CUCM 클러스터가 혼합 모드에서 비보안 모드 컨피그레이션으로 변경됨 예

목차

소개

이 문서에서는 CUCM(Cisco Unified Communications Manager) 보안 모드를 혼합 모드에서 비보안 모드로 변경하는 데 필요한 단계에 대해 설명합니다. 또한 이 이동이 완료될 때 CTL(Certificate Trust List) 파일의 내용이 변경되는 방식도 보여 줍니다.

CUCM 보안 모드를 변경하는 데는 세 가지 주요 부분이 있습니다.

1a. CTL 클라이언트를 실행하고 원하는 보안 모드 변형을 선택합니다.
1b. 원하는 보안 모드 변형을 선택하려면 CLI 명령을 입력합니다.
2. 해당 서비스를 실행하는 모든 CUCM 서버에서 Cisco CallManager 및 Cisco TFTP 서비스를 다시 시작합니다.
3. CTL 파일의 업데이트된 버전을 다운로드할 수 있도록 모든 IP 전화를 다시 시작합니다.

> **참고:** 클러스터 보안 모드가 혼합 모드에서 비보안 모드로 변경되면 CTL 파일은 서버와 전화기에 계속 존재하지만 CTL 파일에는 CCM+TFTP(서버) 인증서가 포함되어 있지 않습니다. CTL 파일에 CCM+TFTP(서버) 인증서가 없으므로 전화기가 CUCM에 Non-Secure로 등록됩니다.

사전 요구 사항

요구 사항

CUCM 버전 10.0(1) 이상에 대해 알고 있는 것이 좋습니다. 또한 다음을 확인합니다.

- CTL 제공자 서비스가 작동하며 클러스터의 모든 활성 TFTP 서버에서 실행됩니다. 기본적으로 서비스는 TCP 포트 2444에서 실행되지만 CUCM 서비스 매개변수 컨피그레이션에서 수정할 수 있습니다.
- CAPF(Certificate Authority Proxy Function) 서비스가 실행 중이며 게시자 노드에서 실행됩니다 .
- 클러스터의 데이터베이스(DB) 복제는 올바르게 작동하며 서버는 실시간으로 데이터를 복제합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CUCM 릴리스 10.0.1.11900-2 클러스터(노드 2개)
- Cisco 7975 IP phone(SCCP(Skinny Call Control Protocol), 펌웨어 버전 SCCP75.9-3-1SR3-1S에 등록됨)
- 클러스터를 혼합 모드로 설정하려면 두 개의 Cisco 보안 토큰이 필요합니다
- 클러스터를 비보안 모드로 설정하려면 이전에 나열된 보안 토큰 중 하나가 필요합니다

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

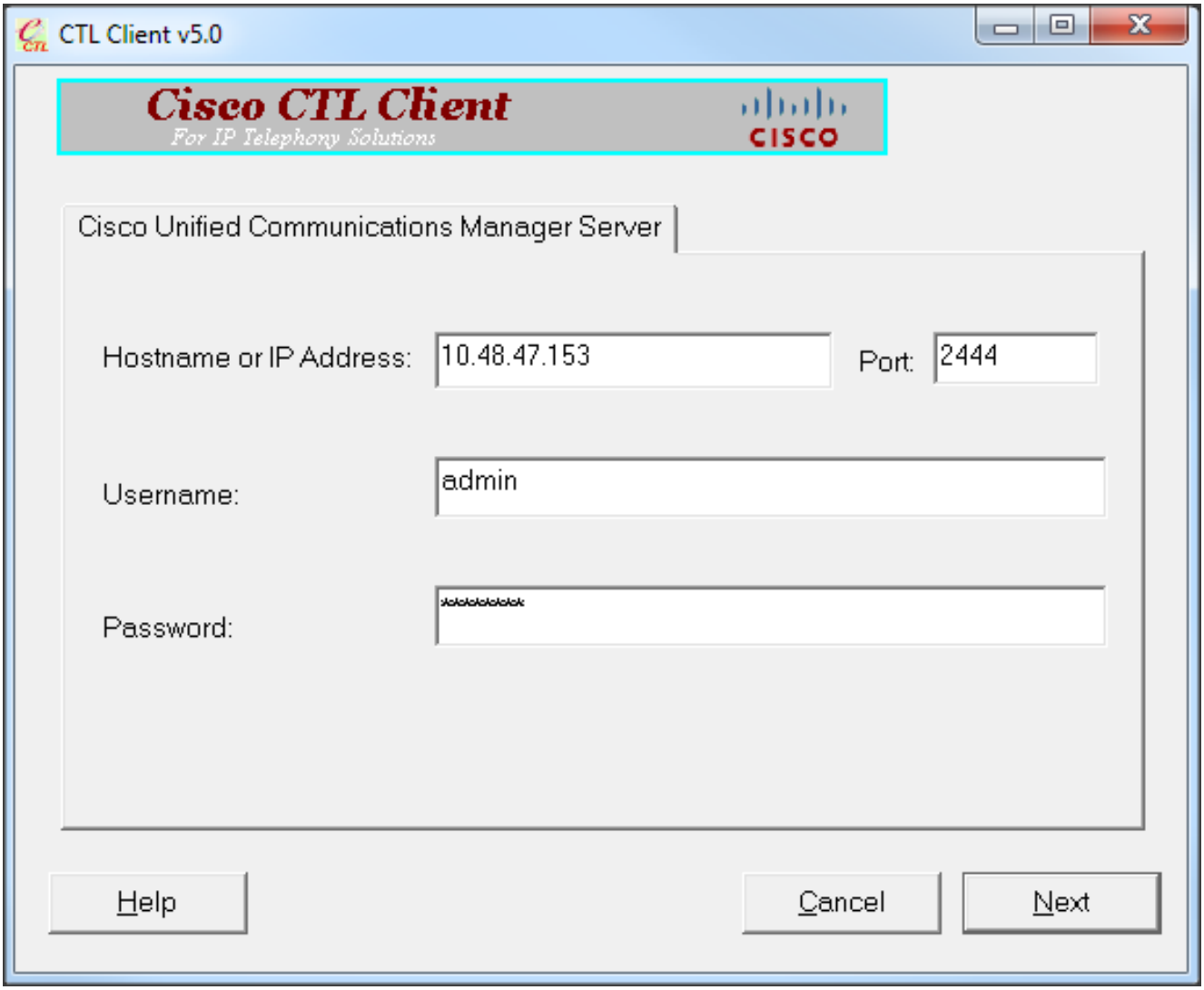
CTL 클라이언트 플러그인을 실행하려면 CUCM Publisher 서버에 있는 최신 CTL 파일을 만들거나 업데이트하기 위해 삽입된 하나 이상의 보안 토큰에 대한 액세스 권한이 있어야 합니다. 즉, CUCM의 현재 CTL 파일에 있는 적어도 하나의 eToken 인증서가 보안 모드를 변경하는 데 사용되는 보안 토큰에 있어야 합니다.

구성

CTL 클라이언트를 사용하여 CUCM 클러스터 보안을 혼합 모드에서 비보안 모드로 변경합니다

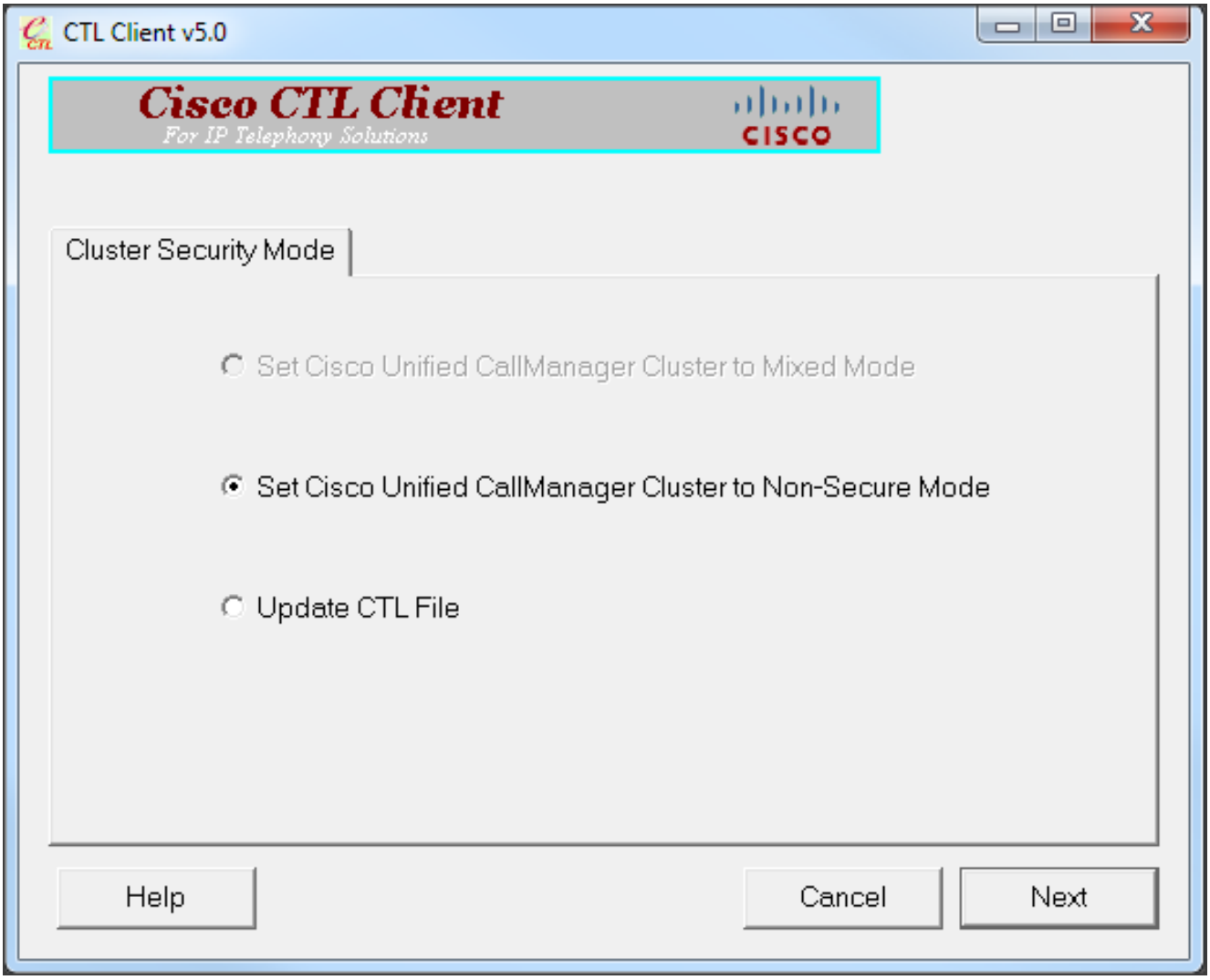
CTL 클라이언트를 사용하여 CUCM 클러스터 보안을 혼합 모드에서 비보안 모드로 변경하려면 다음 단계를 완료합니다.

1. 최신 CTL 파일을 구성하기 위해 삽입한 보안 토큰 하나를 가져옵니다.
2. CTL 클라이언트를 실행합니다. CUCM Pub의 IP 호스트 이름/주소 및 CCM 관리자 자격 증명을 제공합니다. **Next(다음)**를 클릭합니다
   .



3. Set **Cisco Unified CallManager Cluster to Non-Secure Mode** 라디오 **버튼**을 클릭합니다. **Next(다음)**를 클릭합니다

.

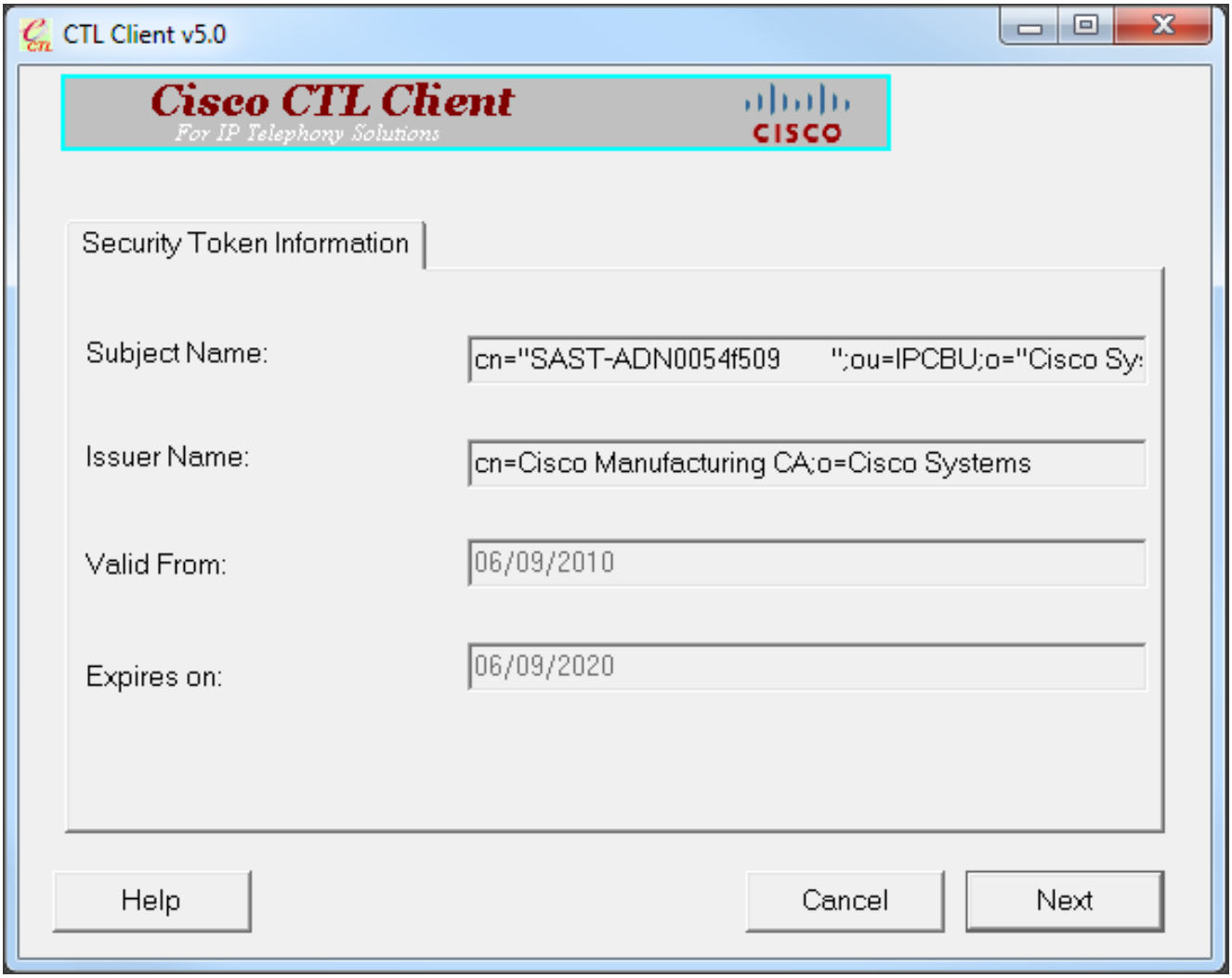


4. 최신 CTL 파일을 구성하기 위해 삽입된 보안 토큰 하나를 삽입하고 OK(**확인**)를 클릭합니다. 이는 CTLFile.tlv의 인증서 목록을 채우는 데 사용된 토큰 중 하나입니다

.

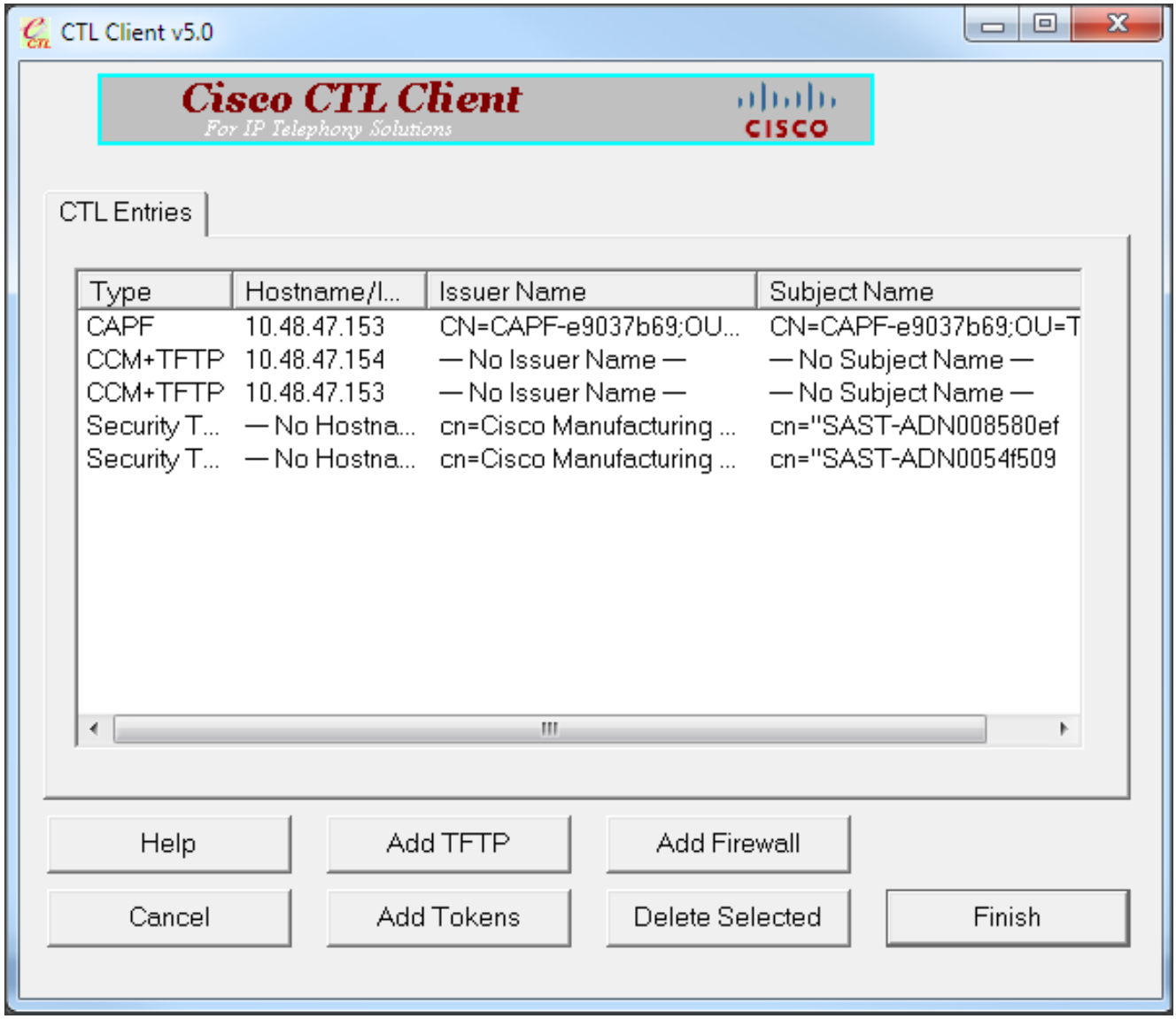
5. 보안 토큰 세부 정보가 표시됩니다. **Next(다음)**를 클릭합니다

.



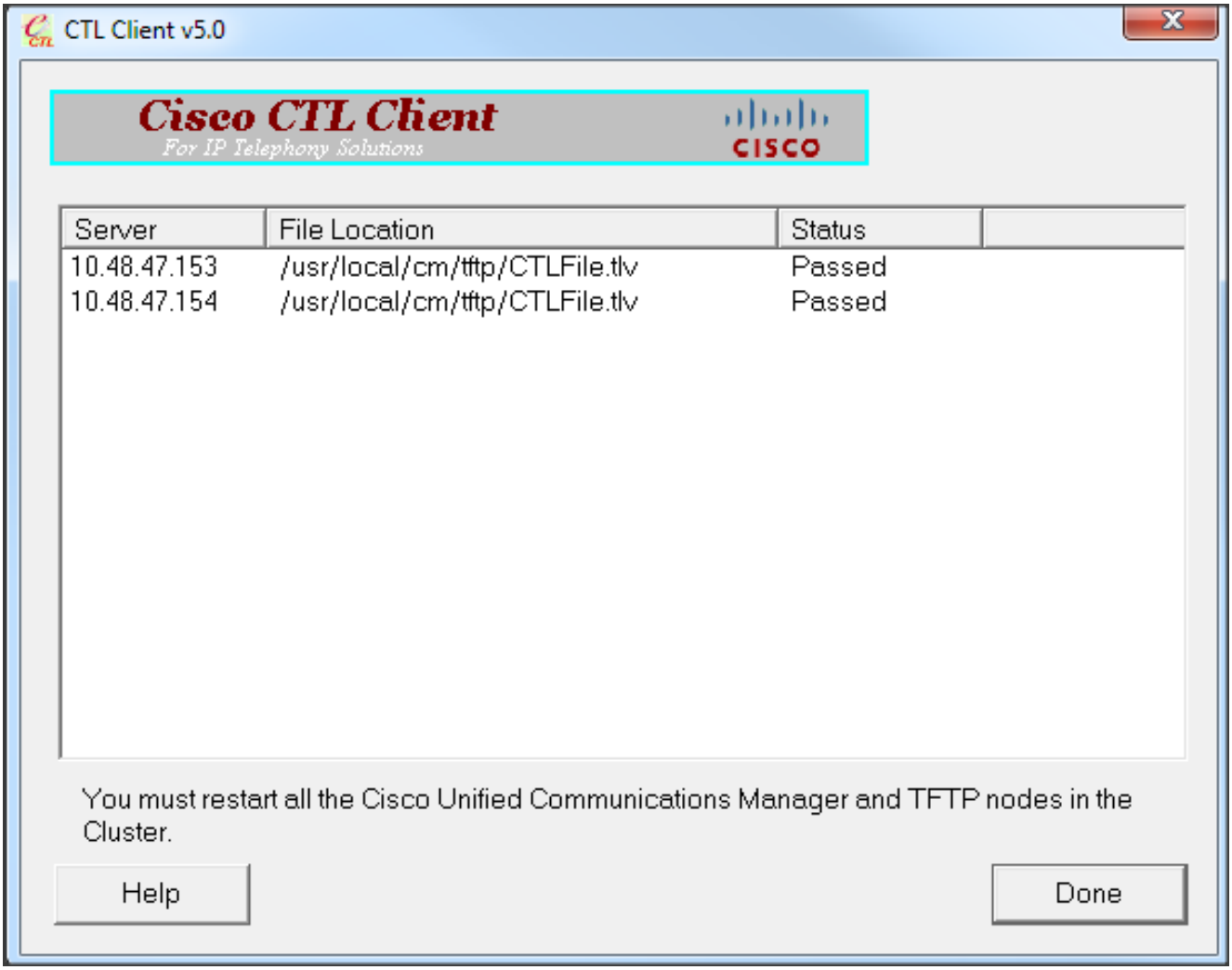
6. CTL 파일의 내용이 표시됩니다. **Finish(마침)**를 클릭합니다. 비밀번호를 입력하라는 프롬프트가 표시되면 **Cisco123**을 **입력합니다**

.

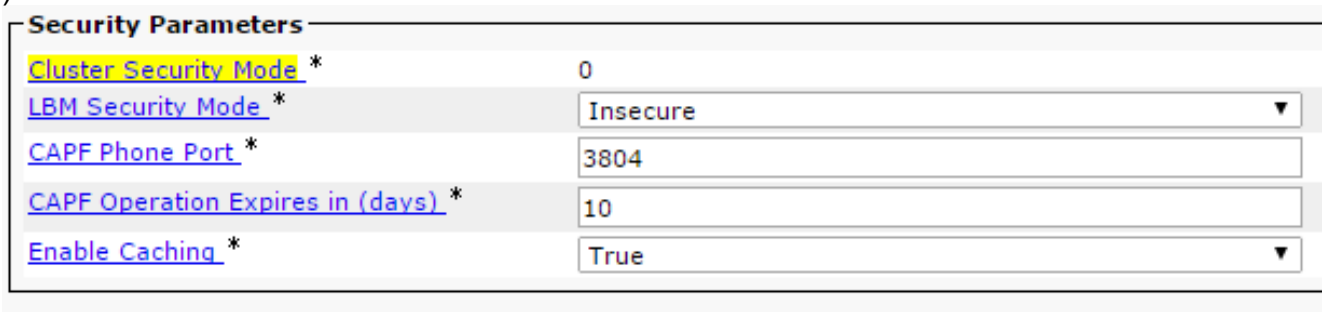


7. CTL 파일이 있는 CUCM 서버 목록이 표시됩니다. 완료를 **클릭합니다**

.



8. CUCM **Admin Page(CUCM 관리 페이지) > System(시스템) > Enterprise Parameters(엔터프라이즈 매개변수)**를 선택하고 클러스터가 비보안 모드로 설정되었는지 확인합니다("0"은 비보안을 나타냄
).



9. 이러한 서비스를 실행하는 클러스터의 모든 노드에서 TFTP 및 Cisco CallManager 서비스를 다시 시작합니다.
10. CUCM TFTP에서 새 버전의 CTL 파일을 가져올 수 있도록 모든 IP 전화를 다시 시작합니다.

CLI를 사용하여 CUCM 클러스터 보안을 혼합 모드에서 비보안 모드로 변경합니다

이 컨피그레이션은 CUCM Release 10.X 이상에만 적용됩니다. CUCM 클러스터 보안 모드를 비보안으로 설정하려면 게시자 CLI에서 **utils ctl set-cluster non-secure-mode** 명령을 입력합니다. 이 작업이 완료되면 이러한 서비스를 실행하는 클러스터의 모든 노드에서 TFTP 및 Cisco CallManager

서비스를 다시 시작합니다.

다음은 이 명령의 사용을 보여 주는 샘플 CLI 출력입니다.

```
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:
```

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

CTLFIle.tlv를 확인하려면 다음 두 가지 방법 중 하나를 사용할 수 있습니다.

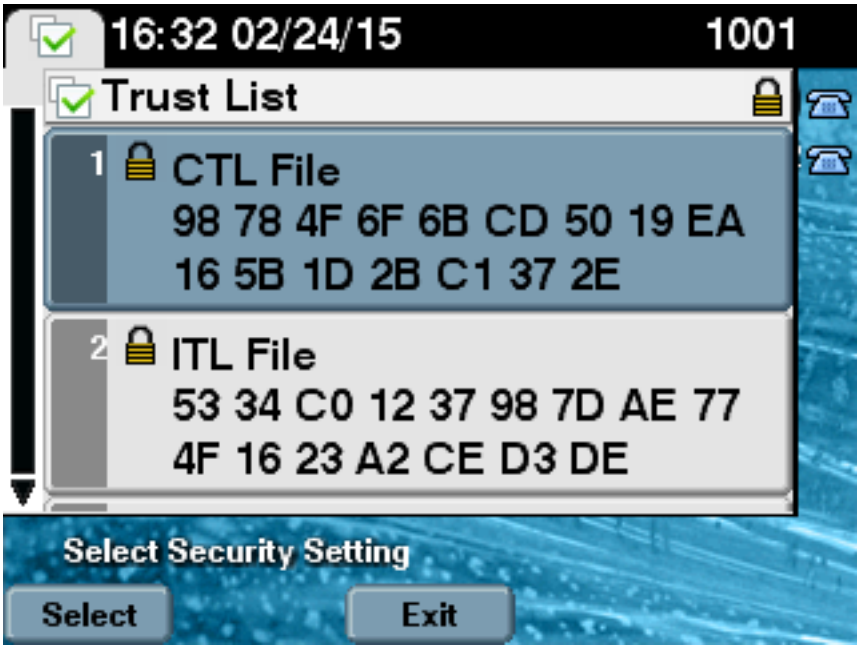
- CUCM TFTP 측에 있는 CTLFIle.tlv의 내용과 MD5 체크섬을 확인하려면 CUCM CLI에서 **show** ctl 명령을 입력합니다. CTLFIle.tlv 파일은 모든 CUCM 노드에서 동일해야 합니다.
- 7975 IP Phone에서 MD5 체크섬을 확인하려면 Settings(설정) > **Security Configuration(보안 컨피그레이션) > Trust List(신뢰 목록) > CTL File(CTL 파일)을** 선택합니다.

  참고: 전화기에서 체크섬을 선택하면 전화기 유형에 따라 MD5 또는 SHA1이 표시됩니다.

CUCM 클러스터를 보안 모드로 설정 - CTL 파일 체크섬

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

IP 전화 측에서는 동일한 CTL 파일이 설치되어 있음을 확인할 수 있습니다(CUCM의 출력과 비교할 때 MD5 체크섬이 일치함).



CUCM Cluster Set to Non-Secure Mode - CTL File Content(CUCM 클러스터가 비보안 모드로 설정됨 - CTL 파일 내용)

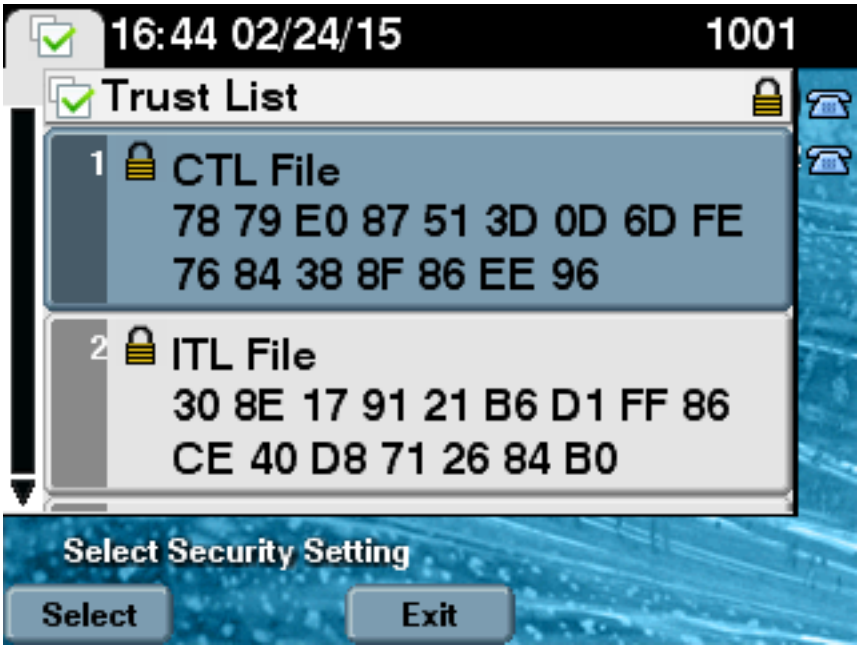
다음은 비보안 모드로 설정된 CUCM 클러스터의 CTL 파일 예입니다. CCM+TFTP 인증서가 비어 있고 어떤 내용도 포함하지 않음을 확인할 수 있습니다. CTL 파일의 나머지 인증서는 변경되지 않으며 CUCM이 혼합 모드로 설정된 경우와 정확히 동일합니다.

```
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:
```

IP Phone 측에서 업데이트된 CTL 파일 버전을 다시 시작하고 다운로드한 후 CUCM의 출력과 비교했을 때 MD5 체크섬이 일치함을 확인할 수 있습니다.



USB 토큰이 손실된 경우 CUCM 클러스터 보안을 혼합 모드에서 비보안 모드로 전환

보안 클러스터의 보안 토큰이 손실될 수 있습니다. 이러한 상황에서는 다음 두 가지 시나리오를 고려해야 합니다.

- 클러스터는 버전 10.0.1 이상을 실행합니다
- 클러스터가 10.x 이전 버전을 실행합니다

첫 번째 시나리오에서는 문제를 복구하기 위해 CLI 섹션과 함께 Change the CUCM Cluster Security from Mixed Mode to Non-Secure Mode에 설명된 절차를 완료합니다. 이 CLI 명령에는 CTL 토큰이 필요하지 않으므로 클러스터가 CTL 클라이언트와 혼합 모드로 설정된 경우에도 사용할 수 있습니다.

CUCM의 10.x 이전 버전이 사용 중일 경우 상황은 더욱 복잡해집니다. 토큰 중 하나의 비밀번호를 잊어버린 경우에도 나머지 토큰을 사용하여 현재 CTL 파일을 사용하여 CTL 클라이언트를 실행할 수 있습니다. 이중화를 위해 가능한 한 빨리 다른 eToken을 가져와 CTL 파일에 추가하는 것이 좋습

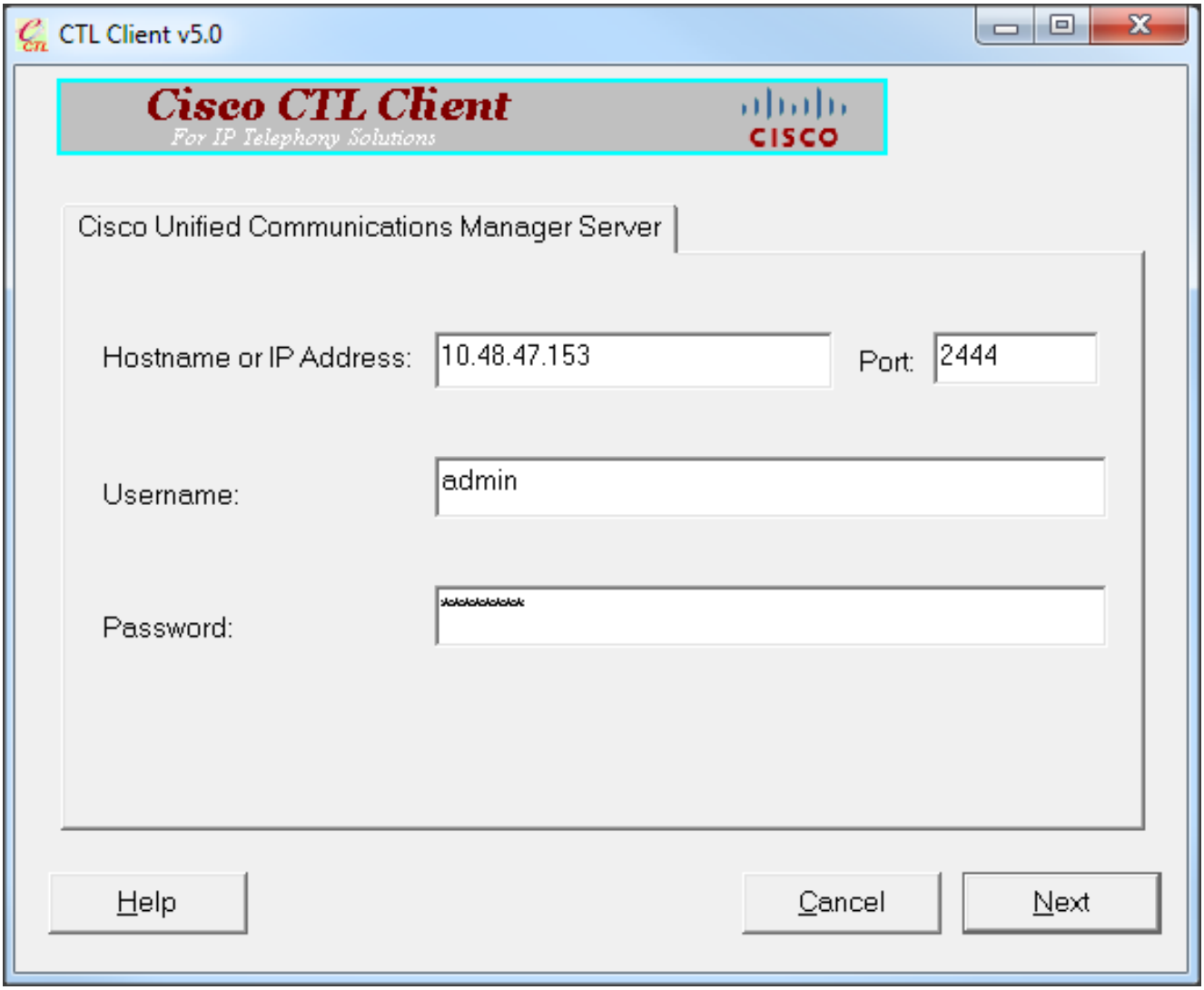
니다. CTL 파일에 나열된 모든 eToken의 비밀번호를 잊어버린 경우 새 eToken 쌍을 가져와서 여기에 설명된 대로 수동 절차를 실행해야 합니다.

1. 모든 TFTP **서버**에서 CTL 파일을 삭제하려면 file delete tftp CTLFile.tlv 명령을 입력합니다.

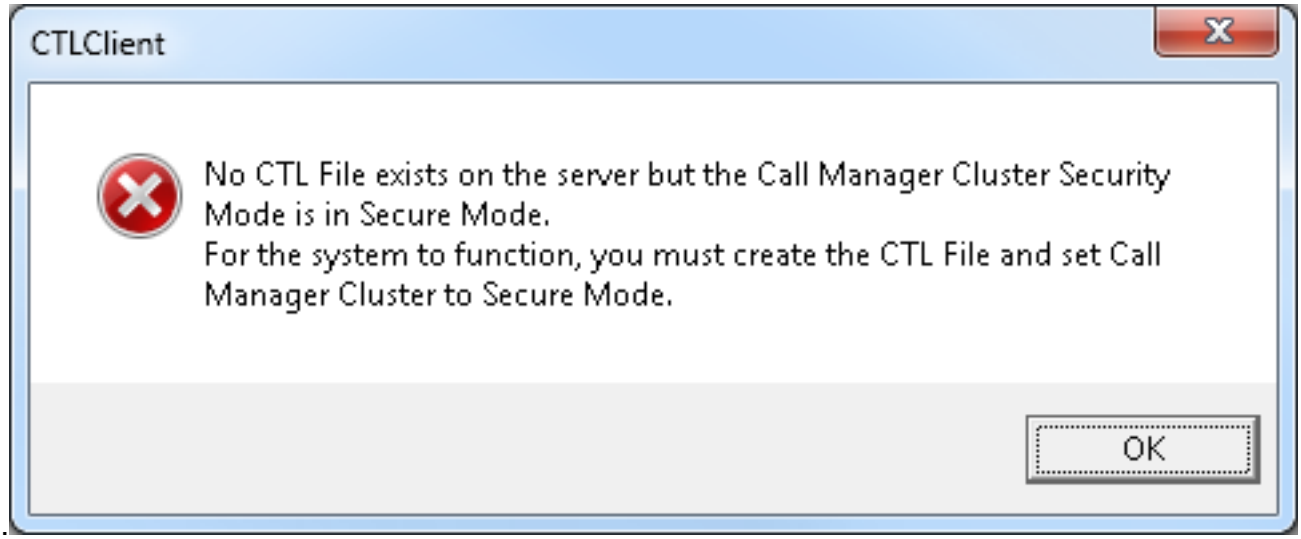
```
admin:file delete tftp CTLFile.tlv
Delete the File CTLFile.tlv?
Enter "y" followed by return to continue: y
files: found = 1, deleted = 1

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. CTL 클라이언트를 실행합니다. CUCM Pub의 IP 호스트 이름/주소 및 CCM 관리자 자격 증명을 입력합니다. **Next(다음)**를 클릭합니다

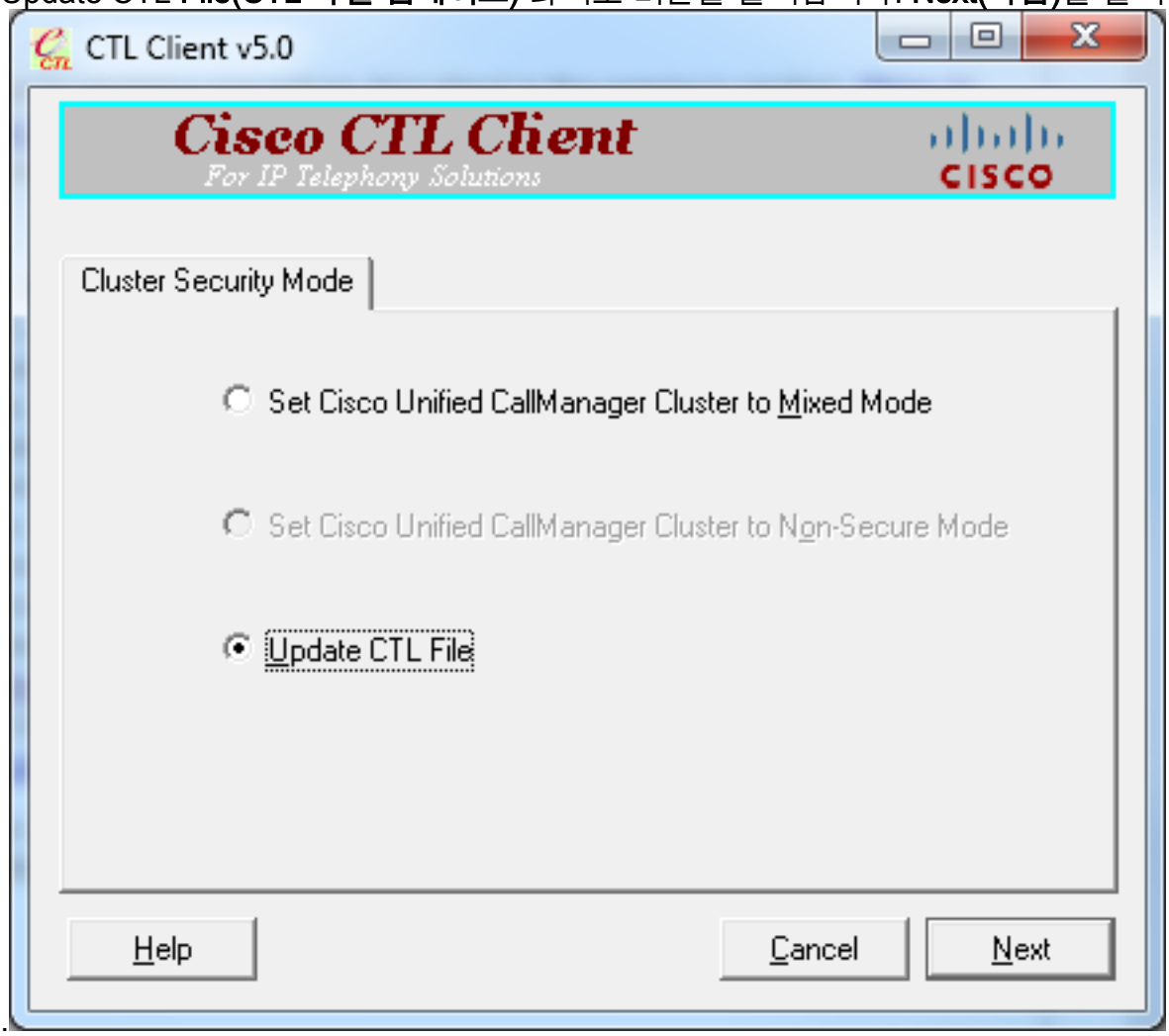
.



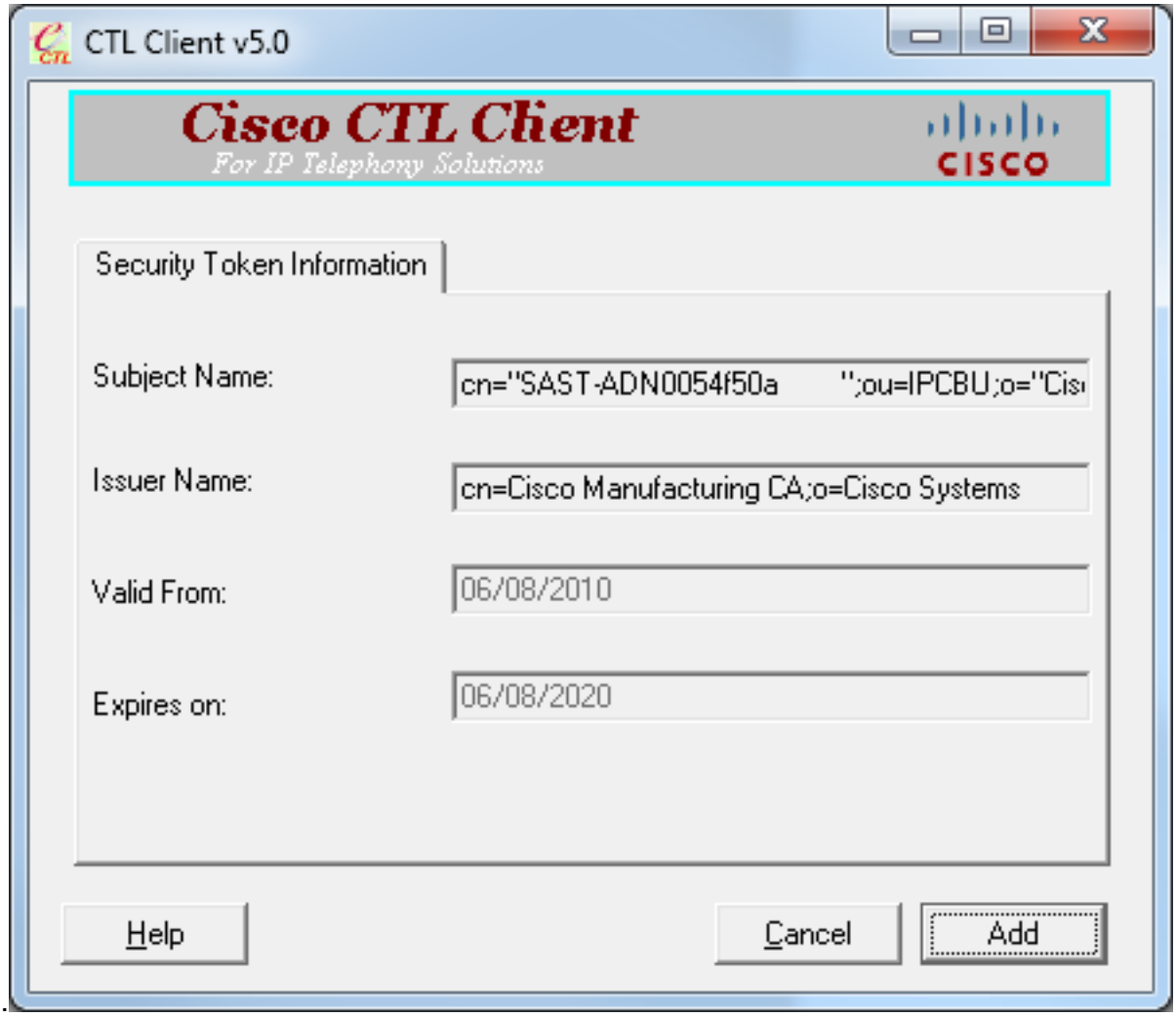
3. 클러스터가 혼합 모드이지만 Publisher에 CTL 파일이 없으므로 이 경고가 표시됩니다. OK(**확인**)를 클릭하여 무시하고 계속 진행합니다



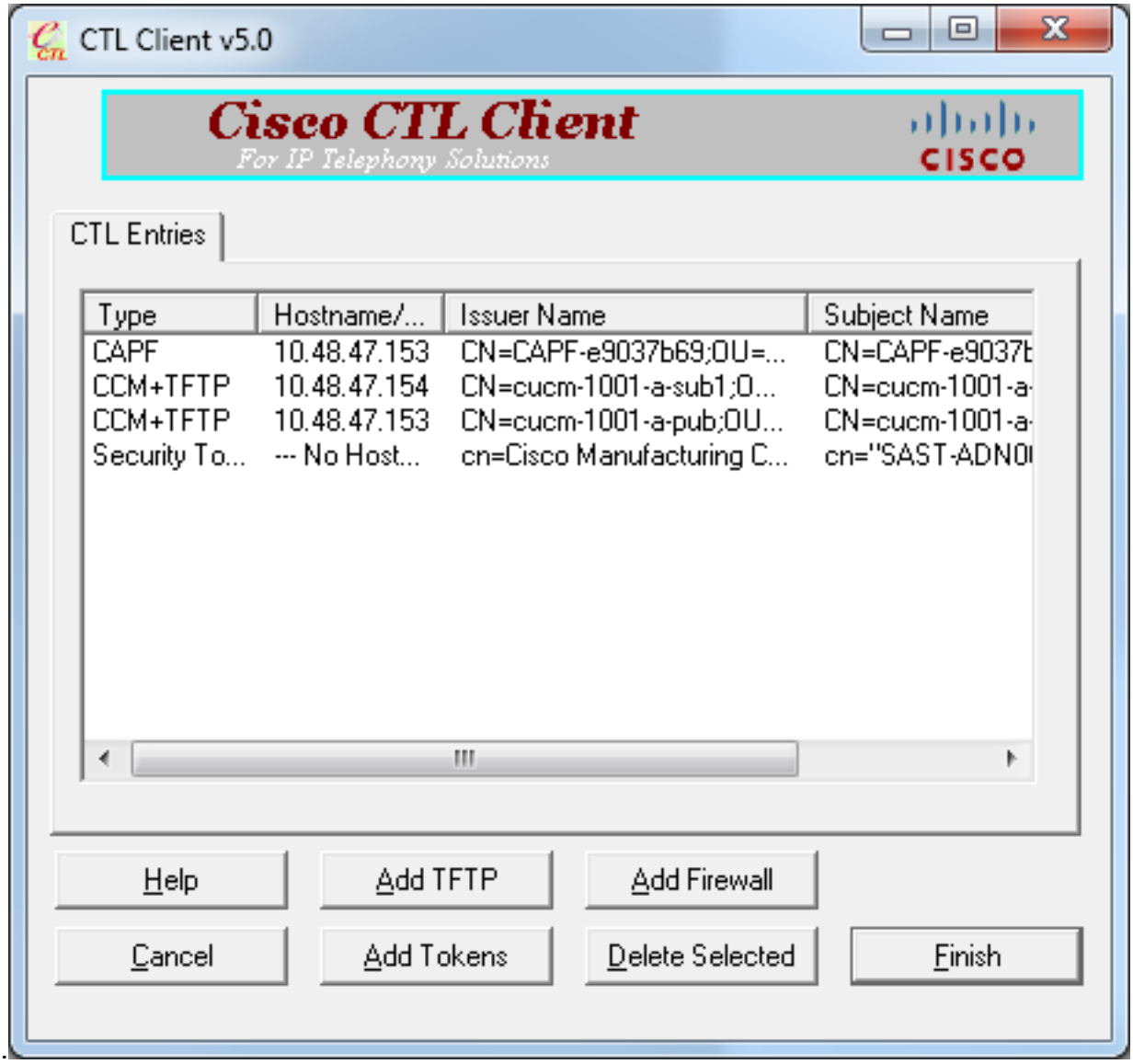
4. Update CTL **File(CTL 파일 업데이트)** 라디오 버튼을 클릭합니다. **Next(다음)**를 클릭합니다



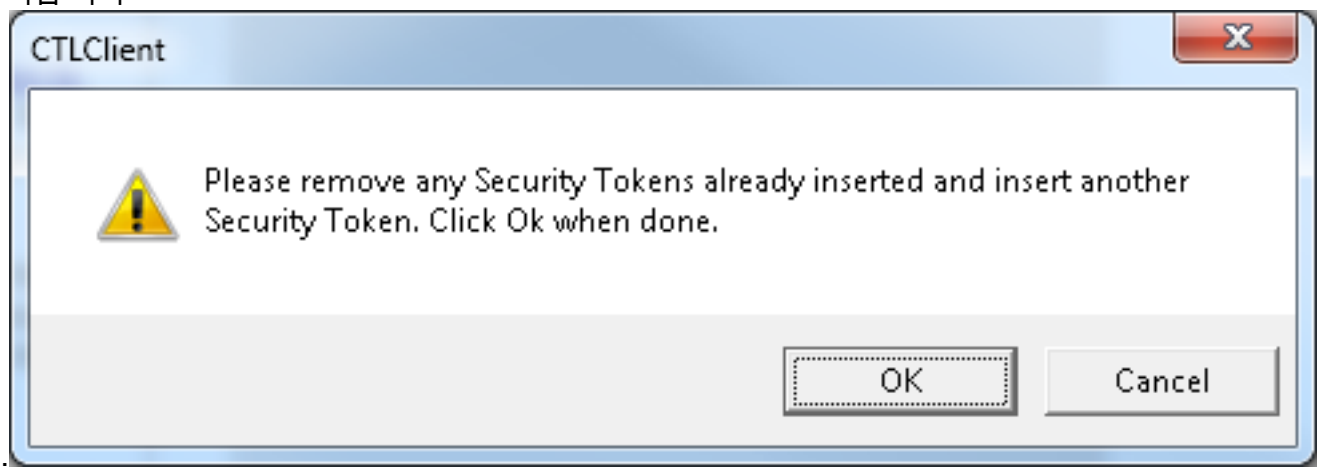
5. CTL 클라이언트는 보안 토큰을 추가하도록 요청합니다. 계속 **진행하려면** Add를 클릭합니다



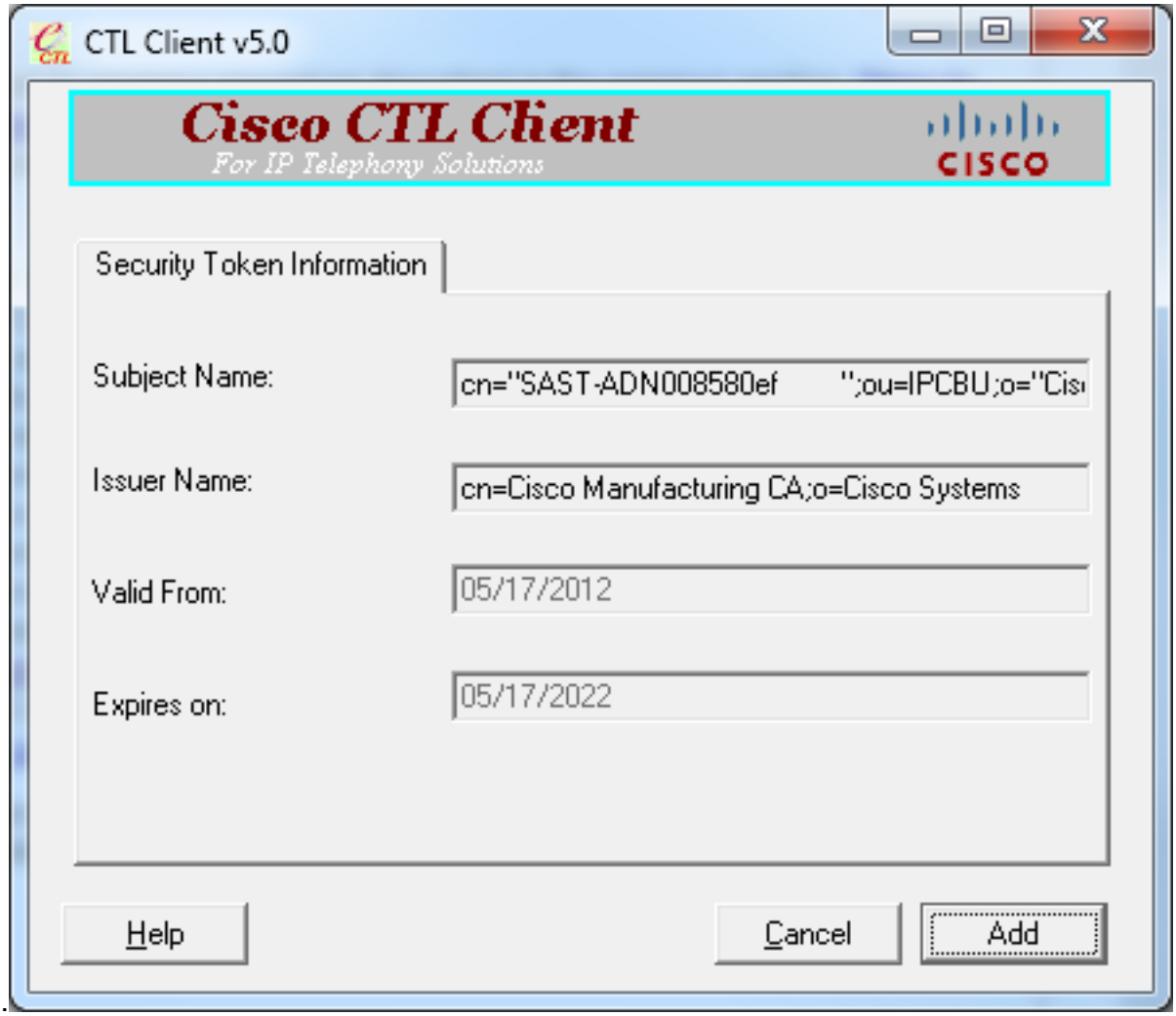
6. 화면에 새 CTL의 모든 항목이 표시됩니다. 새 쌍에서 두 번째 토큰을 추가하려면 Add Tokens를 클릭합니다



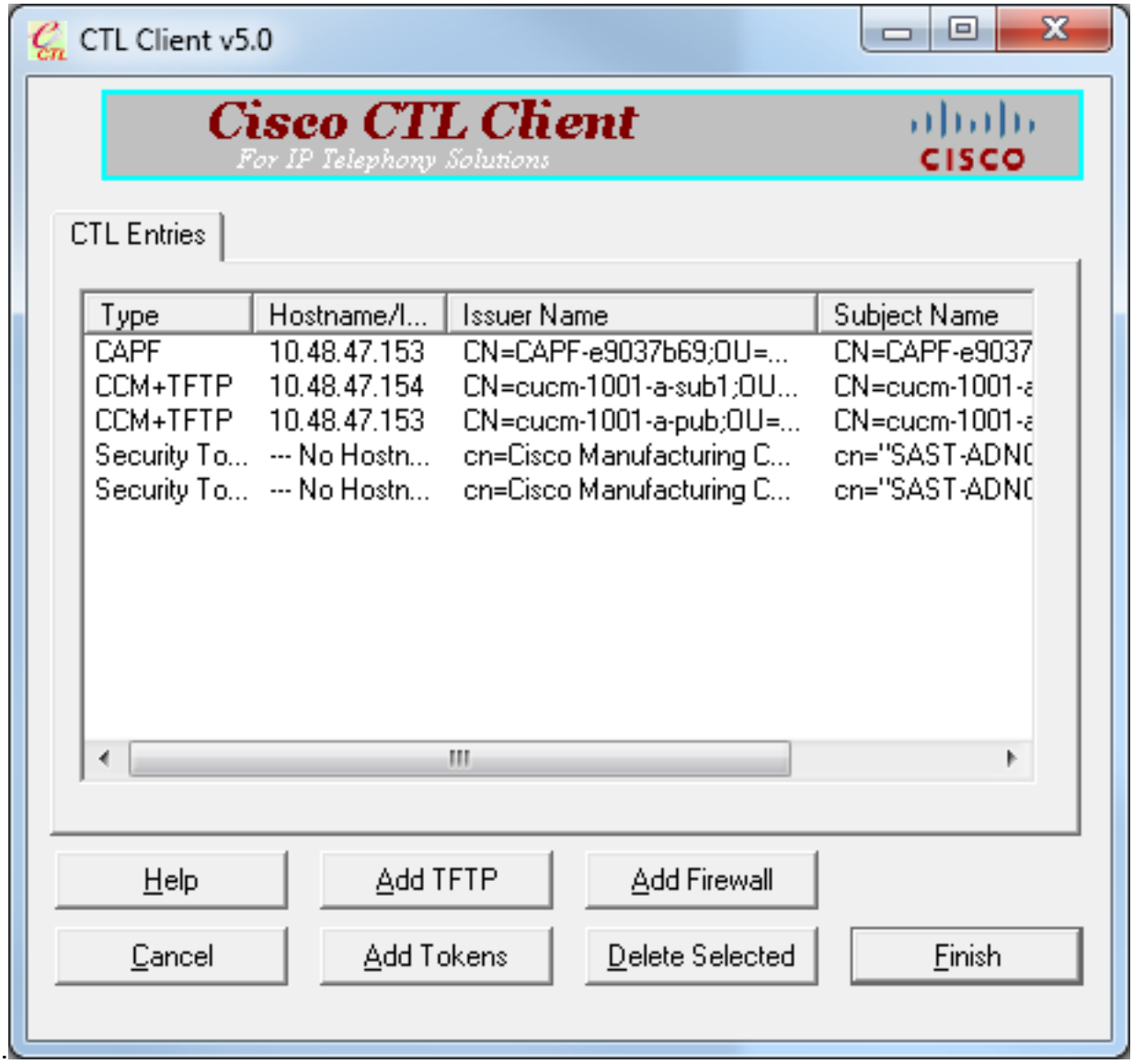
7. 현재 토큰을 제거하고 새 토큰을 삽입하라는 메시지가 표시됩니다. 완료했으면 **OK(확인)**를 클릭합니다



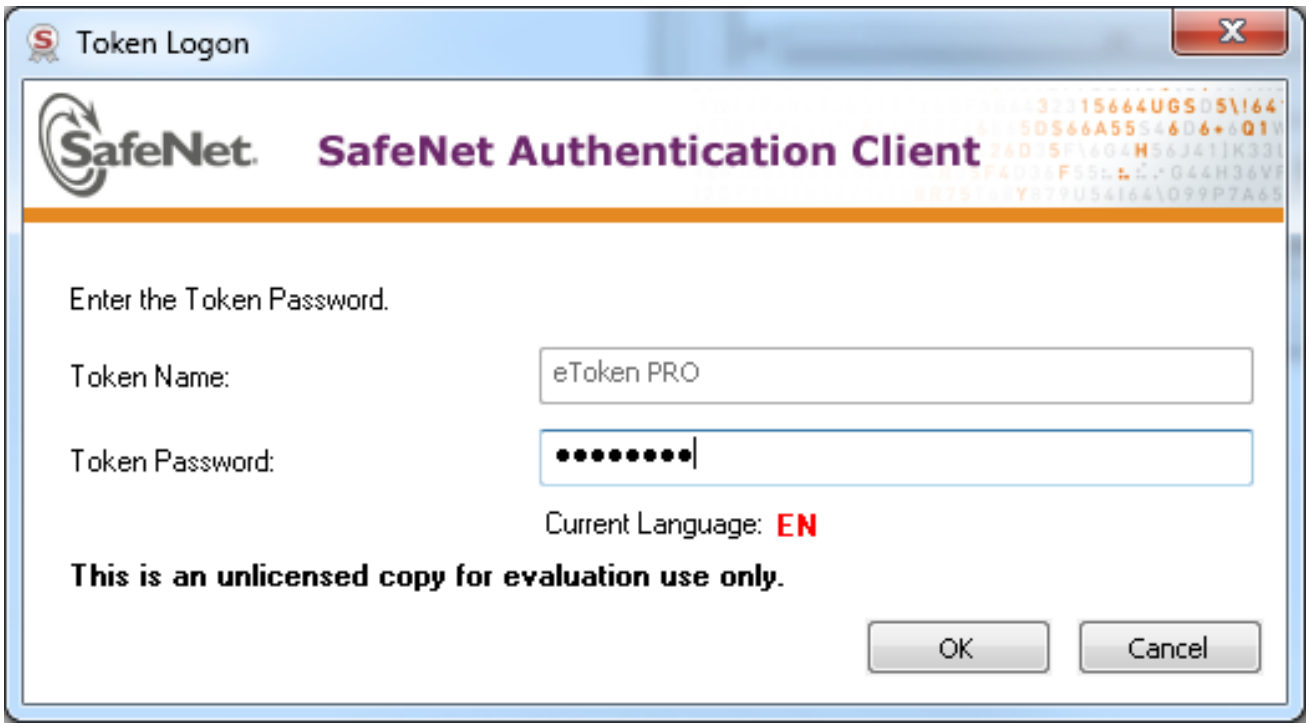
8. 새 토큰의 세부 정보를 보여 주는 화면이 표시됩니다. Add(**추가**)를 클릭하여 확인하고 이 토큰을 추가합니다



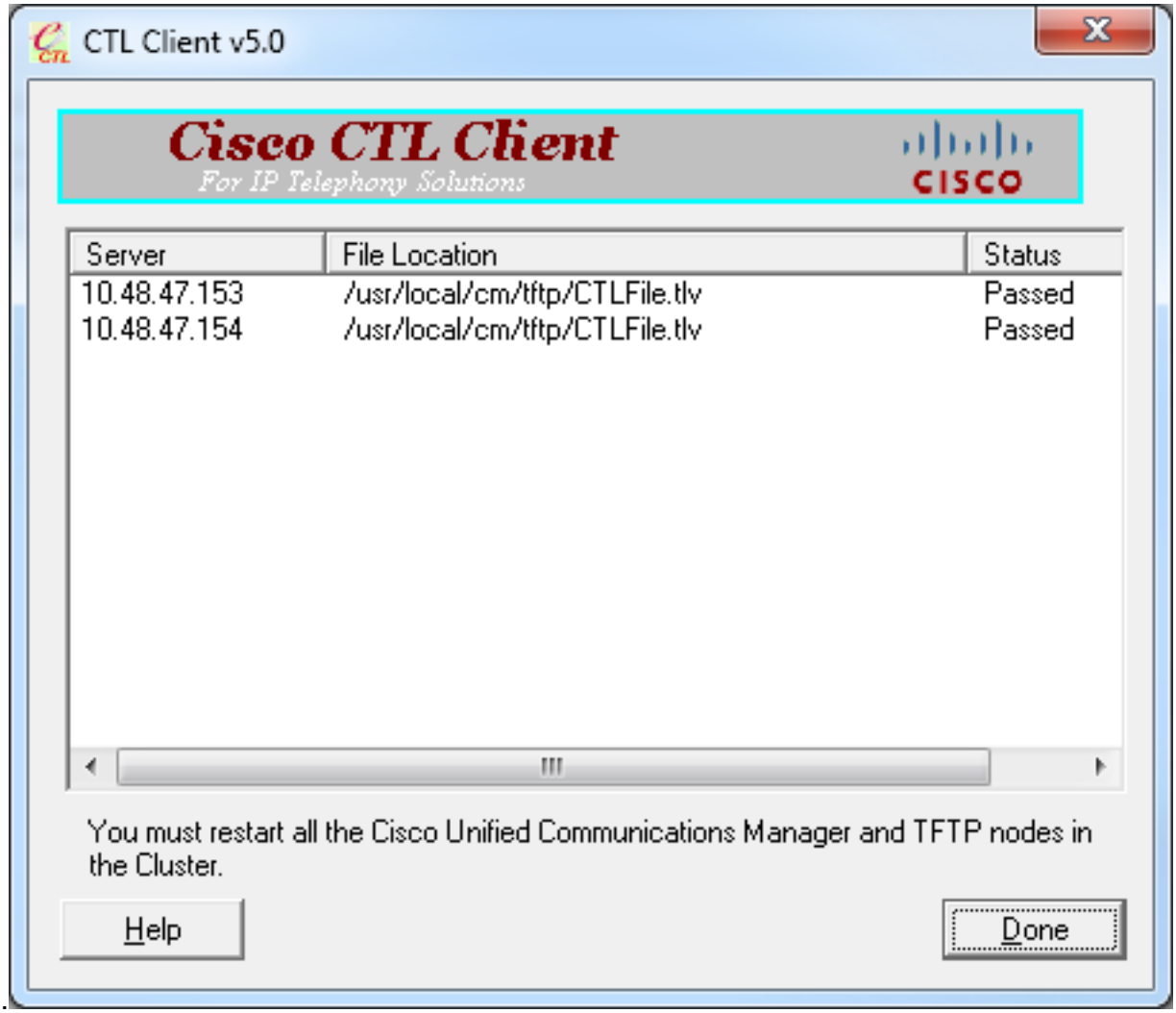
9. 추가된 두 토큰을 모두 표시하는 새 CTL 항목 목록이 표시됩니다. 새 CTL **파일**을 생성하려면 Finish(마침)를 클릭합니다



10. Token Password(토큰 비밀번호) 필드에 **Cisco123**을 입력합니다. OK(**확인**)를 클릭합니다



11. 프로세스가 성공적으로 완료되었다는 확인 메시지가 표시됩니다. Done(**완료**)을 클릭하여 CTL 클라이언트를 확인하고 종료합니다



12. CallManager 서비스(Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Feature Services(제어 센터 - 기능 서비스)) 다음에 Cisco TFTP를 재시작합니다. 새 CTL 파일을 생성해야 합니다. 확인을 위해 **show** ctl 명령을 입력합니다.

```
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. 클러스터의 각 전화기에서 CTL 파일을 삭제합니다(이 절차는 전화기 유형에 따라 다를 수 있습니다. Cisco Unified IP Phone 8961, 9951 및 9971 관리 가이드와 같은 자세한 내용은 설명서를 참조하십시오).**참고:** 전화기는 여전히 등록(전화기의 보안 설정에 따라)할 수 있으며 13단계를 진행하지 않고 작동할 수 있습니다. 그러나 이전 CTL 파일이 설치됩니다. 인증서가 다시 생성되고 다른 서버가 클러스터에 추가되거나 서버 하드웨어가 교체될 경우 문제가 발생할 수 있습니다. 클러스터를 이 상태로 두지 않는 것이 좋습니다.
14. 클러스터를 Non-Secure로 이동합니다. 자세한 내용은 CTL Client를 사용하여 CUCM 클러스터 보안을 혼합 모드에서 비보안 모드로 변경 섹션을 참조하십시오.

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.