CUCM 11.0 encryptie van de volgende generatie - Ellips Curve-encryptie

Inhoud

Inleiding

Dit document beschrijft de configuratie van Next Generation Encryption (NGE) van Cisco Unified Communications Manager (CUCM) 11.0 en vervolgens om te voldoen aan de verbeterde security en prestatievereisten.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco CallManager security basisbeginselen
- Cisco CallManager-certificaatbeheer

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco CUCM 11.0, waar ECDSA-certificaten (Elliptic Curve Digital Signature Algorithm) alleen voor CallManager (CallManager-ECDSA) worden ondersteund.

Opmerking: CUCM 11.5 en ondersteunt later ook de harde-Amerikaanse-DSA-certificaten.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

Dit document kan ook worden gebruikt bij deze softwareproducten en versies die ECDSA-certificaten ondersteunen:

- Cisco Unified CM IM and Presence 11.5
- Cisco Unity Connection versie 11.5

Achtergrondinformatie

Elliptische curve cryptografie (ECC) is een benadering van cryptografie op basis van de openbare sleutel gebaseerd op de algebraïsche structuur van elliptische curves over eindige velden. Een van de belangrijkste voordelen in vergelijking met niet-ECC-cryptografie is hetzelfde beveiligingsniveau dat wordt geboden door sleutels van kleinere afmetingen.

Gemeenschappelijke criteria (CC) garanderen dat de veiligheidskenmerken correct functioneren binnen de oplossing die wordt beoordeeld. Dit wordt bereikt door middel van testen en voldoen aan uitgebreide documentatievereisten.

Het wordt door 26 landen in de hele wereld geaccepteerd en ondersteund door middel van een gemeenschappelijke erkenningsregeling (CCRA).

Cisco Unified Communications Manager release 11.0 ondersteunt ECDSA-certificaten (Elliptic Curve Digital Signature Algorithm).

Deze certificaten zijn sterker dan de op RSA gebaseerde certificaten en zijn vereist voor producten met CC-certificaten. Het commerciële Oplossingen van de overheid van de VS voor Classified Systems (CSfC) programma vereist de certificaat van CC en zo, is het in Cisco Unified Communications Manager release 11.0 en later opgenomen.

De ECDSA-certificaten zijn beschikbaar samen met de bestaande RSA-certificaten op deze gebieden:

- certificaatbeheer
- Proxy-functie (CAPF) van certificeringsinstanties
- Transport Layer Security (TLS) tracering
- Secure Session Initiation Protocol (SIP)-verbindingen
- Computer Telephony Integration (CTI) Manager
- HTTP
- entropie

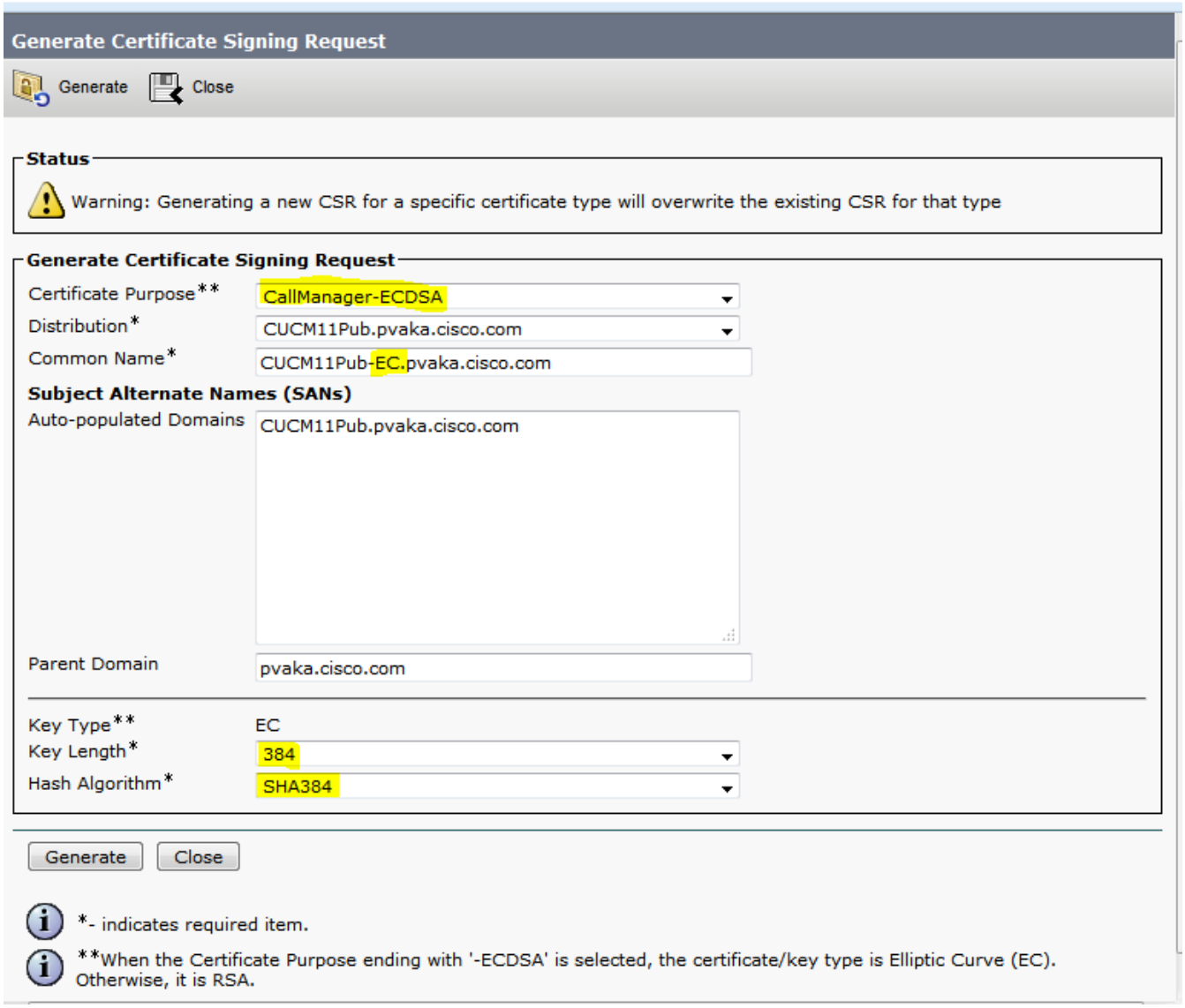
In de volgende delen wordt meer gedetailleerde informatie verstrekt over elk van deze zeven gebieden.

certificaatbeheer

Certificaten genereren met behulp van Ellips Curve-encryptie

Ondersteuning voor ECC vanaf CUCM 11.0 en hoger voor het genereren van een CallManager-certificaat met Elliptical Curve (EC) encryptie:

- De nieuwe optie **CallManager-ECDSA** is beschikbaar zoals in de afbeelding.
- Het vereist dat het gastgedeelte van de gezamenlijke naam in **EG** eindigt. Dit voorkomt het hebben van de zelfde gemeenschappelijke naam als het **CallManager** certificaat.
- In het geval van SAN-certificaat voor meerdere servers moet dit eindigen in **EG-ms**.



- Zowel de zelfondertekende certificaataanvraag als het CSR-verzoek beperken de keuze van het hashalgoritme afhankelijk van de EG-sleutelgrootte.
- Voor een EG 256-sleutelgrootte kan het hashalgoritme SHA256, SHA384 of SHA512 zijn. Voor een EC 384-sleutelgrootte kan het hashalgoritme SHA384 of SHA512 zijn. Voor een EC 521-toets is de enige optie SHA512 .
- De default key size is 384 en default hashing algoritme is SHA384, die kan worden gewijzigd. De beschikbare opties zijn gebaseerd op de gekozen sleutelgrootte.

CLI-configuratie

Er is een nieuwe certificeringseenheid met de naam **CallManager-ECDSA** toegevoegd voor de CLI-opdrachten

- set cert regen [unit] - regenereert zichzelf ondertekende certificering

```
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] - invoer CA-ondertekend certificaat

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

- set csr gen [unit] - genereert CSR-aanvraag (certificaatondertekening) voor de gespecificeerde **eenheid**

```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- set bulk export|consolidate|import tftp - Wanneer tftp de naam van de eenheid is, worden de CallManager-ECDSA certificaten met de CallManager RSA certificaten in bulkoperaties automatisch opgenomen.

CTRL- en ITL-bestanden

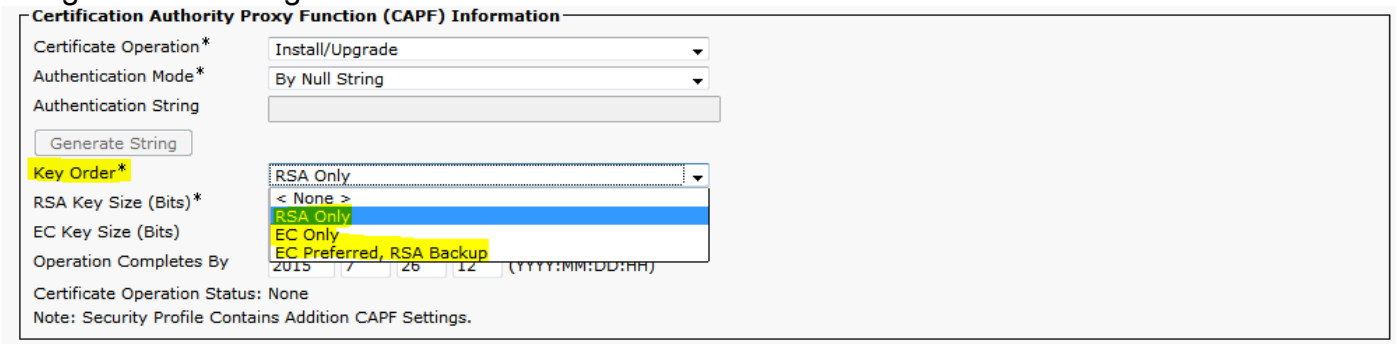
- Zowel certificaatlijst (CTL) als ITL-bestanden (Trust List) hebben **CallManager-ECDSA** aanwezig.
- Het CallManager-ECDSA certificaat heeft de functie van CCM+TFTP in zowel het ITL als het CTL bestand.
- U kunt de **show ctl** of **show itl** opdracht om deze informatie zoals in deze afbeelding te bekijken:

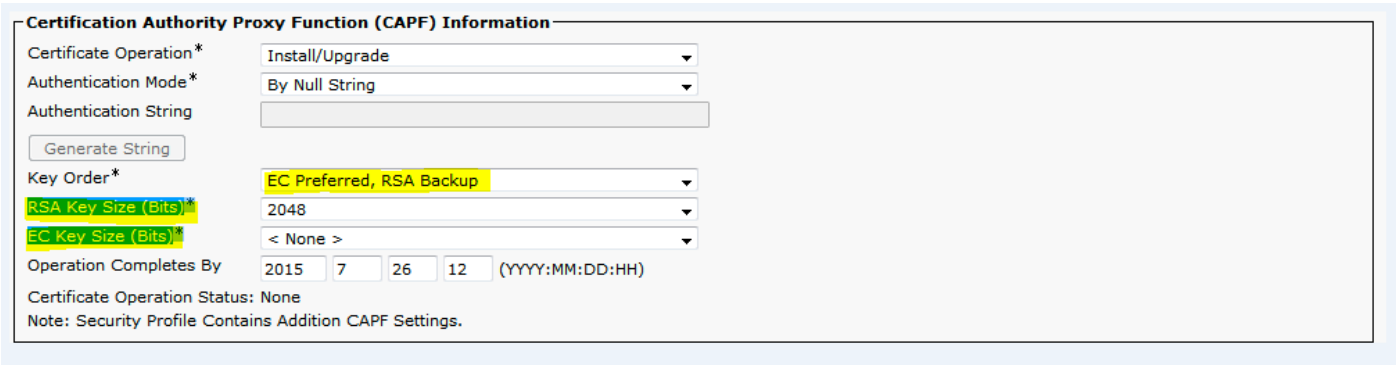
```
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1656
2       DNSNAME         2
3       SUBJECTNAME     65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME 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

- U kunt de **utils ctl update** opdracht gebruiken om het CTL bestand te genereren.

Proxy-functie van certificeringsinstantie

- De Proxy-functie (CAPF) versie 3.0 van de certificaatinstantie in CUCM 11 biedt ondersteuning voor EC-Key Sizes samen met RSA.
- De extra CAPF-opties naast de bestaande CAPF-velden zijn Sleutelvolgorde en EC-sleutelgrootte (bits).
- De bestaande optie Key Size (bits) is gewijzigd in RSA Key Size (bits).
- De sleutelorder biedt alleen ondersteuning voor RSA, EC-only en EC-preferent, RSA-back-upopties.
- De EC Key Size biedt ondersteuning voor sleutelformaten van 256, 384 en 521 bits.
- De RSA Key Size biedt ondersteuning voor 512, 1024 en 2048 bits.
- Als Key Order of RSA only is geselecteerd, kan alleen RSA Key Size worden geselecteerd. Als alleen EC is geselecteerd, kan alleen EC-grootte worden geselecteerd. Wanneer EC-voorkeur wordt gegeven, kan een RSA-back-up worden geselecteerd, zowel RSA als EC-grootte worden geselecteerd.

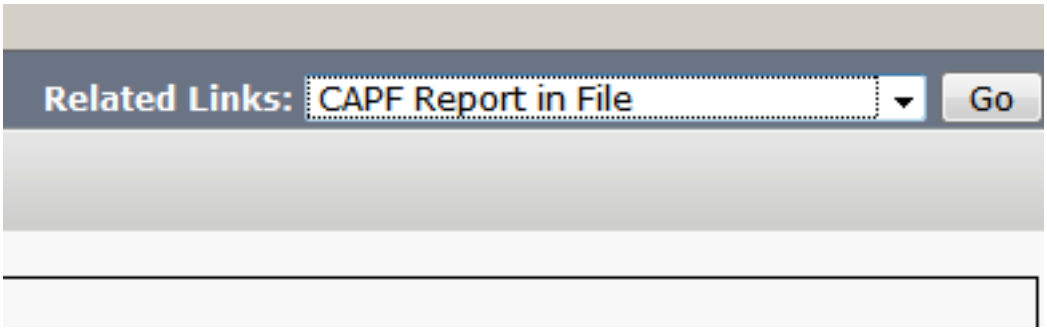




> Opmerking: Op dit moment ondersteunt geen Cisco-endpoints CAPF versie 3, dus kies dus niet de optie Alleen EC. De beheerders die ECDSA Locally Significant Certificates (LSCs) willen ondersteunen kunnen later hun apparaten echter configureren met de EC Voorkeuren RSA Backup optie. Wanneer de eindpunten beginnen om CAPF versie 3 voor ECDSA LSCs te ondersteunen, moeten de beheerders hun LSC opnieuw installeren.

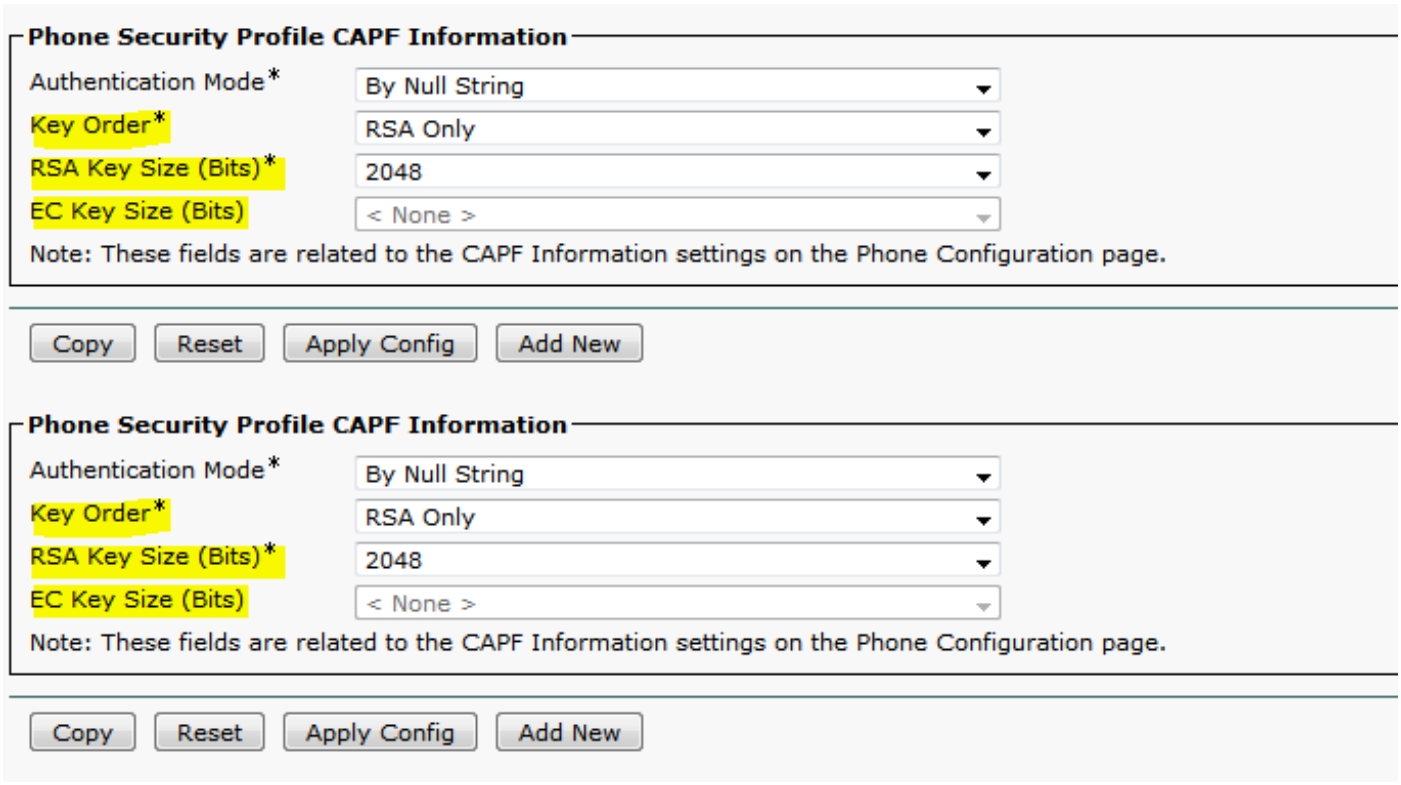
Er worden hier extra CAPF-opties voor telefoon, telefoonbeveiligingsprofiel, eindgebruiker en pagina's van de toepassingsgebruiker weergegeven:

Apparaat > Phone > Verwante links

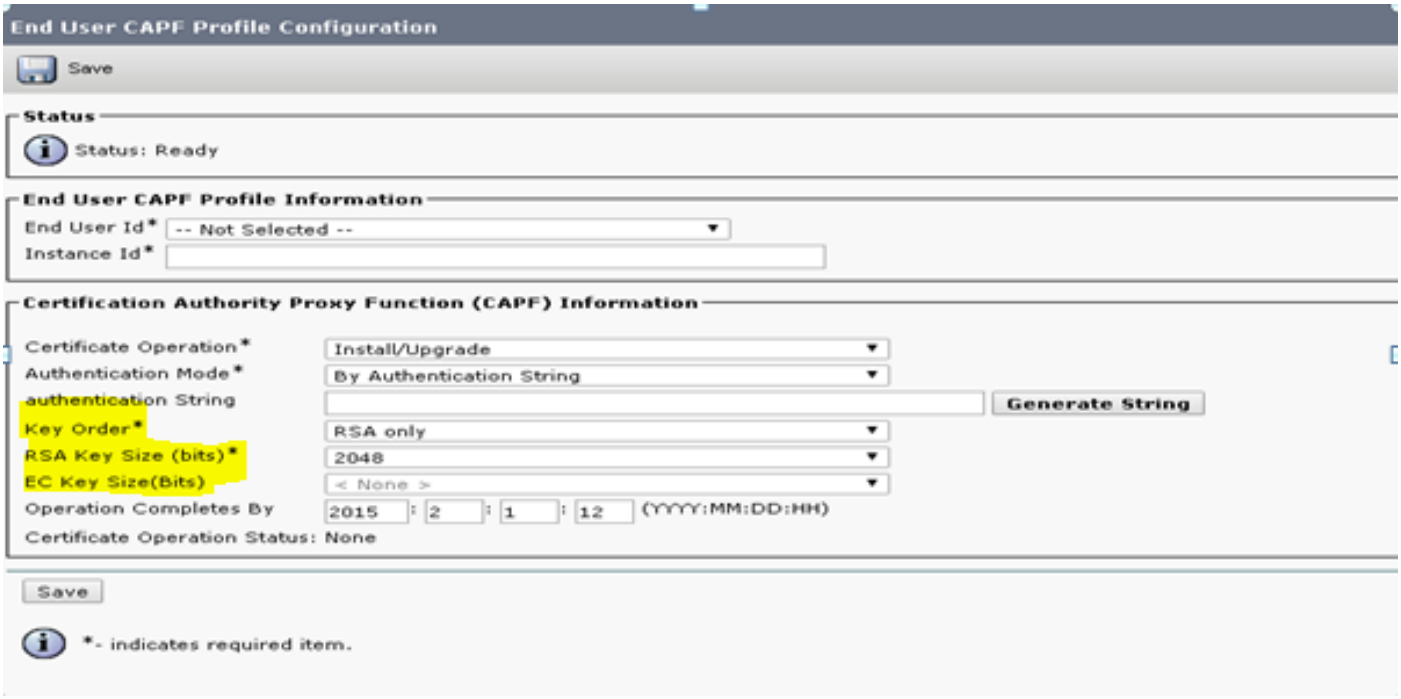


Navigatie naar **systeem > beveiliging > telefoonbeveiligingsprofiel**

Gebruikersbeheer > Gebruikersinstellingen > Toepassingsgebruikersprofiel

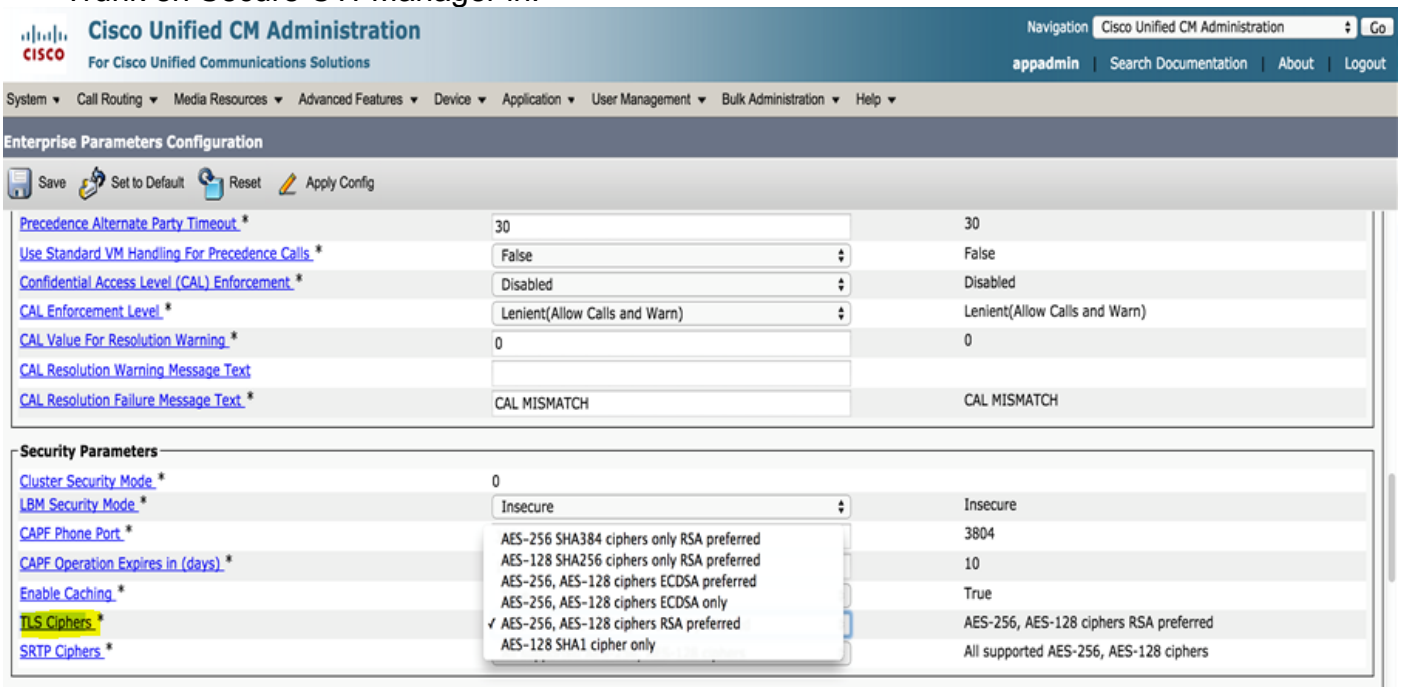


Navigeer naar **gebruikersbeheer > Gebruikersinstellingen > Eindgebruiker CAPF-profiel.**



TLS-CIFERS Enterprise-parameters

- De Enterprise Parameter TLS CIFERS is bijgewerkt om ECDSA-cifen te ondersteunen.
- De client-TLS-cifers van Enterprise Parameter stellen nu de TLS-cifers voor SIP-lijn, SIP Trunk en Secure CTI-Manager in.



Ondersteuning van SIP ECDSA

- Cisco Unified Communications Manager release 11.0 bevat ECDSA-ondersteuning voor SIP-lijnen en SIP-hoofdinterfaces.
- De verbinding tussen Cisco Unified Communications Manager en een telefoon- of videoapparaat voor een eindpunt is een SIP-lijnverbinding terwijl de verbinding tussen twee Cisco Unified Communications Manager een SIP-verbinding is.

- Alle SIP-verbindingen ondersteunen de ECDSA-cifen en gebruiken ECDSA-certificaten.

De Secure SIP-interface is bijgewerkt ter ondersteuning van deze twee cifen:

- TLS_ECDHE_ECDSA_MET_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_MET_AES_128_GCM_SHA256

Dit zijn de scenario's wanneer SIP TLS-verbindingen maakt:

- Wanneer SIP werkt als een TLS-server Wanneer de SIP hoofdinterface van Cisco Unified Communications Manager als TLS-server voor inkomende beveiligde SIP-verbinding fungeert, bepaalt de SIP hoofdinterface of het CallManager-ECDSA-certificaat op schijf bestaat. Als het certificaat op de schijf bestaat, gebruikt de interface van de SIP-stam het certificaat CallManager-ECDSA als de geselecteerde doelreeks isTLS_ECDHE_ECDSA_MET_AES_128_GCM_SHA256 of TLS_ECDHE_ECDSA_MET_AES_256_GCM_SHA384
- Wanneer SIP als een TLS-client werkt Wanneer de SIP-hoofdinterface als een TLS-client fungeert, stuurt de SIP-hoofdinterface een lijst met gevraagde algoritme-series naar de server op basis van het veld TLS-cifers (dat ook de optie ECDSA-ciphers bevat) in de CUCM Enterprise-parameters **The TLS-ciphers**. Deze configuratie bepaalt de TLS-clientsuite en de ondersteunde formaten van het algoritme in volgorde van voorkeur.

  Opmerkingen:
  - Apparaten die een ECDSA-algoritme gebruiken om een verbinding met CUCM te maken, moeten het CallManager-ECDSA-certificaat hebben in hun ITL-bestand (Identity Trust List).
  - de SIP-ondersteuning van de hoofdinterface RSA TLS-algoritme maakt gebruik van aansluitingen van klanten die geen ECDSA-algoritme ondersteunen of wanneer een TLS-verbinding is opgezet met een eerdere versie van CUCM, die ECDSA niet ondersteunen.

Ondersteuning van Secure CTI Manager ECDSA

De Secure CTI Manager-interface is bijgewerkt ter ondersteuning van deze vier cifen:

- TLS_ECDHE_RSA_MET_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_MET_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_MET_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_MET_AES_128_GCM_SHA256

De Secure CTI Manager-interface laadt zowel het CallManager- als CallManager-ECDSA-certificaat. Dit staat de Secure CTI Manager interface toe om de nieuwe ciphers samen met het bestaande RSA algoritme te steunen.

Overeenkomstig de SIP-interface wordt de optie Enterprise Parameter TLS Cphers in Cisco Unified Communications Manager gebruikt om de TLS-ciphers te configureren die worden ondersteund op de beveiligde interface van de CTI Manager.

HTTPS-ondersteuning voor configuratie

- Voor beveiligde configuratie download (bijvoorbeeld Jabber-clients) wordt Cisco Unified Communications Manager release 11.0 verbeterd om HTTPS te ondersteunen, naast de HTTP- en TFTP-interfaces die in de eerdere releases werden gebruikt.

- Indien nodig, gebruiken zowel client als server wederzijdse authenticatie. De klanten die zich bij ECDSA LSC's en versleutelde TFTP-configuraties inschrijven, dienen echter hun LSC te presenteren.
- De HTTPS interface gebruikt zowel de CallManager als de CallManager-ECDSA certificaten als de servercertificaten.

  Opmerkingen:
  - Wanneer u CallManager, CallManager ECDSA of Tomcat certificaten bijwerkt, moet u de TFTP-service deactiveren en opnieuw activeren.
  - Port 6971 wordt gebruikt voor de verificatie van de CallManager- en CallManager-ECDSA-certificaten die door telefoons worden gebruikt.
  - Port 6972 wordt gebruikt voor de echtheidscontrole van de door Jabber gebruikte Tomcat-certificaten.

entropie

Entropie is een meting van de randomiteit van gegevens en helpt bij het bepalen van de minimumdrempel voor gemeenschappelijke criteria vereisten. Om een sterke encryptie te hebben, is een robuuste bron van entropie vereist. Als een sterk encryptie-algoritme, zoals ECDSA, een zwakke bron van entropie gebruikt, kan de encryptie gemakkelijk worden gebroken.

In Cisco Unified Communications Manager release 11.0 wordt de stroombron voor Cisco Unified Communications Manager verbeterd.

Entropy Monitoring Daemon is een ingebouwde optie die geen configuratie vereist. U kunt het echter ook uitschakelen in de Cisco Unified Communications Manager CLI.

Gebruik deze CLI-opdrachten om de EtherSwitch-service te controleren:

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.

Gerelateerde informatie

- Security Guide voor Cisco Unified Communications Manager, release 11.5(1)
- Technische ondersteuning en documentatie – Cisco Systems