CUCM 11.0下一代加密-椭圆曲线加密算法

目录

简介

本文描述介绍， Next_Generation加密(NGE)的配置从Cisco Unified Communications Manager (CUCM) 11.0及以后，符合高级安全和性能要求

先决条件

要求

Cisco 建议您了解以下主题：

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

使用的组件

本文档中的信息根据思科CUCM 11.0，其中edcsa证书为CallManager (CallManagerEDCSA)只支持

注意：CUCM 11.5向前支持TomcatEDCSA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

本文可能也与支持EDCSA证书的这些软件产品和版本一起使用：

- 思科IM和在线状态11.5
- Cisco Unity Connection 11.5

背景信息

椭圆曲线加密算法(ECC)是方法对根据椭圆曲线代数结构的公钥加密在有限的字段的。其中一个与非ECC加密算法比较的主要优点是密钥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。这通过测试和会议广泛的文档需求达到。

已接受和支持的由26国家(地区)世界各地通过普通的标准确认安排(CCRA)

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的证书强和为有普通的标准的产品要求(CC)证明。分级系统(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版本11.0向前包括。

ECDSA证书与现有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
- 安全SIP连接
- 计算机电话集成(CTI)管理器
- HTTP和
- 熵

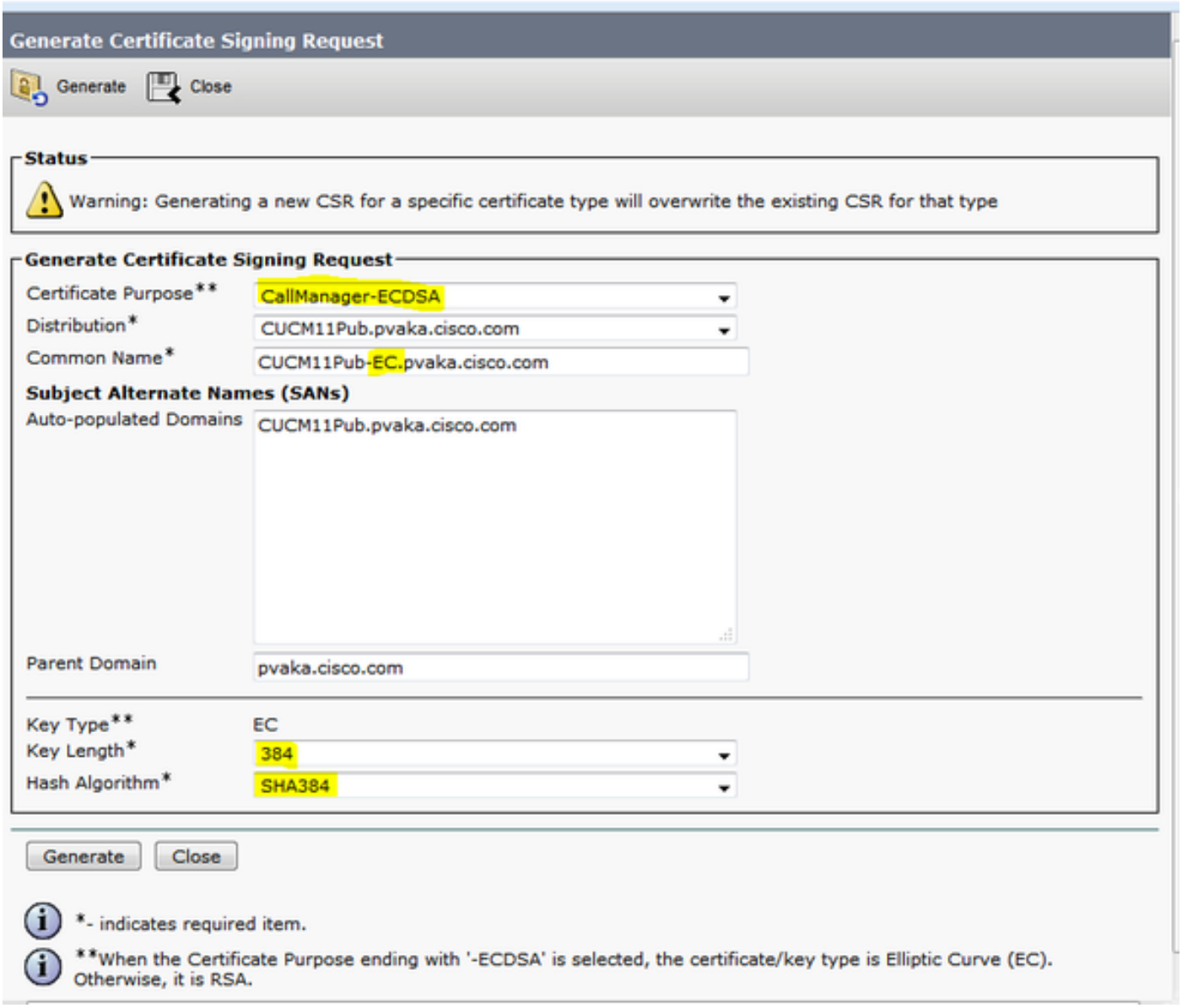
以下部分在上述7个区域中的每一个提供详细信息。

证书管理

生成与EC加密的证书

ECC的支持从向前生成与EC加密的CallManager证书的CUCM 11.0

- 如镜像所显示的新选项CallManager ECDSA联机。
- 要求公用名称的主机部分结束EC，防止有公用名称和CallManager证书一样。
- 在多服务器SAN证书的情况下，这必须结束EC MS。



- 两自签名证书请求和CSR请求根据EC密钥大小限制散列算法选择。
- 对于EC 256密钥大小散列算法可以是SHA256、SHA384或者SHA512。对于EC 384密钥大小散列算法可以是SHA384或SHA512。对于EC 521密钥大小唯一选择是SHA512。
- DEFAULT键大小是384，并且默认哈希算法是SHA384，能更改丢弃下来。选项联机根据选定的密钥大小。

CLI 配置

名为CallManager 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)?
```

- 设置cert导入拥有|信任[unit] –导入CA签名证书

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

- 设置csr gen [unit] –生成指定的单元的证书签署的request(CSR)

```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- 设置大批出口|统一|导入tftp –当tftp是单元名称时， CallManager ECDSA证书获得自动包括与CallManager RSA证书散装操作。

CTL和ITL文件：

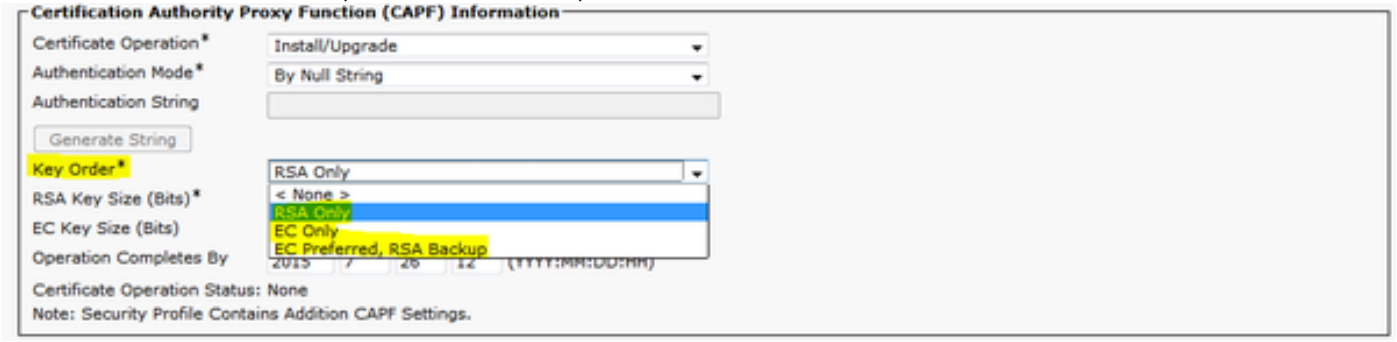
- CTL和ITL文件有CallManager **ECDSA**存在。
- CallManager ECDSA证书有CCM+TFTP的功能在ITL和CTL文件。
- 如镜像所显示，您能使用**显示ctl**或**显示itl**命令查看此信息：

```
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**使用情况ctl更新**生成CTL文件。

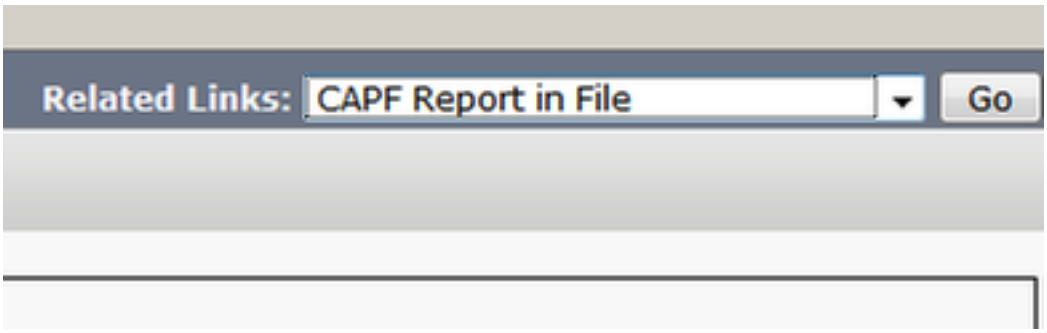
认证机关代理功能(CAPF)

- 在CUCM 11提供支持的CAPF版本3.0与RSA一起的EC密钥大小的。
- 另外的CAPF选项提供除现有CAPF字段之外是关键命令和EC密钥大小(位)。
- 现有密钥大小(位)选项更改对RSA密钥大小(位)。
- 仅RSA，仅EC和EC的关键命令提供支持更喜欢， RSA备份选项。
- 密钥大小的EC密钥大小提供支持256个， 384个和521个位。
- 512个， 1024个和2048个位的RSA密钥大小提供支持
- 当关键仅RSA的命令选择，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，时RSA和EC密钥大小可以选择。



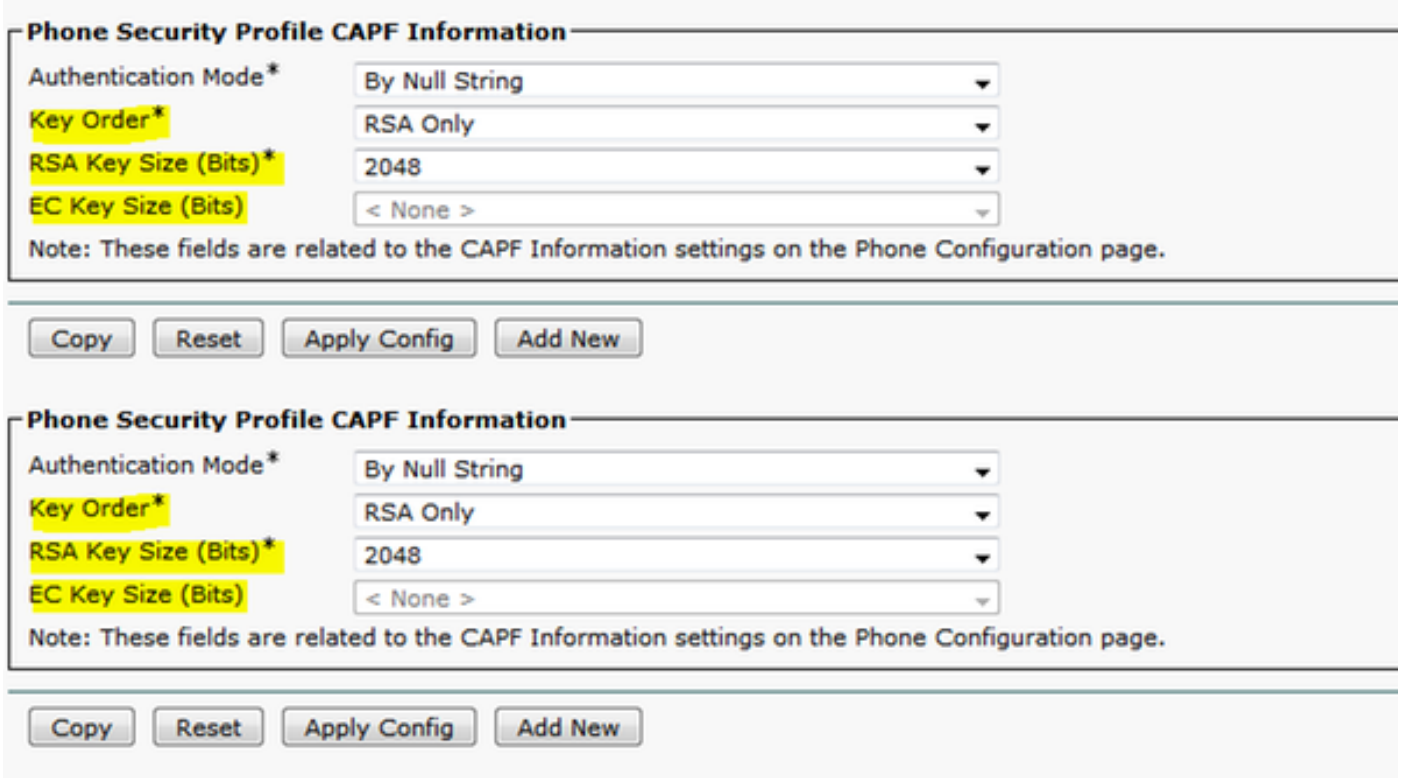
电话、电话安全配置文件、最终用户和应用程序用户页的另外的CAPF选项

Device > Phone >相关链接

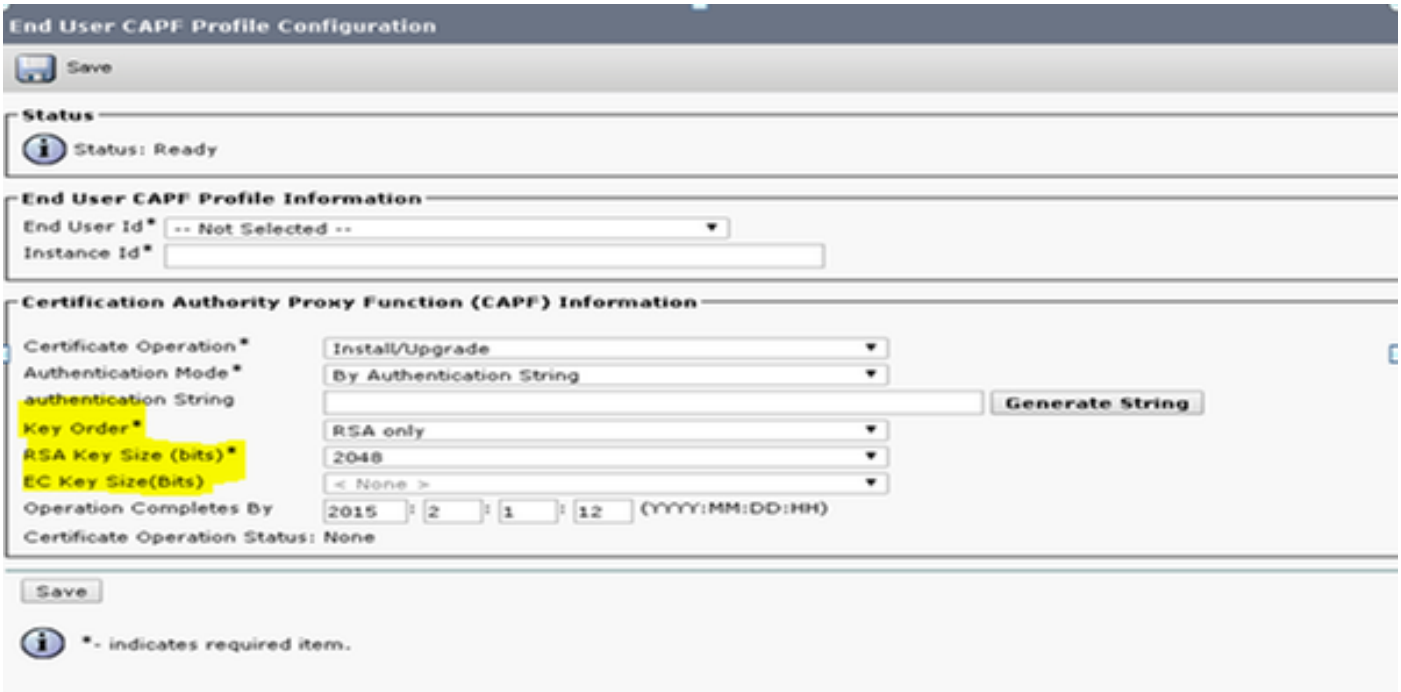


导航对**系统> Security >电话安全配置文件**

用户管理>用户设置>应用程序用户CAPF配置文件

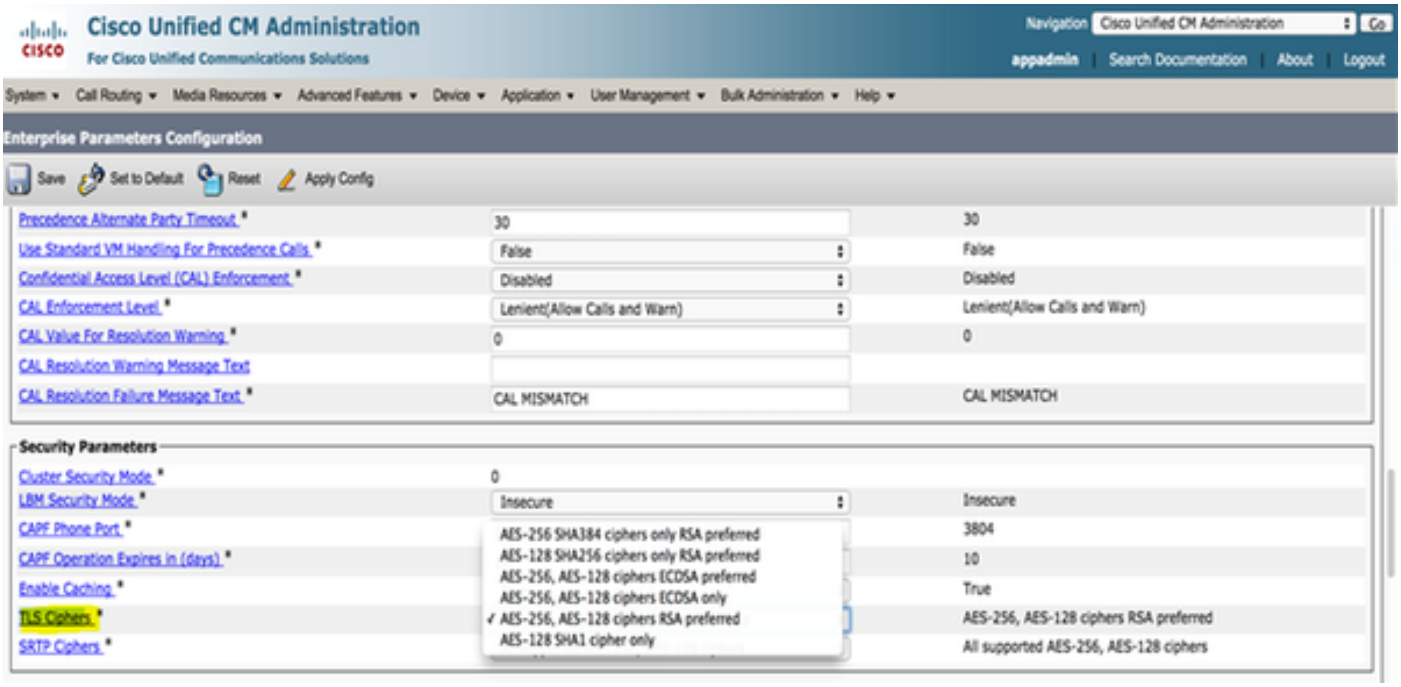


对**用户管理>用户设置>最终用户CAPF的**Navigaet**配置文件。**



TLS密码器企业参数

- 企业参数TLS密码器更新支持ECDSA密码器。
- 企业参数TLS密码器当前设置SIP线路、SIP中继和安全CTI Manager的TLS密码器。



SIP ECDSA支持

- Cisco Unified Communications Manager版本11.0包括SIP线路和SIP中继接口的ECDSA支持。
- Cisco Unified Communications Manager和终端之间的连接打电话或视频设备是SIP线路连接，而两Cisco Unified Communications Manager之间的连接是SIP中继连接。
- 所有SIP连接支持ECDSA密码器并且使用ECDSA证书。

安全SIP接口更新支持这两密码器

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 Communications Manager SIP中继接口作为流入安全SIP连接的时一个TLS服务器，SIP中继接口确定CallManager ECDSA证书是否在磁盘存在。如果证书在磁盘存在，SIP中继接口使用CallManager ECDSA证书，如果选定密码器套件是

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中继接口发送请求的密码器套件列表到根据也包括ECDSA加密选项)的TLS密码器领域的服务器(**TLS加密的**CUCM企业参数的。此配置确定TLS客户端密码器套件列表和支持的密码器套件按照首选的顺序。

注意：1.使用一ECDSA密码器建立对CUCM的联系的设备必须有在他们的标识托拉斯列表(ITL)文件的CallManager ECDSA证书。

注意：2.连接的SIP中继接口支持RSA TLS密码器套件从不支持ECDSA密码器套件的客户端或

，当TLS连接建立与CUCM时更早版本，那不支持ECDSA。

安全CTI Manager ECDSA支持

安全CTI Manager接口更新支持这四密码器：

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 Manager接口负载CallManager和CallManager ECDSA证书。这允许安全CTI Manager接口与现有RSA密码器一起支持新的密码器。
- 类似于SIP接口，在Cisco Unified Communications Manager的企业参数TLS密码器选项用于配置CTI Manager安全接口支持的TLS密码器。

配置下载的HTTPS支持

- 对于安全的配置下载(例如Jabber客户端)， Cisco Unified Communications Manager版本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和加密的TFTP配置的客户端要求提交他们的LSC。
- HTTPS接口使用CallManager和CallManager ECDSA证书作为服务器证书。

注意：1.当您更新CallManager、CallManager ECDSA或者Tomcat证书时，您必须撤销和恢复活动TFTP服务。

注意：2.波尔特6971使用CallManager和CallManager ECDSA证书的验证，使用由电话。

注意：3.波尔特6972使用Tomcat证书的验证，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，熵一稳健来源要求。如果强加密算法，例如ECDSA，使用熵一弱来源，可以容易地中断加密。

在Cisco Unified Communications Manager版本11.0中， Cisco Unified Communications Manager的熵来源改善。

熵监听守护程序是不要求配置的一个内置的功能。然而，您通过Cisco Unified Communications Manager CLI能关掉。

请使用以下CLI命令控制熵监听守护进程服务：

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.

相关信息

- 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
- 技术支持和文档 - Cisco Systems