Cifrado de última generación CUCM 11.0: criptografía de curva elíptica

Contenido

Introducción

Este documento describe la configuración del cifrado de última generación (NGE) de Cisco Unified Communications Manager (CUCM) 11.0 y posteriores para cumplir los requisitos de rendimiento y seguridad mejorados.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conceptos básicos de seguridad de Cisco CallManager
- Administración de certificados de Cisco CallManager

Componentes Utilizados

La información de este documento se basa en Cisco CUCM 11.0, donde sólo se admiten certificados de algoritmo de firma digital de curva elíptica (ECDSA) para CallManager (CallManager-ECDSA).

> **Nota:** CUCM 11.5 y posterior también admite certificados tomcat-ECDSA.

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.

Productos Relacionados

Este documento también se puede utilizar con estos productos de software y versiones que admiten certificados ECDSA:

- IM y presencia de Cisco Unified CM 11.5
- Cisco Unity Connection 11.5

Antecedentes

La criptografía de curva elíptica (ECC) es un acercamiento a la criptografía de clave pública basada en la estructura algebraica de curvas elípticas sobre campos finitos. Una de las principales ventajas en comparación con la criptografía no ECC es el mismo nivel de seguridad que proporcionan las claves de menor tamaño.

Common Criteria (CC) proporciona la garantía de que las funciones de seguridad funcionan correctamente dentro de la solución que se evalúa. Esto se logra mediante pruebas y el cumplimiento de amplios requisitos de documentación.

Es aceptado y apoyado por 26 países en todo el mundo a través del Acuerdo de Reconocimiento de Criterios Comunes (CCRA, por sus siglas en inglés).

La versión 11.0 de Cisco Unified Communications Manager admite certificados de algoritmo de firma digital de curva elíptica (ECDSA).

Estos certificados son más fuertes que los certificados basados en RSA y se requieren para productos que tienen certificaciones CC. El programa de soluciones comerciales del gobierno de EE. UU. para sistemas clasificados (CSfC) requiere la certificación CC, por lo que se incluye en la versión 11.0 y posteriores de Cisco Unified Communications Manager.

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

- Administración de certificados
- Función de proxy de autoridad de certificados (CAPF)
- Seguimiento de seguridad de la capa de transporte (TLS)
- Conexiones de protocolo de inicio de sesión seguro (SIP)
- Administrador de integración de telefonía y ordenador (CTI)
- HTTP
- Entropía

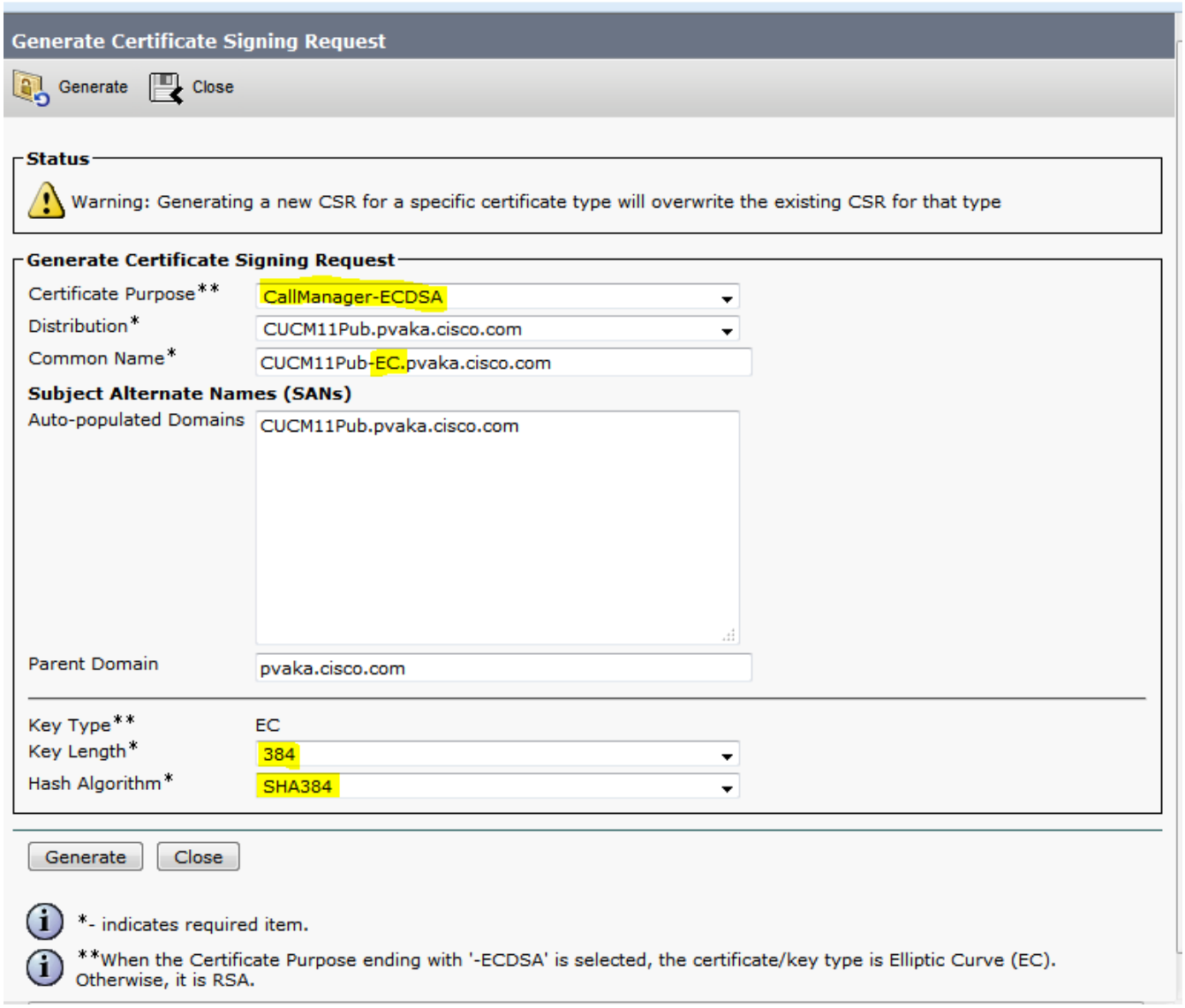
En las secciones siguientes se ofrece información más detallada sobre cada una de esas siete esferas.

Administración de certificados

Generar certificados con cifrado de curva elíptica

Compatibilidad con ECC de CUCM 11.0 y posterior para generar el certificado de CallManager con cifrado de curva elíptica (EC):

- La nueva opción **CallManager-ECDSA** está disponible como se muestra en la imagen.
- Requiere que la parte de host del nombre común termine en **-EC**. Esto evita tener el mismo nombre común que el certificado **CallManager**.
- En el caso de un certificado SAN de servidor múltiple, esto debe terminar en **-EC-ms**.



- Tanto la solicitud de certificado autofirmado como la solicitud CSR limitan las opciones del algoritmo hash dependiendo del tamaño de la clave EC.
- Para un tamaño de clave EC 256, el algoritmo hash puede ser SHA256, SHA384 o SHA512. Para un tamaño de clave EC 384, el algoritmo hash puede ser SHA384 o SHA512. Para un tamaño de clave EC 521, la única opción es SHA512.
- El tamaño de clave predeterminado es 384 y el algoritmo hash predeterminado es SHA384, que se puede cambiar. Las opciones disponibles se basan en el tamaño de clave seleccionado.

Configuración de CLI

Se ha agregado una nueva unidad de certificado denominada **CallManager-ECDSA** para los

comandos CLI

- set cert regen [unit] - regenera el certificado autofirmado

```
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 certificado firmado por CA

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

- set csr gen [unit] - genera una solicitud de firma de certificado (CSR) para la **unidad** especificada

```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- set bulk export|consolidate|import tftp - Cuando tftp es el nombre de la unidad, los certificados de CallManager-ECDSA se incluyen automáticamente con los certificados RSA de CallManager en operaciones masivas.

Archivos CTL e ITL

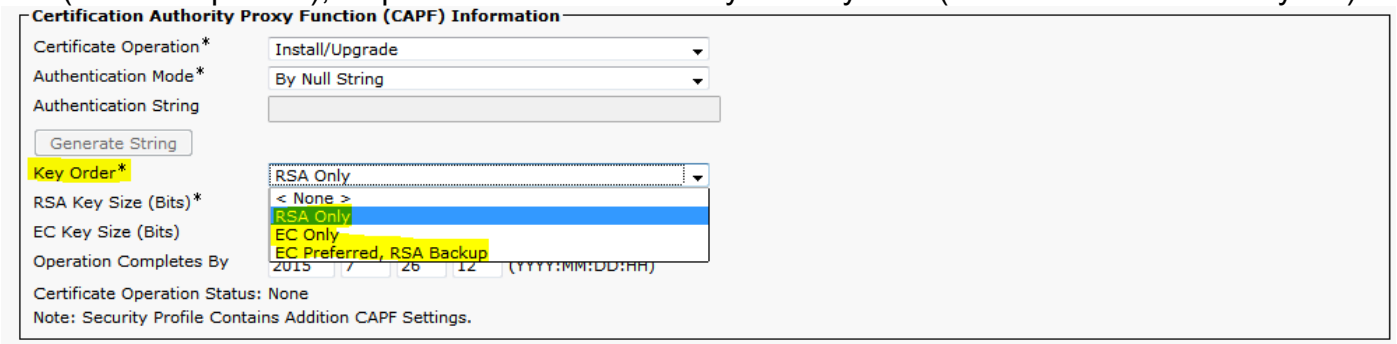
- Tanto los archivos de la lista de confianza de certificados (CTL) como de la lista de confianza de identidad (ITL) tienen **CallManager-ECDSA** presente.
- El certificado CallManager-ECDSA tiene la función de CCM+TFTP tanto en el archivo ITL como en el archivo CTL.
- Puede utilizar el **show ctl** or **show itl** para ver esta información como se muestra en esta imagen:

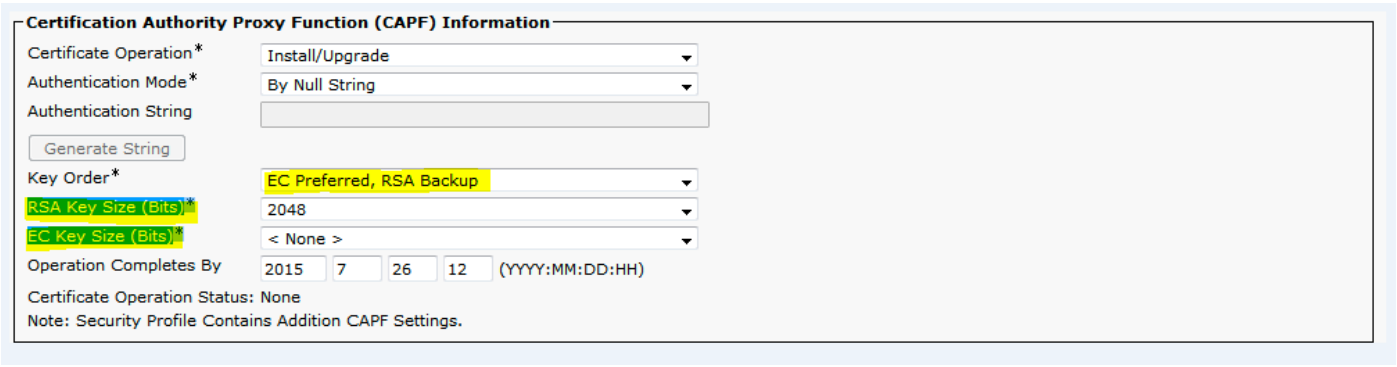
```
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1656
2       DNSNAME         2
3       SUBJECTNAME     65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME 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

- Puede utilizar el comando **utils ctl update** para generar el archivo CTL.

Función Proxy de la Autoridad de Certificados

- La función de proxy de autoridad certificadora (CAPF) versión 3.0 de CUCM 11 admite tamaños de clave CE junto con RSA.
- Las opciones CAPF adicionales proporcionadas además de los campos CAPF existentes son Orden de claves y Tamaño de clave CE (bits).
- La opción Tamaño de clave (bits) existente se ha cambiado a Tamaño de clave RSA (bits).
- El pedido de clave proporciona soporte para las opciones de respaldo RSA Only, EC Only y EC Preferred.
- El tamaño de clave EC proporciona soporte para tamaños de clave de 256, 384 y 521 bits.
- El tamaño de clave RSA proporciona soporte para 512, 1024 y 2048 bits.
- Cuando se selecciona Key Order of RSA Only (Orden de claves de RSA solamente), sólo se puede seleccionar RSA Key Size (Tamaño de clave RSA). Si sólo se selecciona EC, sólo se puede seleccionar EC Key Size (Tamaño de clave EC). Cuando se selecciona EC Preferred (Preferida por EC), se puede seleccionar RSA y EC Key Size (Tamaño de clave RSA y EC).

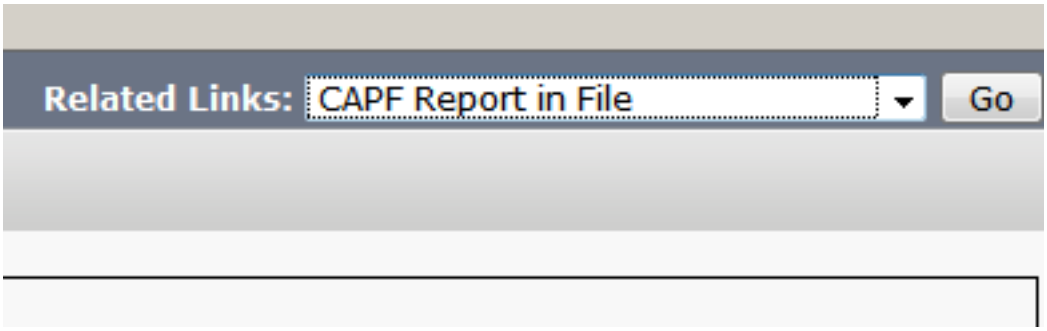




> **Nota:** Actualmente, ningún terminal de Cisco admite la versión 3 de CAPF, por lo que no seleccione la opción EC Only (Sólo EC). Sin embargo, los administradores que deseen admitir certificados ECDSA de importancia local (LSC) más adelante pueden configurar sus dispositivos con la opción EC Preferred RSA Backup (Copia de seguridad CE preferida RSA). Cuando los terminales empiezan a admitir la versión 3 de CAPF para LSC ECDSA, los administradores necesitan reinstalar su LSC.

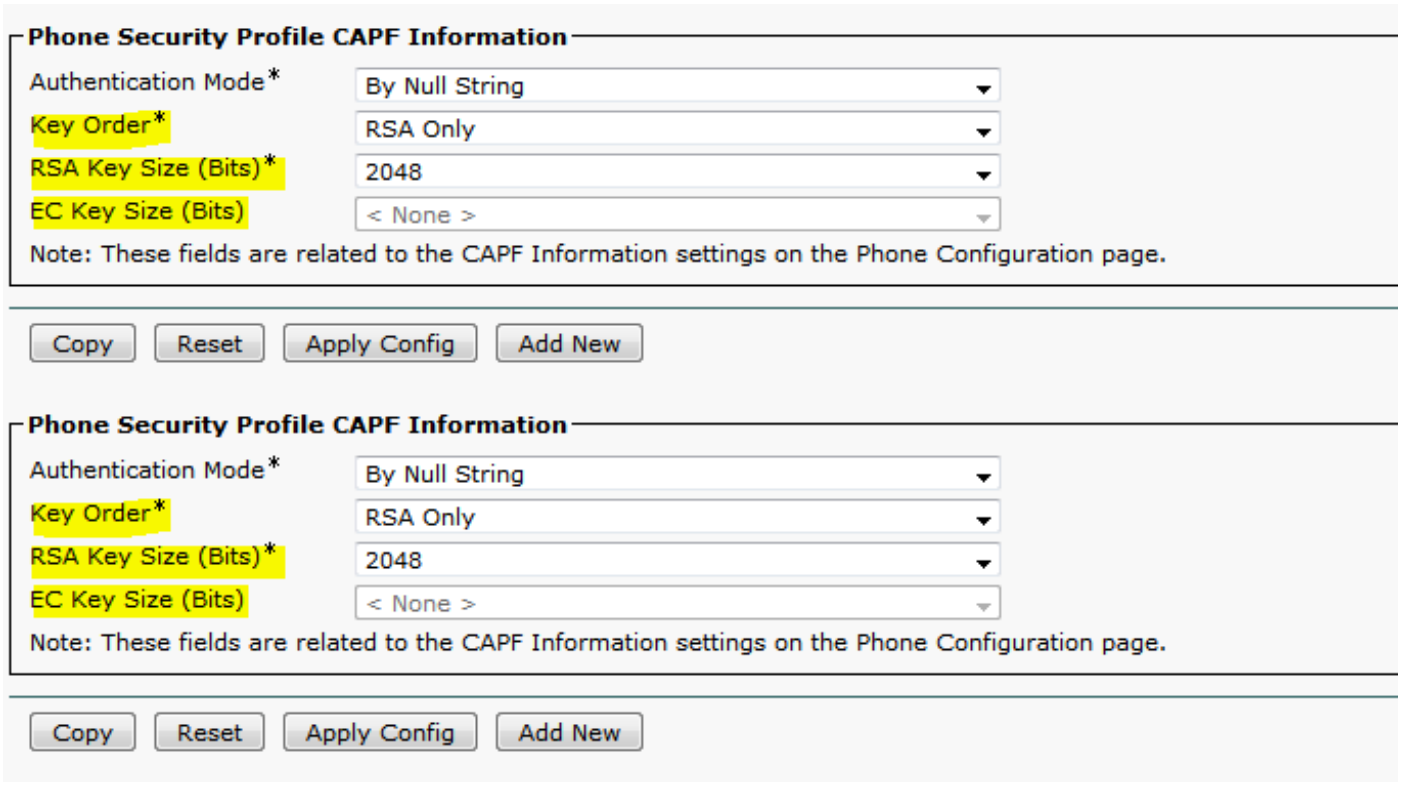
Aquí se muestran opciones CAPF adicionales para las páginas Phone (Teléfono), Phone Security Profile (Perfil de seguridad del teléfono), End User (Usuario final) y Application User Pages (Usuario de la aplicación):

Device > Phone > Related Links

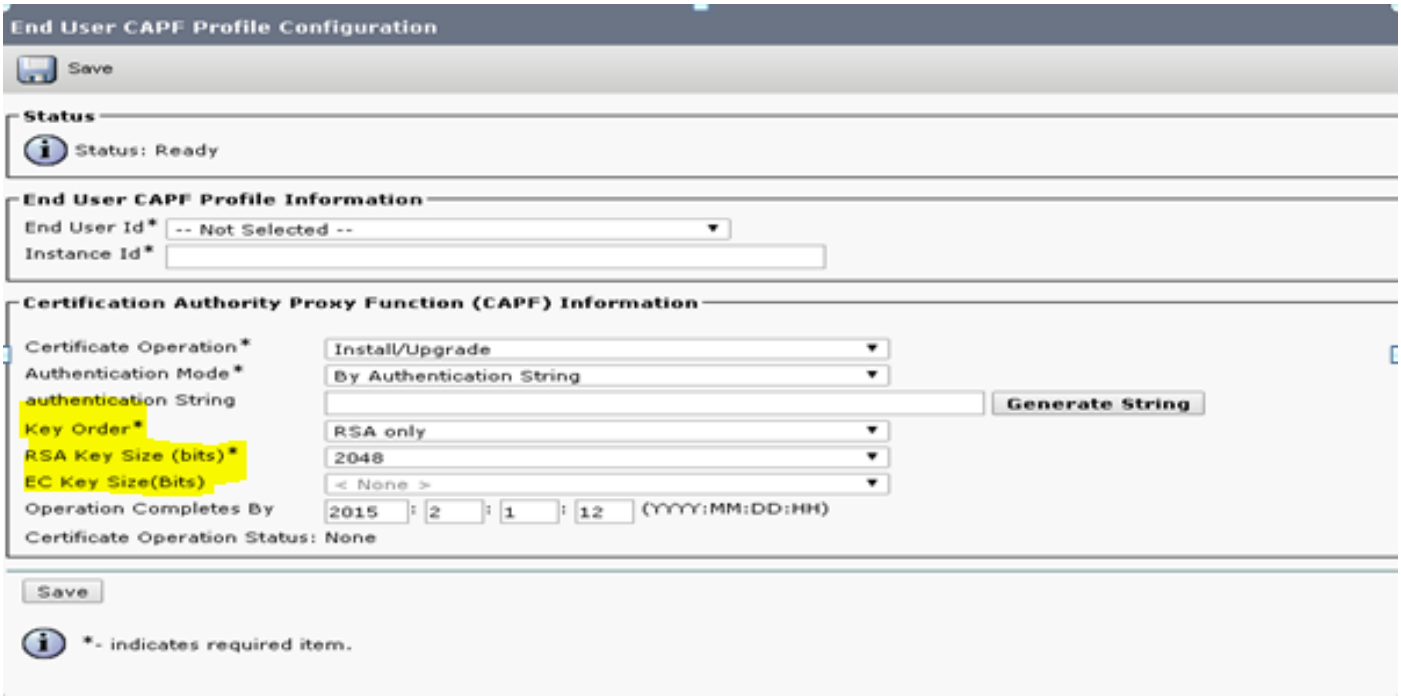


Vaya a **Sistema > Seguridad > Perfil de seguridad del teléfono**

User Management > User Settings > Application User CAPF Profile

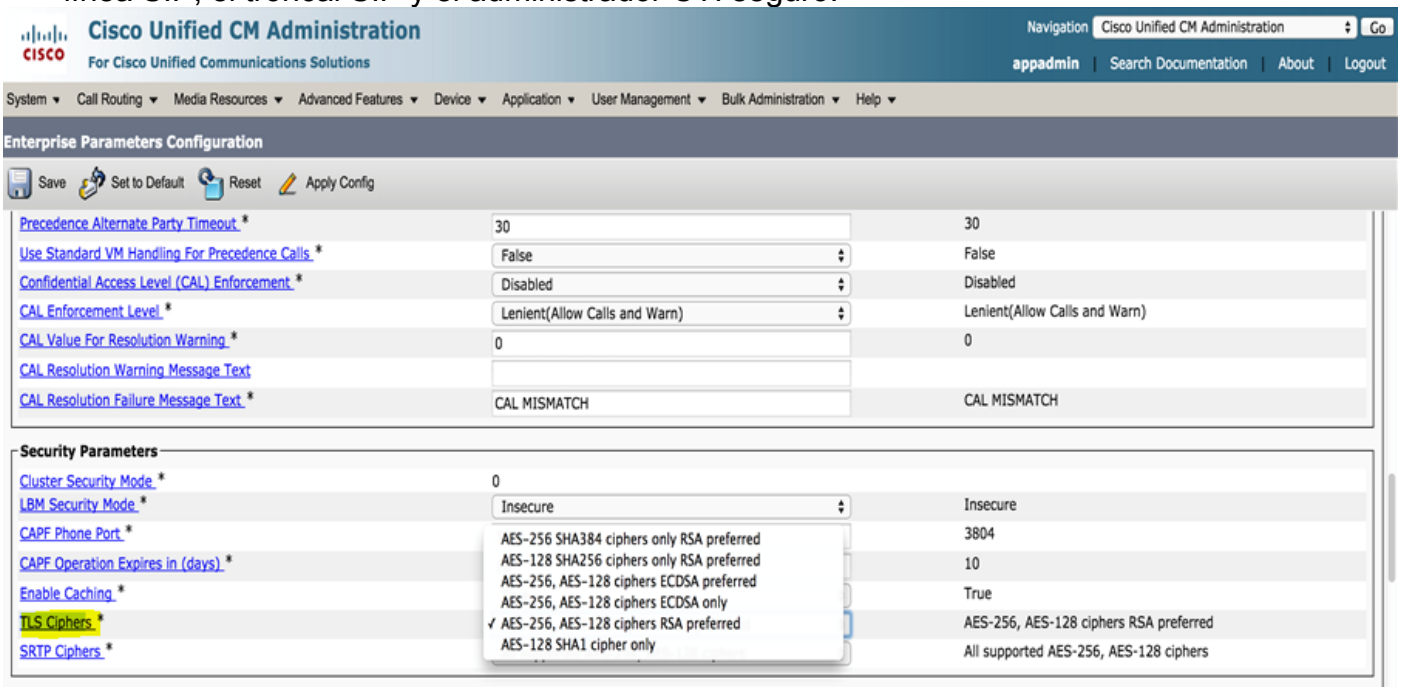


Vaya a **User Management > User Settings > End User CAPF Profile (Administración de usuarios > Configuración de usuario > Perfil CAPF del usuario final).**



Parámetros empresariales de los cifradores TLS

- El parámetro de empresa Ciphers TLS se ha actualizado para admitir los Cifradores ECDSA.
- Los cifradores TLS de parámetro empresarial configuran ahora los cifradores TLS para la línea SIP, el troncal SIP y el administrador CTI seguro.



Compatibilidad con SIP ECDSA

- La versión 11.0 de Cisco Unified Communications Manager incluye compatibilidad con ECDSA para líneas SIP e interfaces troncales SIP.
- La conexión entre Cisco Unified Communications Manager y un teléfono o dispositivo de vídeo del terminal es una conexión de línea SIP, mientras que la conexión entre dos Cisco Unified Communications Manager es una conexión troncal SIP.

- Todas las conexiones SIP admiten los cifrados ECDSA y utilizan certificados ECDSA.

La interfaz SIP segura se actualizó para admitir estas dos claves:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Estos son los escenarios cuando SIP realiza conexiones TLS:

- Cuando SIP actúa como servidor TLS Cuando la interfaz troncal SIP de Cisco Unified Communications Manager actúa como servidor TLS para la conexión SIP segura entrante, la interfaz troncal SIP determina si el certificado CallManager-ECDSA existe en el disco. Si el certificado existe en el disco, la interfaz troncal SIP utiliza el certificado CallManager-ECDSA si el conjunto de cifrado seleccionado esTLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 o TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- Cuando SIP actúa como cliente TLS Cuando la interfaz troncal SIP actúa como cliente de TLS, la interfaz troncal SIP envía una lista de conjuntos de cifrado solicitados al servidor basándose en el campo Cifradores de TLS (que también incluye la opción Cifrados ECDSA) en los Parámetros Empresariales de CUCM **Los Cifers de TLS**. Esta configuración determina la lista del conjunto de conjuntos de cifrado del cliente TLS y los conjuntos de números admitidos en orden de preferencia.

  Notas:
  - Los dispositivos que utilizan un cifrado ECDSA para realizar una conexión a CUCM deben tener el certificado CallManager-ECDSA en su archivo de lista de confianza de identidad (ITL).
  - La interfaz troncal SIP admite conjuntos de cifrado RSA TLS para conexiones de clientes que no soportan conjuntos de cifrado ECDSA o cuando se establece una conexión TLS con una versión anterior de CUCM, que no soportan ECDSA.

Soporte de ECDSA de Secure CTI Manager

La interfaz de Secure CTI Manager se actualizó para admitir estas cuatro claves:

- 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 interfaz de Secure CTI Manager carga el certificado de CallManager y CallManager-ECDSA. Esto permite que la interfaz de Secure CTI Manager admita los nuevos cifrados junto con el cifrado RSA existente.

De forma similar a la interfaz SIP, la opción Cifradores TLS de parámetro empresarial de Cisco Unified Communications Manager se utiliza para configurar los cifradores TLS admitidos en la interfaz segura de CTI Manager.

Soporte HTTPS para Descarga de Configuración

- Para la descarga segura de la configuración (por ejemplo, clientes Jabber), Cisco Unified

Communications Manager versión 11.0 se mejora para admitir HTTPS además de las interfaces HTTP y TFTP que se utilizaron en las versiones anteriores.
- Si es necesario, tanto el cliente como el servidor utilizan la autenticación mutua. Sin embargo, los clientes que están inscritos con los LSCs ECDSA y las configuraciones TFTP cifradas son necesarios para presentar su LSC.
- La interfaz HTTPS utiliza los certificados CallManager y CallManager-ECDSA como certificados de servidor.

Notas:
- Cuando actualiza los certificados CallManager, CallManager ECDSA o Tomcat, debe desactivar y reactivar el servicio TFTP.
- El puerto 6971 se utiliza para la autenticación de los certificados CallManager y CallManager-ECDSA, utilizados por los teléfonos.
- El puerto 6972 se utiliza para la autenticación de los certificados Tomcat, utilizados por Jabber.

Entropía

La entropía es una medida de aleatoriedad de los datos y ayuda a determinar el umbral mínimo para los requisitos de criterios comunes. Para disponer de un cifrado sólido, se requiere una fuente sólida de entropía. Si un algoritmo de cifrado sólido, como ECDSA, utiliza una fuente débil de entropía, el cifrado se puede romper fácilmente.

En la versión 11.0 de Cisco Unified Communications Manager, se mejora el origen de la entropía de Cisco Unified Communications Manager.

Entropy Monitoring Daemon es una función integrada que no requiere configuración. Sin embargo, puede desactivarlo a través de la CLI de Cisco Unified Communications Manager.

Utilice estos comandos CLI para controlar el servicio 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.

Información Relacionada

- Guía de seguridad de Cisco Unified Communications Manager, versión 11.5(1)
- Soporte Técnico y Documentación - Cisco Systems