Cifrado de la última generación CUCM 11.0 - Criptografía elíptica de la curva

Contenido

Introducción

Este documento describe la introducción, configuración del cifrado de la última generación (NGE) del administrador de las Comunicaciones unificadas de Cisco (CUCM) 11.0 y posterior, para cumplir la seguridad mejorada y los requisitos de rendimiento

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Fundamentos de la Seguridad del Cisco Call Manager
- Administración de certificados del Cisco Call Manager

Componentes Utilizados

La información en este documento se basa en Cisco CUCM 11.0, donde los Certificados EDCSA se soportan solamente para el CallManager (el CallManager-EDCSA)

> **Note**: Los soportes Tomcat-EDCSA CUCM 11.5 hacia adelante certifican también

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Este documento se puede también utilizar con estos productos de software y versiones que soporten los Certificados EDCSA:

- Cisco unificó CM IM y la presencia 11.5
- Cisco Unity Connection 11.5

Antecedentes

La criptografía elíptica de la curva (ECC) es un acercamiento al Cifrado de clave pública basado en la estructura algebraica de las curvas elípticas sobre los campos finitos. Uno de los beneficios principales en comparación con la criptografía NON-ECC es el mismo nivel de seguridad proporcionado por las claves de más tamaño pequeño.

Los criterios comunes ofrecen la garantía que las funciones de seguridad actúan correctamente dentro de la solución que es evaluada. Esto se alcanza con la prueba y los requisitos extensos de la documentación de la reunión.

Validado y soportado por 26 países por todo el mundo vía el arreglo de reconocimiento común de los criterios (CCRA)

La versión 11.0 del administrador de las Comunicaciones unificadas de Cisco soporta los Certificados elípticos del Digital Signature Algorithm de la curva (ECDSA).

Estos Certificados son más fuertes que los Certificados RSA-basados y se requieren para los Productos que tienen certificaciones comunes de los criterios (CC). Las soluciones comerciales del gobierno de los EE. UU. para el programa clasificado de los sistemas (CSfC) requieren la certificación del CC y por eso, se incluye en la versión 11.0 del administrador de las Comunicaciones unificadas de Cisco hacia adelante.

Los Certificados ECDSA están disponibles junto con los Certificados existentes RSA en estas áreas:

- Administración de certificados
- Función de proxy del Certificate Authority (CAPF)
- El localizar de Transport Layer Security (TLS)

- Asegure las conexiones del SORBO
- Administrador de Integración de telefonía de computadora (CTI)
- HTTP y
- Entropía

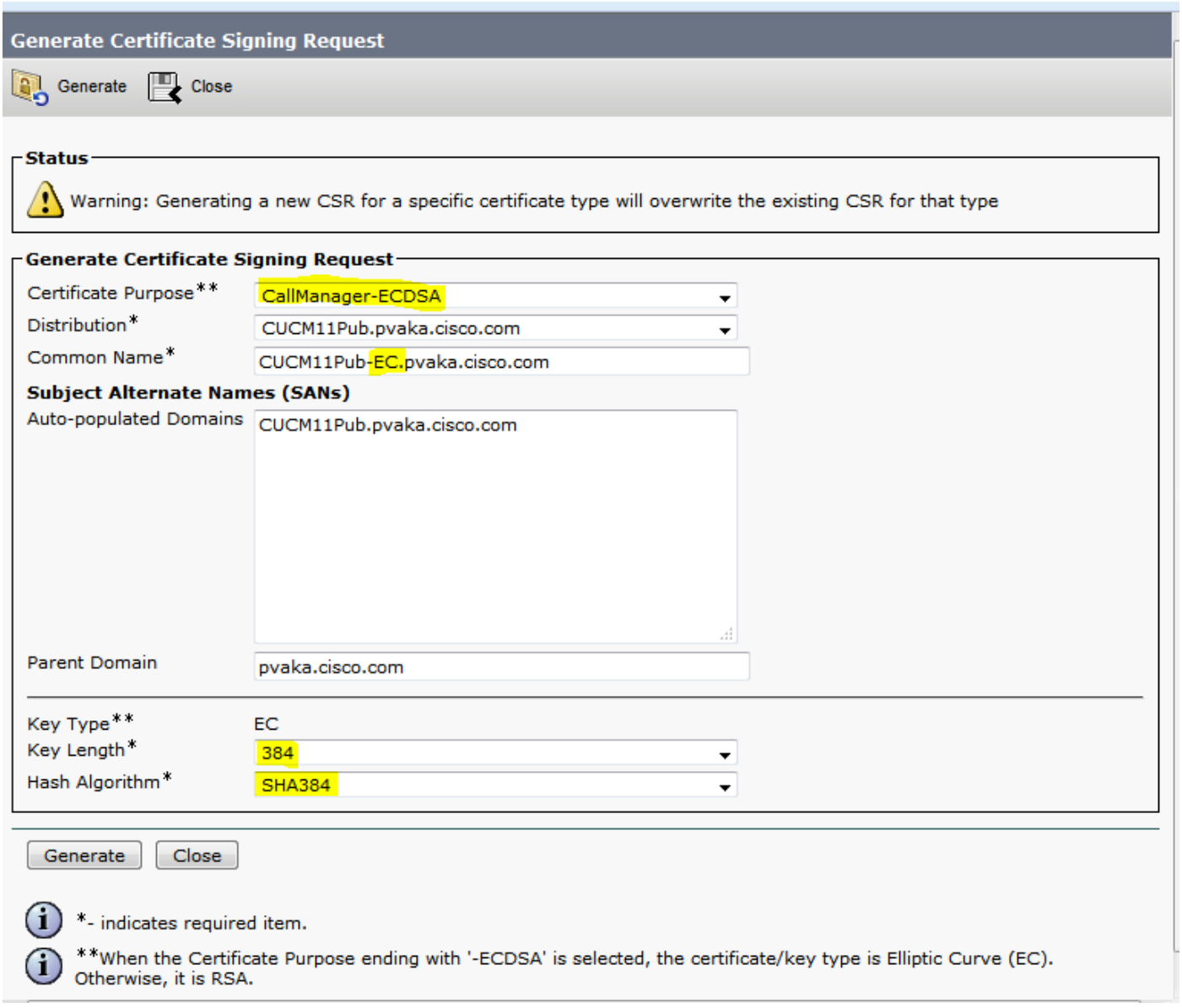
Las siguientes secciones proporcionan más información detallada en cada uno de las 7 áreas antedichas.

Administración de certificados

Generación de los Certificados con el cifrado EC

Soporte para el ECC de CUCM 11.0 hacia adelante para generar el certificado del CallManager con el cifrado EC

- Nuevo **CallManager-ECDSA de la** opción disponible tal y como se muestra en de la imagen.
- Requiere la porción del host del Common Name terminar adentro **– el EC**, para evitar el tener del mismo Common Name que el certificado del **CallManager**.
- En caso del certificado multi del servidor SAN, esto debe terminar adentro **– al EC-ms**.



- Amba la petición del certificado autofirmado y el CSR piden el límite las opciones del algoritmo de troceo dependiendo del tamaño de clave EC.
- Para un tamaño de clave EC 256 el algoritmo de troceo puede ser SHA256, SHA384 o SHA512. Para un tamaño de clave EC 384 el algoritmo de troceo puede ser SHA384 o SHA512. Para un tamaño de clave EC 521 la única opción es SHA512.
- El tamaño de la clave predeterminada es 384 y el algoritmo de troceo del valor por defecto es SHA384, usando el cual puede ser cambiado caen abajo. Las opciones disponibles se basan en el tamaño de clave elegido.

Configuración de CLI

Una nueva unidad del certificado nombrada **CallManager-ECDSA** se ha agregado para los comandos cli

- fije el [unit] CERT regen – certificado autofirmado de los regenerados

```
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)?
```

- fije la importación CERT poseen|[unit] de la confianza – certificado firmado de CA de las importaciones

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

- fije el [unit] GEN csr – genera el request(CSR) de firma del certificado para la unidad especificada

```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- fije la exportación a granel|consolide|importación tftp – Cuando tftp es el nombre de la unidad, los Certificados del CallManager-ECDSA consiguen auto-incluidos con los Certificados del CallManager RSA en las operaciones a granel.

Archivos CTL e ITL

- Los archivos CTL e ITL tienen presente del **CallManager-ECDSA**.
- El certificado del CallManager-ECDSA tiene la función de CCM+TFTP en el archivo ITL y

CTL.

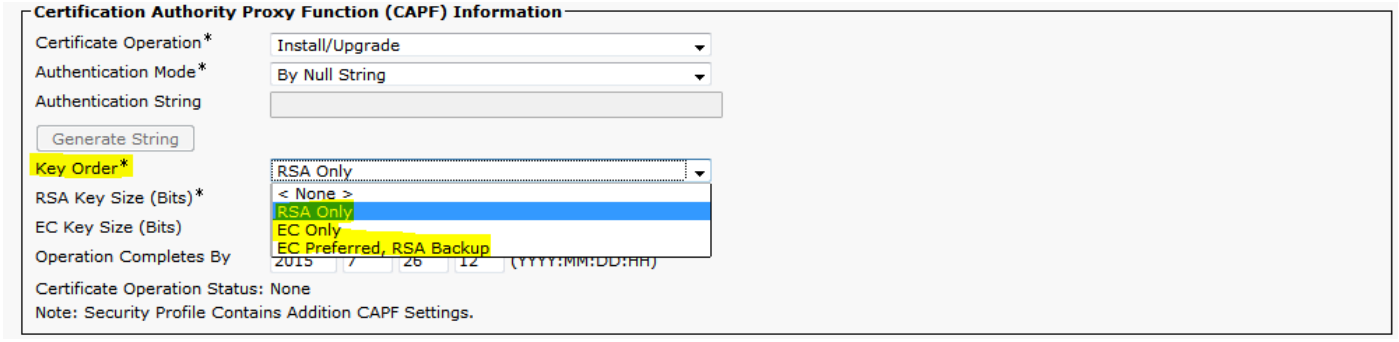
- Usted puede utilizar el **ctl de la demostración** o **mostrar los** comandos **ITL** de ver esta información tal y como se muestra en de la imagen:

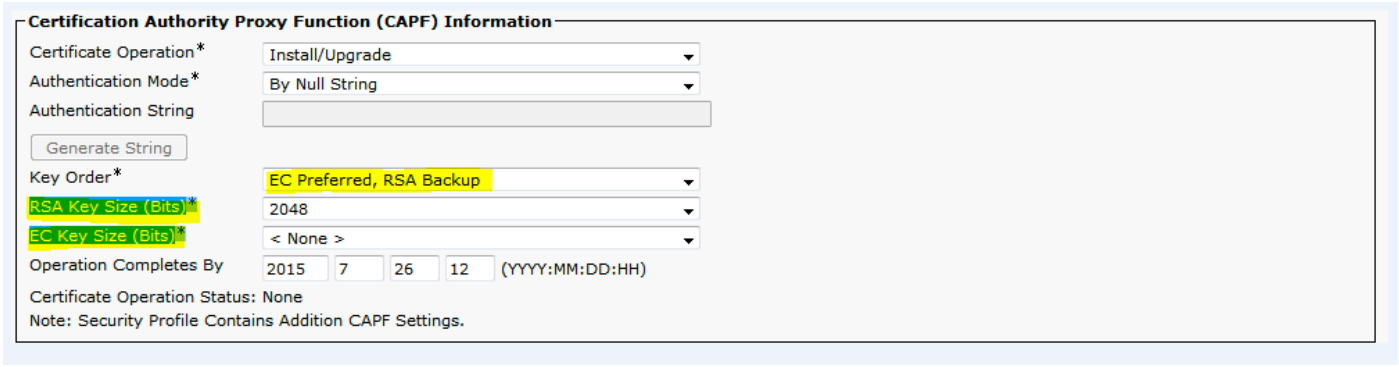
```
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1656
2       DNSNAME         2
3       SUBJECTNAME     65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME 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

- Usted puede utilizar la **actualización del ctl del utils** para generar el archivo CTL.

Función de proxy del Certificate Authority (CAPF)

- La versión 3.0 del CAPF en CUCM 11 proporciona el soporte para los tamaños de clave EC junto con el RSA.
- Las opciones adicionales del CAPF proporcionadas además de los campos existentes del CAPF son orden dominante y tamaño de clave EC (bits).
- La opción existente del tamaño de clave (bits) se ha cambiado al tamaño de clave RSA (bits).
- La orden dominante proporciona el soporte para el RSA solamente, el EC solamente y el EC preferido, las opciones del respaldo RSA.
- El tamaño de clave EC proporciona el soporte para los tamaños de clave 384 y 521 de los bits 256.
- El tamaño de clave RSA proporciona el soporte para 512, 1024 y 2048 bits
- Cuando es dominante la orden del RSA solamente se selecciona, sólo el tamaño de clave RSA puede ser seleccionado. Cuando se selecciona el EC solamente, sólo el tamaño de clave EC puede ser seleccionado. Cuando el EC preferido, respaldo RSA se selecciona, el tamaño de clave RSA y EC puede ser seleccionado.

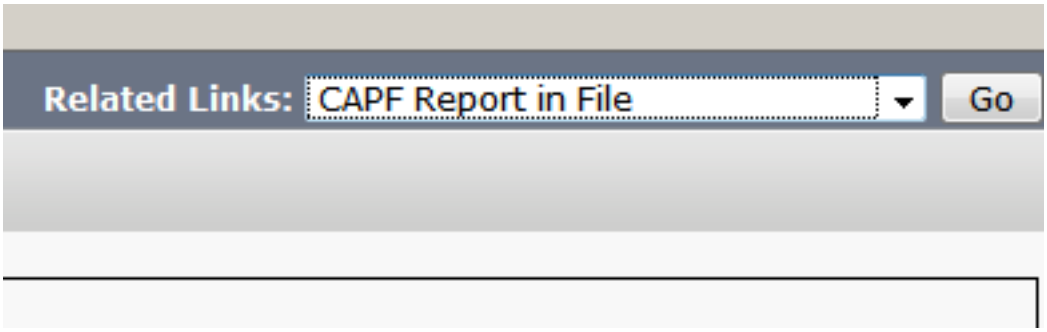




> **Note**: Actualmente, ninguna versión 3 del CAPF de los soportes del punto final de Cisco evita tan seleccionar la opción EC solamente. Sin embargo, los administradores que quieren soportar ECDSA LSC más adelante pueden configurar sus dispositivos con la opción preferida EC del respaldo RSA. Cuando los puntos finales comienzan a soportar la versión 3 del CAPF para ECDSA LSC, los administradores necesitan reinstalar su LSC.

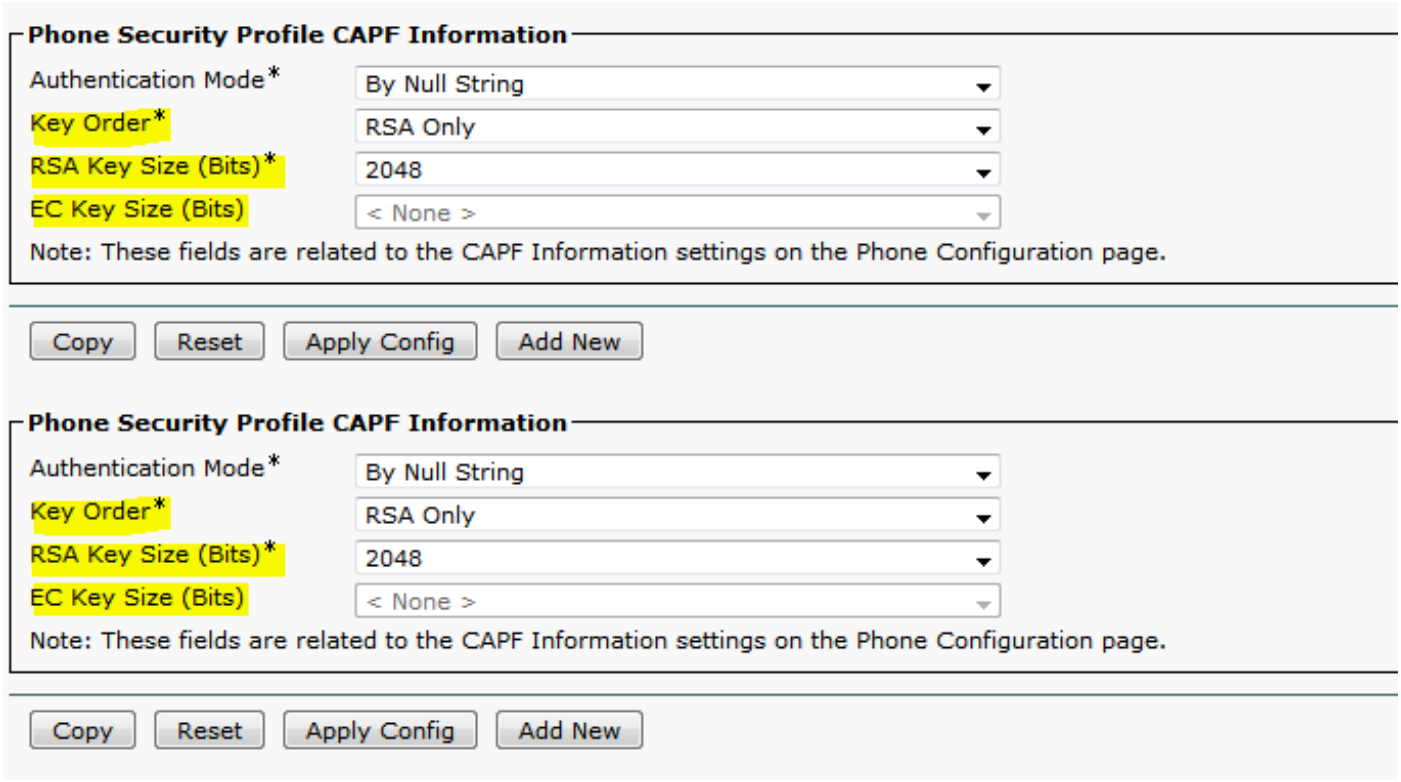
Opciones adicionales del CAPF para el teléfono, el perfil de seguridad del teléfono, el usuario final y las páginas del usuario de la aplicación

El Device (Dispositivo) > Phone (Teléfono) > relacionó los links

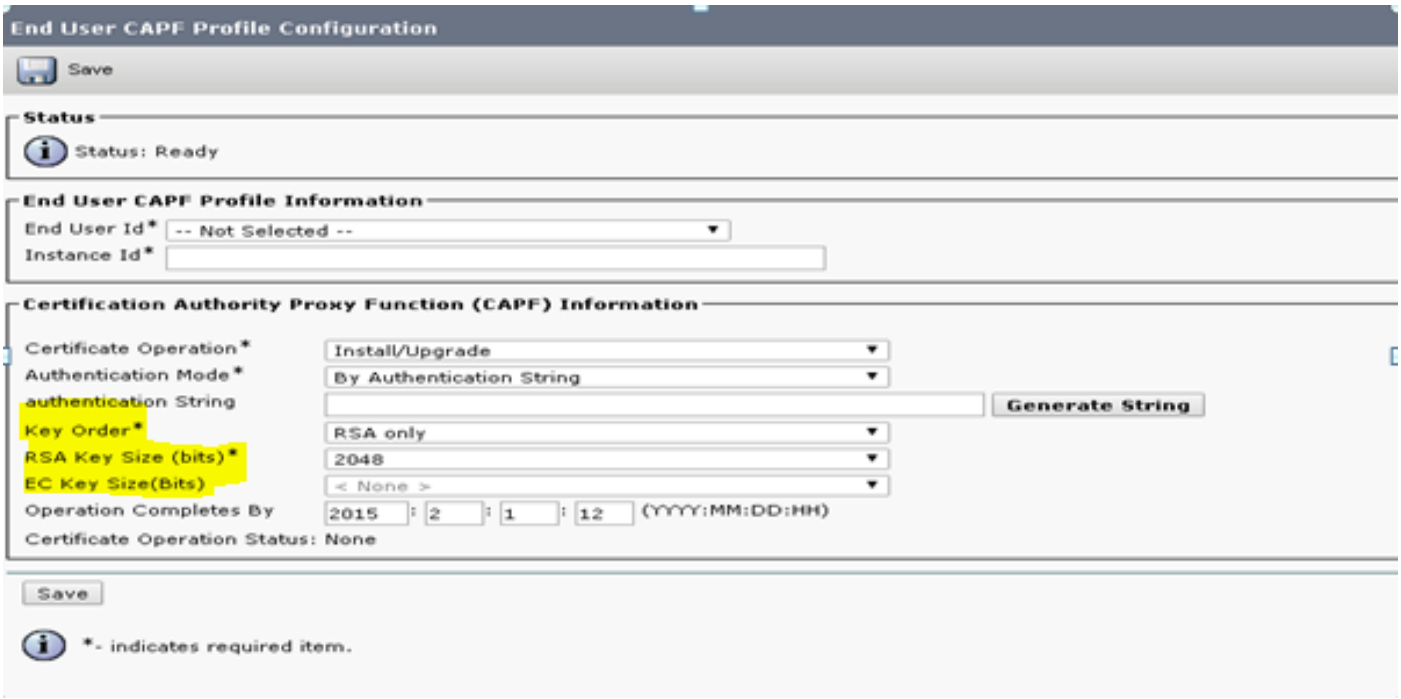


Navegue al **> Security (Seguridad) del sistema > al perfil de seguridad del teléfono**

User Management (Administración de usuario) > perfil del CAPF de los ajustes de usuario > del usuario de la aplicación

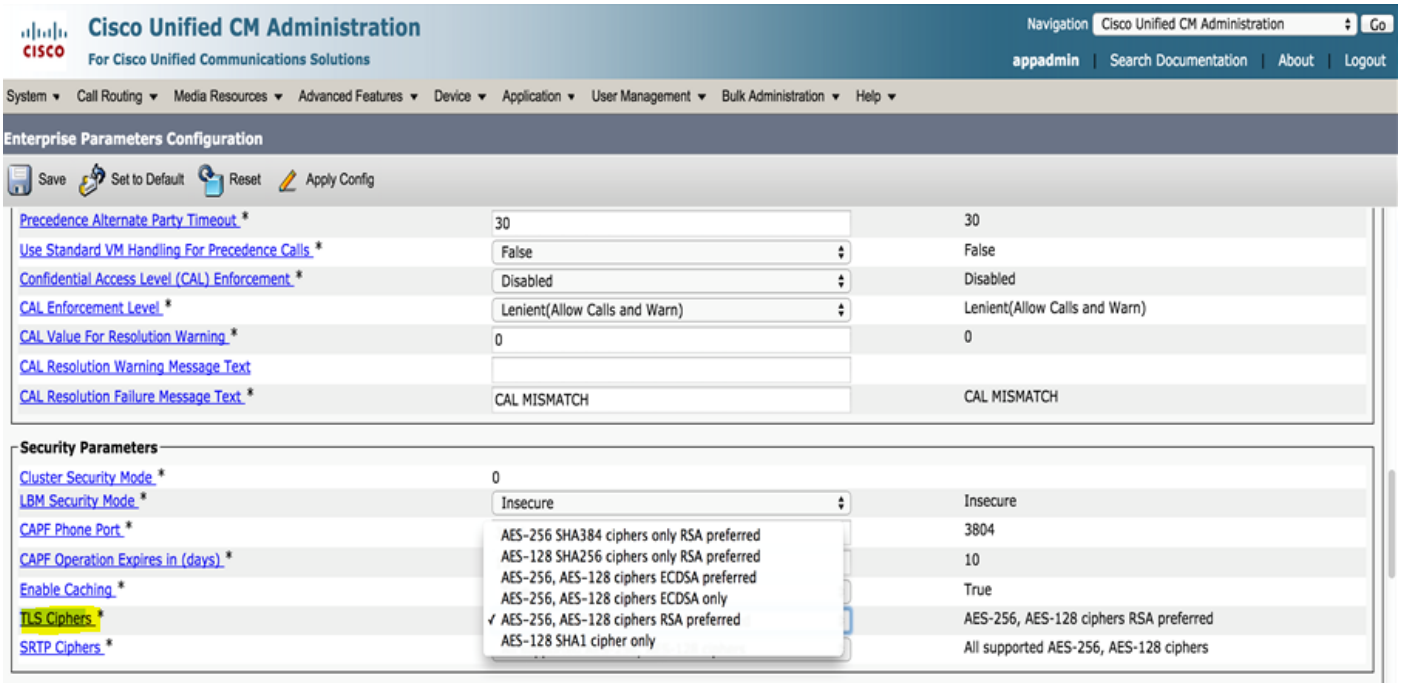


Navegue a **User Management (Administración de usuario) > perfil del CAPF de los ajustes de usuario > del usuario final.**



Parámetros Enterprise de las cifras de TLS

- Las cifras de TLS del parámetro Enterprise se han puesto al día para soportar las cifras ECDSA.
- Las cifras de TLS del parámetro Enterprise ahora fijan las cifras de TLS para la línea del SORBO, trunk del SORBO y aseguran al Administrador CTI.



Soporte del SORBO ECDSA

- La versión 11.0 del administrador de las Comunicaciones unificadas de Cisco incluye el soporte ECDSA para las líneas del SORBO y las interfaces de tronco del SORBO.
- La conexión entre el administrador de las Comunicaciones unificadas de Cisco y un teléfono del punto final o un dispositivo de video es una línea conexión del SORBO mientras que la conexión entre dos administradores de las Comunicaciones unificadas de Cisco es una conexión de tronco del SORBO.
- Todas las conexiones del SORBO soportan las cifras ECDSA y utilizan los Certificados ECDSA.

La interfaz segura del SORBO fue puesta al día para soportar estas dos cifras

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Éstos son los escenarios cuando el SORBO hace las conexiones TLS (de Transport Layer Security):

- Cuando el SORBO actúa como servidor de TLS

Cuando la interfaz de tronco SIP del administrador de las Comunicaciones unificadas de Cisco actúa como servidor TLS para la conexión segura entrante SIP, la interfaz de tronco SIP determina si el certificado del CallManager-ECDSA existe en el disco. Si el certificado existe en el disco, la interfaz de tronco del SORBO utiliza el certificado del CallManager-ECDSA si es la habitación seleccionada de la cifra

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 o
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

- Cuando el SORBO actúa como cliente de TLS

Cuando la interfaz de tronco del SORBO actúa como cliente de TLS, la interfaz de tronco del SORBO envía una lista de habitaciones pedidas de la cifra al servidor basado en el campo de las

cifras de TLS (que también incluye el ECDSA cifra la opción) en los parámetros Enterprise CUCM las **cifras de TLS**. Esta configuración determina la lista de la habitación de la cifra del cliente TLS y las habitaciones soportadas de la cifra en orden de la preferencia.

> **Note**: 1. Los dispositivos que utilizan una cifra ECDSA para hacer una conexión a CUCM deben tener el certificado del CallManager-ECDSA en su archivo de la lista de la confianza de la identidad (ITL).

> **Note**: 2. Las habitaciones de la cifra del soporte RSA TLS de la interfaz de tronco del SORBO para las conexiones de los clientes que no soportan las habitaciones de la cifra ECDSA o cuando una conexión TLS se establece con una versión anterior de CUCM, eso no soportan ECDSA.

Soporte seguro del Administrador CTI. ECDSA

La interfaz segura del Administrador CTI. fue puesta al día para soportar estas cuatro cifras:

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

- La carga segura de la interfaz del Administrador CTI. el certificado del CallManager y del CallManager-ECDSA. Esto permite que la interfaz segura del Administrador CTI. soporte las nuevas cifras junto con la cifra existente RSA.
- Similar a la interfaz del SORBO, la opción de las cifras de TLS del parámetro Enterprise en el administrador de las Comunicaciones unificadas de Cisco se utiliza para configurar las cifras de TLS que se soportan en la interfaz segura del Administrador CTI.

Soporte HTTPS para la descarga de la configuración

- Para la descarga segura de la configuración (por ejemplo clientes del Jabber), la versión 11.0 del administrador de las Comunicaciones unificadas de Cisco se aumenta para soportar el HTTPS además de las interfaces HTTP y TFTP que fueron utilizadas en las versiones anteriores.
- Si procede, ambo autenticación recíproca del uso del cliente y servidor. Sin embargo, requieren a los clientes que se alistan con ECDSA LSC y configuraciones de TFTP cifradas presentar su LSC.
- La interfaz HTTPS utiliza el CallManager y los Certificados del CallManager-ECDSA como los certificados de servidor.

> **Note**: 1. Cuando usted pone al día los Certificados del CallManager, del CallManager ECDSA, o de Tomcat, usted debe desactivar y reactivar servicio TFTP.

Note: 2. El puerto 6971 se utiliza para la autenticación de los Certificados del CallManager y del CallManager-ECDSA, usada por los teléfonos.

Note: 3. El puerto 6972 se utiliza para la autenticación de los Certificados de Tomcat, usada por el Jabber.

Entropía

La entropía es una medida de aleatoriedad de los datos y de las ayudas en determinar el umbral mínimo para los requisitos comunes de los criterios. Para tener encripción fuerte, una fuente robusta de entropía se requiere. Si un algoritmo de encripción fuerte, tal como ECDSA, utiliza una fuente débil de entropía, el cifrado puede estar roto fácilmente.

En la versión 11.0 del administrador de las Comunicaciones unificadas de Cisco, la fuente de la entropía para el administrador de las Comunicaciones unificadas de Cisco se mejora.

La daemon de la supervisión de la entropía es una característica incorporada que no requiere la configuración. Sin embargo, usted puede apagarla a través del administrador CLI de las Comunicaciones unificadas de Cisco.

Utilice los comandos CLI siguientes de controlar el servicio de daemon de la supervisión de la entropía:

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.

Información Relacionada

- 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
- Soporte Técnico y Documentación - Cisco Systems