Cryptage de nouvelle génération CUCM 11.0 - Chiffrement elliptique de curve

Contenu

Introduction

Ce document décrit l'introduction, configuration du cryptage de Next_Generation (NGE) de Cisco Unified Communications Manager (CUCM) 11.0 et plus tard, pour répondre aux exigences de sécurité optimisée et de marche

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Fondements de Sécurité de Cisco Call manager
- Gestion de certificat de Cisco Call manager

[Composants utilisés](#)

Les informations dans ce document sont basées sur Cisco CUCM 11.0, où des Certificats d'edcsa sont seulement pris en charge pour le CallManager (le CallManager-EDCSA)

> Remarque: Les supports Tomcat-EDCSA CUCM 11.5 en avant délivre un certificat aussi bien

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

Ce document peut également être utilisé avec ces logiciels et versions qui prennent en charge des Certificats EDCSA :

- Cisco IM et présence 11.5
- Cisco Unity Connection 11.5

Informations générales

Le chiffrement elliptique de curve (ECC) est une approche à la cryptographie à clé publique basée sur la structure algébrique des curves elliptiques au-dessus des champs finis. Un des principaux bénéfices en comparaison du chiffrement non-ECC est le même niveau de sécurité fourni par des clés de plus de petite taille.

Les critères communs fournit l'assurance que les fonctionnalités de sécurité fonctionnent correctement dans la solution étant évaluée. Ceci est réalisé par des conditions requises étendues de documentation de test et de téléconférence.

Reçu et pris en charge par 26 pays dans le monde entier par l'intermédiaire de l'arrangement de reconnaissance commun de critères (CCRA)

La version 11.0 de Cisco Unified Communications Manager prend en charge les Certificats elliptiques de l'algorithme de signature numérique de curve (ECDSA).

Ces Certificats sont plus forts que les Certificats basés sur RSA et sont exigés pour les Produits qui ont des certifications communes des critères (cc). Les solutions commerciales de gouvernement des USA pour le programme classifié de systèmes (CSfC) exige la certification cc et ainsi, elle est incluse dans la version 11.0 de Cisco Unified Communications Manager en avant.

Les Certificats ECDSA sont disponibles avec les Certificats existants RSA dans ces zones :

- Gestion de certificat
- Fonction de proxy d'autorité de certification (CAPF)
- Suivi de Transport Layer Security (TLS)
- Sécurisez les connexions de SIP

- Gestionnaire du couplage de la téléphonie et de l'informatique (CTI)
- HTTP et
- Entropie

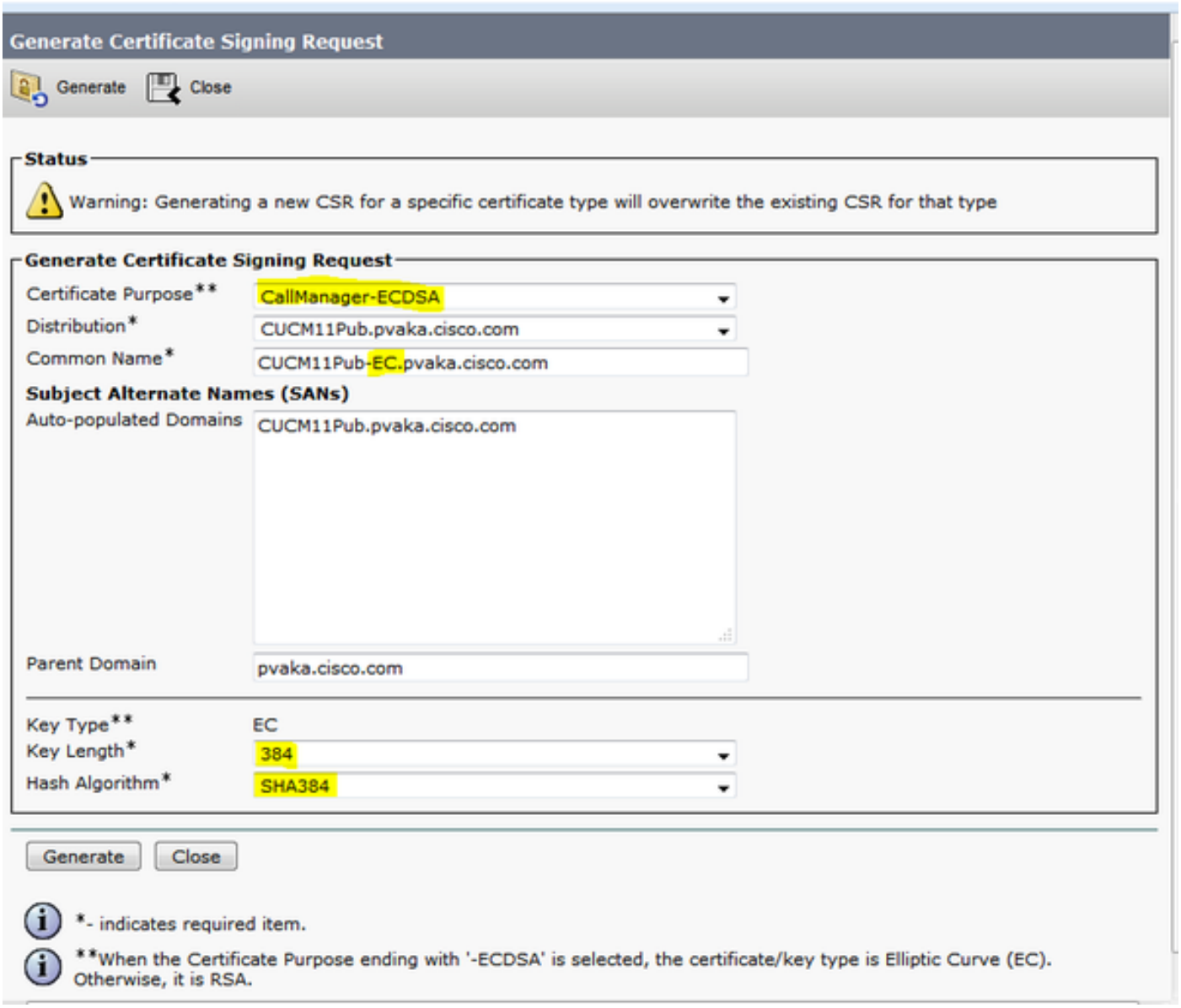
Les sections suivantes fournissent plus d'informations détaillées sur chacune des 7 zones ci-dessus.

Gestion de certificat

Générer des Certificats avec le cryptage EC

Soutien d'ECC de CUCM 11.0 en avant pour générer le certificat de CallManager avec le cryptage EC

- Nouveau **CallManager-ECDSA d'**option disponible suivant les indications de l'image.
- Exige de la partie hôte du nom commun de finir dedans **? L'EC**, pour empêcher avoir le même nom commun que le certificat de **CallManager**.
- En cas de certificat multi du serveur SAN, ceci doit finir dedans **? EC-ms**.



- La les deux la demande auto-signée de certificat et le CSR demandent la limite les choix d'algorithme de hachage selon la taille de clé EC.
- Pour une taille de clé EC 256 l'algorithme de hachage peut être SHA256, SHA384 ou SHA512. Pour une taille de clé EC 384 l'algorithme de hachage peut être SHA384 ou SHA512. Pour une taille de clé EC 521 la seule option est SHA512.
- La taille de clé par défaut est 384 et l'algorithme de hachage de par défaut est SHA384, utilisant lequel peut être changé relâchent vers le bas. 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

- placez le CERT REGEN [unité] ? certificat auto-signé par régénérés

```
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)?
```

- placez l'importation de CERT possèdent|confiance [unité] ? certificat signé des importations CA

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

- placez la génération csr [unité] ? génère le request(CSR) de signature de certificat pour l'unité spécifiée

```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- placez l'exportation en vrac|consolidez|tftp d'importation ? Quand le tftp est le nom d'unité, les Certificats de CallManager-ECDSA obtiennent automatique-inclus avec des Certificats du CallManager RSA en vrac des exécutions.

Fichiers CTL et ITL :

- Les fichiers CTL et ITL ont le présent de **CallManager-ECDSA**.
- Le certificat de CallManager-ECDSA ont la fonction de CCM+TFTP dans l'ITL et le fichier

CTL.

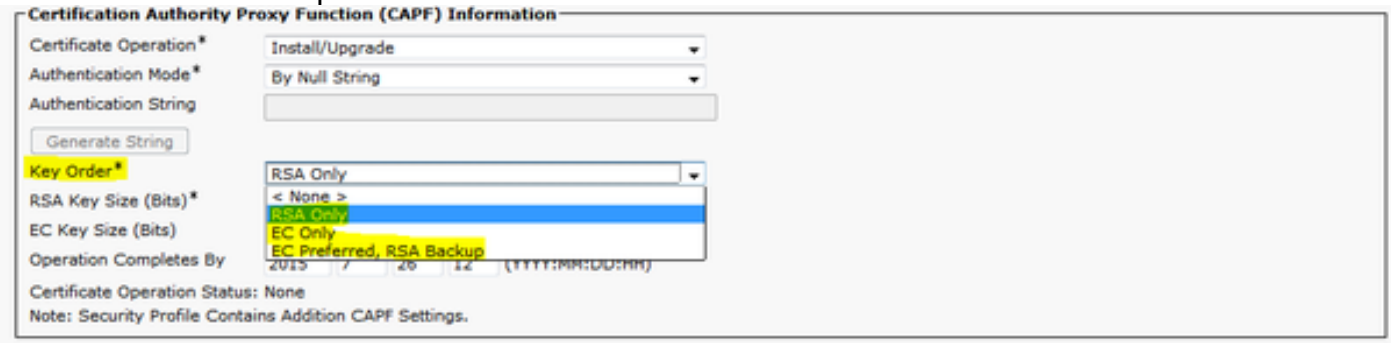
- Vous pouvez utiliser le **ctl d'exposition** ou **afficher des** commandes **ITL** de visualiser ces informations suivant les indications de l'image :

```
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 employer la **mise à jour de ctl d'utils** pour générer le fichier CTL.

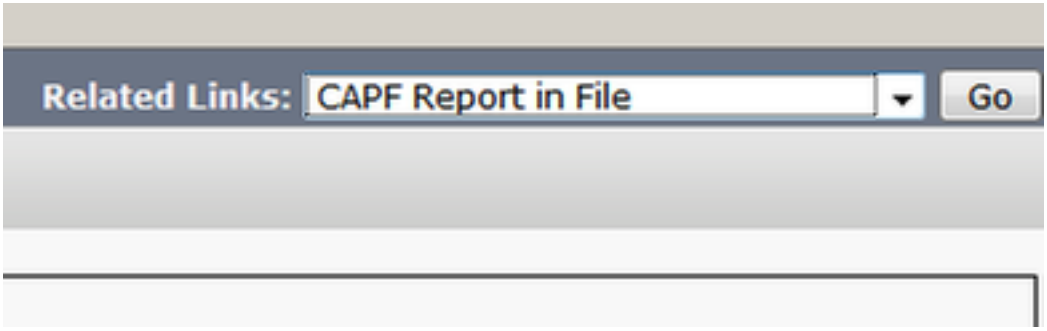
Fonction de proxy d'autorité de certification (CAPF)

- La version 3.0 CAPF dans CUCM 11 fournit le support pour des tailles de clé EC avec la RSA.
- Les options supplémentaires CAPF fournies en plus des champs existants CAPF sont la commande principale et la taille de clé EC (bits).
- L'option existante de taille de clé (bits) a été changée à la taille de clé RSA (bits).
- La commande principale fournit le support pour la RSA seulement, l'EC seulement et l'EC préférée, des options de sauvegarde RSA.
- La taille de clé EC fournit le support pour des tailles de clé de 256, 384 et 521 bits.
- La taille de clé RSA fournit le support pour 512, 1024 et 2048 bits
- Si principale la commande de la RSA seulement est sélectionnée, seulement la taille de clé RSA peut être sélectionnée. Quand l'EC seulement est sélectionnée, seulement la taille de clé EC peut être sélectionnée. Quand l'EC préférée, sauvegarde RSA est sélectionnée, la taille de clé RSA et EC peut être sélectionnée.



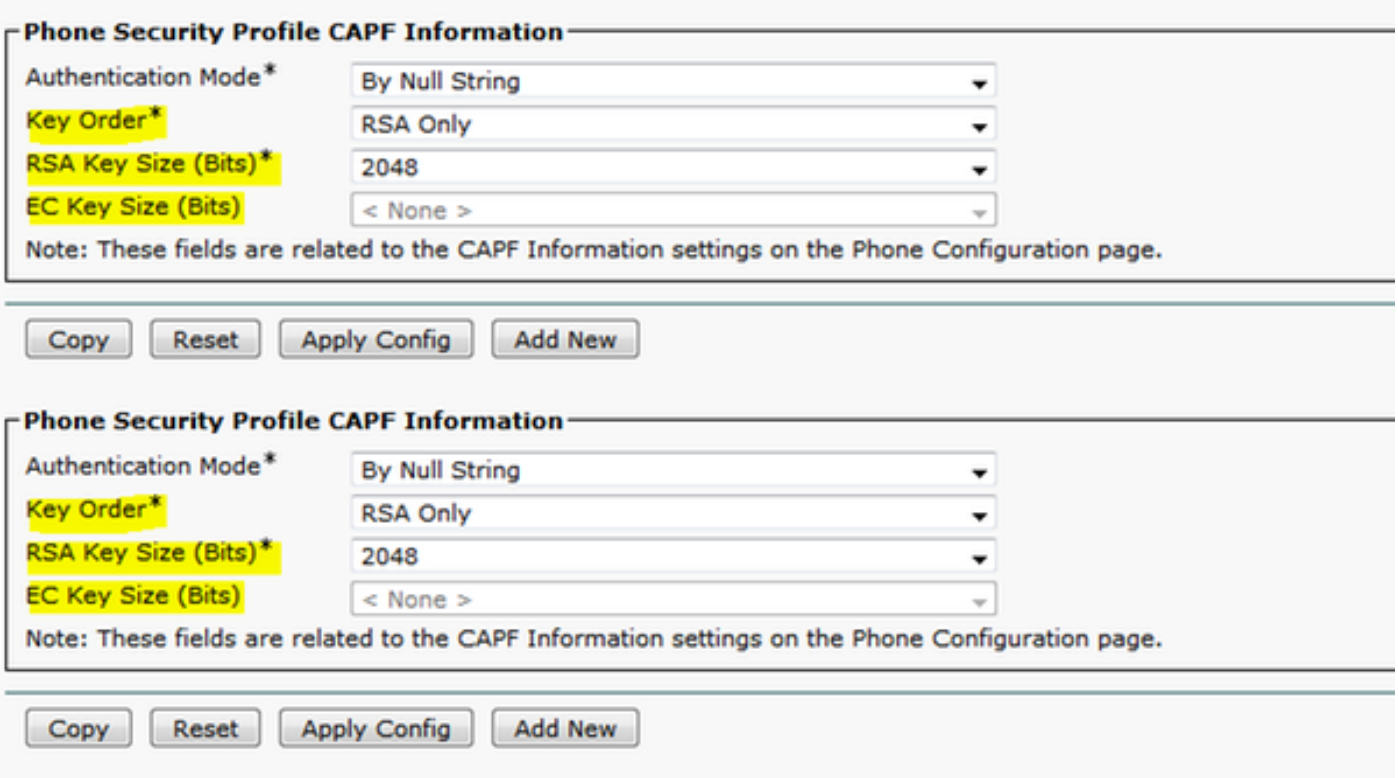
Options supplémentaires CAPF pour le profil de téléphone, de degré de sécurité de téléphone, l'utilisateur final et les pages utilisateur d'application

Device > Phone > liens connexes

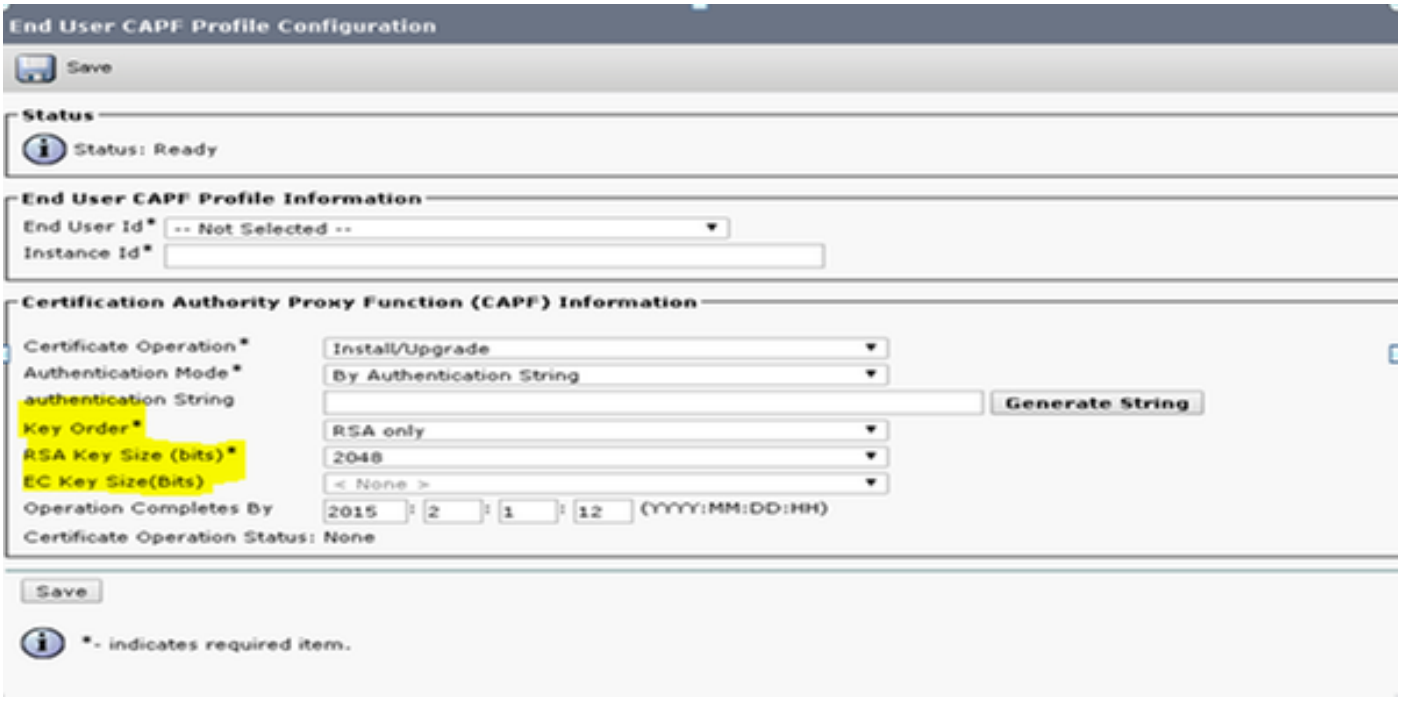


Naviguez **profil** vers de **système > de Sécurité > de téléphone Sécurité**

Gestion des utilisateurs > paramètres utilisateurs > profil de l'utilisateur CAPF d'application

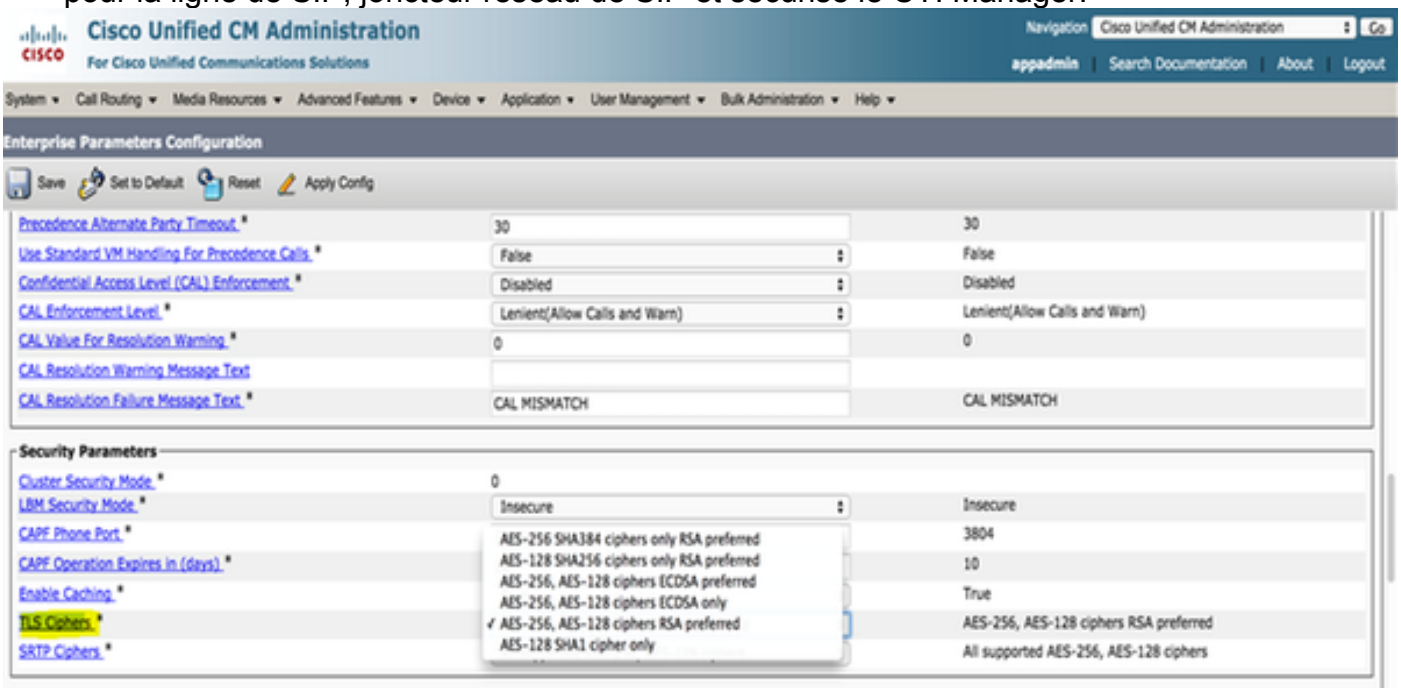


Navigaet à la **gestion des utilisateurs > aux paramètres utilisateurs > au profil de l'utilisateur final CAPF.**



Paramètres d'entreprise de chiffrements de TLS

- Les chiffrements de TLS de paramètre d'entreprise a été mis à jour pour prendre en charge des chiffrements ECDSA.
- Les chiffrements de TLS de paramètre d'entreprise maintenant place les chiffrements de TLS pour la ligne de SIP, joncteur réseau de SIP et sécurise le CTI Manager.



Support du SIP ECDSA

- La version 11.0 de Cisco Unified Communications Manager inclut le soutien ECDSA des interfaces de lignes de SIP et de joncteur réseau de SIP.
- La connexion entre Cisco Unified Communications Manager et un point final téléphonent ou le périphérique vidéo est une ligne connexion de SIP tandis que la connexion entre deux Cisco

Unified Communications Managers est une connexion de jonction de SIP.
- Toutes les connexions de SIP prennent en charge les chiffrements ECDSA et les Certificats de l'utilisation ECDSA.

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

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Ce sont les scénarios quand le SIP établit des rapports de TLS (de Transport Layer Security) :

- Quand le SIP agit en tant que serveur de TLS

Quand l'interface de joncteur réseau de SIP de Cisco Unified Communications Manager agit en tant que serveur de TLS pour la connexion sécurisée entrante de SIP, l'interface de joncteur réseau de SIP détermine si le certificat de CallManager-ECDSA existe sur le disque. Si le certificat existe sur le disque, l'interface de joncteur réseau de SIP utilise le certificat de CallManager-ECDSA si la suite sélectionnée de chiffrement est

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ou
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

- Quand le SIP agit en tant que client de TLS

Quand l'interface de joncteur réseau de SIP agit en tant que client de TLS, l'interface de joncteur réseau de SIP envoie une liste de suites demandées de chiffrement au serveur basé sur le champ de chiffrements de TLS (qui inclut également l'ECDSA chiffre l'option) dans les paramètres d'entreprise CUCM les **chiffrements de TLS**. Cette configuration détermine la liste de suite de chiffrement de client de TLS et les suites prises en charge de chiffrement par ordre préférence.

> Remarque: 1. Les périphériques qui emploient un chiffrement ECDSA pour établir un rapport à CUCM doivent avoir le certificat de CallManager-ECDSA dans leur fichier de la liste de confiance d'identité (ITL).

> Remarque: 2. Le TLS du support RSA d'interface de joncteur réseau de SIP chiffre des suites pour des connexions des clients qui ne prennent en charge pas des suites de chiffrement ECDSA ou quand une connexion de TLS est établie avec une version antérieure de CUCM, cela ne prend en charge pas ECDSA.

Support sécurisé du CTI Manager ECDSA

L'interface sécurisée de CTI Manager a été mise à jour pour prendre en charge ces quatre chiffrements :

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

- Le chargement sécurisé d'interface de CTI Manager le certificat de CallManager et de CallManager-ECDSA. Ceci permet à l'interface sécurisée de CTI Manager pour prendre en charge les nouveaux chiffrements avec le chiffrement existant RSA.
- Semblable à l'interface de SIP, l'option de chiffrements de TLS de paramètre d'entreprise dans Cisco Unified Communications Manager est utilisée pour configurer les chiffrements de TLS qui sont pris en charge sur l'interface sécurisée de CTI Manager.

Soutien HTTPS de téléchargement de configuration

- Pour le téléchargement sécurisé de configuration (par exemple clients de Jabber), la version 11.0 de Cisco Unified Communications Manager est améliorée pour prendre en charge HTTPS en plus des interfaces de HTTP et TFTP qui ont été utilisées dans les versions antérieures.
- S'il y a lieu, les deux authentification mutuelle d'utilisation de client et serveur. Cependant, les clients qui sont inscrits avec ECDSA LSC et configurations chiffrées TFTP sont requis de présenter leur LSC.
- L'interface HTTPS utilise le CallManager et les Certificats de CallManager-ECDSA comme Certificats de serveur.

  Remarque: 1. Quand vous mettez à jour des Certificats de CallManager, de CallManager ECDSA, ou de Tomcat, vous devez désactiver et réactiver le service TFTP.

  Remarque: 2. Le port 6971 est utilisé pour l'authentification des Certificats de CallManager et de CallManager-ECDSA, utilisée par des téléphones.

  Remarque: 3. Le port 6972 est utilisé pour l'authentification des Certificats de Tomcat, utilisée par Jabber.

Entropie

L'entropie est une mesure de caractère aléatoire des données et aide en déterminant le seuil minimum pour des conditions requises communes de critères. Pour avoir le cryptage fort, une source robuste d'entropie est exigée. Si un algorithme de chiffrement fort, tel qu'ECDSA, utilise une source faible d'entropie, le cryptage peut être facilement cassé.

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

Le démon de surveillance d'entropie est une fonctionnalité intégrée qui n'exige pas la configuration. Cependant, vous pouvez l'arrêter par Cisco Unified Communications Manager CLI.

Utilisez les commandes suivantes CLI de contrôler le service de démon de surveillance d'entropie :

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

- 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
- Support et documentation techniques - Cisco Systems