Configuración LSC en el Cisco IP Phone con CUCM

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[MIC contra los LSC](#)
[Configurar](#)
[Topología de red](#)
[Verificación](#)
[Troubleshooting](#)
[Ningún servidor válido del CAPF](#)
[LSC: Conexión fallada](#)
[LSC: Fallado](#)
[Información Relacionada](#)

Introducción

Este documento describe cómo instalar el certificado significativo a localmente - (LSC) en un teléfono del protocolo de Internet de Cisco (Cisco IP Phone).

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Opciones del modo seguro del cluster del administrador de las Comunicaciones unificadas de Cisco (CUCM)
- Certificados X.509
- Certificados instalados de fabricación (MIC)
- LSC
- Operaciones del certificado de la función de proxy del Certificate Authority (CAPF)
- Seguridad por abandono (SBD)
- Archivos iniciales de la lista de la confianza (ITL)

Componentes Utilizados

La información en este documento se basa en las versiones CUCM que soportan el SBD, a saber CUCM 8.0(1) y arriba.

Note: También pertenece solamente a los teléfonos que soportan el SBD. Por ejemplo, los 7940 y 7960 teléfonos no soportan el SBD, ni hacen 7936 y 7937 teléfonos de la conferencia los 7935. Para una lista de dispositivos que soporten el SBD en su versión de CUCM, navegue a **Cisco unificó la información > los informes del sistema > lista unificada de la función del teléfono CM** y funcionan con un informe sobre la **característica: Seguridad por abandono**.

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

MIC contra los LSC

Si usted utiliza la autenticación basada certificado para el 802.1x o el teléfono VPN de Anyconnect, es importante entender la diferencia entre los MIC y los LSC.

Cada Teléfono de Cisco viene con un MIC instalado previamente en la fábrica. Este certificado es firmado por uno de Cisco que fabrica los Certificados de CA, por Cisco que fabrica CA, Cisco que fabrica el certificado SHA2, CAP-RTP-001 o CAP-RTP-002 de CA. Cuando el teléfono presenta este certificado, prueba que es un Teléfono de Cisco válido, pero éste no valida que el teléfono pertenece a un cliente específico o al cluster CUCM. Podía potencialmente ser un teléfono rogue comprado en el mercado libre o traído encima de un diverso sitio.

Los LSC, por otra parte, son instalados intencionalmente en los teléfonos por un administrador, y firmados por el certificado del CAPF CUCM Publisher. Usted configuraría el 802.1x o Anyconnect VPN para confiar en solamente los LSC publicados por las autoridades de certificación conocidas del CAPF. Basar la autenticación certificada en los LSC en vez de los MIC provee de usted un control mucho más granular sobre el cual se confíen en los Dispositivos del teléfono.

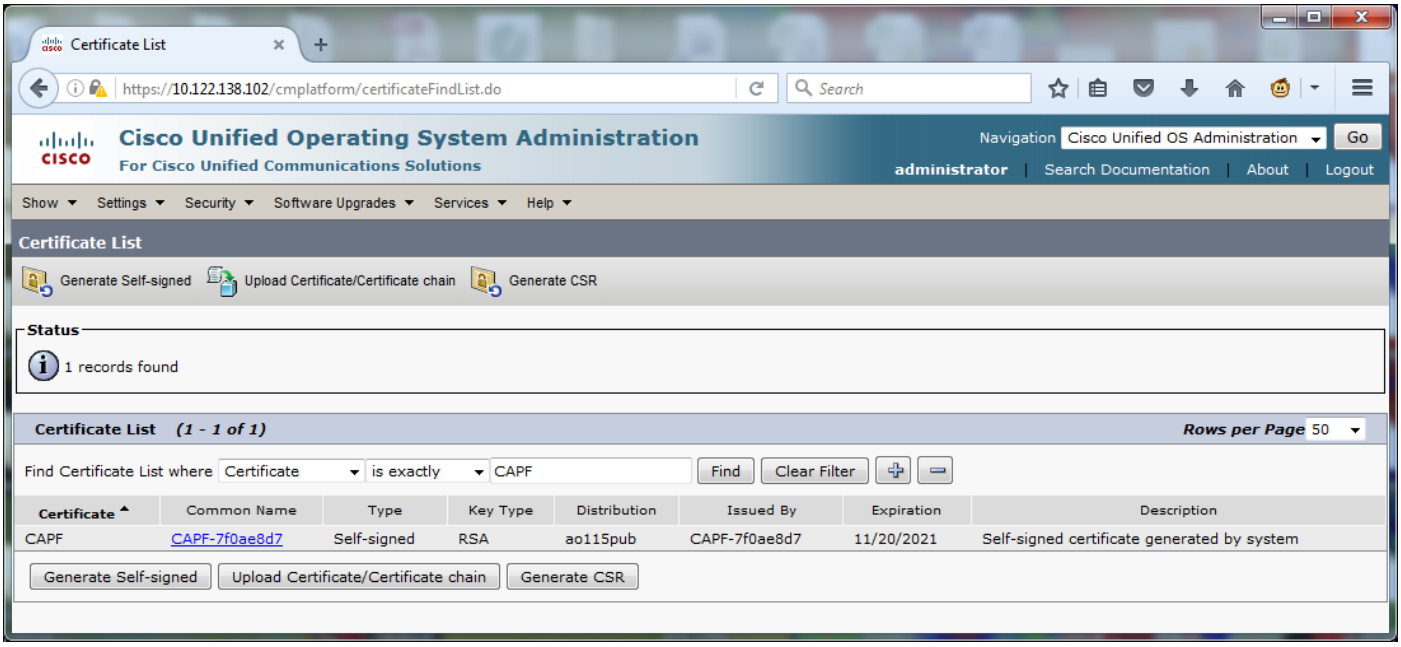
Configurar

Topología de red

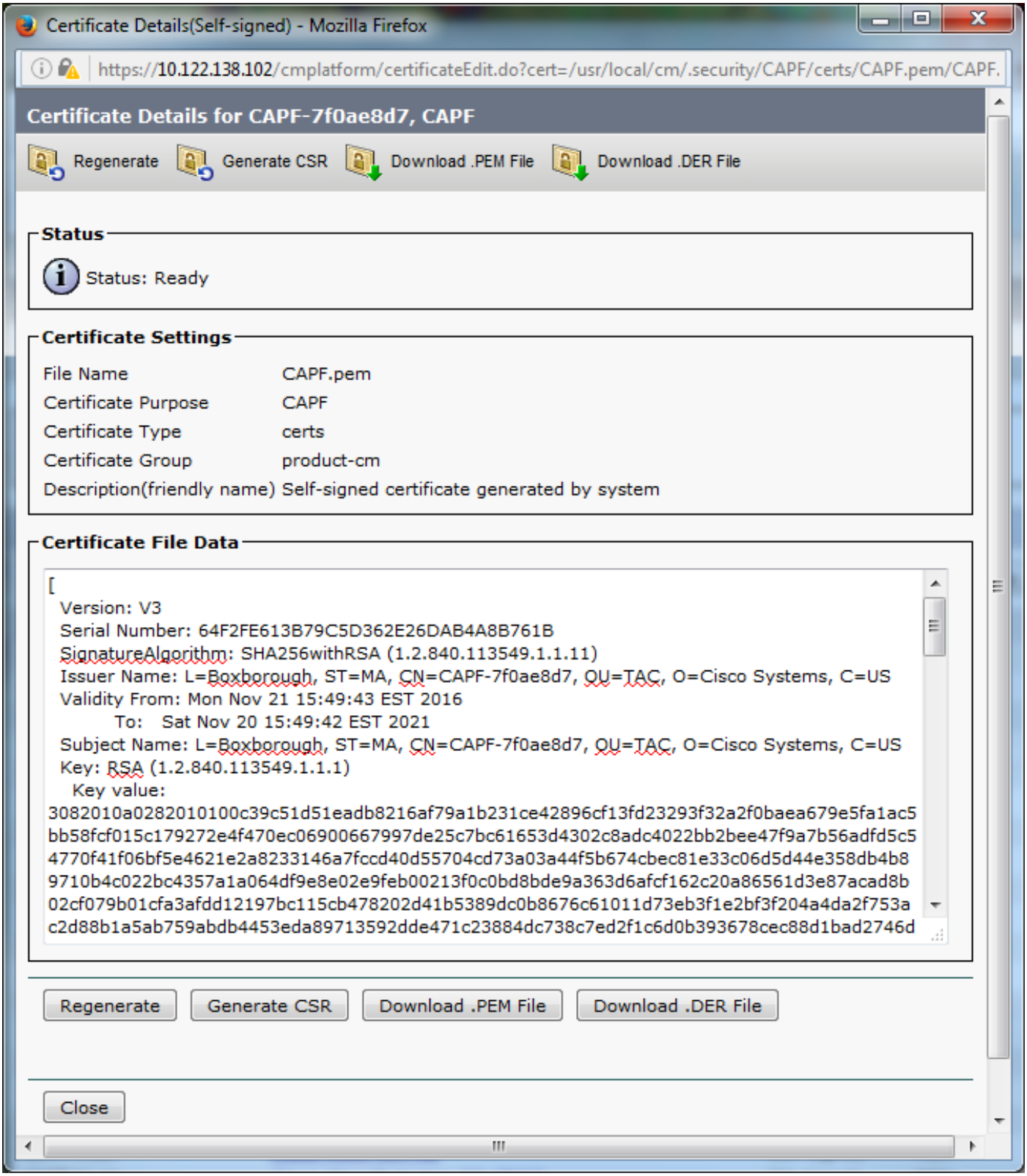
Estos servidores del laboratorio CUCM fueron utilizados para este documento:

- ao115pub - 10.122.138.102 - CUCM Publisher y servidor TFTP
- ao115sub - 10.122.138.103 - suscriptor y servidor TFTP CUCM

Verifique que no haya expirado el certificado del CAPF, ni está alrededor expirar en un futuro próximo. Navegue a **Cisco unificó el Certificate Management (Administración de certificados) del > Security (Seguridad) de la administración OS**, después la **lista del certificado del hallazgo donde está exactamente CAPF el certificado** tal y como se muestra en de la imagen.



Haga clic el **Common Name** para abrir la página de los detalles del certificado. Examine la validez **de:** y **a:** fechas en el cristal de los **datos del archivo de certificado** para determinar cuando expira el certificado, tal y como se muestra en de la imagen.



Si el certificado del CAPF ha expirado, o es pronto expirar, regenerar ese certificado. No se mueva adelante con el LSC instalan el proceso con haber expirado ni pronto expire certificado del CAPF. Esto evita la necesidad de reeditar los LSC en un futuro próximo debido al vencimiento del certificado del CAPF. Para la información sobre cómo regenerar el certificado del CAPF, refiera el artículo de la regeneración del certificado CUCM/del proceso de renovación.

Semejantemente, si usted necesita hacer su certificado del CAPF firmar por un Certificate Authority del otro vendedor, usted tiene una opción a hacer en esta etapa. Ahora complete la generación del archivo del pedido de firma de certificado (CSR) y la importación del certificado firmado del CAPF, o continúe la configuración con un LSC uno mismo-firmado para un examen preliminar. Si usted necesita un certificado firmado otro vendedor del CAPF, es generalmente

sensato configurar esta característica primero con un certificado uno mismo-firmado del CAPF, probar y verificarla, y después cambiar de frente los LSC que son firmados por un certificado firmado otro vendedor del CAPF. Esto simplifica el troubleshooting posterior, si las pruebas con el otro vendedor firmaron el fall del certificado del CAPF.

> Advertencia: Si usted regenera el certificado del CAPF o importa un certificado firmado de tercera persona del CAPF mientras que se activa y se comienza el servicio del CAPF, los teléfonos son reajustados automáticamente por CUCM. Complete estos procedimientos en una ventana de mantenimiento cuando es aceptable que los teléfonos sean reajustados. Para la referencia, vea CSCue55353 - Agregue la advertencia al regenerar el certificado TVS/CCM/CAPF ese llama por teléfono a la restauración.

> **Note**: Si su SBD de los soportes de versión CUCM, este procedimiento de instalación LSC se aplica cueste lo que cueste si su cluster CUCM se fija al modo mezclado o no. El SBD es una versión 8.0(1) y posterior de la parte de CUCM. En estas versiones de CUCM, los archivos ITL contienen el certificado para el servicio del CAPF en el CUCM Publisher. Esto permite que los teléfonos conecten con el CAPF el servicio para soportar las operaciones del certificado por ejemplo instala/actualización y Troubleshooting.

> En las versiones anteriores de CUCM, era necesario configurar el cluster para el modo mezclado para soportar las operaciones del certificado. Pues esto es no más necesario, éste reduce las barreras al uso de los LSC como certificados de identidad del teléfono para la autenticación del 802.1x o para la autenticación de cliente VPN de AnyConnect.

Funcione con el comando **ITL de la demostración** en todos los servidores TFTP en el cluster CUCM. Observe que lo hace el archivo ITL contiene un certificado del CAPF.

Por ejemplo, aquí está un extracto de la **ITL de la demostración** hecha salir del suscriptor ao115sub del laboratorio CUCM.

> **Note**: Hay una entrada de registro ITL en este archivo con una FUNCIÓN del CAPF.

> **Note**: Si su archivo ITL no tiene una entrada del CAPF, inició sesión a su editor CUCM y la confirmó se activa el servicio del CAPF. Para confirmar esto, navegue a **Cisco unificó la utilidad > las herramientas > la activación del servicio > el > Security (Seguridad) CUCM Publisher**, después activan el **servicio de la función de proxy del Certificate Authority de Cisco**. Si el servicio fue desactivado y usted acaba de activarlo, navegue a **Cisco unificó la utilidad > el Tools (Herramientas) > Control Center (Centro de control) – ofrezca los servicios > los servicios del server> CM**, después recomience Cisco servicio TFTP en todos los servidores TFTP en el cluster CUCM para regenerar el archivo ITL. También, asegúrese de que usted no golpee CSCuj78330.

> **Note**: Después de que le hagan, funcione con el comando **ITL de la demostración** en todos los servidores TFTP en el cluster CUCM para verificar que el certificado actual del CAPF CUCM Publisher ahora está incluido en el archivo.

```
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

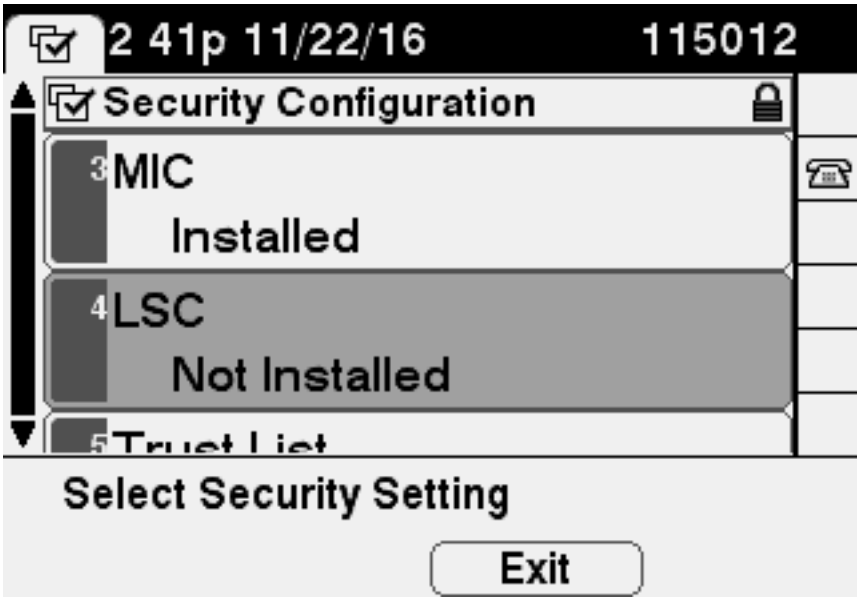
ITL Record #:5

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.
```

Con la entrada del CAPF confirmada como entrada en la ITL, usted puede completar una operación del certificado en un teléfono. En este ejemplo, un certificado de 2048 bits RSA está instalado por medio de la autenticación de la cadena nula.

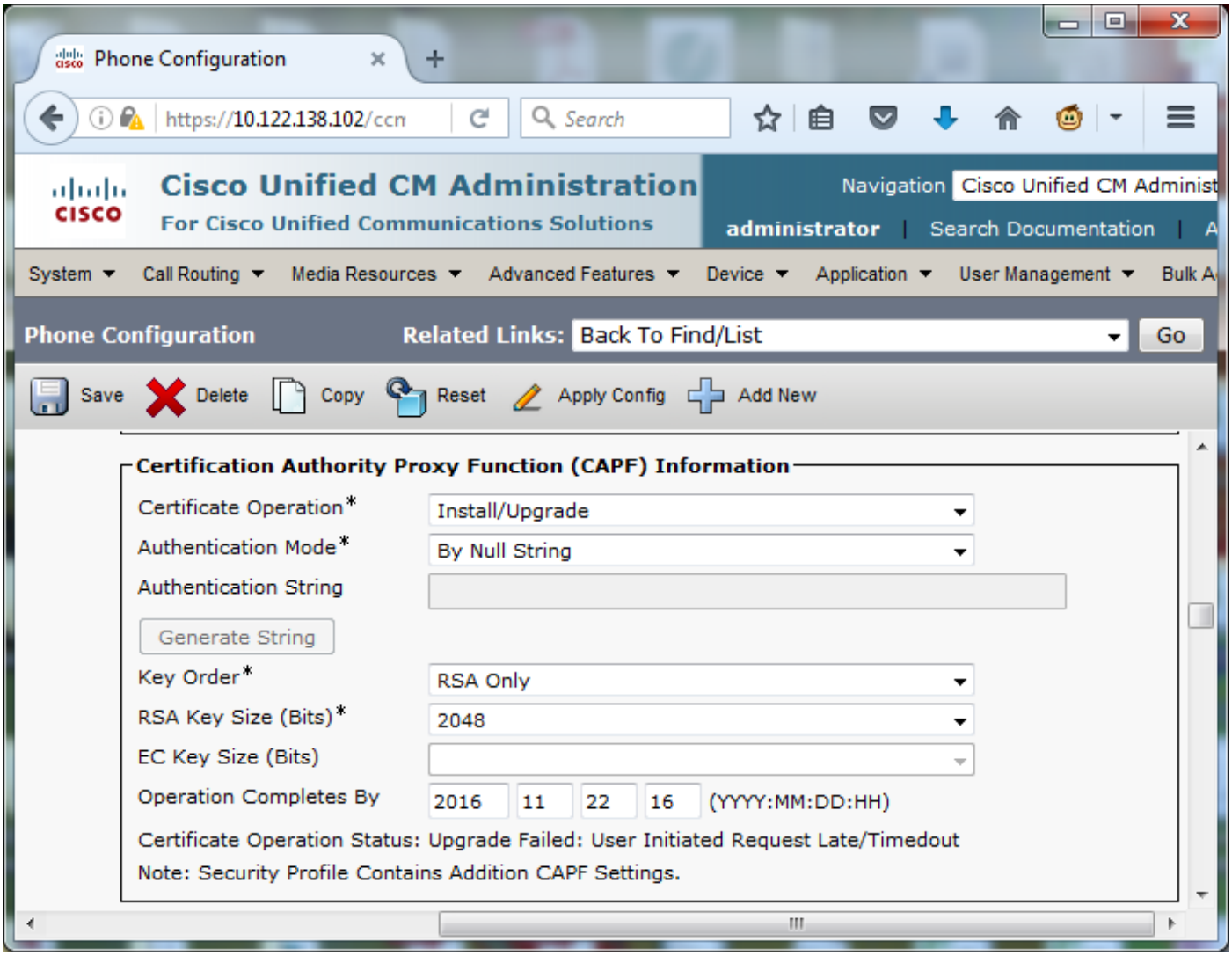
En el teléfono, verifique que un LSC todavía no esté instalado tal y como se muestra en de la imagen. Por ejemplo, en 79XX una serie llama por teléfono, navega a las **configuraciones > 4 - Configuración de seguridad > 4 - LSC**.



Abra la página de la Configuración del teléfono para su teléfono. Navegue a **Cisco unificó la administración > el Device (Dispositivo) > Phone (Teléfono) CM**.

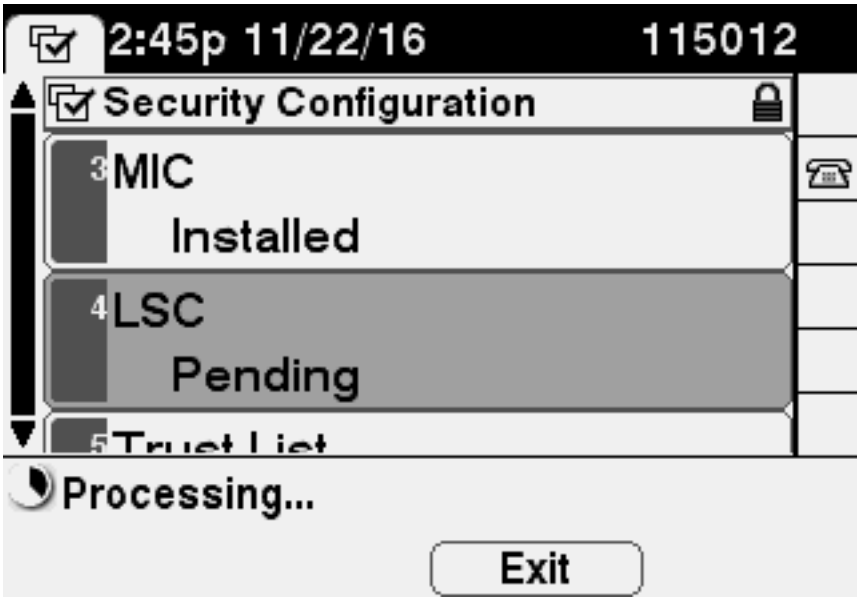
Ingrese estos detalles a la sección de información del CAPF de la configuración del teléfono, tal y como se muestra en de la imagen:

- Para la operación del certificado, selecto **instale/actualización**
- Para el modo de autenticación, seleccione **por la cadena nula**
- Por este ejemplo, deje la orden dominante, el tamaño de clave RSA (bits) y el tamaño de clave EC (bits) fijó a los **valores predeterminados del sistema**.
- Para la operación completa por, ingresan una fecha y hora que sea por lo menos una hora adentro al futuro.

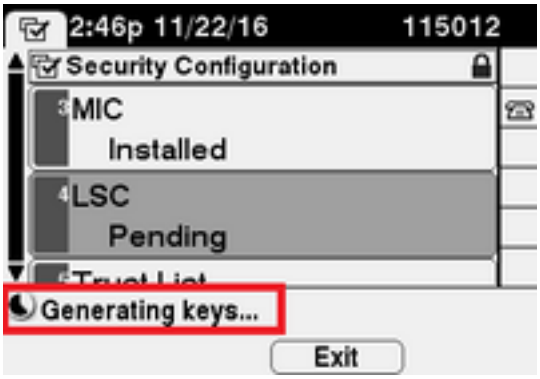


Salve sus cambios de configuración, después **aplique los Config**.

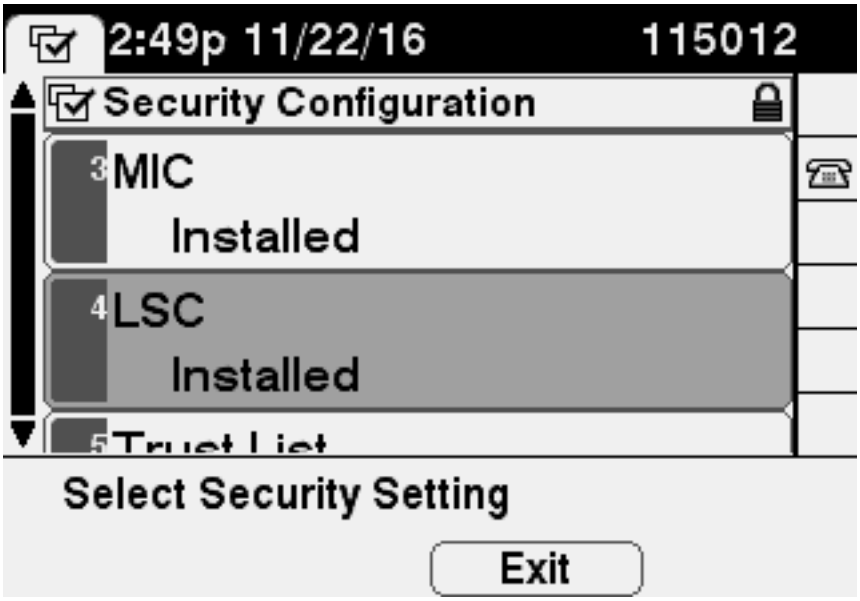
El estatus LSC en el teléfono cambia a **pendiente** tal y como se muestra en de la imagen.



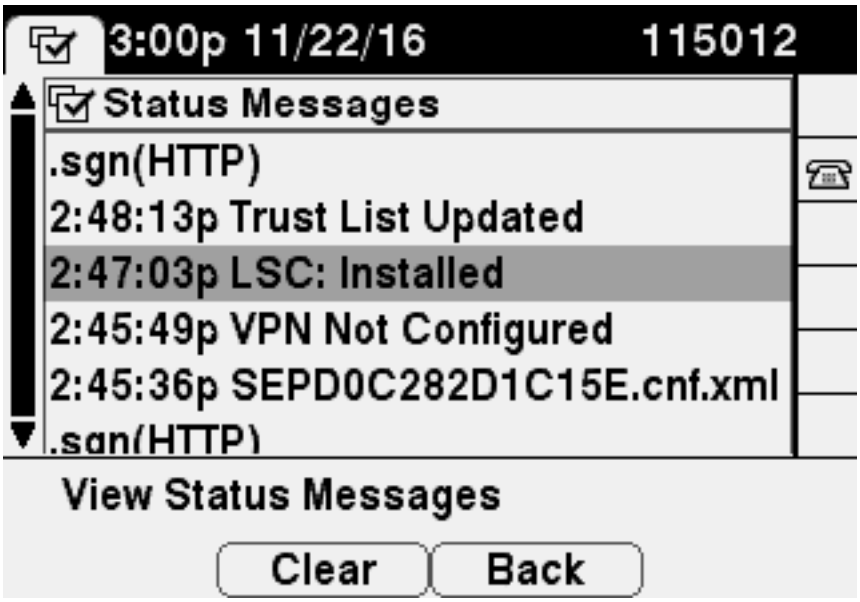
El teléfono genera las claves tal y como se muestra en de la imagen.



Las restauraciones del teléfono, y cuando la restauración completa, los cambios de estado del teléfono LSC a **instalado** tal y como se muestra en de la imagen.



Éste es también **mensajes de estado** bajo visibles en el teléfono tal y como se muestra en de la imagen.



Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Para verificar la instalación del certificado LSC en los teléfonos múltiples, refiera a la sección de informe del CAPF de la generación de la guía de la Seguridad para las Comunicaciones unificadas administrador de Cisco, la versión 11.0(1). Alternativamente, usted puede ver los mismos datos dentro de la interfaz Web de la administración CUCM por medio de los teléfonos del hallazgo por el procedimiento del estatus o de la cadena de la autentificación LSC.

Para obtener las copias de los Certificados LSC instalados en los teléfonos, refiera cómo extraer los Certificados del phonesarticle IP de Cisco.

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

Ningún servidor válido del CAPF

El LSC no puede instalar. Los mensajes de estado del teléfono no muestran **ningún servidor válido del CAPF**. Esto indica que no hay entrada del CAPF en el archivo ITL. Verifique que el servicio del CAPF fuera activado, y después recomience servicio TFTP. Verifique que el archivo ITL contenga un certificado del CAPF después de que el reinicio, reajustara el teléfono para coger el último archivo ITL, y después revise su operación del certificado. Si la Entrada de servidor del CAPF en las visualizaciones del menú de los ajustes de seguridad del teléfono como el nombre de host o Nombre de dominio totalmente calificado (FQDN), confirma el teléfono puede resolver la entrada a una dirección IP.

LSC: Conexión fallada

El LSC no puede instalar. Los mensajes de estado del teléfono muestran el **LSC: Conexión fallada**. Esto puede indicar una de estas condiciones:

- Una discordancía entre el certificado del CAPF en el archivo ITL y el certificado actual, el servicio del CAPF es funcionando.
- Se para o se desactiva el servicio del CAPF.
- El teléfono no puede alcanzar el servicio del CAPF sobre la red.

Verifique el servicio del CAPF se activa, recomienzan el servicio del CAPF, clusterwide de los servicios del reinicio TFTP, reajustan el teléfono para coger el último archivo ITL, y después revisan su operación del certificado. Si persiste el problema, tome a una captura de paquetes del teléfono y del CUCM Publisher, y analícela para ver si hay comunicación bidireccional en el puerto 3804, el puerto predeterminado del servicio del CAPF. Si no, puede haber un problema de red.

LSC: Fallado

El LSC no puede instalar. Los mensajes de estado del teléfono muestran el **LSC: Fallado**. La página web de la Configuración del teléfono muestra el **estado de la operación del certificado: Actualización fallada: Tarde iniciado usuario/Timedout de la petición**. Esto indica que la operación completa por la Fecha y hora ha expirado o es en el pasado. Ingrese una fecha y hora que sea por lo menos una hora adentro al futuro, y después revise su operación del certificado.

Información Relacionada

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

- Teléfono de AnyConnect VPN - Teléfonos IP, troubleshooting ASA, y CUCM
- Servicios de red basados en la identidad: Telefonía IP en el despliegue y la guía de configuración de redes de IEEE 802.1X-Enabled

Hay también un tipo avanzado de configuración de LSC, en quien los Certificados LSC son firmados directamente por un Certificate Authority del otro vendedor, no el certificado del CAPF.

Para los detalles, refiérase: Ejemplo de configuración CA-firmado de tercera persona de la generación y de la importación CUCM LSC

- **Soporte Técnico y Documentación - Cisco Systems**