CUCM 11.0 Crittografia di nuova generazione - Crittografia a curva ellittica

Sommario

Introduzione

Questo documento descrive la configurazione della crittografia di nuova generazione (NGE) da Cisco Unified Communications Manager (CUCM) versione 11.0 e successive per soddisfare i requisiti avanzati di sicurezza e prestazioni.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Nozioni fondamentali sulla sicurezza di Cisco CallManager
- Gestione certificati Cisco CallManager

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco CUCM 11.0, dove i certificati ECDSA (Elliptic Curve Digital Signature Algorithm) sono supportati solo per CallManager (CallManager-ECDSA).

> **Nota:** CUCM versione 11.5 e successive supporta anche i certificati tomcat-ECDSA.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Il presente documento può essere utilizzato anche con i seguenti prodotti software e versioni che supportano i certificati ECDSA:

- Cisco Unified CM IM e Presence 11.5
- Cisco Unity Connection 11.5

Premesse

La crittografia a curva ellittica (ECC) è un approccio alla crittografia a chiave pubblica basato sulla struttura algebrica delle curve ellittiche su campi finiti. Uno dei principali vantaggi rispetto alla crittografia non ECC è lo stesso livello di protezione offerto dalle chiavi di dimensioni inferiori.

Common Criteria (CC) garantisce il corretto funzionamento delle funzionalità di sicurezza all'interno della soluzione in fase di valutazione. Ciò è possibile grazie a test e al rispetto di requisiti di documentazione completi.

Èaccettato e sostenuto da 26 paesi in tutto il mondo attraverso il Common Criteria Recognition Arrangement (CCRA).

Cisco Unified Communications Manager versione 11.0 supporta i certificati ECDSA (Elliptic Curve Digital Signature Algorithm).

Questi certificati sono più avanzati di quelli basati su RSA e sono richiesti per i prodotti con certificazioni CC. Il programma Commercial Solutions for Classified Systems (CSfC) del governo degli Stati Uniti richiede la certificazione CC e pertanto è incluso in Cisco Unified Communications Manager versione 11.0 e successive.

I certificati ECDSA sono disponibili insieme ai certificati RSA esistenti nelle seguenti aree:

- Gestione certificati
- Funzione CAPF (Certification Authority Proxy Function)
- Traccia Transport Layer Security (TLS)
- Connessioni SIP (Secure Session Initiation Protocol)
- Gestione CTI (Computer Telephony Integration)
- HTTP
- Entropia

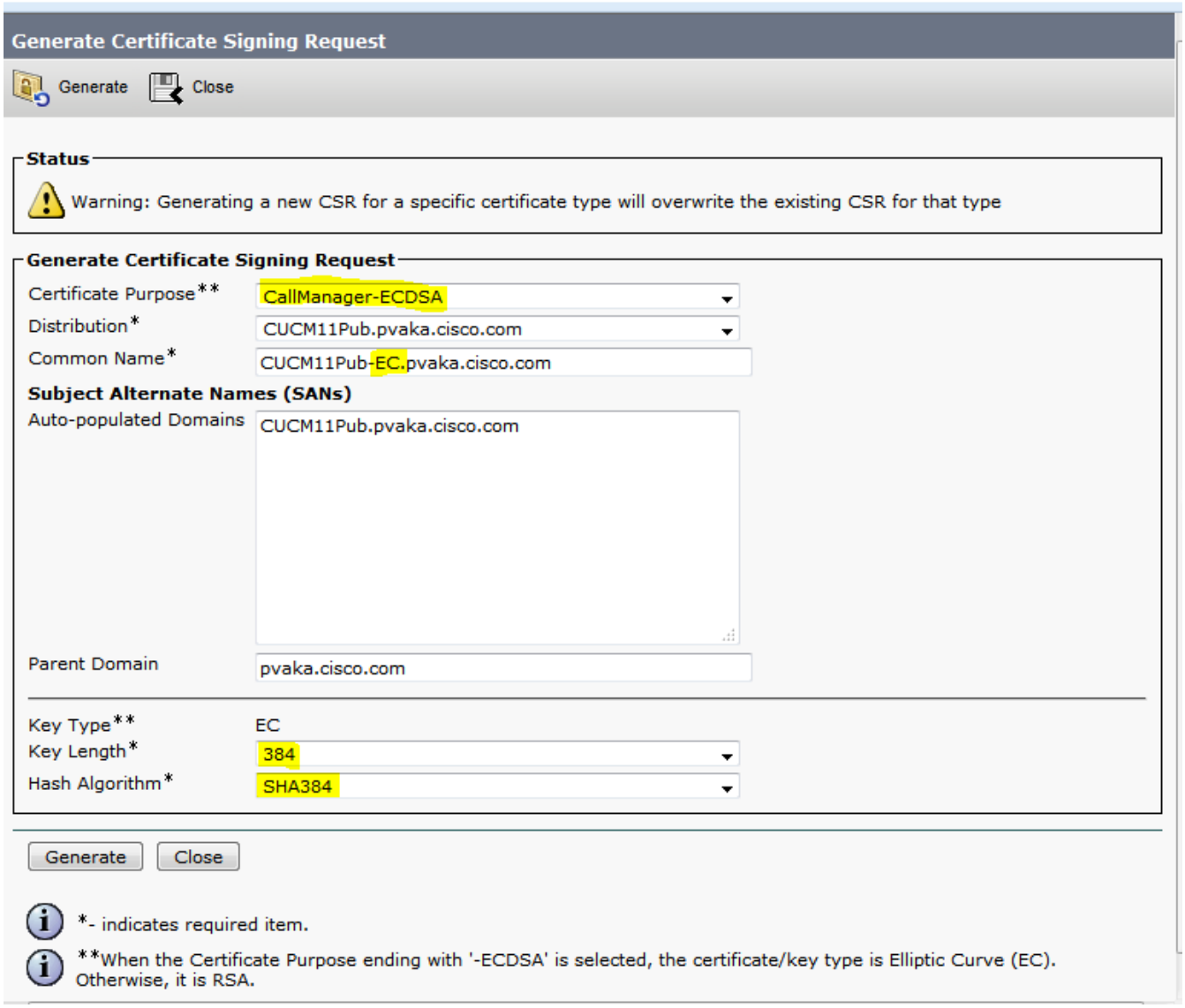
Le sezioni successive forniscono informazioni più dettagliate su ognuna di queste sette aree.

Gestione certificati

Genera certificati con crittografia a curva ellittica

Supporto per ECC da CUCM 11.0 e versioni successive per generare un certificato CallManager con crittografia EC (Elliptical Curve):

- La nuova opzione **CallManager-ECDSA** è disponibile come mostrato nell'immagine.
- Ènecessario che la parte host del nome comune termini in **-EC**. In questo modo si evita di avere lo stesso nome comune del certificato **CallManager**.
- In caso di certificato SAN multiserver, deve terminare in **-EC-ms**.



- Sia la richiesta di certificato autofirmato che la richiesta CSR limitano le scelte dell'algoritmo hash a seconda delle dimensioni della chiave EC.
- Per una dimensione della chiave EC 256, l'algoritmo hash può essere SHA256, SHA384 o SHA512. Per una dimensione della chiave EC 384, l'algoritmo hash può essere SHA384 o SHA512. Per una dimensione della chiave EC 521, l'unica opzione disponibile è SHA512.
- La dimensione della chiave predefinita è 384, mentre l'algoritmo hash predefinito è SHA384, che può essere modificato. Le opzioni disponibili dipendono dalle dimensioni della chiave scelte.

Configurazione CLI

Èstata aggiunta una nuova unità certificato denominata **CallManager-ECDSA** per i comandi CLI

- set cert regen [unit] - rigenera il certificato autofirmato

```
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] - importa certificato firmato da CA

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

- set csr gen [unit] - genera una richiesta di firma del certificato (CSR) per l'**unità** specificata

```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- set bulk export|consolidate|import tftp - Quando tftp è il nome dell'unità, i certificati CallManager-ECDSA vengono inclusi automaticamente con i certificati RSA CallManager nelle operazioni di massa.

File CTL e ITL

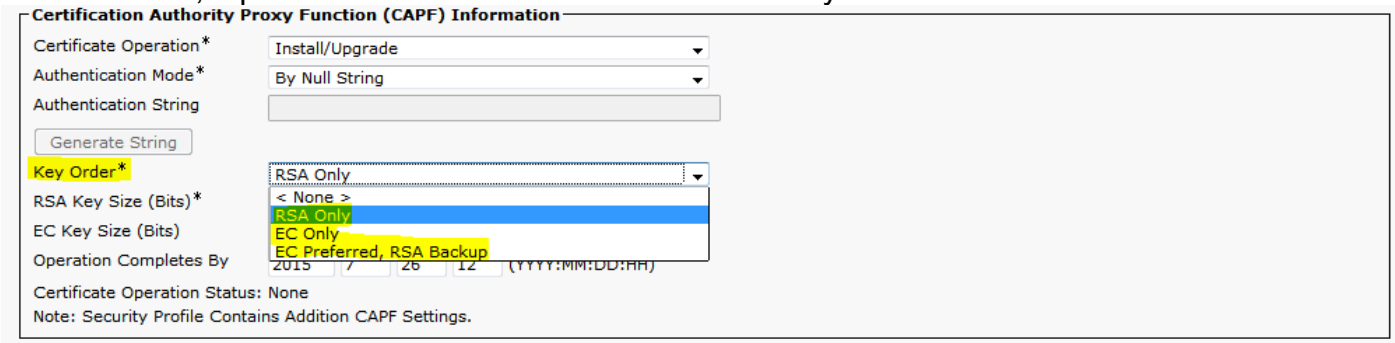
- Sia i file dell'elenco di certificati attendibili (CTL) che quelli dell'elenco di certificati attendibili (ITL) dispongono di **CallManager-ECDSA**.
- Il certificato CallManager-ECDSA ha la funzione CCM+TFTP sia nel file ITL che nel file CTL.
- Èpossibile utilizzare **show ctl** o **show itl** per visualizzare queste informazioni, come mostrato nell'immagine:

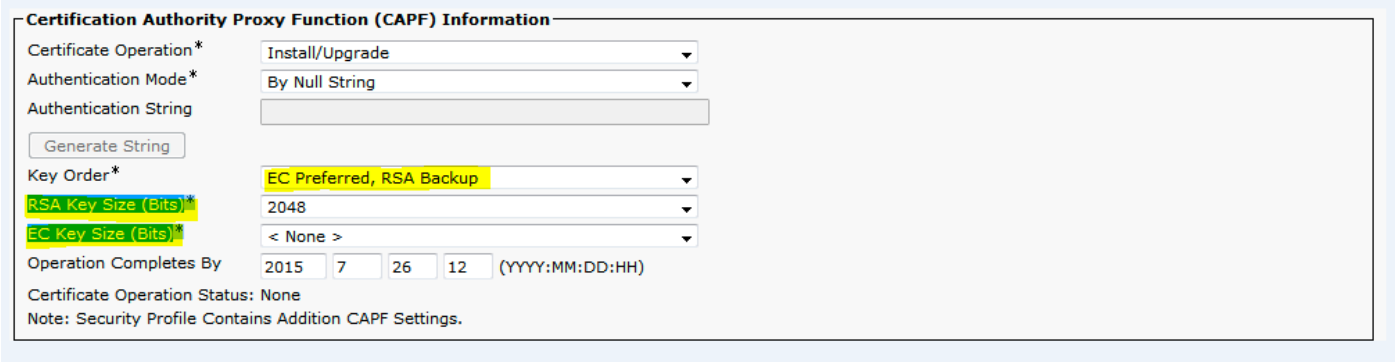
```
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1656
2       DNSNAME         2
3       SUBJECTNAME     65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME 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

- Èpossibile utilizzare il comando **utils ctl update** per generare il file CTL.

Funzione proxy Autorità di certificazione

- La funzione CAPF (Certificate Authority Proxy Function) versione 3.0 in CUCM 11 fornisce il supporto per le dimensioni della chiave EC insieme a RSA.
- Le opzioni CAPF aggiuntive fornite in aggiunta ai campi CAPF esistenti sono Key Order e EC Key Size (bit).
- L'opzione Key Size (bit) esistente è stata modificata in RSA Key Size (bit).
- L'ordine delle chiavi fornisce il supporto per le opzioni di backup RSA Only, EC Only e EC Preferred.
- La dimensione della chiave EC supporta le dimensioni della chiave di 256, 384 e 521 bit.
- Le dimensioni della chiave RSA supportano 512, 1024 e 2048 bit.
- Quando si seleziona l'opzione Key Order of RSA Only, è possibile selezionare solo RSA Key Size. Se è selezionato Solo EC, è possibile selezionare solo EC Key Size. Se si sceglie EC Preferred, è possibile selezionare sia RSA che EC Key Size.

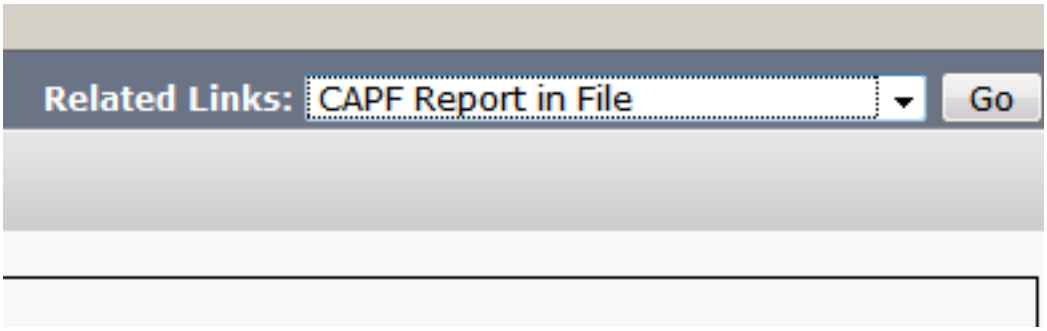




> **Nota:** Attualmente nessun endpoint Cisco supporta CAPF versione 3, quindi non selezionare l'opzione EC Only. Tuttavia, gli amministratori che desiderano supportare i certificati LSC (Locally Significant Certificates) ECDSA in un secondo momento possono configurare i propri dispositivi con l'opzione di backup RSA preferenziale EC. Quando gli endpoint iniziano a supportare CAPF versione 3 per le liste LCS ECDSA, gli amministratori devono reinstallare le rispettive liste LSC.

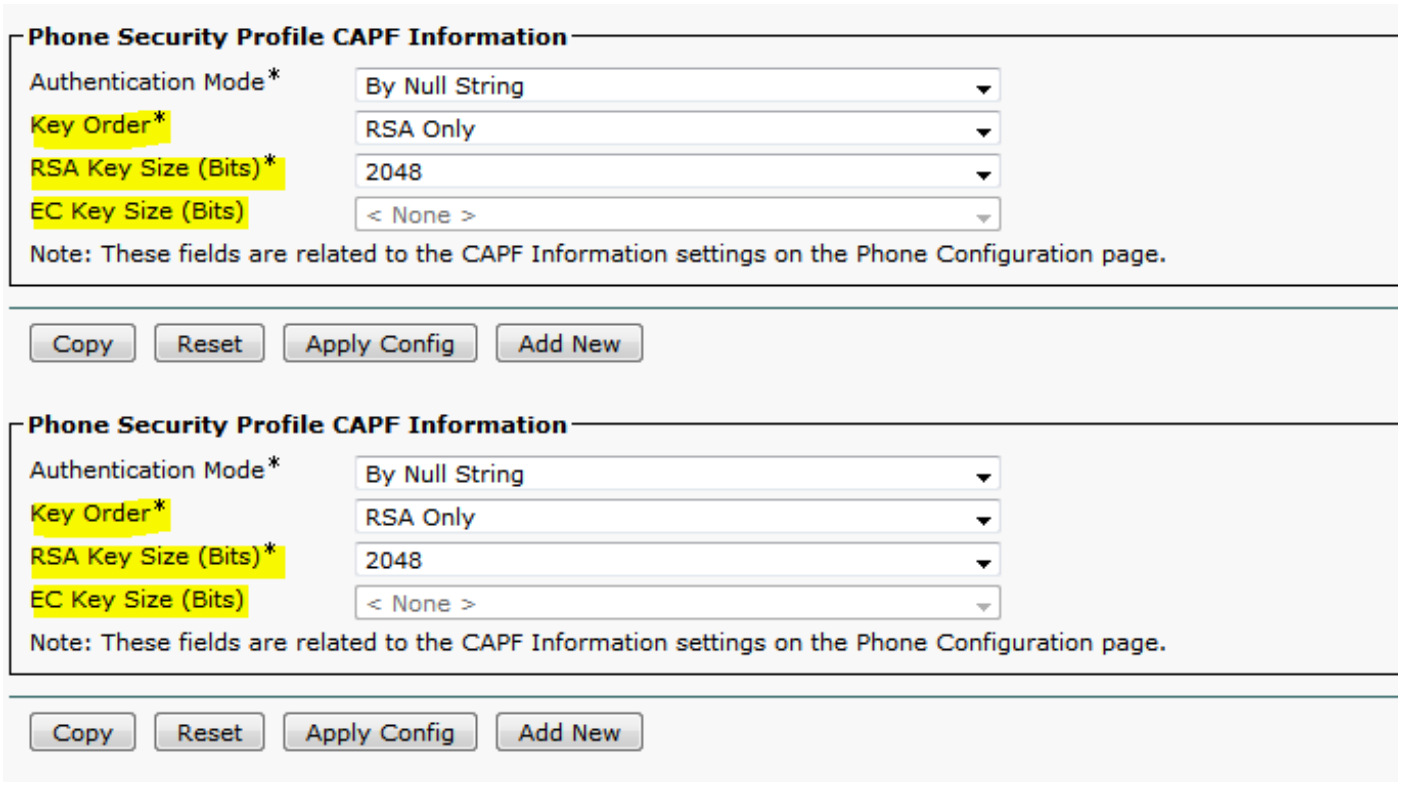
Di seguito sono riportate le opzioni CAPF aggiuntive per le pagine Telefono, Sicurezza telefono, Utente finale e Utente applicazione:

Dispositivo > Telefono > Collegamenti correlati

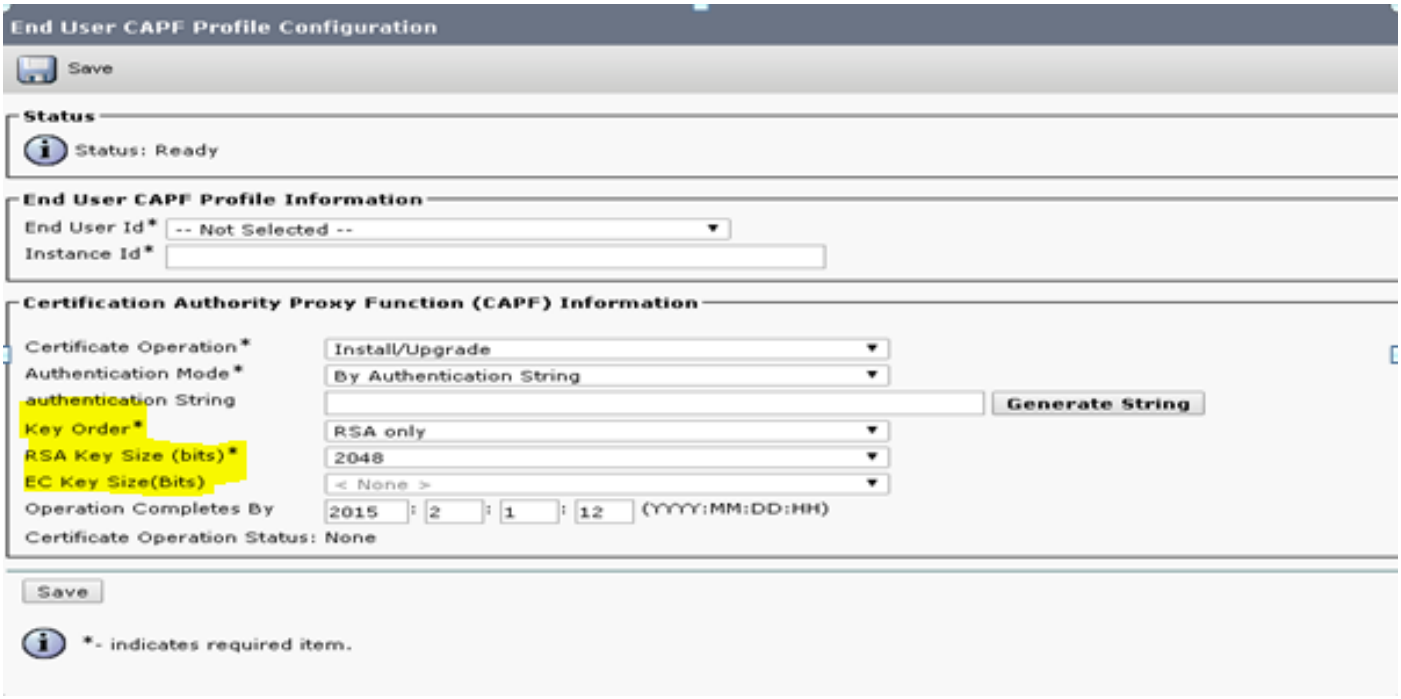


Selezionare **Sistema > Sicurezza > Profilo sicurezza telefono**

Gestione utente > Impostazioni utente > Profilo CAPF utente applicazione

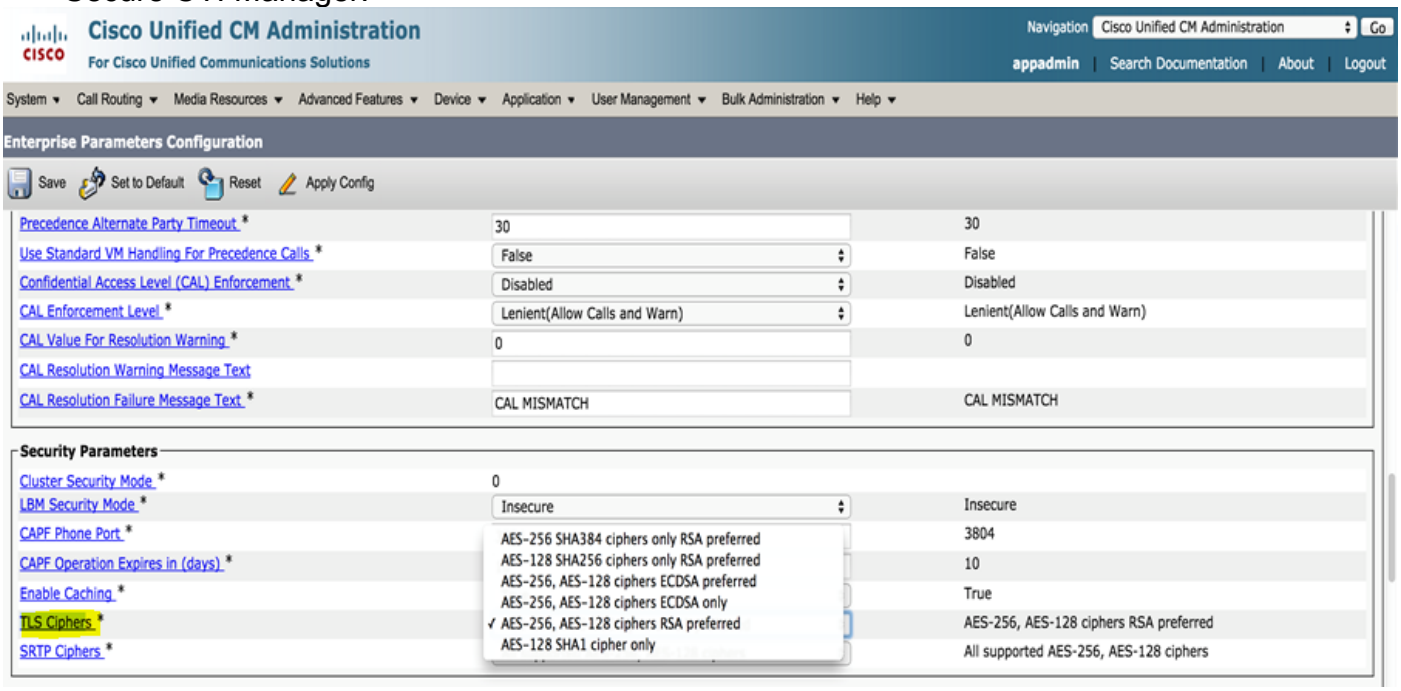


Passare a **Gestione utente > Impostazioni utente > Profilo CAPF utente finale.**



Parametri Enterprise cifratura TLS

- Il parametro Enterprise TLS Ciphers è stato aggiornato per supportare i cifrari ECDSA.
- Il parametro Enterprise TLS Ciphers imposta ora i cifrari TLS per SIP Line, SIP Trunk e Secure CTI Manager.



Supporto SIP ECDSA

- Cisco Unified Communications Manager versione 11.0 include il supporto ECDSA per linee SIP e interfacce trunk SIP.
- La connessione tra Cisco Unified Communications Manager e un telefono endpoint o un dispositivo video è una connessione di linea SIP, mentre la connessione tra due Cisco Unified Communications Manager è una connessione trunk SIP.

- Tutte le connessioni SIP supportano le cifrature ECDSA e utilizzano i certificati ECDSA.

L'interfaccia Secure SIP è stata aggiornata per supportare questi due cifrari:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Di seguito vengono riportati gli scenari in cui il SIP effettua le connessioni TLS:

- Quando il SIP funziona come server TLS Quando l'interfaccia trunk SIP di Cisco Unified Communications Manager opera come server TLS per la connessione SIP protetta in ingresso, l'interfaccia trunk SIP determina se il certificato CallManager-ECDSA esiste sul disco. Se il certificato è presente sul disco, l'interfaccia trunk SIP utilizza il certificato CallManager-ECDSA se la suite di cifratura selezionata èTLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 o TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- Quando il SIP funziona come client TLS Quando l'interfaccia trunk SIP opera come client TLS, l'interfaccia trunk SIP invia un elenco di suite di cifratura richieste al server in base al campo Cifratura TLS (che include anche l'opzione Cifre ECDSA) in Parametri Enterprise CUCM **The TLS Ciphers**. Questa configurazione determina l'elenco delle suite di cifratura client TLS e le suite di cifratura supportate in ordine di preferenza.

  Note:
  - I dispositivi che utilizzano una cifratura ECDSA per effettuare una connessione a CUCM devono avere il certificato CallManager-ECDSA nel proprio file ITL (Identity Trust List).
  - L'interfaccia trunk SIP supporta le suite di cifratura RSA TLS per le connessioni dai client che non supportano le suite di cifratura ECDSA o quando viene stabilita una connessione TLS con una versione precedente di CUCM, che non supportano ECDSA.

Supporto ECDSA Secure CTI Manager

L'interfaccia Secure CTI Manager è stata aggiornata per supportare questi quattro cifrari:

- 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

L'interfaccia Secure CTI Manager carica sia il certificato CallManager che il certificato CallManager-ECDSA. Questo consente all'interfaccia Secure CTI Manager di supportare i nuovi cifrari insieme alla cifratura RSA esistente.

Analogamente all'interfaccia SIP, l'opzione Enterprise Parameter TLS Ciphers in Cisco Unified Communications Manager viene utilizzata per configurare le cifrature TLS supportate sull'interfaccia protetta di CTI Manager.

Download del supporto HTTPS per la configurazione

- Per il download sicuro della configurazione (ad esempio, i client Jabber), Cisco Unified Communications Manager versione 11.0 è stato migliorato per supportare HTTPS, oltre alle interfacce HTTP e TFTP utilizzate nelle versioni precedenti.

- Se necessario, sia il client che il server utilizzano l'autenticazione reciproca. Tuttavia, i client registrati con le configurazioni ECDSA LSC e TFTP crittografate devono presentare le proprie LSC.
- L'interfaccia HTTPS utilizza sia i certificati CallManager che CallManager-ECDSA come certificati del server.

Note:
- Quando si aggiornano i certificati CallManager, CallManager ECDSA o Tomcat, è necessario disattivare e riattivare il servizio TFTP.
- La porta 6971 viene utilizzata per l'autenticazione dei certificati CallManager e CallManager-ECDSA, utilizzati dai telefoni.
- La porta 6972 viene utilizzata per l'autenticazione dei certificati Tomcat, utilizzati da Jabber.

Entropia

L'entropia è una misura della casualità dei dati e aiuta a determinare la soglia minima per i requisiti dei criteri comuni. Per avere una cifratura forte, è necessaria una solida fonte di entropia. Se un algoritmo di cifratura efficace, come l'ECDSA, utilizza una debole fonte di entropia, la cifratura può essere facilmente interrotta.

In Cisco Unified Communications Manager versione 11.0, la fonte di entropia per Cisco Unified Communications Manager è stata migliorata.

Entropy Monitoring Daemon è una funzione integrata che non richiede configurazione. Tuttavia, è possibile disattivarla tramite la CLI di Cisco Unified Communications Manager.

Utilizzare questi comandi CLI per controllare il servizio Entropy Monitoring Daemon:

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.

Informazioni correlate

- Guida alla sicurezza per Cisco Unified Communications Manager, versione 11.5(1)
- Documentazione e supporto tecnico – Cisco Systems