Habilite la característica de configuración cifrada en el CUCM

Contenido

Introducción

Este documento describe el uso de los archivos cifrados del teléfono de la configuración en el administrador de las Comunicaciones unificadas de Cisco (CUCM).

Antecedentes

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

Le no requieren ejecutar el cluster CUCM en el modo mezclado para que esta característica funcione correctamente, pues la información del certificado de la función de proxy del Certificate Authority (CAPF) se contiene dentro del archivo de la lista de la confianza de la identidad (ITL).

> **Note**: Ésta es la ubicación predeterminada para todas las versiones 8.X CUCM y posterior. Para las versiones CUCM antes de la versión 8.X, usted debe asegurarse de que el cluster se ejecute en el modo mezclado si usted desea de utilizar esta característica.

Descripción general de características cifrada de la configuración

Esta sección describe el proceso que ocurre cuando los archivos cifrados del teléfono de la configuración se utilizan dentro del CUCM.

Cuando usted habilita esta característica, reajusta el teléfono, y descarga el archivo de configuración, usted recibe una petición 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 que la característica de configuración cifrada se habilite en el CUCM, servicio TFTP genera no más un archivo de configuración total con la **extensión .cnf.xml.sgn.** En lugar, genera el archivo de configuración parcial, tal y como se muestra en del próximo ejemplo.

> **Note**: Cuando usted utiliza este método por primera vez, el teléfono compara el hash MD5 del certificado del teléfono en el archivo de configuración al hash MD5 localmente - del certificado significativo (LSC) o de los Certificados instalados 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>
<certHash></certHash>
<encrConfig>true</encrConfig>
</device>
```

Si el teléfono identifica un problema, intenta iniciar una sesión con el CAPF, a menos que el modo de autenticación del CAPF corresponda con *por las cadenas de la autentificación*, en este caso usted debe ingresar manualmente la cadena. Aquí están algunos problemas que el teléfono pudo identificar:

- El hash no hace juego.
- El teléfono no contiene un certificado.
- El valor MD5 es en blanco (como en el ejemplo anterior).

> **Note**: El teléfono inicia una sesión de Transport Layer Security (TLS) al servicio del CAPF en el puerto 3804 por abandono.

El certificado del CAPF se debe saber para el teléfono, así que debe ser incluido en o el archivo ITL o Certificate Trust List (Lista de confianza del certificado) el archivo (CTL) (si el cluster se ejecuta en el modo mezclado).

```
76.804108  10.147.94.55   10.48.46.4     TCP    51292 > cisco-com-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-com-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-com-capf [ACK] Seq=55 Ack=720 Win=7280 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 que se establezca la comunicación del CAPF, el teléfono envía la información al CAPF sobre el LSC o el MIC se utiliza que. El CAPF después extrae la clave pública del teléfono del LSC o del MIC, genera un hash MD5, y salva los valores para el hash de la clave pública y del certificado en la base de datos CUCM.

```
admin:run sql select md5hash,name from device where name='SEPA45630BBFA40'
md5hash name
================================ ==============
6e566143c1c14566c9da943d949a79c8 SEPA45630BBFA40
```

Después de que la clave pública se salve en la base de datos, el teléfono reajusta y pide un nuevo archivo de configuración. El teléfono intenta descargar el archivo de configuración con la **extensión cnf.xml.sgn de nuevo**.


```
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>
<certHash>6e566143c1c14566c9da943d949a79c8</certHash>
<encrConfig>true</encrConfig>
</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
```

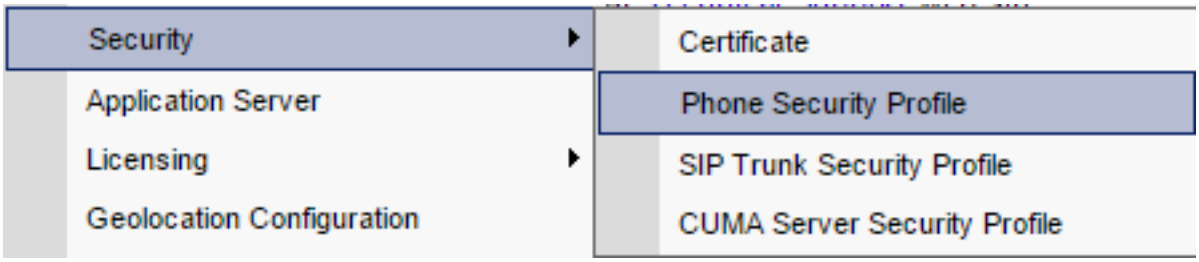
```
............c..)CN=cucm85;OU=It;O=Cisco;L=KRK;ST=PL;C=PL....Z.........)CN=cucm85;
```

```
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.
[...]
```

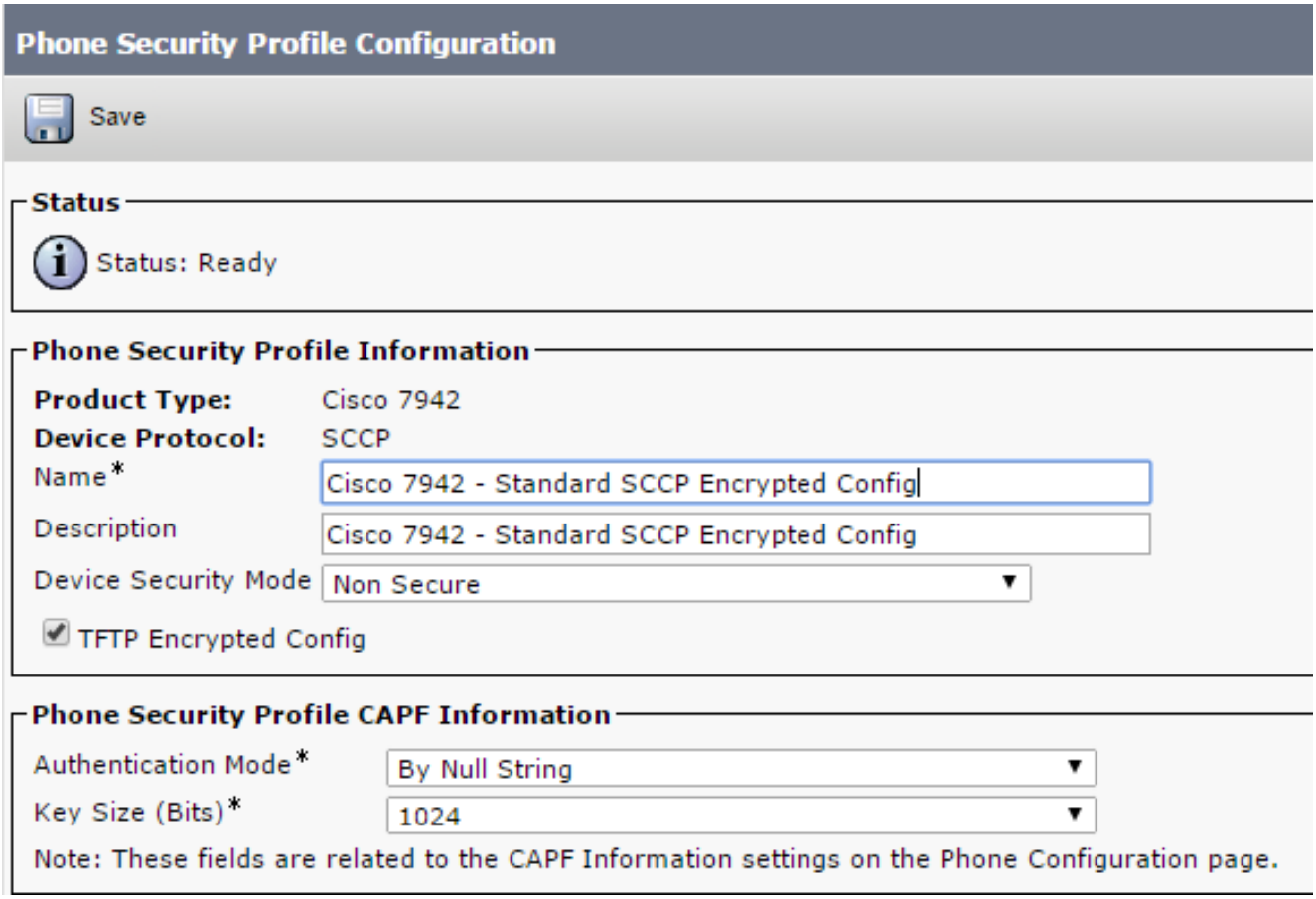
Característica de configuración cifrada permiso

Para habilitar los archivos cifrados del teléfono de la configuración, usted debe crear un nuevo (o editar una corriente) perfil de seguridad del teléfono y asignarlo al teléfono. Complete estos pasos para habilitar la característica de configuración cifrada en el CUCM:

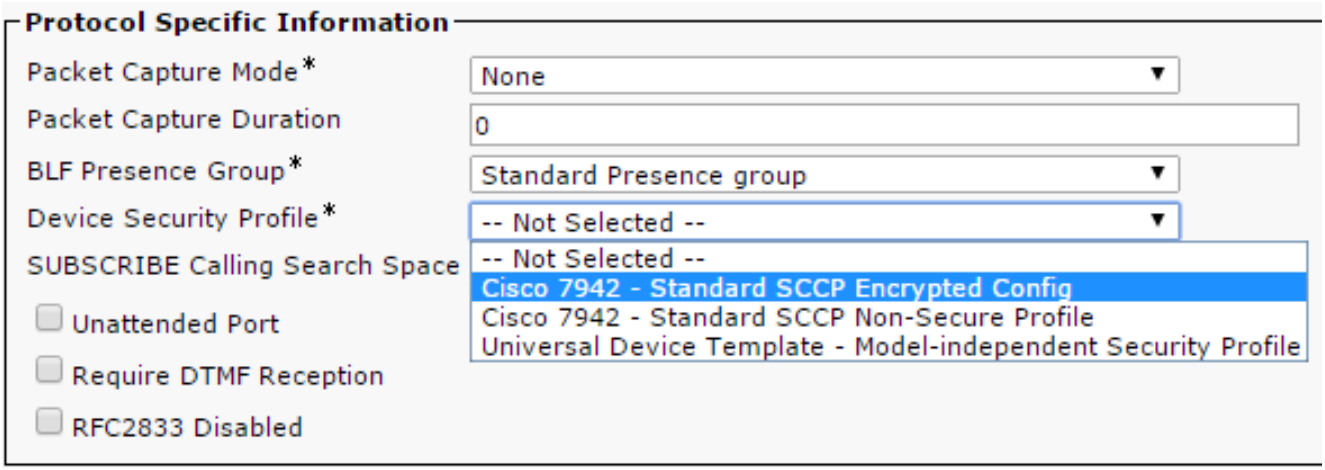
1. El registro en la página de administración CUCM y navega al **> Security (Seguridad) del sistema > al perfil de seguridad del teléfono**:



2. Copie una corriente, o cree un nuevo, llame por teléfono al perfil de seguridad y marque la casilla de verificación **cifrada TFTP de los Config**:



3. Asigne el perfil al teléfono:



Troubleshooting

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

1. Asegúrese de que el servicio del CAPF sea activo y se ejecute correctamente en el nodo de Publisher en el cluster CUCM.

2. Descargue el archivo de configuración parcial y verifiquelo que el puerto y la dirección IP del servicio del CAPF son accesibles del teléfono.

3. Verifique la comunicación TCP en el puerto 3804 al nodo de Publisher.

4. Funcione con el comando previamente mencionado del Lenguaje de consulta estructurado (SQL) para verificar si el servicio del CAPF tiene información sobre el LSC o el MIC que es utilizado por el teléfono.

5. Si todavía persiste el problema, usted puede ser que sea requerido recoger la información adicional del sistema. Recomience el teléfono y recoja esta información:

   Llame por teléfono a los registros de la consolaRegistros de Cisco TFTPRegistros del CAPF de CiscoCapturas de paquetes del CUCM y del teléfono

Refiera a estos recursos para más información sobre cómo funcionar con a las capturas de paquetes del CUCM y del teléfono:

- Recogida de las trazas CUCM de CUCM 8.6.2 para un SENIOR de TAC
- Captura de paquetes en el modelo del dispositivo del administrador de las Comunicaciones unificadas
- Recogida de una captura de paquetes de un Cisco IP Phone

En los registros y las capturas de paquetes, usted debe asegurarse de que funcione el proceso descrito en las secciones anteriores correctamente. Específicamente, verifique eso:

- El teléfono descarga el archivo de configuración parcial con la información correcta del CAPF.
- El teléfono conecta vía TLS con el servicio del CAPF, y eso la información sobre el LSC o el MIC se pone al día en la base de datos.
- El teléfono descarga el archivo de configuración cifrado completo.