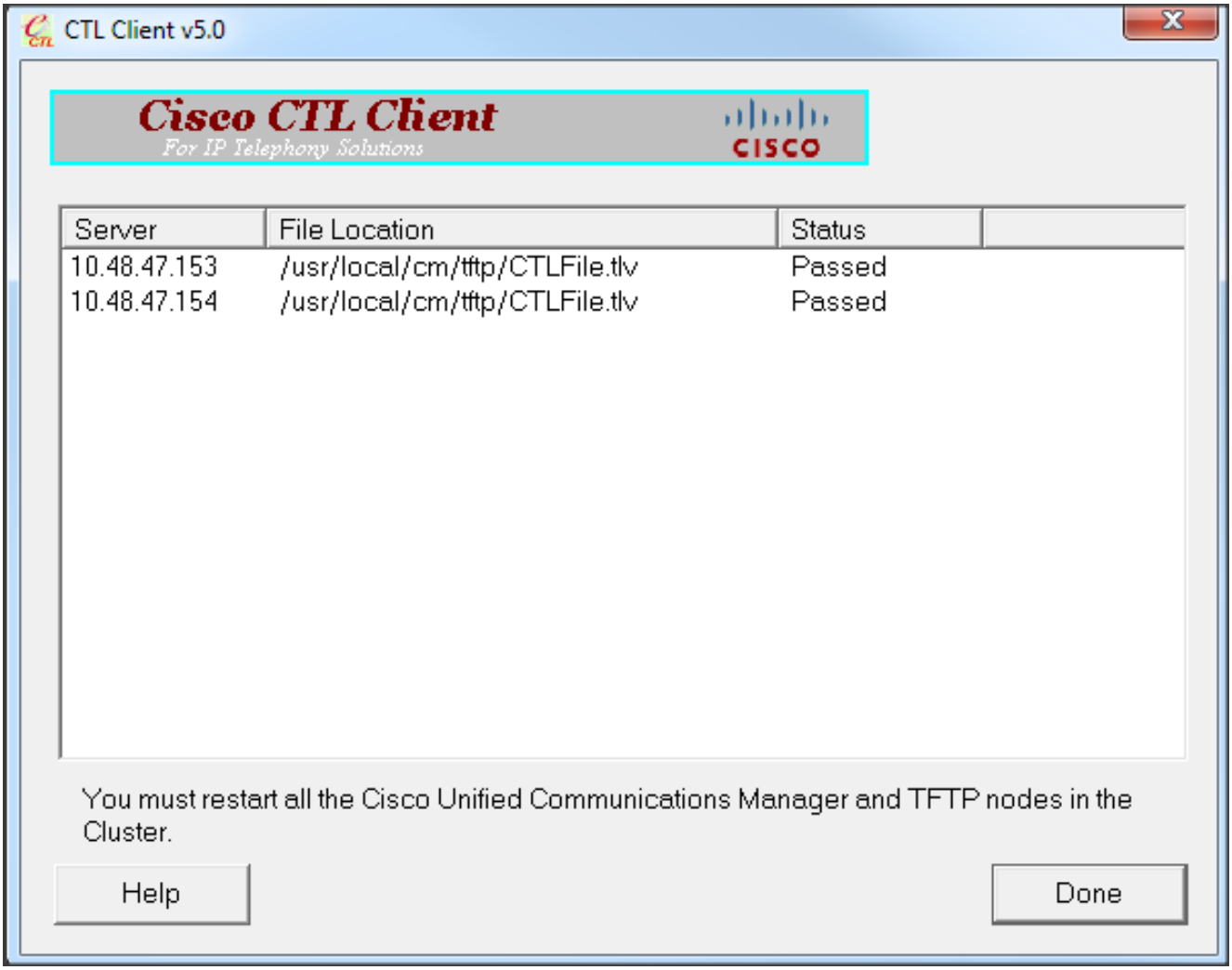
5. يتم عرض تفاصيل الرمز المميز للأمان. انقر فوق **Next (التالي)**.



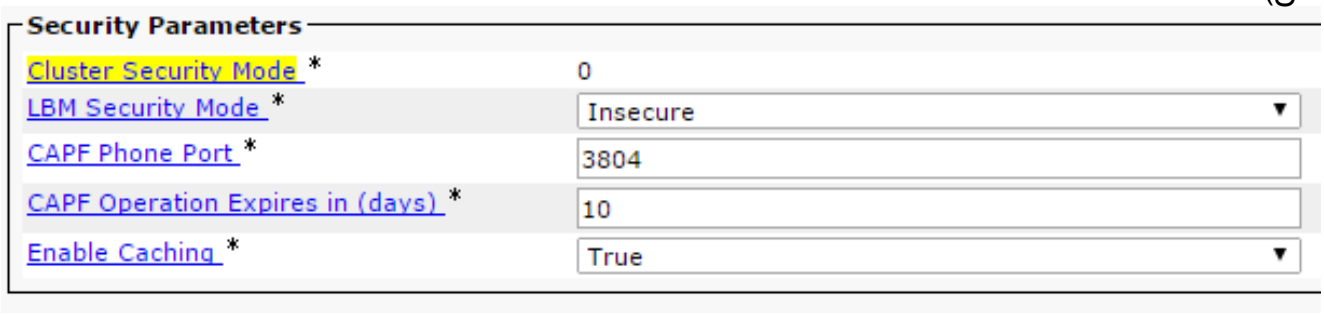
6. يتم عرض محتوى ملف CTL. انقر فوق **إنهاء**. عندما يطلب منك كلمة المرور، دخلت **Cisco123**.



7. يتم عرض قائمة خوادم CUCM الموجودة عليها ملف CTL. طقطقة **تم**.



8. أختر **صفحة إدارة System > CUCM > معلمات Enterprise** وتحقق من تعيين نظام المجموعة على الوضع غير الآمن ("0" يشير إلى غير آمن).



9. قم بإعادة تشغيل خدمات TFTP و Cisco CallManager على جميع العقد في نظام المجموعة التي تقوم بتشغيل هذه الخدمات.
10. قم بإعادة تشغيل جميع هواتف IP حتى تتمكن من الحصول على الإصدار الجديد من ملف CTL من CUCM TFTP.

تغيير أمان مجموعة CUCM من الوضع المختلط إلى الوضع غير الآمن باستخدام CLI (واجهة سطر الأوامر)

هذا التكوين خاص فقط ب CUCM الإصدار x.10 والإصدارات الأحدث. من أجل تعيين وضع أمان نظام المجموعة CUCM على غير آمن، أدخل الأمر **utils set-cluster non-secure-mode** على واجهة سطر الأوامر (CLI) الخاصة

ب Publisher. بعد اكتمال هذا الإجراء، قم بإعادة تشغيل خدمات TFTP و Cisco CallManager على جميع العقد في نظام المجموعة التي تقوم بتشغيل هذه الخدمات.

وفيما يلي نموذج إخراج واجهة سطر الأوامر (CLI) الذي يظهر إستخدام الأمر.

```
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
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

للتحقق من CTLFIle.tlv، يمكنك إستخدام إحدى الطريقتين:

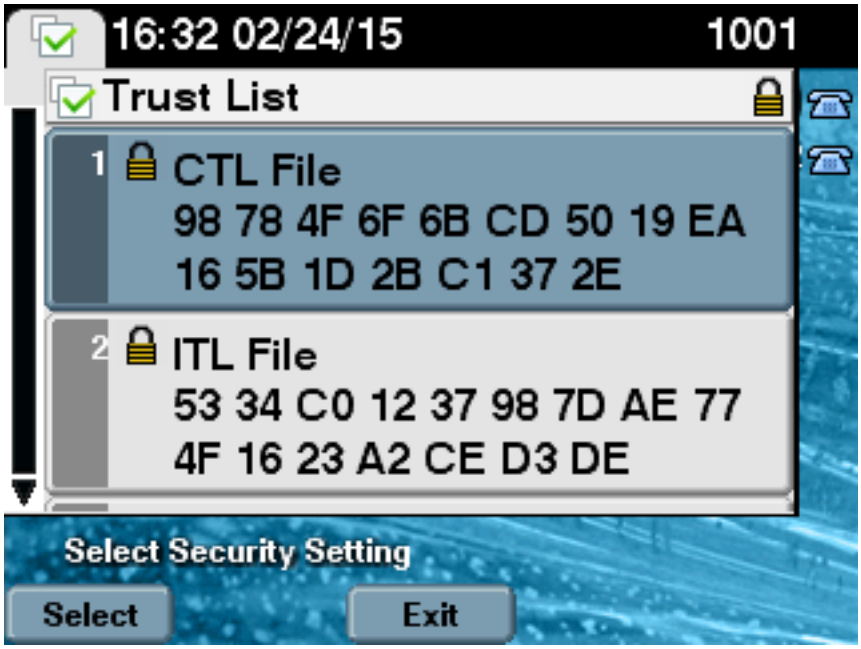
- للتحقق من المحتوى والجملة الاختبارية MD5 الخاصة ب CTLFIle.tlv الموجودة على جانب CUCM TFTP، أدخل الأمر **show ctl** على واجهة سطر الأوامر (CLI) الخاصة ب CUCM. يجب أن يكون ملف CTLFIle.tlv هو نفسه في جميع عقد CUCM.
- للتحقق من المجموع الاختباري MD5 على هاتف IP 7975، أختر **الإعدادات > تكوين الأمان > قائمة الثقة > ملف CTL**.

ملاحظة: عند التحقق من المجموع الاختباري عبر الهاتف، سترى MD5 أو SHA1، معتمدا على نوع الهاتف.

مجموعة CUCM إلى وضع الأمان - المجموع الاختباري لملف CTL

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

على جانب هاتف IP، يمكنك أن ترى أنه يحتوي على نفس ملف CTL المثبت (يطابق المجموع الاختباري MD5 عند مقارنته بمخرجات CUCM).



مجموعة CUCM إلى الوضع غير الآمن - محتوى ملف CTL

فيما يلي مثال على ملف CTL من مجموعة CUCM تم تعيينها إلى الوضع غير الآمن. يمكنك أن ترى أن شهادات CCM+TFTP فارغة ولا تحتوي على أي محتوى. لا يتم تغيير بقية الشهادات الموجودة في ملفات CTL وهي تماما نفسها كما هو الحال عندما تم تعيين CUCM إلى الوضع المختلط.

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

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
FILENAME 12 14
TIMESTAMP 4 15

CTL Record #:1

BYTEPOS TAG LENGTH VALUE
----- ------ --- -------
RECORDLENGTH 2 1186 1
DNSNAME 1 2
SUBJECTNAME 56 cn="SAST-ADN0054f509 ";ou=IPCBU;o="Cisco Systems 3
FUNCTION 2 System Administrator Security Token 4
ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems 5
SERIALNUMBER 10 3C:F9:27:00:00:00:AF:A2:DA:45 6
PUBLICKEY 140 7
(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 9
IPADDRESS 4 10
.This etoken was used to sign the CTL file

CTL Record #:2

BYTEPOS TAG LENGTH VALUE
----- ------ --- -------
RECORDLENGTH 2 1186 1
DNSNAME 1 2
SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems 3
FUNCTION 2 System Administrator Security Token 4
ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems 5
SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31 6
PUBLICKEY 140 7
(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 9
IPADDRESS 4 10
.This etoken was not used to sign the CTL file

CTL Record #:3

BYTEPOS TAG LENGTH VALUE
----- ------ --- -------
RECORDLENGTH 2 33 1
DNSNAME 13 **10.48.47.153** 2
FUNCTION 2 **CCM+TFTP** 4
IPADDRESS 4 10

CTL Record #:4

BYTEPOS TAG LENGTH VALUE
----- ------ --- -------
RECORDLENGTH 2 1004 1
DNSNAME 13 10.48.47.153 2
SUBJECTNAME 60 CN=CAPF-e9037b69;OU=TAC;O=Cisco;L=Krakow;ST=Malopolska;C=PL 3
FUNCTION 2 CAPF 4
ISSUERNAME 60 CN=CAPF-e9037b69;OU=TAC;O=Cisco;L=Krakow;ST=Malopolska;C=PL 5
SERIALNUMBER 16 79:59:16:C1:54:AF:31:0C:0F:AE:EA:97:2E:08:1B:31 6
PUBLICKEY 140 7
(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 9

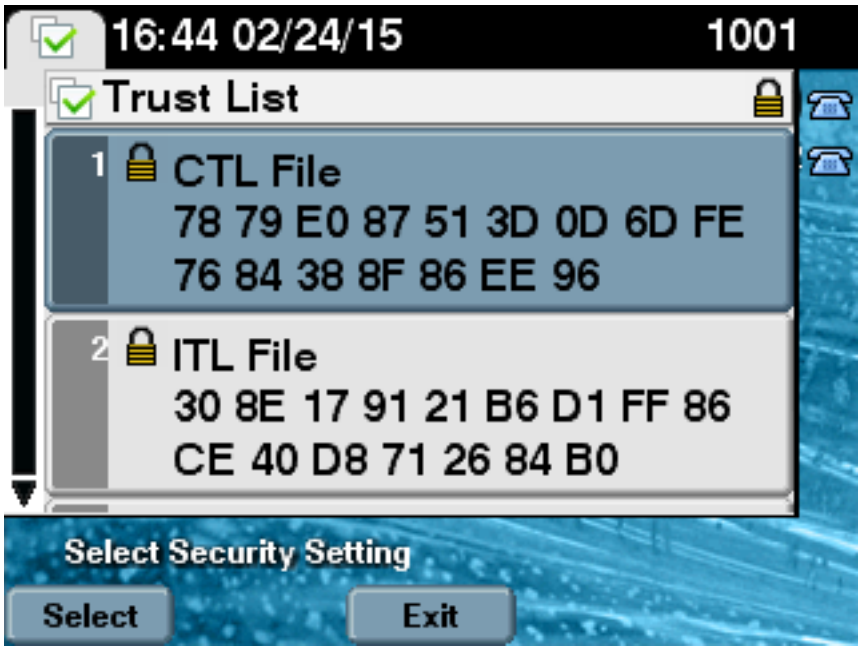
```
                                                IPADDRESS 4 10

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

                                            .The CTL file was verified successfully

                                            :admin
```

على جانب هاتف IP، بعد إعادة تشغيله وتنزيله إصدار ملف CTL المحدث، يمكنك أن ترى أن المجموع الاختباري MD5 يتطابق عند مقارنته بخرج CUCM.



ضع أمان مجموعة CUCM من الوضع المختلط إلى الوضع غير الآمن عند فقد رموز USB المميزة

قد تفقد رموز الأمان المميزة للمجموعات الآمنة. في تلك الحالة، عليك أن تفكر في هذين السيناريوهين:

- يقوم نظام المجموعة بتشغيل الإصدار 10.0.1 أو إصدار أحدث
- يقوم نظام المجموعة بتشغيل إصدار أقدم من x.10

في السيناريو الأول، أكمل الإجراء الموضح في تغيير أمان مجموعة CUCM من الوضع المختلط إلى الوضع غير الآمن باستخدام قسم واجهة سطر الأوامر (CLI) من أجل التعافي من المشكلة. بما أن أمر واجهة سطر الأوامر (CLI) لا يتطلب رمز CTL المميز، فيمكن إستخدامه حتى إذا تم وضع نظام المجموعة في الوضع المختلط مع عميل CTL.

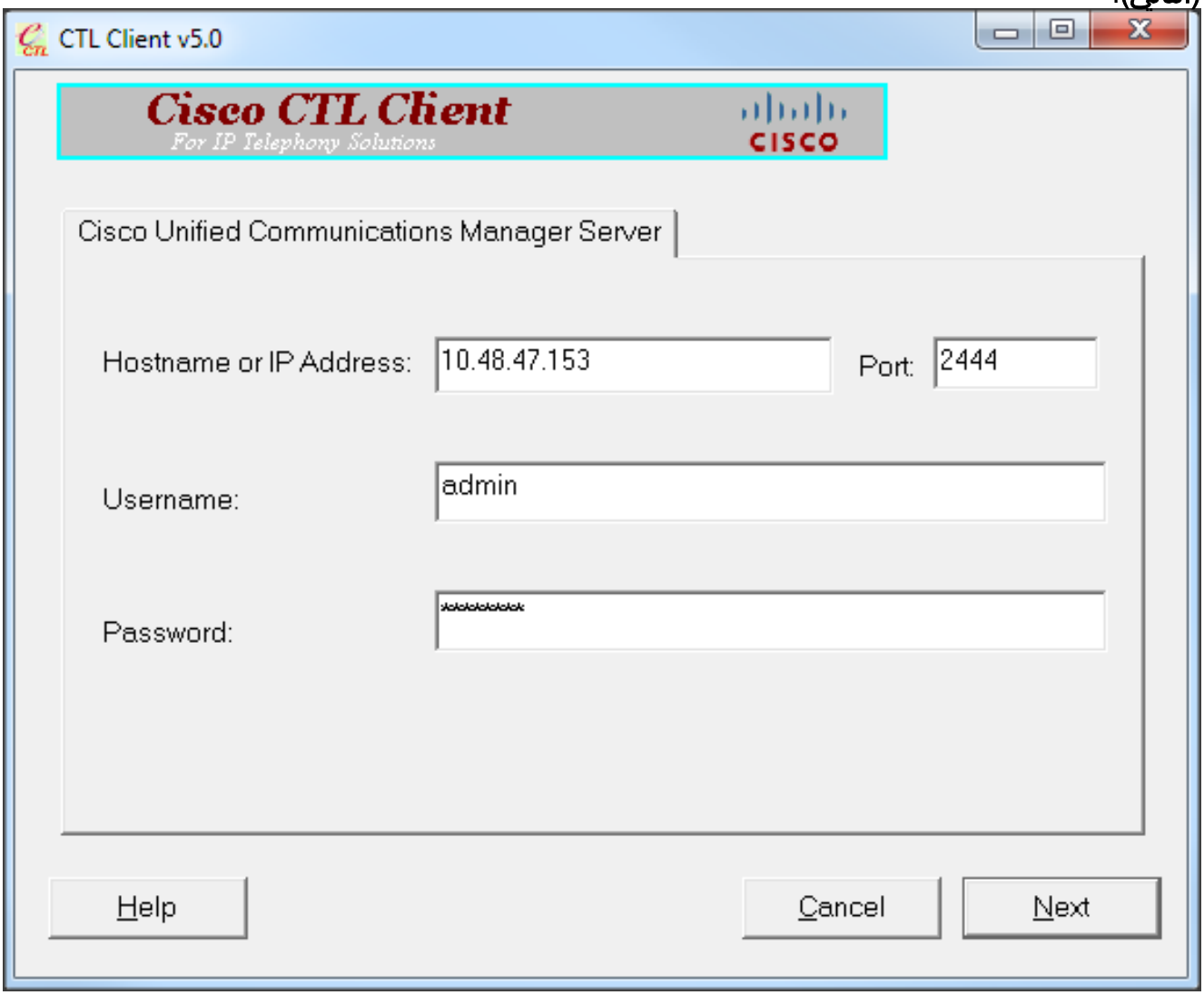
ويصبح الوضع أكثر تعقيدا عندما يكون إصدار أقدم من x.10 من CUCM قيد الاستخدام. إذا فقدت أو نسيت كلمة مرور أحد الرموز المميزة، لا يزال بإمكانك إستخدام الكلمة الأخرى لتشغيل عميل CTL مع ملفات CTL الحالية. يوصى بشدة بالحصول على رمز مميز آخر وإضافته إلى ملف CTL في أقرب وقت ممكن من أجل التكرار. إذا فقدت أو نسيت كلمات المرور الخاصة بجميع الرموز المميزة المدرجة في ملف CTL الخاص بك، فإنك بحاجة إلى الحصول على زوج جديد من الرموز الإلكترونية وتشغيل إجراء يدوي كما هو موضح هنا.

1. أدخل الأمر **file delete tftp ctlfile.tlv** لحذف ملف CTL من جميع خوادم TFTP.

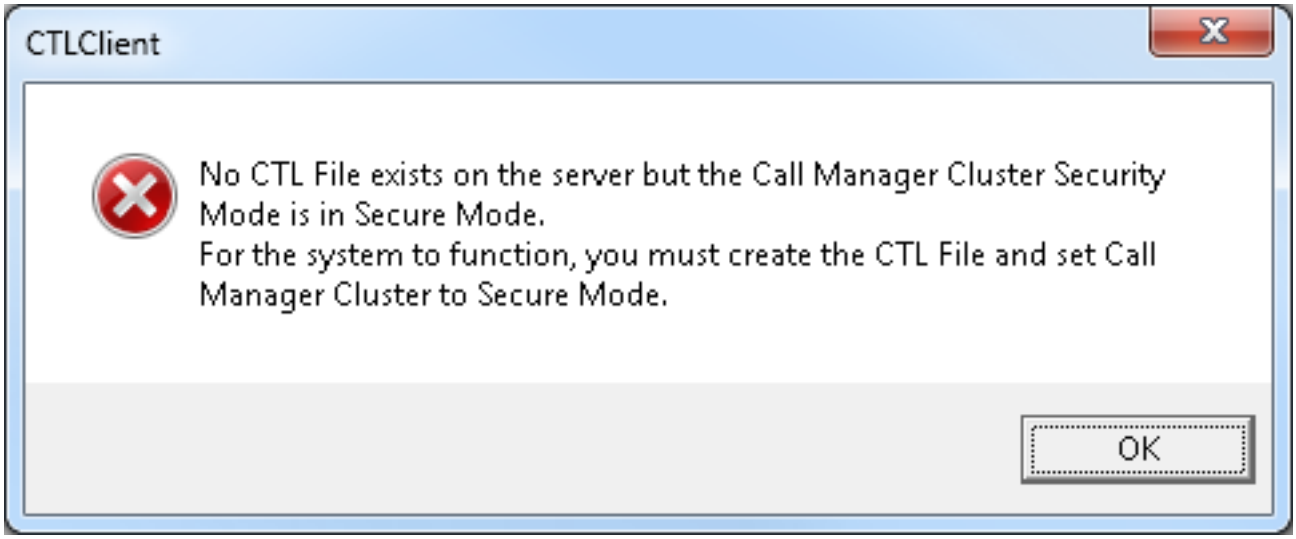
```
admin:file delete tftp CTLFile.tlv
     ?Delete the File CTLFile.tlv
Enter "y" followed by return to continue: y
     files: found = 1, deleted = 1

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
```

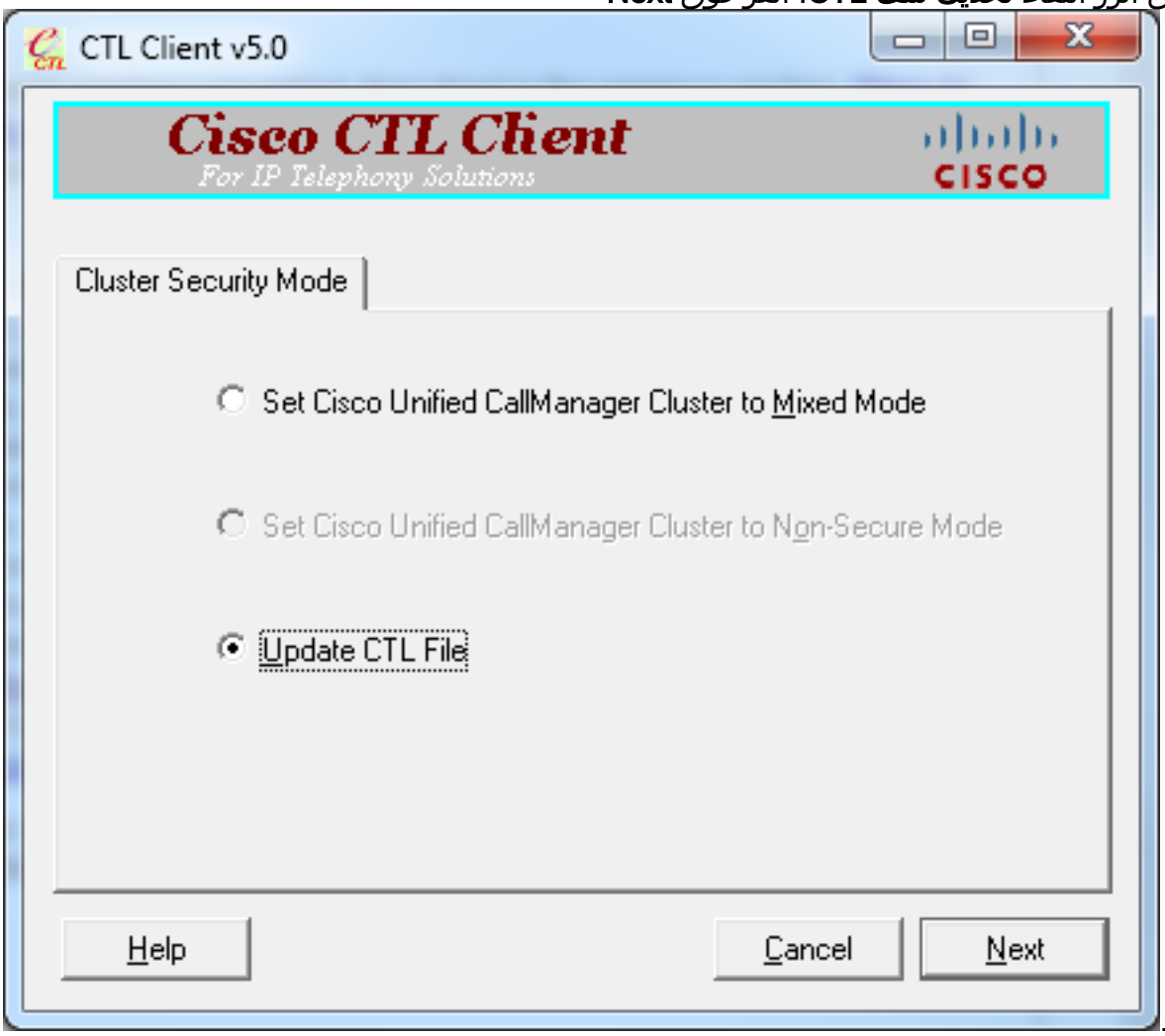
2. قم بتشغيل عميل CTL. دخلت ال ip hostname/address من ال CUCM PUB وال CCM مسؤول ورقة اعتماد. انقر فوق **Next** (التالي).



3. بما أن نظام المجموعة في الوضع المختلط، إلا أنه لا يوجد ملف CTL على Publisher، يتم عرض هذا التحذير. طقطقة in order to **ok** تجاهلت هو ومضت قدما.

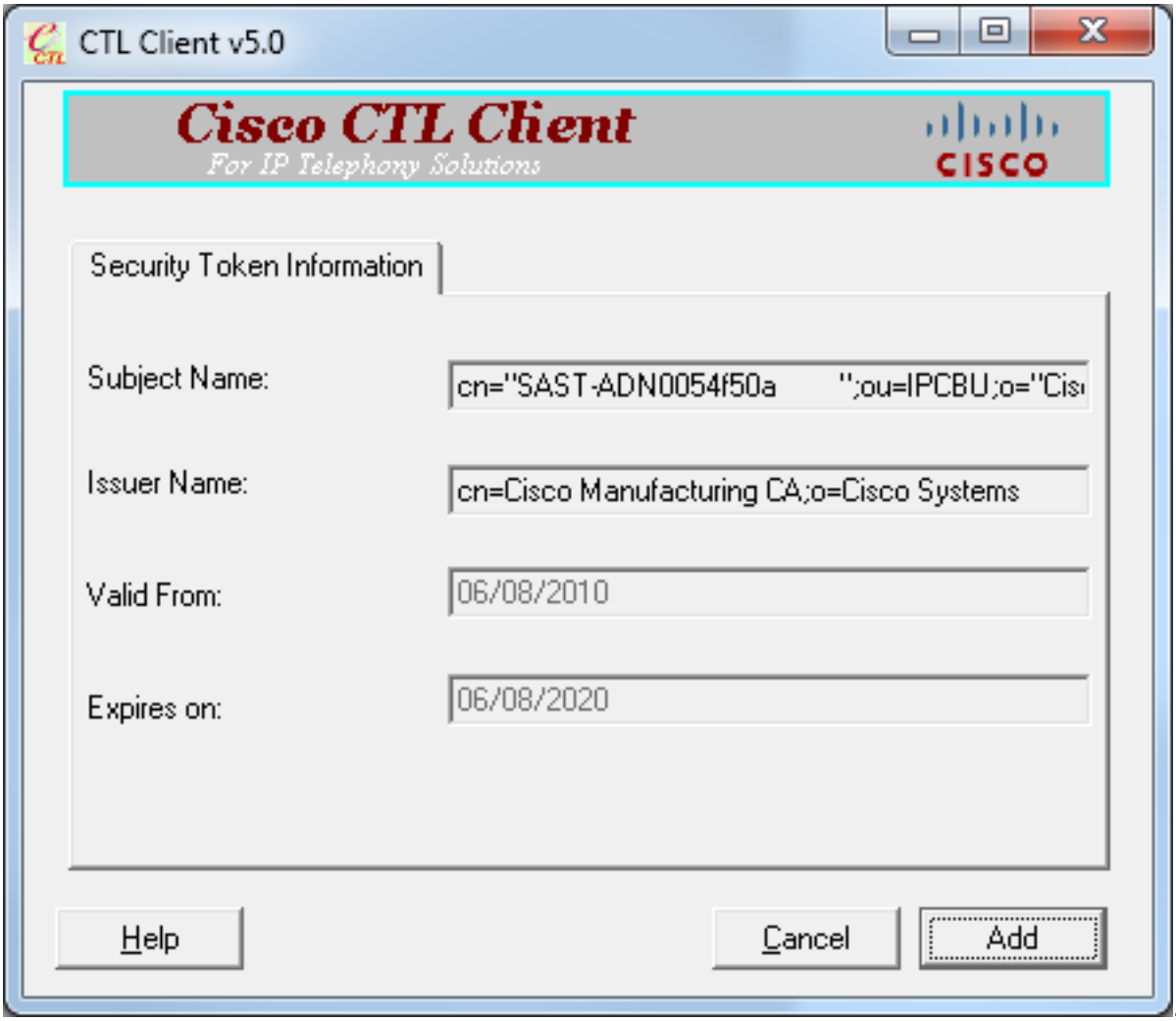


4. انقر فوق الزر انتقاء **تحديث ملف CTL**. انقر فوق **Next**



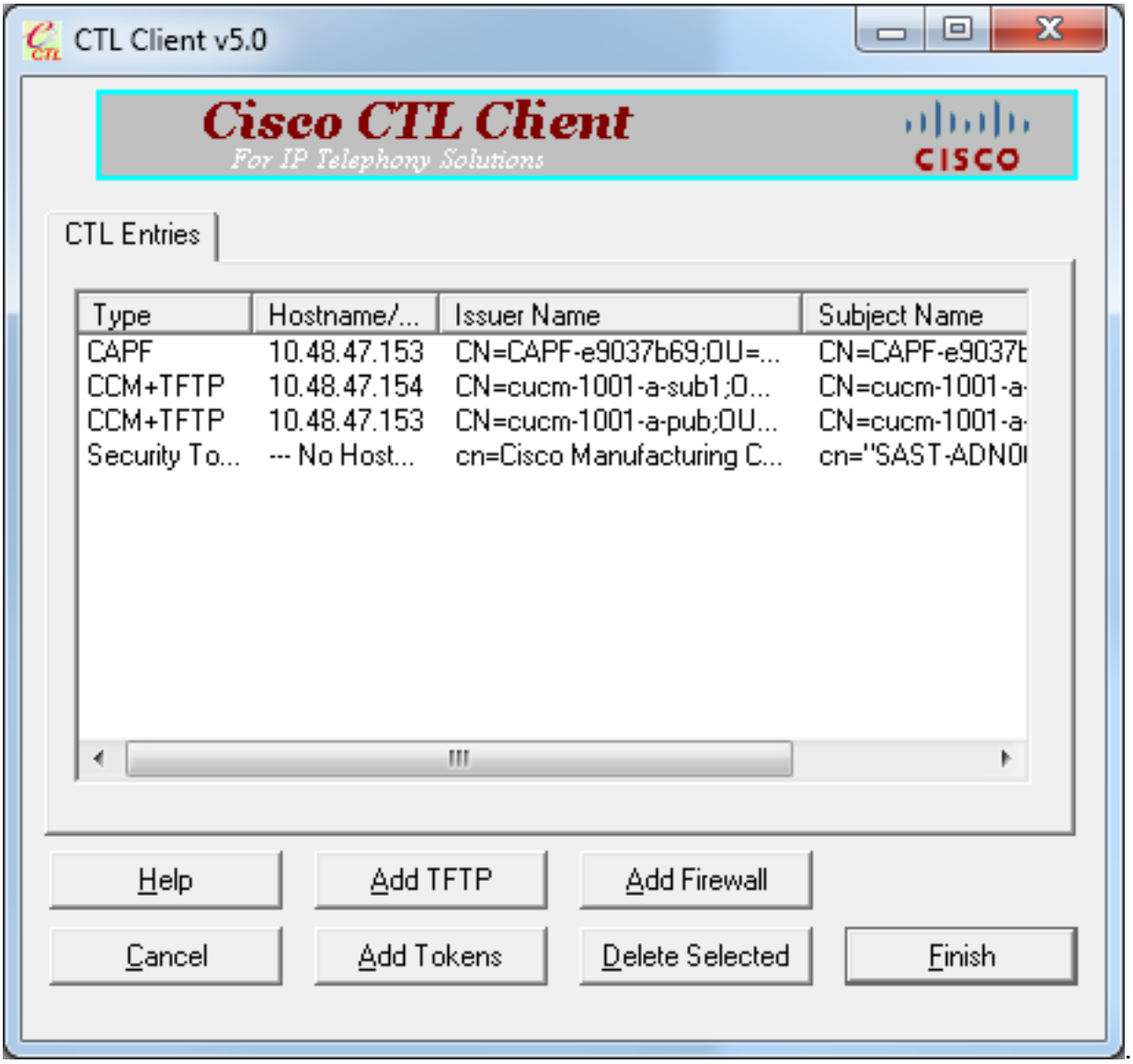
(التالي).

5. يطلب عميل CTL إضافة رمز مميز للأمان. طقطقة **يضيف** in order to



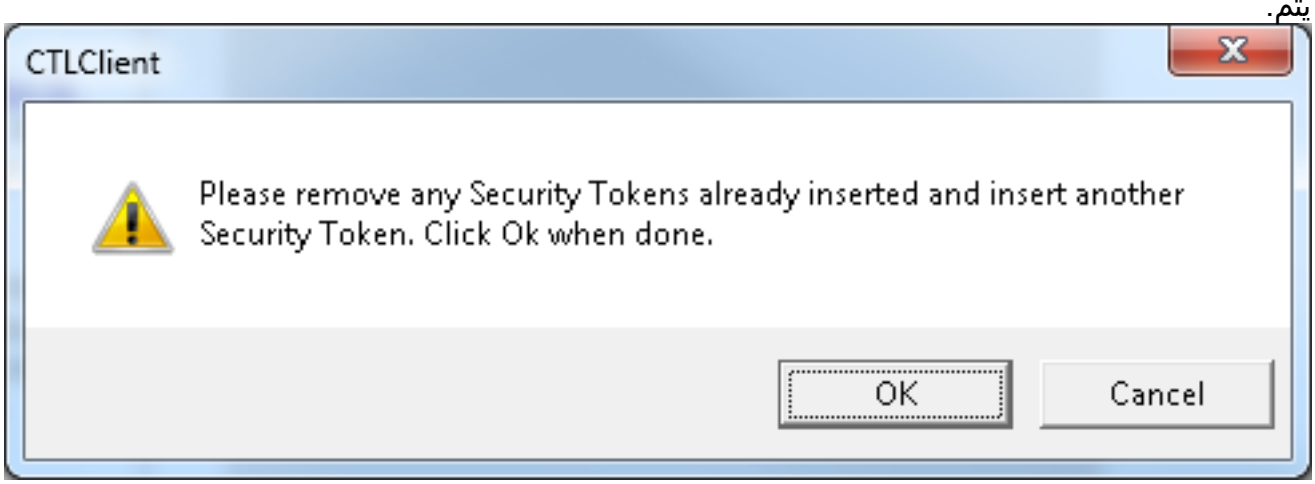
باشرت.

6. تعرض الشاشة كافة الإدخالات في CTL الجديد. انقر فوق **إضافة العلامات المميزة** لإضافة الرمز المميز الثاني من الزوج

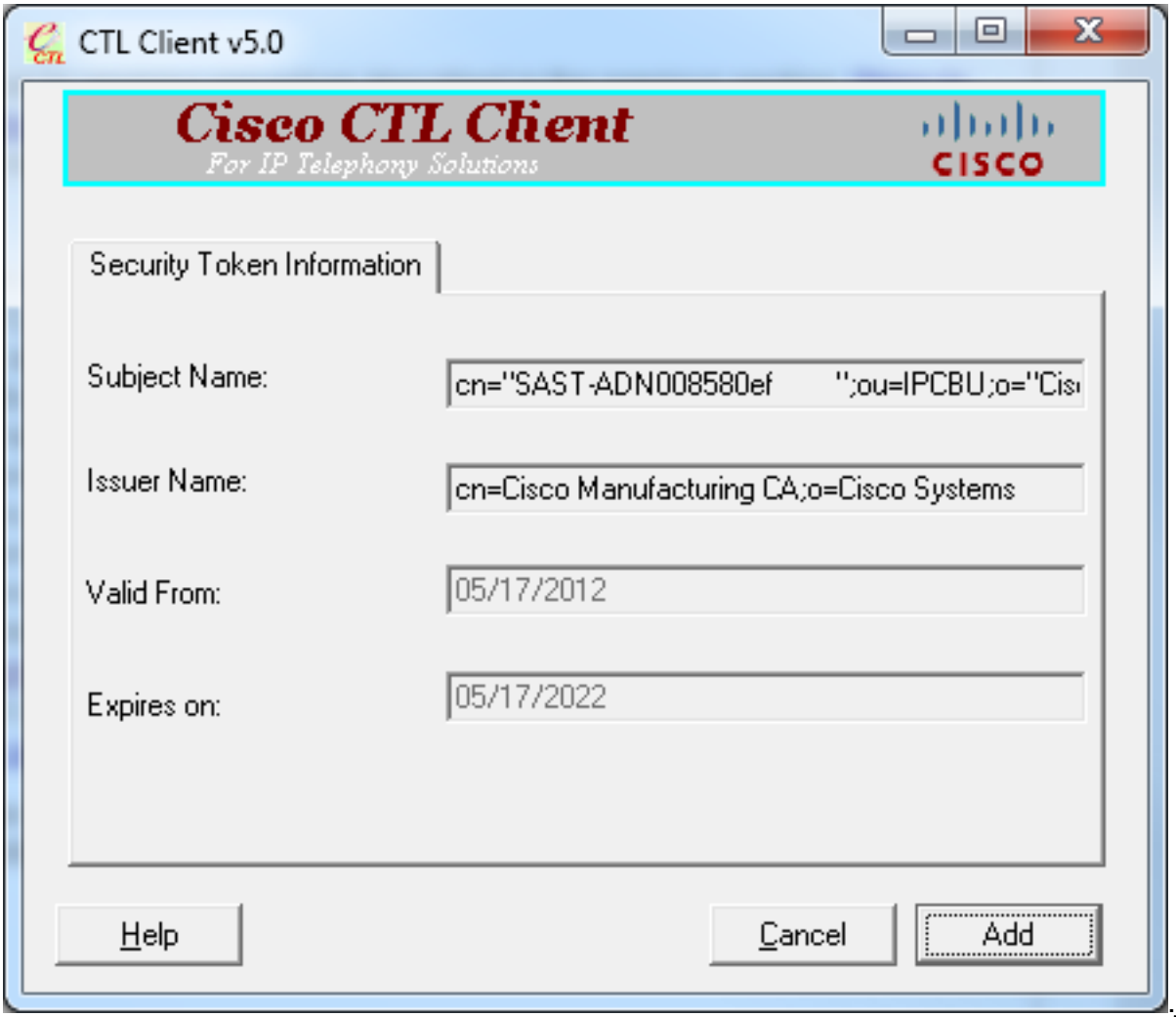


الجديد.

7. ستتم مطالبتك بإزالة الرمز المميز الحالي وإدخال رمز مميز جديد. طقطقة **ok** ما إن يتم.

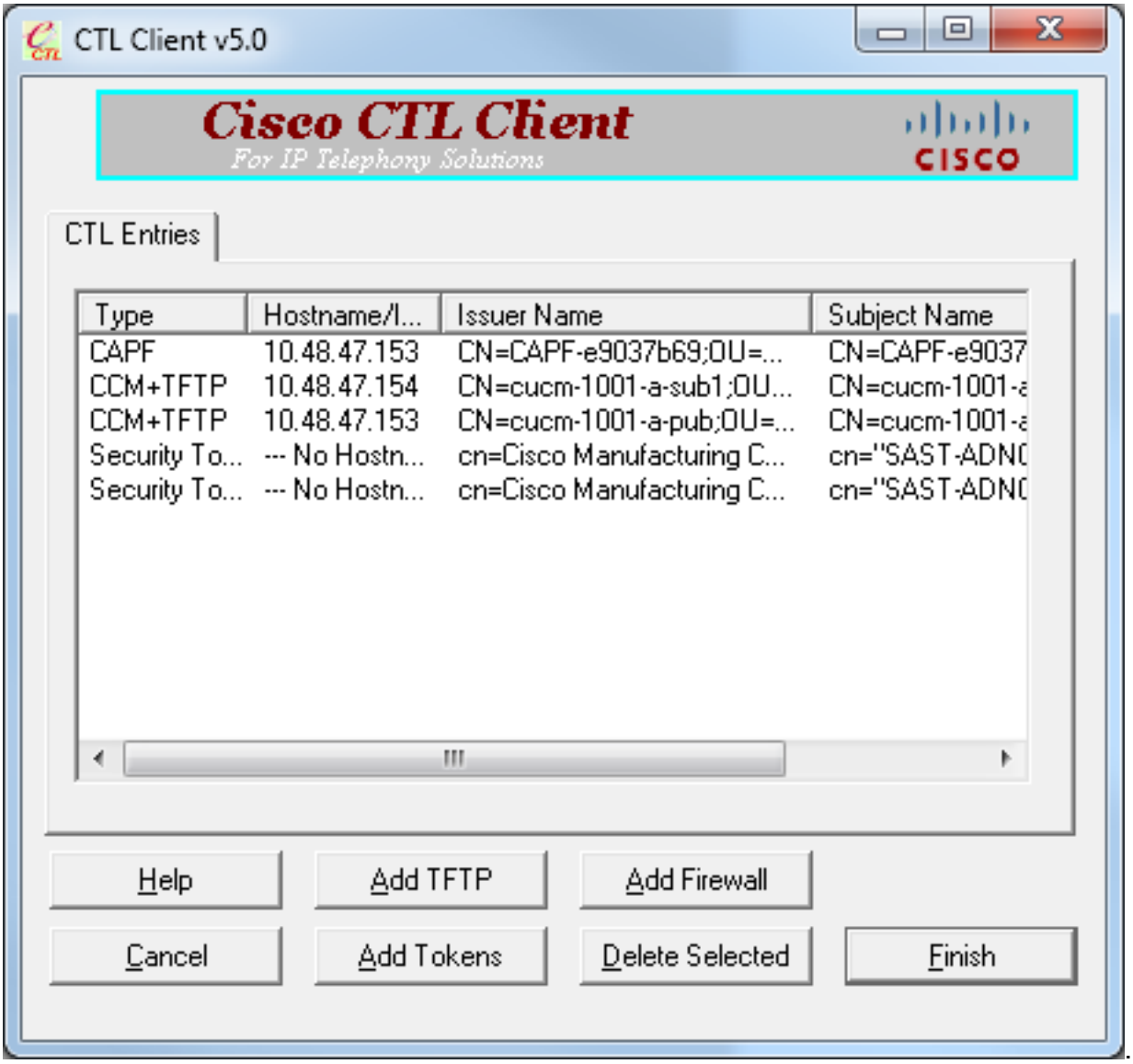


8. يتم عرض شاشة تظهر تفاصيل الرمز المميز الجديد. طقطقة **يضيف** in order to أكدت هم وأضفت هذا الرمز



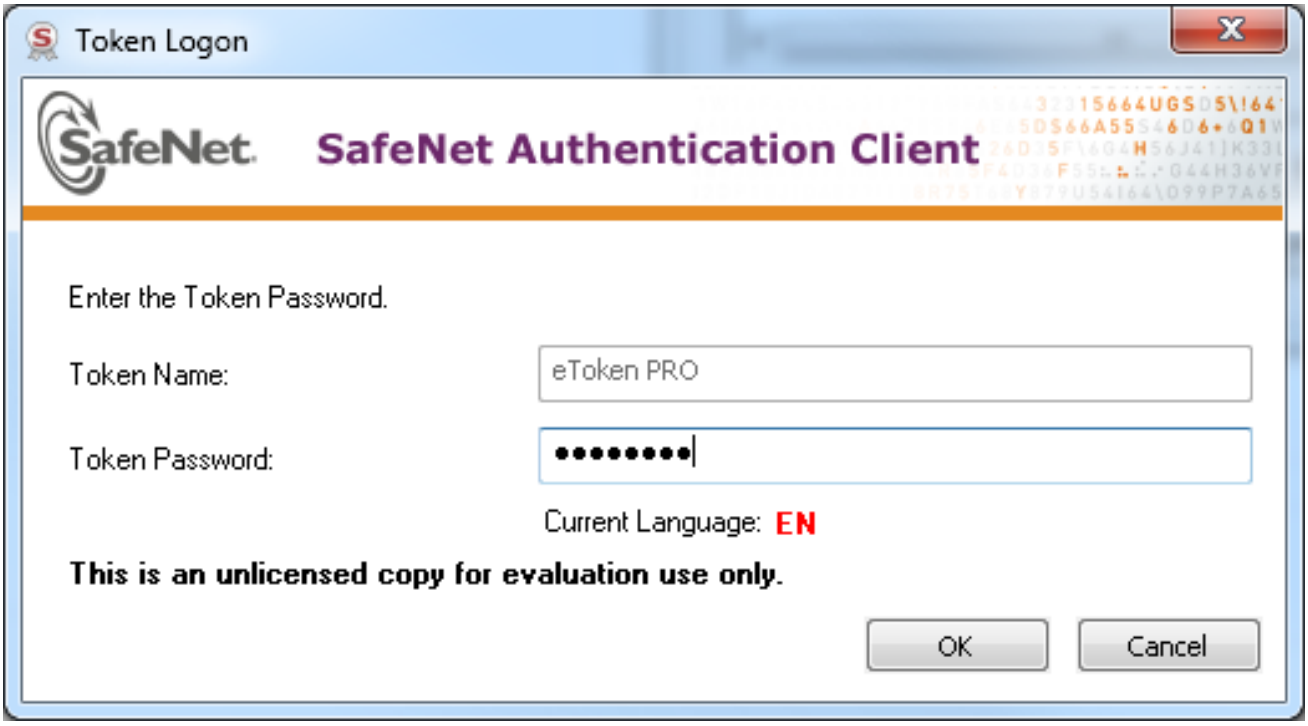
المميز.

9. سيتم تقديم قائمة جديدة بإدخالات CTL التي تظهر كلا الشارات المميزة المضافة. انقر فوق **إنهاء** لإنشاء ملفات CTL

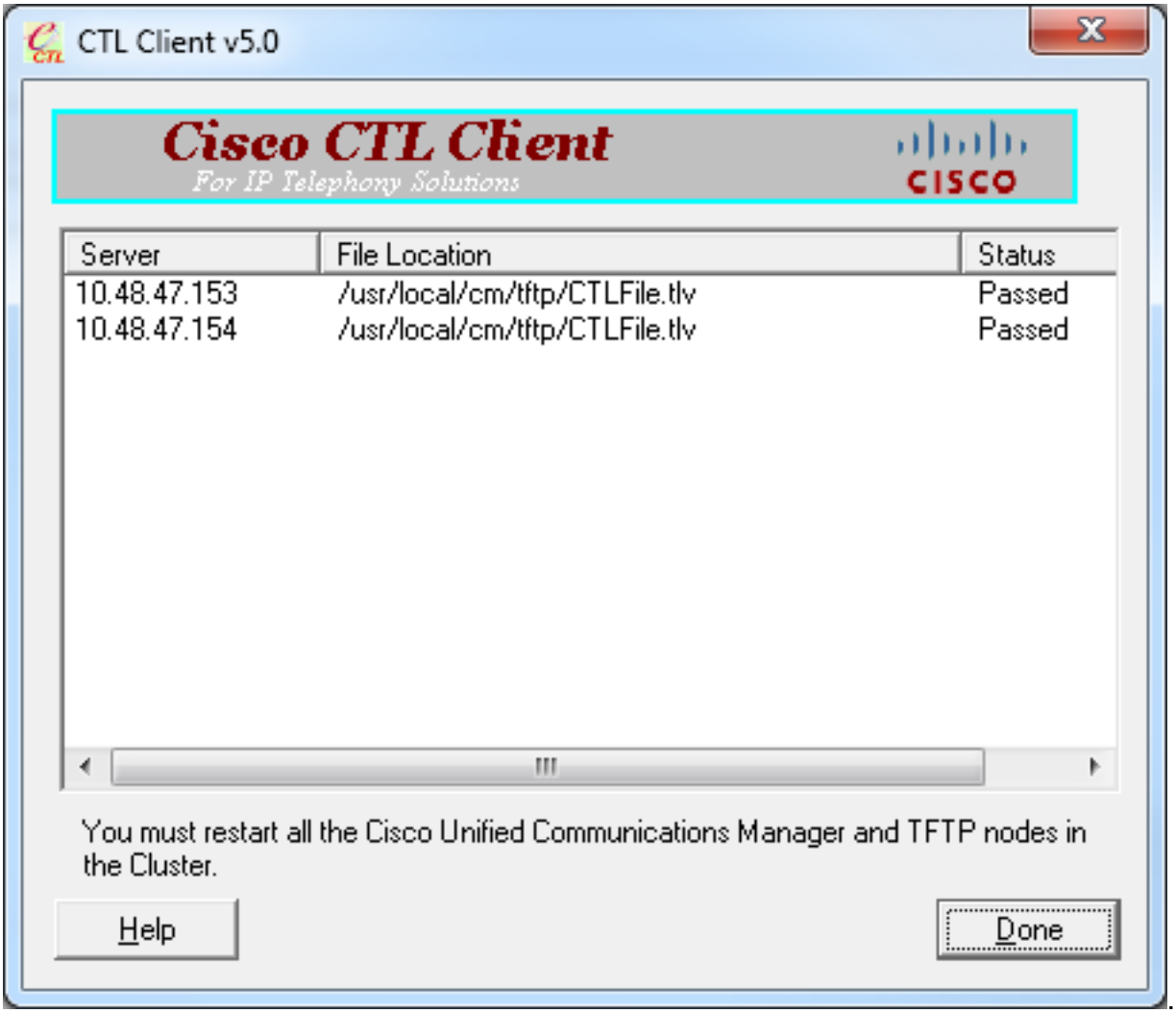


جديدة.

10. في حقل كلمة مرور الرمز المميز، أدخل **Cisco123**. وانقر فوق **OK**.



11. سترى تأكيدا على نجاح العملية. انقر فوق **تم** لتأكيد عميل CTL والخروج



منه.

12. قم بإعادة تشغيل Cisco TFTP متبوعة بخدمة CallManager (الخدمة الموحدة من Cisco > أدوات > مركز التحكم - خدمات الميزات). يجب إنشاء ملف CTL الجديد. أدخل الأمر **show ctl** للتحقق.

```
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. احذف ملف CTL من كل هاتف في المجموعة (قد يختلف هذا الإجراء بناء على نوع الهاتف - يرجى مراجعة الوثائق للحصول على تفاصيل، مثل هاتف بروتوكول الإنترنت الموحد طراز 8961 و 9951 و 9971 من Cisco).**ملاحظة**: قد تظل الهواتف قادرة على التسجيل (اعتمادا على إعدادات الأمان على الهاتف) والعمل دون متابعة الخطوة 13. ومع ذلك، سيتم تثبيت ملف CTL القديم. قد يتسبب ذلك في حدوث مشاكل في حالة إعادة إنشاء الشهادات أو في إضافة خادم آخر إلى نظام المجموعة أو في إستبدال أجهزة الخادم. لا يوصى بترك المجموعة في هذه الحالة.
14. نقل نظام المجموعة إلى نظام غير آمن. راجع تغيير أمان مجموعة CUCM من الوضع المختلط إلى الوضع غير الآمن باستخدام قسم عميل CTL للحصول على تفاصيل.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).