在CUCM上启用加密配置功能

目录

简介

本文档介绍在思科统一通信管理器(CUCM)上使用加密的配置电话文件。

背景信息

对电话使用加密配置文件是CUCM中提供的可选安全功能。

您无需在混合模式下运行CUCM集群，以便此功能正常运行，因为证书颁发机构代理功能(CAPF)证书信息包含在身份信任列表(ITL)文件中。

> **注意**：这是所有CUCM版本8.X及更高版本的默认位置。对于8.X版之前的CUCM版本，如果您希望使用此功能，必须确保集群在混合模式下运行。

加密配置功能概述

本节介绍在CUCM中使用加密的配置电话文件时发生的过程。

启用此功能、重置电话并下载配置文件后，您会收到对扩展名为.cnf.xml.sgn的**文件的请**求：

```
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
```

但是，在CUCM上启用加密配置功能后，TFTP服务不再生成扩展名为.cnf.xml.sgn的完**整配置文**件。相反，它会生成部分配置文件，如下例所示。

> **注意**：首次使用此方法时，电话将配置文件中电话证书的MD5哈希值与本地有效证书(LSC)或制造安装证书(MIC)的MD5哈希值进行比较。

```
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>
```

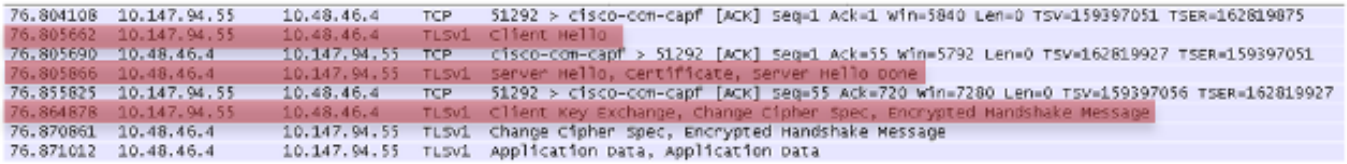
```
</device>
```

如果电话发现问题，它会尝试启动与CAPF的会话，除非CAPF身份验证模式与*By Authentication Strings*匹配，在这种情况下，您必须手动输入字符串。以下是电话可能识别的一些问题：

- 哈希不匹配。
- 电话不包含证书。
- MD5值为空（如上例所示）。

注意：默认情况下，电话在端口3804上发起到CAPF服务的传输层安全(TLS)会话。

CAPF证书必须为电话已知，因此必须包含在ITL文件或证书信任列表(CTL)文件中（如果集群在混合模式下运行）。



建立CAPF通信后，电话会向CAPF发送有关所使用的LSC或MIC的信息。 然后，CAPF从LSC或MIC提取电话公钥，生成MD5哈希值，并将公钥和证书哈希值存储在CUCM数据库中。

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

将公钥存储在数据库中后，电话会重置并请求新的配置文件。电话再次尝试下载扩展名为**cnf.xml.sgn的**配置文件。


```
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>
```

电话再次比较**cerHash，如果它未检测到问题，则下载带有.cnf.xml.enc.sgn扩展名的加密配置文**件。

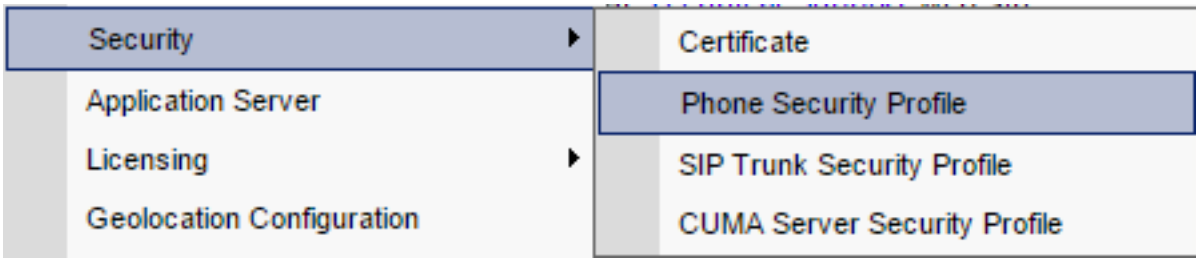

```
130.708816 10.147.94.55     10.48.46.4     HTTP   GET /SEPA45630BBFA40.cnf.xml.enc.sgn HTTP/1.1
```

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

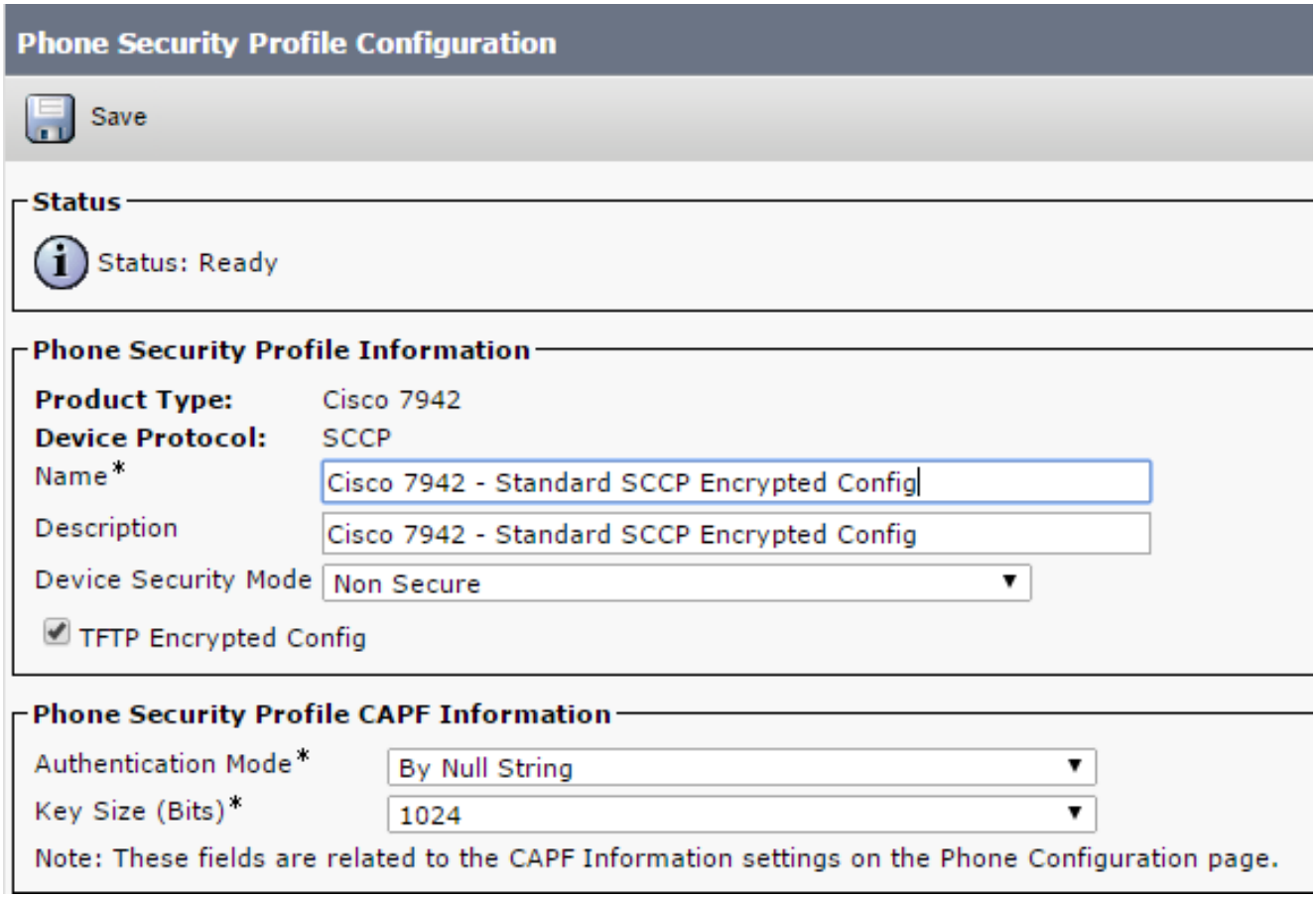
启用加密配置功能

要启用加密的配置电话文件，必须创建新的（或编辑当前的）电话安全配置文件并将其分配给电话。要在CUCM上启用加密配置功能，请完成以下步骤：

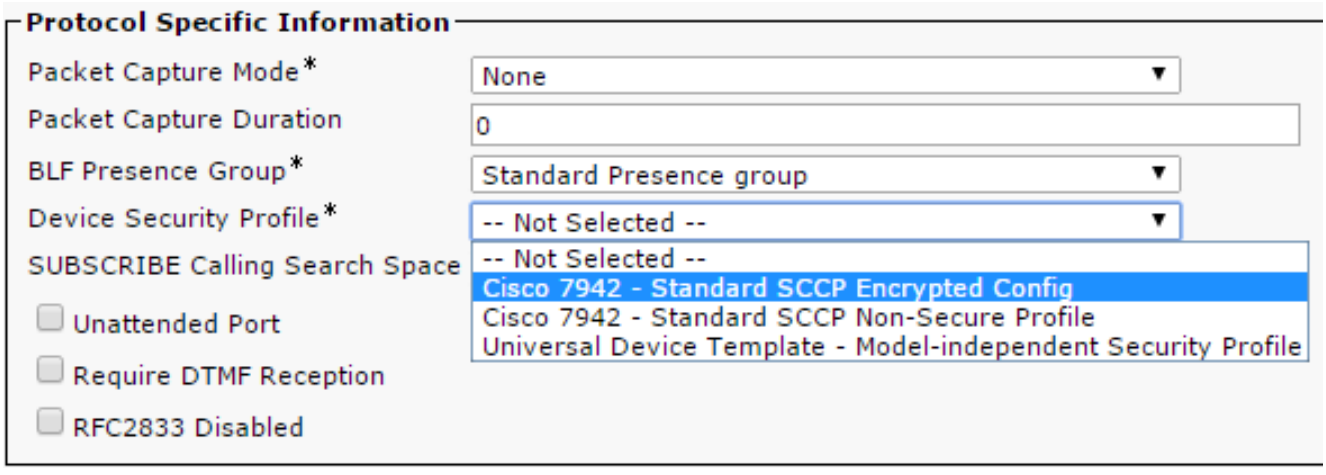
1. 登录CUCM Administration页面并导航至System > Security > **Phone Security Profile**:



2. 复制当前或创建新的电话安全配置文件并选中**TFTP加密配**置复选框：



3. 将配置文件分配给电话：



故障排除

要排除与加密配置功能相关的系统问题，请完成以下步骤：

1. 确保CAPF服务处于活动状态并在CUCM群集的发布方节点上正确运行。

2. 下载部分配置文件，并验证CAPF服务的端口和IP地址是否可从电话访问。

3. 检验端口3804与发布方节点的TCP通信。

4. 运行前面提到的结构化查询语言(SQL)命令，以验证CAPF服务是否包含有关电话使用的LSC或MIC的信息。

5. 如果问题仍然存在，可能需要您从系统收集其他信息。重新启动电话并收集以下信息：

电话控制台日志Cisco TFTP日志思科CAPF日志从CUCM和电话捕获数据包

有关如何从CUCM和电话运行数据包捕获的详细信息，请参阅以下资源：

- 从 CUCM 8.6.2 为 TAC SR 收集 CUCM 跟踪信息
- 统一通信管理器设备型号上的数据包捕获
- 从思科IP电话收集数据包捕获

在日志和数据包捕获中，必须确保前面各节中描述的过程正常运行。具体而言，请验证：

- 电话下载包含正确CAPF信息的部分配置文件。
- 电话通过TLS连接到CAPF服务，并且有关LSC或MIC的信息会在数据库中更新。
- 电话下载完整的加密配置文件。