CUCM 11.0下一代加密 — 椭圆曲线加密

目录

简介

本文档介绍从Cisco Unified Communications Manager(CUCM)11.0及更高版本配置下一代加密(NGE)，以满足增强的安全性和性能要求。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco CallManager安全基础
- Cisco CallManager证书管理

使用的组件

本文档中的信息基于Cisco CUCM 11.0，其中只有CallManager(CallManager-ECDSA)支持椭圆曲线数字签名算法(ECDSA)证书。

> **注意**：CUCM 11.5及更高版本还支持tomcat-ECDSA证书。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

本文档还可与以下支持ECDSA证书的软件产品和版本一起使用：

- 思科Unified CM即时消息和在线状态11.5
- Cisco Unity Connection 11.5

背景信息

椭圆曲线密码(ECC)是一种基于有限域上椭圆曲线代数结构的公钥密码算法的一种方法。与非ECC加密相比，其主要优势之一是较小的密钥提供的安全级别相同。

通用标准(CC)可确保安全功能在正在评估的解决方案中正常运行。这是通过测试和满足大量文档要求来实现的。

它通过共同标准认可安排(CCRA)被全球26个国家接受和支持。

Cisco Unified Communications Manager版本11.0支持椭圆曲线数字签名算法(ECDSA)证书。

这些证书比基于RSA的证书更强，对于具有CC认证的产品是必需的。美国政府保密系统商业解决方案(CSfC)计划需要CC认证，因此，它包含在Cisco Unified Communications Manager 11.0版及更高版本中。

ECDSA证书与以下区域中的现有RSA证书一起可用：

- 证书管理
- 证书颁发机构代理功能(CAPF)
- 传输层安全(TLS)跟踪
- 安全会话发起协议(SIP)连接
- 计算机电话集成(CTI)管理器
- HTTP
- 熵

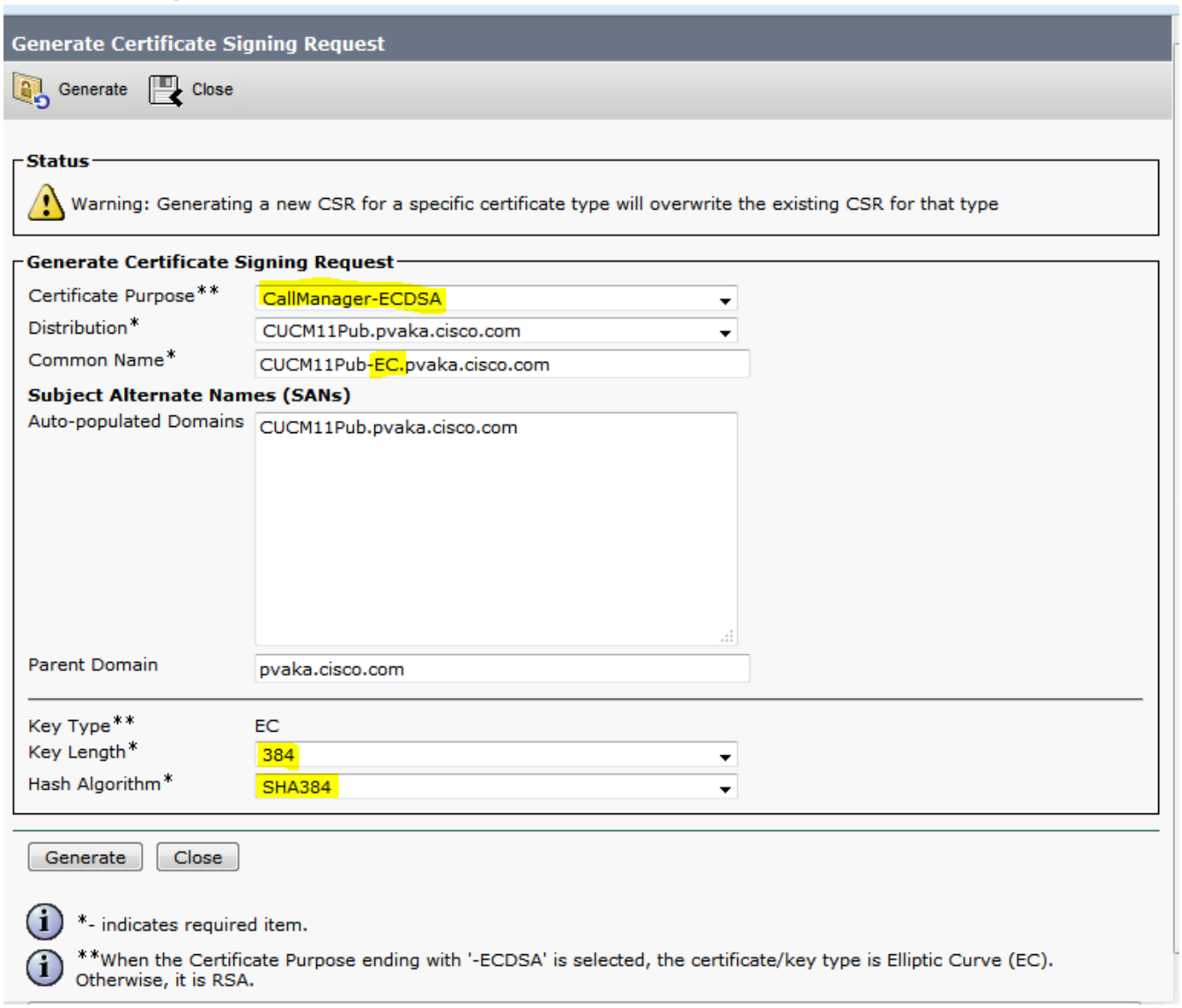
接下来的部分将提供有关这七个领域的详细信息。

证书管理

使用椭圆曲线加密生成证书

支持CUCM 11.0及更高版本的ECC，以生成带椭圆曲线(EC)加密的CallManager证书：

- 新选项**CallManager-ECDSA**可用，如图所示。
- 它要求公共名称的主机部分以EC结**束**。这可防止与CallManager证书具有相同**的公**用名。
- 对于多服务器SAN证书，此证书必须以 — **EC-ms结束**。



- 自签名证书请求和CSR请求都根据EC密钥大小限制散列算法选择。
- 对于EC 256密钥大小，哈希算法可以是SHA256、SHA384或SHA512。对于EC 384密钥大小，哈希算法可以是SHA384或SHA512。对于EC 521密钥大小唯一的选项是SHA512。
- 默认密钥大小为384，默认散列算法为SHA384，可以更改。可用选项取决于所选密钥大小。

CLI 配置

已为CLI命令添**加名为**CallManager-ECDSA的新证书单元

- set cert regen [unit] — 重新生成自签名证书

```
admin:set cert regen ?
Syntax:
set cert regen [name]
name mandatory unit name

admin:set cert regen CallManager-ECDSA

WARNING: This operation will overwrite any CA signed certificate previously imported for  CallManager-
ECDSA
Proceed with regeneration (yes|no)?
```

- set cert import own|trust [unit] — 导入CA签名证书

```
admin:set cert import trust CallManager-ECDSA
Paste the Certificate and Hit Enter
```

- set csr gen [unit] — 为指定设备生成证书签名请求

```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- set bulk export|consolidate|import tftp — 当tftp是设备名称时，CallManager-ECDSA证书将自动包含在批量操作中的CallManager RSA证书中。

CTL和ITL文件

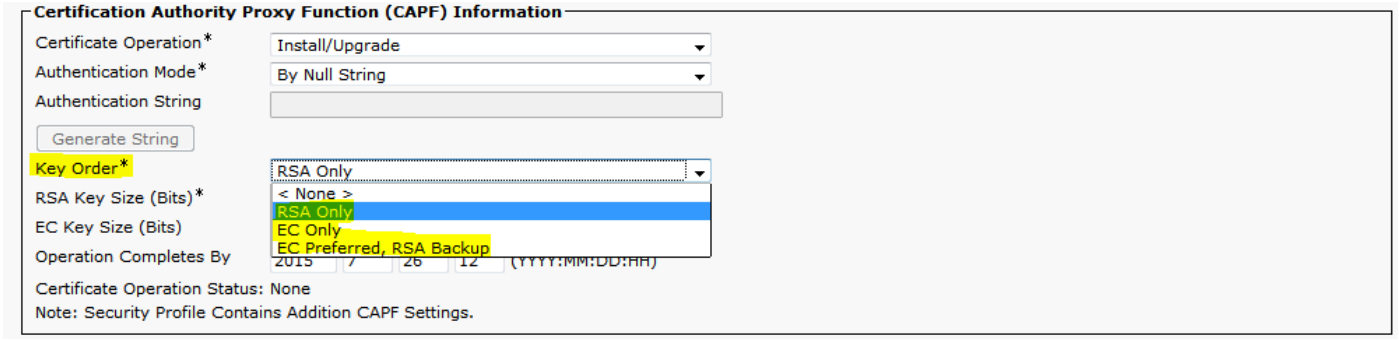
- 证书信任列表(CTL)和标识信任列表(ITL)文件都有CallManager-ECDSA。
- CallManager-ECDSA证书在ITL和CTL文件中均具有CCM+TFTP的功能。
- 您可以使用 **show ctl** 或 **show itl** 命令查看此信息，如下图所示：

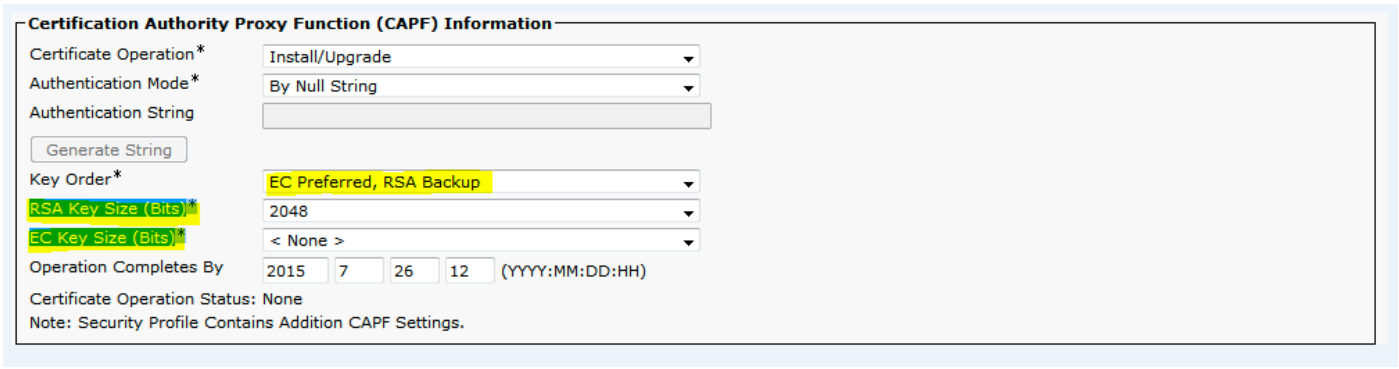
```
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1656
2       DNSNAME         2
3       SUBJECTNAME     65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME      65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
6       SERIALNUMBER    16      61:E4:7E:DA:01:65:E4:68:22:9E:2E:CC:EB:35:18:DD
7       PUBLICKEY       270
8       SIGNATURE       256
9       CERTIFICATE     951     3B D9 E1 B0 68 56 5F ED 73 FF 75 B7 36 3B D1 29 9E 93 36 FD (SHA1 Hash HEX)

        ITL Record #:5
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1071
2       DNSNAME         26      CUCM11Pub.pvaka.cisco.com
3       SUBJECTNAME     68      CN=CUCM11Pub-EC.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME      68      CN=CUCM11Pub-EC.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
6       SERIALNUMBER    16      60:28:0E:23:2C:DC:72:7D:16:B2:16:B1:40:90:20:7E
7       PUBLICKEY       97
8       SIGNATURE       104
9       CERTIFICATE     661     21 C4 B8 E9 71 B0 4C 90 C2 F9 93 30 E0 53 3D 1D DE 86 32 07 (SHA1 Hash HEX)

The ITL file was verified successfully.
```

- 可以使用utils ctl update命令生成CTL文件。

证书颁发机构代理功能

- CUCM 11中的证书颁发机构代理功能(CAPF)版本3.0支持EC密钥大小和RSA。
- 除现有CAPF字段外，还提供其他CAPF选项包括密钥顺序和EC密钥大小（位）。
- 现有的密钥大小（位）选项已更改为RSA密钥大小（位）。
- “密钥订单”提供对“仅RSA”、“仅EC”和“EC首选”、“RSA备份”选项的支持。
- EC密钥大小支持256、384和521位的密钥大小。
- RSA密钥大小支持512、1024和2048位。
- 选择“仅RSA密钥顺序”时，只能选择“RSA密钥大小”。仅选择EC时，只能选择EC密钥大小。选择EC首选，RSA备份时，可以同时选择RSA和EC密钥大小。

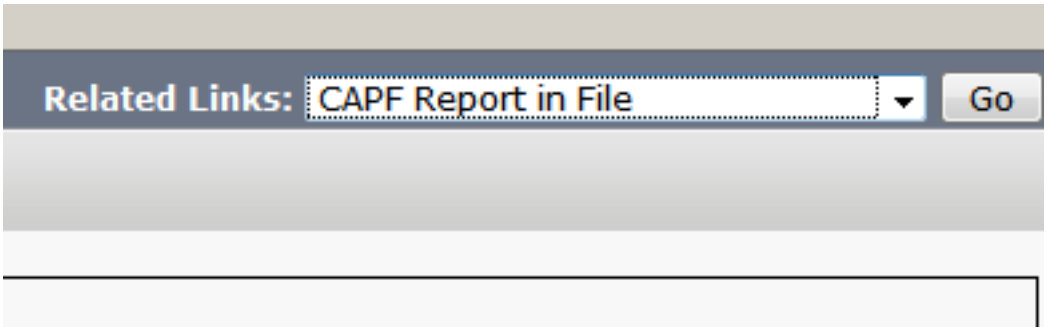




注意：目前没有思科终端支持CAPF版本3，因此请勿选择EC Only选项。但是，以后要支持ECDSA本地有效证书(LSC)的管理员可以使用EC首选RSA备份选项配置其设备。当终端开始支持ECDSA LSC的CAPF第3版时，管理员需要重新安装其LSC。

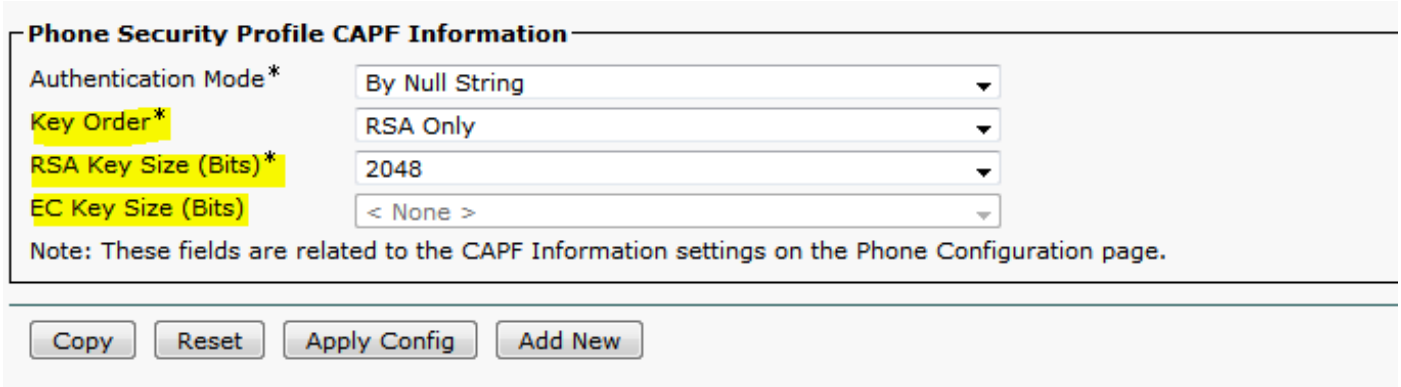
电话、电话安全配置文件、最终用户和应用用户页面的其他CAPF选项如下所示：

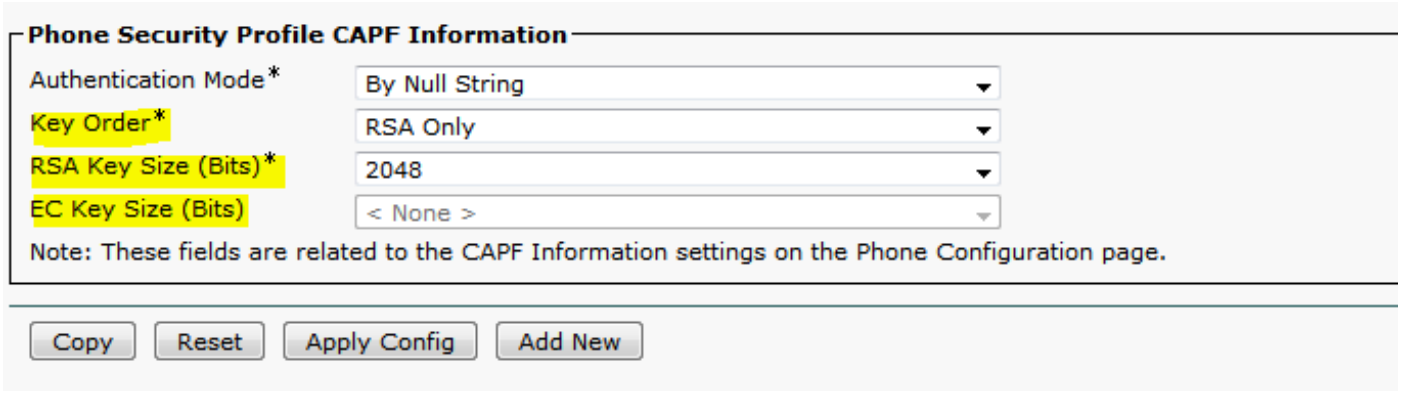
设备>电话>相关链路



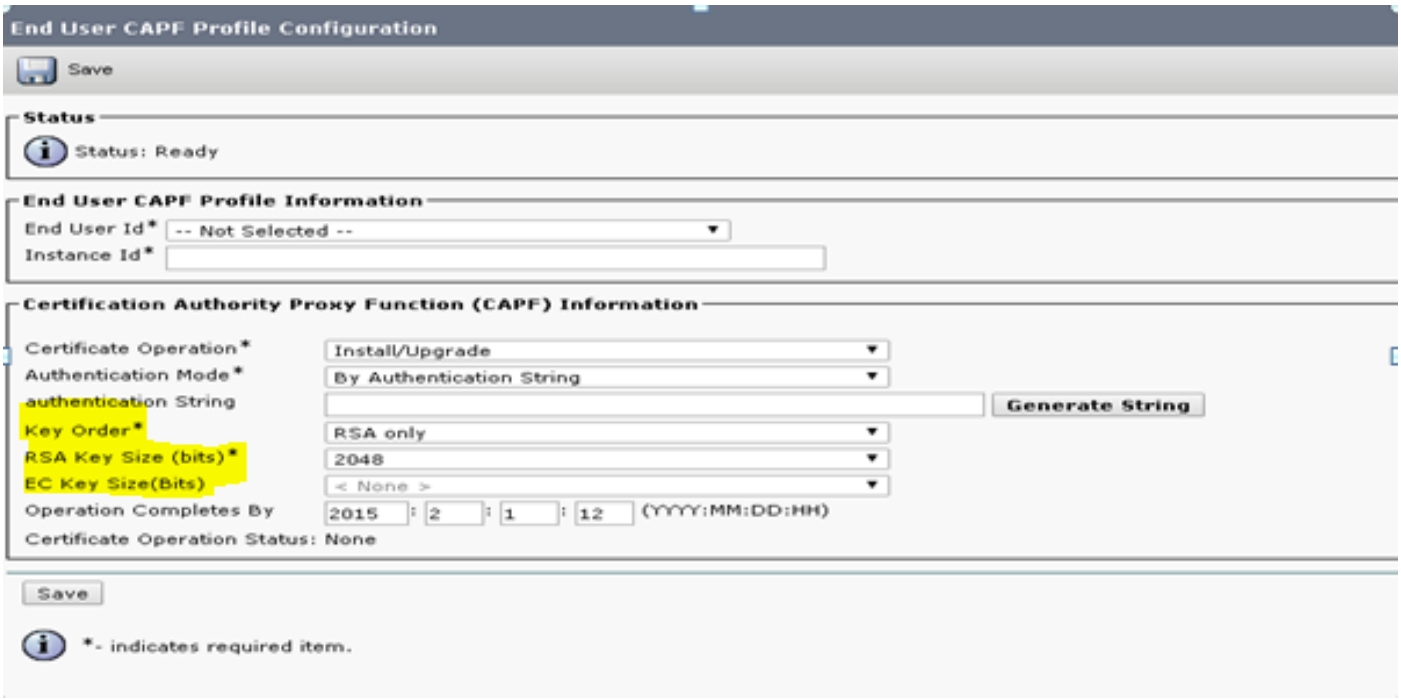
导航至System > Security > Phone security profile

用户管理>用户设置>应用用户CAPF配置文件



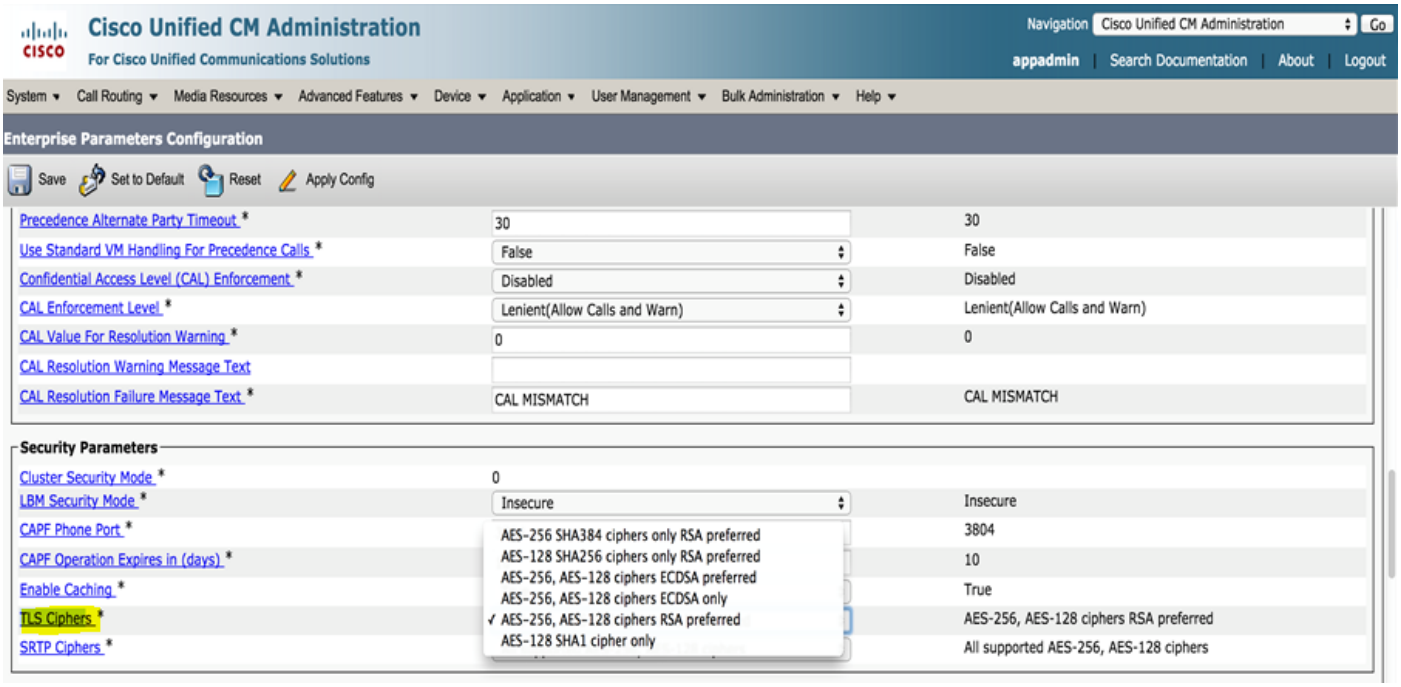


导航至User Management > User Settings > End User CAPF Profile。



TLS密码企业参数

- 企业参数TLS密码已更新为支持ECDSA密码。
- 企业参数TLS密码现在为SIP线路、SIP中继和安全CTI管理器设置TLS密码。



SIP ECDSA支持

- Cisco Unified Communications Manager版本11.0包括对SIP线路和SIP中继接口的ECDSA支持。
- Cisco Unified Communications Manager与终端电话或视频设备之间的连接是SIP线路连接，而两个Cisco Unified Communications Manager之间的连接是SIP中继连接。
- 所有SIP连接都支持ECDSA密码并使用ECDSA证书。

安全SIP接口已更新为支持以下两个密码：

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

以下是SIP进行TLS连接的场景：

- 当SIP充当TLS服务器时 当Cisco Unified Communications Manager的SIP中继接口充当传入安全SIP连接的TLS服务器时，SIP中继接口将确定CallManager-ECDSA证书是否存在于磁盘上。如果证书存在于磁盘上，则SIP中继接口使用CallManager-ECDSA证书(如果所选密码套件为TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256或TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- 当SIP充当TLS客户端时 当SIP中继接口充当TLS客户端时，SIP中继接口根据CUCM企业参数TLS密码中的TLS密码字段（还包括ECDSA密码选项）向服务器发送请求的密**码套件列表**。此配置按优先顺序确定TLS客户端密码套件列表和支持的密码套件。

注意：
— 使用ECDSA密码连接CUCM的设备必须在其身份信任列表(ITL)文件中具有CallManager-ECDSA证书。
- SIP中继接口支持RSA TLS密码套件，用于来自不支持ECDSA密码套件的客户端的连接，或当TLS连接与不支持ECDSA的早期版本CUCM建立时。

安全CTI管理器ECDSA支持

安全CTI管理器接口已更新以支持以下四个密码：

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

安全CTI管理器接口加载CallManager和CallManager-ECDSA证书。这允许安全CTI管理器接口支持新密码和现有RSA密码。

与SIP接口类似，Cisco Unified Communications Manager中的Enterprise Parameter TLS Ciphers选项用于配置CTI Manager安全接口支持的TLS密码。

配置下载的HTTPS支持

- 为了安全配置下载（例如Jabber客户端），除了早期版本中使用的HTTP和TFTP接口外，Cisco Unified Communications Manager版本11.0还增强了支持HTTPS的功能。
- 如果需要，客户端和服务器都使用相互身份验证。但是，注册了ECDSA LSC和加密TFTP配置的客户端必须提供其LSC。
- HTTPS接口使用CallManager和CallManager-ECDSA证书作为服务器证书。

注意：
— 更新CallManager、CallManager ECDSA或Tomcat证书时，必须停用并重新激活TFTP服务。
— 端口6971用于CallManager和CallManager-ECDSA证书（由电话使用）的身份验证。
— 端口6972用于Jabber使用的Tomcat证书的身份验证。

熵

熵是数据随机性的度量，有助于确定通用标准要求的最小阈值。要获得强加密，需要强大的熵源。如果ECDSA等强加密算法使用弱熵源，则加密很容易被破解。

在Cisco Unified Communications Manager版本11.0中，Cisco Unified Communications Manager的熵源得到了改进。

熵监控守护程序是无需配置的内置功能。但是，您可以通过Cisco Unified Communications Manager CLI将其关闭。

使用以下CLI命令以控制熵监控守护程序服务：

CLI Command	Description
utils service start Entropy Monitoring Daemon	Starts the Entropy Monitoring Daemon service.
utils service stop Entropy Monitoring Daemon	Stops the Entropy Monitoring Daemon service.
utils service active Entropy Monitoring Daemon	Activates the Entropy Monitoring Daemon service, which further loads the kernel module.
utils service deactive Entropy Monitoring Daemon	Deactivates the Entropy Monitoring Daemon service, which further unloads the kernel module.

相关信息

- 思科统一通信管理器安全指南，版本11.5(1)
- 技术支持和文档 - Cisco Systems