Regeneração do certificado CUCM/processo de renovação

Índice

Introdução

Este documento fornece recomendada, um procedimento passo a passo regenerar os Certificados usados na liberação 8.x do gerente das comunicações unificadas de Cisco (CUCM) e mais tarde. A Segurança caracteriza à revelia (a ITL) e o Misturado-MODE (CTL) é seja coberto igualmente a fim evitar todas as indisponibilidade indesejadas. Por exemplo, como evitar as edições ou os telefones do registro do telefone que não aceitam alterações de configuração ou firmware.

> **Caution**: Recomenda-se sempre terminar a regeneração do certificado em uma janela de manutenção.

Visão geral

Este documento discute o processo da regeneração do certificado para estes serviços:

- CallManager

- CAPF (função do proxy do Certificate Authority)
- IPsec
- Tomcat
- TV (serviço da verificação da confiança)
- ITLRecovery (somente para CUCM 10.X e mais tarde)
- telefone-VPN-confiança
- telefone-SAST-confiança
- telefone-confiança
- telefone-CTL-confiança

E também estes Certificados do telefone:

- LSC (localmente - Certificados significativos)
- MIC (Certificados instalados fabricante)

Componentes Utilizados

Todas as saídas e screenshots mostrados neste documento são baseados na liberação 9.1(2)SU2a CUCM, porém o procedimento apresentado pode ser usado com liberação 8.x CUCM e mais tarde. As diferenças que são específico da liberação são mencionadas nas seções apropriadas.

A informação neste documento foi baseada em dispositivos em um ambiente de laboratório que começasse com uma configuração esclarecida (PADRÃO). Se sua rede está viva, certifique-se de que você compreende o impacto potencial do comando any e da ação tomados.

Quando regenerar Certificados

A maioria dos Certificados usados em CUCM depois que uma instalação de atualização é certificados auto-assinados emitidos, à revelia, por cinco anos. Note que o intervalo de tempo de cinco anos atualmente não pode ser alterado para ser um intervalo mais curto do tempo em CUCM. Contudo, um Certificate Authority (CA) pode emitir Certificados para quase toda a escala do tempo.

Há igualmente alguns certificados confiáveis (tais como a CAPF-confiança e a CallManager-confiança) que preloaded e têm um período de validade mais longo. Por exemplo, “Cisco que fabrica CA” certificate é fornecido em lojas da confiança CUCM às características específicas e não expirará até o ano 2029.

Os Certificados devem ser regenerados antes que expirem. Quando os Certificados estão a ponto de expirar você receberá avisos em RTMT (visor de SYSLOG) e um email com notificação será enviado se configurado.

Um exemplo de uma notificação da expiração do certificado que detalhe o certificado de "CUCM01.der" expirará “segunda-feira o 19 de maio 14:46" no server CUCM02 na loja “Tomcat-confiança " da confiança é mostrado aqui:

```
At Fri Sep 05 02:00:56 CEST 2014 on node 192.168.1.2, the following
SyslogSeverityMatchFound events generated:
```

```
SeverityMatch : Critical

MatchedEvent : Sep 5 02:00:06 CUCM02 local7 2 : 864: CUCM02.localdomain:
Sep 05 2014 00:00:06.433 UTC : %UC_CERT-2-CertValidfor7days:
%[Message=Certificate expiration Notification. Certificate name:CUCM01.der
Unit:tomcat-trust Type:own-cert Expiration:Mon May 19 14:46:]
[AppID=Cisco Certificate Monitor][ClusterID=][NodeID=CUCM02]:
Alarm to indicate that Certificate has Expired or Expires in less than seven days

AppID : Cisco Syslog Agent

ClusterID :

NodeID : CUCM02

TimeStamp : Fri Sep 05 02:00:16 CEST 2014
```

Se os Certificados do serviço (as lojas do certificado que não são etiquetados com “- confiança”) são expirados já é ainda possível regenerá-los. Mantenha na mente que os certificados expirados puderam ter um impacto em sua funcionalidade CUCM, dependente da configuração do conjunto. As considerações são discutidas nas próximas seções.

Preste serviços de manutenção ao impacto pela loja do certificado

Écrítico para a boa funcionalidade do sistema ter todos os Certificados actualizados através do conjunto CUCM. Se seus Certificados são expirados ou inválido puderam significativamente afetar a funcionalidade normal do sistema. Uma lista de problemas potenciais que você pôde ter quando alguns dos Certificados específicos forem inválidos ou expirado estiver mostrado aqui. O impacto pôde diferir dependente em cima de sua instalação do sistema.

CallManager.pem

- Telefones cifrados/autenticados não se registram.
- TFTP não confiado (os telefones não aceitam arquivos de configuração assinados e/ou arquivos ITL).
- Os serviços de telefone puderam ser afetados.
- Os troncos do Session Initiation Protocol (SIP) ou os recursos de mídia seguros (bridges de conferência, Media Termination Point (MTP), Xcoders, e assim por diante) não se registrarão nem trabalhar-se-ão.
- O pedido AXL falha.

Tomcat.pem

- Os telefones não podem alcançar os serviços HTTP hospedados no nó CUCM, tal como o diretório corporativo.
- Edições da Web GUI de CUCM, tais como incapaz de alcançar páginas do serviço de outros Nós no conjunto.
- Edições transversais do conjunto da mobilidade de extensão ou da mobilidade de extensão.

CAPF.pem

- Os telefones não autenticam para o telefone VPN, o 802.1x, ou o proxy do telefone.
- Não pode emitir Certificados LSC para os telefones.
- Os arquivos de configuração cifrados não funcionam.

IPSec.pem

- A estrutura da recuperação do sistema da Recuperação de desastres (DR) /Disaster (DRF)

não pôde funcionar corretamente.
- Os túneis de IPsec ao gateway (GW) a outros conjuntos CUCM não funcionam.

TV (serviço da verificação da confiança)

- O telefone não pode autenticar o serviço HTTPS. O telefone não pode autenticar arquivos de configuração (este pode afetar quase tudo em CUCM).

telefone-VPN-confiança

- O telefone VPN não funcionará, porque o HTTPS URL do VPN não pode ser autenticado.

  Note: Se isto não existe não se preocupe. Isto é somente para configurações específicas.

telefone-SAST-confiança

- CTL/eTokens precedente não poderá atualizar ou alterar o CTL.

  Note: Se isto não existe não se preocupe. Isto é somente para configurações específicas.

telefone-confiança e telefone-CTL-confiança

- O Correio de voz visual com Unity ou a conexão de unidade não trabalharão.

  Note: Se isto não existe não se preocupe. Isto é somente para configurações específicas.

LSC e MIC

- Os telefones não se registram, telefone não autenticam para telefonar ao VPN, ao proxy do telefone, ou ao 802.1x.

  Note: Os MIC estão na maioria de modelos do telefone à revelia. Os LSC são assinados no CAPF e últimos cinco anos à revelia. Os clientes de software tais como o CIPC (Cisco IP Communicator) e o Jabber não têm um MIC instalados.

Crie os DR alternativos

Recomenda-se criar os DR alternativos antes que você execute todas as alterações principal como este. Os backup CUCM DRF suportarão todos os Certificados no conjunto. Todo o backup/procedimentos de restauração DR pode ser encontrado em Cisco da “Guia de Administração de Sistema Recuperação de desastres para o gerente das comunicações unificadas de Cisco”.

Caution: Mantenha na identificação de bug Cisco CSCtn50405 da mente, backup CUCM DRF faz não Certificados alternativos.

Determine se o conjunto está no Misturado-MODE

A fim determinar se você executa um conjunto CTL/Secure/Mixed-Mode, escolha a **administração unificada Cisco CM > o sistema > parâmetros de empreendimento > o modo de segurança do conjunto (0 == NON-seguros; 1 modo misturado do ==)**.

Se o conjunto está no Misturado-MODE

Se você executa um conjunto CUCM no Misturado-MODE, este significa que o arquivo CTL precisa de ser afinal mudanças actualizadas do certificado. O procedimento em como fazer isto está dentro da documentação do guia da Segurança de Cisco. Contudo, seja certo que você manda pelo menos um eToken da iniciação original da característica Misturado-MODE e a senha do eToken está sabida.

> **Note**: Uma atualização do CTL não acontece automaticamente (como faz em caso do arquivo ITL). Precisa de ser terminada manualmente pelo administrador com o cliente CTL ou o comando CLI.

Em CUCM 10.X e mais tarde você pode pôr o conjunto no Misturado-MODE em duas maneiras:

- Comando CLI - se este método é usado então seu arquivo CTL é assinado com o certificado CallManager.pem do servidor do publicador.

```
admin:show ctl
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 ISSUERNAME 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.
```

- Cliente CTL - se este método é usado então seu arquivo CTL é assinado com um dos eTokens do hardware.

```
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 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 used to sign the CTL file.
```

Note: Você pode mover-se entre o método usado com modo misturado CUCM com Tokenless CTL.

O dependente em cima do método usado para fixar seu conjunto, um procedimento apropriado da atualização CTL precisa de ser usado. O um ou outro tornado a colocar em funcionamento o cliente CTL ou incorpora o comando de **CTLfile da atualização do ctl dos utils do** CLI.

Verifique a Segurança à revelia no conjunto

A vacância de edições ITL é importante, porque as edições ITL podem fazer com que muitas características falhem ou o telefone recusará habitar por todas as mudanças às configurações. As edições ITL podem ser evitadas nestas duas maneiras.

Utilize “preparam o conjunto para o Rollback à característica de pre 8.0"

Esta característica “anula” para fora sua ITL em todos os server, assim que os telefones confiarão todo o servidor TFTP. Os serviços de telefone (por exemplo, mobilidade de extensão) não funcionarão quando este parâmetro é ajustado para retificar. Contudo, os usuários poderão continuar a fazer e receber chamadas telefônica básicas.

Note: Uma mudança a este parâmetro faz com que TODOS OS TELEFONES RESTAUREM.

Uma vez que esta característica é ajustada, todos os servidores TFTP precisam de ser reiniciados (a fim fornecer a ITL nova) e todos os telefones precisam de ser restaurar a fim forçá-la a pedir a ITL “vazia” nova. Uma vez que as mudanças do certificado são terminadas e todos os serviços necessários estiveram reiniciados, esta característica podem ser ajustados de volta a “falso”, ao serviço TFTP reiniciada, e a restauração do telefone (assim que o telefone pode obter o arquivo válido ITL). Então todas as características continuarão a trabalhar como fizeram previamente.

Certificados regenerados na ordem específica

Este procedimento fornece um servidor TFTP arquivo válido/actualizado ITL de um servidor TFTP confiado que esteja disponível.

1. Pare o serviço TFTP no servidor TFTP preliminar.
2. Faça mudanças nos Certificados de servidor TFTP preliminares (como necessário).

3. Restaure os telefones (a fim obter um arquivo novo ITL do servidor TFTP secundário) - o dependente em cima de que os Certificados são regenerados, isto pôde acontecer automaticamente.
4. Uma vez que os telefones retornaram, enfie o serviço TFTP do servidor TFTP preliminar.
5. Faça mudanças do certificado no servidor TFTP secundário.
6. Restaure os telefones (a fim obter um arquivo novo ITL do servidor TFTP preliminar).

Caution: Não edite Certificados em ambos os servidores TFTP ao mesmo tempo. Isto não dá aos telefones nenhum servidor TFTP para confiar e exige o administrador local remover manualmente a ITL de todos os telefones.

Remova e regenere os Certificados em CUCM

Somente os Certificados do serviço (as lojas do certificado que não são etiquetados com "- confiança") podem ser regenerados. Os Certificados nas lojas da confiança (as lojas do certificado que são etiquetados com "- confiança") precisam de ser suprimidos, porque não podem ser regenerados.

Caution: Esteja ciente da identificação de bug Cisco CSCut58407 - Os dispositivos não devem reiniciar quando o CAPF/CallManager/confiança são removidos.

Certificate afinal alterações, o serviço respectivo precisa de ser reiniciado para tomar na mudança. Isto é coberto no após a regeneração/remoção da seção dos Certificados.

Caution: Esteja ciente da identificação de bug Cisco CSCto86463 - Os Certificados suprimidos reaparecem, incapaz de remover os Certificados de CUCM. Esta é uma edição onde os Certificados suprimidos continuem a reaparecer após a remoção. Siga a ação alternativa no defeito.

Regenere Certificados através do CLI

Caution: As regenerações dos Certificados provocam uma atualização automática dos arquivos ITL dentro do conjunto, que provoca uma amplo cluster restauração do telefone de software para permitir que os telefones provoquem uma atualização de sua ITL local. Isto é centrado sobre regenerações do certificado CAPF e de CallManager, mas pode ocorrer com outras lojas do certificado dentro de CUCM, tal como Tomcat.

CAPF regenerado

Em cima da regeneração, o certificado CAPF transfere-se arquivos pela rede automaticamente CAPF-confiança e CallManager-confiança. Também, o CAPF tem sempre um encabeçamento original do nome do sujeito, assim os Certificados previamente usados CAPF serão retidos e usados para a autenticação.

```
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 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 used to sign the CTL file.
```

> **Note**: Se um certificado CAPF obtém expirado, os telefones que usam o LSC não poderão registrar-se a CUCM porque CUCM rejeita seu certificado. Contudo, você pode ainda gerar um LSC novo para o telefone com o certificado novo CAPF. Quando você recarrega o telefone que transfere a configuração e contacta então o CAPF a fim atualizar o LSC. Depois que o LSC é atualizado, o telefone registra-se como ele deva. Isto trabalha enquanto um certificado novo CAPF está no arquivo ITL e no telefone transferidos e confiou o certificado que o assinou (callmanager.pem).

CallManager regenerado

Em cima da regeneração, o CallManager transfere-se arquivos pela rede automaticamente CallManager-confiança.

```
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 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 used to sign the CTL file.
```

IPsec regenerado

Em cima da regeneração, o certificado do IPsec transfere-se arquivos pela rede automaticamente IPsec-confiança.

```
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 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 used to sign the CTL file.
```

Tomcat regenerado

Em cima da regeneração, o certificado de Tomcat transfere-se arquivos pela rede automaticamente Tomcat-confiança.

```
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 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 used to sign the CTL file.
```

TV regenerados

```
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 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 used to sign the CTL file.
```

Que a esperar

Quando você regenera Certificados através do CLI, você está pedido verificar esta mudança. Datilografe **sim** e pressione **entram**.

```
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 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 used to sign the CTL file.
```

Remova os Certificados através do CLI

Remova os Certificados da CAPF-confiança

```
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 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 used to sign the CTL file.
```

Remova os Certificados da CallManager-confiança

```
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 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 used to sign the CTL file.
```

Remova os Certificados da IPsec-confiança

```
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 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 used to sign the CTL file.
```

Remova os Certificados da Tomcat-confiança

```
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 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 used to sign the CTL file.
```

Remova os Certificados da TV-confiança

```
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 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 used to sign the CTL file.
```

Regenere Certificados através da Web GUI

Regenere o CAPF

Em cima da regeneração, o certificado CAPF transfere-se arquivos pela rede automaticamente CAPF-confiança e CallManager-confiança. Também, o certificado CAPF tem sempre um encabeçamento original do nome do sujeito, assim os Certificados previamente usados CAPF são retidos e usados para a autenticação.

```
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 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 used to sign the CTL file.
```

CallManager regenerado

Em cima da regeneração, o certificado CAPF transfere-se arquivos pela rede automaticamente CallManager-confiança.

```
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 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 used to sign the CTL file.
```

IPsec regenerado

Em cima da regeneração, o certificado do IPsec transfere-se arquivos pela rede automaticamente IPsec-confiança.

```
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 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 used to sign the CTL file.
```

Tomcat regenerado

Em cima da regeneração, o certificado de Tomcat transfere-se arquivos pela rede automaticamente Tomcat-confiança.

```
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 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 used to sign the CTL file.
```

TV regenerados

```
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 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 used to sign the CTL file.
```

Remova os Certificados através da Web GUI

```
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 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 used to sign the CTL file.
```

Após a regeneração/remoção dos Certificados

Depois que você remove ou regenera um certificado de uma loja do certificado, o serviço respectivo precisa de ser reiniciado a fim tomar na mudança.

Armazene	Preste serviços de manutenção para reiniciar	Como (== CLI do C; Web GUI do == W)
Tomcat	Tomcat	C : utils service restart Cisco Tomcat G: Cisco unificou a utilidade > as ferramentas > o Control Cent característica presta serviços de manutenção > (server seleto) “CallManager da Cisco seleto” > reinício
CallManager	CallManager; TFTP	E G: Cisco unificou a utilidade > as ferramentas > o Control Cent característica presta serviços de manutenção > (server seleto) “Cisco seleto Tftp” > reinício
CAPF	CAPF (no editor somente)	G: Cisco unificou a utilidade > as ferramentas > o Control Cent característica presta serviços de manutenção > (server seleto) “função seleta do proxy do Certificate Authority Cisco” > reiníci
TV	Serviço da verificação da confiança (no servidor respectivo)	G: Cisco unificou a utilidade > as ferramentas > o Control Cent os serviços de rede > (server seleto) > “Cisco seleto confiam o serviço da verificação” > reinício
IPsec	Local de Cisco DRF (em todos os Nós); Mestre de Cisco DRF (no editor)	C : Local de Cisco DRF do reinício do serviço dos utils E C : mestre de Cisco DRF do reinício do serviço dos utils

Instale/atualização LSC no telefone

Se o certificado CAPF foi regenerado, a seguir os Certificados LSC para todos os telefones no conjunto precisam de ser atualizados com o LSC assinado pelo certificado novo CAPF.

1. Escolha a **utilidade CUCM > a ativação do serviço**. Ative o fornecedor de Cisco CTL e a função do proxy do Certificate Authority de Cisco no servidor do publicador.
2. Do ccmadmin CUCM, escolha o **dispositivo > o telefone.** Escolha o telefone IP que você quer provision sobre um LSC.
3. Na página da configuração de dispositivo sob a operação do certificado, escolha **instalam/elevações > pela corda nula**.
4. Salvar a configuração telefônica no ccmadmin e escolha-a **aplicam a configuração**.

Se o telefone tem o problema com a instalação do LSC, termine estas ações no telefone:

Quando o telefone restaura, vai ao telefone físico e escolhe **ajustes > (6) a configuração de segurança > (4) LSC > ** #** (esta operação destrava o GUI e permite que nós continuem à próxima etapa) **> a atualização** (a atualização não será visível até que você execute a etapa precedente) > **submete-se**.

Não atribua nenhuns Certificados a um telefone a menos que for um telefone wireless (7921/25). Os telefones wireless usam autoridades de certificação da 3ª parte (CA) a fim autenticar-se.

Conclusão

Se você for executado em uma edição ou precisar o auxílio com este procedimento, contacte o centro de assistência técnica da Cisco (TAC) para o auxílio. Neste caso, mantenha seu backup DRF disponível porque estará usado como um último recurso a fim restaurar o serviço se o TAC é incapaz de fazer assim com outros métodos.