CUCM 11.0下一代加密 — 橢圓曲線加密

目錄

簡介

本文檔介紹從Cisco Unified Communications Manager(CUCM)11.0及更高版本配置下一代加密(NGE)以滿足增強的安全性和效能要求。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco CallManager安全基礎知識
- Cisco CallManager憑證管理

採用元件

本檔案中的資訊是根據Cisco CUCM 11.0，其中CallManager(CallManager-ECDSA)僅支援Elliptic Curve Digital Signature Algorithm(ECDSA)憑證。

> **附註**：CUCM 11.5及更高版本也支援tomcat-ECDSA證書。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

本檔案也適用於支援ECDSA憑證的軟體產品和版本：

- Cisco Unified CM IM and Presence 11.5
- Cisco Unity連線11.5

背景資訊

橢圓曲線密碼演算法(ECC)是一種基於有限域上橢圓曲線代數結構的公鑰密碼演算法(PECC)，是一種新的加密演算法。與非ECC加密相比，主要優點之一是較小的金鑰可提供相同級別的安全性。

通用標準(CC)可確保安全功能在所評估的解決方案中正常運行。這是通過測試和滿足廣泛的文檔要求實現的。

通過共同標準認可安排(CCRA)，它被全球26個國家接受和支援。

Cisco Unified Communications Manager 11.0版支援橢圓曲線數位簽章演算法(ECDSA)證書。

這些證書比基於RSA的證書強，並且是具有CC證書的產品所必需的。美國政府的分類系統商業解決方案(CSfC)計畫需要CC認證，因此它包含在Cisco Unified Communications Manager 11.0版及更高版本中。

ECDSA證書與現有的RSA證書一起在以下區域提供：

- 憑證管理
- 憑證授權單位代理功能(CAPF)
- 傳輸層安全(TLS)跟蹤
- 安全作業階段啟始通訊協定(SIP)連線
- 電腦電話整合(CTI)管理員
- HTTP
- 熵

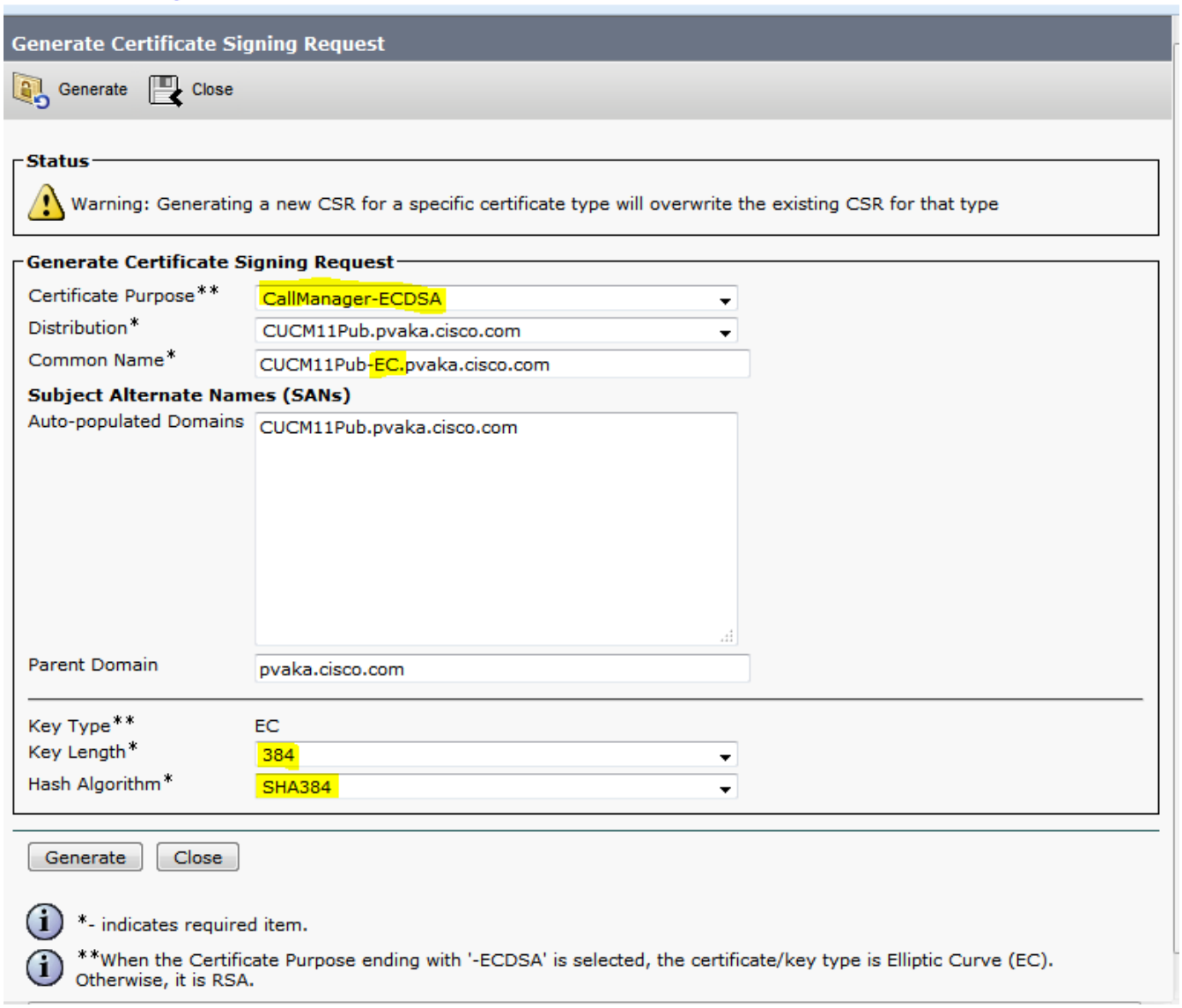
接下來的部分將詳細介紹這七個方面的情況。

憑證管理

使用橢圓曲線加密生成證書

支援CUCM 11.0及更高版本的ECC，以生成橢圓曲線(EC)加密的CallManager證書：

- 新選項**CallManager-ECDSA**可用，如下圖所示。
- 它要求公用名稱的主機部分以**-EC**結尾。這可以防止與CallManager證書具有相同**的公**用名。
- 在多伺服器SAN證書的情況下，此證書必須以**-EC-ms**結尾。



- 自簽名證書請求和CSR請求都根據EC金鑰大小限制雜湊演算法選擇。
- 對於EC 256金鑰大小，雜湊演算法可以是SHA256、SHA384或SHA512。對於EC 384金鑰大小，雜湊演算法可以是SHA384或SHA512。對於EC 521金鑰大小，唯一的選項是SHA512。
- 預設金鑰大小為384，預設雜湊演算法為SHA384，可以更改。可用的選項取決於所選的金鑰大小。

CLI組態

已為CLI命令新增名為**CallManager-ECDSA**的新證書單元

- set cert regen [unit] — 重新生成自簽名證書

```
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] — 匯入CA簽名的證書

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

- set csr gen [unit] — 為指定裝置生成證書簽名請求(CSR)

```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- set bulk export|consolidate|import tftp — 當tftp是裝置名稱時，CallManager-ECDSA證書會在批次操作中自動包含在CallManager RSA證書中。

CTL和ITL檔案

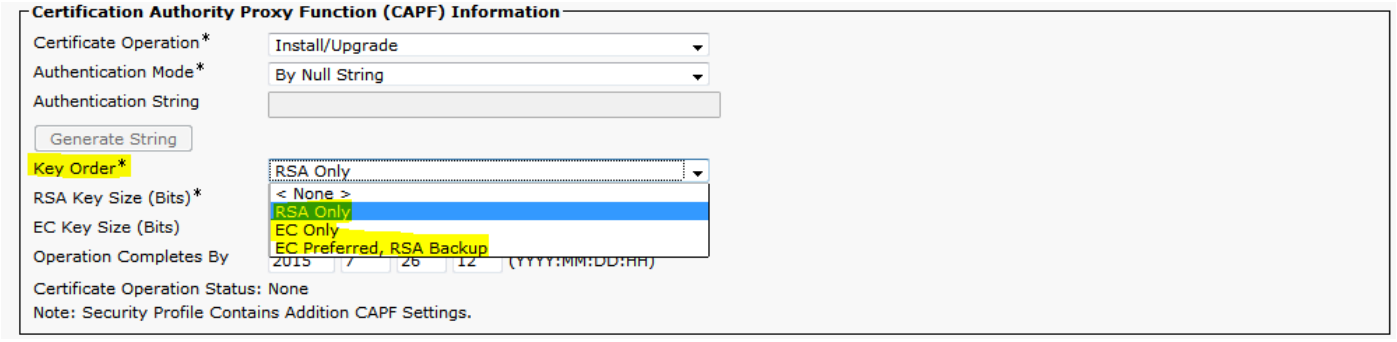
- 證書信任清單(CTL)和標識信任清單(ITL)檔案**都存在CallManager-**ECDSA。
- CallManager-ECDSA證書在ITL和CTL檔案中具有CCM+TFTP功能。
- 您可以使用 **show ctl** 或 **show itl** 命令檢視此資訊，如下圖所示：

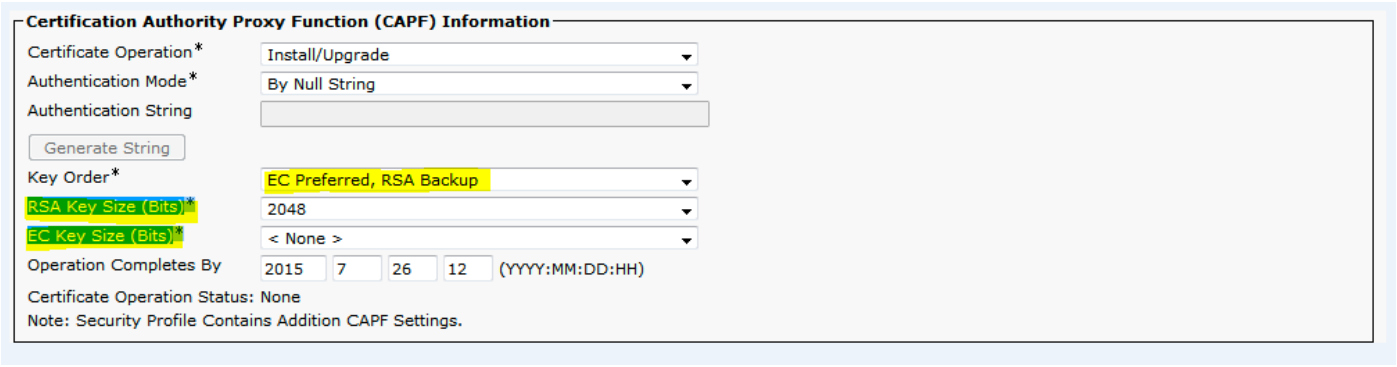
```
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1656
2       DNSNAME         2
3       SUBJECTNAME     65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME 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

- 您可以使用**utils ctl update**命令生成CTL檔案。

證書頒發機構代理函式

- CUCM 11中的證書頒發機構代理功能(CAPF)3.0版支援EC金鑰大小以及RSA。
- 除了現有的CAPF欄位外，還提供了其他CAPF選項：金鑰順序和EC金鑰大小（位）。
- 現有的「金鑰大小（位）」選項已更改為「RSA金鑰大小（位）」。
- 金鑰訂單提供僅支援RSA、僅支援EC和EC首選RSA備份選項。
- EC金鑰大小支援256、384和521位的金鑰大小。
- RSA金鑰大小支援512、1024和2048位。
- 如果選擇「僅RSA金鑰順序」，則只能選擇「RSA金鑰大小」。如果選擇EC only，則只能選擇EC Key Size。選擇EC首選RSA備份時，可以同時選擇RSA和EC金鑰大小。

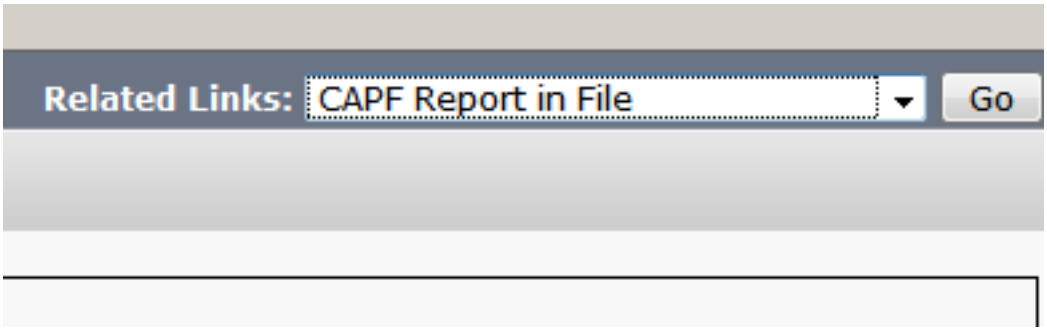




附註：目前沒有思科終端支援CAPF版本3，因此不要選擇EC Only選項。但是，想要稍後支援ECDSA本地重要證書(LSC)的管理員可以使用EC首選RSA備份選項配置其裝置。當終端開始支援ECDSA LSC的CAPF版本3時，管理員需要重新安裝其LSC。

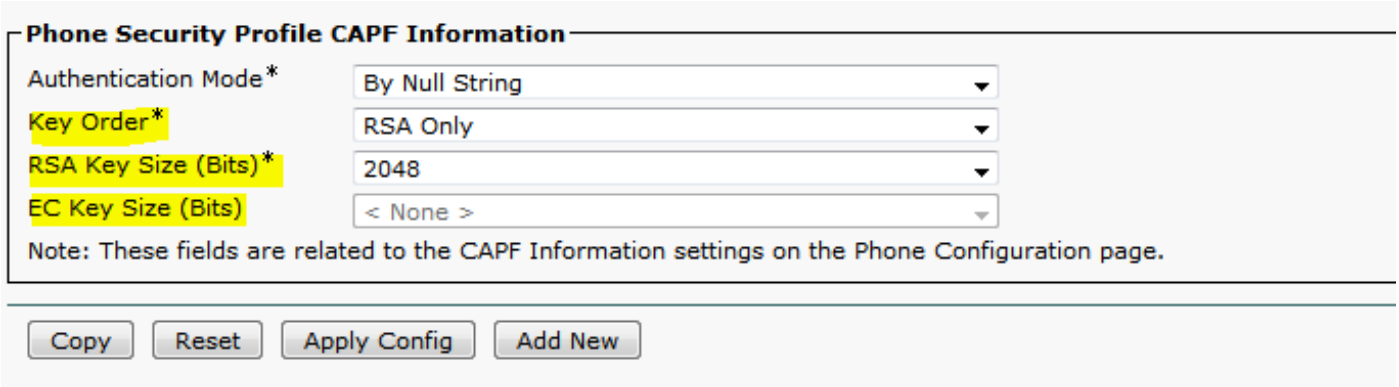
電話、電話安全配置檔案、終端使用者和應用程式使用者頁面的其他CAPF選項如下所示：

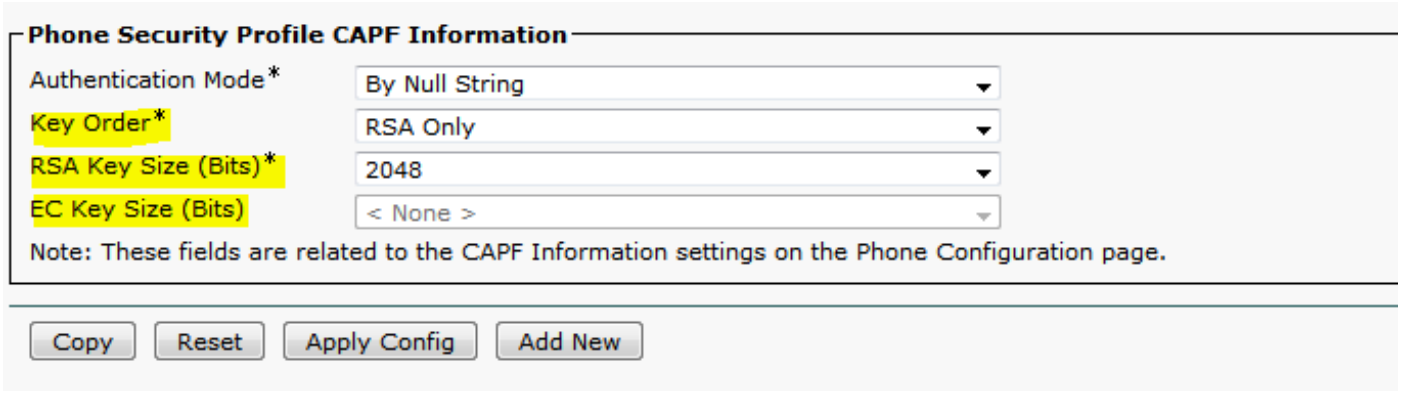
Device > Phone > Related Links



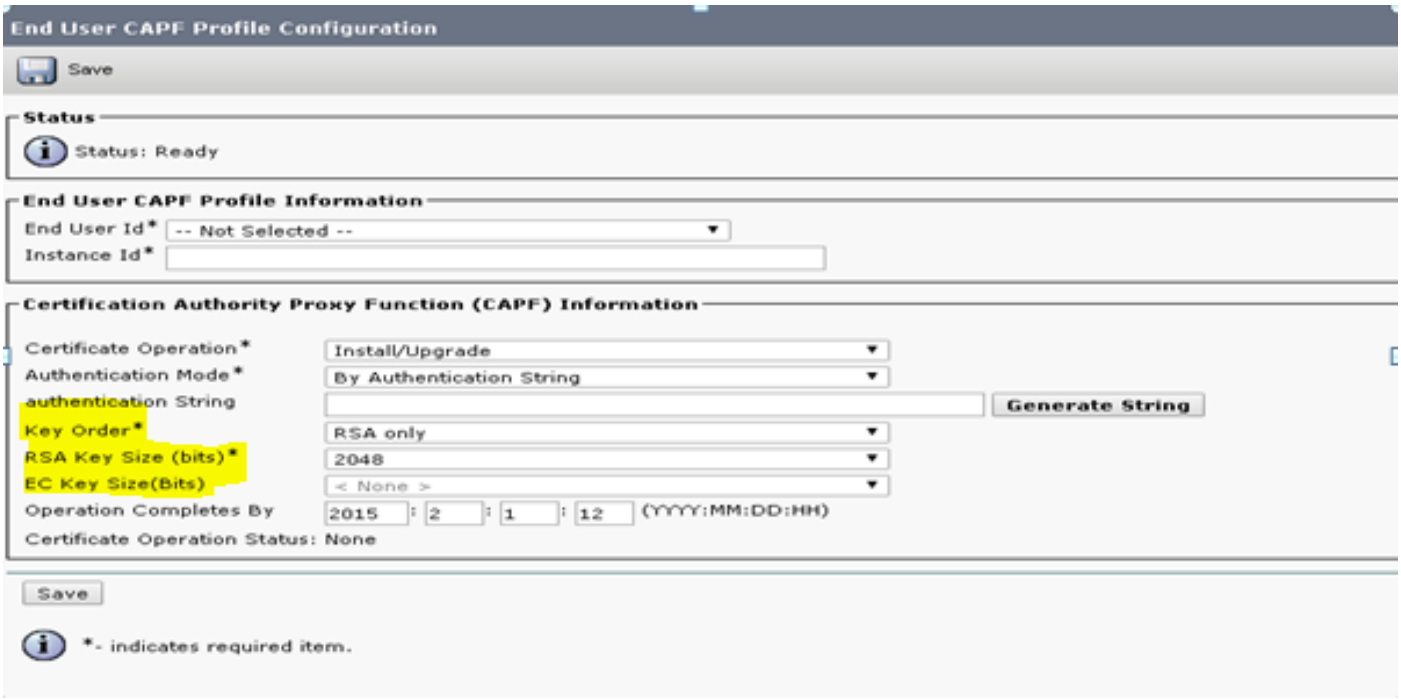
導航到**System > Security > Phone security profile**

使用者管理>使用者設定>應用程式使用者CAPF配置檔案



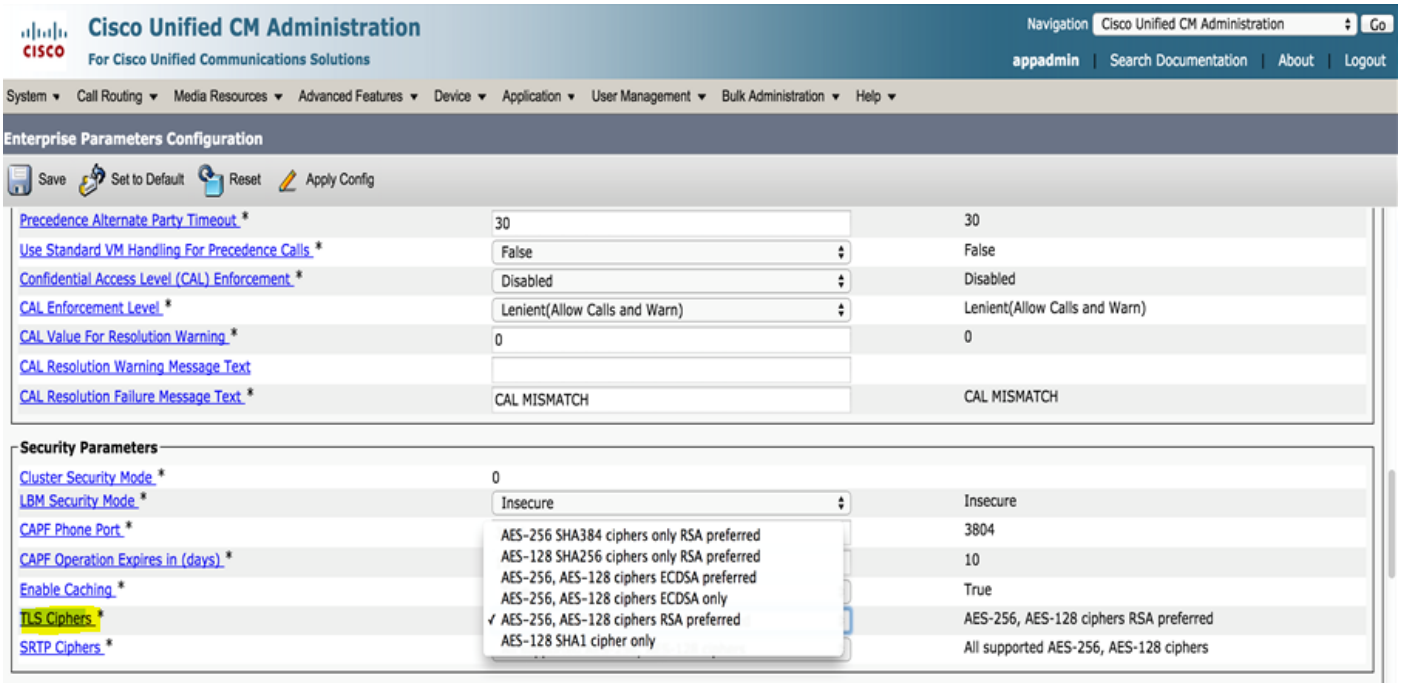


導航至**使用者管理>使用者設定>終端使用者CAPF配置檔案。**



TLS密碼企業引數

- 已更新企業引數TLS密碼以支援ECDSA密碼。
- 企業引數TLS密碼現在為SIP線路、SIP中繼和安全CTI管理器設定TLS密碼。



SIP ECDSA支援

- Cisco Unified Communications Manager 11.0版包括對SIP線路和SIP中繼介面的ECDSA支援。
- Cisco Unified Communications Manager與終端電話或影片裝置之間的連線是SIP線路連線，而兩個思科統一通訊管理器之間的連線是SIP中繼連線。
- 所有SIP連線都支援ECDSA密碼並使用ECDSA證書。

已更新安全SIP介面以支援以下兩個密碼：

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

以下是SIP建立TLS連線的場景：

- 當SIP充當TLS伺服器時 當Cisco Unified Communications Manager的SIP中繼介面用作傳入安全SIP連線的TLS伺服器時，SIP中繼介面將確定CallManager-ECDSA證書是否存在於磁碟上。如果磁碟上存在該證書，則如果選定的密碼套件為TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256或TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- 當SIP充當TLS客戶端時 當SIP中繼介面充當TLS客戶端時，SIP中繼介面會根據CUCM Enterprise Parameters **The TLS Ciphers中的**TLS Ciphers欄位（其中也包括ECDSA ciphers選項）向伺服器傳送請求的密碼套件清單。此配置按優先順序確定TLS客戶端密碼套件清單和支援的密碼套件。

附註：
— 使用ECDSA密碼連線到CUCM的裝置必須在其身份信任清單(ITL)檔案中具有CallManager-ECDSA證書。
- SIP中繼介面支援RSA TLS密碼套件，適用於來自不支援ECDSA密碼套件的客戶端的連線，或者當使用不支援ECDSA的早期版本CUCM建立TLS連線時。

安全CTI管理器ECDSA支援

已更新安全CTI管理器介面以支援以下四個密碼：

- 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管理器介面載入CallManager和CallManager-ECDSA證書。這允許Secure CTI Manager介面支援新密碼和現有的RSA密碼。

與SIP介面類似，Cisco Unified Communications Manager中的「企業引數TLS密碼」選項用於配置CTI Manager安全介面支援的TLS密碼。

適用於組態下載的HTTPS支援

- 對於安全配置下載（例如Jabber客戶端），Cisco Unified Communications Manager 11.0版經過增強，除了在早期版本中使用的HTTP和TFTP介面之外，還支援HTTPS。
- 如果需要，客戶端和伺服器都使用相互身份驗證。但是，註冊了ECDSA LSC和加密TFTP配置的客戶端需要提供其LSC。
- HTTPS介面使用CallManager和CallManager-ECDSA證書作為伺服器證書。

  附註：
  — 更新CallManager、CallManager ECDSA或Tomcat證書時，必須停用並重新啟用TFTP服務。
  — 埠6971用於驗證電話使用的CallManager和CallManager-ECDSA證書。
  — 埠6972用於Jabber使用的Tomcat證書身份驗證。

熵

熵是對資料的隨機性的一種度量、可幫助確定共同標準要求的最小閾值。要具有強加密，需要一個強健的熵源。如果強加密演算法（如ECDSA）使用弱熵源，則加密很容易被破解。

在Cisco Unified Communications Manager 11.0版中，Cisco Unified Communications Manager的熵源得到了改進。

熵監控守護程式是一個不需要配置的內建功能。但是您可以通過Cisco Unified Communications Manager CLI將其關閉。

使用以下CLI命令控制熵監視守護程式服務：

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.

相關資訊

- 思科整合通訊管理員安全指南11.5(1)版
- 技術支援與文件 - Cisco Systems