

トークンレスCTLでのCUCM混合モードの移行

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[無保護モードから混合モードへ \(トークンレス CTL\)](#)

[ハードウェア eToken からトークンレスの解決策へ](#)

[トークンレスの解決策からハードウェア eToken へ](#)

[トークンレス CTL の解決策のための証明書の再生成](#)

はじめに

このドキュメントでは、ハードウェアUSB eTokenを使用する場合としない場合のCisco Unified Communications Manager(CUCM)セキュリティの違いについて説明します。

前提条件

要件

CUCM バージョン 10.0(1) 以降の知識があることが推奨されます。また、次のことを確認してください。

- CUCMバージョン11.5.1SU3以降のライセンスサーバは、Cisco Prime License Manager(PLM)11.5.1SU2以降でなければなりません。これは、CUCMバージョン11.5.1SU3では混合モードを有効にするために暗号化ライセンスが必要であり、PLMでは11.5.1SU2まで暗号化ライセンスをサポートしないためです。

詳細については、『[Cisco Prime License Managerリリース11.5\(1\)SU2リリースノート](#)』を参照してください。

- CUCM パブリッシャ ノードのコマンドライン インターフェイス (CLI) への管理アクセス権を持っている。
- 元に戻ってハードウェア eToken の使用に移行する必要があるシナリオのために、ハードウェア USB eToken にアクセスでき、CTL クライアント プラグインが PC にインストールされている。

さらに明確にするために、この要件は、USB eTokenが必要となる状況がある場合にのみ適用されます。ほとんどの人がUSB eTokenを必要とする可能性は非常に低いです。

- クラスタ内の CUCM のすべてのノード間が完全に接続されている。CTL ファイルは SSH

File Transfer Protocol (SFTP) を使用してクラスタ内のすべてのノードにコピーされるので、このことは非常に重要です。

- クラスタ内のデータベース (DB) の複製が正常に動作しており、サーバがデータをリアルタイムに複製している。
- 導入に含まれるデバイスが Security by Default (TVS) をサポートしている。Security by Default がどのデバイスをサポートするか判断するには、Cisco Unified Reporting の Web ページ (<https://<CUCM IP or FQDN>/cucreports/>) から Unified CM Phone 機能リストを使用できます。

 注: Cisco Jabber および多くの Cisco TelePresence または Cisco 7940/7960 シリーズ IP フォンは、現在デフォルトでセキュリティをサポートしていません。デフォルトでセキュリティがサポートされていないデバイスにトークンレス CTL を導入すると、パブリッシャの CallManager 証明書を変更するようなシステムの更新は、CTL が手動で削除されるまで、それらのデバイスの通常の機能を妨げます。7945 および 7965 以降の電話機など、デフォルトのセキュリティをサポートするデバイスでは、パブリッシャの CallManager 証明書が更新されたときに CTL ファイルをインストールできます。これは、これらのデバイスが信頼検証サービス (TVS) を使用できるためです。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CUCM バージョン 10.5.1.10000-7 (2 ノードのクラスタ)
- ファームウェア バージョン SCCP75.9-3-1SR4-1S を持つ、Skinny Client Control Protocol (SCCP) を使用して登録された Cisco 7975 シリーズ IP フォン
- CTL クライアント ソフトウェアを使用してクラスタを混合モードに設定するのに使用される 2 つのシスコのセキュリティ トークン

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

This document describes the difference between Cisco Unified Communications Manager (CUCM) security with and without the use of hardware USB eTokens.

また、このドキュメントでは、トークンレス証明書信頼リスト (CTL) と、変更後にシステムが適切に機能するように使用されるプロセスを含む基本的な実装シナリオについても説明します。

トークンレス CTL は、CUCM バージョン 10.0(1) 以降の新機能で、ハードウェア USB eToken と CTL クライアント プラグインを使用せずに、CUCM の以前のリリースの要件である、IP フォンによる通話のシグナリングやメディアの暗号化を可能にします。

クラスタが CLI コマンドを使用して混合モードになると、CTL ファイルがパブリッシャ ノードの

CCM+TFTP (サーバ) 証明書で署名され、CTL ファイルには eToken 証明書は存在しません。

 注：パブリッシャでCallManager(CCM+TFTP)証明書を再生成すると、ファイルの署名者が変更されます。デフォルトのセキュリティをサポートしていない電話機およびデバイスも、各デバイスからCTLファイルを手動で削除しない限り、新しいCTLファイルを受け入れません。詳細については、このドキュメントの要件セクションにリストされている最後の要件を参照してください。

無保護モードから混合モードへ (トークンレス CTL)

このセクションでは、CLI を使用して CUCM クラスタのセキュリティを混合モードに移行するのに使用されるプロセスについて説明します。

このシナリオに先立ち、CUCM は無保護モードです。つまり、次の出力に示すように、CTL ファイルがどのノードにも存在せず、登録された IP 電話には Identity Trust List (ITL) ファイルのみが設定されています。

```
<#root>
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:
```

 注：クラスタが混合モードでない間にサーバ上でCTLファイルが見つかった場合、これはクラスタが一度混合モードになり、非混合モードに戻されたこと、およびCTLファイルがクラスタから削除されなかったことを意味します。

コマンド `file delete activelog cm/tftpdata/CTLFile.tlv` は、CUCM クラスタのノードから CTL ファイルを削除します。ただし、コマンドは各ノードで入力する必要があります。明確にするために、サーバに CTL ファイルがあり、クラスタが混合モードでない場合にのみ、このコマンドを使用します。

クラスタが混合モードであるかどうかを確認する簡単な方法は、`run sql select paramname,paramvalue from processconfig where paramname='ClusterSecurityMode'` コマンドを使用することです。パラメータ値が 0 の場合、クラスタは混合モードではありません。

```
run sql select paramname,paramvalue from processconfig where paramname='ClusterSecurityMode'  
paramname          paramvalue  
=====  =====  
ClusterSecurityMode 0
```



新しいトークンレス CTL 機能を用いて、CUCM クラスタ セキュリティを混合モードに移行するには、次の手順を実行します。

1. CUCM パブリッシャ ノードの CLI に対する管理アクセス権を取得します。
2. `utils ctl set-cluster mixed-mode` コマンドを CLI に入力します。

```
<#root>
```

```
admin:
```

```
utils ctl set-cluster mixed-mode
```

```
This operation sets 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. [CUCM Admin Page] > [System] > [Enterprise Parameters] に移動し、クラスタが混合モードに設定されているか確認します (1 の値は混合モードを意味します)。

Security Parameters	
Cluster Security Mode *	1
LBM Security Mode *	Insecure ▼
CAPF Phone Port *	3804
CAPF Operation Expires in (days) *	10
Enable Caching *	True ▼

4. TFTP サービスおよび Cisco CallManager サービスを実行しているクラスタ内のすべてのノードで、これらのサービスを再起動します。
5. IP 電話が CUCM TFTP サービスから CTL ファイルを取得できるように、すべての IP 電話を再起動します。
6. CTL ファイルの内容を確認するために、CLI に show ct コマンドを入力します。
7. CTL ファイルの内容からは、CTL ファイル (このファイルはクラスタ内のすべてのサーバで同じ) に署名するために、CUCM パブリッシャ ノードの CCM+TFTP (サーバ) 証明書が使用されていることがわかります。次に出力例を示します。

```
<#root>
```

```
admin:
```

```
show ct1
```

```
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      ISSUENAME      62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
      SERIALNUMBER    16      ST=Małopołska;C=PL
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=Małopołska;C=PL
4      FUNCTION      2

```

CCM+TFTP

```

5      ISSUENAME      62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
      SERIALNUMBER    16      ST=Małopołska;C=PL
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

```

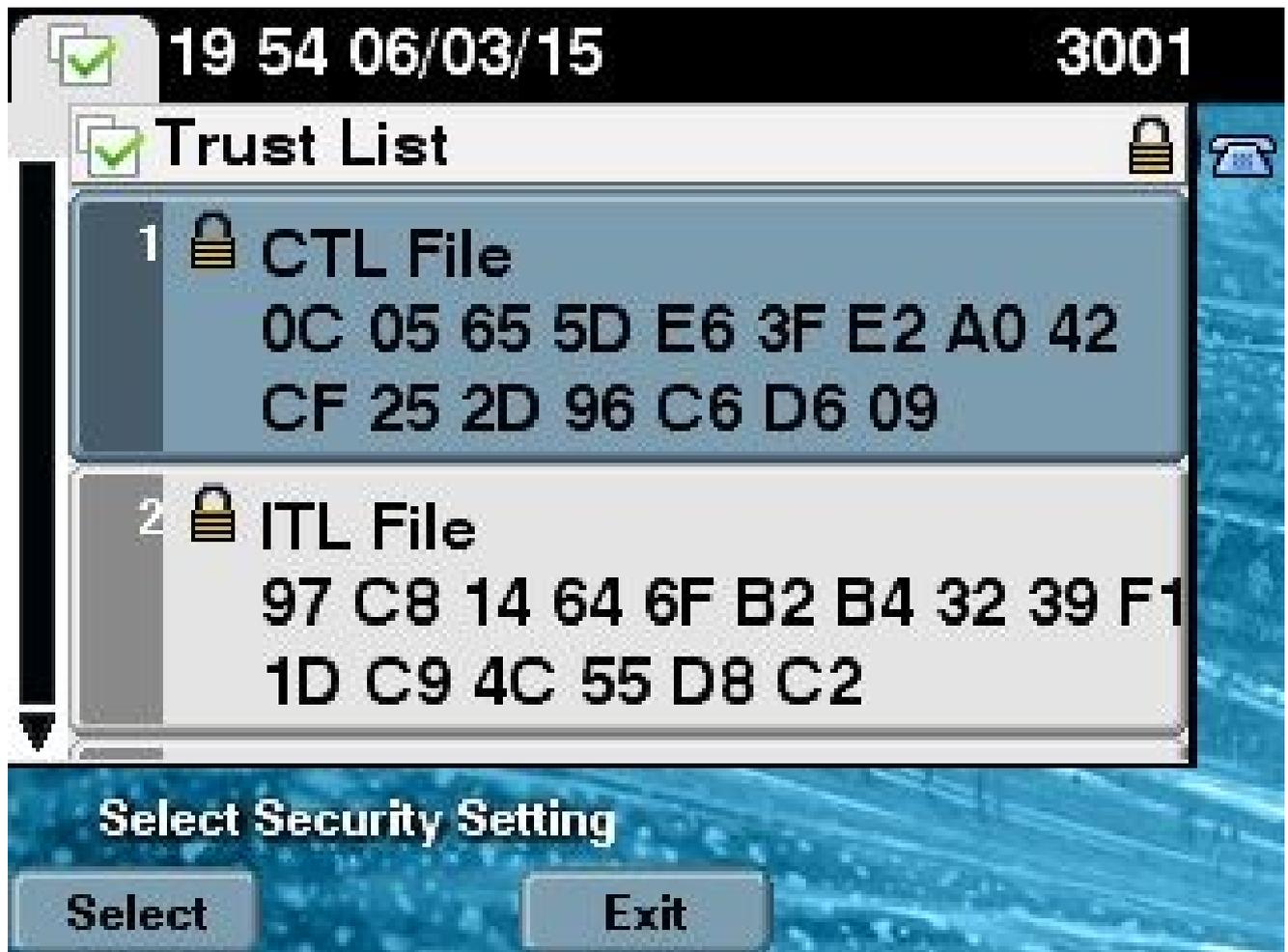
[...]

The CTL file was verified successfully.

- IP 電話側では、サービスを再起動すると、そのサービスによって TFTP サーバ上に存在する CTL ファイルがダウンロードされることを確認できます (CUCM からの出力と比較すると MD5 チェックサムが一致します)。



注：電話のチェックサムを確認すると、電話のタイプに応じてMD5またはSHA1が表示されます。



ハードウェア eToken からトークンレスの解決策へ

このセクションでは、CUCM クラスタ セキュリティをハードウェア eToken から新しいトークンレス ソリューションに移行する方法について説明します。

状況によっては、CTL クライアントを使用して CUCM ですでに混在モードが設定されており、IP 電話は、ハードウェア USB eToken の証明書を含む CTL ファイルを使用している可能性もあります。

このシナリオでは、CTL ファイルがいずれかの USB eToken の証明書によって署名され、IP 電話に設定されています。次に例を示します。

```
<#root>
```

```
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	ISSUENAME	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.



CUCM クラスタ セキュリティをトークンレス CTL の使用に移行するには、次の手順を実行します。

1. CUCM パブリッシャ ノードの CLI に対する管理アクセス権を取得します。
2. `utils ctl update CTLFile` CLI コマンドを入力します。

```
<#root>
```

```
admin:
```

```
utils ctl update CTLFile
```

```
This operation updates 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. TFTP サービスおよび CallManager サービスを実行しているクラスタ内のすべてのノードで、これらのサービスを再起動します。
4. IP 電話が CUCM TFTP サービスから CTL ファイルを取得できるように、すべての IP 電話

を再起動します。

5. CLI に show ctl コマンドを入力し、CTL ファイルの内容を確認します。CTL ファイルの内容からは、CTL ファイルに署名するために、ハードウェア USB eToken の証明書の代わりに CUCM パブリッシャ ノードの CCM+TFTP (サーバ) 証明書が使用されていることがわかります。
6. ここでは、もう 1 点、すべてのハードウェア USB eToken の証明書が CTL ファイルから削除されているという重要な違いがあります。次に出力例を示します。

```
<#root>
```

```
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=Małopolska;C=PL
4	FUNCTION	2	

```
System Administrator Security Token
```

5	ISSUENAME	62	CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow; ST=Małopolska;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=Małopolska;C=PL
4      FUNCTION       2
CCM+TFTP

5      ISSUENAME      62     CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
          ST=Małopolska;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.

 注：出力では、CUCMパブリッシャのCCM+TFTP（サーバ）証明書が署名者ではない場合、Hardware etoken based cluster security modeに戻り、トークンレスソリューションについてもう一度変更を繰り返します。

7. IP 電話側では、IP 電話を再起動すると、その電話によって CTL ファイルの更新されたバージョンがダウンロードされることを確認できます（CUCM からの出力と比較すると MD5 チェックサムが一致します）。



トークンレスの解決策からハードウェア eToken へ

このセクションでは、CUCM クラスタ セキュリティを新しいトークンレスの解決策から元のハードウェア eToken の使用に戻す方法について説明します。

CUCM クラスタ セキュリティが CLI コマンドを使用して混合モードに設定され、CTL ファイルが CUCM パブリッシャ ノードの CCM+TFTP (サーバ) 証明書で署名されると、CTL ファイルにはハードウェア USB eToken 証明書は存在しません。

そのため、CTL クライアントを実行して CTL ファイルを更新する (ハードウェア eToken の使用に戻す) と、次のエラー メッセージが表示されます。

```
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.
```

これは、システムを `utils ctl` コマンドを含まない 10.x バージョン以前にダウングレードする (バージョンを古いものに切り替える) ようなシナリオで特に重要です。

以前の CTL ファイルは、リフレッシュまたは Linux から Linux (L2) へのアップグレードの過程

で移行され (内容は変更されない)、前述のようにこのファイルには eToken 証明書は含まれません。次に出力例を示します。

<#root>

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=Małopolska;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=Małopolska;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=Małopołska;C=PL
4	FUNCTION	2	System Administrator Security Token
5	ISSUERNAME	62	CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow; ST=Małopołska;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=Małopołska;C=PL
4	FUNCTION	2	
CCM+TFTP			
5	ISSUERNAME	62	CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow; ST=Małopołska;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=Małopołska;C=PL
4	FUNCTION	2	CAPF
5	ISSUERNAME	60	CN=CAPF-e41e7d87;OU=TAC;O=Cisco;L=Krakow; ST=Małopołska;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:

このシナリオでは、次の手順を実行し、すべての IP 電話から CTL ファイルを手動で削除するような、失われた eToken のための手順を使用することなく、CTL ファイルを安全にアップグレードしてください。

1. CUCM パブリッシャ ノードの CLI に対する管理アクセス権を取得します。
2. パブリッシャ ノードの CLI に `file delete tftp CTLFile.tlv` command と入力し、CTL ファイルを削除します。

```
<#root>
```

```
admin:
```

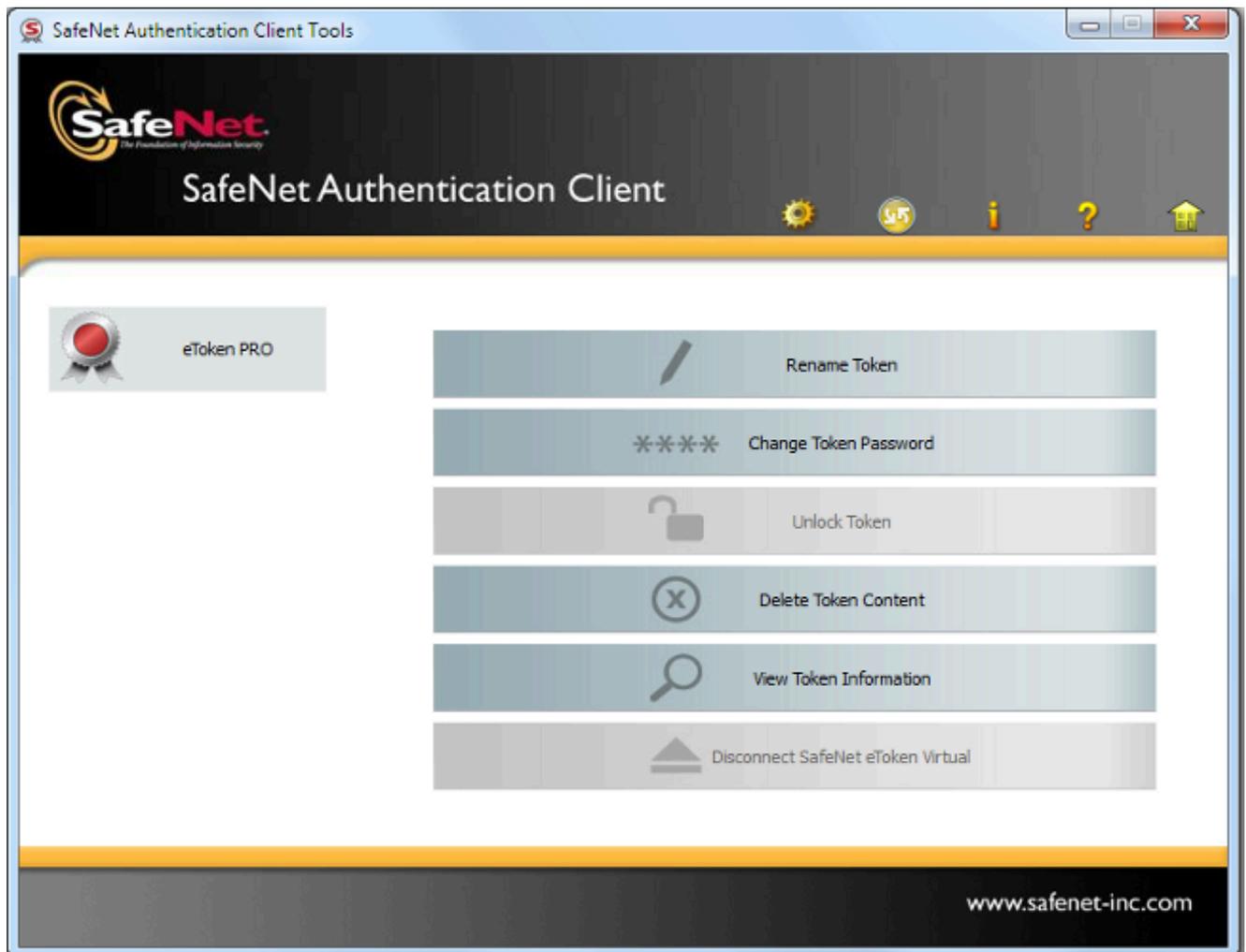
```
file delete tftp CTLFile.tlv
```

```
Delete the File CTLFile.tlv?
```

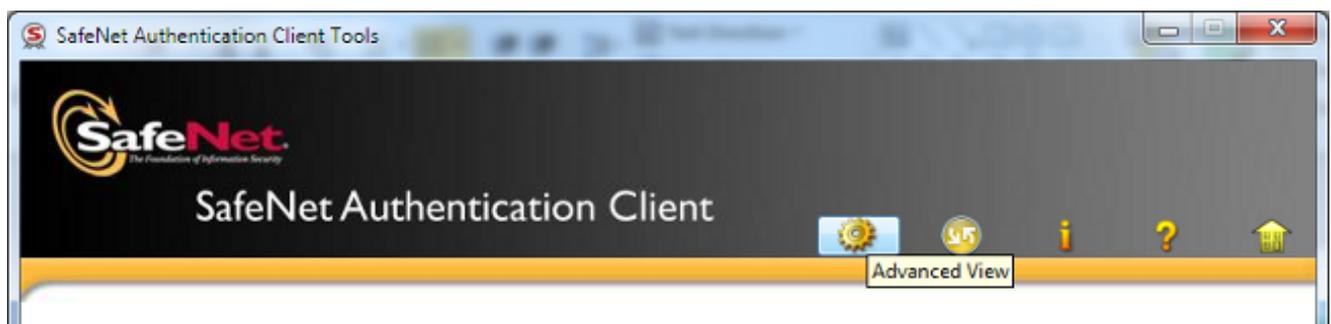
```
Enter "y" followed by return to continue: y
```

```
files: found = 1, deleted = 1
```

3. CTL クライアントがインストールされている Microsoft Windows マシンで SafeNet Authentication Client を開きます (これは、CTL クライアントとともに自動的にインストールされます)

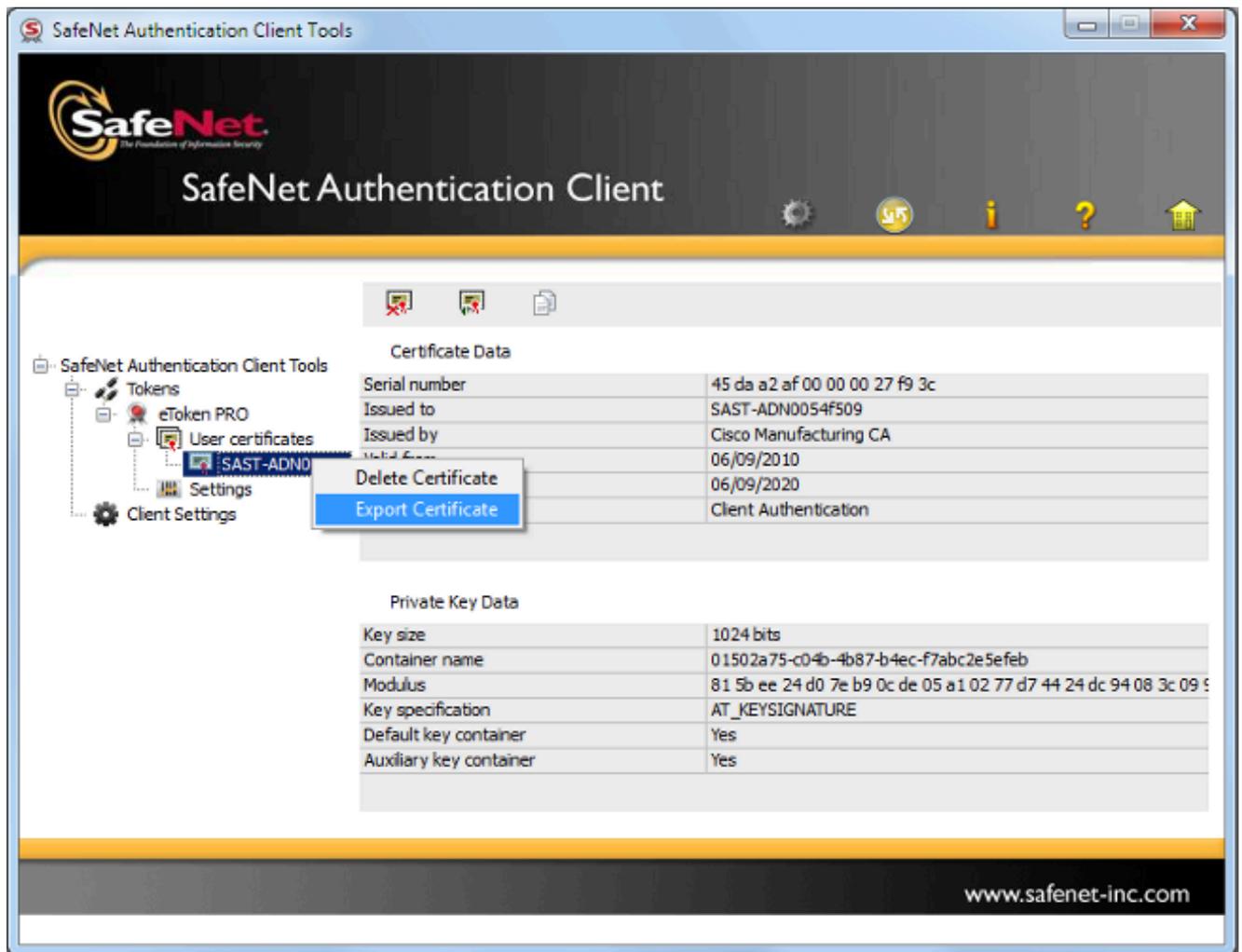


4. SafeNet Authentication Client で [Advanced View] に移動します。



5. 1 番目のハードウェア USB eToken を入力します。

6. User certificates フォルダの下にある証明書を選択し、PC 上のフォルダにそれをエクスポートします。パスワードの入力を求められたら、デフォルト パスワードの Cisco123 を使用します。



7. 2 番目のハードウェア USB eToken に対しても上記の手順を繰り返し、両方の証明書に PC にエクスポートします。

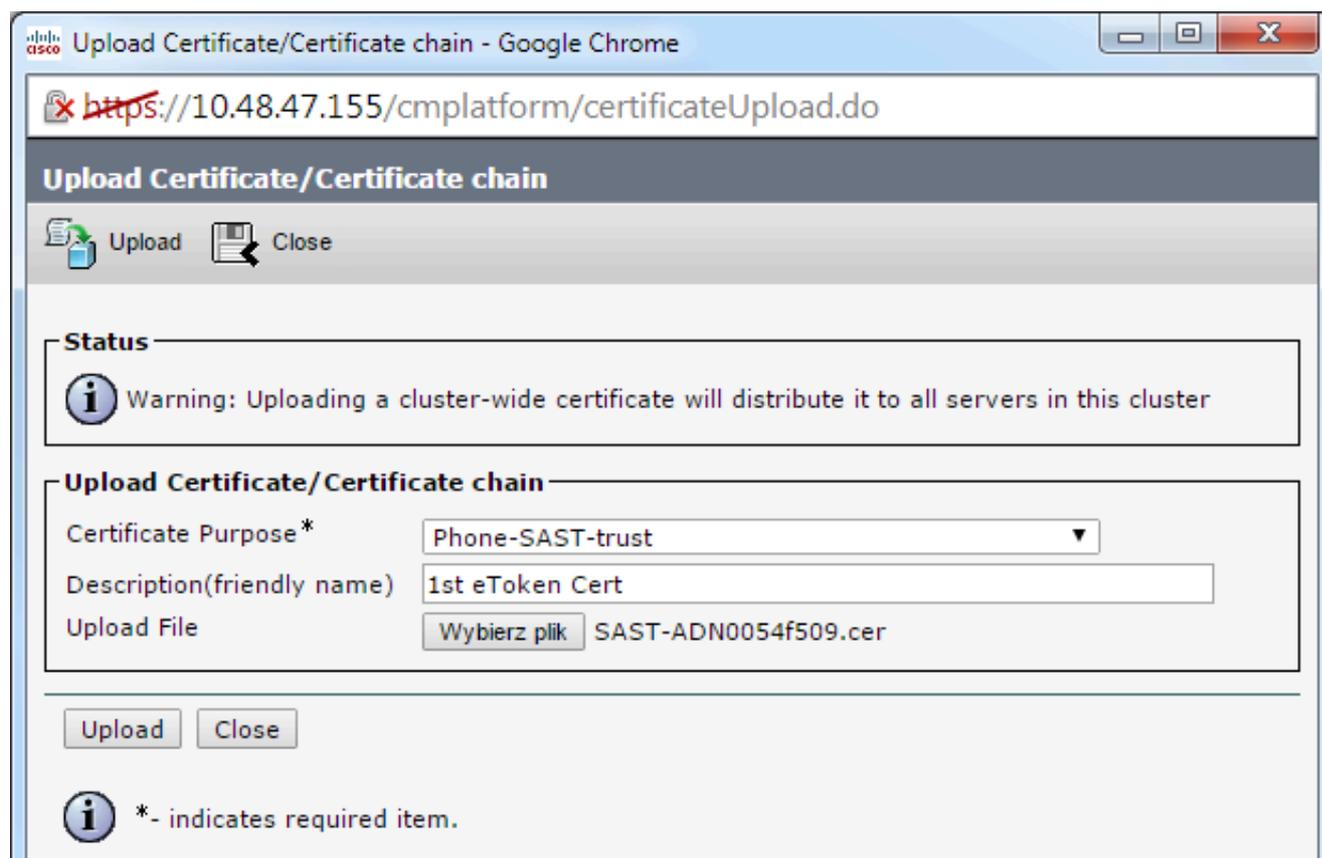
Name	Date modified	Type	Size
SAST-ADN0054f509	06-03-2015 22:32	Security Certificate	1 KB
SAST-ADN008580ef	06-03-2015 22:33	Security Certificate	1 KB

8. Cisco Unified Operating System (OS) Administration にログインし、[Security] > [Certificate Management] > [Upload Certificate] に移動します。



9. [Upload Certificate] ページが表示されます。[Certificate Purpose] ドロップダウンメニュー

から [Phone-SAST-trust] を選択し、1 番目の eToken からエクスポートした証明書を選択します。



Upload Certificate/Certificate chain - Google Chrome

<https://10.48.47.155/cmplatform/certificateUpload.do>

Upload Certificate/Certificate chain

Upload Close

Status

i Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose* Phone-SAST-trust

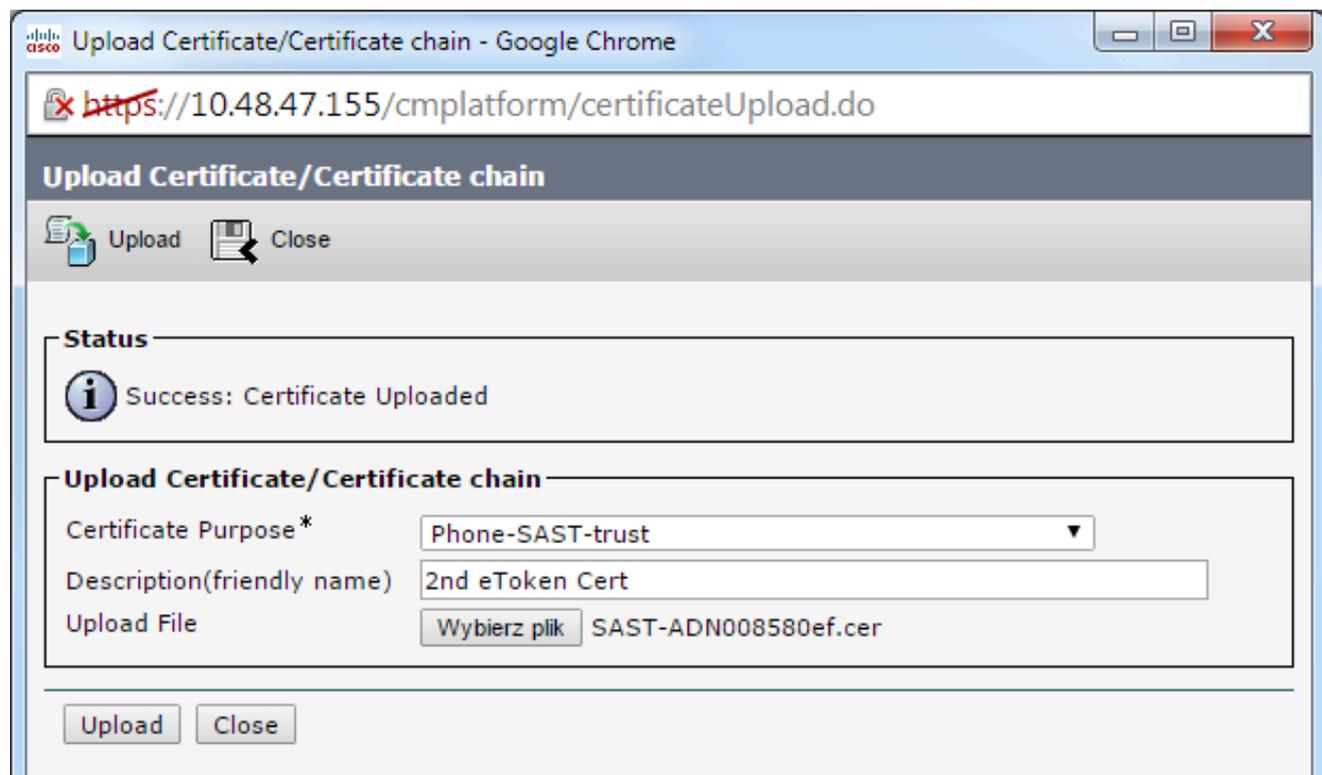
Description(friendly name) 1st eToken Cert

Upload File Wybierz plik SAST-ADN0054f509.cer

Upload Close

i *- indicates required item.

10. 前の手順を実行し、2 番目の eToken からエクスポートした証明書をアップロードします。



Upload Certificate/Certificate chain - Google Chrome

<https://10.48.47.155/cmplatform/certificateUpload.do>

Upload Certificate/Certificate chain

Upload Close

Status

i Success: Certificate Uploaded

Upload Certificate/Certificate chain

Certificate Purpose* Phone-SAST-trust

Description(friendly name) 2nd eToken Cert

Upload File Wybierz plik SAST-ADN008580ef.cer

Upload Close

11. CTL クライアントを実行し、CUCM パブリッシャ ノードの IP アドレス/ホスト名を指定し、CCM 管理者の認証情報を入力します。

Cisco CTL Client
For IP Telephony Solutions

Cisco Unified Communications Manager Server

Hostname or IP Address: 10.48.47.155 Port: 2444

Username: admin

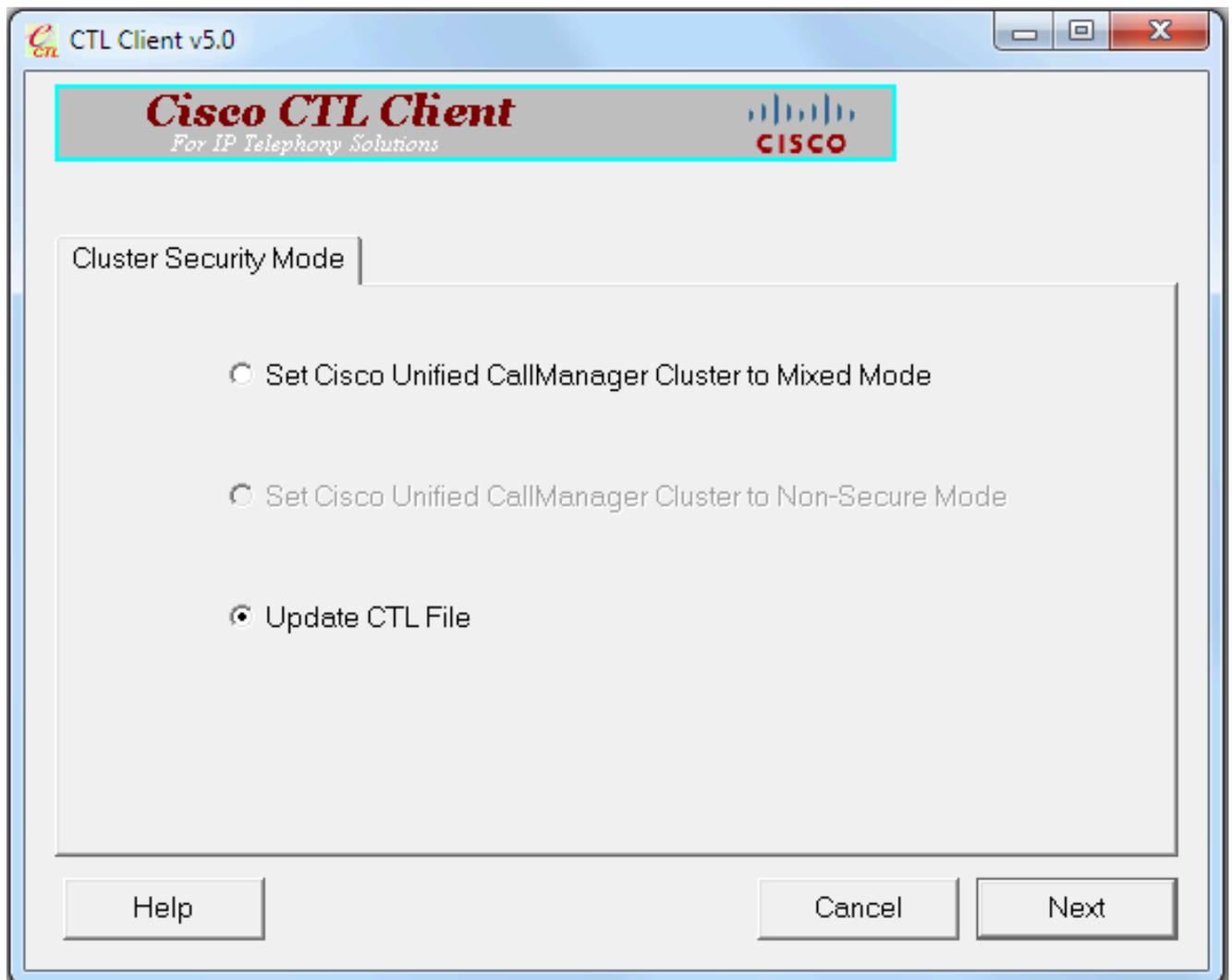
Password: [masked]

Help Cancel Next

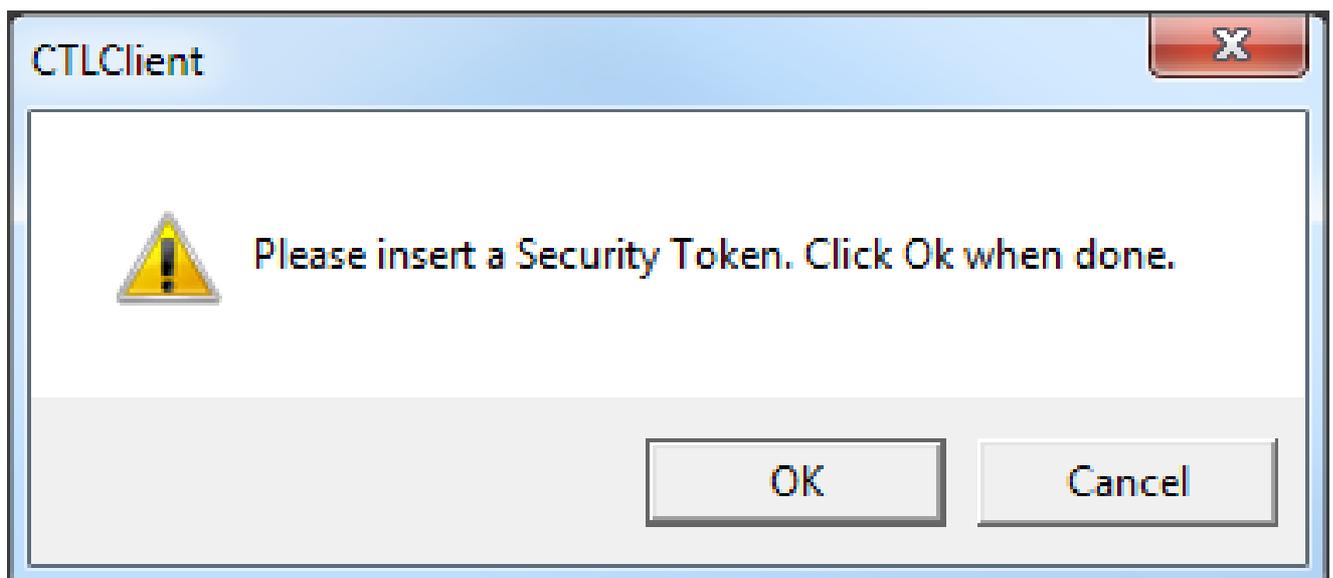
12. クラスタがすでに混在モードになっているけれども、CTL ファイルがパブリッシャ ノード上に存在しないため、この警告メッセージが表示されます (無視するには [OK] をクリックします)。

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.

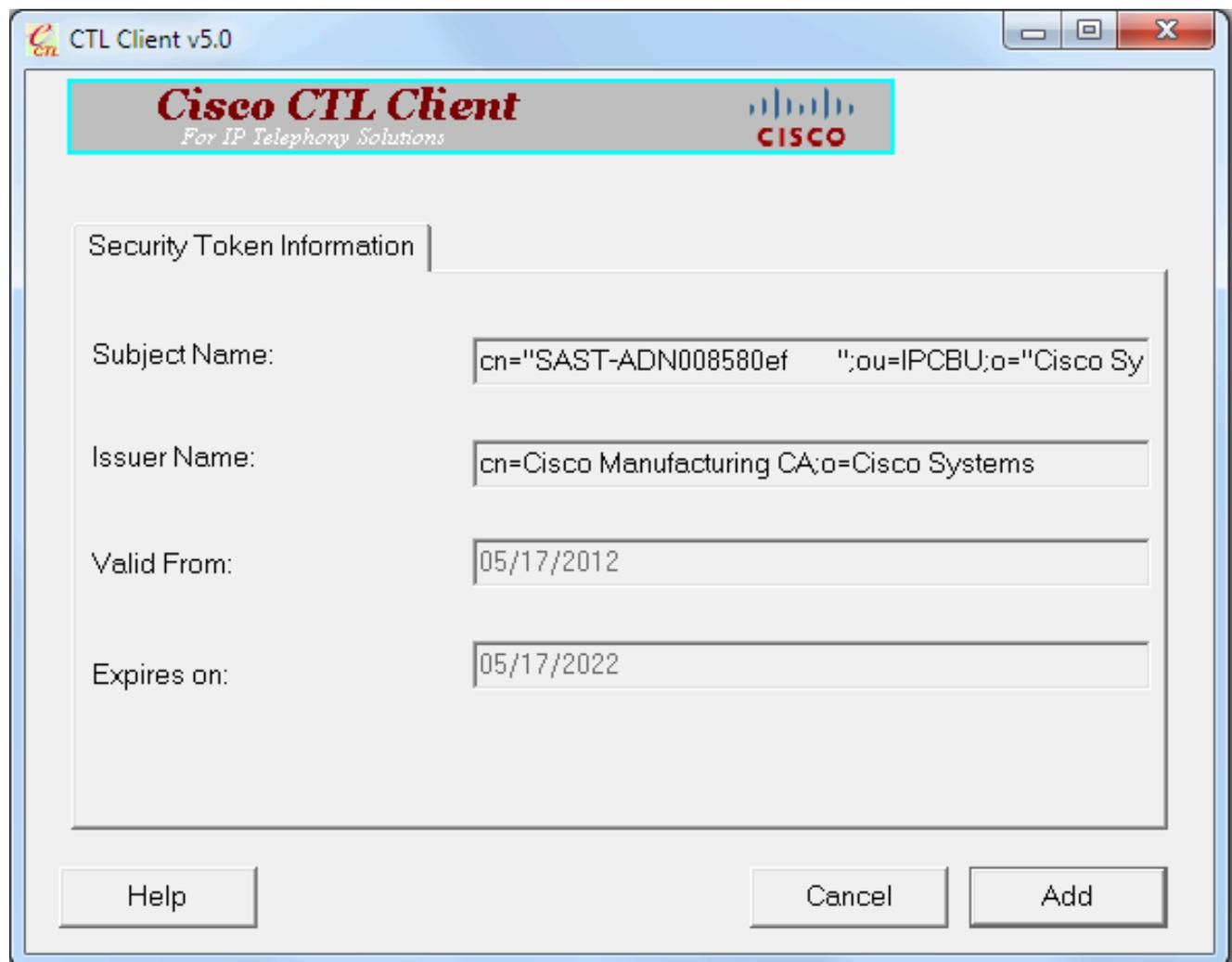
13. CTLクライアントで、Update CTL Fileオプションボタンをクリックし、次にNextをクリックします。



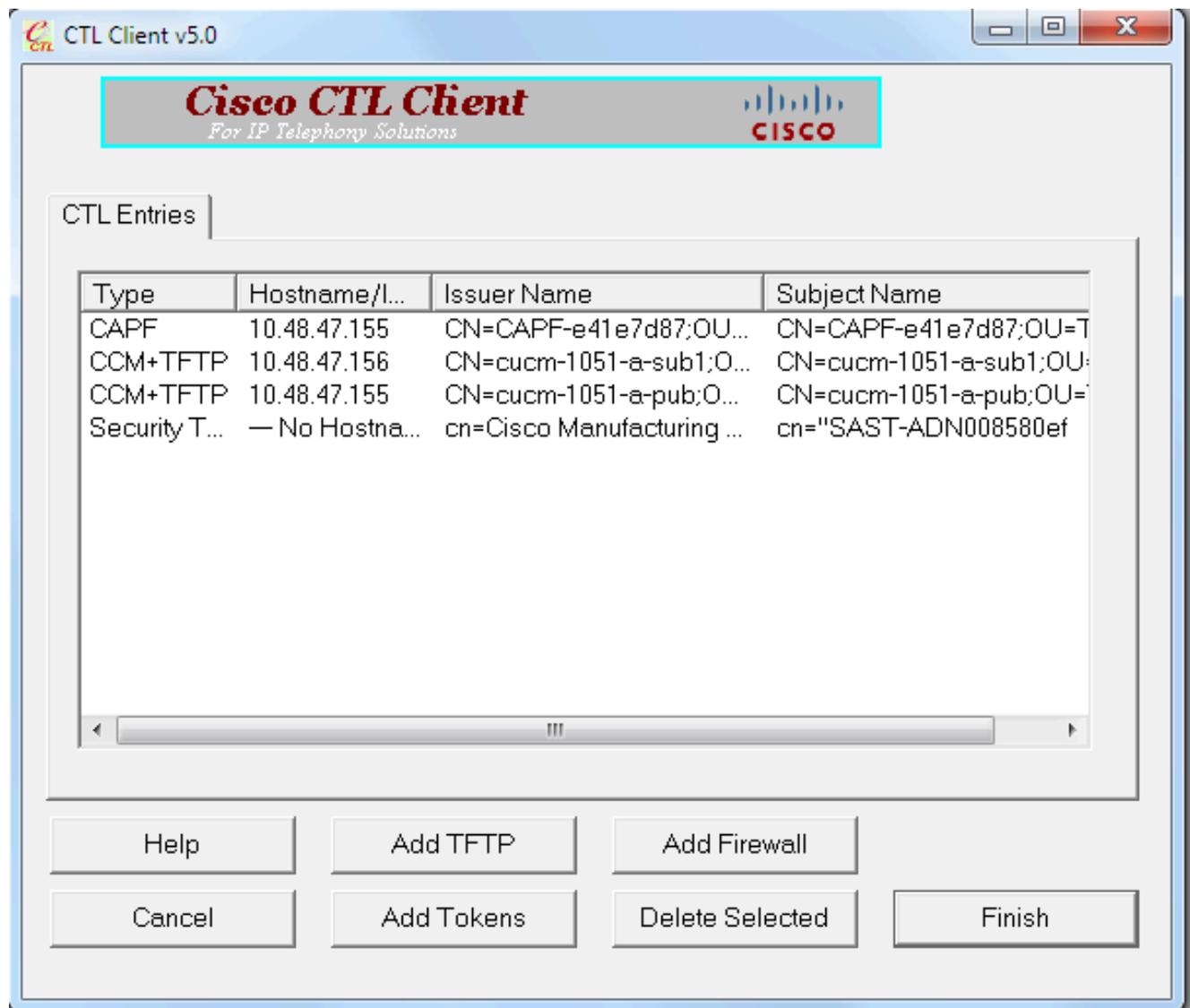
14. 1 番目のセキュリティ トークンを入力し、[OK] をクリックします。



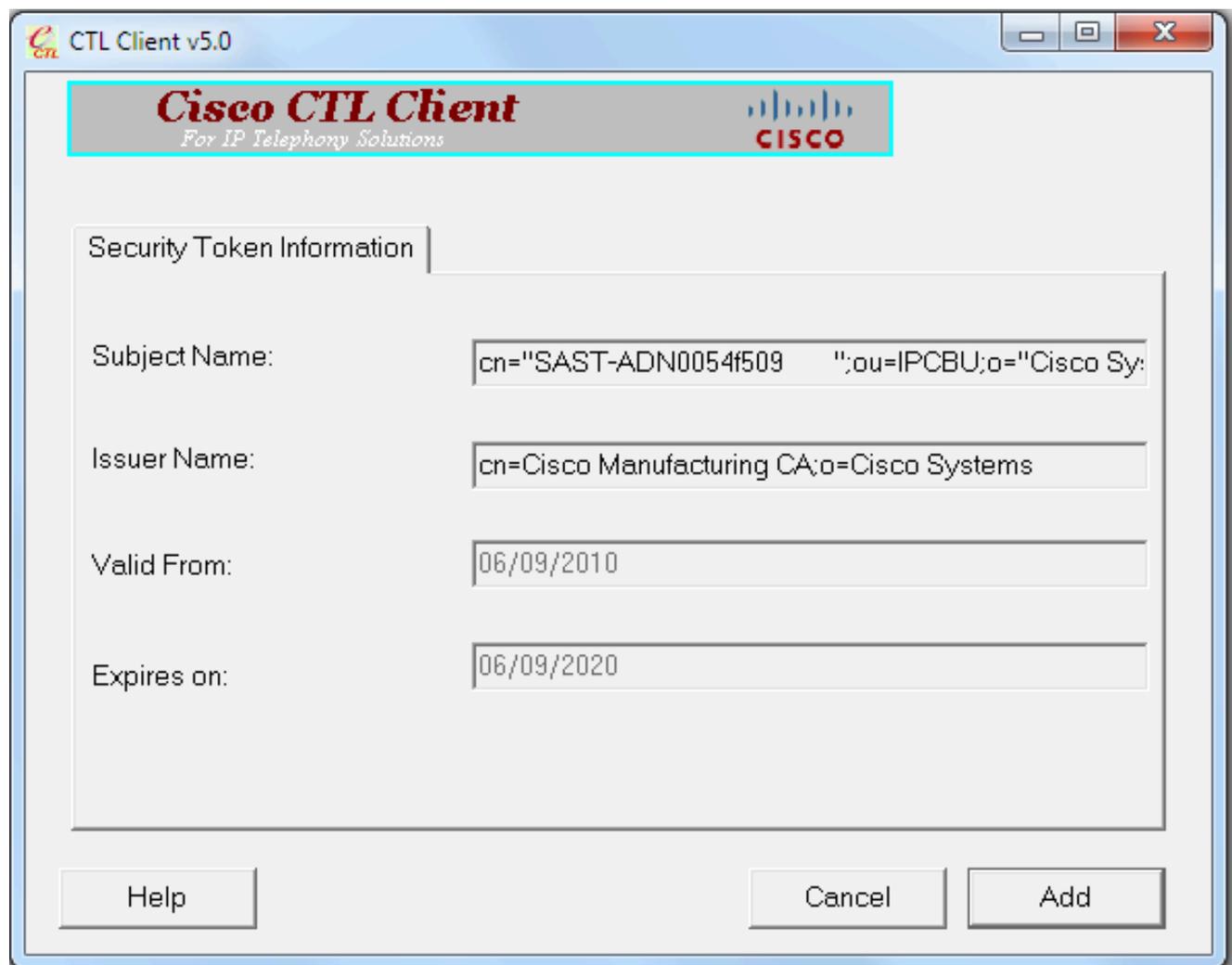
15. セキュリティ トークンの詳細が表示されたら、[Add] をクリックします。



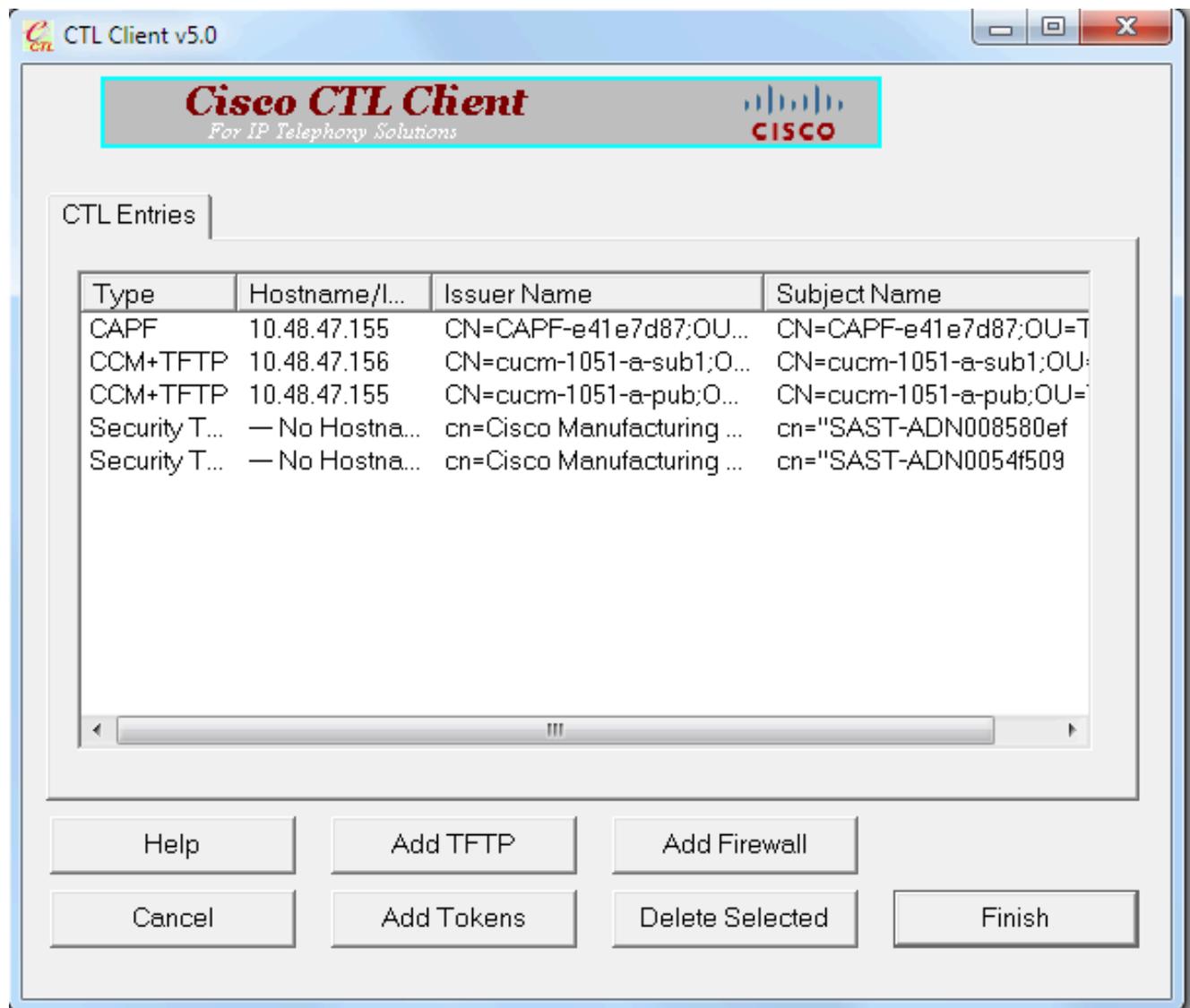
16. CTL ファイルの内容が表示されたら、[Add Tokens] をクリックし、2 番目の USB eToken を追加します。



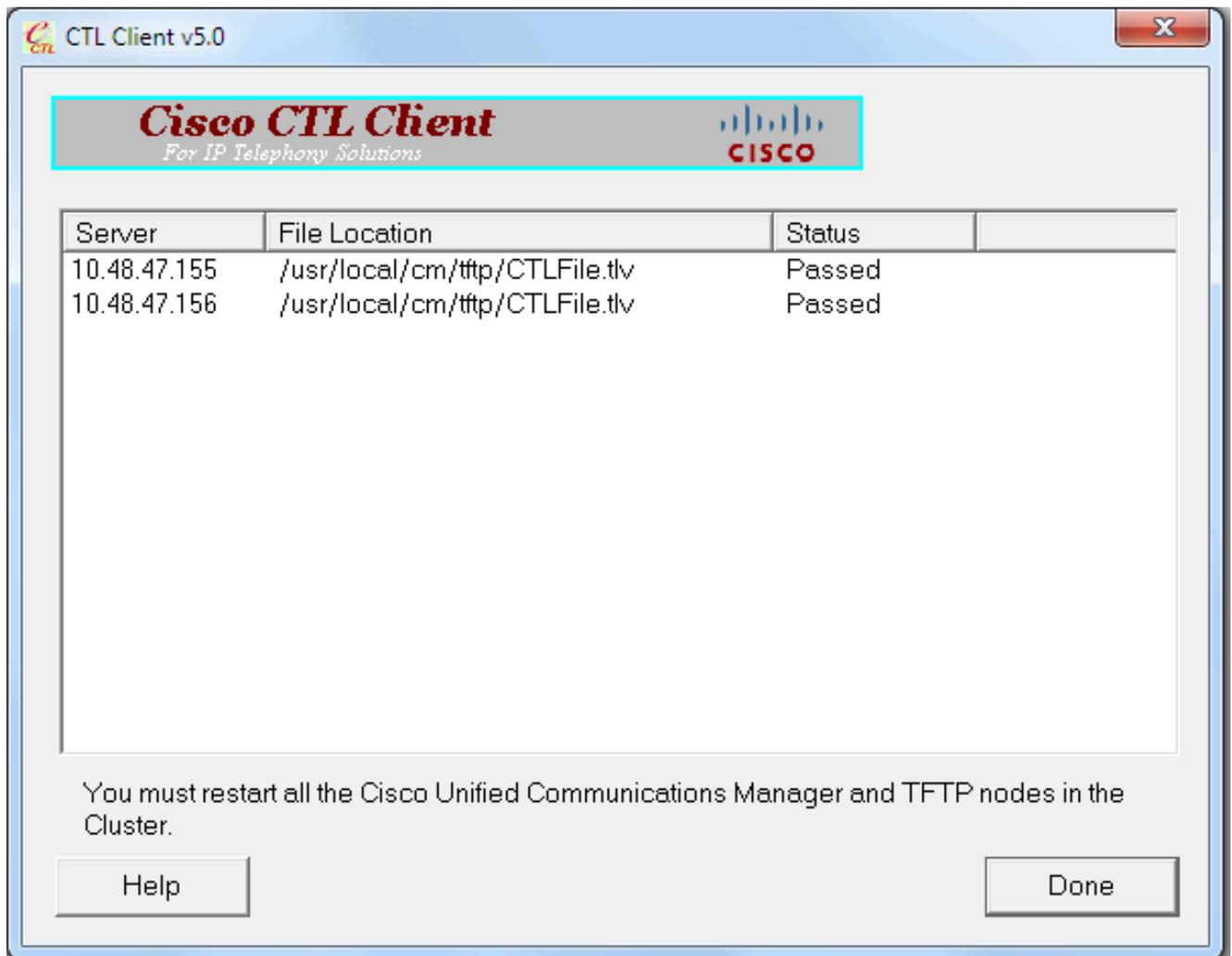
17. セキュリティ トークンの詳細が表示されたら、[Add] をクリックします。



18. CTL ファイルの内容が表示されたら、[Finish] をクリックします。パスワードを求めるプロンプトが表示されたら、「Cisco123」と入力します。



19. CTL ファイルが存在する CUCM サーバのリストが表示されたら、[Done] をクリックします。



20. TFTP サービスおよび CallManager サービスを実行しているクラスタ内のすべてのノードで、これらのサービスを再起動します。
21. IP 電話が CUCM TFTP サービスから新しいバージョンの CTL ファイルを取得できるように、すべての IP 電話を再起動します。
22. CTL ファイルの内容を確認するために、CLI に show ct コマンドを入力します。CTL ファイルには、両方の USB eToken の証明書が含まれます (そのうちの 1 つは、CTL ファイルに署名するために使用されます)。次に出力例を示します。

```
<#root>
```

```
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	ISSUENAME	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	ISSUENAME	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. IP 電話側では、IP 電話を再起動すると、その電話によって CTL ファイルの更新されたバー

ジョンがダウンロードされることを確認できます (CUCM からの出力と比較すると MD5 チェックサムが一致します)。



この変更が可能なのは、以前、eToken 証明書をエクスポートし、CUCM 証明書信頼ストアにアップロードしたためです。IP 電話は、CTL ファイルに署名するために使用されるこの不明な証明書を CUCM で実行中の Trust Verification Service (TVS) に対して確認できます。

このログ スニペットは、Phone-SAST-trust としてアップロードされており、信頼されている不明な eToken 証明書の検証リクエストを使用して、IP 電話が CUCM TVS にコンタクトする方法について説明します。

```
<#root>
```

```
//
```

```
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: 83E908000005545AF31
23:00:22.052 | debug CertificateDBCache::getCertificateInformation - Looking up the
certificate cache using Unique MAP ID : 83E908000005545AF31cn=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 : 83E908000005545AF31cn=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
```

トークンレス CTL の解決策のための証明書の再生成

このセクションでは、トークンレス CTL の解決策を使用する場合に、CUCM クラスタ セキュリティ証明書を再生成する方法について説明します。

CUCM のメンテナンスの過程で、CUCM パブリッシャ ノードである CallManager の証明書が変更されることがあります。

この現象が発生する可能性のあるシナリオとしては、ホスト名の変更、ドメインの変更、または単に証明書の再生成 (証明書の有効期限の終了に起因) が挙げられます。

CTL ファイルが更新されると、IP 電話にインストールされている CTL ファイルに存在する証明書とは異なる証明書で署名されます。

通常、この新しいCTLファイルは受け入れられませんが、CTLファイルに署名するために使用される不明な証明書をIP Phoneが検出すると、IP PhoneはCUCMのTVSサービスに接続します。

 注:TVSサーバリストはIPフォン設定ファイルにあり、IPフォンのデバイスプール(Device Pool) > CallManagerグループからCUCMサーバにマッピングされます。

TVS サーバに対する検証が成功すると、IP 電話は新しいバージョンで CTL ファイルを更新します。これらのイベントは、次のようなシナリオで発生します。

1. CUCM と IP 電話に CTL ファイルが存在します。CTL ファイルに署名するのに、CUCM パブリッシュ ノードの CCM+TFT (サーバ) 証明書が使用されます。

```
<#root>
```

```
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      ISSUENAME       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=Małopolska;C=PL
4	FUNCTION	2	

CCM+TFTP

5	ISSUENAME	62	CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow; ST=Małopolska;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.

Certificate Details for cucm-1051-a-pub, CallManager

 Regenerate  Generate CSR  Download .PEM File  Download .DER File

Status

 Status: Ready

Certificate Settings

File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Self-signed certificate generated by system

Certificate File Data

```
[
Version: V3
Serial Number: 70CAF64E090751B9DF22F49F754FC5BB
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: L=Krakow, ST=Malopolska, CN=cucm-1051-a-pub, OU=TAC, O=Cisco, C=PL
Validity From: Thu Jun 05 18:31:39 CEST 2014
              To: Tue Jun 04 18:31:38 CEST 2019
Subject Name: L=Krakow, ST=Malopolska, CN=cucm-1051-a-pub, OU=TAC, O=Cisco, C=PL
Key: RSA (1.2.840.113549.1.1.1)
Key value:
30818902818100950c9f8791e7677c5bf1a48f1a933549f73ef58d7c0c871b5b77d23a842aa14f5b293
90e586e5945060b109bdf859b4c983cdf21699e3e4abdb0a47ba6f3c04cd7d4f59efeff4a60f6cf3c5db
2ec32988605ae4352e77d647da25fae619dedf9ebb0e0bdd98f8ce70307ba106507a8919df8b8fd9f9
03068a52640a6a84487a90203010001
Extensions: 3 present
```

2. CallManager.pem ファイル (CCM+TFTP 証明書) が再生成され、証明書のシリアル番号が変わったことがわかります。

Certificate Details for cucm-1051-a-pub, CallManager

 Regenerate
  Generate CSR
  Download .PEM File
  Download .DER File

Status

 Status: Ready

Certificate Settings

File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Self-signed certificate generated by system

Certificate File Data

```
[
Version: V3
Serial Number: 6B1D357B6841740B078FEE4A1813D5D6
SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: L=Krakow, ST=Malopolska, CN=cucm-1051-a-pub, OU=TAC, O=Cisco, C=PL
Validity From: Mon Mar 09 17:06:37 CET 2015
To: Sat Mar 07 17:06:36 CET 2020
Subject Name: L=Krakow, ST=Malopolska, CN=cucm-1051-a-pub, OU=TAC, O=Cisco, C=PL
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100c363617e37830eaf5312f4eb3fe68c74e7a037453d26a0514e52476e56d02f78
c19e83623952934279b8dee9b3944a2a43c21714502db749c4141edc4666358974f2248e001e58928
8a608e9a1bc8ef74267e413e03d5d53e61f0705fb564a1dd2744a53840f579a183cd29e9b3e0d5d689
e067b6426c8c8c49078c5c4cc1b6cb6fec83d31ee86661517bf560ef0c01f5ec056db0dcc9746402af2a
b3ed4d66521f6d0b795ac48f78deaafb324dc30962ffa9e96c8615cce6e1a68247f217c83bf324fb3d5c
```

3. CTL ファイルを更新するために、utils ctl update CTLFile コマンドが CLI に入力されます。

```
<#root>
```

```
admin:
```

```
utils ctl update CTLFile
```

```
This operation updates 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. TVS サービスが、新しい CTL ファイルの詳細で、その証明書キャッシュを更新します。

```
<#root>
```

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 ::

6B1D357B6841740B078FEE4A1813D5D6

CN=

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 ::

6B1D357B6841740B078FEE4A1813D5D6

CN=

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. CTL ファイルの内容を確認すると、パブリッシャ ノードの新しい CallManager サーバ証明書でファイルが署名されていることがわかります。

```
<#root>
```

```
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=Małopołska;C=PL
 4 FUNCTION 2

System Administrator Security Token

5 ISSUERNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
 ST=Małopołska;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=Małopołska;C=PL
 4 FUNCTION 2

CCM+TFTP

5 ISSUERNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
 ST=Małopołska;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)

[...]

The CTL file was verified successfully.

6. [Unified Serviceability] ページから、TFTP サービスおよび Cisco CallManager サービスを実行しているクラスタ内のすべてのノードで、これらのサービスが再起動されています。
7. IP 電話が再起動し、CTL ファイルの新しいバージョンに署名するのに使用されている不明な証明書を検証するために、TVS サーバにコンタクトします。

```
<#root>
```

```
//
```

```
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
```

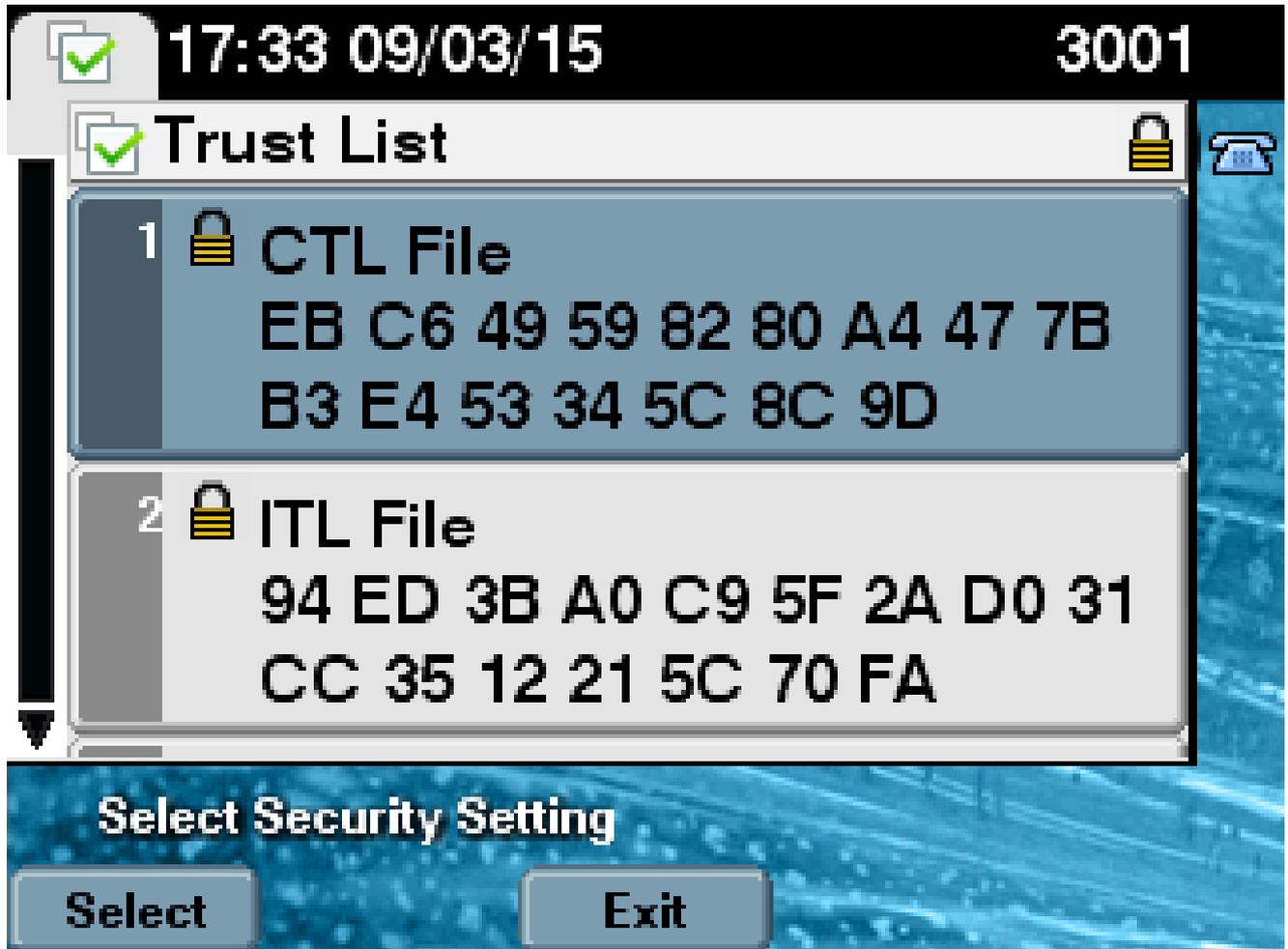
```
//
```

```
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

- 最後に、IP 電話で、CTL ファイルが新しいバージョンで更新されていること、さらには、新しい CTL ファイルの MD5 チェックサムが CUCM のチェックサムと一致することを確認できます。



翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。