# CUCM 11.0下一代加密-椭圆曲线密码学

## Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[背景信息](#)
[证书管理](#)
[生成与EC加密的证书](#)
[CLI 配置](#)
[CTL和ITL文件](#)
[认证机关代理功能(CAPF)](#)
[TLS密码企业参数](#)
[SIP ECDSA技术支持](#)
[安全的CTI Manager ECDSA技术支持](#)
[配置下载的HTTPS技术支持](#)
[熵](#)
[Related Information](#)

## Introduction

本文描述简介，下一代加密(NGE)的配置从Cisco Unified通信管理器(CUCM) 11.0及以后，符合高级安全和性能要求

## Prerequisites

### Requirements

Cisco 建议您了解以下主题：

- Cisco Call Manager安全基础
- Cisco Call Manager证书管理

### Components Used

本文的信息根据Cisco CUCM 11.0，其中EDCSA证书为呼叫管理器(呼叫管理器EDCSA)只支持

**Note**:CUCM 11.5向前支持TomcatEDCSA证书

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

### 相关产品

本文可能也与支持EDCSA证书的这些软件产品和版本一起使用：

- Cisco Unified CM IM和存在11.5
- Cisco Unity Connection 11.5

## 背景信息

椭圆曲线密码学(ECC)是方法对根据椭圆曲线代数结构的公共密钥密码学在有限的字段的。其中一个与非ECC密码学比较的主要优点是键提供的同一个安全级别更加小型。

普通的标准提供保证安全功能在被评估的解决方案内正确地运行。这通过测试和符合广泛的文档要求达到。

接受和支持由26个国家(地区)全世界通过普通的标准确认安排(CCRA)

Cisco Unified Communications Manager Release 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的证书严格和对于有普通的标准的产品是必需的(CC)证明。被分类的系统(CSfC)程序的美国政府商业解决方案要求CC证明然后在Cisco Unified Communications Manager Release 11.0向前包括。

ECDSA证书与现有的RSA证书一起是可用的在这些区域：

- 证书管理
- 认证机关代理功能(CAPF)
- 传输层安全(TLS)跟踪
- 巩固SIP连接
- 计算机电话集成(CTI)管理器
- HTTP和
- 熵

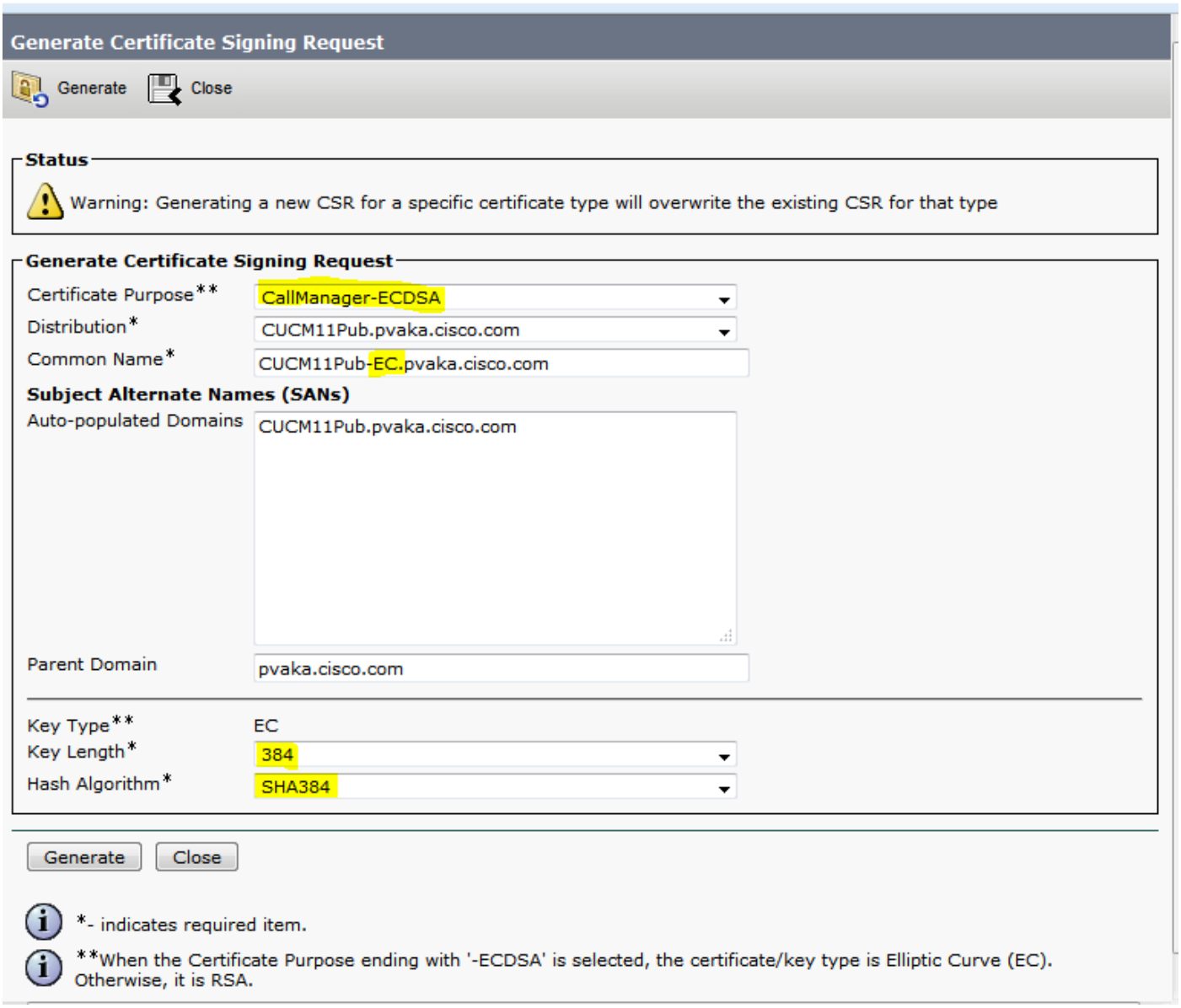
以下部分在上述7个区域中的每一个提供详细信息。

## 证书管理

### 生成与EC加密的证书

ECC的技术支持从向前生成与EC加密的呼叫管理器认证的CUCM 11.0

- 新选项**呼叫管理器ECDSA**可用如镜像所显示。
- 要求普通的名字的主机部分结束**EC**，防止有普通的名字和**呼叫管理器**认证一样。
- 在多服务器SAN认证的情况下，这必须结束EC **MS**。




- 两个自签证书请求和CSR请求根据EC密钥大小限制Hash算法选择。
- 对于EC 256密钥大小Hash算法可以是SHA256、SHA384或者SHA512。对于EC 384密钥大小Hash算法可以是SHA384或SHA512。对于EC 521密钥大小唯一选择是SHA512。
- DEFAULT键大小是384，并且默认Hash算法是SHA384，能更改丢弃下来。可用的选项根据选择的密钥大小。

## CLI 配置

名为**呼叫管理器ECDSA的**新证书单元为cli命令被添加了

- 设置cert regen [unit] –重新生成自签证书

```
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)?
```

- 设置cert导入拥有|信任[unit] –导入CA签名的证书

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

- 设置csr gen [unit] –生成指定的单元的认证签署的request(CSR)

```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- 设置大批导出|统一|导入tftp –当tftp是单元名字时，呼叫管理器ECDSA证书获得自动包括对呼叫管理器RSA证书散装操作。

## CTL和ITL文件

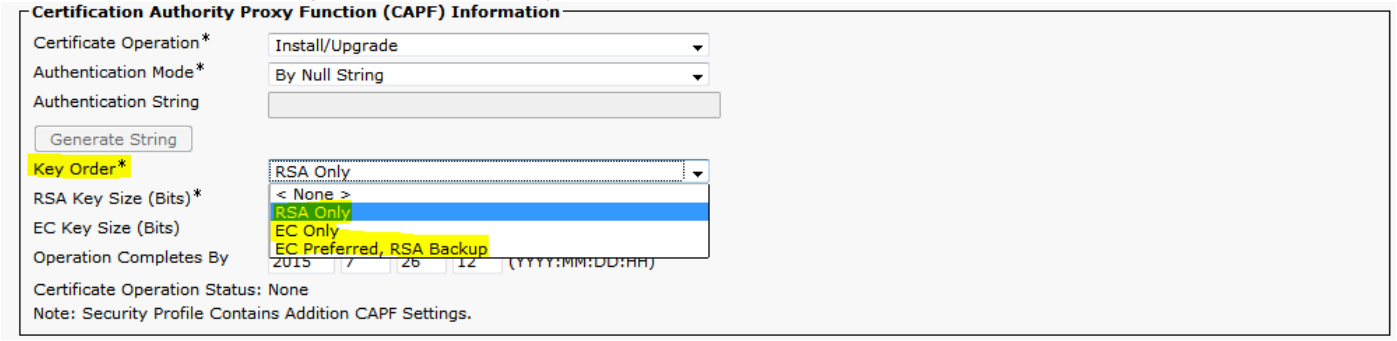
- CTL和ITL文件有**呼叫管理器ECDSA**存在。
- 呼叫管理器ECDSA认证有CCM+TFTP的功能在ITL和CTL文件。
- 如镜像所显示，您能使用**显示ctl**或**显示itl**命令查看此信息：

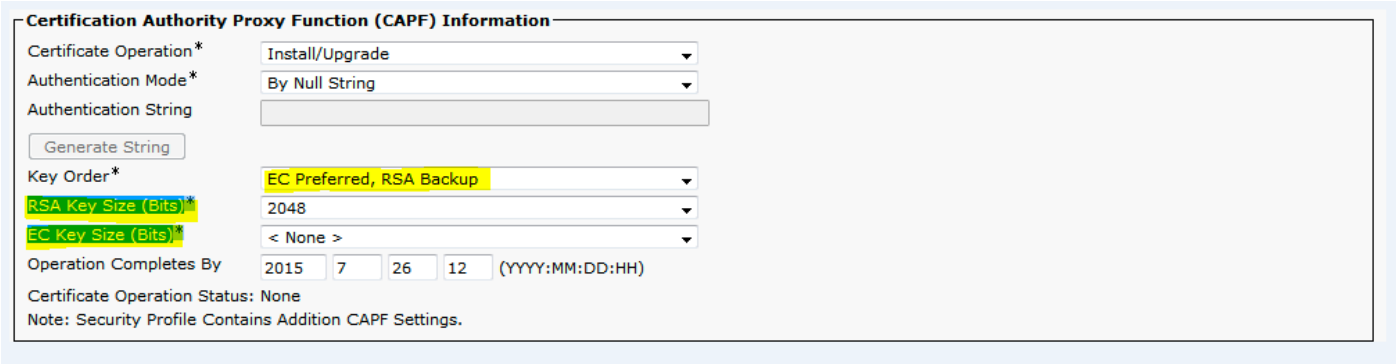
```
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1656
2       DNSNAME         2
3       SUBJECTNAME     65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME      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.
```

- 您能使用**utils ctl更新**生成CTL文件。

# 认证机关代理功能(CAPF)

- 在CUCM 11提供技术支持的CAPF版本3.0的与RSA一起的EC密钥大小。
- 另外的CAPF选项提供除现有的CAPF字段之外是关键命令和EC密钥大小(位)。
- 现有的密钥大小(位)选项更改了到RSA密钥大小(位)。
- 仅RSA的仅关键命令提供技术支持，首选的EC和EC， RSA备份选项。
- 256， 384和521位的密钥大小的EC密钥大小提供技术支持。
- 512， 1024和2048位的RSA密钥大小提供技术支持
- 当关键仅RSA命令选择，只有RSA密钥大小可以选择。当仅EC选择，只有EC密钥大小可以选择。当首选的EC， RSA备份选择， RSA和EC时密钥大小可以选择。

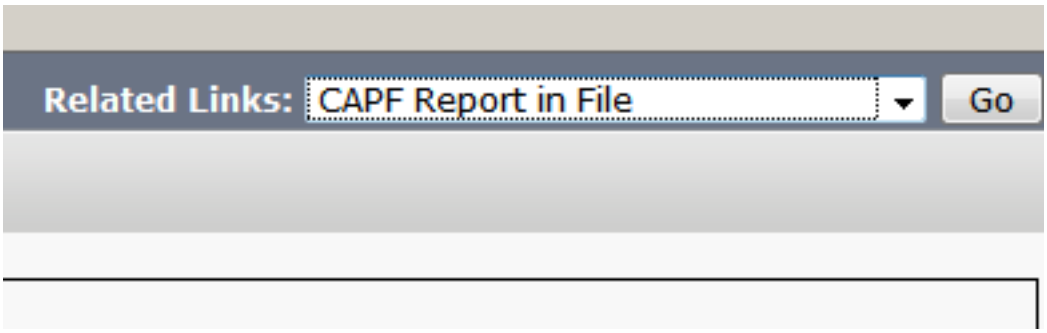



**Note**:目前， Cisco终端支持CAPF版本3不如此避免选择EC唯一选择。然而，要后支持ECDSA LSCs的管理员能用EC首选RSA备份选项配置他们的设备。当终端开始支持ECDSA LSCs的时CAPF版本3，管理员需要重新安装他们的LSC。

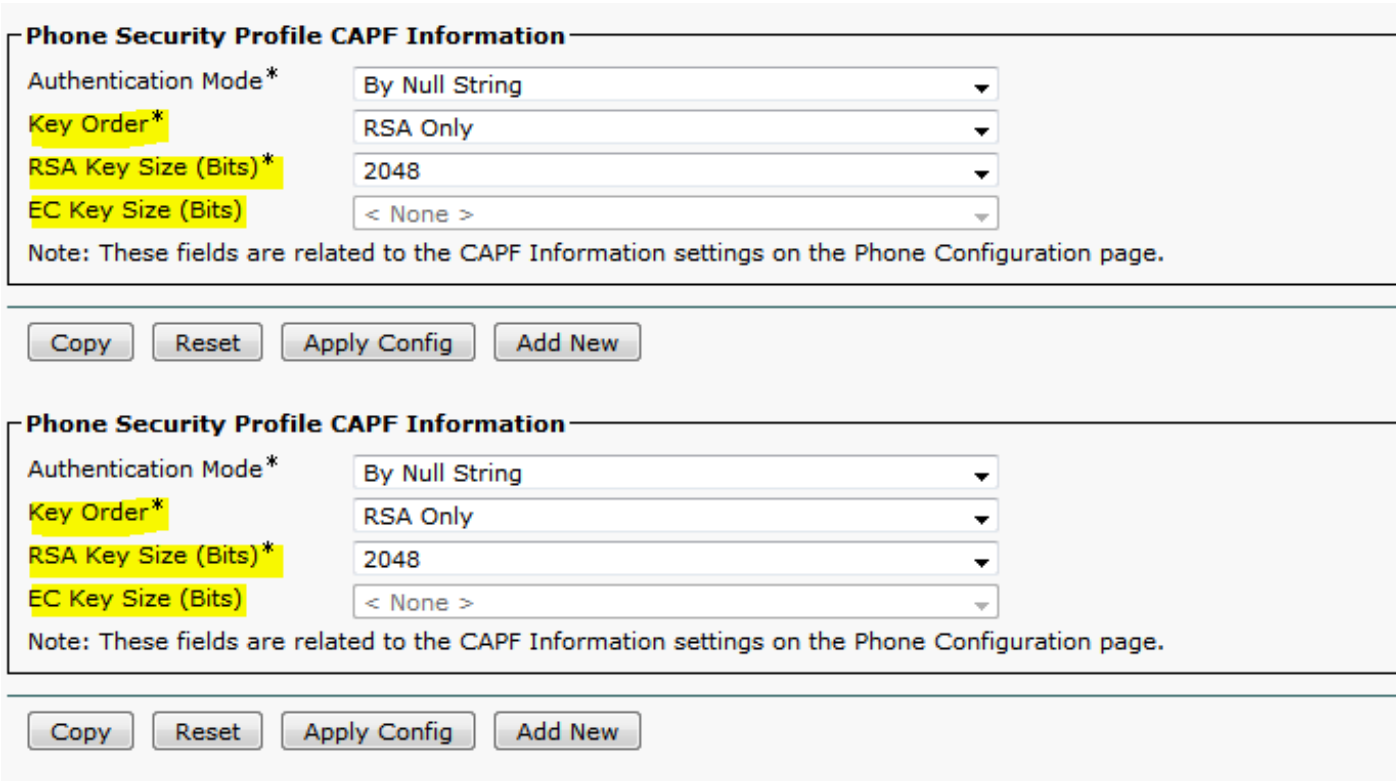
电话、电话安全配置文件、终端用户和应用程序用户页的另外的CAPF选项

Device > Phone >相关链接

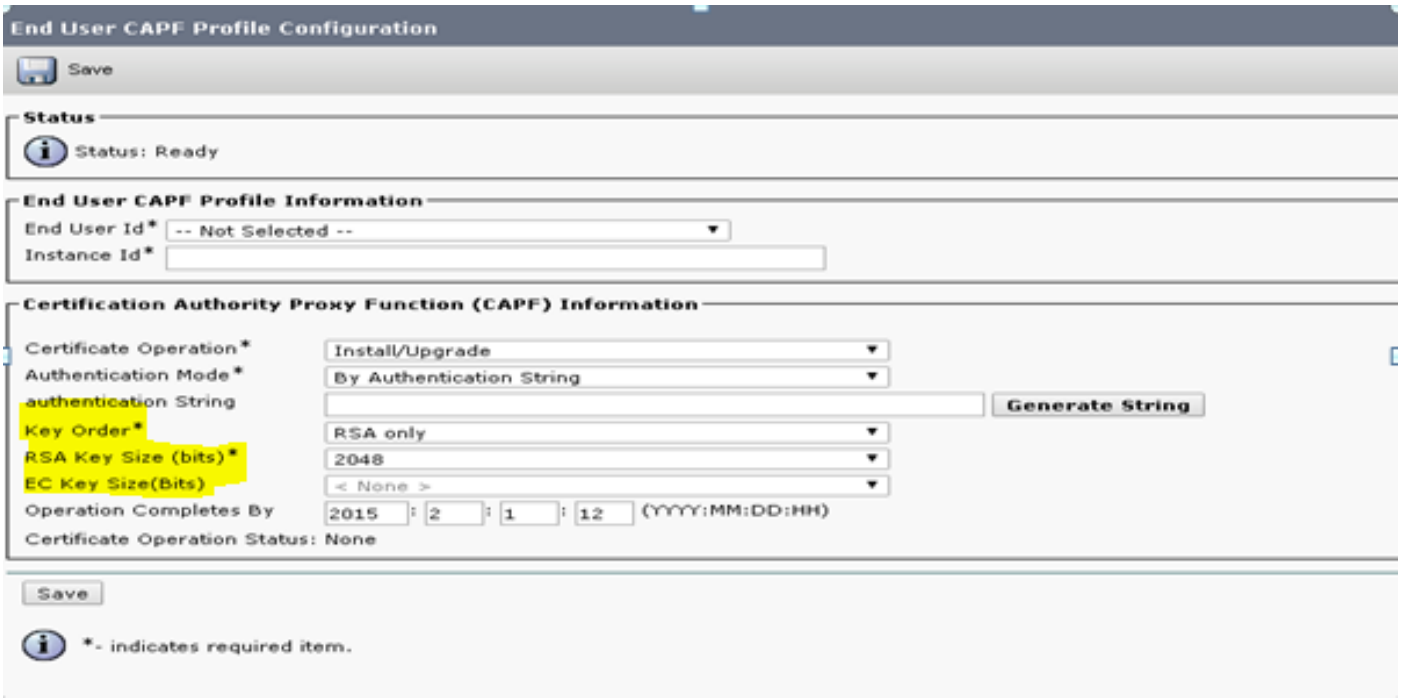


连接对**系统> Security >电话安全配置文件**

**用户管理>用户设置>应用程序用户CAPF配置文件**

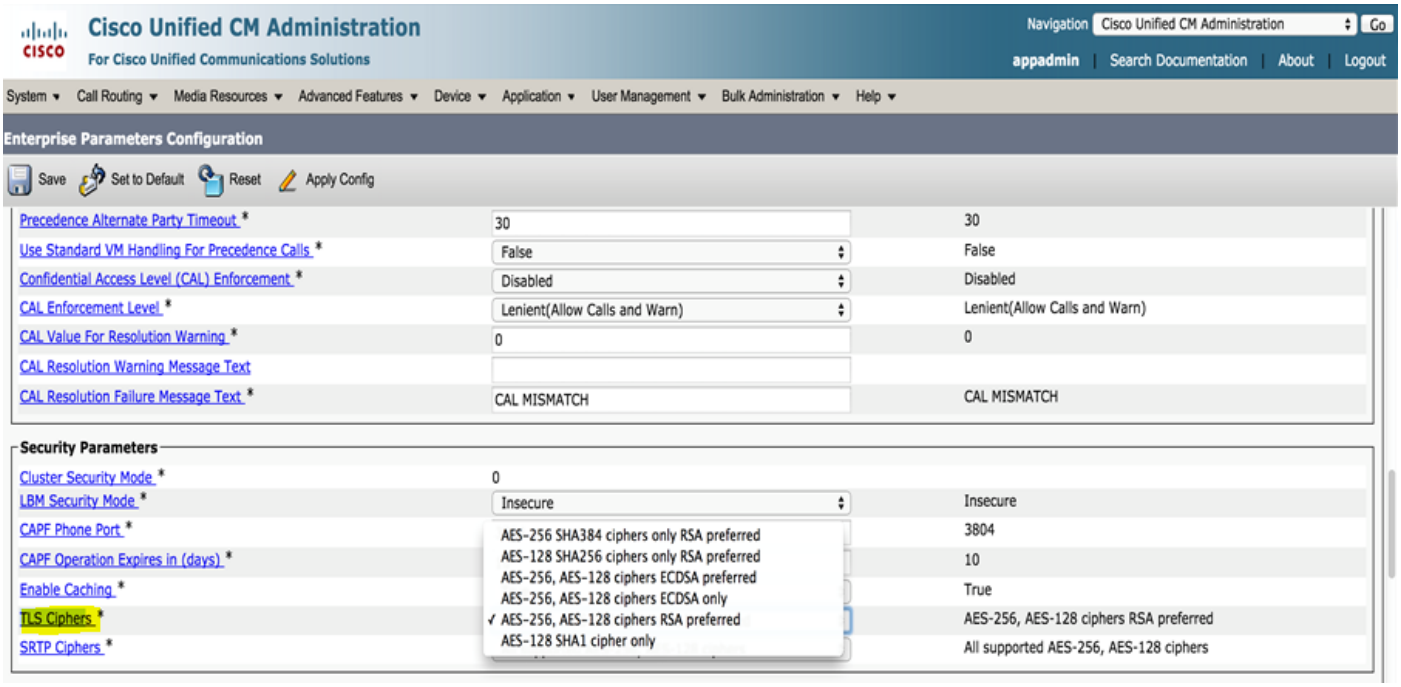



连接对**用户管理>用户设置>终端用户CAPF配置文件。**




# TLS密码企业参数

- 更新企业参数TLS密码支持ECDSA密码。
- 企业参数TLS密码当前设置SIP线路的TLS密码 ， SIP Trunk并且获取CTI Manager。




# SIP ECDSA技术支持

- Cisco Unified Communications Manager Release 11.0包括SIP线路和SIP中继接口的ECDSA技术支持。
- Cisco Unified通信管理器和终端电话或者视频设备之间的连接是SIP线路连接，而两个Cisco Unified通信管理器之间的连接是SIP中继线连接。
- 所有SIP连接支持ECDSA密码并且使用ECDSA证书。

修正安全的SIP接口支持这两个密码

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

这些是方案，当SIP建立(传输层安全)时TLS联系：

- 当SIP作为TLS服务器

当Cisco Unified通信管理器SIP中继接口作为流入安全的SIP连接时的一个TLS服务器， SIP中继接口确定呼叫管理器ECDSA认证是否在磁盘存在。如果认证在磁盘存在， SIP中继接口使用呼叫管理器ECDSA认证，如果所选的密码套件是

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256或
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

- 当SIP作为TLS客户端

当SIP中继接口作为TLS客户端时， SIP中继接口发送被请求的密码套件列表到根据也包括ECDSA加密选项)的TLS密码字段的服务器(在CUCM企业参数**TLS密码**。此配置确定TLS客户端密码套件列表和支持的密码套件按照首选的顺序。

**Note**:1.使用一个ECDSA密码建立与CUCM的联系的设备必须有在他们的身份信任列表(ITL)文件的呼叫管理器ECDSA认证。

Note:2.连接的SIP中继接口支持RSA TLS密码套件从不支持ECDSA密码套件的客户端或，当TLS连接被建立与CUCM时的一个更早版本，那不支持ECDSA。

# 安全的CTI Manager ECDSA技术支持

修正安全的CTI Manager接口支持这四个密码：

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

- 安全的CTI Manager接口负荷呼叫管理器和呼叫管理器ECDSA认证。这允许安全的CTI Manager接口与现有的RSA密码一起支持新的密码。
- 类似于SIP接口，在Cisco Unified通信管理器的企业参数TLS密码选项用于配置CTI Manager安全界面支持的TLS密码。

# 配置下载的HTTPS技术支持

- 对于安全的配置下载(例如Jabber客户端)， Cisco Unified Communications Manager Release 11.0被提高支持HTTPS除在更早版本使用的HTTP和TFTP接口之外。
- 如果必须，两客户端和服务器使用相互验证。然而，登记与ECDSA LSCs和被加密的TFTP配置要求的客户端提交他们的LSC。
- HTTPS接口使用呼叫管理器和呼叫管理器ECDSA证书作为服务器证明。

Note:1.当您更新呼叫管理器、呼叫管理器ECDSA或者Tomcat证书时，您必须撤销和恢复活动TFTP服务。

Note:2.端口6971使用呼叫管理器和呼叫管理器ECDSA证书的认证，使用由电话。

Note:3.端口6972使用Tomcat证书的认证，使用由Jabber。

# 熵

熵是数据的随机性测量并且帮助在确定普通的标准的最低门限值需求。要有强加密，需要熵的一个稳健来源。如果强加密算法，例如ECDSA，使用熵的一个弱的来源，可以容易地中断加密。

在Cisco Unified Communications Manager Release 11.0，改进Cisco Unified通信管理器的熵来源。

熵监控守护程序是不要求配置的一个内置的功能。然而，您能通过Cisco Unified通信管理器CLI关闭

它。

请使用以下CLI命令控制熵监控守护进程服务：

| 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. |

# Related Information

- http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/11_5_1/secugd/CUCM_BK_SEE2CFE1_00_cucm-security-guide-1151/CUCM_BK_SEE2CFE1_00_cucm-security-guide-1151_chapter_011.html#CUCM_RF_C0383C35_00l
- Technical Support & Documentation - Cisco Systems