Configuración de LSC en el teléfono IP con CUCM

Contenido

Introducción

Este documento describe cómo instalar un certificado de importancia local (LSC) en un teléfono de protocolo de Internet de Cisco (teléfono IP de Cisco).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Opciones de modo de seguridad de clúster de Cisco Unified Communications Manager (CUCM)
- Certificados X.509
- Certificados instalados de fabricación (MIC)
- LSC
- Operaciones de certificados de función proxy de autoridad certificadora (CAPF)
- Seguridad predeterminada (SBD)
- Archivos de lista de confianza inicial (ITL)

Componentes Utilizados

La información de este documento se basa en las versiones de CUCM compatibles con SBD, a saber, CUCM 8.0(1) y versiones posteriores.

> **Nota**: solo se aplica a teléfonos que admitan la seguridad predeterminada (SBD). Por ejemplo, los teléfonos 7940 y 7960 no admiten SBD, ni tampoco los teléfonos de conferencia 7935, 7936 y 7937. Para obtener una lista de los dispositivos compatibles con SBD en su versión de CUCM, navegue

---

hasta **Cisco Unified Reporting > Informes del sistema > Lista de características del teléfono de Unified CM** y ejecute un informe sobre la función: Seguridad de forma predeterminada.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

MIC frente a LSC

Si utiliza autenticación basada en certificados para 802.1X o VPN de teléfono Anyconnect, es importante comprender la diferencia entre los MIC y los LSC.

Todos los teléfonos Cisco vienen con un MICRÓFONO preinstalado de fábrica. Este certificado está firmado por uno de los certificados de CA de Cisco Manufacturing, ya sea por la CA de Cisco Manufacturing, por la CA de Cisco Manufacturing SHA2, por el certificado CAP-RTP-001 o por el certificado CAP-RTP-002. Cuando el teléfono presenta este certificado, prueba que es un teléfono válido de Cisco, pero esto no valida que el teléfono pertenezca a un cliente específico o clúster de CUCM. Podría tratarse de un teléfono no autorizado adquirido en el mercado libre o traído de un sitio diferente.

Los LSC, por otra parte, son instalados intencionalmente en los teléfonos por un administrador y están firmados por el certificado CAPF del editor de CUCM. Debe configurar 802.1X o VPN Anyconnect para que confíe únicamente en las LSC emitidas por las autoridades de certificados CAPF conocidas. Basar la autenticación de certificados en LSC en lugar de MIC le proporciona un control mucho más granular sobre qué dispositivos telefónicos son confiables.

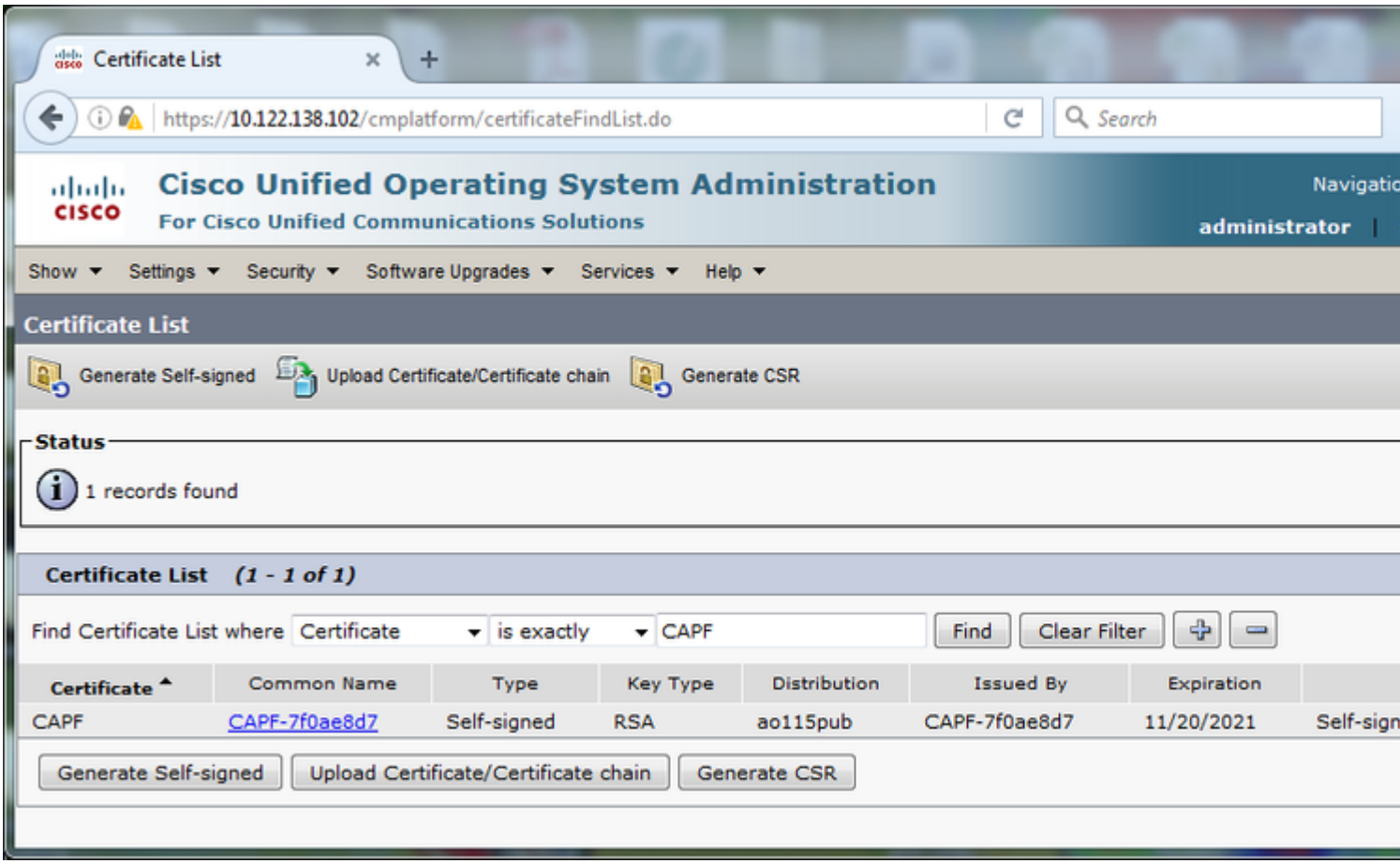
Configurar

Topología de red

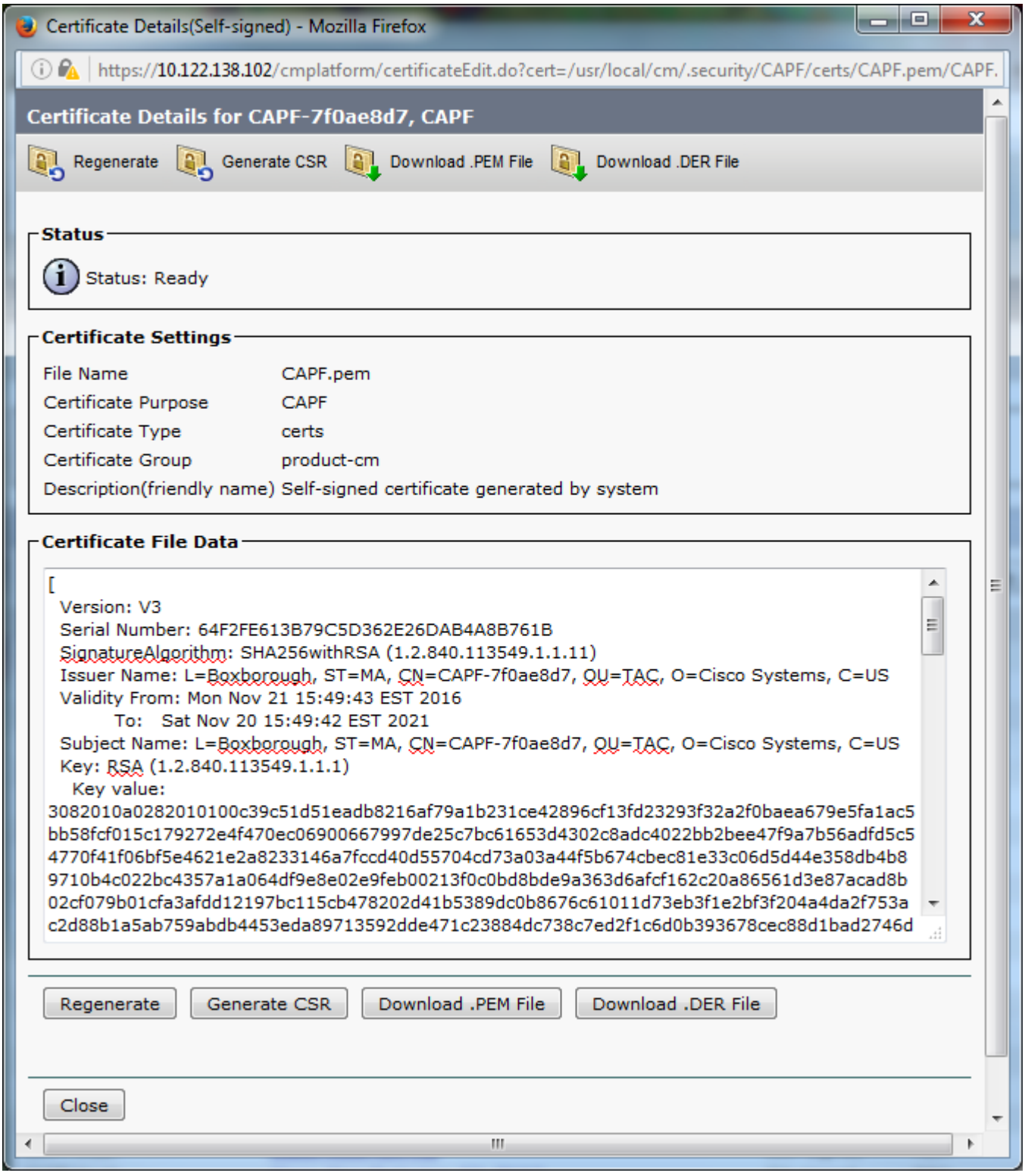
Para este documento se utilizaron estos servidores de laboratorio de CUCM:

- ao115pub - 10.122.138.102 - CUCM Publisher y servidor TFTP
- ao115sub - 10.122.138.103 - Suscriptor de CUCM y servidor TFTP

Compruebe que el certificado CAPF no ha caducado ni lo hará en un futuro próximo. Navegue hasta **Administración de Cisco Unified OS > Seguridad > Administración de certificados**, luego **Buscar lista de certificados donde el certificado es exactamente CAPF** como se muestra en la imagen.



Haga clic en **Nombre Común** para abrir la página Detalles del Certificado. Inspeccione las fechas De Validez: y A: en el panel **Datos de Archivo de Certificado** para determinar cuándo caduca el certificado, como se muestra en la imagen.



Si el certificado CAPF ha caducado o lo hará próximamente, vuelva a generar dicho certificado. No avance con el proceso de instalación de LSC con un certificado CAPF caducado o que está a punto de caducar. Esto evita la necesidad de volver a emitir LSC en un futuro próximo debido a la expiración del certificado CAPF. Para obtener información sobre cómo regenerar el certificado CAPF, consulte el artículo Proceso de regeneración/renovación de certificados de CUCM.

De manera similar, si necesita que su certificado CAPF esté firmado por una autoridad de certificación externa, tiene la opción de elegir en esta etapa. Complete la generación del archivo de solicitud de firma de certificado (CSR) y la importación del certificado CAPF firmado ahora o continúe la configuración con un LSC autofirmado para realizar una prueba preliminar. Si necesita un certificado CAPF firmado por terceros, generalmente es conveniente configurar esta función primero con un certificado CAPF autofirmado, probar

y verificar, y luego volver a implementar los LSC que están firmados por un certificado CAPF firmado por terceros. Esto simplifica la resolución de problemas posterior, si las pruebas con el certificado CAPF firmado por terceros fallan.

> **Advertencia**: si regenera el certificado CAPF o importa un certificado CAPF firmado por terceros mientras el servicio CAPF está activado e iniciado, CUCM restablecerá automáticamente los teléfonos. Complete estos procedimientos en una ventana de mantenimiento cuando sea aceptable restablecer los teléfonos. Para obtener referencias, consulte Cisco bug ID CSCue55353 - Add Warning when Regenerating TVS/CCM/CAPF Certificate that Phones Reset

---

> **Nota**: si la versión de CUCM admite SBD, este procedimiento de instalación de LSC se aplica independientemente de si el clúster de CUCM está configurado en modo mixto o no. SBD forma parte de CUCM versión 8.0(1) y posteriores. En estas versiones de CUCM, los archivos ITL contienen el certificado para el servicio CAPF en el publicador de CUCM. Esto permite que los teléfonos se conecten al servicio CAPF para admitir operaciones de certificados como la instalación/actualización y la resolución de problemas.

> En las versiones anteriores de CUCM, era necesario configurar el clúster para el modo mixto con el fin de admitir operaciones de certificados. Dado que esto ya no es necesario, se reducen las barreras para el uso de LSC como certificados de identidad del teléfono para la autenticación 802.1X o para la autenticación de cliente AnyConnect VPN.

Ejecute el comando **show itl** en todos los servidores TFTP del clúster de CUCM. Observe que el archivo ITL contiene un certificado CAPF.

Por ejemplo, aquí hay un extracto de la salida **show itl** del suscriptor de CUCM del laboratorio ao115sub.

> **Nota**: Hay una entrada ITL Record en este archivo con una FUNCIÓN de CAPF.

> **Nota**: Si el archivo ITL no tiene una entrada CAPF, inicie sesión en el editor de CUCM y confirme que el servicio CAPF está activado. Para confirmar esto, navegue hasta **Serviciabilidad de Cisco Unified > Herramientas > Activación de servicio > Publicador de CUCM > Seguridad**, luego active el **Servicio de función proxy de Cisco Certificate Authority**. Si se desactivó el servicio y lo acaba de activar, navegue hasta **Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de funciones > Servidor > Servicios CM**, y reinicie el servicio TFTP de Cisco en todos los servidores TFTP del clúster de CUCM para regenerar el archivo ITL. Además, asegúrese de no ingresar el ID de bug Cisco CSCuj78330.

> **Nota**: Una vez que haya terminado, ejecute el comando **show itl** en todos los servidores TFTP del clúster de CUCM para verificar que el certificado CAPF actual del publicador de CUCM esté ahora incluido en el archivo.

<#root>

```
ITL Record #:1


----
```

BYTEPOS TAG LENGTH VALUE

------- --- ------ -----

1 RECORDLENGTH 2 727

2 DNSNAME 2

3 SUBJECTNAME 64 CN=CAPF-7f0ae8d7;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US

4 FUNCTION 2 CAPF

5 ISSUERNAME 64 CN=CAPF-7f0ae8d7;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US

6 SERIALNUMBER 16 64:F2:FE:61:3B:79:C5:D3:62:E2:6D:AB:4A:8B:76:1B

7 PUBLICKEY 270

8 SIGNATURE 256

11 CERTHASH 20 C3 E6 97 D0 8A E1 0B F2 31 EC ED 20 EC C5 BC 0F 83 BC BC 5E

12 HASH ALGORITHM 1 null

ITL Record #:2

BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 717
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TVS
5 ISSUERNAME 59 CN=ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 6B:99:31:15:D1:55:5E:75:9C:42:8A:CE:F2:7E:EA:E8
7 PUBLICKEY 270
8 SIGNATURE 256
11 CERTHASH 20 05 9A DE 20 14 55 23 2D 08 20 31 4E B5 9C E9 FE BD 2D 55 87
12 HASH ALGORITHM 1 null

ITL Record #:3

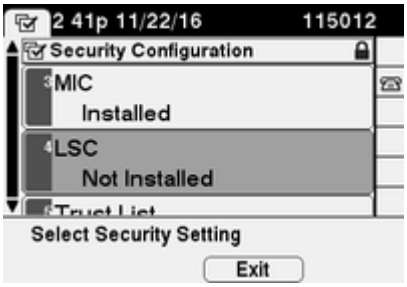
BYTEPOS TAG LENGTH VALUE

```
------- --- ------ -----
1 RECORDLENGTH 2 1680
2 DNSNAME 2
3 SUBJECTNAME 71 CN=ITLRECOVERY_ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 71 CN=ITLRECOVERY_ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 51:BB:2F:1C:EE:80:02:16:62:69:51:9A:14:F6:03:7E
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 963 DF 98 C1 DB E0 61 02 1C 10 18 D8 BA F7 1B 2C AB 4C F8 C9 D5 (SHA1 Hash HEX)
This etoken was not used to sign the ITL file.

 ITL Record #:4
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 717
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TVS
5 ISSUERNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 65:E5:10:72:E7:F8:77:DA:F1:34:D5:E3:5A:E0:17:41
7 PUBLICKEY 270
8 SIGNATURE 256
11 CERTHASH 20 00 44 54 42 B4 8B 26 24 F3 64 3E 57 8D 0E 5F B0 8B 79 3B BF
12 HASH ALGORITHM 1 null

 ITL Record #:5
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1652
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 48:F7:D2:F3:A2:66:37:F2:DD:DF:C4:7C:E6:B9:CD:44
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 959 20 BD 40 75 51 C0 61 5C 14 0D 6C DB 79 E5 9E 5A DF DC 6D 8B (SHA1 Hash HEX)
This etoken was used to sign the ITL file.

 ITL Record #:6
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1652
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TFTP
5 ISSUERNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 48:F7:D2:F3:A2:66:37:F2:DD:DF:C4:7C:E6:B9:CD:44
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 959 20 BD 40 75 51 C0 61 5C 14 0D 6C DB 79 E5 9E 5A DF DC 6D 8B (SHA1 Hash HEX)

 ITL Record #:7
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1031
2 DNSNAME 9 ao115sub
```

```
3 SUBJECTNAME 62 CN=ao115sub-EC;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TFTP
5 ISSUERNAME 62 CN=ao115sub-EC;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 53:CC:1D:87:BA:6A:28:BD:DA:22:B2:49:56:8B:51:6C
7 PUBLICKEY 97
8 SIGNATURE 103
9 CERTIFICATE 651 E0 CF 8A B3 4F 79 CE 93 03 72 C3 7A 3F CF AE C3 3E DE 64 C5 (SHA1 Hash HEX)

The ITL file was verified successfully.
```

Una vez confirmada la entrada CAPF como entrada en el DIT, podrá completar una operación de certificación en un teléfono. En este ejemplo, se instala un certificado RSA de 2048 bits mediante la autenticación de cadena nula.

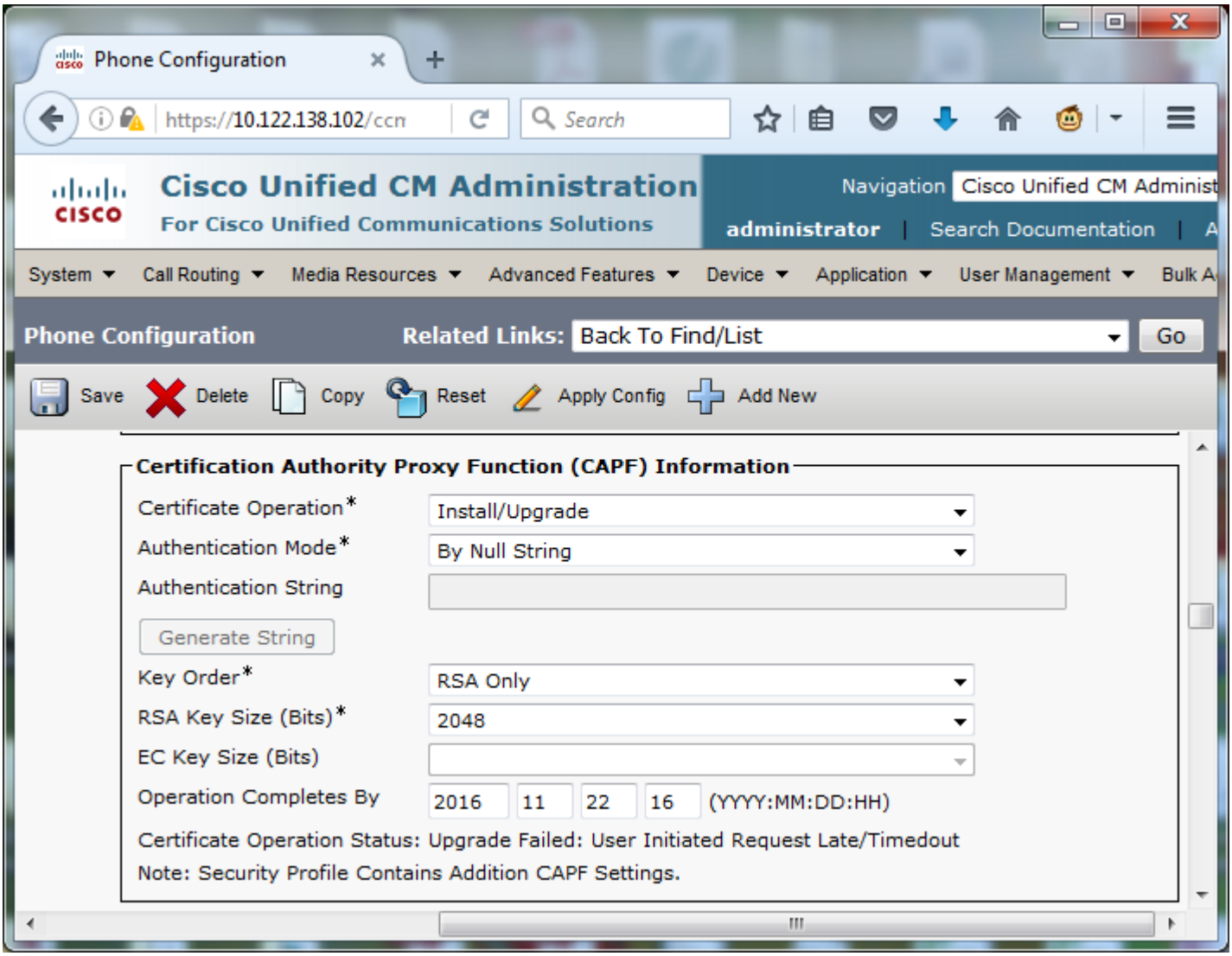
En el teléfono, verifique que un LSC aún no esté instalado como se muestra en la imagen. Por ejemplo, en un teléfono de la serie 79XX, navegue hasta **Settings > 4 - Security Configuration > 4 - LSC**.



Abra la página de configuración del teléfono del teléfono. Vaya a **Administración de Cisco Unified CM > Dispositivo > Teléfono**.

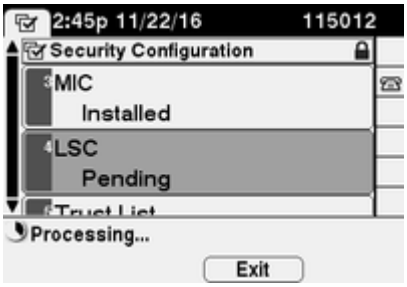
Introduzca estos detalles en la sección CAPF Information (Información de CAPF) de la configuración del teléfono, como se muestra en la imagen:

- Para Certificate Operation, elija **Install/Upgrade**
- Para el Modo de Autenticación, elija **Por Cadena Nula**
- Para este ejemplo, deje el Orden de claves, el Tamaño de clave RSA (bits) y el Tamaño de clave EC (bits) establecidos en los valores predeterminados del sistema.
- En Operación finalizada por, introduzca una fecha y hora que tengan como mínimo una hora en el futuro.

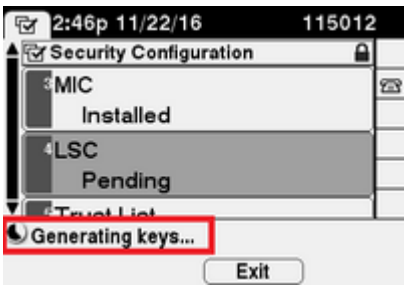


Guarde los cambios de configuración y, a continuación, **aplique la configuración**.

El estado de LSC en el teléfono cambia a Pendiente, como se muestra en la imagen.



El teléfono genera claves como se muestra en la imagen.



El teléfono se restablece y, cuando se completa el restablecimiento, el estado de LSC del teléfono cambia a Instalado, como se muestra en la imagen.

Esto también está visible en Mensajes de estado en el teléfono, como se muestra en la imagen.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Para verificar la instalación del certificado LSC en varios teléfonos, consulte la sección Generar informe CAPF de la Guía de seguridad para Cisco Unified Communications Manager, Release 11.0(1). También puede ver los mismos datos en la interfaz web de administración de CUCM mediante el procedimiento Buscar teléfonos por estado de LSC o Cadena de autenticación.

Para obtener copias de los certificados LSC instalados en los teléfonos, consulte el artículo Cómo recuperar certificados de los teléfonos IP de Cisco.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

No hay servidor CAPF válido

El LSC no puede instalarse. Los mensajes de estado del teléfono muestran **No valid CAPF server**. Esto indica que no hay ninguna entrada CAPF en el archivo ITL. Verifique que se haya activado el servicio CAPF y, a continuación, reinicie el servicio TFTP. Compruebe que el archivo ITL contiene un certificado CAPF después del reinicio, restablezca el teléfono para que recoja el archivo ITL más reciente y, a continuación, vuelva a intentar la operación de certificado. Si la entrada del servidor CAPF en el menú de configuración de seguridad del teléfono aparece como nombre de host o nombre de dominio completo, confirme que el teléfono puede resolver la entrada en una dirección IP.

LSC: error de conexión

El LSC no puede instalarse. Los mensajes de estado del teléfono muestran **LSC: Connection Failed**. Esto puede indicar una de estas condiciones:

- Falta de coincidencia entre el certificado CAPF del archivo ITL y el certificado actual; el servicio CAPF está en uso.
- El servicio CAPF se detiene o se desactiva.
- El teléfono no puede acceder al servicio CAPF a través de la red.

Verifique que el servicio CAPF esté activado, reinicie el servicio CAPF, reinicie los servicios TFTP en todo el clúster, reinicie el teléfono para recoger el último archivo ITL y, a continuación, vuelva a intentar la operación de certificado. Si el problema persiste, tome una captura de paquetes del teléfono y del publicador de CUCM, y analice para ver si hay comunicación bidireccional en el puerto 3804, el puerto de servicio CAPF predeterminado. Si no es así, puede haber un problema de red.

LSC: error

El LSC no puede instalarse. Los mensajes de estado del teléfono muestran **LSC: Failed**. La página web Configuración del teléfono muestra **Estado de operación del certificado: error en la actualización: retraso/tiempo de espera de la solicitud iniciada por el usuario**. Esto indica que la operación se ha completado por fecha y hora y ha caducado o ya ha pasado. Introduzca una fecha y una hora que tengan como mínimo una hora para el futuro y, a continuación, vuelva a intentar la operación de certificado.

LSC: operación pendiente

El LSC no puede instalarse. Los mensajes de estado del teléfono muestran **LSC: Connection Failed**. La página Configuración del teléfono muestra **Estado de Operación del Certificado: Operación Pendiente. Hay diferentes razones por las que se puede ver el estado de Operación de Certificado: Operación Pendiente**. Algunos de ellos pueden incluir:

- ITL en el teléfono es diferente al que se utiliza actualmente en los servidores TFTP confundidos.
- Problemas con ITL corruptos. Cuando esto sucede, los dispositivos pierden su estado de confianza y el comando **utils itl reset localkey** debe ejecutarse desde el publicador de CUCM para obligar a los teléfonos a utilizar ahora el certificado ITLRecrecovery. Si el clúster está en modo mixto, debe utilizar el comando **utils ctl reset localkey.** A continuación, verá un ejemplo de lo que puede ver cuando intenta ver un ITL dañado desde la CLI de CUCM. Si hay un error cuando intenta ver el ITL e intenta ejecutar el comando **utils itl reset localkey**, pero ve el segundo error, éste puede ser un defecto del ID de bug Cisco CSCus3755. Confirme si la versión de CUCM está afectada.

```
admin:show itl
Length of ITL file: 0
ITL File not found. To generate an ITL file, activate or restart the Cisco TFTP service as thi
servers.
Error parsing the ITL File.


admin:utils itl reset localkey
Enter CCM Administrator password :

Locating active Tftp servers in the cluster.....

Unable to determine the active and running  TFTP nodes in the cluster
Ensure that the DB replication is working on all nodes and the correct Password has been en
Then retry the command

Executed command unsuccessfully
chmod: changing permissions of `/var/log/active/cm/trace/dbl/sdi/replication_scripts_output
```

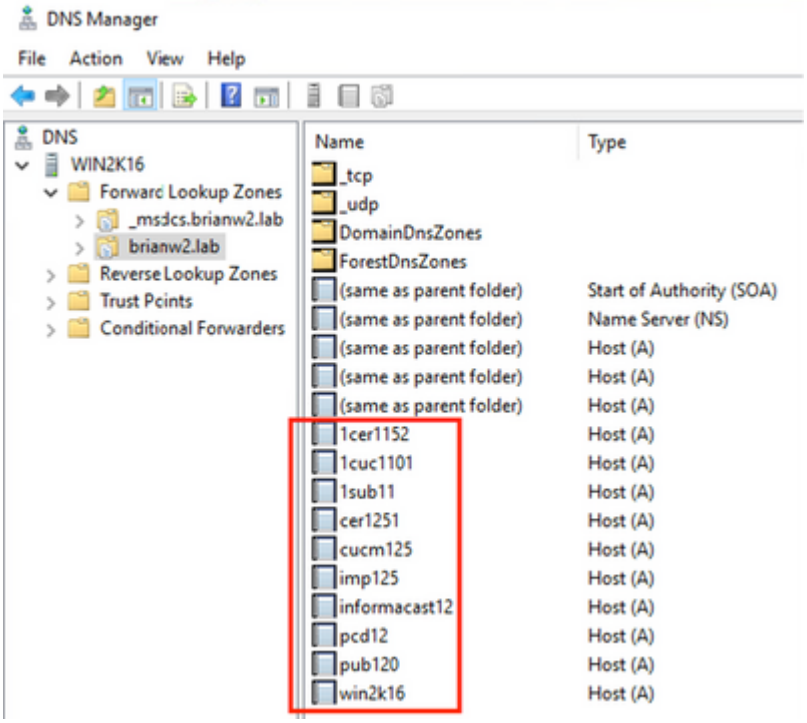
- Los teléfonos no pueden autenticar el nuevo LSC debido a una falla de TVS.

- El teléfono utiliza el certificado MIC, pero la sección Información de la función proxy de la autoridad certificadora (CAPF) de la página de configuración de teléfonos tiene el Modo de autenticación establecido en por certificado existente (Precedencia a LSC).
- El teléfono no puede resolver el FQDN de CUCM.

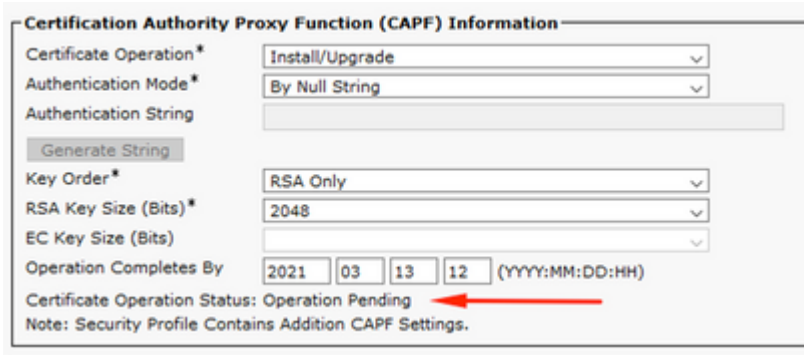
En la última situación, se configura un entorno de laboratorio para simular lo que se vería en los registros si un teléfono no pudiera resolver el FQDN de CUCM. Actualmente, el laboratorio está configurado con estos servidores:

- CUCM Publisher and Subscriber running version 11.5.1.15038-2
- Configuración de Windows 2016 Server como mi servidor DNS

Para la prueba, no hay ninguna entrada DNS configurada para el servidor PUB11 CUCM.



Se intentó enviar un LSC a uno de los teléfonos (8845) del laboratorio. Observe que todavía muestra el estado de operación del certificado: Operación pendiente.

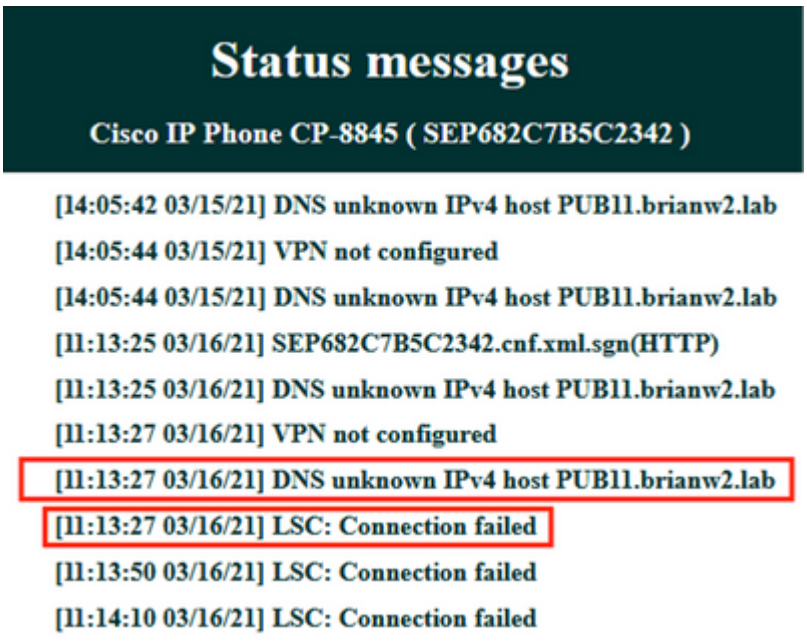


En los registros de la consola telefónica, consulte los intentos del teléfono de consultar su caché local (127.0.0.1), antes de reenviar la consulta a la dirección del servidor DNS configurado.

```
0475 INF Mar 12 15:07:53.686410 dnsmasq[12864]: query[A] PUB11.brianw2.lab from 127.0.0.1
0476 INF Mar 12 15:07:53.686450 dnsmasq[12864]: forwarded PUB11.brianw2.lab to X.X.X.X
```

```
0477 INF Mar 12 15:07:53.694909 dnsmasq[12864]: forwarded PUB11.brianw2.lab to X.X.X.X
0478 INF Mar 12 15:07:53.695263 dnsmasq[12864]: reply PUB11.brianw2.lab is NXDOMAIN-IPv4
0479 INF Mar 12 15:07:53.695833 dnsmasq[12864]: query[A] PUB11.brianw2.lab from 127.0.0.1
0480 INF Mar 12 15:07:53.695865 dnsmasq[12864]: cached PUB11.brianw2.lab is NXDOMAIN-IPv4
0481 WRN Mar 12 15:07:53.697091 (12905:13036) JAVA-configmgr MQThread|NetUtil.traceIPv4DNSErrors:? - DNS

++ However, we see that the phone is not able to resolve the FQDN of the CUCM Publisher. This is because

0482 ERR Mar 12 15:07:53.697267 (12905:13036) JAVA-configmgr MQThread|cip.sec.TvsProperty:? - Failed to

++ Afterwards, we see the CAPF operation fail. This is expected because we do not have a DNS mapping for

0632 NOT Mar 12 15:07:55.760715 (12905:13036) JAVA-configmgr MQThread|cip.sec.CertificateProperty:? - Ce
0633 NOT Mar 12 15:07:55.761649 (322:17812) SECUREAPP-RCAPF_START_MODE: Start CAPF - mode:[1]([NULL_STR]
0634 NOT Mar 12 15:07:55.761749 (322:17812) SECUREAPP-CAPF_CLNT_INIT:CAPF clnt initialized
0635 NOT Mar 12 15:07:55.761808 (322:17812) SECUREAPP-CAPFClnt: SetDelayTimer - set with value <0>
0636 ERR Mar 12 15:07:55.761903 (322:17812) SECUREAPP-Sec create BIO - invalid parameter.
0637 ERR Mar 12 15:07:55.761984 (322:17812) SECUREAPP-SEC_CAPF_BIO_F: CAPF create bio failed
0638 ERR Mar 12 15:07:55.762040 (322:17812) SECUREAPP-SEC_CAPF_OP_F: CAPF operation failed, ret -7
0639 CRT Mar 12 15:07:55.863826 (12905:13036) JAVA-configmgr MQThread|cip.sec.CertificateProperty$1:? -

++ What we would expect to see is something similar to the following where DNS replies with the IP addre

4288 INF Mar 12 16:34:06.162666 dnsmasq[12864]: query[A] PUB11.brianw2.lab from 127.0.0.1
4289 INF Mar 12 16:34:06.162826 dnsmasq[12864]: forwarded PUB11.brianw2.lab to X.X.X.X
4290 INF Mar 12 16:34:06.164908 dnsmasq[12864]: reply PUB11.brianw2.lab is X.X.X.X
4291 NOT Mar 12 16:34:06.165024 (12905:13036) JAVA-configmgr MQThread|cip.sec.TvsProperty:? - Resolve Tv
```

Vea en los mensajes de estado del teléfono a continuación, que el teléfono no puede resolver PUB11.brianw2.lab. Luego vea el mensaje **LSC: Connection failed**.



Defectos a considerar:

Cisco bug ID CSCub6243 - La instalación de LSC falla intermitentemente y luego congela el servidor CAPF

Defecto de mejora a considerar:

ID de bug de Cisco CSCuz18034: se necesita informe para los terminales instalados de LSC junto con el estado de vencimiento

Información Relacionada

Estos documentos proporcionan más información sobre el uso de LSC en el contexto de la autenticación de cliente VPN AnyConnect y la autenticación 802.1X.

- Solución de problemas de AnyConnect VPN Phone - IP Phones, ASA y CUCM
- Servicios de red basados en identidad: Guía de implementación y configuración de telefonía IP en redes compatibles con IEEE 802.1X

También existe un tipo avanzado de configuración LSC, en el que los certificados LSC están firmados directamente por una autoridad de certificación de terceros, no por el certificado CAPF.

Para obtener más información, consulte: Ejemplo de Configuración de Importación y Generación de LSC Firmados por CA de Terceros de CUCM

- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).