centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1460

Procedimiento de empleo seguro
Cisco Unified Communications Manager (C220 M5 y C240 M5)

Abril de 2024

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid.

NIPO: 083-24-147-5.
Fecha de Edición: abril 2024.

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.04.12 09:53:31 +02'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

El objeto del presente documento es la solución *Cisco Unified Communications Manager*. Dicha solución se compone tanto de una parte software como una parte hardware.

Cisco Unified Communications Manager (CUCM) es un software de telefonía IP que se utiliza para gestionar las llamadas y la mensajería dentro de una organización. Este software es parte de una suite de productos de comunicaciones unificadas de Cisco que incluyen mensajería de voz, videoconferencia, mensajería instantánea y presencia.

El CUCM proporciona funciones avanzadas de telefonía necesarias para soportar un entorno de negocio de hoy en día. Estas características incluyen enrutamiento y traducción de llamadas, supervisión de llamadas, control de conferencias, y más. Además, el CUCM puede integrarse con otras aplicaciones de negocio, como el correo electrónico y los sistemas de calendario, para proporcionar una solución completa de comunicaciones unificadas.

En cuanto al componente hardware, este documento hace referencia a los servidores Cisco C220 M5 y C240 M5, que son parte de la serie de servidores UCS de Cisco que proporcionan un rendimiento, flexibilidad y eficiencia adecuados para desplegar en ellos la solución CUCM.

El servidor C220 M5 es un servidor en rack de 1U que ofrece un equilibrio entre rendimiento y densidad. Es ideal para implementaciones generales de propósito que requieren alta densidad y rendimiento.

Por otro lado, el servidor C240 M5 es un servidor en rack de 2U que ofrece un mayor rendimiento y capacidad de expansión. Está diseñado para cargas de trabajo que requieren gran cantidad de recursos de almacenamiento y memoria.

2. OBJETO Y ALCANCE

2.1 HARDWARE

Los equipos hardware que se han evaluado en este documento son los siguientes modelos:

- Servidor UCS C220 M5
- Servidor UCS C240 M5

2.2 SOFTWARE

El software evaluado en este documento es el *Cisco Unified Communications Manager* versiones 12.5 y 14.

3. ORGANIZACIÓN DEL DOCUMENTO

Este documento se compone de los siguientes apartados:

a) Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado **5**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado **6**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

d) Apartado **7**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL HARWARE

El equipo hardware debe ser examinado para comprobar que no ha sido manipulado durante su entrega confirmando los siguientes pasos:

1. Antes de abrir el paquete entregado que contiene el equipo, compruebe que el paquete tiene la serigrafía y el logo de Cisco. Si no es así, contacte con el proveedor del equipo (Cisco o un distribuidor autorizado).
2. Compruebe que el paquete no ha sido abierto y vuelto a sellar fijándose en la cinta que lo cierra. Si el paquete parece haber sido abierto y sellado de nuevo contacte con el proveedor del equipo (Cisco o un distribuidor autorizado).
3. Compruebe que el paquete contiene la impresión resistente a manipulaciones de Cisco en la cara externa de la caja de cartón. Si no es así, contacte con el proveedor del equipo (Cisco o un distribuidor autorizado). La impresión contiene el número de producto de Cisco, su número de serie e información adicional sobre el contenido de la caja.
4. Revise el número de serie del equipo especificado en la documentación del pedido. El número de seria que figura en la etiqueta blanca de la caja debe corresponderse con el número de serie del dispositivo. Compruebe que el número concuerda con el de la factura enviada por correo. Si no es así, contacte con el proveedor del equipo (Cisco o un distribuidor autorizado).
5. Compruebe que el pedido fue enviado por el proveedor esperado (Cisco o un distribuidor autorizado). Para llevar a cabo este proceso verifique el código de envío/paquete junto con la empresa de transporte. Compruebe también que los números de serie de los productos enviados concuerdan con los números de serie de los productos recibidos. Esta verificación se debe llevar a cabo haciendo uso de un mecanismo externo al proceso de envío, por ejemplo, teléfono o servicio online de rastreo de paquetes.
6. Una vez abierto el paquete revise el dispositivo. Compruebe que el número de serie mostrado es el mismo que aparece en la documentación de envío y en la factura. Si no es así, contacte con el proveedor del equipo (Cisco o un distribuidor autorizado). Revise también que el equipo tiene una de las siguientes identificaciones externas:

Modelo	Identificación externa
UCS C220 M5	Cisco UCS-C220-M5
UCS C240 M5	Cisco UCS-C240-M5

Tabla 1 - Productos e identificación externa

4.2 ENTREGA SEGURA DEL SOFTWARE

El sistema hardware de Cisco se refiere a los productos Cisco UCS. Se ha de referir a la guía de los productos UCS para la instalación del software de gestión del equipo hardware en sí mismo (Cisco IMC) y del software de virtualización (como puede ser VMware ESXi).

La solución *Cisco Unified Communications Manager* (CUCM) corre sobre una máquina virtual instalada sobre sistemas hardware virtualizables basados en VMware vSphere ESXi.

Es posible que sea necesario descargar e instalar la última versión de software. Para ello, proceder a la descarga desde el "Software Center" de Cisco: https://software.cisco.com/download/home

El software para descargar contiene un checksum para su comprobación. Por lo que previo a la descarga se debe copiar el checksum.

En la ilustración 1, tenemos un ejemplo de la página de descarga del software versión 12.5. En ella se puede ver como el último campo del menú emergente contiene un campo denominado SHA512 Checksum.

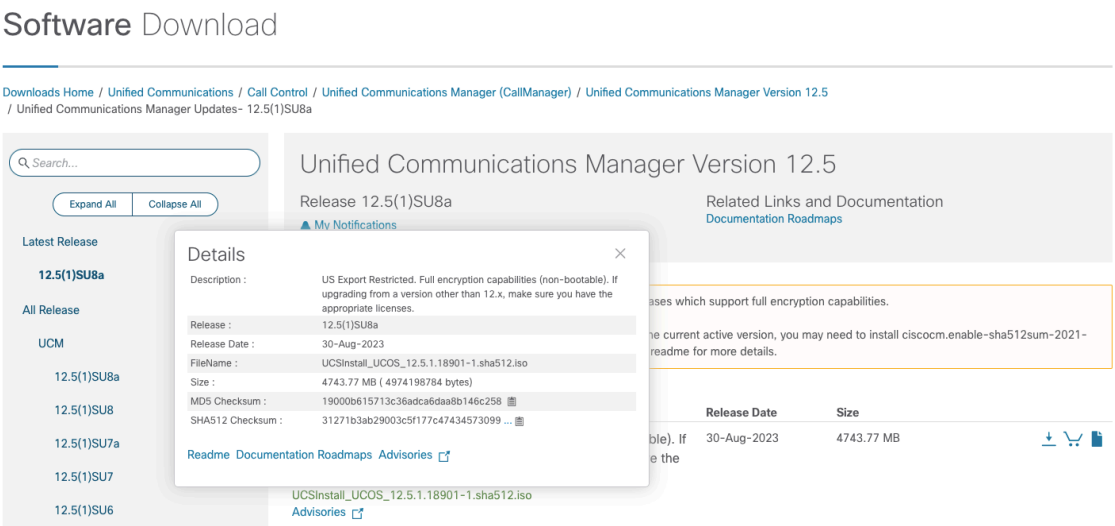

Ilustración 1 – Captura de pantalla de la página de descarga del software

Una vez completada la descarga, el administrador puede chequear los *upgrade_logs* que se han generado. Estos logs contienen los archivos descargados y permiten al administrador comparar el hash publicado (ver Ilustración 1) con el hash que aparece en dichos logs. Si ambos coinciden, la descarga del software es segura y se puede proseguir con la instalación. Si no es así, contacte con el proveedor del equipo (Cisco o un distribuidor autorizado).

Para la instalación de la actualización, se ha de referir a los documentos [1], en las guías "*Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service*", apartado "*Upgrade Install Image from Local Source*" ó "*Upgrade Install Image from Remote Server*".

4.3 ENTORNO DE INSTALACIÓN SEGURO

Los equipos hardware deben instalarse en una ubicación físicamente segura donde sólo se permita el acceso físico al personal autorizado.

En cuanto al software, el CUCM al tratarse de una solución cerrada en forma de paquete llave en mano (o "*appliance*"), está disponible en formato de fichero ISO firmado por Cisco. No se trata de una distribución abierta o de propósito general.

Cisco distribuye su software de CUCM, firmado digitalmente. Por lo tanto, todas las imágenes software de instalación y de actualización de la solución han de estar digitalmente firmadas por Cisco.

En este sentido el sistema operativo contenido, tampoco es una distribución de propósito general. Los módulos no necesarios están excluidos, y los servicios no utilizados están deshabilitados o borrados.

Cisco realiza cambios y refuerzos propietarios para aumentar la seguridad de este software.

Como solución cerrada, no es posible y no está permitido la instalación de:

- Agentes anti-virus, agentes UPS, agentes de gestión, etc.
- Cualquier otro software de terceros.
- Ningún software ajeno a la solución.

4.4 REGISTRO Y LICENCIAS

El sistema de licencias se denomina *Smart Software Licensing*.

Una vez instalado el CUCM estará operativo en modo demostración (un máximo de 90 días) hasta que sea registrado en Cisco Smart Software Manager (CSSM) mediante el uso de una cuenta Smart Licensing adecuada (en el portal de Cisco: https://software.cisco.com/), donde el CUCM reportará las licencias necesarias para su correcto uso.

La información referente al CSSM se puede encontrar en la referencia [2].

En el CSSM se pueden ver las licencias adquiridas. Cuando el CSSM recibe las informaciones sobre el uso de las licencias modificando el contador de las licencias usadas.

El detalle de las licencias disponibles en CUCM se puede encontrar en la referencia [3], en la guía "*Feature Configuration Guide for Cisco Unified Communications Manager*", en el apartado de *Licensing*.

4.5 COMPONENTES DEL ENTORNO DE GESTIÓN

Referirse a las guías CCN de Seguridad de UCS para los componentes del entorno de gestión de los servidores hardware.

El CUCM como solución cerrada, no tiene accesibles los interfaces de gestión nativa del Sistema Operativo, de las Bases de Datos, *runtime*, y otros componentes software.

El acceso a dichos interfaces operativos está oculto y bloqueado, o borrado directamente.

Los mecanismos de gestión necesarios están accesibles mediante el uso permitido de un interfaz GUI desde un navegador web, por comandos CLI o por API. Cisco ha reforzado la seguridad de dichos interfaces mediante diferentes mecanismos, como son refuerzo de la complejidad requerida de contraseñas, SSH (en lugar de Telnet) y protocolo TLS 1.2.

El acceso en modo *root* al Sistema Operativo no está activo por defecto.

Para situaciones de emergencia donde no se pueda solucionar el problema mediante el acceso a los interfaces disponibles (GUI/CLI/API), se puede generar una cuenta remota "*Remote Account*" para que el servicio Cisco TAC exclusivamente tenga acceso *root* de forma temporal. Siempre existe un parámetro de expiración automática para dicha cuenta.

En definitiva, la solución requiere los siguientes componentes en un entorno de gestión segura:

- Puesto de gestión con protocolo HTTPS
  Este puesto hace referencia a una estación de trabajo con un navegador HTTPS instalado, que se emplea para la configuración y administración del equipo.
- Puesto de gestión con cliente SSH
  Este puesto hace referencia a cualquier estación de trabajo con un cliente SSHv2 instalado, que se emplea para la configuración y administración del equipo, mediante una sesión CLI.

5. FASE DE INSTALACIÓN

El detalle completo de la instalación de la solución se encuentra en la guía *Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service*, referida en [1].

La solución puede consistir en más de un nodo CUCM. Si este es el caso las siguientes modificaciones en firewalls existentes en el entorno de instalación deben tenerse en cuenta durante la fase de instalación del software de la solución:

- Desactivación de las reglas del firewall para el tráfico exclusivo entre nodos si éste se encuentra en la ruta entre cualquiera de los nodos.
- Incrementar los valores de *timeout* del firewall para tráfico exclusivo entre nodos durante el proceso de instalación.

6. FASE DE CONFIGURACIÓN

Durante la fase de instalación del software, un administrado autorizado debe hacer uso de la herramienta *Platform Installation Wizard* para asegurar una configuración inicial básica correcta. La descripción detallada de este proceso se encuentra en las guías de referencia en [1].

Durante este proceso de configuración básica se deben configurar las siguientes credenciales que se utilizarán para la configuración y gestión de la solución de forma segura:

- Credencial de Administrador: Nombre de Usuario Administrador y Contraseña.
- Credencial de Aplicación: Nombre de Usuario de Aplicación y Contraseña.
- Contraseña de Seguridad de la solución. La solución utiliza esta contraseña para autorizar la comunicación entre los diferentes nodos de la solución, está contraseña debe ser idéntica en todos los nodos de la solución.

Las contraseñas anteriores deben cumplir los requisitos de complejidad para ser catalogada como segura:

- Deben comenzar por un carácter alfanumérico.
- Deben de tener al menos 14 caracteres.
- Pueden contener caracteres alfanuméricos, guion medio o guion bajo.

6.1 MODO DE OPERACIÓN SEGURO

Para una total seguridad la solución, ésta debe ejecutarse en el modo de operación seguro, activando el modo *Common Criteria* en todos y cada uno de los nodos de la solución.

Para ello es necesario activar previamente el modo FIPS (*Federal Information Processing Standards*) en todos los nodos de la solución.

Para activar el modo FIPS, hay que proceder como sigue.

Desde una sesión CLI hay que introducir el siguiente comando:

```
utils fips enable
```

```
[Enter Yes]
```

El nodo se reiniciará automáticamente como parte del proceso de activación.

Para verificar que se ha activado correctamente hay que utilizar el comando siguiente:

```
utils fips status
```

Con este comando el nodo en cuestión regenera los siguientes certificados: *CallManager, Tomcat, IPSec, TVS, CAPF, SSH, ITLRecovery*.

Además, todos los certificados firmados por una CA externa, si los hay, tendrán que ser regenerados y cargados en el nodo de nuevo.

Una vez activado el modo FIPS, hay que proceder con activar el modo *Common Criteria*. Este modo de operación permite a la solución cumplir con la certificación funcional *Common Criteria*.

En el modo *Common Criteria* se requieren certificados X.509 v3 que permiten conexiones seguras TLS 1.2.

Desde los clientes remotos, para activar TLS proceder como sigue:

(1) Instalar Soap UI versión 5.2.1

(2) Para Microsoft Windows:

a. Navegar a `C:\Program Files\SmartBear\SoapUI-5.2.1\bin`

b. Editar el fichero `SoapUI-5.2.1.vmoptions` para añadir:

`-Dsoapui.https.protocols=TLSv1.2,TLSv1,SSLv3`

(3) Para Linux:

a. Editar el fichero `bin/soaup.sh` para añadir:

`JAVA_OPTS="$JAVA_OPTS -Dsoapui.https.protocols=SSLv3,TLSv1.2"`

(4) Para OSX:

a. Navegar a `/Applications/SoapUI-{VERSION}.app/Contents`

b. Editar el fichero `moptions.txt` para añadir:

`-Dsoapui.https.protocols=TLSv1.2,TLSv1,SSLv3`

(5) Reiniciar la herramienta `SoapUI`

Para activar el modo *Common Criteria*, hay que proceder como sigue.

Desde una sesión CLI hay que introducir el siguiente comando:

```
utils fips_common_criteria enable
```

`[Enter Yes]`

Todos los requisitos, condicionantes, dependencias y restricciones de cómo realizar este proceso y del modo *Common Criteria* en sí mismo se encuentran en detalle en la referencia [4], capítulo *FIPS Mode Setup*.

6.2 AUTENTICACIÓN Y CIFRADO (ENCRIPTACIÓN)

La solución CUCM utiliza los siguientes mecanismos de autenticación.

- Autenticación de las imágenes de software de los terminales de comunicación (*Cisco Unified* IP Phones principalmente) de la solución.

  Se basa en la firma de los ficheros binarios que se instalan de forma automática durante el proceso de instalación del sistema *Cisco Unified Communications Manager*, y de los que son descargados e instalados posteriormente desde la web de Cisco.

- Autenticación de Ficheros, basada en la firma digital que permite validar todo tipos de ficheros que se utilizan en la solución, como son ficheros de configuración de los teléfonos, ficheros que contienen tonos de llamada, idioma del terminal, ficheros CTL (que contiene la lista de certificados de confianza), etc.

  El proceso de descarga de dichos ficheros siempre es mediante el servicio de TFTP que corre en los nodos de CUCM, y es el encargado de la firma de los ficheros.

- Autenticación de la Señalización que verifica la integridad de la señalización, basada en ficheros que contienen un listado de certificados de confianza, llamado *Certificate Trust List* (CTL), y el protocolo TLS.

- Autenticación de los dispositivos remotos (*Cisco Unified* IP Phones, troncales SIP, o aplicaciones JTAPI/TAPI/CTI), basado en el intercambio y aceptación de certificados digitales entre los servidores CUCM y los remotos.

  Se crea un fichero *CiscoCTL* (que permite autenticar tanto a nivel de nodo CUCM como a nivel de aplicación) por un lado, y el proceso basado en *Certificate Authority Proxy Function* (CAPF) que permite autenticar terminales y aplicaciones JTAPI/TAPI/CTI) por otro lado.

- Autenticación *Digest* para los troncales SIP y terminales SIP. Basado en credenciales *digest*, similares a las credenciales tipo nombre de usuario y contraseña.

Desde el punto de vista de los usuarios finales de la solución, todas las credenciales de inicio de sesión se cifran con SHA2.

Para una completa seguridad en las comunicaciones que ofrece la solución, los siguientes tipos de tráfico han de cifrarse o encriptarse:

- Tanto para el tráfico de señalización, protocolos SCCP y SIP con el protocolo TLS.
- Protocolos de señalización MGCP y H.323 sobre IPSec.
- Tráfico de media RTP entre destinos finales y con la propia solución CUCM, sobre SRTP.

El CUCM para TLS (SIP) y SRTP soporta el mecanismo de cifrado *Advanced Encryption Standard* (AES) 256 junto con SHA-2 (*Secure Hash Algorithm*), de acuerdo con FIPS (*Federal Information Processing Standards*).

Para TLS 1.2, el soporte de AES 256 y SHA-2 se puede hacer con los siguientes mecanismos de cifrado:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Donde:

- TLS es *Transport Layer Security*
- ECDH es el algoritmo *Elliptic curve Diffie–Hellman*
- RSA es el algoritmo *Rivest Shamir Adleman*
- AES es *Advanced Encryption Standards*
- GCM es *Galois/Counter Mode*

Además de lo anterior, el CUCM soporta TLS_RSA_WITH_AES_128_CBC_SHA.

El uso de RSA con clave de 2048 bits se permite para ENS Alto cuando el nivel de amenaza es Bajo, para lo cual en el canal de administración se imponen restricciones para reducir la amenaza, tales como el uso de TLS trusted path/channels.

Los mecanismos de cifrado han de utilizar certificados firmados por una autoridad de certificación (CA).

En este sentido, la solución CUCM utiliza dos tipos de certificados:

- Certificados auto firmados por el propio CUCM, para su uso propio ó para el uso en nombre de terceros (terminales teléfonos principalmente). Esto último lo hace con la función *Certificate Authority Proxy Function* (CAPF).
- Certificados firmados por una tercera autoridad certificadora (CA). Esto se hace mediante la generación de un *Certificate Signing Request* (CSR), que dicha CA puede firmar.

  Es recomendable utilizar este tipo de certificados (firmados por una CA) cuando las comunicaciones van más allá de la frontera interior del firewall de la organización.

Los certificados firmados por una CA externa requieren de la configuración de los mismos en la solución CUCM.

Para ello, si queremos conectar un sistema remoto utilizando un certificado firmado por una CA externa se ha de realizar lo siguiente:

- Instalar en la lista de certificados de confianza del CUCM la cadena del certificado raíz de dicha CA.
- Instalar en la lista de certificados de confianza del CUCM el certificado firmado por la CA externa que utilizará el sistema remoto.

Si además queremos que el CUCM utilice certificados firmados por una CA externa, hay que realizar los pasos anteriores, pero generando antes de nada un CSR desde el CUCM para que la autoridad certificadora lo firme.

En el CUCM existen los siguientes tipos de listas de certificados de confianza, que usa la solución para diferentes propósitos:

- *Common Trust Store* utilizado para Tomcat y aplicaciones web
- IPSec-trust
- CAPF-trust
- Userlicensing-trust
- TVS-trust
- Phone-SAST-trust
- Phone-CTL-trust

La documentación en detalle de configuración, requisitos y limitaciones sobre de autenticación y cifrado de la solución se encuentra en **[4].**

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

La gestión local básica del sistema operativo de cada uno de los nodos se hace mediante SSH, estando el protocolo TELNET desactivado por seguridad.

El principal mecanismo de gestión de la solución es mediante un navegador desde una estación remota. Esta conexión utiliza el protocolo *Hypertext Transfer Protocol over Secure Sockets Layer* (SSL), junto con los certificados Tomcat instalados en la solución. El protocolo HTTP está desactivado por defecto en la solución, y totalmente bloqueado a partir de la versión 12.5SU7.

La solución CUCM soporta SSL y TLS para las conexiones HTTPS. Cisco recomienda TLS en lugar de SSL para la gestión web.

Las siguientes aplicaciones dentro de la solución CUCM soportan HTTPS:

- ccmadmin – Administración del CUCM
- ccmservice – *Cisco Unified Serviceability*

- cmplatform – Administración del sistema operativo
- cmuser – *Cisco Personal Assistant*
- ast – *Real Time Monitoring Tool*
- RTMTReports – *Real Time Monitoring Tool* generación de reportes
- PktCap – Herrmienta de reolución de problemas de Cisco TAC (como por ejemplo captura de tráfico de paquetes).
- art – Análisis y reports de CDRs.
- taps – *Unified Communications Manager Auto-Register Phone Tool*
- dna – Analizador de marcación
- drf – *Disaster Recovery System*
- SOAP – *Simple Object Access Protocol* API para la lectura y escritura en las bases de datos del CUCM.

  Por motivos de seguridad todas las aplicaciones que utilizan SOAP requieren HTTPS, no es posible el uso de HTTP.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

Durante el proceso de instalación descrito en la referencia [1], en paso *Administrator Login Configuration* se configura el usuario administrador de la solución.

La contraseña del usuario de administración tiene que cumplir con los requisitos de complejidad para ser catalogada como segura. Debe comenzar por un carácter alfanumérico, debe de tener al menos 14 caracteres, y pueden contener caracteres alfanuméricos, guion medio ó guion bajo.

Por otro lado, las políticas de seguridad del resto de cuentas de usuario final se pueden configurar desde el GUI del CUCM, en *User management* >> *User settings* >> *Credential Policy*

También es posible comprobar el estado de bloqueo de una cuenta, desde el CLI con el siguiente comando:

```
show accountlocking
```

En caso de estar bloqueada y se desee desbloquear, se debe utilizar el siguiente comando desde el CLI:

```
set accountlocking enable
```

Desde el CLI también se puede configurar los intentos de *login* y la duración del bloqueo con los siguientes comandos:

```
set accountlocking count _
set accountlocking unlocktime seconds
```

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

El uso de los puertos TCP y UDP por la solución CUCM se organiza en las siguientes categorías:

- Puertos intracluster entre los diferentes nodos CUCM.
- Puertos para Servicios comunes (*Common Service*).
- Puertos entre el CUCM y el servidor LDAP.
- Tráfico web desde los usuarios de administración o usuarios finales del CUCM.
- Tráfico web desde el CUCM y los teléfonos IP.
- Tráfico de señalización, de media y otros flujos de tráfico entre el CUCM y los teléfonos IP.
- Tráfico de señalización, de media y otros flujos de tráfico entre el CUCM y *gateways*.
- Comunicaciones entre aplicaciones y el CUCM.
- Comunicaciones entre clientes CTL y firewalls.

La lista detallada, con el número de puerto, y la descripción de estos se encuentra en la referencia **[7],** capítulo "*Cisco Unified Communications Manager TCP and UDP Port Usage*".

6.5 SERVIDORES DE AUTENTICACIÓN

La solución CUCM soporta *Security Assertion Markup Language Single Sign-On* (SAML SSO).

El detalle de su configuración se encuentre en la referencia [8]. Esta guía contiene una revisión global de la solución, los requisitos necesarios para su implementación y el detalle de su configuración.

6.6 SINCRONIZACIÓN

Cisco recomienda el uso de servidores NTP para la sincronización correcta del reloj en la solución (nodo principal de la solución o *Publisher*). El *Publisher* a su vez proporcionará la sincronización, igualmente mediante NTP al resto de servidores de la solución (*Cluster*).

Para ello, durante la fase de instalación del software, mediante la herramienta *Platform Installation Wizard* (descripción detallada de este proceso se encuentra en la referencia [1]), se deben configurar los servidores NTP que usará la solución.

Cisco recomienda la configuración de al menos tres servidores NTP.

6.7 ACTUALIZACIONES

Las diferentes opciones de actualización de la solución se detallan en la referencia [9].

6.8 ALTA DISPONIBILIDAD

La guía completa de la capacidad de alta disponibilidad y redundancia de la solución CUCM se encuentra en la referencia [10].

6.9 AUDITORÍA

El CUCM realiza auditorías de seguridad en el Sistema Operativo, Bases de Datos y el resto de software de aplicación; resultando en los siguientes registros de eventos:

- Linux auditd log.
- Unified CM Application audit log.
- Informix database audit log.

El detalle del funcionamiento de estos logs se encuentra en la referencia [6], capítulo "*Audit Logs*".

En esta misma referencia se detalla como configurar un servidor remoto de *syslog*, capítulo "*Alarms*".

6.10 BACKUP

Cisco recomienda realizar copias de seguridad de la solución de forma periódica.

El procedimiento para realizar dichas copias de seguridad se encuentra detallado en la referencia [11], capítulo "*Disaster Recovery*".

6.11 FUNCIONES DE SEGURIDAD

El CUCM permite cumplir con los siguientes (incluidos, pero no limitados) requisitos de seguridad (*infosec*):

- Definición de políticas de contraseñas.

  Todas las políticas de contraseñas y PINs se almacenan de forma cifrada y encriptada.

- Políticas de bloqueo de cuentas y credenciales.
- Configuración del mensaje de aviso y consentimiento en el inicio de sesión **(***login banner*).

- Protocolos TLS/SRTP para el tráfico de señalización y de media.
- Configuraciones de refuerzo de la seguridad de los teléfonos IP.
- IPSec para securizar conexiones que no utilicen TLS.
- Utilización de una CA externa para la firma de certificados PKI en lugar de los auto-firmados.
- Activación del modo FIPS o el modo *Common Criteria*.
- Activación de SAML para *single sign-on*, incluyendo soporte de lectores de *smart cards* y *bio-metric*.
- Mostrar todas las conexiones de red, procesos y paquetes activos.

  El siguiente comando muestra el detalle de los puertos abiertos, equivalente a "*netstat -an*" en Unix.

```
show network status detail all nodns
```

  El siguiente comando muestra la lista de todos los procesos e información crítica de los mismos, equivalente a "*ps -ef*" en Unix.

```
show process list detail
```

  El siguiente comando muestra el nombre y versión de los paquetes activos en el Sistema Operativo.

```
show packages active
```

Todos los detalles de la configuración de seguridad de la solución se encuentran en la referencia [4].

Las soluciones CUCM son regularmente testeadas y validadas para cumplir con certificaciones gubernamentales como:

- Department of Defense Information Network Approved Products List (DoDIN APL)
- FIPS 140-2 Level 1
- FedRAMP
- Common Criteria
- Applicable U.S. Department of Defense Security Technical Implementation Guides (STIGs)

7. FASE DE OPERACIÓN

Durante la fase de operación del equipo, el administrador debe llevar a cabo las siguientes tareas de mantenimiento:

- Mantenimiento del control de acceso al equipo.
- Comprobaciones periódicas del hardware y software para asegurar que no se ha introducido hardware o software no autorizado.
- Seguir las alertas de seguridad de Cisco (*Security Advisories*) que publica periódicamente y, si es necesario, aplicar un parche.
- Mantenimiento de los registros de auditoría. Estos registros estarán protegidos contra borrados y modificaciones no autorizados, y solamente el personal de seguridad autorizado podrá acceder a ellos.

8. REFERENCIAS

[1] Guías de Instalación
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html

[2] «*Smart Licensing Deployment Guide*»
https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html

[3] Guias de Configuración
Para versión 12, disponible en:
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-version-12-5/model.html#Configuration
Para versión 14, disponible en:
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-version-14/model.html

[4] «*Security Guide for Cisco Unified Communications Manager*»
Para versión 12, disponible en:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/12_5_1_SU1/cucm_b_security-guide-125SU1/cucm_b_security-guide-for-cisco-unified125SU1_chapter_011011.html
Para versión 14, disponible en:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/14SU2/cucm_b_security-guide-14su2.html

[5] *«Cisco Unified CDR Analysis and Reporting Administration Guide»*
Para versión 12, disponible en:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/12_5_1/Car/cucm_b_cdr-analysis-reporting-admin-guide-1251/cucm_b_cdr-analysis-reporting-admin-guide-1251_chapter_010.html

[6] Para versión 12, disponible en:
«Cisco Unified Serviceability Administration Guide»
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1SU1/cucm_b_serviceability-admin-guide-1251su1/cucm_b_serviceability-admin-guide-1251su1_chapter_0111.html
Para versión 14, disponible en:
«Administration Guide for Cisco Unified Communications Manager»
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/14SU2/adminGd/cucm_b_administration-guide-14su2/cucm_b_test-adminguide_chapter_010100.html

[7] *«System Configuration Guide for Cisco Unified Communications Manager»*
Para versión 12, disponible en:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1SU3/systemConfig/cucm_b_system-configuration-guide-1251su3/cucm_m_tcp-and-udp-port-usage-12-0.html
Para versión 14, disponible en:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/14/systemConfig/cucm_b_system-configuration-guide-14su2.html

[8] *«SAML SSO Deployment Guide for Cisco Unified Communications Applications»*
Para versión 12, disponible en:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/SAML_SSO_deployment_guide/12_5_1/cucm_b_saml-sso-deployment-guide-12_5/cucm_b_saml-sso-deployment-guide-1201_preface_00.html
Para versión 14, disponible en:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/SAML_SSO_deployment_guide/14/cucm_b_saml-sso-deployment-guide-Release-14.html

[9] *«Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service»*
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html

[10] *«Cisco Collaboration Solutions Design Guidance»*
Disponible en:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/UCgoList.html

[11] *«Administration Guide for Cisco Unified Communications Manager»*
Para versión 12, disponible en:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1SU6/adminGd/cucm_b_administration-guide-1251su6/cucm_b_test-adminguide_chapter_01010.html
Para versión 14, disponible en:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/14SU2/adminGd/cucm_b_administration-guide-14su2/cucm_b_test-adminguide_chapter_010100.html

9. ABREVIATURAS

AAA	Administration, Authorization, and Accounting
AES	Advanced Encryption Standard
CLI	Command Line Interface
CM	Configuration Management
CSR	Certificate Signing Request
CSSM	Cisco Smart Software Manager
CUCM	Cisco Unified Communications Manager
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
ESA	Email Security Appliance
ENS	Esquema Nacional de Seguridad.
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Trasfer Protocol
HTTPS	Hypertext Trasfer Protocol Secure
ICMP	Internet Control Message Protocol
IMAP4S	Internet Message Protocol Secure version 4
IMC	Integrated Management Controller
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
NDcPP	collaborative Network Device Protection Profile
NTP	Network Time Protocol
OS	Operating System
POST	Power On Self Test
PP	Protection Profile
RADIUS	Remote Authenticatio Dial in User Service
RSA	Rivest, Shamir and Adleman
SCP	Secure Copy Protocol
SMTP	Simple Mail Transfer Protocol
SMTPS	Simple Mail Transfer Protocol over TLS
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TCP	Transport Control Protocol
TCP/IP	Transport Control Protocol/ Internet Protocol
TLS	Transport Layer Security
TFTP	Trivial File Transfer Protocol
UCS	Unified Computing System

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL