CUCM 11.0 Cryptage nouvelle génération - Cryptographie elliptique des courbes

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Informations générales](#)
[Gestion des certificats](#)
[Générer des certificats avec chiffrement à courbes elliptiques](#)
[Configuration CLI](#)
[Fichiers CTL et ITL](#)
[Fonction proxy d'autorité de certification](#)
[Paramètres TLS Ciphers Enterprise](#)
[Support SIP ECDSA](#)
[Prise en charge ECDSA de Secure CTI Manager](#)
[Prise en charge HTTPS pour le téléchargement de configuration](#)
[Entropie](#)
[Informations connexes](#)

Introduction

Ce document décrit la configuration du cryptage nouvelle génération (NGE) de Cisco Unified Communications Manager (CUCM) 11.0 et versions ultérieures pour répondre aux exigences de sécurité et de performances améliorées.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Notions de base sur la sécurité de Cisco CallManager
- Gestion des certificats Cisco CallManager

Components Used

Les informations de ce document sont basées sur Cisco CUCM 11.0, où les certificats ECDSA (Elliptic Curve Digital Signature Algorithm) ne sont pris en charge que pour CallManager (CallManager-ECDSA).

Note: CUCM 11.5 et versions ultérieures prend également en charge les certificats ECDSA-

cat.

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.

Produits connexes

Ce document peut également être utilisé avec ces produits logiciels et versions qui prennent en charge les certificats ECDSA :

- Messagerie instantanée et présence Cisco Unified CM 11,5
- Cisco Unity Connection 11.5

Informations générales

La cryptographie à courbe elliptique (ECC) est une approche de la cryptographie à clé publique basée sur la structure algébrique des courbes elliptiques sur des champs finis. L'un des principaux avantages par rapport à la cryptographie non ECC est le même niveau de sécurité fourni par les clés de taille plus petite.

Common Criteria (CC) garantit que les fonctionnalités de sécurité fonctionnent correctement dans la solution évaluée. Pour y parvenir, il faut tester et satisfaire à de nombreuses exigences en matière de documentation.

Elle est acceptée et appuyée par 26 pays dans le monde entier par le biais de l'Arrangement de reconnaissance des critères communs (ADRC).

Cisco Unified Communications Manager version 11.0 prend en charge les certificats ECDSA (Elliptic Curve Digital Signature Algorithm).

Ces certificats sont plus forts que les certificats basés sur RSA et sont requis pour les produits qui ont des certifications CC. Le programme Commercial Solutions for Classified Systems (CSfC) du gouvernement américain nécessite la certification CC. Il est donc inclus dans Cisco Unified Communications Manager version 11.0 et ultérieure.

Les certificats ECDSA sont disponibles avec les certificats RSA existants dans ces domaines :

- Gestion des certificats
- Fonction de proxy d'autorité de certification (CAPF)
- Suivi TLS (Transport Layer Security)
- Connexions SIP (Secure Session Initiation Protocol)
- Gestionnaire CTI (Computer Telephony Integration)
- HTTP
- Entropie

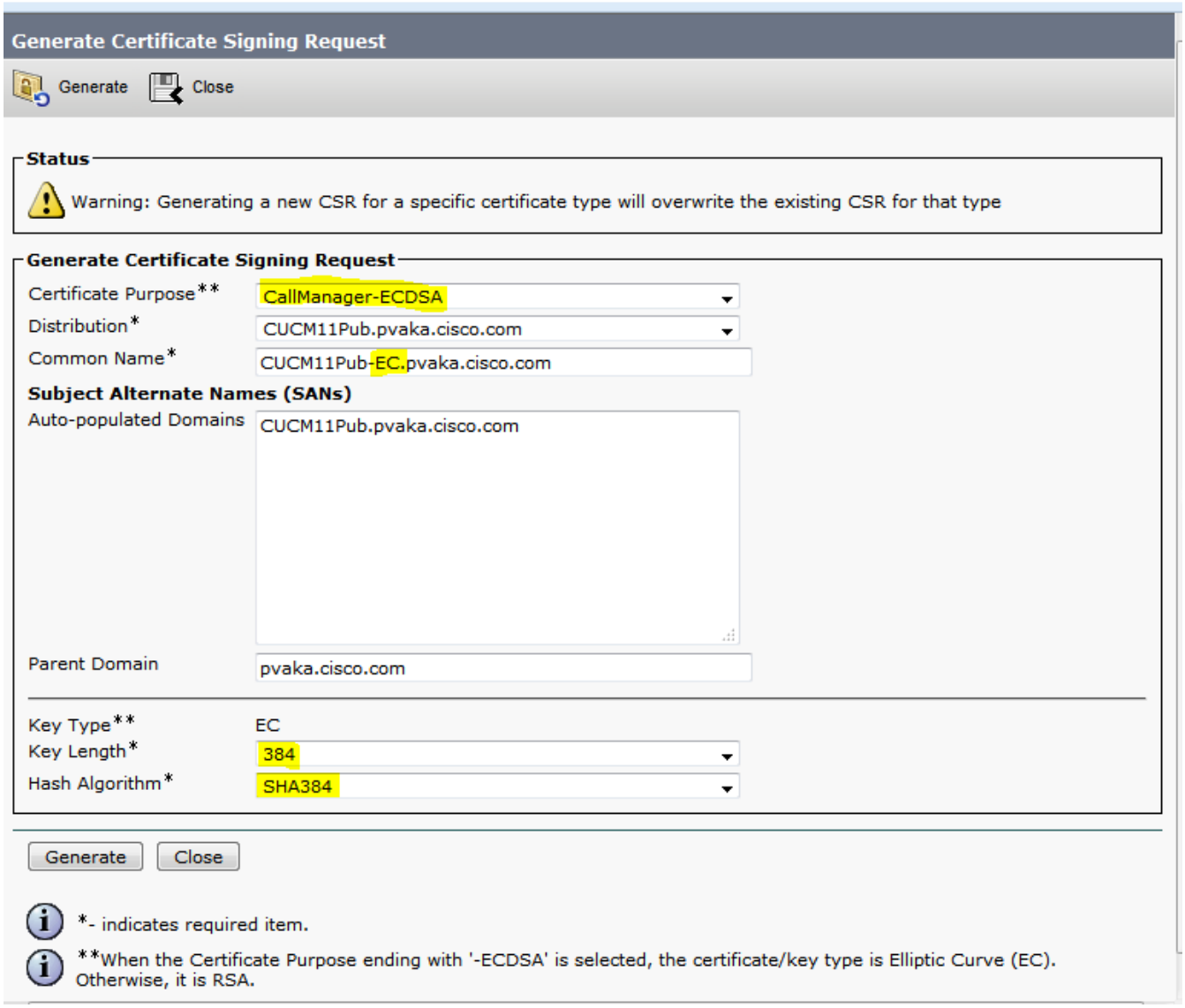
Les sections suivantes fournissent des renseignements plus détaillés sur chacun de ces sept domaines.

Gestion des certificats

Générer des certificats avec chiffrement à courbes elliptiques

Prise en charge d'ECC à partir de CUCM 11.0 et versions ultérieures pour générer un certificat CallManager avec cryptage de courbe elliptique (EC) :

- La nouvelle option **CallManager-ECDSA** est disponible comme l'illustre l'image.
- Elle nécessite que la partie hôte du nom commun se termine dans **-EC**. Cela empêche d'avoir le même nom commun que le certificat **CallManager**.
- Dans le cas d'un certificat SAN multiserveur, cette opération doit se terminer par **-EC-ms**.



- La demande de certificat auto-signée et la demande CSR limitent les choix d'algorithmes de hachage en fonction de la taille de clé EC.
- Pour une clé EC 256, l'algorithme de hachage peut être SHA256, SHA384 ou SHA512. Pour une clé EC 384, l'algorithme de hachage peut être SHA384 ou SHA512. Pour un format de clé EC 521, la seule option est SHA512.
- La taille de clé par défaut est 384 et l'algorithme de hachage par défaut est SHA384, qui peut être modifié. Les options disponibles sont basées sur la taille de clé choisie.

Configuration CLI

Une nouvelle unité de certificat nommée **CallManager-ECDSA** a été ajoutée pour les commandes CLI

- set cert regen [unit] - régénère le certificat auto-signé

```
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] - importe le certificat signé de l'AC

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

- set csr gen [unit] - génère une demande de signature de certificat (CSR) pour l'**unité** spécifiée

```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- set bulk export|consolidate|import tftp - Lorsque tftp est le nom de l'unité, les certificats CallManager-ECDSA sont automatiquement inclus avec les certificats RSA CallManager dans les opérations en bloc.

Fichiers CTL et ITL

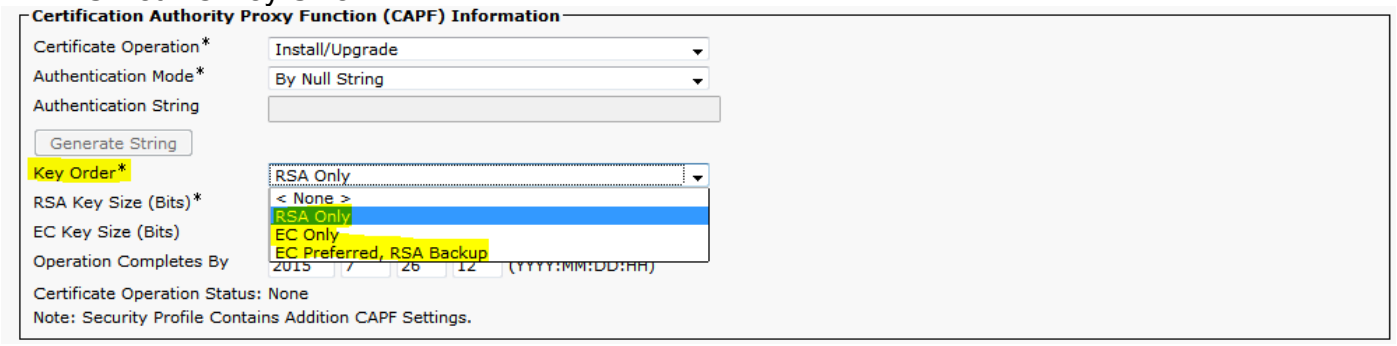
- Les fichiers CTL (Certificate Trust List) et ITL (Identity Trust List) ont **CallManager-ECDSA** présent.
- Le certificat CallManager-ECDSA a la fonction CCM+TFTP dans les fichiers ITL et CTL.
- Vous pouvez utiliser le **show ctl** ou **show itl** pour afficher ces informations, comme le montre cette image :

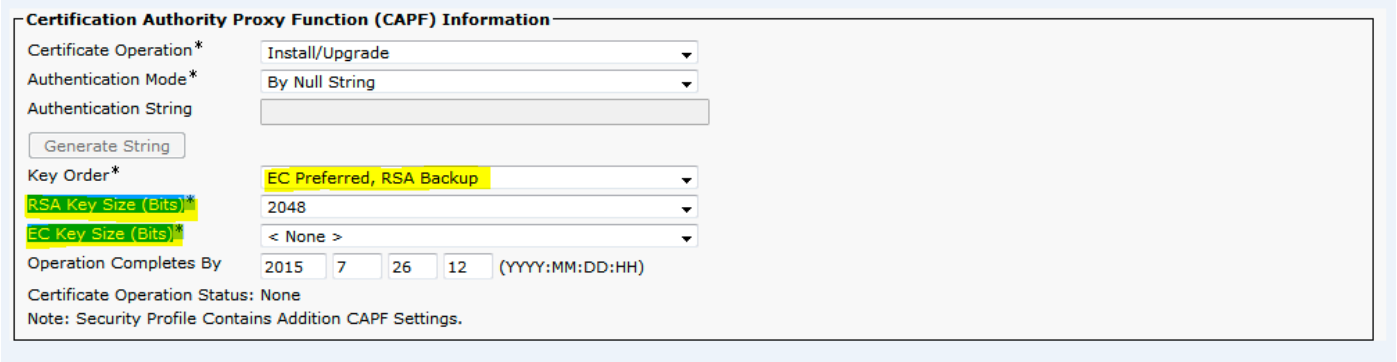
```
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1656
2       DNSNAME         2
3       SUBJECTNAME     65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME 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

- Vous pouvez utiliser la commande **utils ctl update** pour générer le fichier CTL.

Fonction proxy d'autorité de certification

- La version 3.0 de la fonction CAPF (Certificate Authority Proxy Function) de CUCM 11 prend en charge les tailles de clés EC avec RSA.
- Les options CAPF supplémentaires fournies en plus des champs CAPF existants sont Key Order et EC Key Size (bits).
- L'option Key Size (bits) existante a été remplacée par RSA Key Size (bits).
- La commande Key Order prend en charge les options de sauvegarde RSA Only, EC Only et EC Preferred.
- La taille de clé EC prend en charge les tailles de clé de 256, 384 et 521 bits.
- La taille de clé RSA prend en charge les bits 512, 1024 et 2048.
- Lorsque l'ordre des clés de RSA Only est sélectionné, seule la taille des clés RSA peut être sélectionnée. Lorsque EC uniquement est sélectionné, seule la taille de clé EC peut être sélectionnée. Lorsque la sauvegarde RSA est sélectionnée, il est possible de sélectionner RSA et EC Key Size.

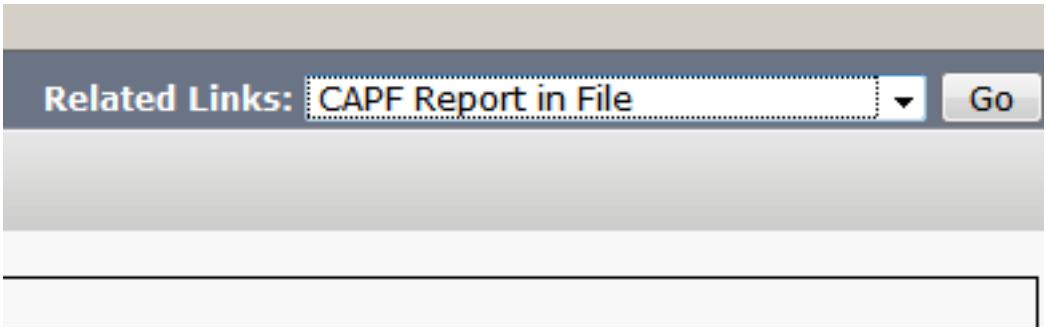




> **Note**: Actuellement, aucun terminal Cisco ne prend en charge CAPF version 3. Ne sélectionnez donc pas l'option EC Only. Cependant, les administrateurs qui souhaitent prendre en charge les certificats d'importance locale (LSC) ECDSA ultérieurement peuvent configurer leurs périphériques avec l'option de sauvegarde RSA privilégiée EC. Lorsque les terminaux commencent à prendre en charge CAPF version 3 pour les LSC ECDSA, les administrateurs doivent réinstaller leur LSC.

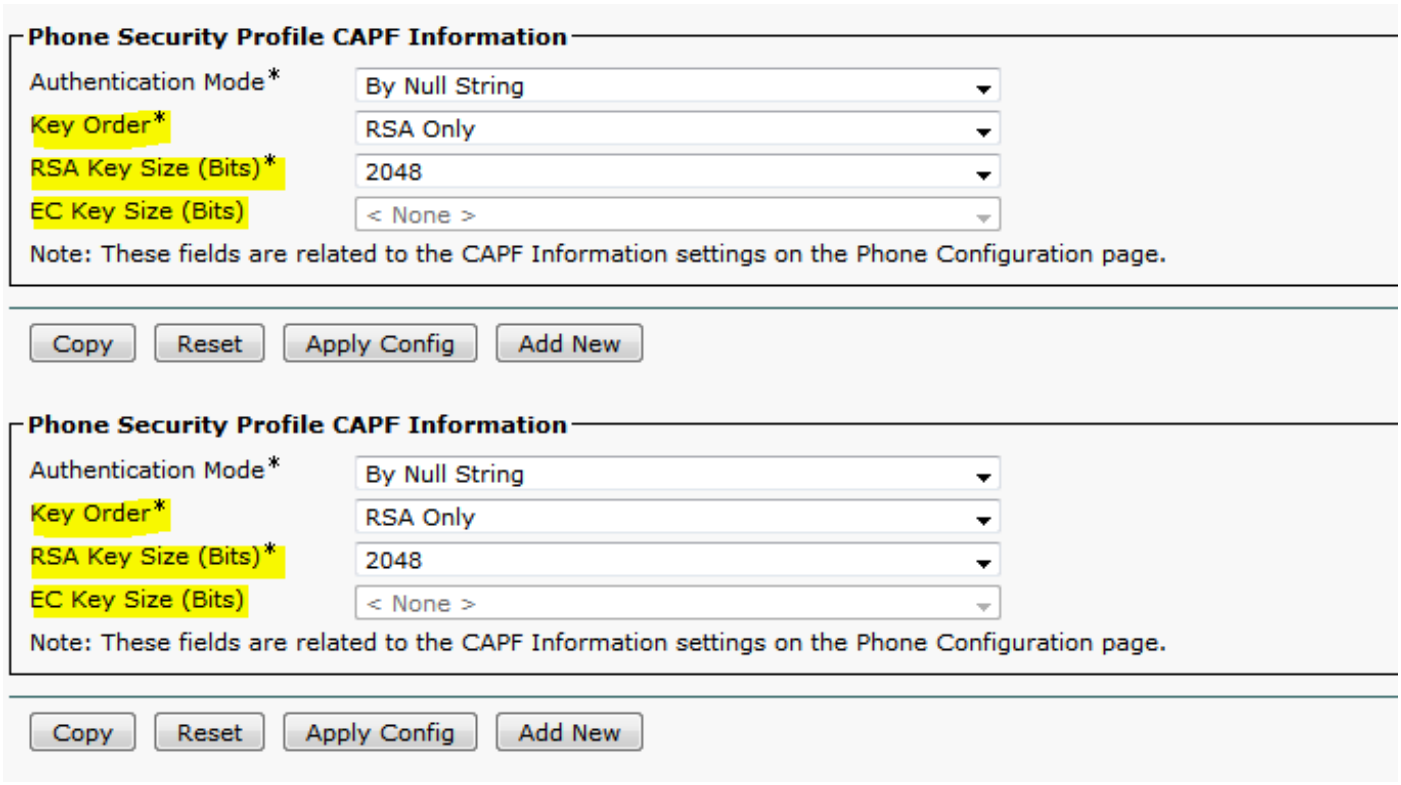
Les options CAPF supplémentaires pour les pages Phone, Phone Security Profile, End User et Application User sont présentées ici :

Périphérique > Téléphone > Liens associés

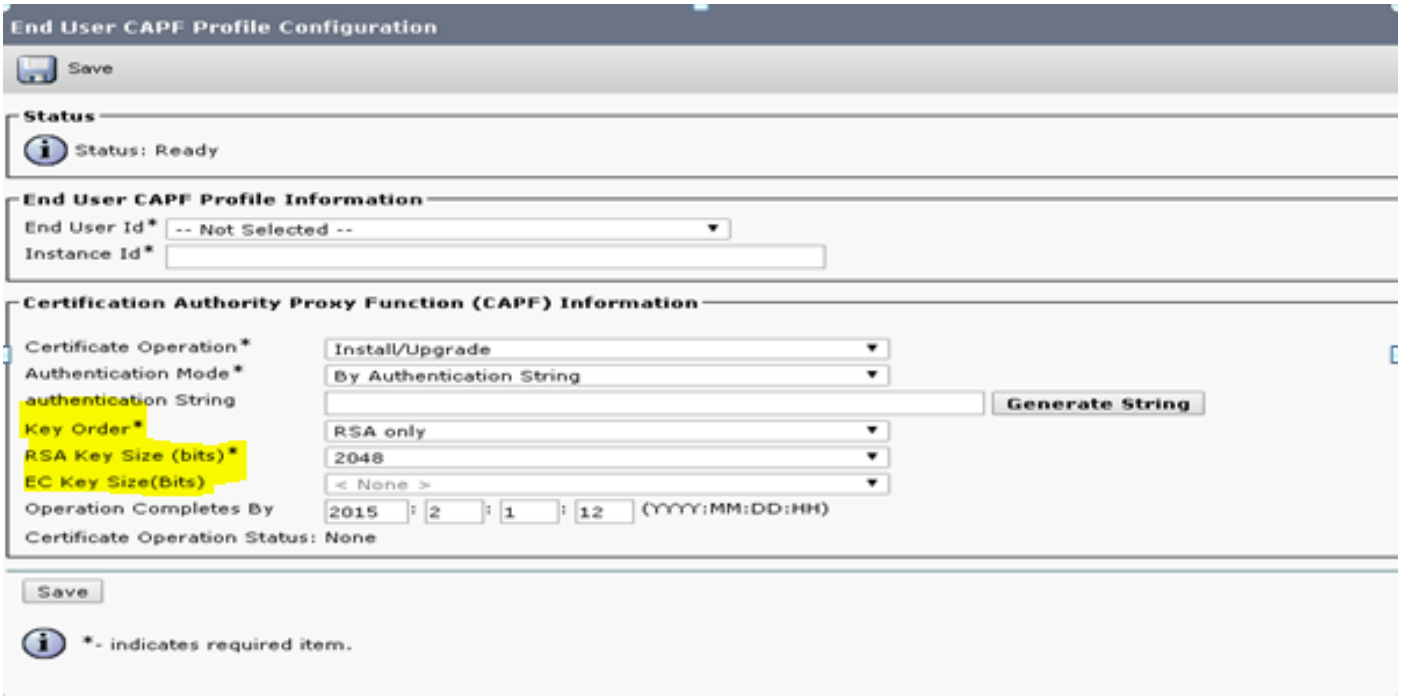


Accédez à **Système > Sécurité > Profil de sécurité du téléphone**

Gestion des utilisateurs > Paramètres utilisateur > Profil CAPF utilisateur d'application

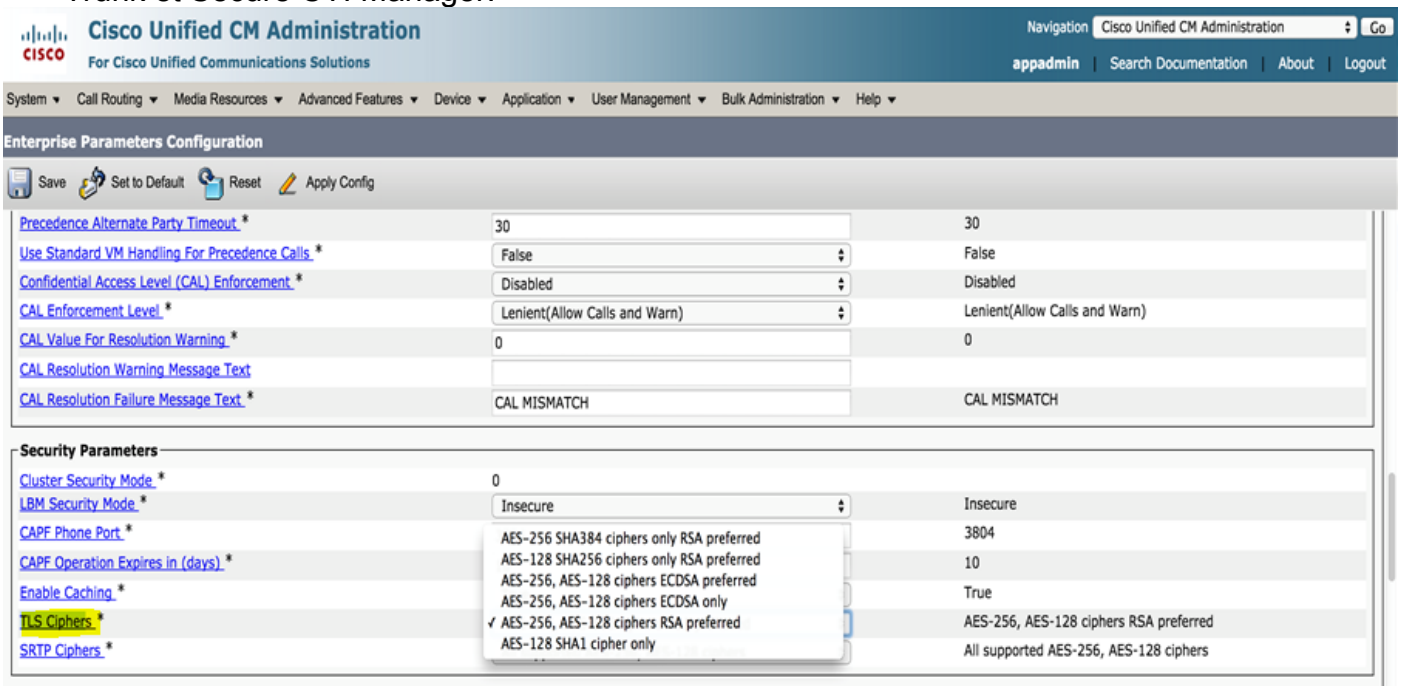


Accédez à **User Management > User Settings > End User CAPF Profile.**



Paramètres TLS Ciphers Enterprise

- Le paramètre d'entreprise TLS Ciphers a été mis à jour pour prendre en charge les chiffrements ECDSA.
- Le paramètre d'entreprise TLS Ciphers définit désormais les TLS Ciphers pour SIP Line, SIP Trunk et Secure CTI Manager.



Support SIP ECDSA

- Cisco Unified Communications Manager version 11.0 inclut la prise en charge de l'ECDSA pour les lignes SIP et les interfaces de liaison SIP.
- La connexion entre Cisco Unified Communications Manager et un téléphone ou un périphérique vidéo d'un point d'extrémité est une connexion de ligne SIP tandis que la

connexion entre deux Cisco Unified Communications Manager est une connexion de liaison SIP.
- Toutes les connexions SIP prennent en charge les chiffrements ECDSA et utilisent des certificats ECDSA.

L'interface SIP sécurisée a été mise à jour pour prendre en charge ces deux chiffrement :

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Voici les scénarios dans lesquels SIP établit des connexions TLS :

- Lorsque SIP agit en tant que serveur TLS Lorsque l'interface de liaison SIP de Cisco Unified Communications Manager agit en tant que serveur TLS pour la connexion SIP sécurisée entrante, l'interface de liaison SIP détermine si le certificat CallManager-ECDSA existe sur le disque. Si le certificat existe sur le disque, l'interface de liaison SIP utilise le certificat CallManager-ECDSA si la suite de chiffrement sélectionnée estTLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ou TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- Lorsque SIP agit en tant que client TLS Lorsque l'interface de liaison SIP agit en tant que client TLS, l'interface de liaison SIP envoie au serveur une liste des suites de chiffrement demandées en fonction du champ Chiffres TLS (qui inclut également l'option Chiffres ECDSA) dans les paramètres d'entreprise CUCM **Chiffres TLS**. Cette configuration détermine la liste des suites de chiffrement client TLS et les suites de chiffrement prises en charge par ordre de préférence.

  Remarques :
  - Les périphériques qui utilisent un chiffrement ECDSA pour établir une connexion à CUCM doivent avoir le certificat CallManager-ECDSA dans leur fichier de liste de confiance d'identité (ITL).
  - L'interface de liaison SIP prend en charge les suites de chiffrement RSA TLS pour les connexions de clients qui ne prennent pas en charge les suites de chiffrement ECDSA ou lorsqu'une connexion TLS est établie avec une version antérieure de CUCM, qui ne prennent pas en charge ECDSA.

Prise en charge ECDSA de Secure CTI Manager

L'interface Secure CTI Manager a été mise à jour pour prendre en charge ces quatre chiffrement :

- 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'interface Secure CTI Manager charge le certificat CallManager et CallManager-ECDSA. Cela permet à l'interface Secure CTI Manager de prendre en charge les nouveaux chiffrements ainsi que le chiffrement RSA existant.

Tout comme l'interface SIP, l'option Chiffres TLS de paramètre d'entreprise dans Cisco Unified Communications Manager est utilisée pour configurer les Chiffres TLS pris en charge sur l'interface sécurisée de CTI Manager.

Prise en charge HTTPS pour le téléchargement de configuration

- Pour le téléchargement sécurisé de la configuration (par exemple, les clients Jabber), Cisco Unified Communications Manager version 11.0 est amélioré pour prendre en charge HTTPS en plus des interfaces HTTP et TFTP utilisées dans les versions précédentes.
- Si nécessaire, le client et le serveur utilisent l'authentification mutuelle. Cependant, les clients inscrits avec des LSC ECDSA et des configurations TFTP cryptées sont requis pour présenter leur LSC.
- L'interface HTTPS utilise les certificats CallManager et CallManager-ECDSA comme certificats de serveur.

Remarques :
- Lorsque vous mettez à jour les certificats CallManager, CallManager ECDSA ou Tomcat, vous devez désactiver et réactiver le service TFTP.
- Le port 6971 est utilisé pour l'authentification des certificats CallManager et CallManager-ECDSA, utilisés par les téléphones.
- Le port 6972 est utilisé pour l'authentification des certificats Tomcat, utilisés par Jabber.

Entropie

L'entropie est une mesure du caractère aléatoire des données et aide à déterminer le seuil minimal pour les critères communs. Pour disposer d'un chiffrement fort, une source robuste d'entropie est requise. Si un algorithme de chiffrement fort, tel que ECDSA, utilise une source faible d'entropie, le chiffrement peut facilement être rompu.

Dans Cisco Unified Communications Manager version 11.0, la source d'entropie de Cisco Unified Communications Manager est améliorée.

Le démon de surveillance entrante est une fonctionnalité intégrée qui ne nécessite aucune configuration. Cependant, vous pouvez l'éteindre via l'interface de ligne de commande de Cisco Unified Communications Manager.

Utilisez ces commandes CLI afin de contrôler le service de démon de surveillance entrante :

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.

Informations connexes

- Guide de sécurité pour Cisco Unified Communications Manager, version 11.5(1)
- Support et documentation techniques - Cisco Systems