排除CUCM中证书续订的常见问题

简介

本文档介绍在Cisco Unified Communications Manager(CUCM)中重新生成证书后的常见问题以及如何解决这些问题。

先决条件

要求

Cisco 建议您了解以下主题：

- CUCM证书续订流程
- CUCM GUI界面
- Expressway服务器
- 通过CUCM进程注册设备
- 证书颁发机构代理功能
- Cisco Unified Communications Manager安全指南

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CUCM版本15

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

业务影响

此表显示您的操作中每次证书续订对业务的影响。仔细阅读此信息。根据每个证书的风险级别，在数小时后或安静时段续订所需的证书。

Low Impact Medium Impact. High Impact.

Type	Risk	Trust List	Impact	Phone Restart	Service Restart
Tomcat		-	Web services, SSO, EM/EMCC Login	None	Tomcat
IPSec		-	DRS, Ipsec Tunnels	None	DRF Master/Local
CAPF		CTL + ITL	LSC must be updated, secure features	All	CAPF
Callmanager		CTL + ITL	Registration, TL issues, Trunks, CTI	All	CM,CTI,TFTP
TVS		ITL	Verification of TLs, CFG files, https connection	Some	TVS
ITLRecovery		CTL + ITL	Signer or SAST backup for ITL/CTL	All	

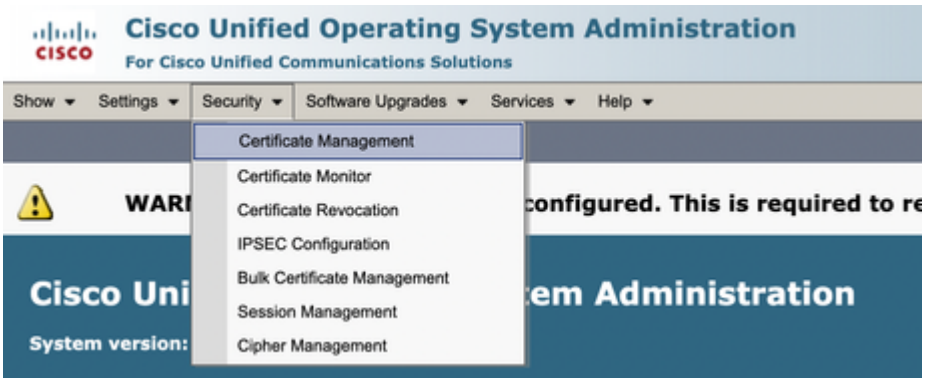
情形 1：电话在呼叫管理器、TVS和ITL证书续订后未注册

注意：此方案适用于CUCM混合模式和非安全集群下的部署，此外，还适用于自签名证书和CA证书。

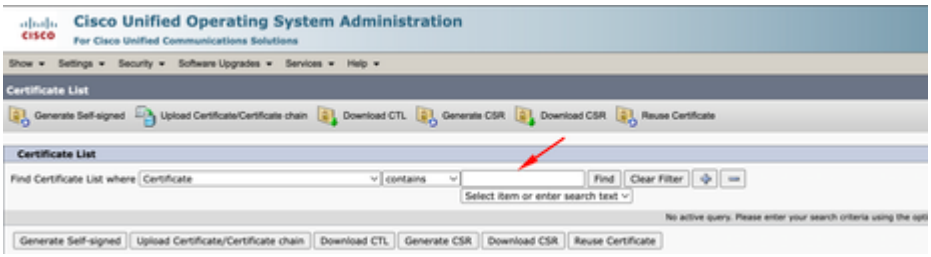
当Call Manager、TVS和ITL证书过期并且它们同时续订时，这会导致所有电话处于未注册状态，从而对系统造成重大影响，这是预期行为，因为我们将触发电话不信任CUCM。

确认

1.确保证书在Cisco Unified OS Administration > Security > Certificate Management下已过期

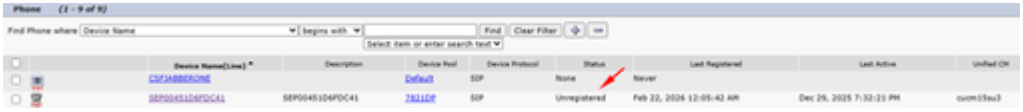


2.按Callmanager、TVS或ITL在页面顶部的过滤器下搜索，并使用包含或开头为选项：



3.证书必须在到期列下显示最新和详细内容（对于TVS和ITL证书相同）

4.一旦在证书续订后验证一切正常，电话将显示为Unregistered状态。



解决方案

有2个选项可以解决此问题：

1. 对电话执行出厂重置，使电话删除当前的安全设置并允许电话获取新证书
2. 从发布方节点上的CLI更新ITL和CTL证书并使用命令 utils itl reset localkey。
   此步骤影响所有电话，包括已注册的电话，请确保在数小时后执行此操作。

场景2：在Tomcat证书续订后，单点登录不起作用

注意：此方案可应用于使用集群范围协议或单节点协议进行单点登录配置的部署

使用单点登录(SSO)登录CUCM时，它显示错误消息¨Error while processing saml response¨或

¨Error while processing saml response无法解密密钥¨

确认

1. 确保所有节点包含有效的tomcat证书（如果自签名）或包含关联的新多san tomcat证书。
2. 通过CLI在所有CUCM节点中使用set samltrace level debug以激活调试级别的SSO日志
3. 通过再次登录CUCM并使用SSO方法重新创建问题。
4. 在事件发生后收集Tomcat SSO日志，并验证您是否收到以下消息：
   -

```
2026-01-10 06:06:31,274 ERROR [http-nio-81-exec-157]  cpi.sso.saml.sp.security.authenticatio
com.sun.identity.saml2.common.SAML2Exception: Failed to decrypt the secret key.
              at com.sun.identity.saml2.xmlenc.FMEncProvider.getEncryptionKey(FMEncProvider.
              at com.sun.identity.saml2.xmlenc.FMEncProvider.decrypt(FMEncProvider.java:607)
              at com.sun.identity.saml2.assertion.impl.EncryptedAssertionImpl.decrypt(Encryp
...
```

解决方案

在Tomcat证书续订后导出CUCM元数据，并导入到身份提供程序服务器，以确保他们具有用于此通信的新tomcat证书。

在启用SSO部署的情况下更新tomcat的过程：

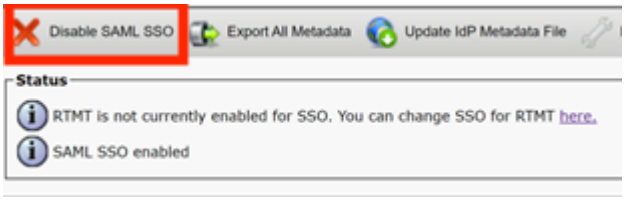
⚠ 警告：技术支持中心(TAC)建议采取后续步骤，以防止在更新Tomcat证书后出现任何问题，并建议在数小时后执行此过程。

Low Impact

1.在所有CUCM节点中禁用SSO

- 访问CM Administration > System > SAML Single Sign-on

- 选择禁用SAML SSO

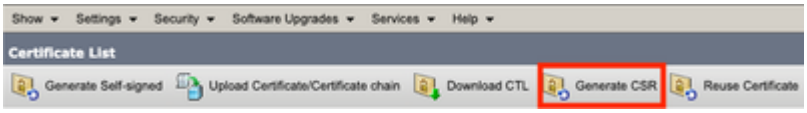


- 如果使用每节点协议，则需要通过GUI在所有其余节点中执行此过程。

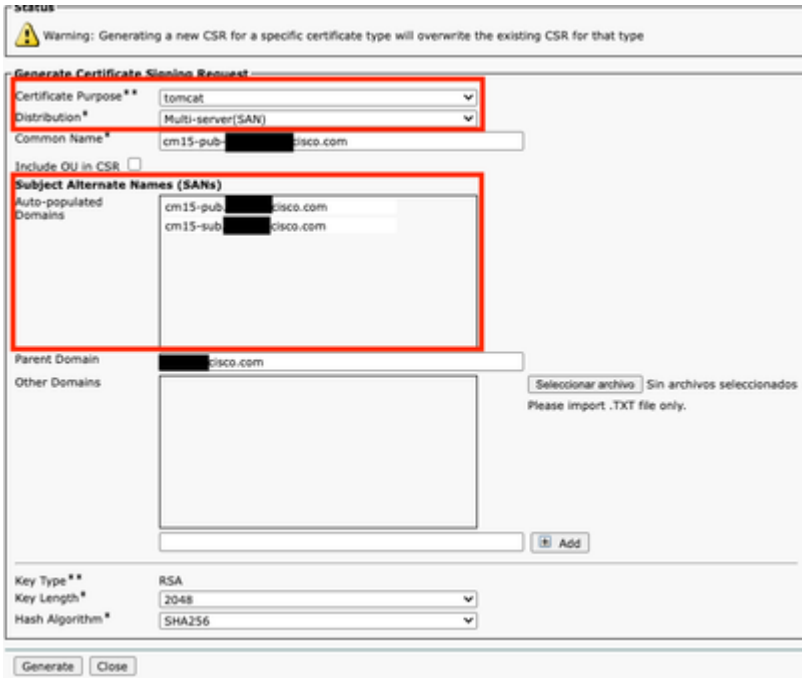
2.在CUCM集群中续订Tomcat证书

在CUCM集群中续订Tomcat multi-san证书的整体过程：

- 导航到OS administration > Security > Certificate management。
- 选择生成 CSR



- 在Certificate Portuse中选择Tomcat。
- 选择Multi-SAN in Distribution。
- 确保集群中的所有节点都列在自动填充的域下。



- 选择生成。确保在集群中的所有节点中创建CSR。
- 从CUCM发布服务器下载生成的CSR并使用证书颁发机构(CA)服务器对其进行签名。
- 转至OS administration > Security > Certificate management。选择Upload certificate/Certificate chain。
- 以Tomcat-trust身份上传CA证书。
- 重复步骤6，现在将Tomcat签名证书作为Tomcat上传。
- 完成并验证所有节点都应用了新的tomcat证书后，使用此命令utils service restart Cisco Tomcat，在集群中的所有节点中通过CLI重新启动Tomcat服务。

有关详细信息，请参阅以下文档：

- 重新生成Tomcat自签名证书
- 重新生成Tomcat CA签名证书。

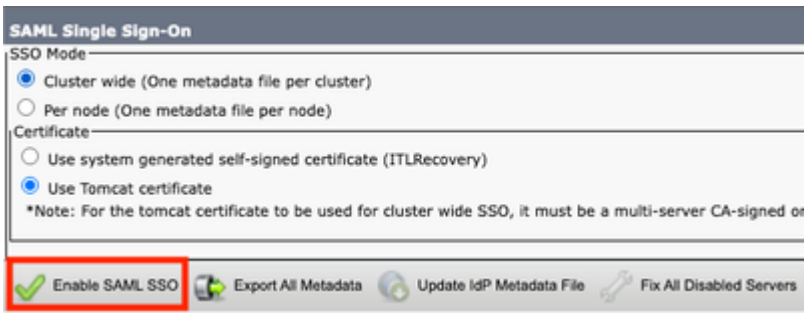
3.导出服务提供商(SP)元数据

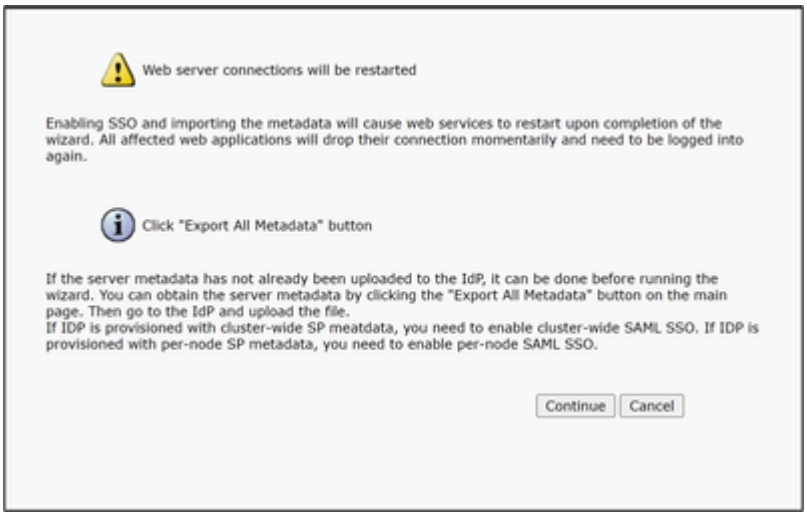
- 转至CM administration > System > Single Sign-On
- 配置SSO选项(在本例中，在SSO模式上配置集群范围,在证书上使用tomcat证书配置为示例)，然后选择导出所有元数据

- 将SP元数据导入到身份提供程序(IdP)服务器。有关详细信息，请参阅在身份提供程序上配置SAML SSO

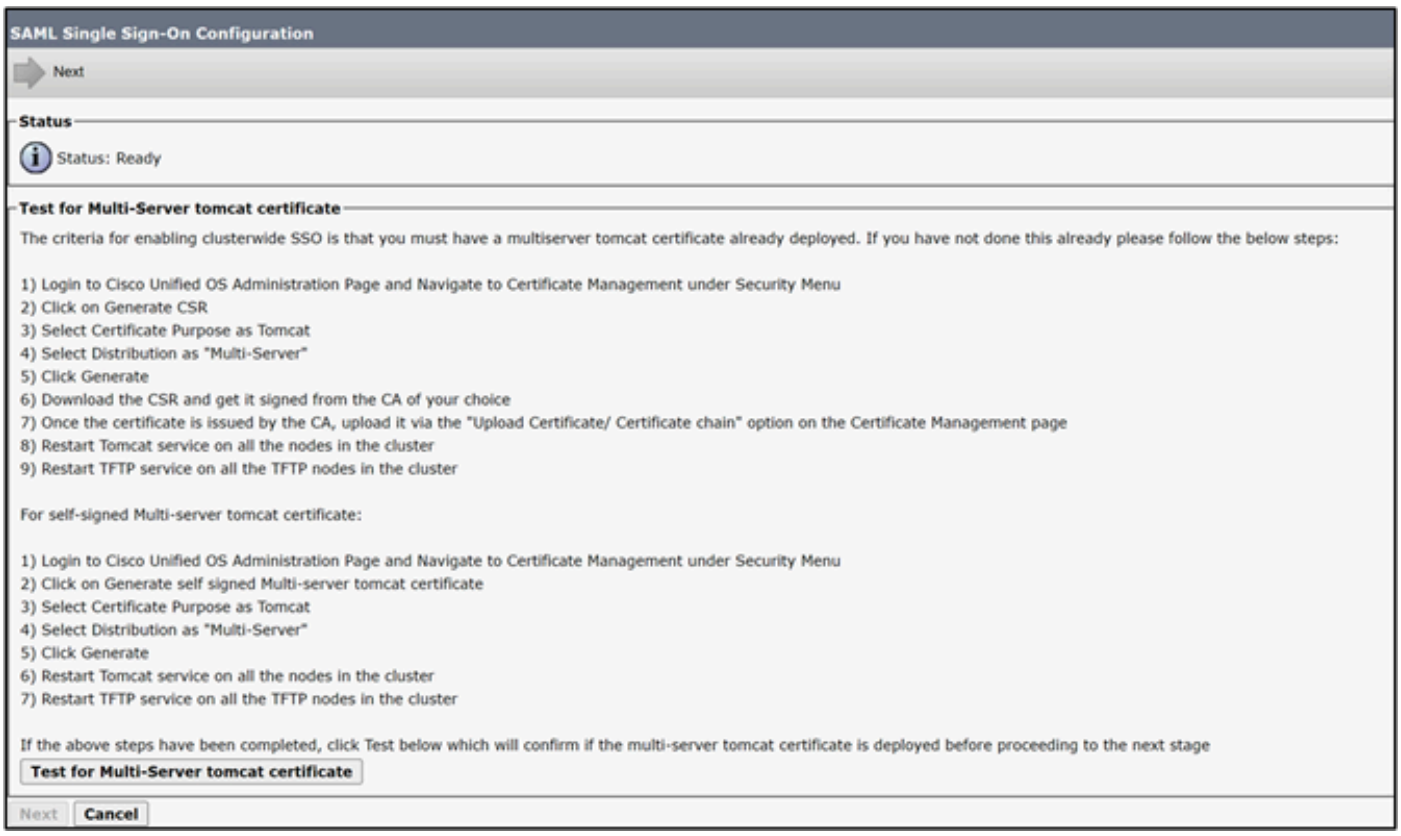
4.在CUCM集群中启用SSO

- 转至CM administration > System > Single Sign-On
- 在导出CUCM元数据时选择了相同的SSO选项，请选择Enable SAML SSO并选择continue。

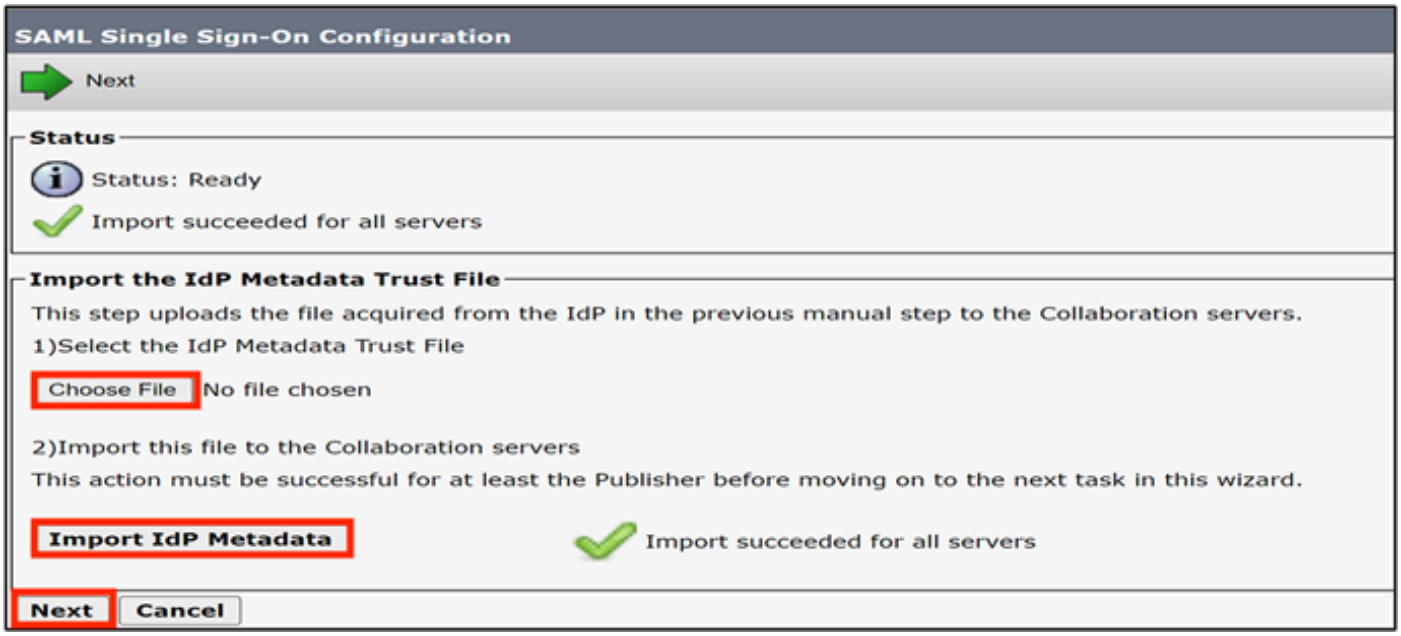




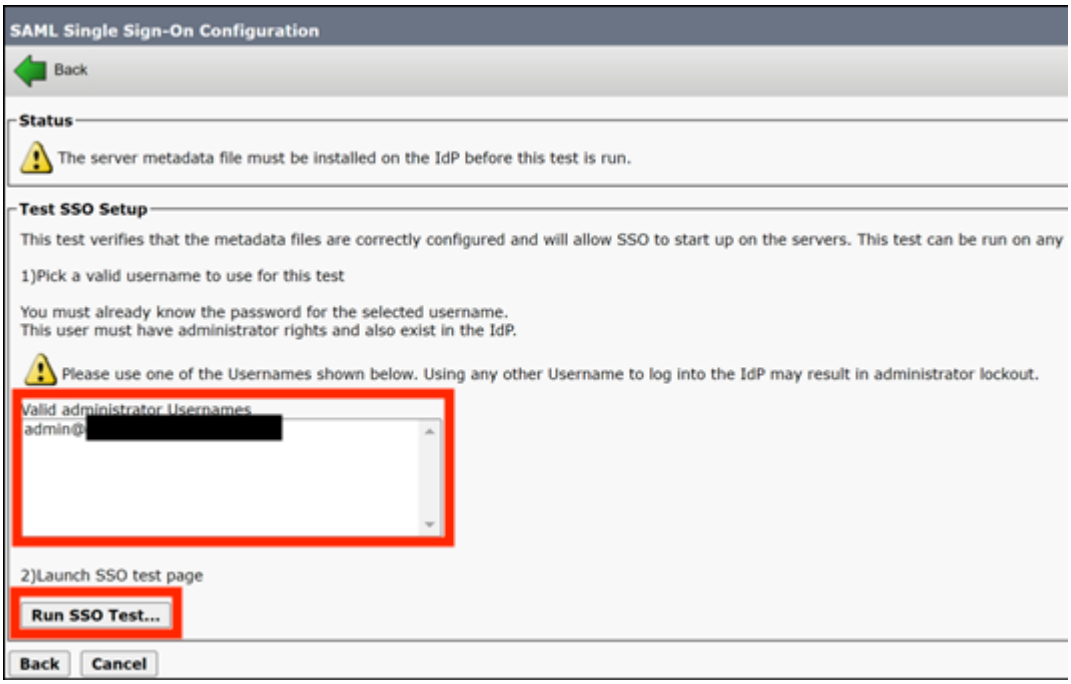
- 如果是在集群范围内，此步骤可用于检查所有节点中的多san证书，请选择Test for multi-server tomcat certificate。完成后，选择下一步。

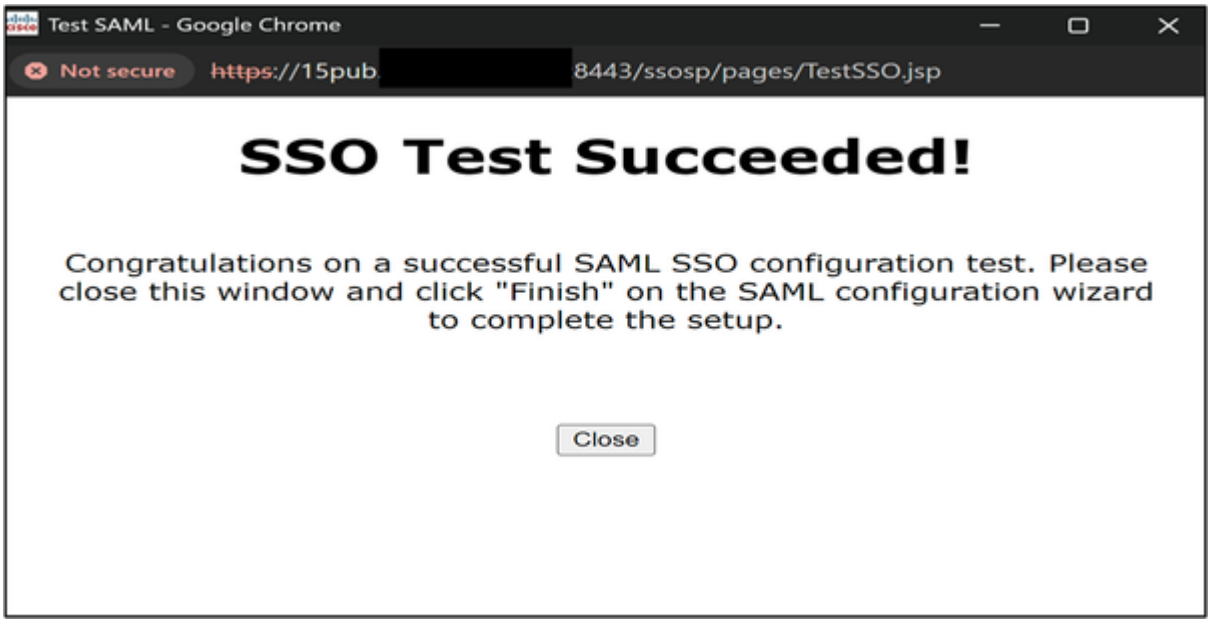


- 上传IdP元数据，选择导入IdP元数据，完成后，选择“下一步”



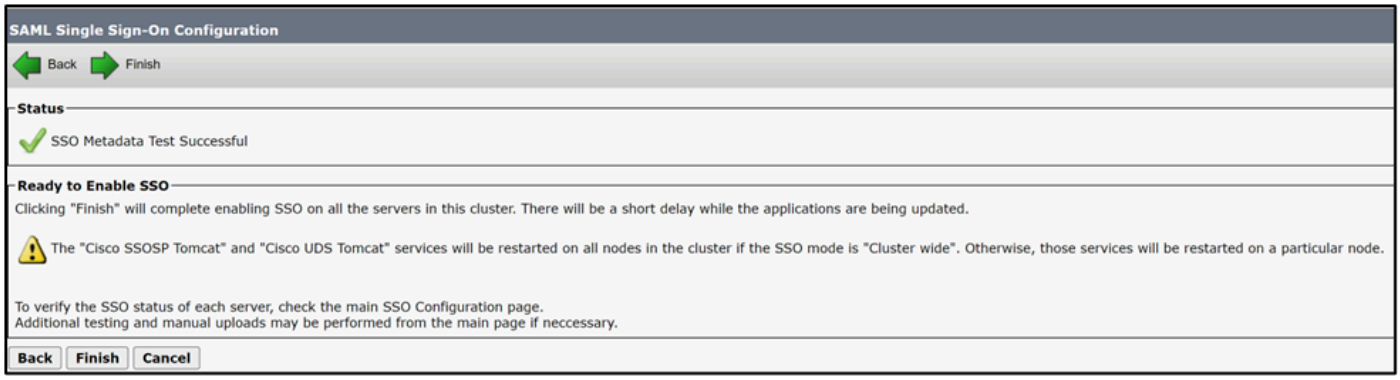
- 在Test SSO Setup中，选择分配了Standard CCM Super Users组的用户，然后选择Run SSO Test，直到成功为止。





4.启用SSO后重新启动所需的服务。

- 启用SSO会重新启动tomcat服务。



但是，TAC建议在SSO启用流程后在所有节点中手动重新启动Tomcat(utils service restart Cisco Tomcat)和UDS Tomcat(utils service restart CiscoUDSTomcat)服务。

情形 3：证书续订后的移动和远程访问注册问题

在混合模式部署中续订Call manager、Tomcat和Expressway C证书后，Webex应用无法通过移动

和远程访问(MRA)向CUCM注册。

确认

1. CUCM Call manager和Tomcat证书是CA签名证书。
2. CUCM和Expressway部署在混合模式(TLS)上运行。
3. inspect Expressway-C logs显示“SSL例程：ssl3_read_bytes:tlsv1 alert unknown ca”。
   <#root>

```
2026-01-29T14:01:16.974-05:00 exp-c traffic_server[2030]: UTCTime="2026-01-29 19:01:16,974" Module
HTTPMSG:
|GET /CSFmarcoalh.cnf.xml HTTP/1.1
 Host: expc.cisco.com:6972
 Accept: */*
 Cookie:<CONCEALED>
 User-Agent: WebEx/0.0.0.0
 TrackingID: fxxxxxxx-86f6-4030-8259-0b768c07723e
 Client-ip: xxx.xxx.xxx.xxx
 X-Forwarded-For: xxx.xxx.xxx.xxx, 127.0.0.1
 Via: https/1.1 vcs[0fxxxxxx-c853-xxxx-aa16-0a290bf56fc8] (ATS), http/1.1 vcs[5xxxxxxx-7feb-4xxx-9

 |

2026-01-29T14:01:16.974-05:00 exp-c traffic_server[2030]:[ET_NET 1]ERROR:SSL connection failed for

SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca
```

解决方案

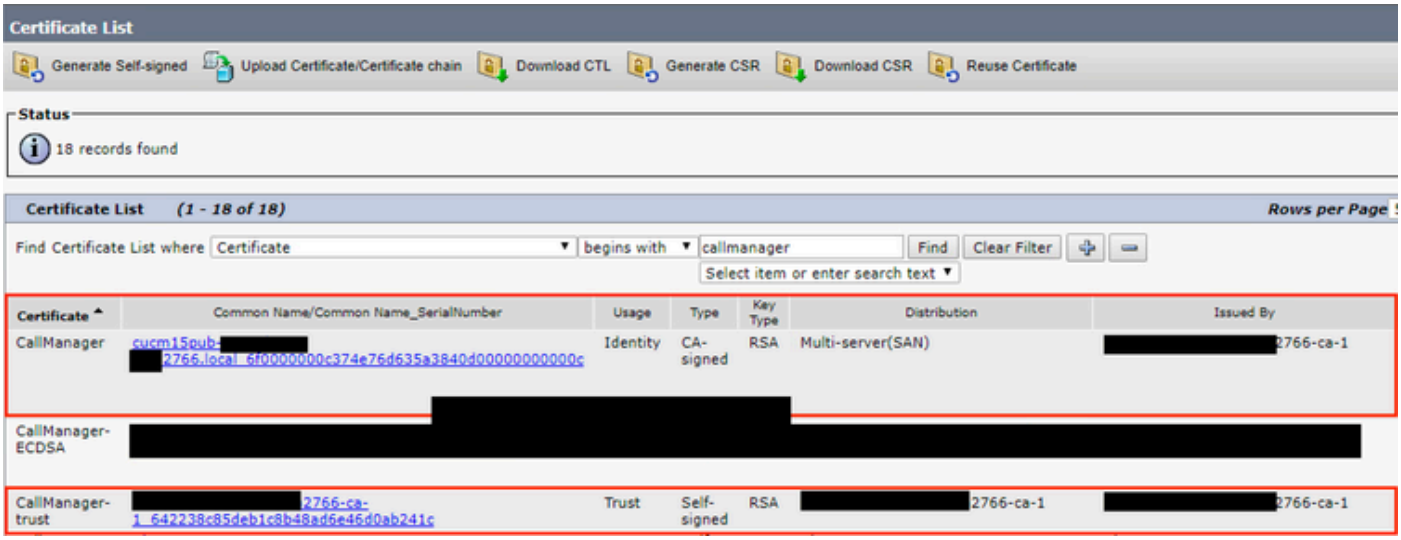
在CUCM和Expressway-C之间导出和导入证书，以确保信任关系。

⚠ 警告：TAC建议在数小时后执行此操作，因为此过程需要重新启动服务。业务影响是

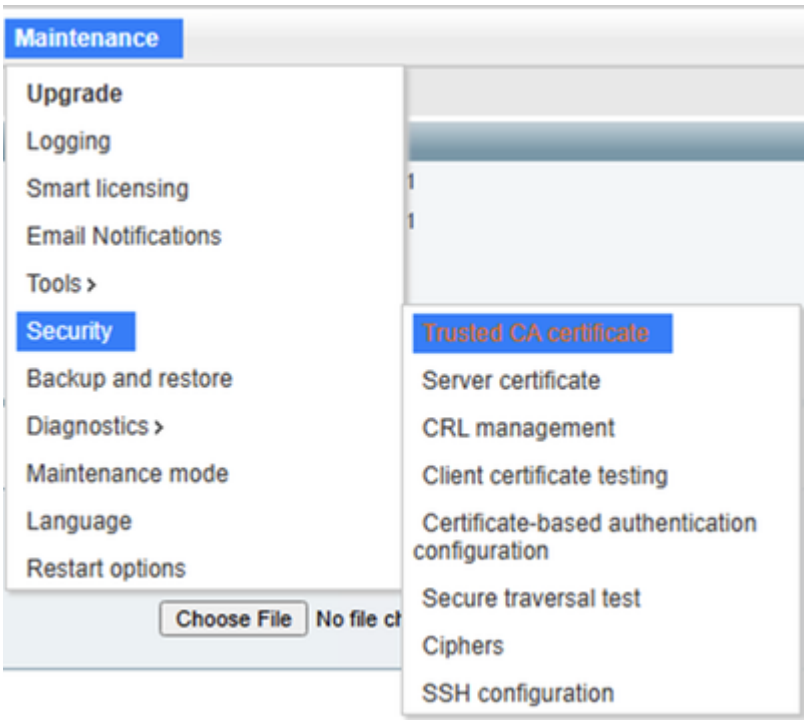
Medium Impact.

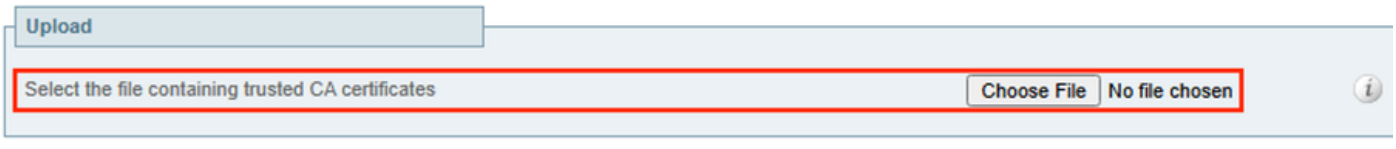
1. 使用CA签名证书在CUCM和Expressway之间完成信任关系的过程

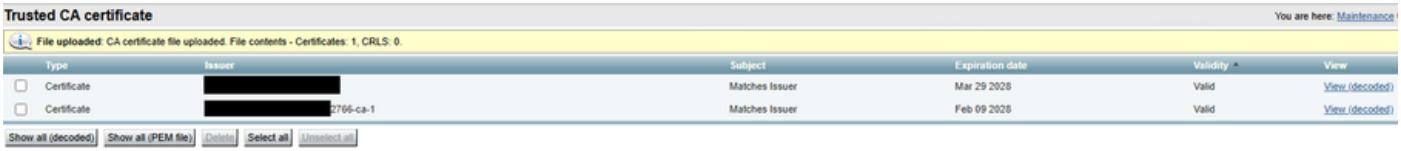
导航到OS administration > Security > Certificate management，然后下载签署Call Manager和Tomcat证书的根CA证书和中间（如果有）。



然后导航到Expressway-C >维护>安全>受信任CA证书，并上传Call Manager和Tomcat证书的CA证书。

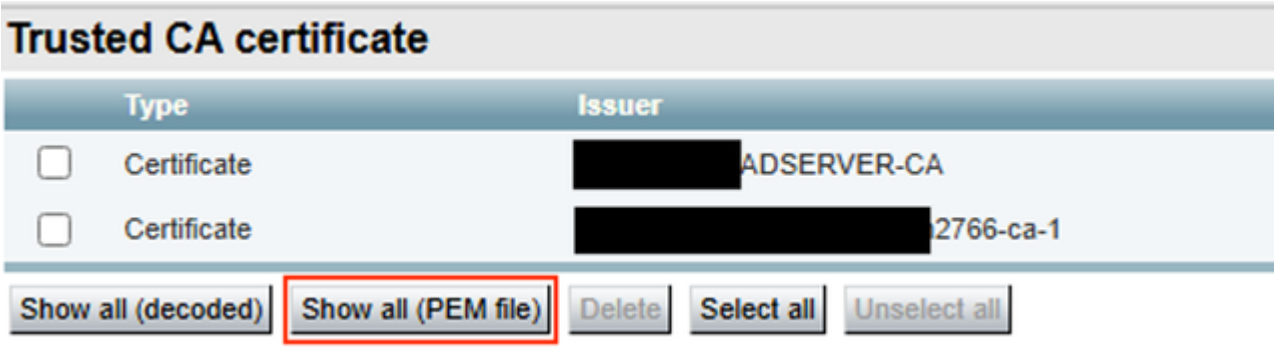




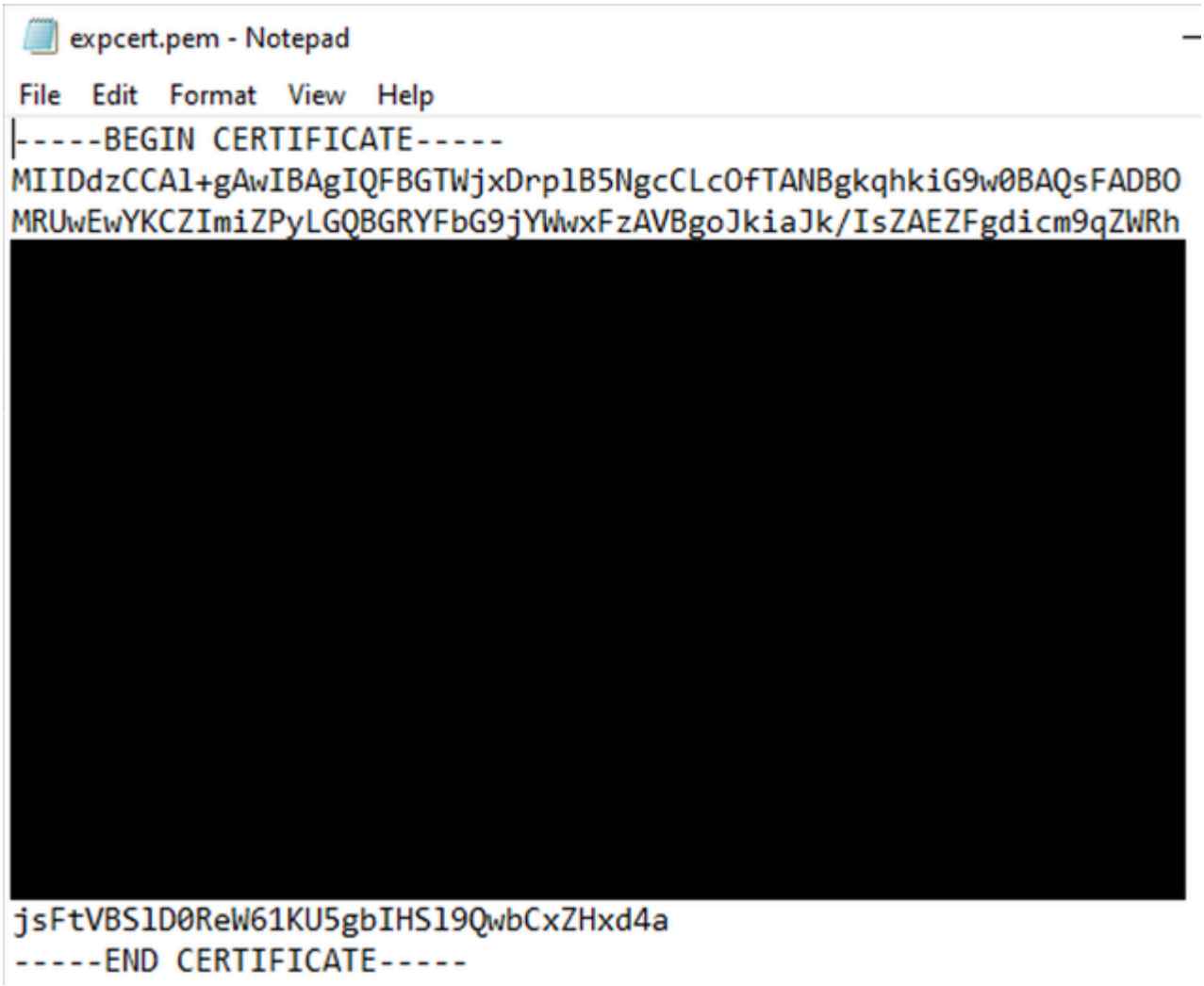


注意：在Call Manager和Tomcat证书为自签名的场景中，下载实际的Call Manager和Tomcat证书并将其上传到Expressway。

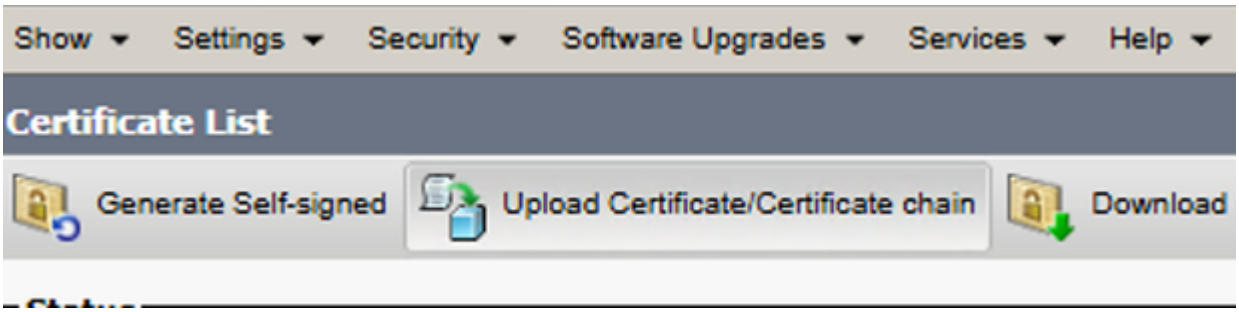
导航到Expressway-C >维护>安全>受信任CA证书>显示所有（PEM文件）

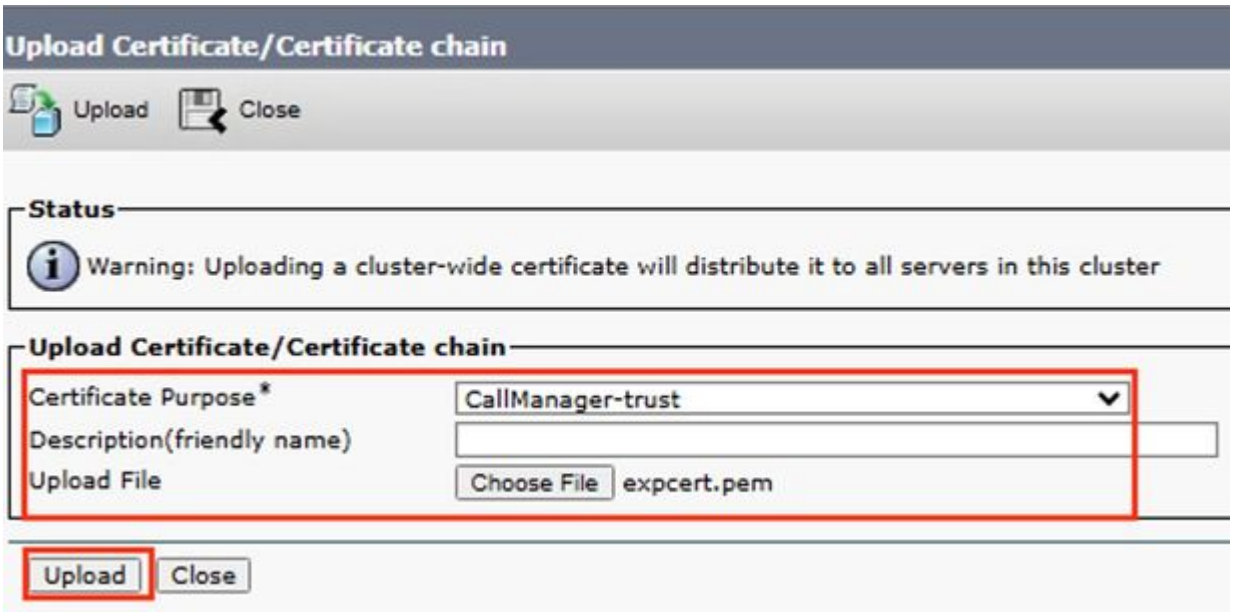


复制签署Expressway-C的CA证书的PEM值，并将其保存为txt文件。



导航到OS administration > Security > Certificate management，然后选择Upload Certificate/Certificate Chain，将Expressway-C CA证书上传为Tomcat-trust和Call Manager-trust





在CUCM群集中重新启动所需的服务：

- 导航到Cisco Unified Serviceability > Tools > Control Center - Feature Services，并在运行该服务的所有节点中重新启动Cisco CallManager服务。
- 导航到Cisco Unified Serviceability > Tools > Control Center - Feature Services，并在运行该服务的所有节点中重新启动Cisco TFTP服务。
- 使用utils service restart Cisco Tomcat命令通过CLI在集群中的所有节点中重新启动Tomcat。
- 使用utils service restart Cisco HAProxy命令通过CLI在集群中的所有节点中重新启动Cisco HAproxy服务。

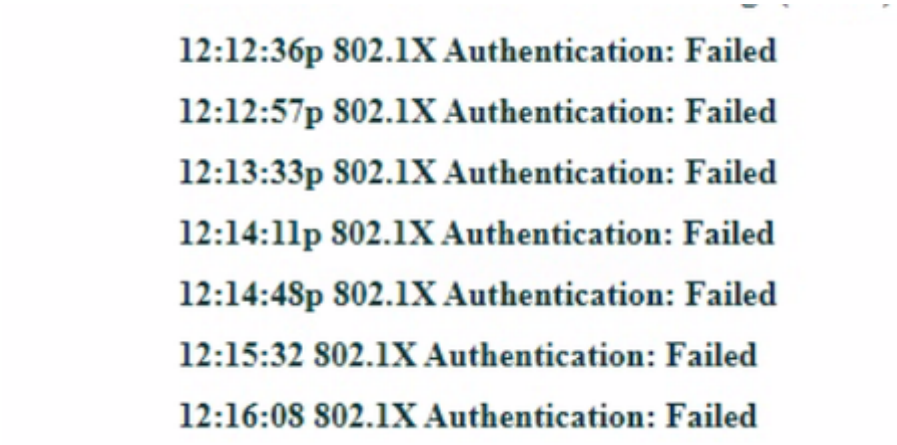
场景 4：证书颁发机构代理功能证书原因的更新

场景 4.1：802.1x身份验证失败

在CUCM发布服务器上重新生成证书授权代理功能(CAPF)证书后，电话不使用ASA进行身份验证。

确认

1. 电话状态消息显示“802.1x Authentication:失败"



2. 检查受影响服务器的电话日志并查找“SSL_ERROR_WANT_READ”

```
4592 NOT Feb 17 11:01:25.041733 (349-349) PAE: -Secure Connection Handshake in progress - status SSL_ER
4593 NOT Feb 17 11:01:25.041826 (349-349) PAE: -EV_REQUEST_REC, ST_AUTHENTICATING->ST_AUTHENTICATING
++ EAP-Failure
4594 NOT Feb 17 11:01:25.041898 (349-349) PAE: -send EAP-Resp/TLS - id 9
4595 NOT Feb 17 11:01:25.042032 (349-349) PAE: -authWhile timer set: 30 sec
4596 NOT Feb 17 11:01:27.061822 (349-349) PAE: -[0001-0] 08-cc-a7-1c-bb-ae vid=0xfff=4095 static=0 pri=
4597 NOT Feb 17 11:01:27.061950 (349-349) PAE: -port=0
4598 NOT Feb 17 11:01:27.062009 (349-349) PAE: -cprCdpGetPort address:  8:CC:A7:1C:BB:AE  Phyport=0 app
4599 NOT Feb 17 11:01:27.062068 (349-349) PAE: - >>>>>>>>>>>>>> port obtained = 0 for mac macAddress 08:
4600 NOT Feb 17 11:01:27.062134 (349-349) PAE: -rcvd EAP-Failure
4601 NOT Feb 17 11:01:27.062189 (349-349) PAE: -EV_FAILURE, ST_AUTHENTICATING->ST_HELD
4602 WRN Feb 17 11:01:27.062462 (349-349) PAE: -802.1X auth FAILED
4603 NOT Feb 17 11:01:27.062550 (349-349) PAE: -paeInfoToInetd: PAE info sent to NETSD
4604 NOT Feb 17 11:01:27.062717 (1786-1880) JAVA-Calling handleNetSDEvent
4605 WRN Feb 17 11:01:27.062953 (1786-1880) JAVA-Thread-11|cip.sec.Security:? - Security: Received a pr
4606 DEB Feb 17 11:01:27.063039 (1786-1880) JAVA-openQue(): que->/tmp/pae_msg_que, key->0x101019ab
4607 DEB Feb 17 11:01:27.063069 (1786-1880) JAVA-openQue(): que->/tmp/pae_rsp_que, key->0x10101c4c
4608 DEB Feb 17 11:01:27.063091 (1786-1880) JAVA-getpaeinfo: send pae info message paeCmd.mtype=1880, p
4609 DEB Feb 17 11:01:27.063121 (1786-1880) JAVA-getpaeinfo: recv pae info resp ret=-1, errno=No messag
4610 NOT Feb 17 11:01:27.063306 (349-349) PAE: -paeInfoToInetd: Netsd event NETSD_EV_PAE sent to NETSD
4611 NOT Feb 17 11:01:27.063370 (349-349) PAE: - PAE RE-AUTH, not sending SEC_DOWN Netsd event for CDP
4612 NOT Feb 17 11:01:27.063423 (349-349) PAE: -paeSetLastSupStatus: LastSupStatus 0
4613 NOT Feb 17 11:01:27.063475 (349-349) PAE: -heldWhile timer set: 60 sec
4614 NOT Feb 17 11:01:27.064074 (349-349) PAE: -paeNetsdRcvMsg(349): PAE event: status: FAIL : Resource
```

解决方案

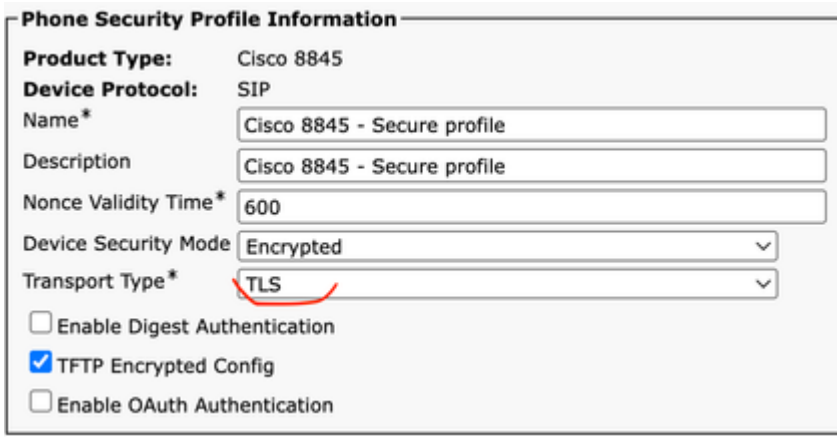
从CUCM发布服务器下载CAPF证书并上传到身份验证服务器，绕过802.1x以允许注册并在受影响的电话上安装LSC证书。

场景 4.2：电话未在TLS模式下使用安全配置文件的CUCM中注册。

在CUCM发布服务器上重新生成CAPF证书后，电话将显示“Phone is registering”。

确认

1. 受影响的电话包含启用TLS模式的安全配置文件。



2. 受影响的电话已安装LSC认证。
3. 确保CAPF证书是最新的。

4. 登录到CUCM发布程序，并使用显示旧CAPF证书序列号的show ctl命令。
5. 然后将电话安全配置文件更改为非安全。

解决方案

在CUCM上重新生成CTL文件，并重新启动所需的服务，以确保电话获得包含CAPF文件的新CTL文件。

⚠ 警告：TAC建议在数小时后执行此操作，因为此过程需要重新启动服务。业务影响是

Medium Impact.

确保成功续订CAPF的程序。

```
admin:utils ctl update CTLFile
This operation will update the CTLFile. Do you want to continue? (y/n): y

Updating CTL file
CTL file Updated
Please reset all Encrypted and Authenticated phones for the CTL file updates to take effect.
```

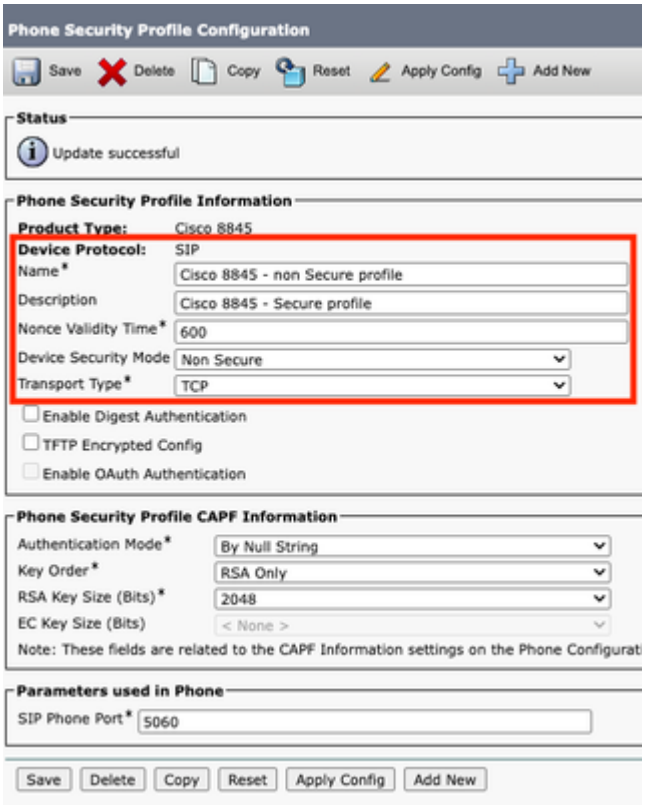
在CAPF重新生成后更新CTL文件。登录发布服务器的CLI，然后输入命令utils ctl update CTLFile。

1. 导航到Cisco Unified Serviceability > Tools > Control Center - Feature Services in CUCM publisher并重新启动CAPF服务。
2. 导航到Cisco Unified Serviceability > Tools > Control Center - Network Services，并在运行该服务的所有节点中重新启动Cisco Trust Verification Service。
3. 导航到Cisco Unified Serviceability > Tools > Control Center - Feature Services，并在运行该服务的所有节点中重新启动Cisco TFTP Service

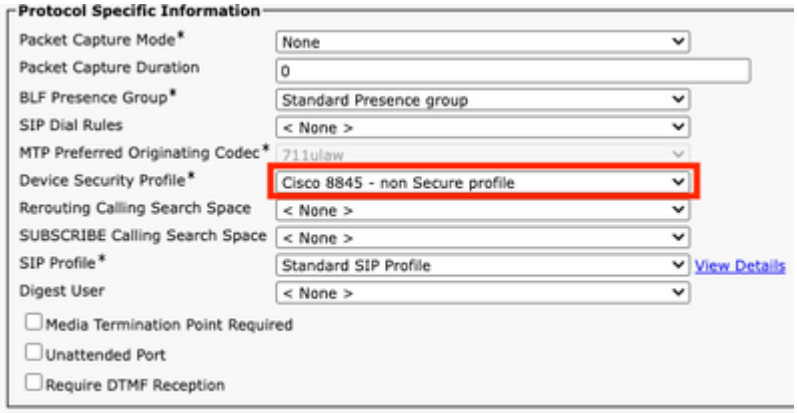
- 导航到CM administration > System > Security > Phone Security Profile。

- 复制分配给所需电话的当前电话安全配置文件。

- 将Name and Device Security Mode（名称和设备安全模式）更改为Non Secure，然后选择Save and Apply Config将此更改应用到所有所需的电话。

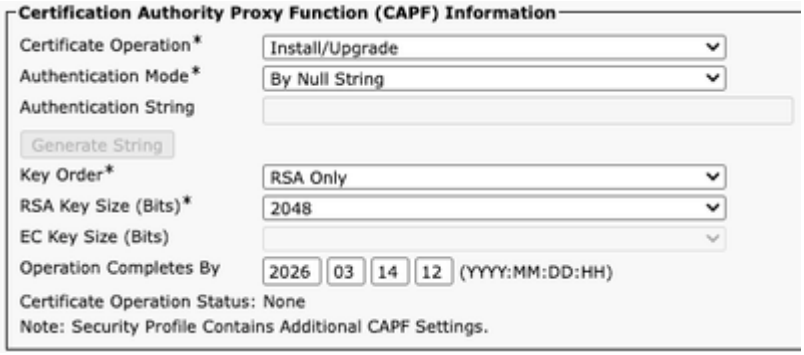


- 将创建的Device Security Profile应用到所需的电话配置，选择Save and Apply Config。



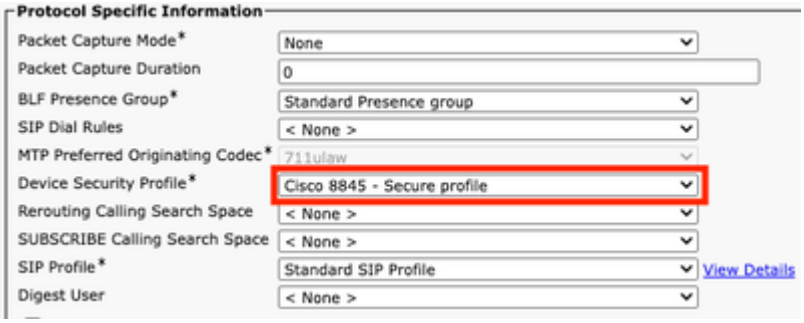
使用受影响电话的设备配置中的CAPF信息部分在所需电话中安装LSC证书。

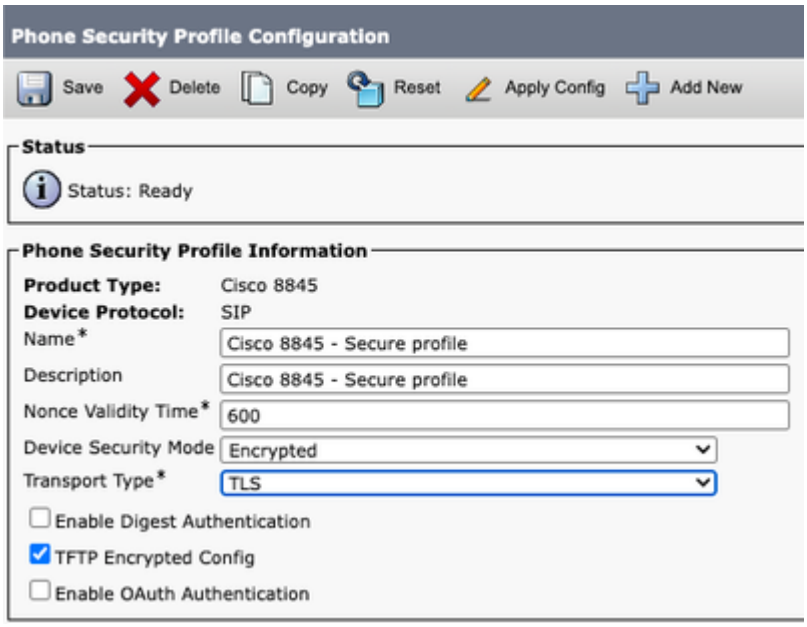
- 在CAPF信息中，选择Install/Upgrade in Certificate Operation。



- 选择保存并应用配置。
- 等待证书操作状态显示操作已完成。

在电话配置的协议特定信息部分中，选择已创建的启用了TLS的安全配置文件。





相关信息

- https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/214231-certificate-regeneration-process-for-cis.html
- https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/217138-regeneration-of-cucm-ca-signed-certifica.html
- https://www.cisco.com/c/en/us/support/docs/content-networking/certificates/213295-how-to-install-an-lsc-on-a-cisco-ip-phon.html
- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X15-2/mra/exwy_b_mra-deployment-guide-x152.html

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。