

Cluster do CUCM alterado do modo misto para o modo não seguro Exemplo de configuração

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Alterar a segurança de cluster do CUCM do modo misto para o modo não seguro com o cliente CTL](#)

[Altere a segurança de cluster do CUCM do modo misto para o modo não seguro com a CLI](#)

[Verificar](#)

[Cluster CUCM definido para modo de segurança - Soma de verificação de arquivo CTL](#)

[Cluster do CUCM definido como modo não seguro - Conteúdo do arquivo CTL](#)

[Coloque a segurança de cluster CUCM do modo misto para o modo não seguro quando houver perda de tokens USB](#)

[Troubleshoot](#)

Introduction

O documento descreve as etapas necessárias para alterar o Modo de segurança do Cisco Unified Communications Manager (CUCM) de Modo misto para Modo não seguro. Ele também mostra como o conteúdo de um arquivo CTL (Certificate Trust List) é alterado quando essa movimentação é concluída.

Há três partes principais para alterar o modo de segurança do CUCM:

- 1 bis. Execute o cliente CTL e selecione a variante desejada do Modo de Segurança.
- 1-B. Insira o comando CLI para selecionar a variante desejada do Modo de segurança.
2. Reinicie os serviços Cisco CallManager e Cisco TFTP em todos os servidores CUCM que executam esses serviços.
3. Reinicie todos os telefones IP para que eles possam baixar a versão atualizada do arquivo CTL.

Note: Se o modo de segurança do cluster for alterado do modo Misto para o modo Não Seguro, o arquivo CTL ainda existirá no(s) servidor(es) e nos telefones, mas o arquivo CTL não conterá nenhum certificado CCM+TFTP (servidor). Como os certificados CCM+TFTP (servidor) não existem no arquivo CTL, isso força o telefone a se registrar como Não seguro com o CUCM.

Prerequisites

Requirements

A Cisco recomenda que você tenha experiência com o CUCM versão 10.0 (1) ou posterior. Além disso, verifique se:

- O serviço Provedor de CTL está ativo e é executado em todos os servidores TFTP ativos no cluster. Por padrão, o serviço é executado na porta TCP 2444, mas isso pode ser modificado na configuração do parâmetro de serviço do CUCM.
- Os Serviços de Função de Proxy de Autoridade de Certificação (CAPF) estão ativos e em execução no nó Publicador.
- A replicação do banco de dados (DB) no cluster funciona corretamente e os servidores replicam dados em tempo real.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cluster de dois nós do CUCM versão 10.0.1.11900-2
- Telefone IP Cisco 7975 (registrado com Skinny Call Control Protocol (SCCP), versão de firmware SCCP75.9-3-1SR3-1S)
- Dois tokens de segurança da Cisco são necessários para definir o cluster para o modo Misto
- Um dos tokens de segurança listados anteriormente é necessário para definir o cluster para o modo Não seguro

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

Para executar o plug-in do cliente CTL, é necessário ter acesso a pelo menos um token de segurança que foi inserido para criar ou atualizar o arquivo CTL mais recente existente no servidor do editor CUCM. Em outras palavras, pelo menos um dos certificados eToken existentes no arquivo CTL atual no CUCM deve estar no token de segurança usado para alterar o modo de segurança.

Configurar

Alterar a segurança de cluster do CUCM do modo misto para o modo não seguro com o cliente CTL

Conclua estas etapas para alterar a segurança do cluster CUCM do modo Misto para o modo Não seguro com o cliente CTL:

1. Obtenha um token de segurança que você inseriu para configurar o arquivo CTL mais recente.
2. Execute o cliente CTL. Forneça o nome/endereço do host IP da Pub do CUCM e as credenciais de administrador do CCM. Clique em Next.

CTL Client v5.0

Cisco CTL Client
For IP Telephony Solutions

CISCO

Cisco Unified Communications Manager Server

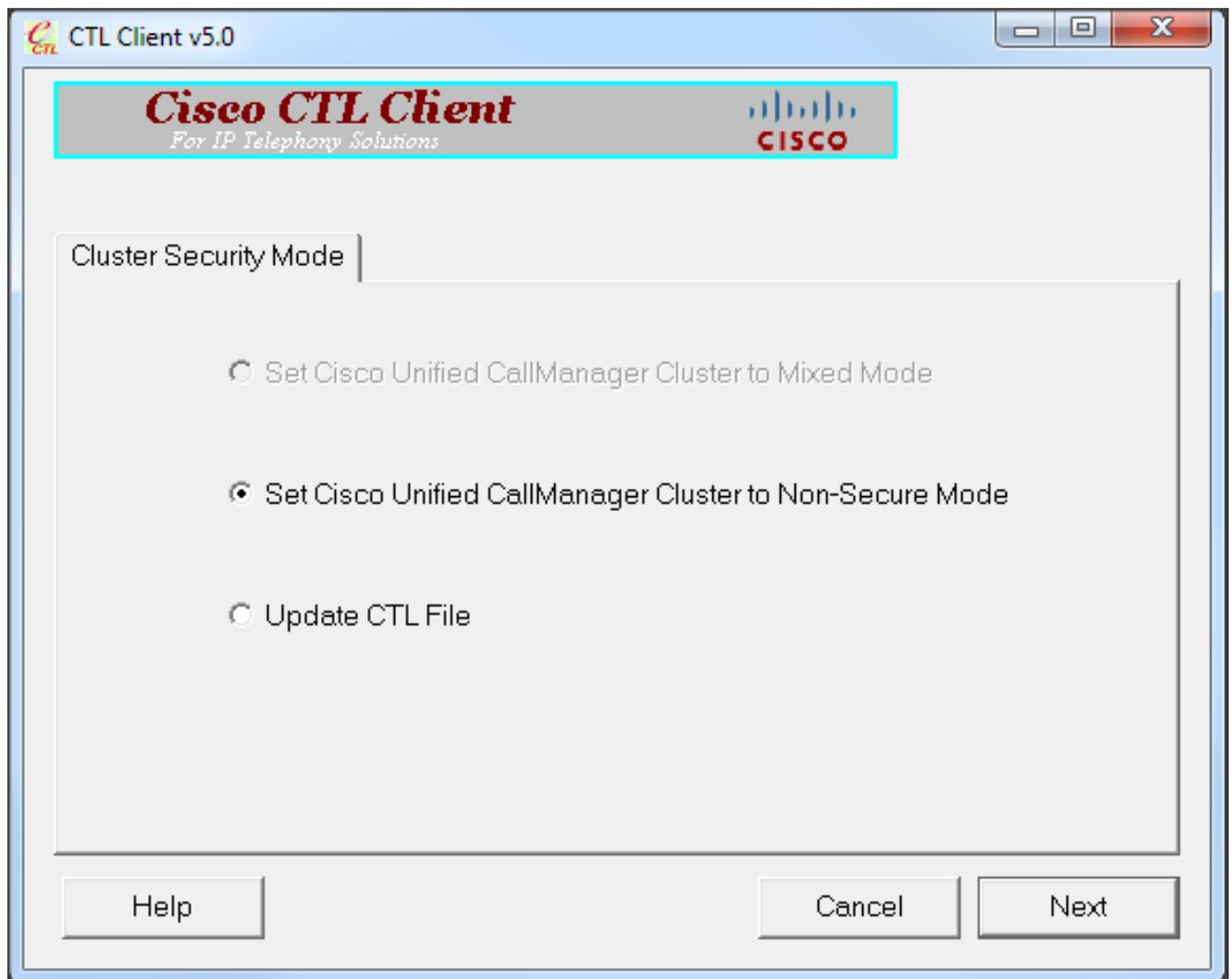
Hostname or IP Address: 10.48.47.153 Port: 2444

Username: admin

Password: *

Help Cancel Next

3. Clique no botão de opção **Set Cisco Unified CallManager Cluster to Non-Secure Mode**. Clique em Next.

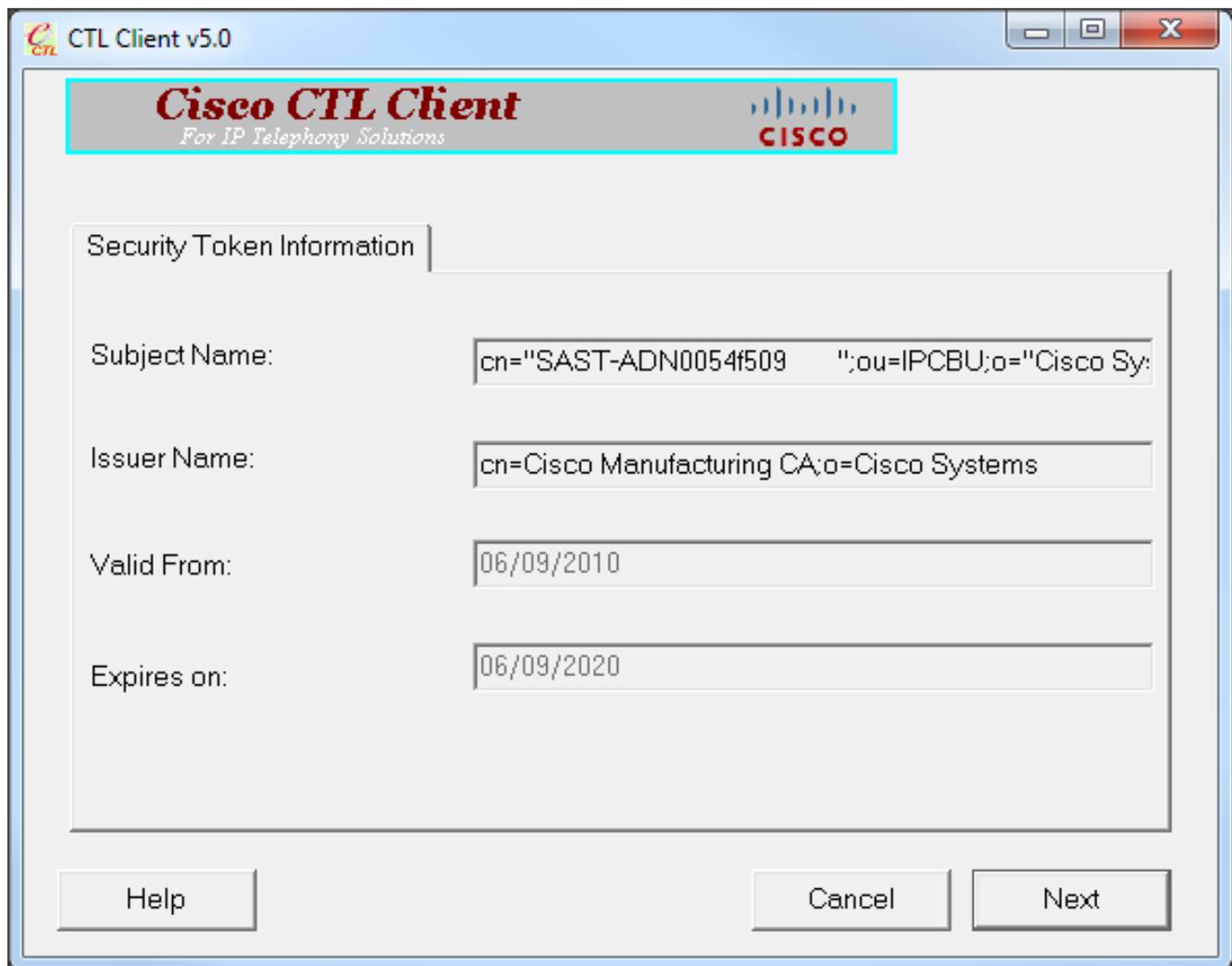


4. Insira um token de segurança que foi inserido para configurar o arquivo CTL mais recente e clique em **OK**. Este é um dos tokens que foi usado para preencher a lista de certificados no

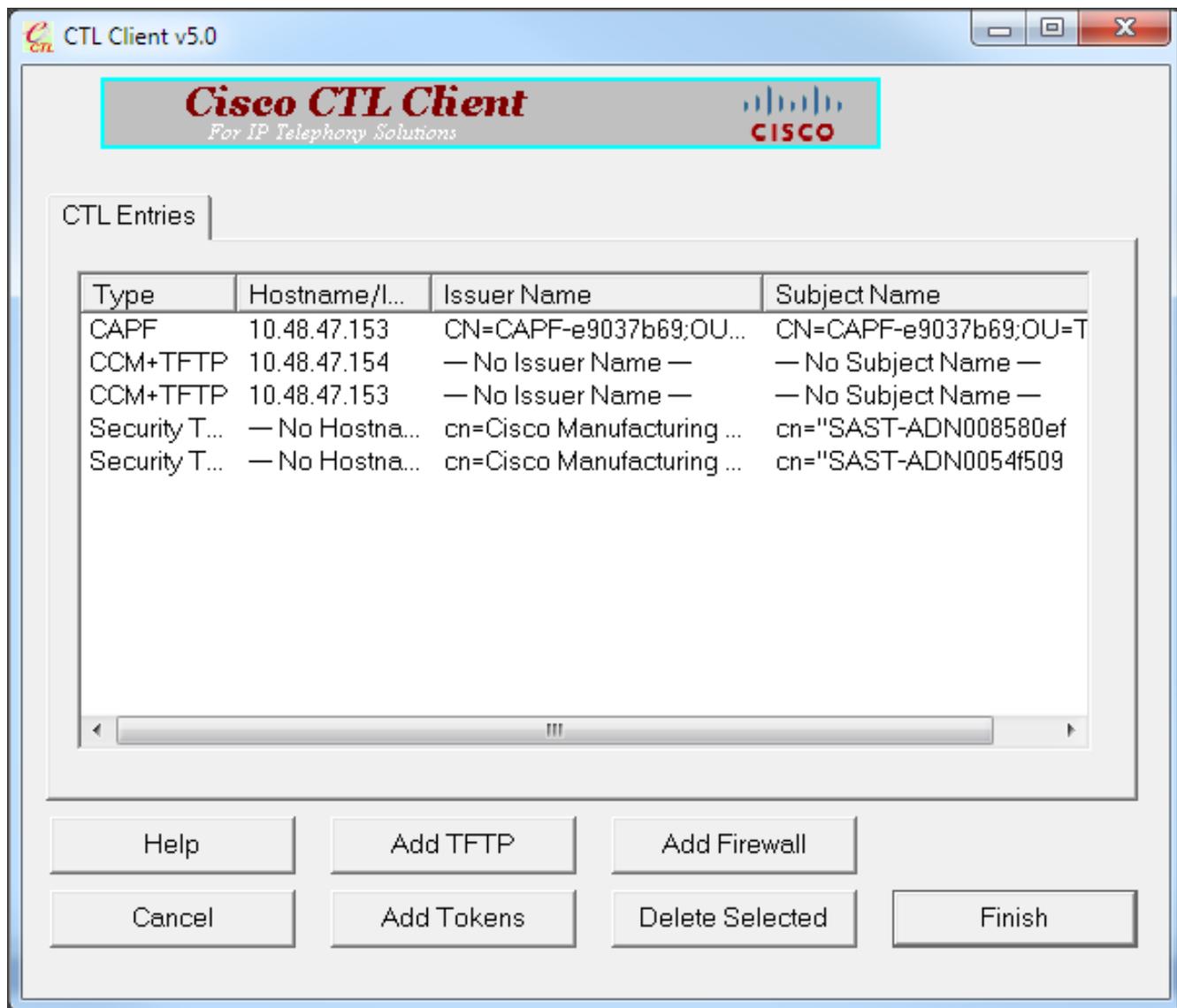


CTLFile.tv.

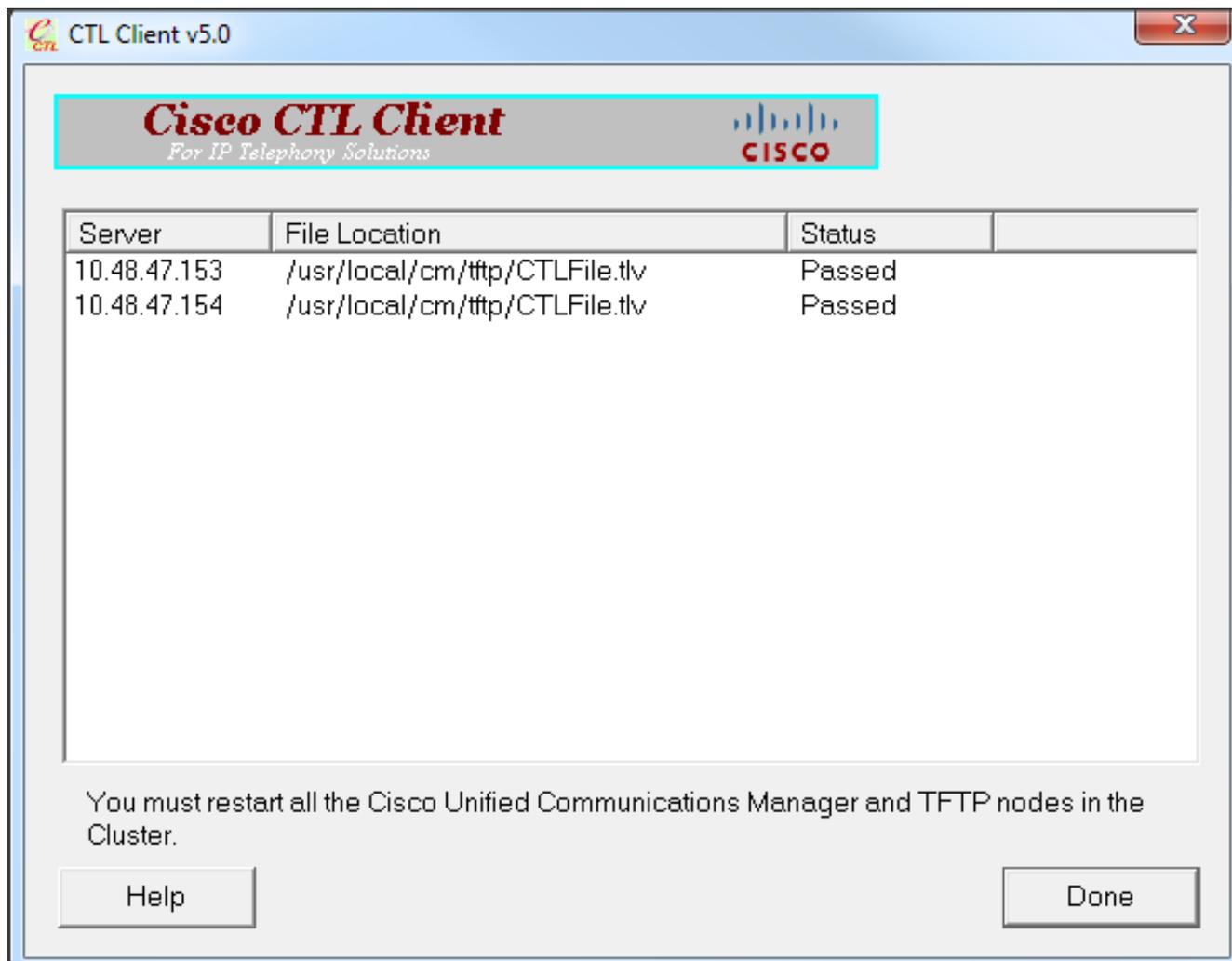
5. Os detalhes do Token de segurança são exibidos. Clique em **Next**.



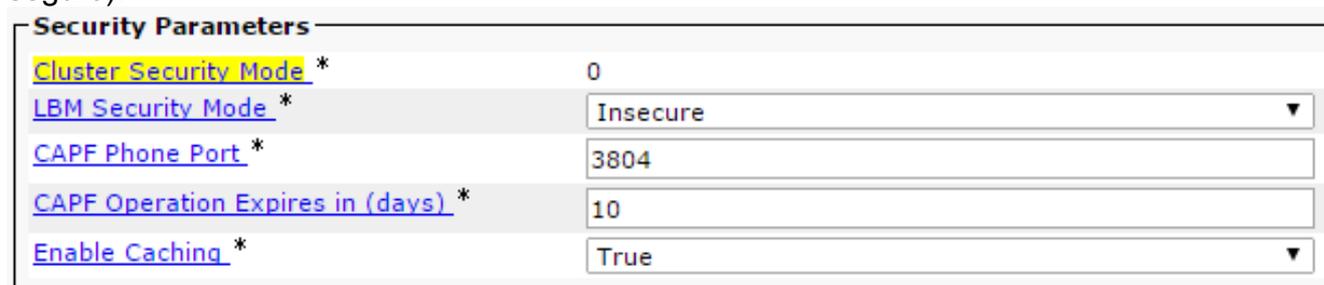
6. O conteúdo do arquivo CTL é exibido. Clique em Finish. Quando solicitada a senha, digite **Cisco123**.



7. A lista de servidores CUCM em que o arquivo CTL existe é exibida. Clique em Concluído.



8. Escolha **CUCM Admin Page > System > Enterprise Parameters** e verifique se o cluster foi definido para o modo não seguro ("0" indica não seguro).



9. Reinicie os serviços TFTP e Cisco CallManager em todos os nós no cluster que executa esses serviços.
10. Reinicie todos os telefones IP para que possam obter a nova versão do arquivo CTL do CUCM TFTP.

Altere a segurança de cluster do CUCM do modo misto para o modo não seguro com a CLI

Essa configuração é somente para o CUCM versão 10.X e posterior. Para definir o modo de segurança de cluster do CUCM como Não seguro, insira o comando **utils ctl set-cluster non-**

secure-mode na CLI do editor. Após a conclusão, reinicie os serviços TFTP e Cisco CallManager em todos os nós no cluster que executa esses serviços.

Este é um exemplo de saída CLI que mostra o uso do comando.

```
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:
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Para verificar o CTLFile.tlv, você pode usar um dos dois métodos:

- Para verificar o conteúdo e a soma de verificação MD5 do CTLFile.tlv presente no lado do CUCM TFTP, insira o comando **show ctl** na CLI do CUCM. O arquivo CTLFile.tlv deve ser o mesmo em todos os nós do CUCM.
- Para verificar a soma de verificação MD5 no telefone IP 7975, escolha **Settings > Security Configuration > Trust List > CTL File**.

Note: Quando você verifica o checksum no telefone, você verá MD5 ou SHA1, dependendo do tipo de telefone.

Cluster CUCM definido para modo de segurança - Soma de verificação de arquivo CTL

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

No lado do telefone IP, você pode ver que ele tem o mesmo arquivo CTL instalado (soma de verificação MD5 corresponde quando comparado à saída do CUCM).



Cluster do CUCM definido como modo não seguro - Conteúdo do arquivo CTL

Este é um exemplo de um arquivo CTL de um cluster CUCM definido para o modo Não seguro. Você pode ver que os certificados CCM+TFTP estão vazios e não contêm conteúdo. O restante dos certificados nos arquivos CTL não são alterados e são exatamente os mesmos de quando o CUCM foi definido para o modo Misto.

```
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 ISSUERNAM 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 ISSUERNAM 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 ISSUERNAM 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
```

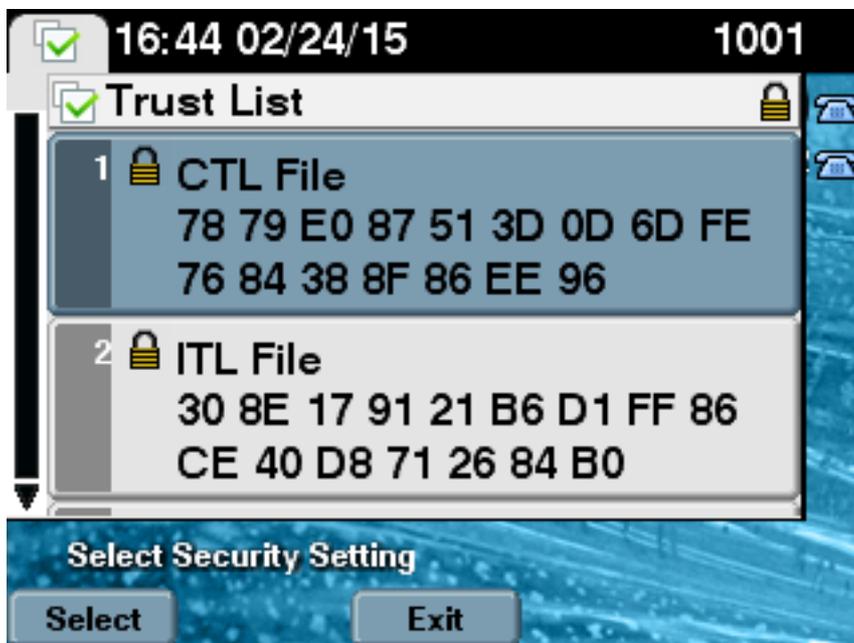
CTL Record #:5

```
-----
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:

No lado do telefone IP, depois que ele foi reiniciado e baixou a versão atualizada do arquivo CTL, você pode ver que a soma de verificação MD5 corresponde quando comparada à saída do CUCM.



Coloque a segurança de cluster CUCM do modo misto para o modo não seguro quando houver perda de tokens USB

Os tokens de segurança para clusters protegidos podem ser perdidos. Nessa situação, você precisa considerar estes dois cenários:

- O cluster executa a versão 10.0.1 ou posterior
- O cluster executa uma versão anterior à 10.x

No primeiro cenário, conclua o procedimento descrito na seção [Alterar a segurança do cluster do CUCM do modo misto para o modo não seguro com a CLI](#) para se recuperar do problema. Como esse comando CLI não requer um token CTL, ele poderia ser usado mesmo se o cluster fosse colocado no modo Misto com o cliente CTL.

A situação fica mais complexa quando uma versão anterior à 10.x do CUCM está em uso. Se você perder ou esquecer a senha de um dos tokens, ainda poderá usar o outro para executar o

cliente CTL com os arquivos CTL atuais. É altamente recomendável obter outro eToken e adicioná-lo ao arquivo CTL assim que possível para fins de redundância. Se você perder ou esquecer as senhas de todos os eTokens listados em seu arquivo CTL, precisará obter um novo par de eTokens e executar um procedimento manual, conforme explicado aqui.

1. Insira o comando **file delete tftp CTLFile.tlv** para excluir o arquivo CTL de todos os servidores 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
```

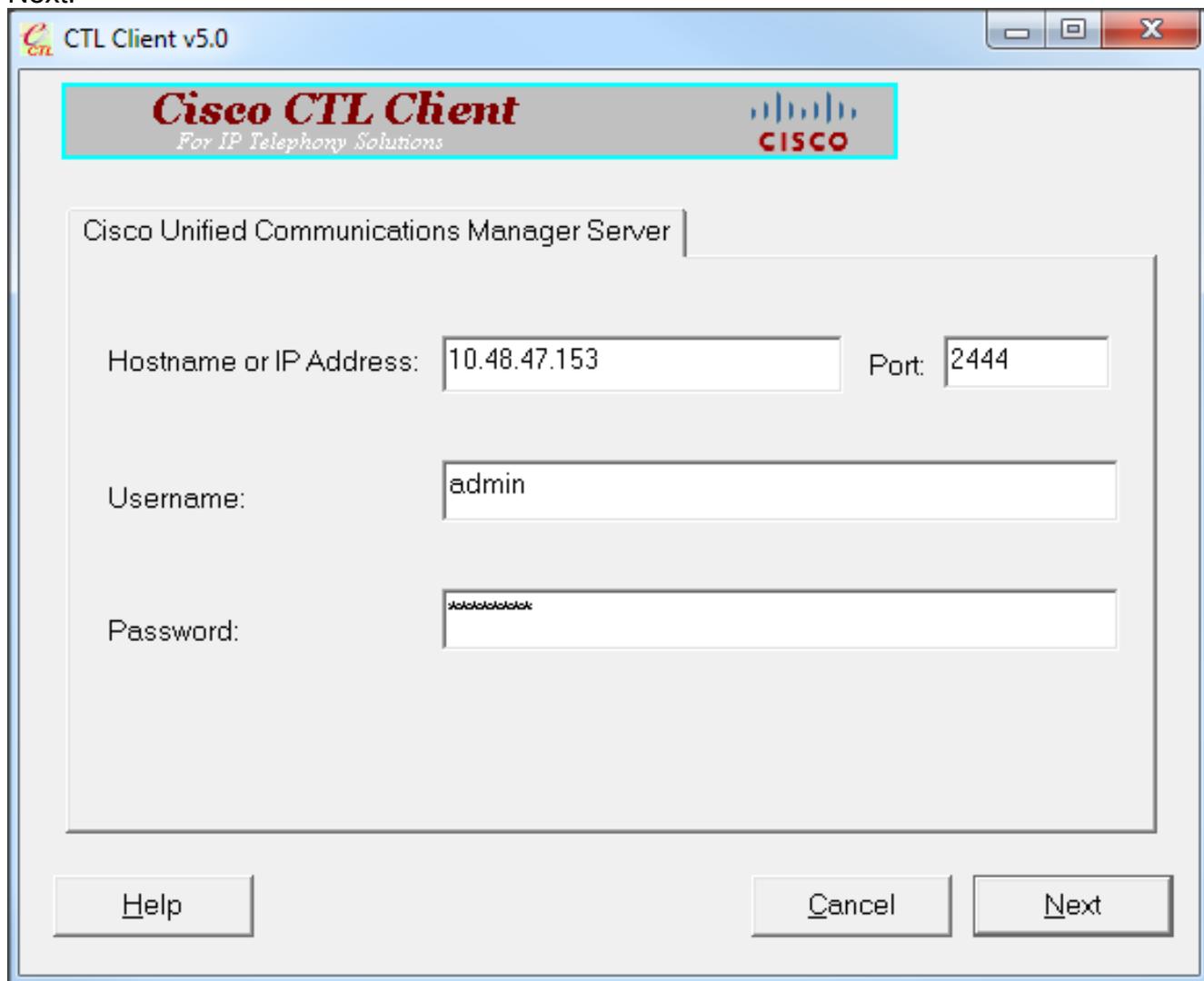
```
Length of CTL file: 0
```

```
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. Execute o cliente CTL. Insira o nome do host IP/endereço da Pub do CUCM e as credenciais de administrador do CCM. Clique em **Next**.



CTL Client v5.0

Cisco CTL Client
For IP Telephony Solutions

Cisco Unified Communications Manager Server

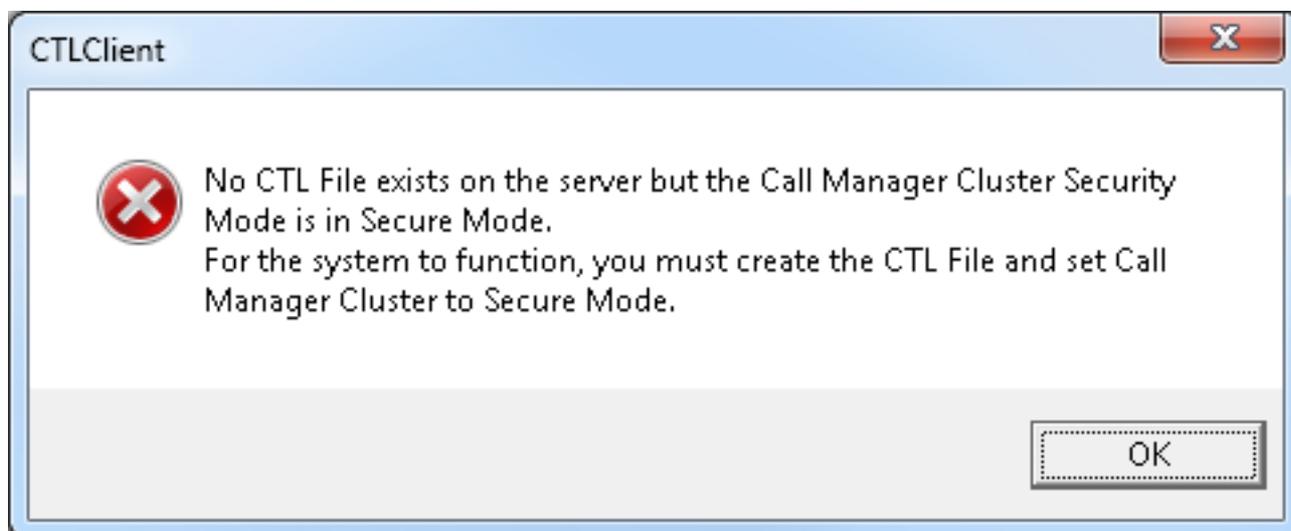
Hostname or IP Address: 10.48.47.153 Port: 2444

Username: admin

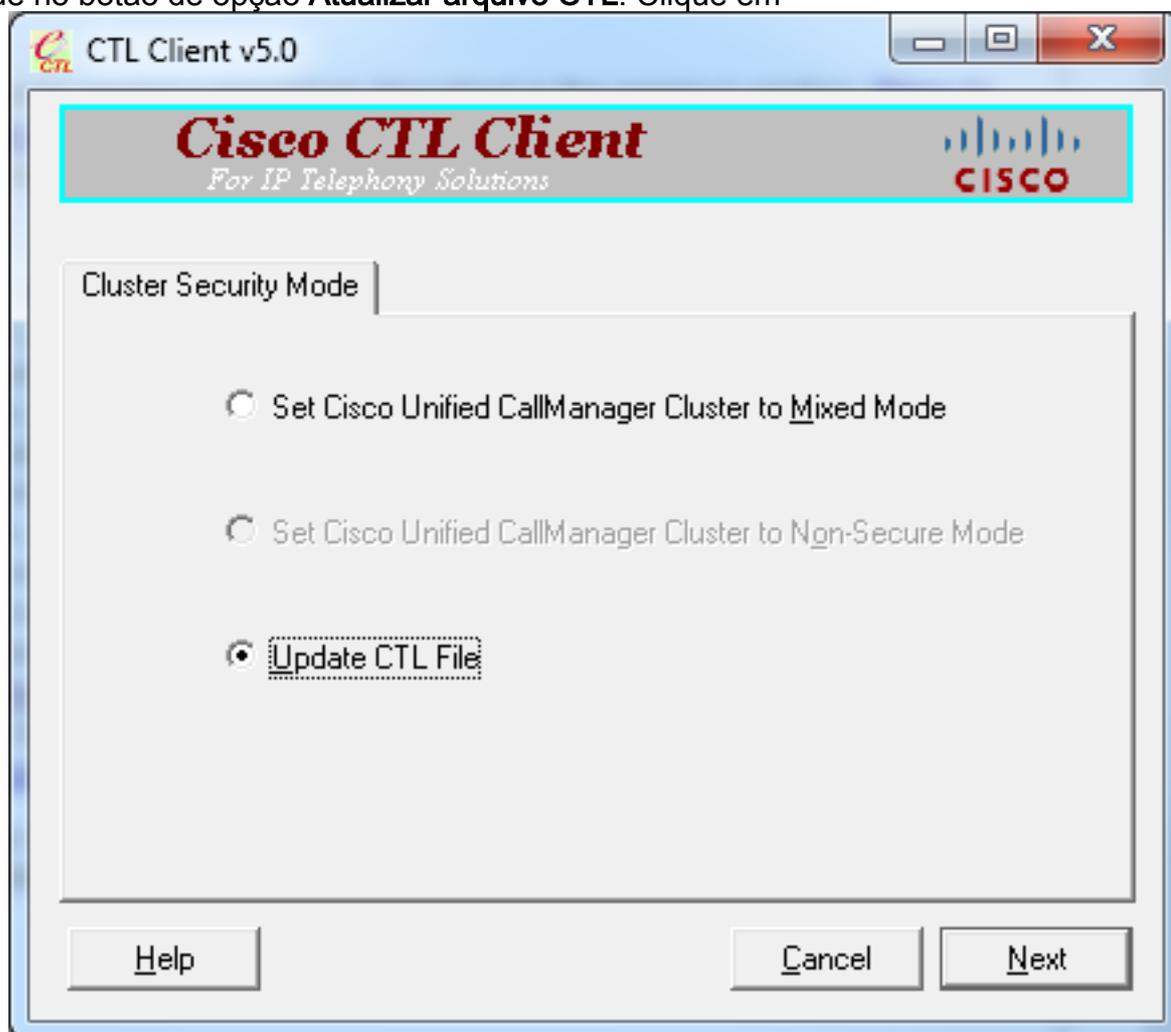
Password: *

Help Cancel Next

3. Como o cluster está no modo Misto, mas não houver nenhum arquivo CTL no Publisher, este aviso será exibido. Clique em **OK** para ignorá-lo e continuar.

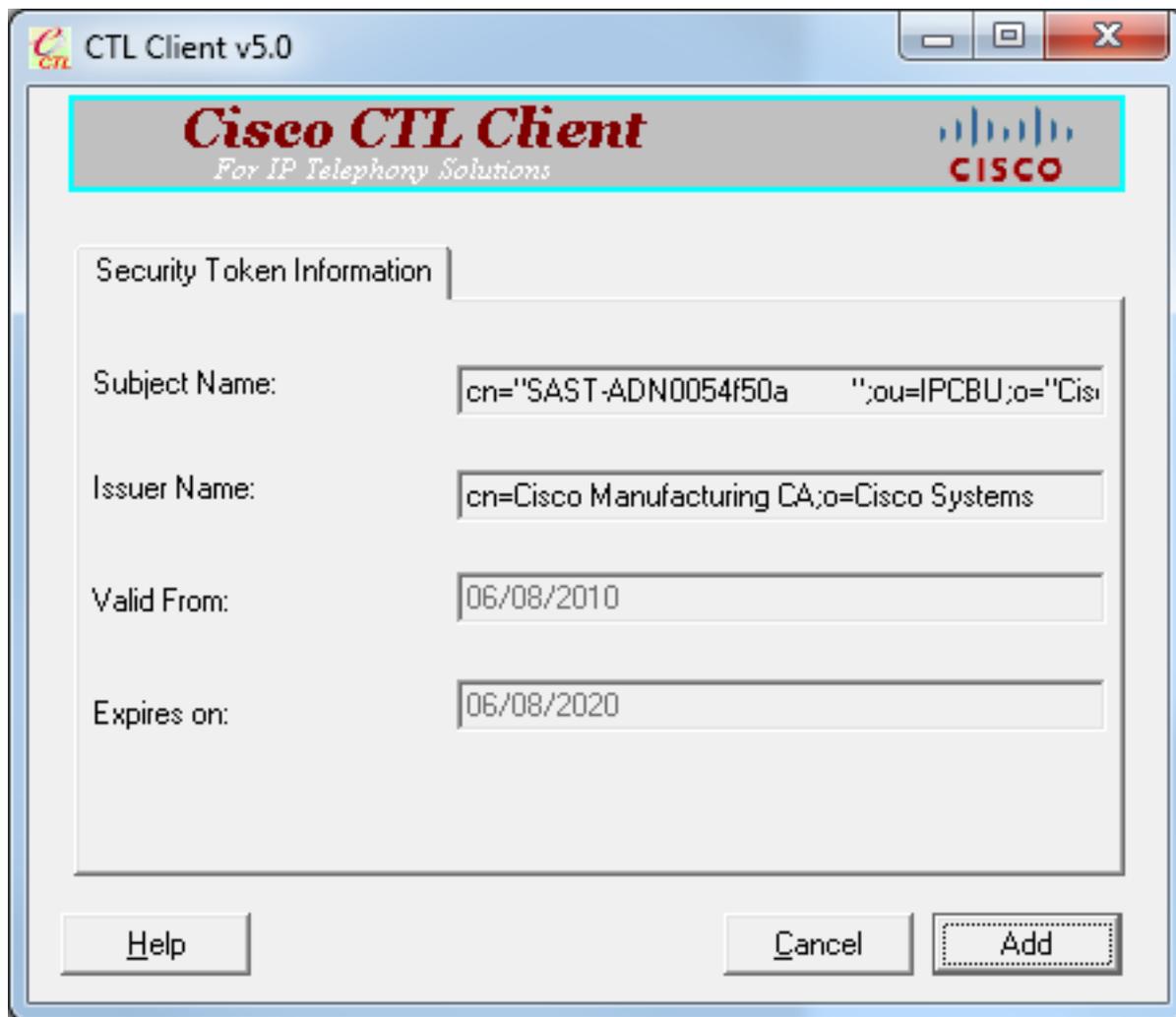


4. Clique no botão de opção **Atualizar arquivo CTL**. Clique em

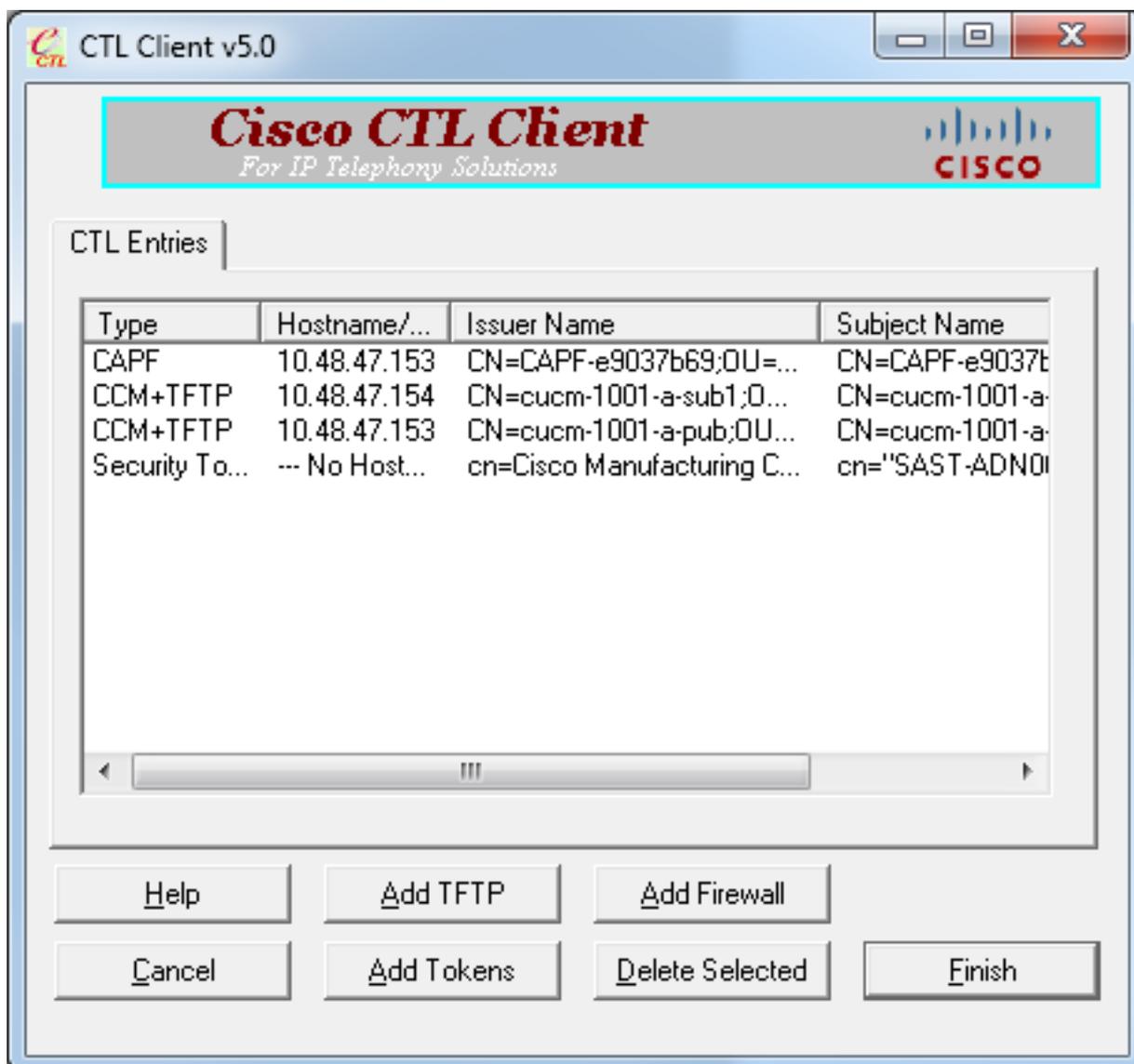


Next.

5. O cliente CTL pede para adicionar um Token de Segurança. Clique em **Add** para continuar.

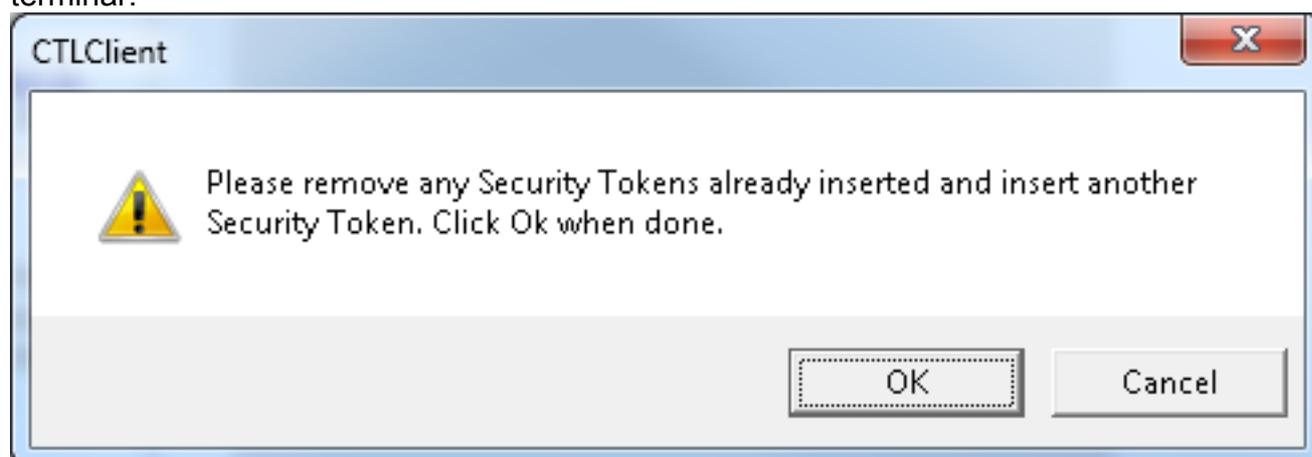


6. A tela exibe todas as entradas na nova lista de certificados confiáveis. Clique em **Add Tokens** para adicionar o segundo token do novo

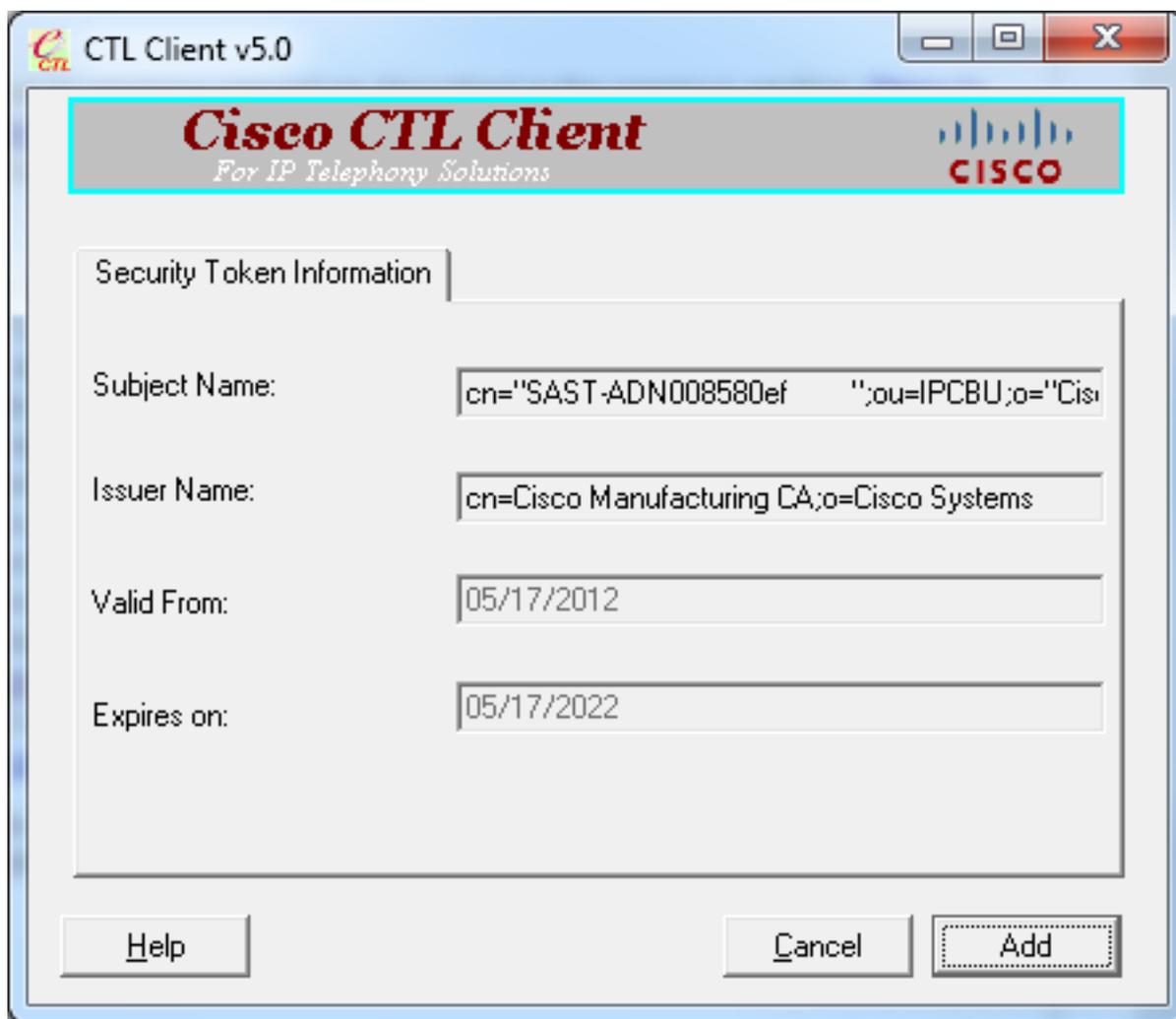


par.

7. Você será solicitado a remover o token atual e inserir um novo. Clique em **OK** quando terminar.

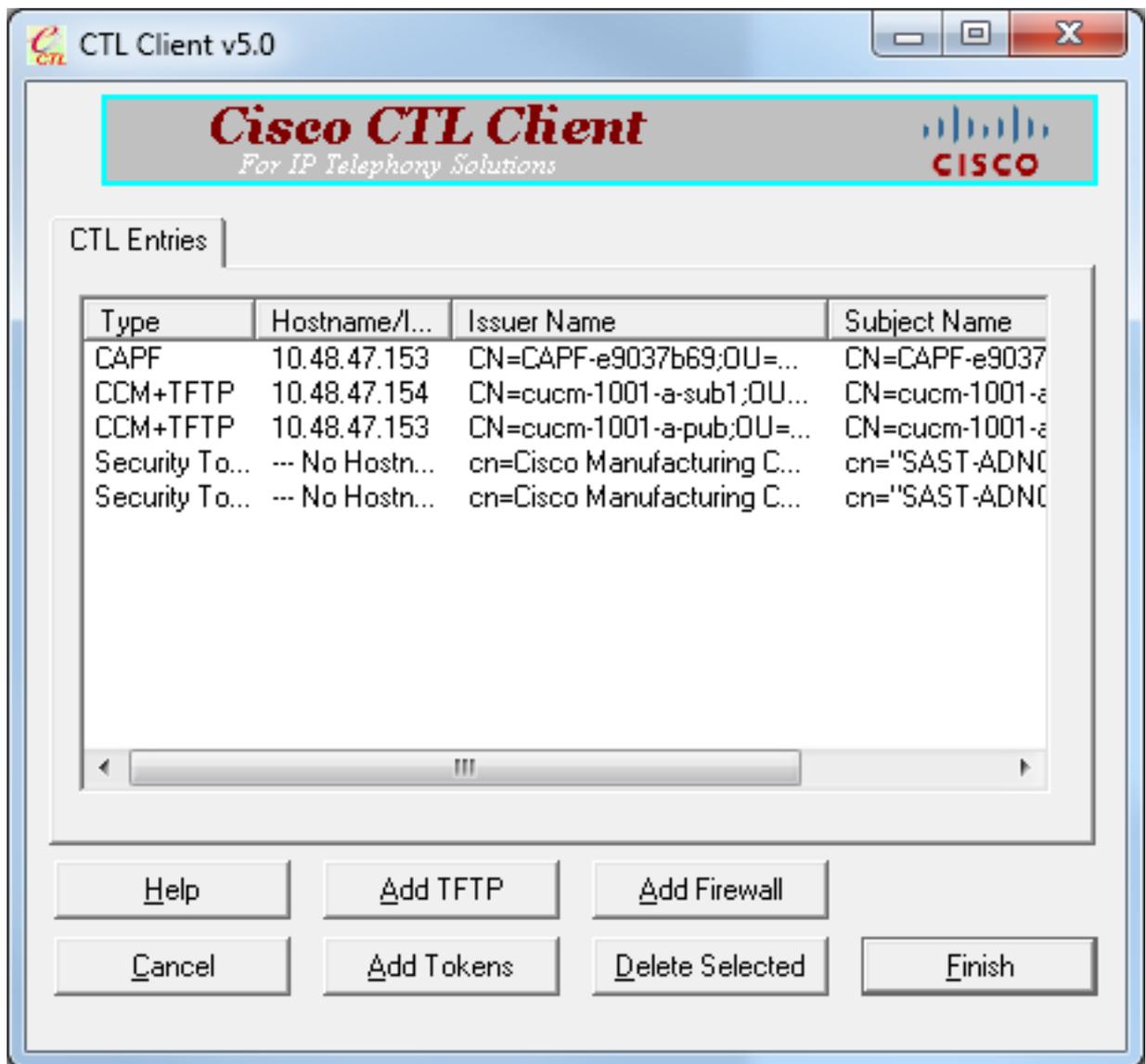


8. Uma tela que mostra detalhes do novo token é exibida. Clique em **Add** para confirmá-los e adicionar este



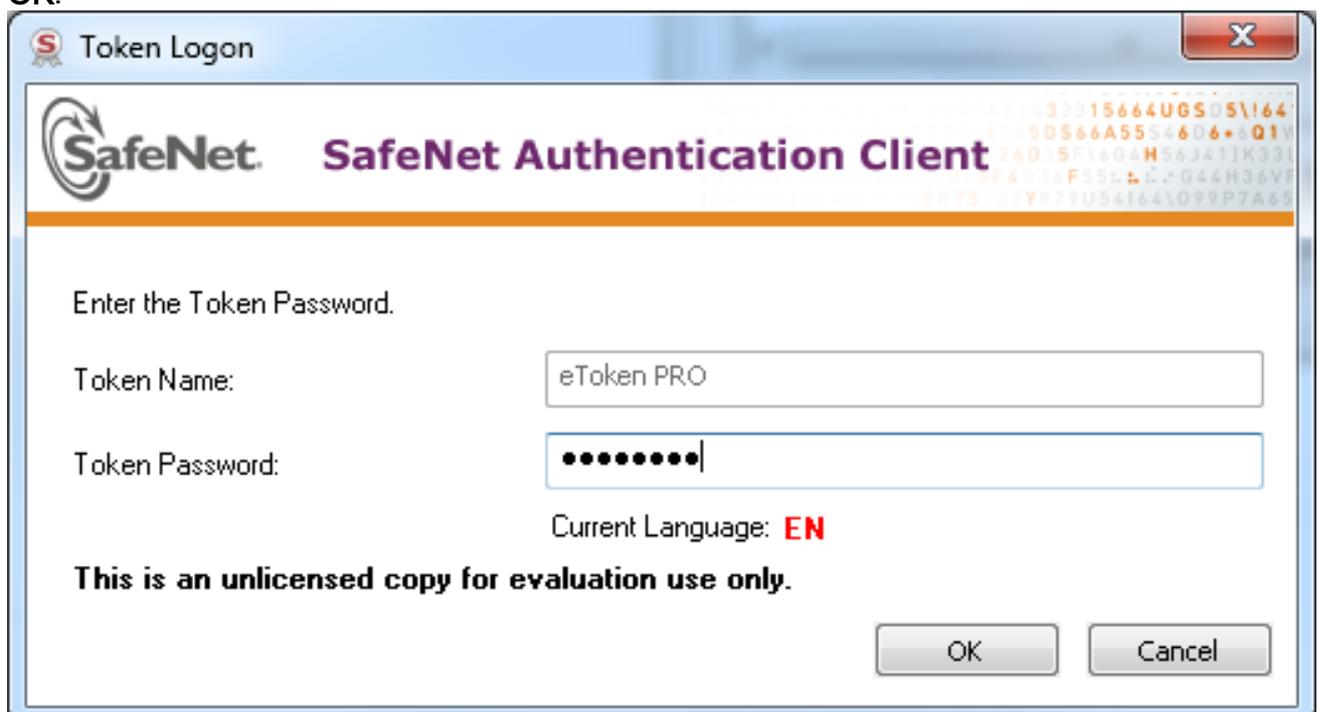
token.

9. Você verá uma nova lista de entradas CTL que mostra os dois Tokens adicionados. Clique em **Finish** para gerar novos arquivos

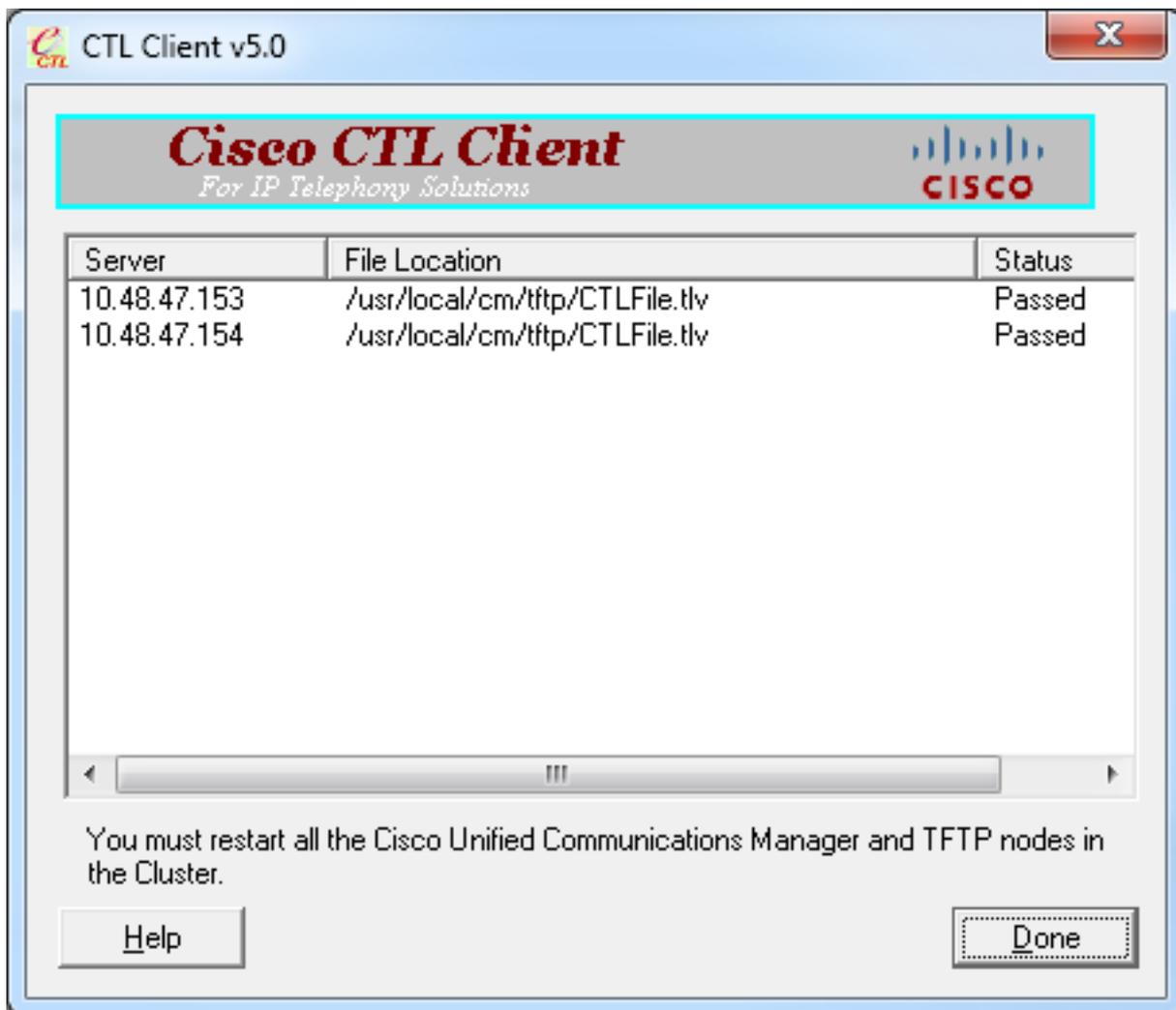


CTL.

- No campo Senha do token, digite **Cisco123**. Clique em **OK**.



- Você verá a confirmação de que o processo foi bem-sucedido. Clique em **Concluído** para confirmar e sair do cliente



CTL.

12. Reinicie o Cisco TFTP seguido pelo serviço CallManager (Cisco Unified Serviceability > Tools > Control Center - Serviços de recursos). O novo arquivo CTL deve ser gerado. Insira o comando **show ctl** para verificação.

```
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. Exclua o arquivo CTL de cada telefone no cluster (esse procedimento pode variar com base no tipo de telefone - consulte a documentação para obter detalhes, como o [Guia de Administração do Telefone IP Unificado da Cisco 8961, 9951 e 9971](#)). **Note:** Os telefones ainda poderão ser registrados (dependendo das configurações de segurança no telefone) e funcionar sem prosseguir com a etapa 13. No entanto, eles terão o arquivo CTL antigo instalado. Isso pode causar problemas se os certificados forem regenerados, outro servidor for adicionado ao cluster ou se o hardware do servidor for substituído. Não é recomendável deixar o cluster neste status.
14. Mova o cluster para Não seguro. Consulte a seção [Alterar a segurança do cluster CUCM do modo misto para o modo não seguro com o cliente CTL](#) para obter detalhes.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta

configuração.