

Habilitar la función de configuración cifrada en CUCM

Contenido

[Introducción](#)

[Antecedentes](#)

[Descripción general de la función de configuración cifrada](#)

[Habilitar la función de configuración cifrada](#)

[Troubleshoot](#)

Introducción

Este documento describe el uso de archivos de teléfono de configuración cifrada en Cisco Unified Communications Manager (CUCM).

Antecedentes

El uso de archivos de configuración cifrados para teléfonos es una función de seguridad opcional disponible en CUCM.

No es necesario ejecutar el clúster de CUCM en modo mixto para que esta función funcione correctamente, ya que la información de certificado de función proxy de autoridad certificadora (CAPF) se incluye en el archivo de lista de confianza de identidad (ITL).

Nota: Esta es la ubicación predeterminada para todas las versiones 8.X y posteriores de CUCM. Para las versiones de CUCM anteriores a la versión 8.X, debe asegurarse de que el clúster se ejecute en modo mixto si desea utilizar esta función.

Descripción general de la función de configuración cifrada

En esta sección se describe el proceso que se produce cuando se utilizan archivos de teléfono de configuración cifrada dentro de CUCM.

Cuando habilita esta función, restablece el teléfono y descarga el archivo de configuración, recibe una solicitud para el archivo con una extensión `.cnf.xml.sgn`:

```
73.824626 10.147.94.55 10.48.46.4 HTTP GET /ITLSEPA45630BBFA40.tlv HTTP/1.1
74.110351 10.147.94.55 10.48.46.4 HTTP GET /SEPA45630BBFA40.cnf.xml.sgn HTTP/1.1
```



Sin embargo, después de habilitar la función de configuración cifrada en CUCM, el servicio TFTP

ya no genera un archivo de configuración completo con la extensión **.cnf.xml.sgn**. En su lugar, genera el archivo de configuración parcial, como se muestra en el siguiente ejemplo.

Nota: Cuando se utiliza este método por primera vez, el teléfono compara el hash MD5 del certificado telefónico del archivo de configuración con el hash MD5 del certificado de significación local (LSC) o los certificados instalados de fabricación (MIC).

```
HTTP/1.1 200 OK
Content-length: 759
Cache-Control: no-store
Content-type: */*
<fullConfig>False</fullConfig>
<loadInformation>SIP75.9-3-1SR2-1S</loadInformation>
<ipAddressMode>0</ipAddressMode>
<capfAuthMode>0</capfAuthMode>
<capfList>
<capf>
<phonePort>3804</phonePort>
<processNodeName>10.48.46.4</processNodeName>
</capf>
</capfList>
```

</device>

Si el teléfono identifica un problema, intenta iniciar una sesión con CAPF, a menos que el modo de autenticación CAPF coincida con *By Authentication Strings*, en cuyo caso debe ingresar manualmente la cadena. Estos son algunos de los problemas que el teléfono podría identificar:

- El hash no coincide.
- El teléfono no contiene ningún certificado.
- El valor MD5 está en blanco (como en el ejemplo anterior).



Nota: El teléfono inicia una sesión de seguridad de la capa de transporte (TLS) al servicio CAPF en el puerto 3804 de forma predeterminada.

El certificado CAPF debe ser conocido para el teléfono, por lo que debe incluirse en el archivo ITL o en el archivo de lista de confianza de certificados (CTL) (si el clúster se ejecuta en modo mixto).

76.804108	10.147.94.55	10.48.46.4	TCP	51292 > cisco-con-capf [ACK] seq=1 ack=1 win=5840 Len=0 TSV=159397051 TSER=162819875
76.805662	10.147.94.55	10.48.46.4	TLSv1	Client Hello
76.805690	10.48.46.4	10.147.94.55	TCP	cisco-con-capf > 51292 [ACK] seq=1 ack=55 win=5792 Len=0 TSV=162819927 TSER=159397051
76.805866	10.48.46.4	10.147.94.55	TLSv1	server hello, certificate, server Hello done
76.855825	10.147.94.55	10.48.46.4	TCP	51292 > cisco-con-capf [ACK] seq=55 ack=720 win=7200 Len=0 TSV=159397056 TSER=162819927
76.864878	10.147.94.55	10.48.46.4	TLSv1	Client Key Exchange, change cipher spec, Encrypted Handshake Message
76.870861	10.48.46.4	10.147.94.55	TLSv1	Change cipher spec, Encrypted Handshake Message
76.871012	10.48.46.4	10.147.94.55	TLSv1	Application data, Application data

Después de establecer la comunicación CAPF, el teléfono envía información al CAPF sobre el LSC o el MIC que se utiliza. A continuación, CAPF extrae la clave pública del teléfono del LSC o MIC, genera un hash MD5 y almacena los valores para la clave pública y el hash de certificado en la base de datos de CUCM.

```
admin:run sql select md5hash,name from device where name='SEPA45630BBFA40'
md5hash name
```

```
=====
6e566143c1c14566c9da943d949a79c8 SEPA45630BBFA40
```

Después de almacenar la clave pública en la base de datos, el teléfono se restablece y solicita un nuevo archivo de configuración. El teléfono intenta descargar el archivo de configuración con la extensión **cnf.xml.sgn** una vez más.



```
128.078706 10.147.94.55 10.48.46.4 HTTP GET /SEPA45630BBFA40.cnf.xml.sgn HTTP/1.1
```

```
HTTP/1.1 200 OK
Content-length: 759
Cache-Control: no-store
Content-type: */*
<fullConfig>False</fullConfig>
<loadInformation>SIP75.9-3-1SR2-1S</loadInformation>
<ipAddressMode>0</ipAddressMode>
<capfAuthMode>0</capfAuthMode>
<capfList>
<capf>
<phonePort>3804</phonePort>
<processNodeName>10.48.46.4</processNodeName>
</capf>
</capfList>
```

```
</device>
```

El teléfono compara el **cerHash** otra vez y, si no detecta el problema, descarga el archivo de configuración cifrado con la extensión **.cnf.xml.enc.sgn**.



```
130.708816 10.147.94.55 10.48.46.4 HTTP GET /SEPA45630BBFA40.cnf.xml.enc.sgn HTTP/1.1
```

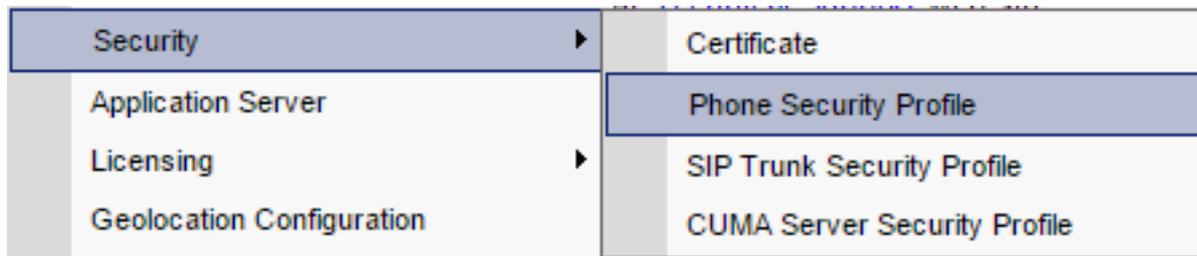
```
.....c..)CN=cucm85;OU=It;O=Cisco;L=KRK;ST=PL;C=PL....Z.....)CN=cucm85;
OU=It;O=Cisco;L=KRK;ST=PL;C=PL.....
```

```
.....C.<...Y6.Lh.|(..w+...0.a.&.
O.....V...T...Z..R^..f....|.=.e.@...5.....G...[.....n.....=
.A..H.(...Z...{.!%[... SEPA45630BBFA40.cnf.xml.enc.sgn....R.DD..M.....
Uu.C..@.....
.....m.b.....6y ..x.^b..-8.^..^'.4.<Wb.n.....5...we.0@..g..
V7.,..r.9
Qs>..) .w....pt/...}A. ' ]
.r.t%G..d_ ;u.rEI.pr.F
.....M..r...o.N
.=.g.^P....Pz....J..E.S...d|Z).....J..&..I....7.r..g8.{f..o.....:~..U...5G+V.
[...]
```

Habilitar la función de configuración cifrada

Para habilitar los archivos de configuración cifrada del teléfono, debe crear un nuevo perfil de seguridad del teléfono (o editar uno actual) y asignarlo al teléfono. Complete estos pasos para habilitar la función de configuración cifrada en CUCM:

1. Inicie sesión en la página de administración de CUCM y navegue hasta **Sistema > Seguridad > Perfil de seguridad del teléfono**:



2. Copie un perfil de seguridad del teléfono actual o cree uno nuevo y marque la casilla de verificación **TFTP Encrypted Config**:

Phone Security Profile Configuration

 Save

Status

 Status: Ready

Phone Security Profile Information

Product Type: Cisco 7942
Device Protocol: SCCP
Name*
Description
Device Security Mode
 TFTP Encrypted Config

Phone Security Profile CAPF Information

Authentication Mode*
Key Size (Bits)*
 Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

3. Asigne el perfil al teléfono:

Protocol Specific Information

Packet Capture Mode*
Packet Capture Duration
BLF Presence Group*
Device Security Profile*
SUBSCRIBE Calling Search Space
 Unattended Port
 Require DTMF Reception
 RFC2833 Disabled

Device Security Profile* dropdown menu options:
 -- Not Selected --
 Cisco 7942 - Standard SCCP Encrypted Config
 Cisco 7942 - Standard SCCP Non-Secure Profile
 Universal Device Template - Model-independent Security Profile

Troubleshoot

Complete estos pasos para resolver problemas del sistema con respecto a la función de configuración cifrada:

1. Asegúrese de que el servicio CAPF esté activo y se ejecute correctamente en el nodo Publisher del clúster de CUCM.
2. Descargue el archivo de configuración parcial y verifique que el puerto y la dirección IP del servicio CAPF sean accesibles desde el teléfono.

3. Verifique la comunicación TCP en el puerto 3804 al nodo Publisher.
4. Ejecute el comando SQL (Lenguaje de consulta estructurado) mencionado anteriormente para verificar si el servicio CAPF tiene información sobre el LSC o el MIC que utiliza el teléfono.
5. Si el problema persiste, es posible que se le solicite que recopile información adicional del sistema. Reinicie el teléfono y recopile esta información:

Registros de la consola del teléfono
Registros TFTP de Cisco
Registros de Cisco CAPF
Capturas de paquetes desde CUCM y el teléfono

Consulte estos recursos para obtener información adicional sobre cómo ejecutar capturas de paquetes desde CUCM y el teléfono:

- [Recopilación de trazas de CUCM de CUCM 8.6.2 para SR de TAC](#)
- [Captura de paquetes en el modelo de dispositivo Unified Communications Manager](#)
- [Recopilación de una captura de paquetes de un teléfono IP de Cisco](#)

En los registros y capturas de paquetes, debe asegurarse de que el proceso descrito en las secciones anteriores funciona correctamente. Concretamente, verifique que:

- El teléfono descarga el archivo de configuración parcial con la información CAPF correcta.
- El teléfono se conecta a través de TLS al servicio CAPF y la información sobre LSC o MIC se actualiza en la base de datos.
- El teléfono descarga el archivo de configuración cifrado completo.