Guía de administración del teléfono IP 8832 para conferencias de Cisco para Cisco Unified Communications Manager

Primera publicación: 2017-09-15

Última modificación: 2023-06-16

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

LAS ESPECIFICACIONES E INFORMACIÓN RELATIVAS A LOS PRODUCTOS DE ESTE MANUAL ESTÁN SUJETAS A CAMBIOS SIN PREVIO AVISO. TODAS LAS DECLARACIONES, INFORMACIONES Y RECOMENDACIONES INCLUIDAS EN ESTE MANUAL SE CONSIDERAN PRECISAS; SIN EMBARGO, NO SE PRESENTAN GARANTÍAS DE NINGÚN TIPO, NI EXPRESAS NI IMPLÍCITAS. LOS USUARIOS DEBEN ASUMIR LA PLENA RESPONSABILIDAD DE SU APLICACIÓN EN TODOS LOS PRODUCTOS.

LA LICENCIA DE SOFTWARE Y LA GARANTÍA LIMITADA DEL PRODUCTO AL QUE ACOMPAÑAN SE EXPONEN EN EL PAQUETE DE INFORMACIÓN QUE SE ENVÍA CON EL PRODUCTO Y SE INCLUYEN EN EL PRESENTE DOCUMENTO A TRAVÉS DE ESTA REFERENCIA. SI NO ENCUENTRA LA LICENCIA DEL SOFTWARE O LA GARANTÍA LIMITADA, PÓNGASE EN CONTACTO CON SU REPRESENTANTE DE CISCO PARA OBTENER UNA COPIA.

La siguiente información concierne al cumplimiento de los requisitos de la FCC para los dispositivos de Clase A: este equipo ha sido probado y cumple con los límites establecidos para un dispositivo digital de Clase A, de conformidad con el apartado 15 del reglamento de la FCC. Estos límites están diseñados para proporcionar una protección razonable frente a cualquier interferencia perjudicial al utilizar el equipo en un entorno comercial. Este equipo genera, usa y puede emitir energía de radiofrecuencia y, en caso de no instalarse ni usarse de conformidad con el manual de instrucciones, podría causar interferencias perjudiciales que dificultarían las comunicaciones por radio. La conexión de este equipo en una zona residencial puede provocar interferencias perjudiciales; en tal caso, se exigirá a los usuarios que corran con los gastos de la reparación de dichos daños.

La siguiente información concierne al cumplimiento de los requisitos de la FCC para los dispositivos de Clase B: este equipo ha sido probado y cumple con los límites establecidos para un dispositivo digital de Clase B, de conformidad con el apartado 15 del reglamento de la FCC. Estos límites han sido diseñados con el objetivo de proporcionar una protección razonable frente a interferencias perjudiciales en instalaciones residenciales. Este equipo genera, usa y puede emitir energía de radiofrecuencia y, en caso de no instalarse ni usarse de conformidad con las instrucciones, podría causar interferencias perjudiciales que dificultarían las comunicaciones por radio. Sin embargo, no es posible garantizar que no vayan a producirse interferencias en una instalación determinada. Si el equipo causa interferencias en la recepción de señales de radio o televisión (lo que se puede determinar apagando y encendiendo el equipo), se recomienda a los usuarios que intenten corregir las interferencias mediante uno o varios de los métodos que se indican a continuación:

- Reoriente o reubique la antena receptora.
- Aumente la distancia entre los equipos y el receptor.
- Conecte el equipo a una toma en un circuito diferente al que se encuentra conectado el receptor.
- Solicite ayuda al distribuidor o a un técnico experto en radio y televisión.

Las modificaciones realizadas en el producto que no estén autorizadas por Cisco podrían anular la aprobación de la FCC y negarle el permiso para utilizar el producto.

La implementación por parte de Cisco de la compresión del encabezado de TCP es una adaptación de un programa desarrollado por la Universidad de California, Berkeley (UCB) como parte de la versión de dominio público del sistema operativo UNIX de la UCB. Todos los derechos reservados. Copyright © 1981, Regentes de la Universidad de California.

NO OBSTANTE CUALQUIER OTRA GARANTÍA QUE AQUÍ SE DESCRIBA, TODOS LOS ARCHIVOS DE DOCUMENTO Y SOFTWARE DE ESTOS PROVEEDORES SE PROPORCIONAN "TAL CUAL" CON TODOS LOS ERRORES QUE PUDIERAN INCLUIR. CISCO Y LOS PROVEEDORES ANTERIORMENTE MENCIONADOS NIEGAN CUALQUIER GARANTÍA, EXPRESA O IMPLÍCITA, INCLUIDAS, SIN LIMITACIÓN, AQUELLAS DE COMERCIABILIDAD, ADECUACIÓN A UN FIN DETERMINADO E INCUMPLIMIENTO O QUE PUEDAN SURGIR DE UN PROCESO DE NEGOCIACIÓN, USO O PRÁCTICA COMERCIAL.

BAJO NINGUNA CIRCUNSTANCIA CISCO O SUS PROVEEDORES SERÁN RESPONSABLES DE NINGÚN DAÑO INDIRECTO, ESPECIAL, SECUNDARIO O FORTUITO, INCLUIDOS ENTRE OTROS, LA PÉRDIDA DE GANANCIAS, O LA PÉRDIDA O EL DAÑO DE DATOS COMO CONSECUENCIA DEL USO O INCAPACIDAD DE USO DE ESTE MANUAL, INCLUSO EN EL CASO DE QUE CISCO O SUS PROVEEDORES HAYAN SIDO NOTIFICADOS SOBRE LA POSIBILIDAD DE QUE SE PRODUZCAN TALES DAÑOS.

Cualquier dirección de protocolo de Internet (IP) o número de teléfono utilizado en este documento no pretende ser una dirección o un número de teléfono real. Cualquier ejemplo, salida de visualización de comandos, diagrama de topología de red y figura incluida en el documento se muestra solo con fines ilustrativos. El uso de direcciones IP o números de teléfono reales en el material ilustrativo no es intencionado, sino mera coincidencia.

Se carece de control sobre todas las copias impresas y duplicados en formato electrónico de este documento. Consulte la versión en línea actual para obtener la versión más reciente.

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones y los números de teléfono están disponibles en el sitio web de Cisco: www.cisco.com/go/offices.

Cisco y el logo de Cisco son marcas comerciales o marcas registradas de Cisco y sus filiales en EE.UU. y otros países. Para ver una lista de las marcas comerciales de Cisco, diríjase al siguiente enlace: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Las marcas comerciales de terceros mencionadas son propiedad de sus respectivos dueños. El uso de la palabra socio no implica una asociación entre Cisco y cualquier otra empresa. (1721R)

CONTENIDO

CAPÍTULO 1

Información nueva y modificada

Información nueva y modificada para la versión de firmware 14.2(1)

La siguiente información es nueva o se ha modificado para la versión de firmware 14.2 (1).

Función	Novedades o cambios
Compatibilidad con SIP OAuth en SRST	Mejoras de seguridad para la red del teléfono, en la página 74

Información nueva y modificada para la versión de firmware 14.1(1)

La siguiente información es nueva o se ha modificado para la versión de firmware 14.1(1).

Función	Novedades o cambios
Soporte de SIP OAuth para Proxy TFTP	Mejoras de seguridad para la red del teléfono, en la página 74

Función	Novedades o cambios
Migración de teléfono sin carga de transición	Migración del teléfono a un teléfono multiplataforma directamente, en la página 96

Información nueva y modificada para la versión de firmware 14.0(1)

Tabla 1: Información nueva y modificada

Función	Novedades o cambios
Mejora en la supervisión de aparcamiento de llamadas	Configuración específica del producto, en la página 100
Mejoras en OAuth de SIP	Mejoras de seguridad para la red del teléfono, en la página 74
Mejoras en OAuth para MRA	Mobile and Remote Access mediante Expressway, en la página 121
Mejoras de la interfaz de usuario	Survivable Remote Site Telephony, en la página 64

A partir de la versión de firmware 14.0, los teléfonos admiten DTLS 1.2. DTLS 1.2 necesita Cisco Adaptive Security Appliance (ASA) versión 9.10 o posterior. La versión mínima de DTLS se configura para una conexión VPN en ASA. Para obtener más información, consulte *Libro de ASDM 3: Guía de configuración de Cisco ASA serie VPN* en https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

Información nueva y modificada para la versión de firmware 12.8(1)

La siguiente información es nueva o se ha modificado para la versión de firmware 12.8 (1).

Función	Contenido nuevo o modificado
Migración de datos del teléfono	Cambiar el modelo de teléfono de un usuario, en la página 53
Agregar información adicional sobre el campo de acceso web	Configuración específica del producto, en la página 100

Información nueva y modificada para la versión de firmware 12.7(1)

No se necesitan actualizaciones de la guía de administración para la versión de firmware 12.7(1).

Información nueva y modificada para la versión de firmware 12.6(1)

No se necesitan actualizaciones de la guía de administración para la versión de firmware 12.6(1).

Información nueva y modificada para la versión de firmware 12.5(1)SR3

Todas las referencias de la documentación de Cisco Unified Communications Manager se han actualizado para incluir todas las versiones de Cisco Unified Communications Manager.

Tabla 2: Revisiones de la Guía de administración del teléfono IP 8832 de Cisco para la versión de firmware 12.5(1)SR3

Revisión	Sección actualizada
Compatibilidad con la incorporación de código de activación y Mobile and Remote Access	Incorporación de código de activación y Mobile and Remote Access, en la página 29
Compatibilidad con el uso de la herramienta de informe de problemas desde Cisco Unified Communications Manager.	Crear un informe de problemas de teléfono desde Cisco Unified Communications Manager, en la página 169

Información nueva y modificada para la versión de firmware 12.5(1)SR2

No se necesitan actualizaciones de la guía de administración para la versión de firmware 12.5(1)SR2.

La versión de firmware 12.5(1)SR2 sustituye las versiones 12.5(1) y 12.5(1)SR1. Las versiones de firmware 12.5(1) y 12.5(1)SR1 se han sustituido por la versión 12.5(1)SR2.

Información nueva y modificada para la versión de firmware 12.5(1)SR1

En la tabla siguiente se describen los cambios realizados en la *Guía de administración del teléfono IP para conferencias 8832 de Cisco para Cisco Unified Communications Manager* en relación con la compatibilidad con la versión de firmware 12.5(1)SR1.

Tabla 3: Revisiones de la Guía de administración del teléfono IP 8832 para conferencias de Cisco para la versión de firmware 12.5(1)SR1.

Revisión	Sección nueva o actualizada
Compatibilidad con curva elíptica	Características de seguridad admitidas, en la página 75

Información nueva y modificada para la versión de firmware 12.5(1)

En la tabla siguiente se describen los cambios realizados en la *Guía de administración de Teléfonos IP para conferencias 8832 de Cisco para Cisco Unified Communications Manager* en relación con la compatibilidad con la versión de firmware 12.5(1).

Tabla 4: Revisiones de la Guía de administración del teléfono IP 8832 para conferencias de Cisco para la versión de firmware 12.5(1).

Revisión	Sección nueva o actualizada
Compatibilidad con la mensajería silenciosa en Cisco Unified Communications Manager Express	Interacción con Cisco Unified Communications Manager Express, en la página 23
Compatibilidad para desactivar los cifrados TLS	Configuración específica del producto, en la página 100
Mejora de la compatibilidad con la marcación en bloque para el temporizador entre dígitos T.302.	Configuración específica del producto, en la página 100

Información nueva y modificada para la versión de firmware 12.1(1)

En la tabla siguiente se describen los cambios realizados en la *Guía de administración de teléfono IP 8832 para conferencias de Cisco para Cisco Unified Communications Manager* en relación con la compatibilidad con la versión de firmware 12.1(1).

Revisión	Sección nueva o actualizada
Compatibilidad con Inyector PoE de teléfono IP 8832 para conferencias de Cisco	• Requisitos de alimentación del teléfono, en la página 18 • Formas de proporcionar alimentación al teléfono para conferencias, en la página 33 • Instalación del teléfono para conferencias, en la página 31
Compatibilidad con micrófonos inalámbricos	• Teléfono IP 8832 para conferencias de Cisco, en la página 9 • Micrófono de expansión inalámbrico (8832 solo), en la página 13 • Instalación de micrófonos de expansión inalámbricos, en la página 36 • Instalación de la base de carga del micrófono inalámbrico, en la página 37
Compatibilidad con conexión en cadena	• Teléfono IP 8832 para conferencias de Cisco, en la página 9 • Modo de conexión en cadena, en la página 31 • Instalación del teléfono para conferencias en modo de conexión en cadena, en la página 38 • Un teléfono en modo de conexión en cadena no funciona, en la página 168
Compatibilidad con Inyector Ethernet No PoE de teléfono IP 8832 para conferencias de Cisco	• Instalación del teléfono para conferencias, en la página 31 • Formas de proporcionar alimentación al teléfono para conferencias, en la página 33

Revisión	Sección nueva o actualizada
Compatibilidad con Wi-Fi	• Instalación del teléfono para conferencias, en la página 31 • Formas de proporcionar alimentación al teléfono para conferencias, en la página 33 • Establecimiento del campo Nombre de dominio, en la página 46 • Activación de la LAN inalámbrica en el teléfono, en la página 47 • Configuración de la LAN inalámbrica en Cisco Unified Communications Manager, en la página 47 • Configuración de la LAN inalámbrica desde el teléfono, en la página 48 • Establecer el número de intentos de autenticación de WLAN, en la página 50 • Habilitar el modo de mensaje de WLAN, en la página 50 • Configuración de un perfil Wi-Fi mediante Cisco Unified Communications Manager, en la página 51 • Configuración de un grupo Wi-Fi mediante Cisco Unified Communications Manager, en la página 53
Compatibilidad con Mobile and Remote Access mediante Expressway	• Mobile and Remote Access mediante Expressway, en la página 121 • Ejemplos de implementación, en la página 123 • Configuración de credenciales de usuario persistentes para el inicio de sesión de Expressway, en la página 123
Compatibilidad para activar o desactivar TLS 1.2 para el acceso del servidor web.	Configuración específica del producto, en la página 100
Compatibilidad con el códec de audio G722.2 AMR-WB	• Teléfono IP 8832 para conferencias de Cisco, en la página 9 • Campos de Estadísticas de llamadas, en la página 140

PARTE I

Acerca del teléfono IP para conferencias de Cisco

CAPÍTULO 2

Hardware del teléfono IP para conferencias de Cisco

Teléfono IP 8832 para conferencias de Cisco

El Teléfono IP 8832 para conferencias de Cisco y 8832NR mejoran las comunicaciones basadas en las personas. Combina un excelente audio de alta definición (HD) y cobertura de 360 grados para salas de conferencias de tamaño mediano a grande y para directivos. Proporciona una experiencia de sonido para audiófilos con un altavoz dúplex completo de manos libres de audio de banda ancha (G.722) bidireccional. Este teléfono es una solución simple que satisface los desafíos de las salas más diferentes.

Figura 1: Teléfono IP 8832 para conferencias de Cisco

El teléfono para conferencias tiene micrófonos sensibles con una cobertura de 360 grados. Esta cobertura le permite hablar con una voz normal y ser oído claramente a una distancia de hasta 10 pies (3 m). El teléfono

también incluye una tecnología resistente a interferencias de teléfonos móviles y otros dispositivos inalámbricos, lo que garantiza comunicaciones claras sin distracciones. El teléfono proporciona una pantalla color y botones de teclas programables para acceder a las funciones de usuario. Solo con la unidad de base el teléfono proporciona cobertura en una sala de 20 x 20 pies (6,1 x 6,1 m) y un máximo de 10 personas.

Hay disponibles dos micrófonos de expansión con cables para usarse con el teléfono. Al alejar los micrófonos de expansión de la unidad de base se proporciona mayor cobertura en salas de conferencias grandes. Con la unidad de base y los micrófonos de expansión, el teléfono para conferencias proporciona cobertura en una sala de 20 x 34 pies (6,1 x 10 m) y un máximo de 22 personas.

El teléfono también es compatible con un conjunto opcional de dos micrófonos de expansión inalámbricos. Con la unidad de base y los micrófonos de expansión inalámbricos, el teléfono para conferencias proporciona cobertura en una sala de 20 x 40 pies (6,1 x 12,2 m) y un máximo de 26 personas. Para cubrir una sala de 20 x 40 pies (6,1 x 12,2 m), recomendamos que coloque cada micrófono a una distancia máxima de 10 pies (3 m) de la base.

Puede conectar dos unidades base para aumentar la cobertura de una sala. Esta configuración requiere el kit de conexión en cadena opcional y puede admitir dos micrófonos de expansión (ya sea con cables o inalámbricos, pero no una mezcla de los dos tipos). Si utiliza micrófonos inalámbricos con el kit de conexión en cadena, la configuración proporciona cobertura para una sala de hasta 6,1 x 15,2 m y hasta 38 personas. Si utiliza micrófonos con cables con el kit de conexión en cadena, la configuración proporciona cobertura para una sala de hasta 6,1 x 17,4 m y hasta 42 personas.

La versión Teléfono IP 8832NR para conferencias de Cisco (sin radio) no admite los micrófonos de expansión inalámbricos, Wi-Fi o Bluetooth.

Como otros dispositivos, el teléfono IP de Cisco se debe configurar y administrar. Estos teléfonos permiten la codificación y la decodificación de los códecs siguientes:

- G.711 ley A
- G.711 ley Mu
- G.722
- G722.2 AMR-WB
- G.729a/G.729ab
- G.726
- iLBC
- Opus

⚠

Precaución Si se usa un teléfono móvil o GSM o una radio bidireccional muy cerca de un teléfono IP de Cisco, se podrían producir interferencias. Para obtener más datos, consulte la documentación del fabricante del dispositivo que causa las interferencias.

Los teléfonos IP de Cisco proporcionan funciones de telefonía tradicionales, como desvío y transferencia de llamadas, rellamadas, marcación rápida, llamadas de conferencia y acceso a sistemas de mensajería de voz. Los teléfonos IP de Cisco también ofrecen otras funciones.

Como ocurre con otros dispositivos de red, debe configurar los teléfonos IP de Cisco a fin de prepararlos para acceder a Cisco Unified Communications Manager y al resto de la red IP. Si usa DHCP, tendrá que hacer

menos ajustes para configurar el teléfono. Sin embargo, si la red lo requiere, puede configurar manualmente datos como una dirección IP, el servidor TFTP o la información de subred.

Los teléfonos IP de Cisco pueden interactuar con otros servicios y dispositivos de la red IP para proporcionar funciones avanzadas. Por ejemplo, puede integrar Cisco Unified Communications Manager con el directorio estándar LDAP3 (protocolo de acceso a directorio ligero 3) a fin de permitir a los usuarios buscar información de contacto de los compañeros de trabajo directamente desde sus teléfonos IP. También puede usar XML para permitir a los usuarios acceder a información como la previsión meteorológica, la bolsa, frases del día y otros datos de Internet.

Por último, dado que el teléfono IP de Cisco es un dispositivo de red, puede obtener información de estado detallada directamente de él. Esta información puede ayudarle a resolver cualquier problema que se puedan encontrar los usuarios al usar los teléfonos IP. También puede obtener estadísticas sobre una llamada activa o sobre las versiones de firmware presentes en el teléfono.

Para poder funcionar en la red de telefonía IP, el teléfono IP de Cisco debe conectarse a un dispositivo de red, como un switch Cisco Catalyst. También debe registrar el teléfono IP de Cisco en un sistema Cisco Unified Communications Manager antes de enviar y recibir llamadas.

Botones y hardware del teléfono IP 8832 para conferencias de Cisco

En las ilustraciones siguientes se muestra el teléfono IP 8832 para conferencias de Cisco.

Figura 2: Botones y características de teléfono IP 8832 para conferencias de Cisco

En la siguiente tabla se describen los botones del teléfono IP 8832 para conferencias de Cisco.

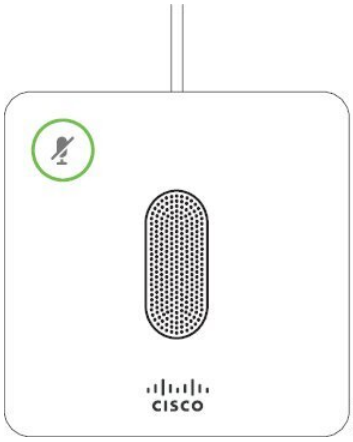
Tabla 5: Botones de teléfono IP 8832 para conferencias de Cisco

1	Barra LED	Indica los estados de las llamadas: • Verde, fijo: llamada activa • Verde, parpadeante: llamada entrante • Verde, intermitente: llamada en espera • Rojo, fijo: llamada silenciada
2	Puerto de micrófono de expansión	El cable del micrófono de expansión con cables se conecta en el puerto.
3	Barra de **Silenciar**	La enciende o apaga el micrófono. Cuando se silencia el micrófono, la barra LED se muestra iluminada en rojo.
4	Botones de teclas programadas	Permite acceder a las funciones y servicios.
5	Barra de navegación y botón de **selección**	Desplácese a través de los menús, resalte los elementos y seleccione el elemento resaltado.
6	Botón **Volumen**	Permite ajustar el volumen del teléfono con altavoz (descolgado) y el volumen del timbre (colgado). Al cambiar el volumen, la barra LED se enciende en blanco para mostrar el cambio de volumen.

Micrófono de expansión con cables (8832 solo)

The Teléfono IP 8832 para conferencias de Cisco admite dos micrófonos de expansión con cables, que están disponibles en un kit opcional. Use los micrófonos de expansión en las salas de mayor tamaño o en una habitación abarrotada. Para obtener los resultados óptimos, se recomienda colocar los micrófonos a una distancia entre 3 pies (0,91 m) y 7 pies (2,1 m) del teléfono.

Figura 3: Micrófono de expansión con cables



Si se encuentra en una llamada, el LED del micrófono de expansión alrededor del botón **Silenciar** se ilumina en verde.

Cuando se silencia el micrófono, la luz LED se ilumina en rojo. Al presionar el botón **Silenciar**, el teléfono y los micrófonos de expansión se silencian.

Temas relacionados

Instalación de los micrófonos de expansión con cables, en la página 35

Micrófono de expansión inalámbrico (8832 solo)

El Teléfono IP 8832 para conferencias de Cisco es compatible con dos micrófonos de expansión inalámbricos, disponibles con una base de carga en un kit opcional. Cuando el micrófono sin cables se coloca en la base de carga para la carga, el LED de la base se ilumina de color blanco.

Figura 4: micrófono inalámbrico

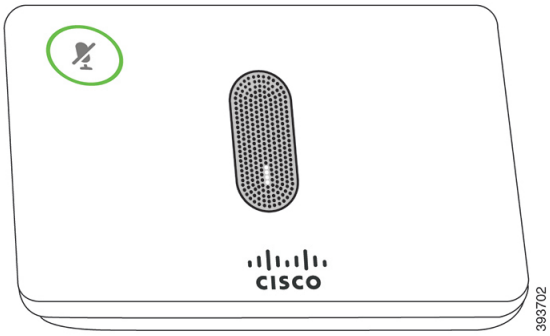
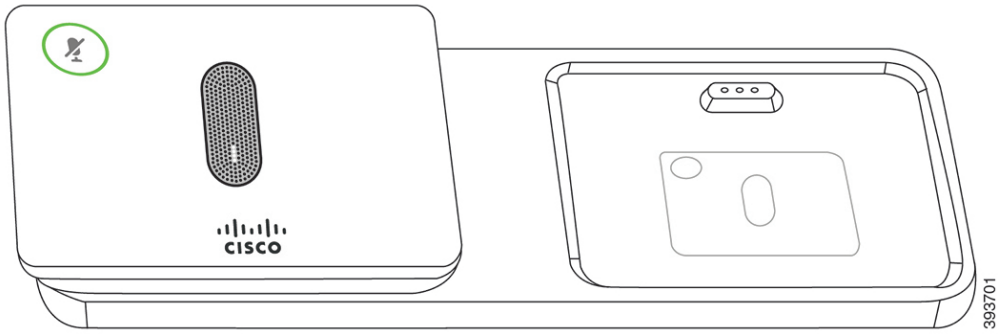


Figura 5: Micrófono inalámbrico montado en la base de carga



Si el teléfono para conferencias se encuentra en una llamada, el LED del micrófono de expansión alrededor del botón **Silenciar** se ilumina en verde.

Cuando el micrófono está silenciado, el LED se ilumina en rojo. Al presionar el botón **Silenciar**, el teléfono y los micrófonos de expansión se silencian.

Si el teléfono se vincula con un micrófono inalámbrico (por ejemplo, el Micrófono inalámbrico 1) y conecta el micrófono inalámbrico a un cargador, al pulsar la tecla programable **Mostrar det.** se indica el nivel de carga de ese micrófono.

Cuando el teléfono se vincula con un micrófono inalámbrico y conecte un micrófono con cables, el micrófono inalámbrico se desvincula y el teléfono se vincula con el micrófono con cables. Aparece una notificación en la pantalla del teléfono que indica que el micrófono con cables está conectado.

Temas relacionados

Instalación de micrófonos de expansión inalámbricos, en la página 36
Instalación de la base de carga del micrófono inalámbrico, en la página 37

Documentación relacionada

Use las secciones siguientes para obtener información relacionada.

Documentación del teléfono IP 8832 para conferencias de Cisco

Busque documentación específica para su idioma, modelo de teléfono y sistema de control de llamadas en la página de asistencia del producto del teléfono IP serie 7800 de Cisco.

Cisco Unified Communications Manager Documentación

Consulte la *Cisco Unified Communications Manager Guía de la documentación* y otras publicaciones específicas de su versión de Cisco Unified Communications Manager. Diríjase a la siguiente URL de documentación:

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

Cisco Unified Communications Manager Express Documentación

Consulte las publicaciones específicas de su idioma, modelo de teléfono y versión de Cisco Unified Communications Manager Express. Diríjase a la siguiente URL de documentación:

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-express/tsd-products-support-series-home.html

Documentación del servicio Cisco Hosted Collaboration

Consulte la *Cisco Hosted Collaboration Solution Guía de la documentación* y otras publicaciones específicas de su versión de Cisco Hosted Collaboration Solution. Diríjase a la siguiente URL:

https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html

Documentación de Cisco Business Edition 4000

Consulte la *Cisco Business Edition 4000 Guía de la documentación* y otras publicaciones específicas de su versión de Cisco Business Edition 4000. Diríjase a la siguiente URL:

https://www.cisco.com/c/en/us/support/unified-communications/business-edition-4000/tsd-products-support-series-home.html

Documentación, asistencia e instrucciones de seguridad

Para obtener información sobre cómo obtener documentación y asistencia, aportar comentarios de la documentación, revisar las instrucciones de seguridad y otros documentos recomendados, así como documentación general de Cisco, consulte el boletín mensual *Novedades de la documentación sobre productos de Cisco*, que también incluye toda la documentación técnica nueva y revisada de Cisco, en:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Suscríbase a *Novedades de la documentación sobre productos de Cisco* como fuente RSS y configure el contenido para que se le envíe directamente al escritorio usando una aplicación de lectura. Las fuentes RSS son un servicio gratuito, y Cisco admite actualmente la versión 2.0 de RSS.

Información general sobre la seguridad de productos de Cisco

Este producto tiene funciones criptográficas y está sujeto a las leyes locales y de EE. UU. sobre importación, exportación, transferencia y uso. El suministro de productos criptográficos de Cisco no otorga a terceros ningún derecho para la importación, exportación, distribución o uso del cifrado. Los importadores, exportadores, distribuidores o usuarios son responsables del cumplimiento de las leyes locales y de Estados Unidos. La utilización de este producto supone la aceptación del cumplimiento de las leyes y las normativas aplicables. Si no es posible cumplir las leyes locales y estadounidenses, deberá devolver el producto de inmediato.

Encontrará más información sobre las normas de exportación de EE. UU. en: https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear.

Diferencias de terminología

En este documento, el término *Teléfono IP de Cisco* incluye el Teléfono IP 8832 para conferencias de Cisco.

En la tabla siguiente se resaltan algunas de las diferencias de terminología de la *Guía del usuario del Teléfono IP 8832 para conferencias de Cisco*, la *Guía de administración de los teléfonos IP 8832 para conferencias de Cisco para Cisco Unified Communications Manager* y de la documentación de Cisco Unified Communications Manager.

Tabla 6: Diferencias de terminología

Guía del usuario	Guía de administración
Indicadores de mensajes	Indicador de mensaje en espera (MWI)
Sistema de correo de voz	Sistema de mensajería de voz

CAPÍTULO 3

Datos técnicos

Especificaciones físicas y ambientales de funcionamiento

En la tabla siguiente se muestran las especificaciones del entorno físico y operativo para el teléfono para conferencias.

Tabla 7: Especificaciones físicas y operativas

Especificación	Valor o intervalo
Temperatura de funcionamiento	De 0 a 40 °C (de 32 a 104 °F)
Humedad relativa de funcionamiento	10% a 90% (sin condensación)
Temperatura de almacenamiento	De –10 a 60 °C (de 14 a 140 °F)
Alto	10,9 pulgadas (278 mm)
Anchura	10,9 pulgadas (278 mm)
Profundidad	2,4 pulgadas (61,3 mm)
Peso	4,07 lb (1852 g)
Alimentación	IEEE PoE clase 3 a través de un inyector PoE. El teléfono es comp con Cisco Discovery Protocol y el protocolo de descubrimiento de Otras opciones incluyen un inyector Ethernet no PoE si los conmut Wi-Fi, se necesita un adaptador de alimentación del teléfono IP 88

Especificación	Valor o intervalo
Funciones de seguridad	Arranque seguro
Cables	USB-C
Requisitos de distancia	La especificación de Ethernet presupone que la longitud máxima del c (330 pies).

Para obtener más información, consulte la *Hoja de datos del teléfono IP 8832 para conferencias de Cisco*: https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/datasheet-listing.html

Requisitos de alimentación del teléfono

El Teléfono IP 8832 para conferencias de Cisco puede utilizar estas fuentes de alimentación:

- Implementación de alimentación a través de Ethernet (PoE) con un Inyector PoE de teléfono IP 8832 para conferencias de Cisco
- Implementación de Ethernet sin PoE con un Inyector Ethernet No PoE de teléfono IP 8832 para conferencias de Cisco
- Implementación de Wi-Fi con un adaptador de alimentación de teléfono IP 8832 para conferencias de Cisco

Tabla 8: Directrices para alimentar el teléfono IP para conferencias de Cisco

Tipo de alimentación	Instrucciones
Alimentación PoE: la proporcionan Inyector PoE de teléfono IP 8832 para conferencias de Cisco o Inyector Ethernet para teléfono IP 8832 para conferencias de Cisco a través del cable USB-C conectado al teléfono.	Si utiliza Inyector PoE de teléfono IP 8832 para conferencias de Cisco o Inyector Ethernet para teléfono IP 8832 para conferencias de Cisco, asegúrese de que el conmutador tenga una fuente de alimentación de reserva para garantizar el funcionamiento ininterrumpido del teléfono. Asegúrese de que la versión de CatOS o IOS que se ejecuta en el conmutador admite la implementación prevista del teléfono. Consulte en la documentación del switch los datos de la versión del sistema operativo. Si va a instalar un teléfono que reciba alimentación por PoE, conecte el inyector a la LAN antes de conectar el cable USB-C al teléfono. Cuando quite un teléfono que use PoE, desconecte el cable USB-C del teléfono antes de quitar la alimentación del adaptador.

Tipo de alimentación	Instrucciones
Alimentación externa • Implementación de Ethernet sin PoE con un Inyector Ethernet No PoE de teléfono IP 8832 para conferencias de Cisco • Implementación de Wi-Fi con un adaptador de alimentación de teléfono IP 8832 para conferencias de Cisco • Implementación de Ethernet sin PoE con un Inyector Ethernet para teléfono IP 8832 para conferencias de Cisco y un adaptador de alimentación de teléfono IP 8832 para conferencias de Cisco	Si va a instalar un teléfono que reciba alimentación con una fuente externa, conecte el inyector a la alimentación y a Ethernet antes de conectar el cable USB-C al teléfono. Cuando quite un teléfono que use alimentación externa, desconecte el cable USB-C del teléfono antes de quitar la alimentación del adaptador.

Interrupción del suministro eléctrico

Para acceder a los servicios de emergencia a través del teléfono es necesario que este reciba energía. En caso de que se produzca una interrupción del suministro eléctrico, no será posible marcar el número del servicio de emergencia hasta que este no se restablezca. Si se produce un fallo o interrupción del suministro eléctrico, puede que sea necesario restablecer o volver a configurar el equipo para poder utilizar la marcación del número del servicio de emergencia.

Reducción del consumo eléctrico

Puede reducir la cantidad de energía que consume el teléfono IP de Cisco con los modos Ahorro de energía o EnergyWise (Power Save Plus).

Ahorro de energía

En el modo Ahorro de energía, la luz de fondo de la pantalla no se ilumina si el teléfono no está en uso. El teléfono permanece en el modo de ahorro de energía durante el tiempo programado o hasta que el usuario presione cualquier botón.

Power Save Plus (EnergyWise)

El teléfono IP de Cisco admite el modo EnergyWise (Power Save Plus) de Cisco. Si la red contiene un controlador de EnergyWise (EW, por ejemplo, un switch de Cisco con esta función activada), puede configurar estos teléfonos para que se suspendan (se apaguen) y se activen (se enciendan) según una programación para reducir aún más el consumo energético.

Configure cada teléfono para activar o desactivar la configuración de EnergyWise. Si EnergyWise está activado, puede configurar una hora de suspensión y activación, así como otros parámetros. Estos parámetros se envían al teléfono como parte del archivo XML de configuración del teléfono.

Temas relacionados

Programación de la función de ahorro de energía para el teléfono IP de Cisco, en la página 113
Programación de EnergyWise en el teléfono IP de Cisco, en la página 114

Protocolos de red

La Teléfono IP 8832 para conferencias de Cisco admite muchos estándares del sector y los protocolos de red de Cisco necesarios para la comunicación por voz. En la tabla siguiente se ofrece una descripción general de los protocolos de red admitidos por los teléfonos.

Tabla 9: Protocolos de red admitidos en los teléfonos IP para conferencias de Cisco

Protocolo de red	Propósito	Notas de uso
Protocolo de arranque-asignación (Bootstrap o BootP)	BootP permite a un dispositivo de red, como un teléfono, descubrir cierta información de inicio, como la dirección IP.	—
Protocolo de descubrimiento de Cisco (CDP)	CDP es un protocolo de descubrimiento de dispositivos que se ejecuta en todos los equipos fabricados por Cisco. Un dispositivo puede usar CDP para anunciar su existencia a otros dispositivos y recibir información sobre los demás dispositivos de la red.	Los teléfonos usan CDP para comunicar informació cada puerto y datos de configuración de calidad de s
Protocolo de configuración dinámica de host (DHCP).	DHCP asigna de forma dinámica una dirección IP a los dispositivos de red. El protocolo DHCP permite conectar un teléfono IP a la red y hacer que el teléfono sea operativo sin necesidad de asignar manualmente una dirección IP ni de configurar parámetros de red adicionales.	DHCP está activado de manera predeterminada. Si subred, la puerta de enlace y el servidor TFTP en ca Se recomienda usar la opción personalizada de DHC un valor de opción. Consulte en la documentación d configuraciones adicionales admitidas de DHCP. **Nota** Si no puede usar la opción 150, use la c
Protocolo de transferencia de hipertexto (HTTP)	HTTP es el protocolo estándar para transferir información y mover documentos por Internet.	Los teléfonos usan HTTP para los servicios XML, e
Protocolo de transferencia de hipertexto seguro (HTTPS)	El protocolo de transferencia de hipertexto seguro (HTTPS) es una combinación del protocolo de transferencia de hipertexto y el protocolo SSL/TLS para proporcionar cifrado y asegurar la identificación de los servidores.	Las aplicaciones web que admiten HTTP y HTTPS la URL HTTPS. Si la conexión con los servicios se realiza mediante
IEEE 802.1X	El estándar IEEE 802.1X define un protocolo de control y autenticación cliente-servidor que impide que los clientes no autorizados se conecten a una LAN mediante los puertos a los que se puede acceder de forma pública. Hasta que el cliente no está autenticado, el control de acceso 802.1X solo permite el tráfico del protocolo de autenticación extensible vía LAN (EAPOL) a través del puerto al que está conectado el cliente. Cuando la autenticación se realiza correctamente, el tráfico normal puede pasar por el puerto.	El teléfono implementa el estándar IEEE 802.1X mec y EAP-TLS. Si la autenticación 802.1X está activada en el teléfo

Protocolo de red	Propósito	Notas de uso
Protocolo de Internet (IP)	IP es un protocolo de mensajería que dirige y envía paquetes por la red.	Para comunicarse con el protocolo IP, los dispos asignadas. Las direcciones IP, las subredes y las identificaci el protocolo de configuración de host dinámica (cada teléfono de forma local. Los teléfonos admiten direcciones IPv6. Para obt Communications Manager.
Protocolo de descubrimiento de capa de enlace (LLDP)	LLDP es un protocolo de descubrimiento de red estandarizado (similar a CDP) que se admite en algunos dispositivos de Cisco y de otros fabricantes.	El teléfono admite LLDP en el puerto PC.
Protocolo de descubrimiento de capa de enlace - dispositivos de terminales de medios (LLDP-MED)	LLDP-MED es una extensión del estándar LLDP desarrollado para los productos de voz.	El teléfono admite LLDP-MED en el puerto SW • Configuración de VLAN de voz • Detección de dispositivos • Administración de la energía • Gestión de inventario. Para obtener más información sobre la compatib *Discovery Protocol* (LLDP-MED y el protocolo https://www.cisco.com/en/US/tech/tk652/tk701/
Protocolo de transporte en tiempo real (RTP)	RTP es un protocolo estándar para el transporte en tiempo real de datos, como voz y vídeo interactivo, a través de redes de datos.	Los teléfonos usan el protocolo RTP para enviar
Protocolo de control en tiempo real (RTCP)	RTCP funciona junto con RTP para proporcionar datos de QoS (como la fluctuación, la latencia o la demora de ida y vuelta) en flujos RTP.	RTCP está activado de manera predeterminada.
Protocolo de descripción de sesión (SDP)	SDP es la porción del protocolo SIP que determina qué parámetros están disponibles durante una conexión entre dos terminales. Las conferencias se establecen mediante el uso exclusivo de las capacidades de SDP que admiten todos los terminales de la conferencia.	Las capacidades de SDP, como los tipos de códec mediante Cisco Unified Communications Manag pueden permitir la configuración de estos parám
Protocolo de inicio de sesión (SIP)	SIP es el estándar de la Internet Engineering Task Force (IETF) para las conferencias multimedia a través de IP. SIP es un protocolo de control de la capa de aplicación basado en ASCII (definido en RFC 3261) que se puede usar para establecer, mantener e interrumpir llamadas entre dos o más terminales.	Al igual que otros protocolos de VoIP, SIP está d dentro de una red de telefonía de paquetes. La se de la red. La administración de sesiones aporta l
Protocolo de transferencia en tiempo real seguro (SRTP)	SRTP es una extensión del perfil de audio y vídeo del protocolo en tiempo real (RTP) y garantiza la integridad de los paquetes de RTP y del protocolo de control en tiempo real (RTCP) al aportar autenticación, integridad y cifrado de los paquetes de medios entre dos terminales.	Los teléfonos usan SRTP para el cifrado de los m

Protocolo de red	Propósito	Notas de uso
Protocolo de control de transmisión (TCP)	TCP es un protocolo de transporte dirigido a la conexión.	Los teléfonos usan TCP para conectarse a Cisco Un
Seguridad de la capa de transporte (TLS)	TLS es un protocolo estándar para asegurar y autenticar las comunicaciones.	Cuando se implementa la seguridad, los teléfono us Communications Manager. Para obtener más datos, Communications Manager.
Protocolo de transferencia de archivos trivial (TFTP)	TFTP permite transferir archivos por la red. En el teléfono, TFTP permite obtener un archivo de configuración específico para el tipo de teléfono.	TFTP requiere que haya un servidor TFTP en la red que el teléfono use un servidor TFTP distinto al esp servidor TFTP mediante el menú Configuración de Para obtener más datos, consulte la documentación
Protocolo de datagramas de usuario (UDP)	UDP es un protocolo de mensajería sin conexión para entregar paquetes de datos.	UDP se usa solo para los flujos RTP. La señalizació

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

Interacción con Cisco Unified Communications Manager Edition

Cisco Unified Communications Manager es un sistema de procesamiento de llamadas abierto estándar del sector. El software de Cisco Unified Communications Manager permite configurar y derribar las barreras de las llamadas entre teléfonos, integrando funciones de centralita tradicionales con la red IP empresarial. Cisco Unified Communications Manager administra los componentes del sistema de telefonía, como los teléfonos, las puertas de enlace de acceso y los recursos necesarios para realizar funciones como conferencias de llamadas y planificación de ruta. Cisco Unified Communications Manager también proporciona lo siguiente:

- Firmware para teléfonos.
- Archivos de lista de confianza de certificado (CTL) y de lista de confianza de identidad (ITL) mediante los servicios TFTP y HTTP.
- Registro del teléfono.
- Conservación de la llamada, para que las sesiones de medios continúen si se pierde la señal entre el administrador de comunicaciones principal y el teléfono.

Para obtener información sobre cómo configurar Cisco Unified Communications Manager para que funcione con los teléfonos descritos en este capítulo, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Nota Si el modelo de teléfono que desea configurar no aparece en la lista desplegable Tipo de teléfono de Administración de Cisco Unified Communications Manager, instale el paquete de dispositivo más reciente para su versión de Cisco Unified Communications Manager que encontrará en Cisco.com.

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

Interacción con Cisco Unified Communications Manager Express

Si el teléfono funciona con Cisco Unified Communications Manager Express (Unified CME), debe pasar al modo CME.

Si un usuario invoca la función de conferencia, la etiqueta permite al teléfono usar un puente de conferencia de hardware local o de red.

Los teléfonos no admiten las acciones siguientes:

- Transferir: solo se admite en caso de transferencia de llamadas conectadas.
- Conferencia: solo se admite en caso de transferencia de llamadas conectadas.
- Conectar: se admite si se usa el botón Conferencia o el acceso mediante rellamada.
- Espera: se admite si se usa el botón Espera.
- Intrusión y conexión: no compatible.
- Transferencia directa: no compatible.
- Seleccionar: no compatible.

Los usuarios no pueden crear llamadas de conferencia ni transferir llamadas entre distintas líneas.

Unified CME admite llamadas de intercomunicación, también conocida como mensajería silenciosa. Pero el teléfono rechaza el mensaje durante las llamadas.

Interacción con el sistema de mensajería de voz

Cisco Unified Communications Manager le permite la integración con distintos sistemas de mensajería de voz, incluido el sistema de mensajería de voz de Cisco Unity Connection. Dado que es posible integrarse con varios sistemas, debe proporcionar a los usuarios información sobre cómo usar su sistema específico.

Para activar la posibilidad de transferir a un usuario al buzón de voz, establezca un patrón de marcación *xxxxx y configúrelo como desvío incondicional al buzón de voz. Para obtener más datos, consulte la documentación de Cisco Unified Communications Manager.

Proporcione la información siguiente a cada usuario:

- Cómo acceder a la cuenta del sistema de mensajería de voz.

  Asegúrese de haber usado Cisco Unified Communications Manager para configurar el botón Mensajes en el teléfono IP de Cisco.

- La contraseña inicial para acceder al sistema de mensajería de voz.

  Configure una contraseña predeterminada del sistema de mensajería de voz para todos los usuarios.

- Cómo indica el teléfono que hay mensajes de voz a la espera.

  Use Cisco Unified Communications Manager para configurar un método indicador de mensajes en espera (MWI).

Archivos de configuración del teléfono

Los archivos de configuración de un teléfono se almacenan en el servidor TFTP y definen los parámetros para conectar con Cisco Unified Communications Manager. En general, siempre que realice un cambio en Cisco Unified Communications Manager que requiera restablecer el teléfono, se realiza un cambio automático en el archivo de configuración del teléfono.

Los archivos de configuración también contienen detalles sobre la carga de imagen que el teléfono debe ejecutar. Si la carga de imagen es distinta a la cargada actualmente en un teléfono, este se pone en contacto con el servidor TFTP para solicitar los archivos de carga necesarios.

Si configura los valores de seguridad en Cisco Unified Communications Manager Administration, el archivo de configuración del teléfono contendrá información confidencial. Para garantizar la privacidad del archivo de configuración, debe configurarlo para el cifrado. Para obtener más datos, consulte la documentación de su versión concreta de Cisco Unified Communications Manager. El teléfono solicita un archivo de configuración siempre que se restablece y se registra en Cisco Unified Communications Manager.

El teléfono accede a un archivo de configuración predeterminado denominado XmlDefault.cnf.xml desde el servidor TFTP cuando se dan las condiciones siguientes:

- Ha activado el registro automático en Cisco Unified Communications Manager
- El teléfono no se ha agregado a la base de datos de Cisco Unified Communications Manager.
- El teléfono se está registrando por primera vez.

Comportamiento del teléfono durante horas de congestión de red

Cualquier circunstancia que degrade el rendimiento de la red puede afectar a la calidad del audio y, en algunos casos, puede provocar que una llamada se interrumpa. Algunas actividades, entre otras, que degradan la red pueden ser:

- Las tareas administrativas, como la exploración de puertos internos o las exploraciones de seguridad.
- Los ataques que pueda recibir la red, como ataques de denegación de servicio.

Interfaz de programación de aplicaciones

Cisco admite la utilización de la API del teléfono por parte de aplicaciones de terceros que han sido probadas y certificadas a través de Cisco por el desarrollador aplicaciones de terceros. Cualquier problema telefónico relacionado con la interacción de aplicaciones no certificadas debe ser resuelto por el tercero y no será atendido por Cisco.

Para el modelo de soporte de las aplicaciones/soluciones de terceros certificadas por Cisco, consulte el sitio web del programa Cisco Solution Partner Program para obtener más detalles.

PARTE II

Instalación del teléfono IP para conferencias de Cisco

CAPÍTULO 4

Instalación del teléfono

Verificación de la configuración de red

A medida que implementan un nuevo sistema de telefonía IP, los administradores del sistema y de la red deben completar varias tareas de configuración inicial a fin de preparar la red para el servicio de telefonía IP. Para obtener información y las listas de comprobación de preparación y configuración de la red de telefonía IP de Cisco, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Para que el teléfono funcione correctamente como terminal en la red, esta debe cumplir unos requisitos concretos. Un requisito es el ancho de banda adecuado. Los teléfonos requieren más ancho de banda que los 32 kbps recomendados al registrarse en Cisco Unified Communications Manager. Tenga en cuenta este requisito de mayor ancho de banda cuando configure el ancho de banda de QoS. Para obtener más información, consulte *Diseños de la red de referencia de la solución (SRND) de Cisco Collaboration System 12.x* o posterior (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.html).

Nota El teléfono muestra la fecha y hora de Cisco Unified Communications Manager. La hora mostrada en el teléfono puede diferir de la de Cisco Unified Communications Manager hasta en 10 segundos.

Procedimiento

Paso 1 Configure una red VoIP que cumpla los requisitos siguientes:

- La VoIP se configura en los routers y gateways.
- Cisco Unified Communications Manager está instalado en la red y configurado para administrar el procesamiento de llamadas.

Paso 2 Configure la red para que admita uno de los elementos siguientes:

- Compatibilidad con DHCP.
- Asignación manual de dirección IP, gateway y máscara de subred.

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

Incorporación de código de activación para los teléfonos internos

Puede utilizar la incorporación del código de activación para configurar rápidamente los nuevos teléfonos sin registro automático. Con este enfoque, controlar el proceso de incorporación del teléfono mediante una de las siguientes acciones:

- Herramienta de administración masiva (BAT) de Cisco Unified Communications
- Interfaz de administración de Cisco Unified Communications Manager
- Servicio web XML administrativo (AXL)

Active esta función desde la sección **Información del dispositivo** de la página de configuración del teléfono. Seleccione **Requerir código de activación de incorporación** si desea que esta función se aplique a un solo teléfono interno.

Los usuarios deben introducir un código de activación antes de que sus teléfonos se puedan registrar. La incorporación del código de activación se puede aplicar a teléfonos individuales, un grupo de teléfonos, o en toda una red.

Este es un método sencillo para que los usuarios incorporen sus teléfonos porque solo introducen un código de activación de 16 dígitos. Los códigos se introducen manualmente o con un código QR si un teléfono tiene una cámara de vídeo. Le recomendamos que utilice un método seguro para proporcionar esta información a los usuarios. Pero si se ha asignado un usuario a un teléfono, esta información está disponible en el Portal de autoayuda. El registro de auditoría registra cuándo un usuario accede al código desde el portal.

Los códigos de activación solo se pueden utilizar una vez y caducan de forma predeterminada después de 1 semana. Si un código de caducidad, deberá proporcionar uno nuevo al usuario.

Encontrará que este enfoque es una forma fácil de mantener la seguridad de su red, ya que un teléfono no puede registrarse hasta que se verifiquen el certificado de fabricación instalado (MIC) y el código de activación. Este método también es una forma cómoda de incorporar teléfonos de forma masiva porque no utiliza la herramienta para la asistencia de teléfonos registrados automáticamente (TAPS) o el registro automático. La tasa de incorporación es un teléfono por segundo o unos 3600 los teléfonos por hora. Pueden añadirse teléfonos con la administración de Cisco Unified Communications Manager, con el servicio web XML de administración (AXL) o con BAT.

Restablecer una vez que se configuran para incorporación del código de activación de teléfonos existentes. No se registran hasta que se introduce el código de activación y se comprueba el micrófono del teléfono. Informe a los usuarios actuales de que va a realizar una transición hacia la incorporación del código de activación antes de implementarla.

Para obtener más información, consulte *Guía de administración de Cisco Unified Communications Manager, IM y Servicio de presencia, versión 12.0(1)* o posterior.

Incorporación de código de activación y Mobile and Remote Access

Puede utilizar la incorporación de código de activación con Mobile and Remote Access al implementar teléfonos IP de Cisco para los usuarios remotos. Esta función es una forma segura de implementar teléfonos externos cuando el registro automático no es necesario. Sin embargo, puede configurar un teléfono para el registro automático cuando las instalaciones y los códigos de activación son locales. Esta función es similar a la incorporación de código de activación para teléfonos internos, pero también permite que el código de activación esté disponible para los teléfonos externos.

La incorporación de código de activación para Mobile and Remote Access requiere Cisco Unified Communications Manager 12.5(1)SU1 o posterior y Cisco Expressway X12.5 o posterior. Las licencias inteligentes también se deben habilitar.

Active esta función en Cisco Unified Communications Manager Administration, pero tenga en cuenta lo siguiente:

- Active esta función desde la sección **Información del dispositivo** de la página de configuración del teléfono.
- Seleccione **Requerir código de activación de incorporación** si desea que esta función se aplique a un solo teléfono interno.
- Seleccione **Permitir código de activación a través de MRA** y **Solicitar código de activación para incorporación** si desea utilizar la incorporación de activación para un único teléfono externo. Si el teléfono está interno, cambia al modo de Mobile and Remote Access y usa Expressway. Si el teléfono no puede acceder a Expressway, no se registrará hasta que no se encuentre fuera de las instalaciones.

Para obtener más información, consulte los siguientes documentos:

- *Guía de administración para Cisco Unified Communications Manager e IM and Presence Service, versión 12.0(1)*
- *Mobile and Remote Access mediante Cisco Expressway* para Cisco Expressway X12.5 o posterior

Activación del registro automático para los teléfonos

El teléfono IP de Cisco requiere Cisco Unified Communications Manager para administrar el procesamiento de llamadas. Consulte la documentación de su versión concreta de Cisco Unified Communications Manager o la ayuda contextual de la administración de ese sistema para asegurarse de que está configurado correctamente para administrar el teléfono y para enrutar y procesar de forma adecuada las llamadas.

Antes de instalar el teléfono IP de Cisco, debe seleccionar un método para agregar teléfonos a la base de datos de Cisco Unified Communications Manager.

Si habilita el registro automático antes de instalar los teléfonos, podrá hacer lo siguiente:

- Agregar teléfonos sin tener que recopilar antes sus direcciones MAC.
- Agregar automáticamente un teléfono IP de Cisco a la base de datos de Cisco Unified Communications Manager al conectar físicamente el teléfono a la red de telefonía IP. Durante el registro automático, Cisco Unified Communications Manager asigna el siguiente número de directorio de la secuencia al teléfono.
- Introducir rápidamente los teléfonos en la base de datos de Cisco Unified Communications Manager y modificar la configuración oportuna, como los números de directorio, en ese sistema.
- Mover los teléfonos registrados automáticamente a ubicaciones nuevas y asignarlos a grupos de dispositivos distintos sin que los números de directorio se vean afectados.

El registro automático está desactivado de manera predeterminada. En algunos casos puede ser útil emplear el registro automático; por ejemplo, si desea asignar un número de directorio específico al teléfono o si desea usar una conexión segura con Cisco Unified Communications Manager. Para obtener información sobre cómo habilitar el registro automático, consulte la documentación de su versión concreta de Cisco Unified Communications Manager. Si configura el clúster para el modo mixto mediante el cliente de Cisco CTL, el registro automático se desactiva automáticamente, pero puede activarlo. Si configura el clúster para el modo no seguro mediante el cliente de Cisco CTL, el registro automático no se habilita automáticamente.

Puede agregar teléfonos con el registro automático y TAPS, la herramienta de compatibilidad para teléfonos registrados automáticamente, sin tener que recopilar antes sus direcciones MAC.

TAPS funciona con la Herramienta de administración por lotes (BAT) para actualizar un lote de teléfonos que ya se han agregado a la base de datos de Cisco Unified Communications Manager con direcciones MAC simuladas. Use TAPS para actualizar las direcciones MAC y para descargar las configuraciones predefinidas de los teléfonos.

Cisco recomienda usar el registro automático y TAPS para agregar menos de 100 teléfonos a la red. Para agregar más de 100 teléfonos, use la Herramienta de administración por lotes (BAT).

Para implementar TAPS, tanto usted como el usuario final deben marcar un número de directorio de TAPS y seguir las indicaciones de voz. Cuando se complete el proceso, el teléfono incluirá el número de directorio y otros ajustes y se actualizará en Cisco Unified Communications Manager Administration con la dirección MAC correcta.

Verifique que el registro automático está habilitado y configurado correctamente en Administración de Cisco Unified Communications Manager antes de conectar cualquier teléfono IP de Cisco a la red. Para obtener información sobre cómo habilitar y configurar el registro automático, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Para que TAPS funcione, el registro automático debe estar habilitado en Cisco Unified Communications Manager Administration.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, haga clic en **Sistema** > **Cisco Unified CM**.

Paso 2 Haga clic en **Buscar** y seleccione el servidor necesario.

Paso 3 En **Información de registro automático**, configure estos campos.

- **Plantilla de dispositivo universal**
- **Plantilla de línea universal**
- **Primer número de directorio**
- **Último número de directorio**

Paso 4 Quite la marca de la casilla de verificación **Registro automático desactivado en este Cisco Unified Communications Manager**.

Paso 5 Haga clic en **Guardar**.

Paso 6 Haga clic en **Aplicar configuración**.

Modo de conexión en cadena

Puede conectar dos teléfonos de conferencia mediante un Adaptador inteligente y los cables USB-C que se proporcionan en el kit de conexión en cadena para ampliar el área de cobertura en una sala.

En el modo de conexión en cadena, ambas unidades reciben la alimentación mediante el adaptador inteligente conectado al adaptador de alimentación. Solo puede usar un micrófono externo por unidad. Puede usar un par de micrófonos con cables con las unidades o bien un par de micrófonos inalámbricos con las mismas, pero no una combinación de los tipos de micrófonos. Cuando se conecta un micrófono inalámbrico con una de las unidades, se desvincula de cualquier micrófono inalámbrico que esté conectado a la misma unidad. Siempre que haya una llamada activa, los LED y las opciones de menú de la pantalla del teléfono de ambas unidades se sincronizarán.

Temas relacionados

Instalación del teléfono para conferencias en modo de conexión en cadena, en la página 38
Un teléfono en modo de conexión en cadena no funciona, en la página 168

Instalación del teléfono para conferencias

Cuando el teléfono se conecta a la red, se inicia el proceso de encendido del teléfono y este se registra en Cisco Unified Communications Manager. Si desactiva el servicio DHCP, deberá configurar los ajustes de red en el teléfono.

Si ha usado el registro automático, debe actualizar los datos de configuración específicos del teléfono; por ejemplo, asociar el teléfono con un usuario y cambiar la tabla de botones o el número de directorio.

Una vez que se conecte el teléfono, determina si debe instalarse una nueva carga de firmware en el teléfono.

Si utiliza el teléfono para conferencias en modo de conexión en cadena, consulte Instalación del teléfono para conferencias en modo de conexión en cadena, en la página 38.

Antes de empezar

Asegúrese de que tiene instalada la versión de firmware más reciente en su Cisco Unified Communications Manager. Compruebe los paquetes de dispositivo actualizados aquí:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/matrix/CMDP_BK_CCBDA741_00_cucm-device-package-compatibility-matrix.html

Procedimiento

Paso 1 Seleccione la fuente de alimentación del teléfono:

- Implementación de alimentación a través de Ethernet (PoE) con un Inyector PoE de teléfono IP 8832 para conferencias de Cisco
- Implementación de Ethernet sin PoE con un Inyector Ethernet No PoE de teléfono IP 8832 para conferencias de Cisco
- Implementación de Wi-Fi con un adaptador de alimentación de teléfono IP 8832 para conferencias de Cisco

Para obtener más información, consulte Formas de proporcionar alimentación al teléfono para conferencias, en la página 33.

Paso 2 Conecte el teléfono al conmutador.

- Si usa PoE:
  1. Enchufe el cable Ethernet en el puerto LAN.
  2. Enchufe el otro extremo del cable Ethernet en Inyector PoE de teléfono IP 8832 para conferencias de Cisco o Inyector Ethernet para teléfono IP 8832 para conferencias de Cisco.
  3. Conecte el inyector al teléfono para conferencias con el cable USB-C.
- Si no usa PoE:
  1. Si utiliza Inyector Ethernet para teléfono IP 8832 para conferencias de Cisco, conecte el adaptador de alimentación a una toma de corriente.
  2. Conecte el adaptador de alimentación al inyector Ethernet mediante un cable USB-C.

     O

     Si utiliza Inyector Ethernet No PoE de teléfono IP 8832 para conferencias de Cisco, conéctelo a una toma de corriente.
  3. Enchufe el cable Ethernet en el inyector Ethernet sin PoE o en el inyector Ethernet.
  4. Enchufe el cable Ethernet en el puerto LAN.
  5. Conecte el inyector Ethernet sin PoE o el inyector Ethernet al teléfono para conferencias con otro cable USB-C.
- Si utiliza Wi-Fi:
  1. Conecte el adaptador de alimentación del teléfono IP 8832 para conferencias de Cisco en la toma de corriente.
  2. Conecte el adaptador de alimentación al teléfono para conferencias mediante un cable USB-C.

Nota En lugar del adaptador de alimentación, puede utilizar el inyector Ethernet sin PoE para la alimentación del teléfono. Sin embargo, primero debe desconectar el cable LAN. El teléfono solo se conecta a Wi-Fi cuando no está disponible la conexión Ethernet.

Paso 3 Supervise el proceso de encendido del teléfono. Este paso comprueba que el teléfono se ha configurado correctamente.

Paso 4 Si no desea usar el registro automático, configure manualmente la configuración de seguridad en el teléfono.

Paso 5 Permita que el teléfono se actualice a la imagen de firmware actual que se encuentra almacenada en su Cisco Unified Communications Manager.

Paso 6 Efectúe alguna llamada con el teléfono para comprobar que el teléfono y sus características funcionan correctamente.

Paso 7 Proporcione información a los usuarios sobre el uso de los teléfonos y la configuración de las opciones. Este paso garantiza que los usuarios dispondrán de información adecuada para usar correctamente sus teléfonos de Cisco.

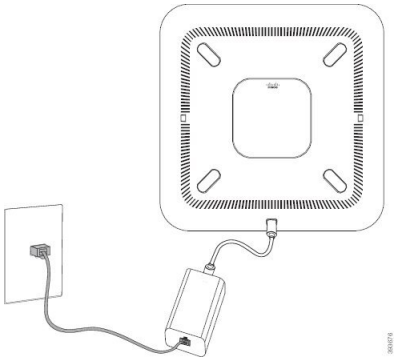
Formas de proporcionar alimentación al teléfono para conferencias

El teléfono para conferencia necesita alimentación de una de estas fuentes:

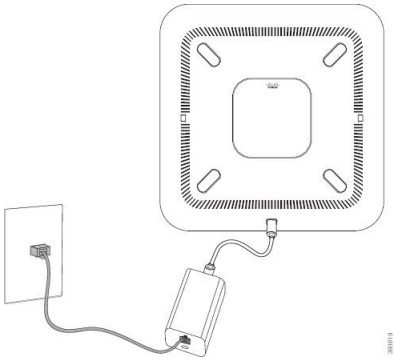
- Alimentación a través de Ethernet (PoE).
  - América del Norte
    - Inyector PoE de teléfono IP 8832 para conferencias de Cisco
    - Inyector Ethernet para teléfono IP 8832 para conferencias de Cisco
  - Fuera de Norteamérica: Inyector PoE de teléfono IP 8832 para conferencias de Cisco.
- Ethernet no PoE
  - América del Norte
    - Inyector Ethernet No PoE de teléfono IP 8832 para conferencias de Cisco
    - Inyector Ethernet para teléfono IP 8832 para conferencias de Cisco con un adaptador de alimentación de teléfono IP 8832 para conferencias de Cisco conectado a una toma eléctrica.
  - Fuera de Norteamérica: Inyector Ethernet No PoE de teléfono IP 8832 para conferencias de Cisco.
- Wi-Fi: utilice el adaptador de alimentación del teléfono IP 8832 para conferencias de Cisco conectado a una toma eléctrica.

Figura 6: Opciones de alimentación PoE del teléfono para conferencias

En la siguiente figura se muestran las dos opciones de alimentación PoE.



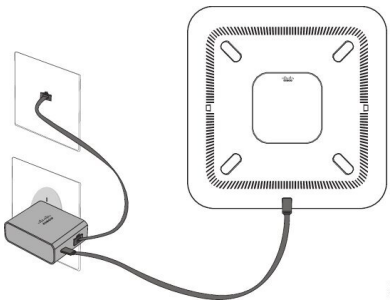
Inyector PoE de teléfono IP 8832 para conferencias de Cisco con la opción de alimentación PoE



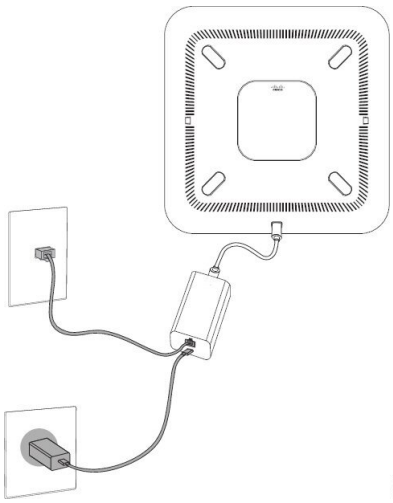
Inyector Ethernet para teléfono IP 8832 para conferencias de Cisco con la opción de alimentación PoE

Figura 7: Opciones de alimentación Ethernet del teléfono para conferencias

En la siguiente figura se muestran las dos opciones de alimentación a través de Ethernet.



Inyector Ethernet No PoE de teléfono IP 8832 para conferencias de Cisco con la opción de alimentación Ethernet



Inyector Ethernet para teléfono IP 8832 para conferencias de Cisco con la opción de alimentación Ethernet

Figura 8: Opción de alimentación del teléfono para conferencias cuando está conectado a una red Wi-Fi

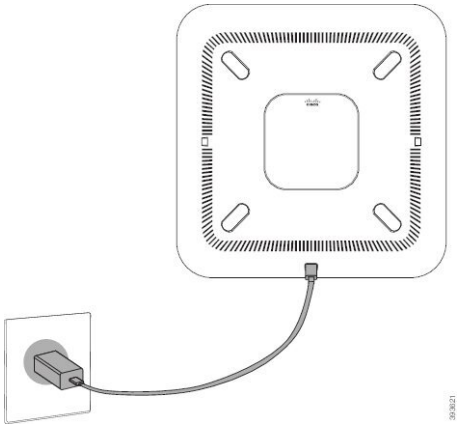
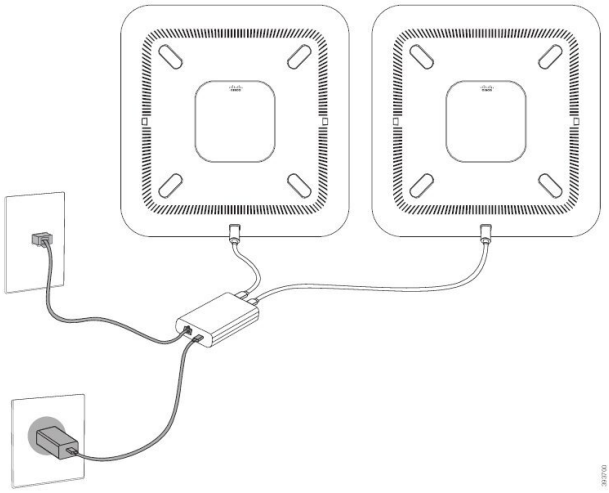


Figura 9: Opción de alimentación del teléfono para conferencias en modo conexión en cadena

En la siguiente figura se muestra la opción de alimentación cuando el teléfono está conectado en el modo de conexión en cadena.



Instalación de los micrófonos de expansión con cables

El teléfono admite un kit opcional con dos micrófonos de expansión con cables. Puede colocar los micrófonos a una distancia máxima de 7 pies (2,13 m) del teléfono. Para obtener los resultados óptimos, coloque los micrófonos a una distancia entre 3 pies (0,91m) y 7 pies (2,1m) del teléfono.

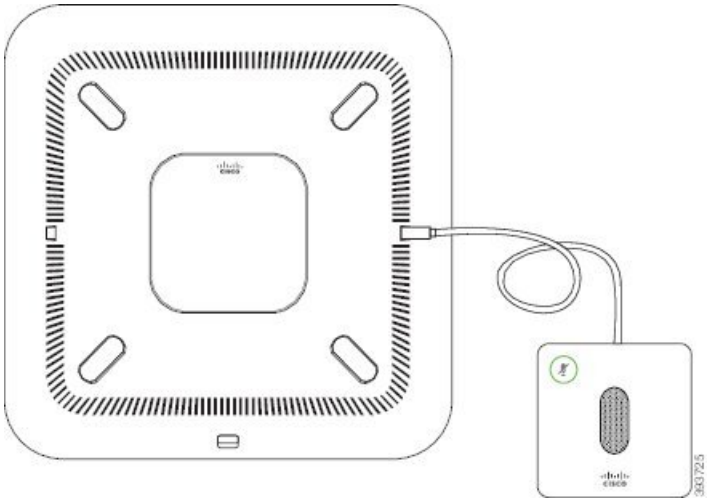
Procedimiento

Paso 1 Conecte el extremo del cable del micrófono en el puerto lateral del teléfono.

Paso 2 Extienda el cable del micrófono hasta la posición deseada.

En la siguiente ilustración se muestra la instalación de un micrófono de expansión con cables.

Figura 10: Instalación del micrófono de expansión con cables



Instalación de micrófonos de expansión inalámbricos

El teléfono de conferencia proporciona la opción de conectar dos micrófonos de expansión inalámbricos.

Nota Debe usar dos micrófonos con cables o dos micrófonos inalámbricos con el teléfono, pero nunca una mezcla de los dos tipos.

Si el teléfono se encuentra en una llamada, el LED del micrófono de expansión se ilumina en verde. Para silenciar el micrófono de expansión, presione la tecla **Silenciar**. Cuando el micrófono está silenciado, el LED se ilumina en rojo. Cuando la batería en el micrófono está baja, el LED indicador de nivel de batería parpadea rápidamente.

Antes de empezar

Antes de instalar los micrófonos de expansión inalámbricos, desconecte los micrófonos de expansión con cables. No puede utilizar ambos micrófonos de expansión con cable e inalámbricos al mismo tiempo.

Procedimiento

Paso 1 Coloque la placa de montaje en mesa en la ubicación de la superficie de la mesa en la que desea colocar el micrófono.

Paso 2 Quite el adhesivo de la cinta adhesiva doble de la parte inferior de la placa de montaje en mesa. Coloque la placa de montaje en mesa para adherirla a la superficie de la mesa.

Paso 3 Acople el micrófono a la placa de montaje en mesa. El micrófono tiene imanes integrados para ajustar la unidad en su lugar.

Puede mover el micrófono y la placa montaje en mesa adherida a otra ubicación en la superficie de la mesa según sea necesario. Procure proteger la unidad cuando la mueva.

Temas relacionados

Micrófono de expansión inalámbrico (8832 solo), en la página 13
Instalación de la base de carga del micrófono inalámbrico, en la página 37

Instalación de la base de carga del micrófono inalámbrico

Puede usar la base de carga para cargar la batería del micrófono inalámbrico.

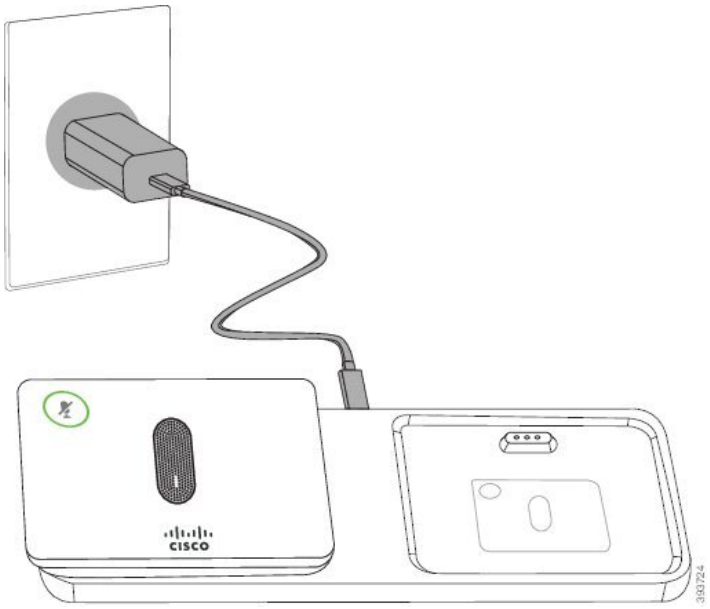
Procedimiento

Paso 1 Conecte el adaptador de alimentación de la base de carga a la red eléctrica.

Paso 2 Enchufe un extremo del cable USB a la base de carga y el otro extremo al adaptador de alimentación.

En la siguiente ilustración se muestra la instalación de la base de carga de un micrófono inalámbrico.

Figura 11: Instalación de la base de carga del micrófono inalámbrico



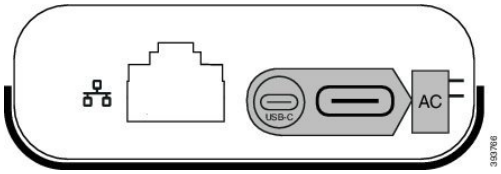
Temas relacionados

Micrófono de expansión inalámbrico (8832 solo), en la página 13
Instalación de micrófonos de expansión inalámbricos, en la página 36

Instalación del teléfono para conferencias en modo de conexión en cadena

El kit de conexión en cadena contiene un Adaptador inteligente, un cable LAN corto, dos cables USB-C largos y gruesos, y un cable USB-C más corto y delgado. En el modo de conexión en cadena, los teléfonos para conferencias necesitan alimentación externa de una toma de corriente. Debe usar el Adaptador inteligente para conectar entre sí de los teléfonos. Los cables USB-C largos van al teléfono y el corto al adaptador de alimentación. Consulte la siguiente figura cuando conecte el adaptador de alimentación y el puerto LAN a Adaptador inteligente.

Figura 12: Puerto de alimentación y puerto LAN del adaptador inteligente



Solo puede usar un micrófono por unidad.

Nota Debe usar dos micrófonos con cables o dos micrófonos inalámbricos con el teléfono, pero nunca una mezcla de los dos tipos.

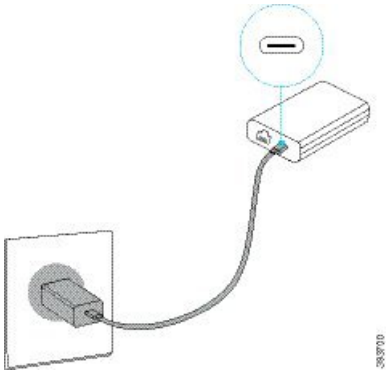
El cable USB-C del adaptador de alimentación es más delgado que los cables USB-C que se conectan al teléfono.

Procedimiento

Paso 1 Conecte el adaptador de alimentación a la red eléctrica.

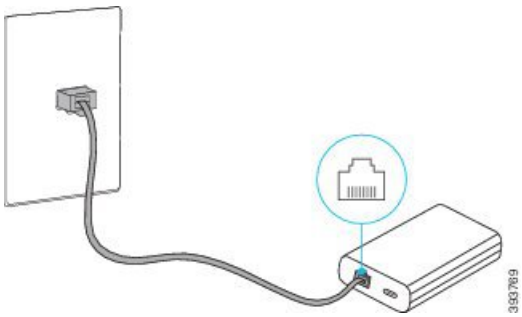
Paso 2 Conecte el cable USB-C corto y más delgado del adaptador de alimentación a Adaptador inteligente.

Figura 13: Puerto USB del adaptador inteligente conectado a la toma de corriente



Paso 3 Necesario: Conecte el cable Ethernet a Adaptador inteligente y el puerto LAN.

Figura 14: Puerto LAN del adaptador inteligente conectado al puerto LAN en la toma de pared

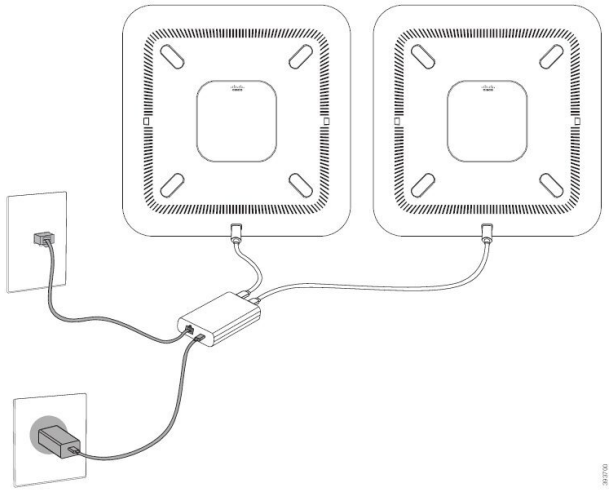


Paso 4 Conecte el primer teléfono a Adaptador inteligente con el cable USB-C más largo y grueso.

Paso 5 Conecte el segundo teléfono a Adaptador inteligente con un cable USB-C.

En la siguiente figura se muestra la instalación del teléfono para conferencias en modo de conexión en cadena.

Figura 15: Instalación del teléfono para conferencias en modo de conexión en cadena



Temas relacionados

Modo de conexión en cadena, en la página 31
Un teléfono en modo de conexión en cadena no funciona, en la página 168

Reinicio del teléfono para conferencias desde la imagen de copia de seguridad

Su teléfono IP 8832 para conferencias de Cisco tiene otra imagen de copia de seguridad que le permite recuperar el teléfono si la imagen predeterminada se ha visto comprometida.

Para reiniciar el teléfono desde la imagen de copia de seguridad, realice el siguiente procedimiento.

Procedimiento

Paso 1 Mantenga pulsada la tecla * mientras conecta la alimentación al teléfono para conferencias.

Paso 2 Después de que la luz de la barra LED se encienda de color verde y después se apague, puede soltar la tecla *.

Paso 3 El teléfono para conferencias se reinicia desde la imagen de copia de seguridad.

Configuración del teléfono en los menús

El teléfono incluye muchos ajustes de red configurables que puede ser necesario modificar para que los usuarios puedan usarlo. Puede acceder a estos ajustes y cambiar algunos en los menús del teléfono.

El teléfono incluye los siguientes menús de configuración:

- Configuración de red: incluye opciones para ver y configurar varios ajustes de red.
  - Configuración de IPv4: este submenú proporciona opciones de red adicionales.
  - Configuración de IPv6: este submenú proporciona opciones de red adicionales.
- Configuración de seguridad: incluye opciones para ver y configurar varios ajustes de seguridad.

Nota Es posible controlar si un teléfono tiene acceso al menú Configuración o a las opciones de este menú. Utilice el campo **Acceso a la configuración** en la ventana de configuración del teléfono de Cisco Unified Communications Manager Administration para controlar el acceso. El campo **Acceso a la configuración** acepta estos valores:

- Activado: permite el acceso al menú Configuración.
- Desactivado: impide el acceso a la mayoría de las entradas del menú Configuración. El usuario puede seguir accediendo a **Configuración** > **Estado**.
- Restringido: permite el acceso a los elementos de menú Preferencias de usuario y Estado , así como guardar los cambios de volumen. Impide el acceso a otras opciones del menú Configuración.

Si no puede acceder a una opción del menú Configuración de administración, compruebe el campo **Acceso a la configuración**.

Puede configurar los ajustes que solo se podrán visualizar en el teléfono en Cisco Unified Communications Manager Administration.

Procedimiento

Paso 1 Presione **Configuración**.

Paso 2 Seleccione **Config. admin**.

Paso 3 Si fuera necesario, introduzca la contraseña y haga clic en **Conectar**.

Paso 4 Seleccione **Configuración de red** o **Configuración de seguridad**.

Paso 5 Lleve a cabo una de las acciones siguientes para mostrar el menú deseado:

- Use las flechas de navegación para seleccionar el menú deseado y presione **Seleccionar**.

- Use el teclado del teléfono para introducir el número correspondiente al menú.

Paso 6 Para mostrar un submenú, repita el paso 5.

Paso 7 Para salir de un menú, presione **Atrás** .

Temas relacionados

Reinicio o restablecimiento del teléfono para conferencias, en la página 175
Configuración de los ajustes de red, en la página 42
Configuración de los ajustes de seguridad

Aplicación de una contraseña al teléfono

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, navegue hasta la ventana de configuración Perfil de teléfono común (**Dispositivo** > **Configuración del dispositivo** > **Perfil de teléfono común**).

Paso 2 Introduzca una contraseña en la opción Contraseña de desbloqueo del teléfono local.

Paso 3 Aplique la contraseña al perfil de teléfono común que use el teléfono.

Introducción de texto y opciones de menú desde el teléfono

Cuando edite el valor de una opción, siga estas instrucciones:

- Use las flechas del control de navegación para resaltar el campo que desea editar. Presione **Seleccionar** en el control de navegación para activar el campo. Cuando el campo esté activado, puede introducir valores.
- Use las teclas del teclado para introducir números y letras.
- Para introducir letras con el teclado, use la tecla de número correspondiente. Presione la tecla una o más veces para mostrar una letra concreta. Por ejemplo, pulse la tecla **2** una vez para «a,» dos veces rápidamente para «b,» y tres veces rápidamente para «c.» Tras hacer una pausa, el cursor avanza automáticamente para permitirle introducir la siguiente letra.
- Si comete un error, presione la tecla programable . Esta tecla programable elimina el carácter situado a la izquierda del cursor.
- Presione **Revertir** antes de presionar **Aplicar** para descartar los cambios que haya efectuado.
- Para introducir un punto (por ejemplo, en una dirección IP), presione ***** en el teclado.
- Para introducir dos puntos para una dirección IPv6, presione ***** en el teclado.

Nota El teléfono IP de Cisco ofrece varios métodos para restablecer o restaurar los ajustes de las opciones, si fuera necesario.

Configuración de los ajustes de red

Procedimiento

Paso 1 Presione **Configuración**.

Paso 2 Seleccione **Configuración de administración** > **Configuración de red** > **Configuración de Ethernet**.

Paso 3 Configure los campos tal y como se describe en Campos de configuración de red, en la página 42. Después de configurar los campos, es posible que tenga que reiniciar el teléfono.

Campos de configuración de red

El menú Configuración de red contiene los campos y los submenús de IPv4 e IPv6.

Para modificar algunos campos, deberá desactivar DHCP.

Tabla 10: Menú Configuración de red

Entrada	Tipo	Valor predeterminado	Descripción
Configuración de IPv4	Menú		Consulte la tabla «Submenú de configuración IPv4». Esta opción solo se muestra en el modo de pila dual.
Configuración de IPv6	Menú		Consulte la tabla «Submenú de configuración IPv6».
Nombre de host	cadena		El nombre de host del teléfono. Si usa DHCP, este nombre se asigna automáticamente.
Nombre de dominio	cadena		El nombre del dominio del sistema de nombre de dominio (DNS) en el que se encuentra el teléfono. Para cambiar este campo, desactive DHCP.
ID de VLAN operativo			La red de área local virtual (VLAN) operativa configurada en un switch Cisco Catalyst de la que es miembro el teléfono.
ID de VLAN administrativo			La VLAN auxiliar de la que es miembro el teléfono.

Entrada	Tipo	Valor predeterminado	Descripción
Config. puerto switch	Negociación automática 10 medio 10 completo 100 medio 100 completo	Negociación automática	La velocidad y dúplex del puerto PC, donde: • 10 medio = 10-BaseT/semidúplex • 10 completo = 10-BaseT/dúplex completo • 100 medio = 100-BaseT/semidúplex • 100 completo = 100-BaseT/dúplex completo
LLDP-MED: puerto switch	Desactivado Habilitado	Habilitado	Indica si LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery) está habilitado en el puerto de switch.

Tabla 11: Submenú Configuración de IPv4

Entrada	Tipo	Valor predeterminado	Descripción
DHCP	Desactivado Habilitado	Habilitado	Activa o desactiva el uso de DHCP.
Dirección IP			Indica la dirección del protocolo de Internet versión 4 (IPv4) del teléfono. Para cambiar este campo, desactive DHCP.
Máscara de subred			La máscara de subred que usa el teléfono. Para cambiar este campo, desactive DHCP.
Router predeterminado 1			El router predeterminado que usa el teléfono. Para cambiar este campo, desactive DHCP.
Servidor DNS 1			Servidor DNS (sistema de nombres de dominio) principal (servidor DNS 1) que usa el teléfono. Para cambiar este campo, desactive DHCP.

Entrada	Tipo	Valor predeterminado	Descripción
Servidor DNS 2			Servidor DNS (sistema de nombres de dominio) principal (servidor DNS 2) que usa el teléfono.
Servidor DNS 3			Servidor DNS (sistema de nombres de dominio) principal (servidor DNS 3) que usa el teléfono.
TFTP alternativo	No Sí	No	Indica si el teléfono usa un servidor TFTP alternativo.
Servidor TFTP 1			El servidor de protocolo de transferencia de archivos trivial (TFTP) primario que usa el teléfono. Si activa la opción TFTP alternativo, debe introducir un valor distinto a cero en la opción Servidor TFTP 1. Si en el archivo CTL o ITL del teléfono no aparecen ni el servidor TFTP principal ni el de copia de seguridad, debe desbloquear el archivo antes de guardar los cambios en la opción Servidor TFTP 1. En este caso, el teléfono elimina el archivo cuando se guardan los cambios en la opción Servidor TFTP 1. Se descarga un nuevo archivo CTL o ITL de la nueva dirección del servidor TFTP 1. Consulte las notas de TFTP después de la tabla final.
Servidor TFTP 2			Servidor TFTP secundario que usa el teléfono. Si en el archivo CTL o ITL del teléfono no aparecen ni el servidor TFTP principal ni el de copia de seguridad, debe desbloquear el archivo antes de guardar los cambios en la opción Servidor TFTP 2. En este caso, el teléfono elimina el archivo cuando se guardan los cambios en la opción Servidor TFTP 2. Se descarga un nuevo archivo CTL o ITL de la nueva dirección del servidor TFTP 2. Consulte la sección Notas de TFTP después de la tabla final.

Entrada	Tipo	Valor predeterminado	Descripción
Dirección DHCP liberada	No Sí	No	

Tabla 12: Submenú Configuración de IPv6

Entrada	Tipo	Valor predeterminado	Descripción
DHCPv6 habilitado	Desactivado Habilitado	Habilitado	Activa o desactiva el uso de DHCP IPv6.
Dirección IPv6			Indica la dirección IPv6 del teléfono. Para cambiar este campo, desactive DHCP.
Longitud de prefijo de IPv6			Longitud de la dirección IPv6. Para cambiar este campo, desactive DHCP.
Router predeterminado 1 de IPv6			Router de IPv6 predeterminado. Para cambiar este campo, desactive DHCP.
Servidor DNS 1 de IPv6			Servidor DNS IPv6 primario Para cambiar este campo, desactive DHCP.
TFTP alternativo de IPv6	No Sí	No	Indica si el teléfono usa un servidor TFTP IPv6 alternativo.
Servidor TFTP 1 de IPv6			El servidor TFTP IPv6 primario que usa el teléfono. Consulte la sección Notas de TFTP después de esta tabla.
Servidor TFTP 2 de IPv6			El servidor TFTP IPv6 secundario que usa el teléfono. Consulte la sección Notas de TFTP después de esta tabla.
Dirección IPv6 liberada	No Sí	No	

Antes de poder configurar las opciones de IPv6 en el dispositivo, las direcciones IPv6 deben activarse y configurarse en Cisco Unified Communication Administration. Los campos de configuración de dispositivos siguientes se aplican a la configuración de IPv6:

- Modo de direcciones IP.
- Modo de direcciones IP preferidas para señalización.

Si las direcciones IPv6 están activadas en el clúster de Unified, la configuración predeterminada para el modo de direcciones IP es IPv4 e IPv6. En este modo de direcciones, el teléfono adquirirá y usará una dirección IPv4 y una dirección IPv6. Usará una u otra según requieran los medios. El teléfono usa la dirección IPv4 o IPv6 para las señales de control de llamadas.

Para obtener más información sobre IPv6, consulte:

- «Configuración de dispositivo común» en la *Guía de características y servicios de Cisco Unified Communications Manager*, capítulo «Compatibilidad de IPv6 en dispositivos Cisco Unified Communications».
- La *Guía de implementación de IPv6 de Cisco Collaboration Systems versión 12.0* se encuentra aquí: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html

Notas de TFTP

Cuando el teléfono busca el servidor TFTP, da precedencia a los servidores TFTP asignados de forma manual, independientemente del protocolo. Si la configuración incluye servidores TFTP tanto IPv6 como IPv4, el teléfono ordena por prioridad la búsqueda del servidor TFTP y da precedencia a los servidores TFTP IPv6 e IPv4 asignados de forma manual. El teléfono busca los servidores TFTP en este orden:

1. Cualquier servidor TFTP IPv4 asignado manualmente.
2. Cualquier servidor IPv6 asignado manualmente.
3. Servidores TFTP asignados por DHCP.
4. Servidores TFTP asignados por DHCPv6.

Para obtener información sobre los archivos CTL e ITL, consulte la *Guía de seguridad de Cisco Unified Communications Manager*.

Establecimiento del campo Nombre de dominio

Procedimiento

Paso 1 En la opción DHCP habilitado establezca **No**.

Paso 2 Diríjase a la opción Nombre de dominio, pulse **Seleccionar** e introduzca un nombre de dominio nuevo.

Paso 3 Presione **Aplicar**.

Activación de la LAN inalámbrica en el teléfono

Asegúrese de que la cobertura de Wi-Fi de las instalaciones donde se implementa la LAN inalámbrica es apta para transmitir paquetes de voz.

Se recomienda un método de itinerancia rápida segura para los usuarios de Wi-Fi. Le recomendamos que utilice 802.11r (FT).

Para obtener todos los detalles sobre la configuración, consulte la *Guía de implementación en LAN inalámbrica de los teléfonos IP serie 8832 de Cisco* en esta ubicación:

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html

La *Guía de implementación en LAN inalámbrica de los teléfonos IP serie 8832 de Cisco* incluye los siguientes datos de configuración:

- Configuración de red inalámbrica
- Configuración de red inalámbrica en Cisco Unified Communications Manager Administration
- Configuración de red inalámbrica en el teléfono IP de Cisco

Antes de empezar

Asegúrese de que la red Wi-Fi esté activada en el teléfono y que el cable Ethernet esté desconectado.

Procedimiento

Paso 1 Para activar la aplicación, pulse **Configuración**.

Paso 2 Desplácese a **Config. admin** > **Configuración de red** > **Configuración del cliente Wi-Fi** > **Inalámbrico**.

Paso 3 Pulse **Activado**.

Configuración de la LAN inalámbrica en Cisco Unified Communications Manager

En Cisco Unified Communications Manager Administration, debe activar un parámetro denominado «Wi-Fi» para el teléfono de conferencia.

Nota En la ventana de configuración del teléfono de Cisco Unified Communications Manager Administration (**Dispositivo** > **Teléfono**), use la dirección MAC de la línea con cables cuando tenga que configurar la dirección MAC. El registro de Cisco Unified Communications Manager no usa la dirección MAC inalámbrica.

Lleve a cabo el procedimiento siguiente en Cisco Unified Communications Manager Administration.

Procedimiento

Paso 1 Para activar la LAN inalámbrica en un teléfono concreto, lleve a cabo los pasos siguientes:

a) Seleccione **Dispositivo** > **Teléfono**.
b) Localice el teléfono necesario.
c) Seleccione el ajuste **Activado** para el parámetro Wi-Fi en la sección de diseño de configuración específica del producto.
d) Marque la casilla de verificación **Cancelar configuración común**.

Paso 2 Para activar la LAN inalámbrica para un grupo de teléfonos:

a) Seleccione **Dispositivo** > **Configuración del dispositivo** > **Perfil de teléfono común**.
b) Seleccione el ajuste **Activado** para activar el parámetro Wi-Fi.

Nota Para asegurarse de que la configuración de este paso funcione, desmarque la casilla de verificación **Cancelar configuración común** mencionada en el paso 1d.

c) Marque la casilla de verificación **Cancelar configuración común**.
d) Asocie los teléfonos con ese perfil de teléfono común en **Dispositivo** > **Teléfono**.

Paso 3 Para activar la LAN inalámbrica para todos los teléfonos que admiten WLAN de la red:

a) Seleccione **Sistema** > **Configuración de teléfono empresarial**.
b) Seleccione el ajuste **Activado** para activar el parámetro Wi-Fi.

Nota Para asegurarse de que la configuración de este paso funcione, desmarque la casilla de verificación **Cancelar configuración común** mencionada en el paso 1d y el paso 2c.

c) Marque la casilla de verificación **Cancelar configuración común**.

Configuración de la LAN inalámbrica desde el teléfono

Antes de que el teléfono IP de Cisco se pueda conectar a la WLAN, debe configurar el perfil de red para el teléfono con los valores adecuados de la WLAN. Puede usar el menú **Configuración de red** en el teléfono para acceder al submenú **Configuración del cliente Wi-Fi** y establecer la configuración de WLAN.

Nota La opción **Configuración del cliente Wi-Fi** no aparece en el menú **Configuración de red** cuando se desactiva Wi-Fi en Cisco Unified Communications Manager.

Para obtener información adicional, consulte *Guía de implementación WLAN de teléfono IP 8832 para conferencias de Cisco*, que se encuentra aquí: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html.

Antes de empezar

Configure de la LAN inalámbrica desde Cisco Unified Communications Manager.

Procedimiento

Paso 1 Presione **Configuración**.

Paso 2 Seleccione **Config. admin.** > **Configuración de red** > **Configuración del cliente Wi-Fi**.

Paso 3 Configure los valores de la comunicación inalámbrica como se describe en la tabla siguiente.

Tabla 13: Opciones del menú Configuración del cliente Wi-Fi

Opción	Descripción	Para cambiarla
Inalámbrico	Activa o desactiva la radio inalámbrica en el teléfono IP de Cisco.	Desplácese a la opción **Inalámbri** conmutador para activarla o desac
Nombre de red	Le permite conectarse a una red inalámbrica mediante la ventana **Elegir una red**. Esta ventana dispone de dos teclas programables: **Atrás** y **Otros**.	En la ventana **Elegir una red**, sele a la que desea conectarse.
Acceso de inicio de sesión Wi-Fi	Activa la visualización de la ventana de inicio de sesión Wi-Fi.	Diríjase a la opción de **inicio de se** use el conmutador para activarla o
Configuración de IPv4	En el submenú Configuración de IPv4 puede hacer lo siguiente: • Habilitar o deshabilitar el teléfono para que use la dirección IP que asigna el servidor DHCP. • Establecer manualmente la dirección IP, la máscara de subred, los routers predeterminados, el servidor DNS, y los servidores TFTP alternativos. Para más información sobre los campos de dirección IPv4, consulte la tabla "Submenú de configuración IPv4".	Desplácese a **Configuración de I** **Seleccionar**.
Configuración de IPv6	En el submenú Configuración de IPv6 puede hacer lo siguiente: • Habilitar o deshabilitar el teléfono para que use la dirección IPv6 que asigna el servidor DHCPv6 o que adquiere SLAAC mediante un router IPv6. • Establecer manualmente la dirección IPv6, la longitud del prefijo, los routers predeterminados, el servidor DNS, y los servidores TFTP alternativos. Para más información sobre los campos de dirección IPv6, consulte la tabla "Submenú de configuración IPv6".	Desplácese a **Configuración de I** **Seleccionar**.
Dirección MAC	La dirección de control de acceso a los medios (MAC) única del teléfono.	Solo visualización. No es posible c

Opción	Descripción	Para cambiarla
Nombre de dominio	El nombre del dominio del sistema de nombre de dominio (DNS) en el que se encuentra el teléfono.	Consulte Establecimiento del campo N dominio, en la página 46.

Paso 4 Pulse **Guardar** para aplicar los cambios o presione **Revertir** para descartar la conexión.

Establecer el número de intentos de autenticación de WLAN

Una solicitud de autenticación es una confirmación de credenciales de inicio de sesión del usuario. Se produce cuando un teléfono que ya ha participado en una red Wi-Fi intenta volver a conectarse al servidor Wi-Fi. Por ejemplo, cuando se agota el tiempo de espera de una sesión de Wi-Fi o se pierde la conexión Wi-Fi y, a continuación, vuelve a adquirirse.

Puede configurar el número de veces que un teléfono Wi-Fi envía una solicitud de autenticación al servidor Wi-Fi. El número de intentos predeterminado es 2, pero puede ajustar este parámetro de 1 a 3. Si un teléfono falla la autenticación, se le pedirá al usuario que vuelva a iniciar sesión.

Puede aplicar intentos de autenticación de WLAN a teléfonos individuales, a un grupo de teléfonos o a todos los teléfonos Wi-Fi de la red.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Dispositivo** > **Teléfono** y localice el teléfono.

Paso 2 Diríjase al área Configuración específica del producto y defina el campo **Intentos de autenticación de WLAN**.

Paso 3 Seleccione **Guardar**.

Paso 4 Seleccione **Aplicar configuración**.

Paso 5 Reinicie el teléfono.

Habilitar el modo de mensaje de WLAN

Active el modo de mensaje de perfil de WLAN 1 si desea que el usuario inicie sesión en la red Wi-Fi cuando el teléfono se encienda o se restablezca.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Dispositivo** > **Teléfono**.

Paso 2 Busque el teléfono que desea configurar.

Paso 3 Diríjase al área Configuración específica del producto y establezca el campo **Modo de mensaje de perfil de WLAN 1** en **Activar**.

Paso 4 Seleccione **Guardar**.

Paso 5 Seleccione **Aplicar configuración**.

Paso 6 Reinicie el teléfono.

Configuración de un perfil Wi-Fi mediante Cisco Unified Communications Manager

Puede configurar un perfil Wi-Fi y, a continuación, asignar el perfil a los teléfonos compatibles con Wi-Fi. El perfil contiene los parámetros necesarios para que los teléfonos se conecten a la Cisco Unified Communications Manager con Wi-Fi. Al crear y utilizar un perfil Wi-Fi, usted o los usuarios no tienen que configurar la red inalámbrica para teléfonos individuales.

Se admiten perfiles Wi-Fi en Cisco Unified Communications Manager, versión 10.5(2) o posterior. EAP-FAST, PEAP-GTC y PEAP-MSCHAPv2 se admiten en Cisco Unified Communications Manager versión 10.0 y posteriores. Opus es compatible con Cisco Unified Communications Manager 11.0 yo posterior.

Un perfil Wi-Fi permite evitar o limitar los cambios en la configuración Wi-Fi del teléfono por el usuario.

Le recomendamos que utilice un perfil de seguridad con el cifrado de TFTP activado para proteger las claves y contraseñas cuando utilice un perfil Wi-Fi.

Cuando configura los teléfonos para usar EAP-FAST, PEAP-MSCHAPV, o la autenticación PEAP-GTC, los usuarios necesitan ID de usuario y contraseñas individuales para iniciar sesión en el teléfono.

Los teléfonos solo admiten un certificado de servidor que puede instalarse con SCEP o con el método de instalación manual, pero no con ambos métodos. Los teléfonos no son compatibles con el método TFTP de instalación de certificados.

Procedimiento

Paso 1 En Cisco Unified Communications Administration, seleccione **Dispositivo** > **Configuración del dispositivo** > **Perfil de red LAN inalámbrica**.

Paso 2 Haga clic en **Agregar nuevo.**

Paso 3 En la sección **Información del perfil de red LAN inalámbrica**, establezca los parámetros:

- **Nombre**: introduzca un nombre único para el perfil Wi-Fi. Este nombre se muestra en el teléfono.
- **Descripción**: introduzca una descripción para el perfil Wi-Fi para ayudarle a distinguir este perfil de otros perfiles Wi-Fi.
- **Usuario modificable**: seleccione una opción:
  - **Permitido**: indica que el usuario puede realizar cambios en la configuración de la red Wi-Fi de su teléfono. Esta opción está activada de forma predeterminada.
  - **No permitido**: indica que el usuario no puede realizar cambios en la configuración de la red Wi-Fi en el teléfono.
  - **Restringido**: indica que el usuario puede cambiar el nombre de usuario y la contraseña Wi-Fi de su teléfono. Sin embargo, los usuarios no pueden realizar cambios en otra configuración de Wi-Fi en el teléfono.

Paso 4 En la sección **Configuración inalámbrica**, establezca los parámetros:

- **SSID (nombre de red)**: introduzca el nombre de red disponible en el entorno del usuario a la que puede conectarse el teléfono. Este nombre se muestra en la lista de redes disponibles en el teléfono y el teléfono puede conectarse a esta red inalámbrica.
- **Banda de frecuencia**: las opciones disponibles son Auto, 2,4 GHz y 5 GHz. Este campo determina la banda de frecuencia que utiliza la conexión inalámbrica. Si selecciona Auto, el teléfono intenta utilizar la banda de 5 GHz primero y solo utiliza la banda de 2,4 GHz cuando la de 5 GHz no está disponible.

Paso 5 En la sección **Configuración de autenticación**, establezca el **Método de autenticación** en uno de estos métodos de autenticación: EAP-FAST, EAP-TLS, PEAP-MSCHAPv2, PEAP-GTC, PSK, WEP y Ninguno.

Después de configurar este campo, puede ver los campos adicionales que necesite configurar.

- **Certificado de usuario**: es necesario para la autenticación EAP-TLS. Seleccione **Instalado en fábrica** o **Instalado por el usuario**. El teléfono necesita que se instale un certificado, automáticamente desde el SCEP o manualmente desde la página de administración del teléfono.
- **Frase de contraseña PSK**: es necesaria para la autenticación de PSK. Introduzca la frase de contraseña de 8-63 caracteres ASCII o de 64 caracteres hexadecimales.
- **Clave WEP**: necesaria para la autenticación WEP. Introduzca la clave WEP ASCII o hexadecimal 40/102 o 64/128.
  - 40/104 ASCII es de 5 caracteres.
  - 64/128 ASCII es de 13 caracteres.
  - 40/104 HEX es de 10 caracteres.
  - 64/128 HEX es de 26 caracteres.
- **Proporcionar credenciales compartidas**: es necesario para la autenticación EAP-FAST, PEAP-MSCHAPv2 y PEAP-GTC.
  - Si el usuario administra el nombre de usuario y la contraseña, deje los campos **Nombre de usuario** y **Contraseña** en blanco.
  - Si todos los usuarios comparten el mismo nombre de usuario y contraseña, puede introducir la información en los campos **Nombre de usuario** y **Contraseña**.
  - Introduzca una descripción en el campo **Descripción de la contraseña**.

Nota Si necesita asignar a cada usuario un único nombre de usuario y contraseña, debe crear un perfil para cada usuario.

Paso 6 Haga clic en **Guardar**.

Qué hacer a continuación

Aplique el grupo de perfil WLAN a un grupo de dispositivos (**Sistema** > **Grupo de dispositivos**) o directamente en el teléfono (**Dispositivo** > **Teléfono**).

Configuración de un grupo Wi-Fi mediante Cisco Unified Communications Manager

Puede crear un grupo de perfiles de red LAN inalámbrica y agregar cualquier perfil de red LAN inalámbrica a este grupo. El grupo de perfil se puede asignar a continuación al teléfono cuando este se configure.

Procedimiento

Paso 1 En Cisco Unified Communications Administration, seleccione **Dispositivo** > **Configuración del dispositivo** > **Grupo de perfiles de red LAN inalámbrica**.

También puede definir un grupo de perfiles de red LAN inalámbrica desde **Sistema** > **Grupo de dispositivos**.

Paso 2 Haga clic en **Agregar nuevo.**

Paso 3 En la sección **Información del grupo de perfiles de red LAN inalámbrica** , introduzca un nombre de grupo y descripción.

Paso 4 En la sección **Perfiles para este grupo de perfiles de red LAN inalámbrica**, seleccione un perfil de disponible desde la lista **Perfiles disponibles** y mueva el perfil seleccionado a la lista **Perfiles seleccionados**.

Cuando se selecciona más de un perfil de red LAN inalámbrica, el teléfono usa solo el primer perfil de red LAN inalámbrica.

Paso 5 Haga clic en **Guardar**.

Verificación del inicio del teléfono

Cuando el teléfono recibe alimentación, efectúa de forma automática un proceso de diagnóstico de inicio.

Procedimiento

Encienda el teléfono.

Cuando se muestra la pantalla principal, significa se ha iniciado correctamente.

Cambiar el modelo de teléfono de un usuario

Usted o su usuario pueden cambiar el modelo de teléfono de un usuario. El cambio puede ser necesario por varios motivos, por ejemplo:

- Ha actualizado Cisco Unified Communications Manager (Unified CM) a una versión de software que no es compatible con el modelo de teléfono.
- El usuario desea un modelo de teléfono diferente del modelo actual.

- El teléfono requiere reparación o sustitución.

Unified CM identifica el teléfono antiguo y utiliza la dirección MAC del teléfono antiguo para identificar la antigua configuración del teléfono. Unified CM copia la antigua configuración del teléfono en la entrada del nuevo teléfono. El nuevo teléfono tiene la misma configuración que el teléfono antiguo.

Limitación: si el teléfono antiguo tiene más líneas o botones de línea que el teléfono nuevo, el nuevo teléfono no tendrá líneas adicionales ni botones de línea configurados.

El teléfono se reiniciará cuando se complete la configuración.

Antes de empezar

Configure su Cisco Unified Communications Manager de acuerdo con las instrucciones de la *Guía de configuración de funciones de Cisco Unified Communications Manager*.

Necesita un nuevo teléfono sin utilizar que tenga preinstalada la versión de firmware 12.8(1) o posterior.

Procedimiento

Paso 1 Apague el teléfono antiguo.

Paso 2 Encienda el teléfono nuevo.

Paso 3 En el teléfono nuevo, seleccione **Sustituir un teléfono existente**.

Paso 4 Introduzca la extensión principal del teléfono antiguo.

Paso 5 Si el teléfono antiguo tiene un PIN asignado, introduzca el PIN.

Paso 6 Presione **Enviar**.

Paso 7 Si hay más de un dispositivo para el usuario, seleccione el dispositivo que desea sustituir y pulse **Continuar**.

CAPÍTULO 5

Instalación del teléfono en Cisco Unified Communications Manager

Configuración del teléfono IP para conferencias de Cisco

Si el registro automático no está activado y el teléfono no existe en la base de datos de Cisco Unified Communications Manager, debe configurar manualmente el teléfono IP de Cisco en Cisco Unified Communications Manager Administration. Algunas tareas de este procedimiento son opcionales y dependen del sistema y las necesidades del usuario.

Para obtener más información sobre cualquiera de los pasos, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Lleve a cabo los pasos de configuración del procedimiento siguiente mediante Cisco Unified Communications Manager Administration.

Procedimiento

Paso 1 Recopile la información siguiente sobre el teléfono:

- El modelo del teléfono.
- La dirección MAC: consulte Determinación de la dirección MAC del teléfono, en la página 60
- La ubicación física del teléfono.
- El nombre o el ID del usuario del teléfono.
- El grupo de dispositivos.

- La partición, el espacio de búsqueda de llamadas y la información de la ubicación.
- Número de directorio (DN) para asignar al teléfono
- El usuario de Cisco Unified Communications Manager que se debe asociar con el teléfono.
- La información de uso del teléfono que afecta a la plantilla de tecla programable, la plantilla de teclas programadas, las funciones del teléfono, los servicios de telefonía IP o las aplicaciones del teléfono.

Para obtener más datos, consulte la documentación de su versión concreta de Cisco Unified Communications Manager y consulte los enlaces relacionados.

Paso 2 Verifique que cuenta con suficientes licencias para el teléfono.

Para obtener más datos, consulte la documentación sobre las licencias de su versión concreta de Cisco Unified Communications Manager.

Paso 3 Defina los grupos de dispositivos. Seleccione **Sistema** > **Grupo de dispositivos**.

Los grupos de dispositivos definen características comunes para los dispositivos, como la región, el grupo de fecha/hora, y la plantilla de tecla programable.

Paso 4 Defina el perfil de teléfono común. Seleccione **Dispositivo** > **Configuración de dispositivo** > **Perfil telefónico común**.

Los perfiles de teléfono común proporcionan datos que el servidor TFTP de Cisco requiere, así como la configuración del teléfono común, como la función No molestar y las opciones de control de características.

Paso 5 Defina un espacio de búsqueda de llamadas. En Cisco Unified Communications Manager Administration, haga clic en **Llamada en espera** > **Clase de control** > **Espacio de búsqueda de llamadas**.

Un espacio de búsqueda de llamadas es una colección de particiones en las que se busca para determinar cómo se enrutará un número marcado. El espacio de búsqueda de llamadas del dispositivo y el del número de directorio se usan a la vez. El espacio del número de directorio tiene precedencia sobre el espacio del dispositivo.

Paso 6 Configure un perfil de seguridad para el tipo de dispositivo y el protocolo. Seleccione **Sistema** > **Seguridad** > **Perfil de seguridad del teléfono**.

Paso 7 Configure el teléfono. Seleccione **Dispositivo** > **Teléfono**.

a) Localice el teléfono que desea modificar, o agregue un teléfono nuevo.
b) Configure el teléfono completando los campos requeridos del panel Información de dispositivo de la ventana de configuración del teléfono.
   - Dirección MAC (obligatorio): asegúrese de que el valor está formado por 12 caracteres hexadecimales.
   - Descripción: introduzca una descripción útil que le sirva en caso de que deba realizar una búsqueda de información sobre el usuario.
   - Grupo de dispositivos (obligatorio).
   - Perfil de teléfono común.
   - Espacio de búsqueda de llamadas.
   - Ubicación.
   - Propietario (Usuario o Anónimo) y, si se ha seleccionado Usuario, el ID de usuario propietario

El dispositivo y su configuración predeterminada se agregan a la base de datos de Cisco Unified Communications Manager.

Para obtener información sobre los campos de configuración específicos del producto, seleccione el botón de ayuda «?» Botón Ayuda en la ventana Configuración de teléfono y el enlace relacionado.

Nota Si desea agregar tanto el teléfono como el usuario a la base de datos de Cisco Unified Communications Manager al mismo tiempo, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

c) En la sección de información específica de protocolo de esa ventana, seleccione un perfil de seguridad de dispositivo y establezca el modo de seguridad.

Nota Seleccione un perfil de seguridad basado en la estrategia de seguridad general de la empresa. Si el teléfono no admite funciones de seguridad, seleccione un perfil no seguro.

d) En la sección de información de la extensión, marque la casilla Habilitar movilidad de extensión si el teléfono admite Cisco Extension Mobility.

e) Haga clic en **Guardar**.

Paso 8 Seleccione **Dispositivo** > **Configuración del dispositivo** > **Perfil SIP** para configurar los parámetros SIP.

Paso 9 Seleccione **Dispositivo** > **Teléfono** para configurar números de directorio (líneas) en el teléfono completando los campos requeridos de la ventana de configuración del número de directorio.

a) Busque el teléfono.

b) En la ventana de configuración del teléfono, haga clic en Línea 1 en el panel de la izquierda de la ventana.

Los teléfonos para conferencias tienen una sola línea.

c) En el campo Número de directorio, introduzca un número válido que se pueda marcar.

Nota Este campo debe contener el mismo número que aparece en el campo Número de teléfono de la ventana de configuración del usuario final.

d) En la lista desplegable Partición de ruta, seleccione la partición a la que pertenece el número de directorio. Si no desea restringir el acceso al número de directorio, seleccione <None> para la partición.

e) En la lista desplegable Espacio de búsqueda de llamadas, seleccione el espacio oportuno. El valor que elija se aplicará a todos los dispositivos que usan este número de directorio.

f) En las secciones Captura de llamada y Configuración de desvío de llamadas, seleccione los elementos (por ejemplo, Desviar todas o Desviar si ocupado Interna) y los destinos correspondientes a los que se enviarán las llamadas.

Ejemplo:

Si desea que las llamadas internas y externas entrantes que reciban una señal de ocupado se desvíen al buzón de voz para esta línea, marque la casilla de verificación Buzón de voz situada junto a los elementos Desviar si ocupado Interna y Desviar si ocupado Externa de la columna de la izquierda de las secciones de Captura de llamada y Configuración de desvío de llamadas.

g) En la línea 1 del panel Dispositivo, configure los campos siguientes:

- Visualización (campo de ID de autor de llamada interno): puede introducir el nombre y los apellidos del usuario de este dispositivo para que su nombre se muestre en todas las llamadas internas. Deje el campo vacío para que el sistema muestre la extensión del teléfono.
- Máscara de número de teléfono externo: indica el número de teléfono (o la máscara) que se usa para enviar la información de ID de la persona que llama cuando se efectúa una llamada desde esta línea.

Es posible introducir un máximo de 24 caracteres numéricos y «X». Las X representan el número de directorio y deben aparecer al final del patrón.

Ejemplo:

Si especifica la máscara 408902XXXX, la llamadas externas desde la extensión 6640 muestran como número de ID de la persona que llama el 4089026640.

Este ajuste solo se aplica al dispositivo actual, a no ser que marque la casilla de verificación situada a la derecha (Actualizar configuración de dispositivo compartido) y haga clic en **Propagar seleccionado**. La casilla de verificación de la derecha solo se muestra si otros dispositivos comparten este número de directorio.

h) Seleccione **Guardar**.

Para obtener más información sobre los números de directorio, consulte la documentación de su versión concreta de Cisco Unified Communications Manager y los enlaces relacionados.

Paso 10 (Opcional) Asocie el usuario con un teléfono. Haga clic en **Asociar usuarios finales** en la parte inferior de la ventana de configuración del teléfono para asociar a un usuario a la línea que se está configurando.

a) Use la opción **Buscar** y los campos de búsqueda para localizar al usuario.
b) Marque la casilla de verificación situada junto al nombre de usuario y haga clic en **Agregar seleccionados**.

El nombre de usuario y el ID de usuario aparecen en el panel Usuarios asociados con línea de la ventana de configuración del número de directorio.

c) Seleccione **Guardar**.

El usuario está ya asociado con la línea 1 en el teléfono.

Paso 11 (Opcional) Asocie al usuario con el dispositivo:

a) Seleccione **Administración de usuarios** > **Usuario final**.
b) Use los cuadros de búsqueda y la opción **Buscar** para localizar al usuario que ha agregado.
c) Haga clic en el ID de usuario.
d) En la sección Asociaciones del número de directorio de la pantalla, defina la Extensión primaria en la lista desplegable.
e) (Opcional) En la sección de información de movilidad, marque la casilla para activar la movilidad.
f) En la sección de información de permisos, use los botones de **Agregar a grupo de control de acceso** para agregar a este usuario a cualquier grupo de usuarios.

Por ejemplo, puede agregar al usuario a un grupo definido como Grupo de usuarios finales CCM estándar.

g) Para ver los detalles de un grupo, selecciónelo y haga clic en **Ver detalles**.
h) En la sección Extension Mobility, marque la casilla Habilitar extensión móvil entre clústeres en caso de que el usuario pueda usar este servicio.
i) En la sección de información del dispositivo, haga clic en **Asociaciones del dispositivo**.
j) Use los campos de búsqueda y la opción **Buscar** para localizar el dispositivo que desea asociar al usuario.
k) Seleccione el dispositivo y haga clic en **Guardar Seleccionados/Cambios**.
l) Haga clic en la opción **Ir** situada junto al enlace relacionado «Volver al usuario» de la esquina superior derecha de la pantalla.
m) Seleccione **Guardar**.

Paso 12 Personalice las plantillas de teclas programadas. Seleccione **Dispositivo** > **Configuración del dispositivo** > **Plantilla de teclas programadas**.

Use la página para agregar, eliminar o cambiar el orden de las teclas programadas que se muestran en el teléfono del usuario según las necesidades de uso de este.

El teléfono para conferencias tiene requisitos de tecla programable especiales. Consulte los enlaces relacionados para obtener más información.

Paso 13 Configure los servicios de teléfono IP de Cisco y asígnelos. Seleccione **Dispositivo** > **Configuración del dispositivo** > **Servicios de telefonía**.

Proporcione servicios de teléfono IP al teléfono.

Nota Los usuarios pueden agregar o cambiar servicios en sus teléfonos mediante el portal de autoayuda de Cisco Unified Communications.

Paso 14 (Opcional) Agregue la información del usuario al directorio global para Cisco Unified Communications Manager. Seleccione **Administración de usuarios** > **Usuario final**, haga clic en **Agregar nuevo** y configure los campos requeridos. Los campos requeridos se indican con un asterisco (*).

Nota Si su empresa usa un directorio LDAP (protocolo de acceso a directorios ligero) para almacenar información sobre los usuarios, puede instalar y configurar Cisco Unified Communications para emplear su directorio LDAP actual; consulte Configuración del directorio corporativo, en la página 127. Si activa el campo Habilitar sincronización en los campos del servidor LDAP, no podrá agregar usuarios adicionales desde Cisco Unified Communications Manager Administration.

a) Defina los campos de ID y apellidos del usuario.
b) Asigne una contraseña (para el portal de autoayuda).
c) Asigne un PIN (para Cisco Extension Mobility y el directorio personal).
d) Asocie el usuario con un teléfono.

Proporcione a los usuarios control sobre su teléfono; por ejemplo, para que puedan desviar llamadas o agregar números de marcación rápida o servicios.

Nota Algunos teléfonos, como los que se encuentran en las salas de conferencias, no tienen ningún usuario asociado.

Paso 15 (Opcional) Asocie un usuario a un grupo de usuarios. Seleccione **Administración de usuarios** > **Configuración de usuario** > **Grupo de control de acceso**.

Asigne a los usuarios una lista común de funciones y permisos que se apliquen a todos los usuarios de un grupo de usuarios. Los administradores pueden administrar grupos de usuarios, funciones y permisos a fin de controlar el nivel de acceso (y, por lo tanto, el nivel de seguridad) de los usuarios del sistema.

Para que los usuarios finales puedan acceder al portal Autogestión de Cisco Unified Communications, debe agregar usuarios al grupo de usuarios finales estándar de Cisco Communications Manager.

Temas relacionados

Configuración específica del producto, en la página 100
Configuración y características del teléfono IP para conferencias de Cisco, en la página 95
Cisco Unified Communications Manager Documentación, en la página 14
Configuración de una nueva plantilla de teclas programables, en la página 96

Determinación de la dirección MAC del teléfono

Para agregar teléfonos a Cisco Unified Communications Manager, debe determinar la dirección MAC de un teléfono.

Procedimiento

Lleve a cabo una de las acciones siguientes:

- En el teléfono, seleccione **Configuración** > **Información del teléfono** y busque el campo Dirección MAC.
- Busque la etiqueta MAC en la parte trasera del teléfono.
- Abra la página web del teléfono y haga clic en **Información de dispositivo**.

Métodos de adición de teléfonos

Antes de instalar el teléfono IP de Cisco, debe seleccionar una de las opciones siguientes para agregar teléfonos a la base de datos de Cisco Unified Communications Manager.

- Adición de teléfonos de manera individual con Cisco Unified Communications Manager Administration.
- Adición de varios teléfonos con la herramienta de administración masiva (BAT).
- Registro automático.
- BAT y la herramienta para la asistencia de teléfonos registrados automáticamente (TAPS).

Antes de agregar teléfonos individualmente o con BAT, necesita la dirección MAC del teléfono. Para obtener más información, consulte Determinación de la dirección MAC del teléfono, en la página 60.

Para obtener más información sobre la Herramienta de administración por lotes, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

Adición de teléfonos individualmente

Recopile la dirección MAC y la información del teléfono que desea agregar a Cisco Unified Communications Manager.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Dispositivo** > **Teléfono**.

Paso 2 Haga clic en **Agregar nuevo.**

Paso 3 Seleccione el tipo de teléfono.

Paso 4 Seleccione **Siguiente**.

Paso 5 Complete la información sobre el teléfono, incluida la dirección MAC.

Para obtener instrucciones completas e información conceptual sobre Cisco Unified Communications Manager, consulte la documentación de su versión concreta de este sistema.

Paso 6 Seleccione **Guardar**.

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

Adición de teléfonos con una plantilla de teléfono de BAT

La Herramienta de administración por lotes (BAT) de Cisco Unified Communications permite realizar operaciones por lotes, incluido el registro de varios teléfonos.

Para agregar teléfonos solo mediante BAT (no junto con TAPS), debe obtener la dirección MAC adecuada de cada teléfono.

Para obtener más información sobre el uso de BAT, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Procedimiento

Paso 1 En Cisco Unified Communications Administration, seleccione **Administración masiva** > **Teléfonos** > **Plantilla de teléfono**.

Paso 2 Haga clic en **Agregar nuevo.**

Paso 3 Seleccione un tipo de teléfono y haga clic en **Siguiente**.

Paso 4 Introduzca los detalles de los parámetros específicos del teléfono, como el grupo de dispositivos, la plantilla de botones de teléfono y el perfil de seguridad del dispositivo.

Paso 5 Haga clic en **Guardar**.

Paso 6 Seleccione **Dispositivo** > **Teléfono** > **Nuevo** para agregar un teléfono mediante la plantilla de teléfono de BAT.

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

Adición de usuarios a Cisco Unified Communications Manager

Puede mostrar y modificar la información sobre los usuarios registrados en Cisco Unified Communications Manager. Cisco Unified Communications Manager también permite a cada usuario realizar estas tareas:

- Acceder al directorio corporativo y a otros directorios personalizados desde un teléfono IP de Cisco.
- Crear un directorio personal.

- Configurar números de marcación rápida y de desvío de llamadas.
- Suscribirse a servicios a los que se puede acceder desde un teléfono IP de Cisco.

Procedimiento

Paso 1 Para agregar usuarios individualmente, consulte Adición de un usuario directamente a Cisco Unified Communications Manager, en la página 62.

Paso 2 Para agregar usuarios en lotes, use la Herramienta de administración por lotes. Este método también permite establecer una contraseña predeterminada idéntica para todos los usuarios.

Para obtener más datos, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

Adición de usuarios desde un directorio LDAP externo

Si ha agregado a un usuario a un directorio LDAP (un directorio que no sea de un servidor de Cisco Unified Communications), puede sincronizar de inmediato el directorio LDAP con la instancia de Cisco Unified Communications Manager en la que vaya a agregar al usuario y su teléfono.

Nota Si no sincroniza el directorio LDAP con Cisco Unified Communications Manager de inmediato, la programación de sincronización de la ventana Directorio LDAP determina cuándo está prevista la siguiente sincronización automática. La sincronización se puede producir antes de que pueda asociar un usuario nuevo a un dispositivo.

Procedimiento

Paso 1 Inicie sesión en Cisco Unified Communications Manager Administration.

Paso 2 Seleccione **Sistema** > **LDAP** > **Directorio LDAP**.

Paso 3 Use la opción **Buscar** para localizar su directorio LDAP.

Paso 4 Haga clic en el nombre del directorio LDAP.

Paso 5 Haga clic en **Realizar sincronización completa ahora**.

Adición de un usuario directamente a Cisco Unified Communications Manager

Si no usa un directorio LDAP (protocolo de acceso a directorio ligero), puede agregar a un usuario directamente con Cisco Unified Communications Manager Administration mediante estos pasos.

Nota Si LDAP se sincroniza, no podrá agregar a un usuario con Cisco Unified Communications Manager Administration.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Administración de usuarios** > **Usuario final**.

Paso 2 Haga clic en **Agregar nuevo.**

Paso 3 En el panel Información de usuario, introduzca lo siguiente:

- ID de usuario: Introduzca el nombre de identificación del usuario final. Cisco Unified Communications Manager no permite modificar el ID de usuario una vez creado. Puede usar los caracteres especiales siguientes: =, +, <, >, #,;, \,, «», así como espacios en blanco. **Ejemplo**: juansalas.
- Contraseña y Confirmar contraseña: introduzca al menos cinco caracteres alfanuméricos o especiales para la contraseña del usuario final. Puede usar los caracteres especiales siguientes: =, +, <, >, #,;, \,, «», así como espacios en blanco.
- Apellidos: Introduzca los apellidos del usuario final. Puede utilizar los siguientes caracteres especiales: =, +, <, >, #, ;, \, , «», así como espacios en blanco. **Ejemplo**: salas.
- Número de teléfono: introduzca el número de directorio principal del usuario final. Los usuarios finales pueden tener varias líneas en sus teléfonos. **Ejemplo**: 26640 (el número de teléfono empresarial interno de Juan Salas).

Paso 4 Haga clic en **Guardar**.

Adición de un usuario a un grupo de usuarios finales

Para agregar un usuario al grupo de usuarios finales estándar de Cisco Unified Communications Manager, lleve a cabo estos pasos:

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Administración de usuarios** > **Configuración de usuario** > **Grupo de control de acceso**.

Se abre la ventana de búsqueda y lista de usuarios.

Paso 2 Introduzca los criterios de búsqueda oportunos y haga clic en **Buscar**.

Paso 3 Seleccione el enlace **Usuarios finales de CCM estándar**. Se abre la ventana de configuración del grupo de usuario para los usuarios finales de CCM estándar.

Paso 4 Seleccione **Agregar usuarios finales a grupo**. Se abre la ventana de búsqueda y lista de usuarios.

Paso 5 Use los cuadros de lista desplegable Buscar usuario para localizar a los usuarios que desea agregar y haga clic en **Buscar**.

Se muestra una lista de usuarios que coinciden con los criterios de búsqueda.

Paso 6 En la lista de registros que aparece, haga clic en la casilla de verificación situada junto a los usuarios que desee agregar al grupo. Si la lista es larga, use los enlaces de la parte inferior para ver más resultados.

Nota La lista de resultados de la búsqueda no muestra a los usuarios que ya pertenecen al grupo.

Paso 7 Seleccione **Agregar seleccionados**.

Asociación de teléfonos con usuarios

Los teléfonos se asocian con los usuarios en la ventana Usuario final de Cisco Unified Communications Manager.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Administración de usuarios** > **Usuario final**.

Se abre la ventana de búsqueda y lista de usuarios.

Paso 2 Introduzca los criterios de búsqueda oportunos y haga clic en **Buscar**.

Paso 3 En la lista de registros que aparecen, seleccione el enlace del usuario.

Paso 4 Seleccione **Asociación de dispositivo**.

Se abre la ventana de asociación de dispositivo del usuario.

Paso 5 Introduzca los criterios de búsqueda oportunos y haga clic en **Buscar**.

Paso 6 Para seleccionar el dispositivo que desea asociar con el usuario, marque la casilla de verificación situada a la izquierda del dispositivo.

Paso 7 Seleccione **Guardar Seleccionados/Cambios** para asociar el dispositivo con el usuario.

Paso 8 En la lista desplegable Enlaces relacionados de la esquina superior derecha de la ventana, seleccione **Volver al usuario** y haga clic en **Ir**.

Se abre la ventana de configuración del usuario final y, en el panel de dispositivos controlados se muestran los dispositivos asociados que ha seleccionado.

Paso 9 Seleccione **Guardar Seleccionados/Cambios**.

Survivable Remote Site Telephony

Survivable Remote Site Telephony (SRST) garantiza que es posible seguir accediendo a las funciones básicas del teléfono si la comunicación con la instancia de Cisco Unified Communications Manager de control se

interrumpe. En esa situación, el teléfono puede mantener una llamada activa en curso y el usuario puede acceder a un subconjunto de las funciones disponibles. Si se produce un fallo de comunicación, el usuario recibe un mensaje de alerta en el teléfono.

Para obtener información sobre SRST, consulte https://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/tsd-products-support-series-home.html

En la tabla siguiente se describen las funciones que están disponibles durante el fallo.

Tabla 14: Compatibilidad de funciones de SRST

Función	Compatible	Notas
Nueva llamada	Sí	
Fin llamada	Sí	
Rellamar	Sí	
Contestar	Sí	
Espera	Sí	
Continuar	Sí	
Conferencia	Sí	Solo a tres partes y solo con combinación local.
Lista de conferencias	No	
Transferencia	Sí	Solo para consulta.
Transferencia a llamadas activas (transferencia directa)	No	
Contestación automática	Sí	
Llamada en espera	Sí	
Identificar a la persona que llama	Sí	
Presentación de sesión unificada	Sí	La única función admitida es Conferencia debido a las limitaciones de las demás características.
Buzón de voz	Sí	El buzón de voz no se sincroniza con otros usuarios del clúster de Cisco Unified Communications Manager.

Función	Compatible	Notas
Desvío incondicional	Sí	El estado de desvío solo está disponible en el teléfono que establece el desvío, ya que en el modo SRST no hay apariencias de línea compartida. Los ajustes de Desvío incondicional de Cisco Unified Communications Manager no se conservan durante el fallo en SRST, ni se recuperan tras el fallo de SRST a Communications Manager. Todos los desvíos incondicionales aún en curso en Communications Manager deben indicarse cuando el dispositivo se vuelve a conectar con Communications Manager después del fallo de comunicación.
Marcación rápida	Sí	
Al buzón de voz (Desviar)	No	No se muestra la tecla programada Desviar.
Filtros de línea	Parcial	Las líneas son compatibles pero no se pueden compartir.
Supervisión de aparcamiento	No	No se muestra la tecla programada Aparcar.
Indicación de mensaje en espera mejorada	sí	Las señales de recuento de mensajes aparecen en la pantalla del teléfono.
Aparcamiento de llamadas dirigido	No	No se muestra la tecla programada.
Reversión en espera	sí	
Espera remota	No	Las llamadas aparecen como llamadas en espera local.
Meet Me	No	No se muestra la tecla programada Meet Me.
Captura	sí	
Captura de llamadas de grupo	No	No se muestra la tecla programada.
Captura de otros	No	No se muestra la tecla programada.
ID de llamadas maliciosas	sí	
QRT	sí	
Grupo de salto	No	No se muestra la tecla programada.
Movilidad	No	No se muestra la tecla programada.
Privacidad	No	No se muestra la tecla programada.

Función	Compatible	Notas
Retrollamada	No	No se muestra la tecla programada Retrollamada.
URL de servicio	sí	No se muestra la tecla de línea programable con una URL de servicio asignada.

CAPÍTULO 6

Administración del portal de autoayuda

Descripción general del portal de autoayuda

En el portal de autoayuda de Cisco Unified Communications, los usuarios pueden personalizar y controlar las funciones y la configuración del teléfono.

Como administrador, se encarga de controlar el acceso al portal de autoayuda. También debe proporcionar información a los usuarios para que puedan acceder al portal de autoayuda.

Para que un usuario pueda acceder al portal de autoayuda de Cisco Unified Communications, usted debe usar Cisco Unified Communications Manager Administration para agregar al usuario a un grupo estándar de usuarios finales de Cisco Unified Communications Manager.

Debe proporcionar a los usuarios finales la información siguiente sobre el portal de autoayuda:

- La dirección URL para acceder a la aplicación. La URL es:

  `https://<server_name:portnumber>/ucmuser/`, donde server_name es el host en el que está instalado el servidor web y portnumber es el número del puerto en ese host.

- Un ID de usuario y una contraseña predeterminada para acceder a la aplicación.

- Una descripción general de las tareas que los usuarios pueden realizar con el portal.

Estos ajustes corresponden a los valores que introduce al agregar al usuario en Cisco Unified Communications Manager.

Para obtener más datos, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

Configuración del acceso de usuario al portal de autoayuda

Para que un usuario pueda acceder al portal de autoayuda, debe autorizar su acceso.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Administración de usuarios** > **Usuario final**.

Paso 2 Busque el usuario.

Paso 3 Haga clic en el enlace del ID de usuario.

Paso 4 Asegúrese de que el usuario tiene configurados una contraseña y un PIN.

Paso 5 En la sección Información de permisos, asegúrese de que la lista Grupos incluya **Usuarios finales de CCM estándar**.

Paso 6 Seleccione **Guardar**.

Personalización de la presentación del portal de autoayuda

En el portal de autoayuda se muestran la mayoría de las opciones. Sin embargo, debe establecer las opciones siguientes mediante los ajustes de la configuración de parámetros empresariales en Cisco Unified Communications Manager Administration:

- Mostrar configuración de timbre.
- Mostrar configuración de etiqueta de línea.

Nota La configuración se aplica a todas las páginas del portal de autoayuda del sitio.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Sistema** > **Parámetros empresariales**.

Paso 2 En la sección Portal de autoayuda, establezca el campo **Servidor predeterminado del portal de autoayuda**.

Paso 3 Active o desactive los parámetros a los que puede acceder el usuario en el portal.

Paso 4 Seleccione **Guardar**.

PARTE III

Administración del teléfono IP para conferencias de Cisco

CAPÍTULO 7

Seguridad del teléfono IP para conferencias de Cisco

Descripción general de la seguridad del teléfono IP de Cisco

Las funciones de seguridad protegen contra muchas amenazas, como las relacionadas con la identidad del teléfono y con los datos. Estas funciones establecen y mantienen secuencias de comunicación autenticadas entre el teléfono y el servidor de Cisco Unified Communications Manager y garantizan que el teléfono use solo archivos firmados digitalmente.

La versión 8.5(1) y posteriores de Cisco Unified Communications Manager incluyen la característica Seguridad predeterminada, que proporciona las siguientes funciones de seguridad para los teléfonos IP de Cisco sin tener que ejecutar el cliente de CTL:

- Firma de los archivos de configuración del teléfono.
- Cifrado del archivo de configuración del teléfono.
- HTTPS con Tomcat y otros servicios web.

Nota Para las funciones de señales y medios seguros sigue siendo necesario ejecutar el cliente de CTL y usar tokens electrónicos de hardware.

Para obtener más información sobre las funciones de seguridad, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Después de realizar las tareas necesarias asociadas con la función proxy de entidad emisora de certificados (CAPF), en los teléfonos se instala un Locally Significant Certificate (LSC). Puede usar Cisco Unified Communications Manager Administration para configurar un LSC. Para obtener más datos, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Un LSC no puede utilizarse como certificado de usuario para EAP-TLS con autenticación de WLAN.

Como alternativa, puede iniciar la instalación de un LSC desde el menú de configuración de seguridad del teléfono. Este menú permite actualizar o eliminar un LSC.

El teléfono IP 8832 para conferencias de Cisco cumple con el estándar federal de procesamiento de información (FIPS). Para que funcione correctamente, el modo FIPS requiere un tamaño de clave RSA de 2048 bits o mayor. Si el certificado de servidor RSA no es de 2048 bits o superior, el teléfono no se registrará con Cisco Unified Communications Manager y se muestra `Fallo al registrar el teléfono. El tamaño de clave de certificado no cumple con FIPS` en los mensajes de estado del teléfono.

No puede utilizar las claves privadas (LSC o MIC) en el modo FIPS.

Si el teléfono tiene un LSC que sea menor que 2048 bits, deberá actualizar el tamaño de clave LSC a 2048 bits como mínimo antes de activar FIPS.

Temas relacionados

Configuración de un certificado significativo local, en la página 77
Cisco Unified Communications Manager Documentación, en la página 14

Mejoras de seguridad para la red del teléfono

Puede activar Cisco Unified Communications Manager 11.5 (1) y 12.0(1) para que funcione en un entorno de seguridad mejorado. Con estas mejoras, la red del teléfono funciona en un conjunto de controles estrictos de administración de riesgos y seguridad para protegerle a usted y a sus usuarios.

Cisco Unified Communications Manager 12.5(1) no es compatible con un entorno de seguridad mejorado. Desactive FIPS antes de actualizar a Cisco Unified Communications Manager 12.5(1) o su TFTP y demás servicios no funcionarán correctamente.

El entorno de seguridad mejorado incluye las siguientes funciones:

- Autenticación de búsqueda de contactos.
- TCP como protocolo predeterminado para el inicio de sesión remoto de auditoría.
- Modo FIPS.
- Una política de credenciales mejorada.
- Compatibilidad con la familia de SHA-2 de hash para firmas digitales.
- Compatibilidad con un tamaño de clave RSA de 512 y 4096 bits.

Con Cisco Unified Communications Manager versión 14.0 y el firmware versión 14.0 y posterior del teléfono IP de Cisco, los teléfonos admiten la autenticación de OAuth de SIP.

OAuth es compatible con el protocolo de transferencia de archivos trivial (TFTP) de proxy con Cisco Unified Communications Manager versión 14.0(1)SU1 o posterior, así como con el la versión 14.1(1) del firmware del teléfono IP de Cisco. Proxy TFTP y OAuth para proxy TFTP no son compatibles con el Mobile Remote Access (MRA).

Para obtener información adicional sobre la seguridad, consulte lo siguiente:

- *Guía de configuración del sistema para Cisco Unified Communications Manager*, versión 14.0(1) o posterior (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html).

- *Guía de seguridad de Cisco Unified Communications Manager* (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html)
- OAuth de SIP: *Guía de configuración de funciones de Cisco Unified Communications Manager* (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html)

Nota Su teléfono IP de Cisco solo puede almacenar un número limitado de archivos de la lista de confianza de identidad (ITL). Los archivos ITL no pueden superar el límite de 64.000 en el teléfono, por lo que debe limitar el número de archivos que Cisco Unified Communications Manager puede enviar al teléfono.

Características de seguridad admitidas

Las funciones de seguridad protegen contra muchas amenazas, como las relacionadas con la identidad del teléfono y con los datos. Estas funciones establecen y mantienen secuencias de comunicación autenticadas entre el teléfono y el servidor de Cisco Unified Communications Manager y garantizan que el teléfono use solo archivos firmados digitalmente.

La versión 8.5(1) y posteriores de Cisco Unified Communications Manager incluyen la característica Seguridad predeterminada, que proporciona las siguientes funciones de seguridad para los teléfonos IP de Cisco sin tener que ejecutar el cliente de CTL:

- Firma de los archivos de configuración del teléfono.
- Cifrado del archivo de configuración del teléfono.
- HTTPS con Tomcat y otros servicios web.

Nota Para las funciones de señales y medios seguros sigue siendo necesario ejecutar el cliente de CTL y usar tokens electrónicos de hardware.

Al implementar seguridad en el sistema Cisco Unified Communications Manager se evitan robos de identidad del teléfono y del servidor de Cisco Unified Communications Manager y se impide la alteración de los datos, así como de las señales de llamadas y los flujos de medios.

Para proteger contra estas amenazas, la red de telefonía IP de Cisco establece y mantiene flujos de comunicación seguros (cifrados) entre un teléfono y el servidor, firma digitalmente los archivos antes de transferirlos a un teléfono y cifra los flujos de medios y las señales de llamada entre los teléfonos IP de Cisco.

Después de realizar las tareas necesarias asociadas con la función proxy de entidad emisora de certificados (CAPF), en los teléfonos se instala un Locally Significant Certificate (LSC). Puede usar Cisco Unified Communications Manager Administration para configurar un LSC, como se describe en la Guía de seguridad de Cisco Unified Communications Manager. Como alternativa, puede iniciar la instalación de un LSC desde el menú de configuración de seguridad del teléfono. Este menú permite actualizar o eliminar un LSC.

Un LSC no puede utilizarse como certificado de usuario para EAP-TLS con autenticación de WLAN.

Los teléfonos usan el perfil de seguridad, donde se define si el dispositivo es seguro o no lo es. Para obtener información sobre cómo aplicar el perfil de seguridad al teléfono, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Si configura los valores de seguridad en Cisco Unified Communications Manager Administration, el archivo de configuración del teléfono contendrá información confidencial. Para garantizar la privacidad del archivo de configuración, debe configurarlo para el cifrado. Para más detalles, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Al implementar seguridad en el sistema Cisco Unified Communications Manager se evitan robos de identidad del teléfono y del servidor de Cisco Unified Communications Manager y se impide la alteración de los datos, así como de las señales de llamadas y los flujos de medios.

En la tabla siguiente se ofrece una descripción general de las funciones de seguridad que admite el teléfono IP 8832 para conferencias de Cisco. Para obtener más información sobre estas funciones, Cisco Unified Communications Manager y la seguridad del teléfono IP de Cisco, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Tabla 15: Descripción general de funciones de seguridad

Función	Descripción
Autenticación de imagen	Los archivos binarios firmados (con la extensión .sbn) evitan q alterar la imagen, el proceso de autenticación del teléfono falla
Instalación de certificado del sitio del cliente	Cada teléfono necesita un certificado exclusivo para la autentic (MIC), pero para aportar más seguridad, es posible especificar certificado mediante la función proxy de entidad de certificaci (LSC) desde el menú de configuración de seguridad del teléfo
Autent. dispositivo	Se produce entre el servidor de Cisco Unified Communication Determina si se debe producir una conexión segura entre el tel necesario, crea una ruta de señalización segura entre las entida registrará los teléfonos a no ser que los pueda autenticar.
Autenticación del archivo	Valida los archivos firmados digitalmente que descarga el telé alterado después de su creación. Los archivos que no superan l rechaza esos archivos sin procesarlos más.
Autenticación de señalización	Se usa el protocolo TLS para validar que los paquetes de señal
Certificado instalado en fábrica	Cada teléfono contiene un certificado instalado en fábrica (MI identidad única permanente del teléfono y permite a Cisco Uni
Referencia SRST segura	Después de configurar una referencia SRST para la seguridad Communications Manager Administration, el servidor TFTP a al teléfono. A continuación, un teléfono seguro usa una conexi
Cifrado de medios	Usa SRTP para garantizar que los flujos de medios entre los di lea los datos. Incluye la creación de un par de claves principale la seguridad necesaria en la entrega de las claves mientras esta
Función proxy de entidad emisora de certificados (CAPF)	Implementa partes del procedimiento de generación del certifi teléfono para generar la clave e instalar el certificado. La funci emisoras especificadas por el cliente en nombre del teléfono, c

Función	Descripción
Perfiles de seguridad	Define si el teléfono no es seguro o si está autenticado o ci
Archivos de configuración cifrados	Permite garantizar la privacidad de los archivos de configu
Desactivación opcional de la función de servidor web de un teléfono	Es posible impedir el acceso a la página web de un teléfon
Fortalecimiento del teléfono	Opciones de seguridad adicionales que se pueden controla • Desactivar el acceso a las páginas web en un teléfono. **Nota** Puede consultar la configuración actual de las del teléfono.
Autenticación 802.1X	El teléfono puede usar la autenticación 802.1X para solicit
Cifrado AES 256	Si se conectan a la versión 10.5(2) y posteriores de Cisco U TLS y SIP para el cifrado de las señales y los medios. Esto basado en AES-256 que cumpla los estándares SHA-2 (alg (FIPS) de Estados Unidos. Los nuevos cifrados son los sig • Para las conexiones TLS: • TLS_ECDHE_RSA_WITH_AES_256_GCM_S • TLS_ECDHE_RSA_WITH_AES_128_GCM_S • Para sRTP: • AEAD_AES_256_GCM • AEAD_AES_128_GCM Para obtener más datos, consulte la documentación de Cisc
Certificados de Elliptic Curve Digital Signature Algorithm (ECDSA).	Como parte de la certificación Common Criteria (CC), Cis 11.0. Esto afecta a todos los productos de sistemas operativ

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

Configuración de un certificado significativo local

Esta tarea se aplica a la configuración de un LSC con el método de cadena de autenticación.

Antes de empezar

Asegúrese de que las configuraciones de seguridad de la instancia adecuada de Cisco Unified Communications Manager y de la función proxy de entidad emisora de certificados (CAPF) están completas:

- El archivo CTL o ITL tiene un certificado CAPF.

- En la administración del sistema operativo de Cisco Unified Communications, compruebe que el certificado CAPF está instalado.
- CAPF se está ejecutando y se ha configurado.

Para obtener más información sobre estos ajustes, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Procedimiento

Paso 1 Obtenga el código de autenticación de CAPF que se estableció cuando se configuró CAPF.

Paso 2 En el teléfono, elija **Configuración**.

Paso 3 Elija **Config. admin.** > **Configuración de seguridad**.

Nota Puede controlar el acceso al menú Configuración mediante el campo Acceso a la configuración en la ventana de configuración del teléfono de Cisco Unified Communications Manager Administration.

Paso 4 Seleccione **LSC** y pulse **Seleccionar** o **Actualizar**.

Se le solicitará que introduzca una cadena de autenticación en el teléfono.

Paso 5 Introduzca el código de autenticación y pulse **Enviar**.

El teléfono empieza a instalar, actualizar o eliminar el LSC, según cómo se haya configurado CAPF. Durante el procedimiento, aparece una serie de mensajes en el campo de opciones del LSC del menú Configuración de seguridad para que pueda supervisar el progreso. Cuando se complete el procedimiento, se mostrarán las indicaciones Instalado o No instalado en el teléfono.

El proceso de instalación, actualización o eliminación del LSC puede tardar algún tiempo en completarse.

Si el proceso de instalación del teléfono se realiza correctamente, se muestra el mensaje `Instalado`. Si en el teléfono se muestra `No instalado`, puede que la cadena de autorización sea incorrecta o que la actualización del teléfono no se haya activado. Si la operación de CAPF elimina el LSC, en el teléfono se muestra el mensaje `No instalado` para indicar que la operación se ha realizado correctamente. Los mensajes de error se registran en el servidor CAPF. Consulte la documentación del servidor CAPF para localizar los registros y comprender los mensajes de error.

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

Activación del modo FIPS

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Dispositivo** > **Teléfono** y localice el teléfono.

Paso 2 Diríjase a la sección de configuración específica del producto.

Paso 3 Establezca el campo **Modo FIPS** en Activado.

Paso 4 Seleccione **Aplicar configuración**.

Paso 5 Seleccione **Guardar**.

Paso 6 Reinicie el teléfono.

Seguridad de las llamadas telefónicas

Cuando se implementa la seguridad para un teléfono, es posible identificar las llamadas seguras por los iconos de la pantalla del teléfono. También se puede determinar si el teléfono conectado es seguro y está protegido por el tono de seguridad que se reproduce al principio de la llamada.

En una llamada segura, todas las señales de llamada y los flujos de medios están cifrados. Una llamada segura ofrece un alto nivel de seguridad y aporta integridad y privacidad. Si una llamada en curso está cifrada, el icono de progreso de la llamada a la derecha del temporizador de duración de la llamada en la pantalla del teléfono cambia al icono siguiente:  .

Nota Si la llamada se enruta a través de segmentos que no son IP, por ejemplo, PSTN, podría no ser segura aunque esté cifrada dentro de la red IP y tenga asociado un icono de candado.

En una llamada segura, el tono de seguridad se reproduce al principio para indicar que el otro teléfono conectado también recibe y transmite audio seguro. Si la llamada se conecta a un teléfono no protegido, no se reproduce el tono de seguridad.

Nota Las llamadas seguras se admiten entre dos teléfonos. Es posible configurar una conferencia segura, Cisco Extension Mobility y líneas compartidas mediante un puente de conferencia seguro.

Si un teléfono está configurado como seguro (cifrado y de confianza) en Cisco Unified Communications Manager, se le puede asignar el estado de «protegido». Después, y si así lo desea, el teléfono protegido se puede configurar para que reproduzca un tono de indicación al principio de una llamada:

- Dispositivo protegido: para cambiar el estado de un teléfono seguro a protegido, marque la casilla de verificación Dispositivo protegido en la ventana de configuración del teléfono en Cisco Unified Communications Manager Administration (**Dispositivo** > **Teléfono**).
- Reproducir tono de indicación de seguridad: para permitir que el teléfono protegido reproduzca un tono de indicación de seguridad o de llamada no segura, establezca el valor Verdadero en el ajuste Reproducir tono de indicación de seguridad. De forma predeterminada, el valor es Falso. Esta opción se puede establecer en Cisco Unified Communications Manager Administration (**Sistema** > **Parámetros de servicio**). Seleccione el servidor y el servicio Unified Communications Manager. En la ventana de configuración del parámetro de servicio, seleccione la opción del área Función - Tono seguro. Por defecto es Falso.

Identificación de llamadas de conferencia seguras

Puede iniciar una llamada de conferencia segura y supervisar el nivel de seguridad de los participantes. Para establecer una llamada de conferencia segura, se usa este procedimiento:

1. Un usuario inicia la conferencia desde un teléfono seguro.
2. Cisco Unified Communications Manager asigna un puente de conferencia segura a la llamada.
3. A medida que se agregan participantes, Cisco Unified Communications Manager verifica el modo de seguridad de cada teléfono y mantiene el nivel de seguridad para la conferencia.
4. El teléfono muestra el nivel de seguridad de la llamada de conferencia. En las conferencias seguras se muestra el icono de seguridad a la derecha de **Conferencia** en la pantalla del teléfono.

Nota Las llamadas seguras se admiten entre dos teléfonos. En los teléfonos protegidos, algunas funciones, como la llamada de conferencia, las líneas compartidas y Extension Mobility no se encuentran disponibles cuando se configura la llamada segura.

En la tabla siguiente se proporciona información sobre los cambios de los niveles de seguridad de conferencias según el nivel de seguridad del teléfono que inicio la llamada, los niveles de seguridad de los participantes y la disponibilidad de puentes de conferencia seguros.

Tabla 16: Restricciones de seguridad con las llamadas de conferencia

Nivel de seguridad del teléfono que inicia la llamada	Función usada	Nivel de seguridad de los participantes	Resultados de la acción
No seguro	Conferencia	Seguro	Puente de conferencia no seguro. Conferencia no segura.
Seguro	Conferencia	Al menos un miembro no es seguro	Puente de conferencia seguro. Conferencia no segura.
Seguro	Conferencia	Seguro	Puente de conferencia seguro. Conferencia de nivel de cifrado seguro.

No seguro	Meet Me	Nivel de seguridad mínimo cifrado	El teléfono que inicia la llamada recibe el mer
			`cumple el nivel de seguridad, l`
			`rechazada.`

Seguro	Meet Me	Nivel de seguridad mínimo no seguro	Puente de conferencia seguro. La conferencia acepta todas las llamadas.

Identificación de llamadas telefónicas seguras

Una llamada segura se establece cuando su teléfono y el del interlocutor se configuran para las llamadas seguras. El otro teléfono puede encontrarse en la misma red IP de Cisco o en otra red distinta. Las llamadas

seguras solo se pueden realizar entre dos teléfonos. Las llamadas de conferencia podrían admitir una llamada segura tras configurar un puente de conferencia segura.

Para establecer una llamada segura se usa este procedimiento:

1. Un usuario inicia la llamada desde un teléfono seguro (modo de seguridad garantizada).
2. El teléfono muestra el icono de seguridad en la pantalla. Este icono indica que el teléfono está configurado para las llamadas seguras, pero eso no significa que el otro teléfono conectado también lo esté.
3. El usuario oye un tono de seguridad si la llamada se conecta a otro teléfono seguro, lo que indica que ambos extremos de la conversación están cifrados y son seguros. Si se establece una llamada con un teléfono no seguro, el usuario no oye el tono de seguridad.

Nota Las llamadas seguras se admiten entre dos teléfonos. En los teléfonos protegidos, algunas funciones, como la llamada de conferencia, las líneas compartidas y Extension Mobility no se encuentran disponibles cuando se configura la llamada segura.

Los tonos de indicación de seguridad o riesgo solo se reproducen en teléfonos protegidos. En los teléfonos no protegidos nunca se escuchan tonos. Si el estado de llamada general cambia durante una llamada, el tono de indicación cambia y el teléfono protegido emitirá el tono adecuado.

Los teléfonos protegidos emiten un tono en los siguientes casos:

- Si la opción para reproducir el tono de indicación de seguridad está activada:
  - Cuando se establecen medios seguros de extremo a extremo de la llamada y el estado de la llamada es seguro, el teléfono reproduce el tono de indicación de seguridad (tres pitidos largos con pausas).
  - Cuando se establecen medios no seguros de un extremo a otro de la llamada y el estado de la llamada es no seguro, el teléfono reproduce el tono de indicación de riesgo (seis pitidos largos con pausas cortas).

Si la opción para reproducir el tono de indicación de seguridad está desactivada, no se reproduce ningún tono.

Cifrado para la intrusión

Cisco Unified Communications Manager comprueba el estado de seguridad del teléfono cuando se establecen las conferencias y cambia la indicación correspondiente de esta o bloquea el final de la llamada para mantener la integridad y la seguridad del sistema.

Un usuario no puede realizar la intrusión en una llamada cifrada si el teléfono que utiliza no está configurado para el cifrado. Cuando la intrusión falla en este caso, se reproduce un tono de reordenar (ocupado rápido) en el teléfono donde se inició la intrusión.

Si el teléfono inicial está configurado para el cifrado, la persona que inicia la intrusión puede acceder a una llamada no segura desde el teléfono cifrado. Después de la intrusión, Cisco Unified Communications Manager clasifica la llamada como no segura.

Si el teléfono inicial está configurado para el cifrado, la persona que inicia la intrusión puede acceder a una llamada cifrada y el teléfono indica que la llamada está cifrada.

Seguridad de WLAN

Dado que todos los dispositivos WLAN que se encuentran dentro de la cobertura pueden recibir todos el tráfico de WLAN restante, asegurar las comunicaciones de voz resulta fundamental para las WLAN. Para garantizar que cualquier intruso no pueda manipular ni interceptar el tráfico de voz, la arquitectura Cisco SAFE Security es compatible con los puntos de acceso del teléfono IP de Cisco y de Cisco Aironet. Para obtener más información sobre la seguridad en las redes, consulte http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html.

La solución de telefonía IP inalámbrica de Cisco proporciona seguridad de la red inalámbrica que impide los inicios de sesión no autorizados y las comunicaciones peligrosas mediante el uso de los siguientes métodos de autenticación compatibles con el teléfono IP inalámbrico de Cisco:

- Autenticación abierta: cualquier dispositivo inalámbrico puede solicitar autenticación en un sistema abierto. El punto de acceso que recibe la petición puede otorgar la autenticación a cualquier solicitante o solo a los que se encuentren en una lista de usuarios. La comunicación entre el dispositivo inalámbrico y el punto de acceso podría no estar cifrada o los dispositivos pueden usar claves WEP (Wired Equivalent Privacy, privacidad equivalente a cableado) para proporcionar seguridad. Los dispositivos que usan WEP solo intentan autenticarse con un punto de acceso que use WEP.
- Autenticación de protocolo de autenticación ampliable-autenticación flexible a través de túnel seguro (EAP-FAST): esta arquitectura de seguridad cliente-servidor cifra las transacciones EAP en un túnel de seguridad de nivel de transporte (TLS) entre el punto de acceso y el servidor RADIUS, como el servidor Access Control Server (ACS) de Cisco.

  El túnel TLS usa credenciales de acceso protegidas (PAC) para la autenticación entre el cliente (el teléfono) y el servidor RADIUS. El servidor envía un ID de autoridad (AID) al cliente (el teléfono), que a su vez seleccione la PAC adecuada. El cliente (el teléfono) devuelve una PAC opaca al servidor RADIUS. El servidor descifra la PAC con la clave principal. Ambos terminales contienen ahora la clave de PAC y se crea el túnel TLS. EAP-FAST admite el aprovisionamiento automático de la PAC, pero hay que habilitarlo en el servidor RADIUS.

Nota En Cisco ACS, de forma predeterminada, la PAC caduca en una semana. Si el teléfono tiene una PAC caducada, la autenticación con el servidor RADIUS lleva más tiempo, ya que el teléfono debe conseguir una PAC nueva. Para evitar retrasos por el aprovisionamiento de la PAC, defina el período de caducidad de la PAC en 90 días o más en los servidores ACS o RADIUS.

- Autenticación EAP-TLS (protocolo de autenticación ampliable mediante seguridad de capa de transporte): EAP-TLS requiere un certificado de cliente para la autenticación y el acceso a la red. En el caso de EAP-TLS con cable, el certificado de cliente puede ser el MIC del teléfono o un LSC. LSC es el certificado de autenticación de cliente recomendado para EAP-TLS con cable.
- Protocolo de autenticación ampliable protegido (PEAP): el esquema de autenticación mutua basada en contraseña propiedad de Cisco entre el cliente (el teléfono) y un servidor RADIUS. El teléfono IP de Cisco puede usar PEAP para la autenticación con la red inalámbrica. Solo se admite PEAP-MSCHAPV2. PEAP-GTC no es compatible.

Los esquemas de autenticación siguientes usan el servidor RADIUS para administrar las claves de autenticación:

- WPA/WPA2: usa la información del servidor RADIUS para generar claves únicas para la autenticación. Dado que estas claves se generan en el servidor RADIUS centralizado, WPA/WPA2 proporciona más seguridad que las claves precompartidas WPA almacenadas en el punto de acceso y el teléfono.
- Itinerancia rápida y segura: usa la información del servidor RADIUS y de un servidor de dominio inalámbrico (WDS) para administrar y autenticar las claves. El WDS crea una memoria caché de credenciales de seguridad para los dispositivos cliente habilitados para CCKM a fin de conseguir una reautenticación rápida y segura. Los teléfonos IP serie 8800 de Cisco admiten 802.11r (FT). Se admiten 11r (FT) y CCKM para permitir una itinerancia rápida y segura. Pero Cisco recomienda utilizar el método de transferencia inalámbrica 802.11r (FT).

Con WPA/WPA2 y CCKM, las claves de cifrado no se introducen en el teléfono, sino que se derivan automáticamente entre el punto de acceso y el teléfono. Pero es preciso introducir el nombre de usuario y la contraseña de EAP que se usan para la autenticación en todos los teléfonos.

Para garantizar que el tráfico de voz sea seguro, el teléfono IP de Cisco admite WEP, TKIP y los estándares de cifrado avanzados (AES) para el cifrado. Si estos mecanismos se usan para el cifrado, tanto los paquetes SIP de señalización como los paquetes del protocolo de transporte en tiempo real (RTP) se cifran entre el punto de acceso y el teléfono IP de Cisco.

WEP

Con el uso de WEP en la red inalámbrica, la autenticación se produce en el punto de acceso mediante la autenticación abierta o con clave compartida. Para que las conexiones se realicen correctamente, la clave WEP que se configure en el teléfono debe coincidir con la que se configure en el punto de acceso. El teléfono IP de Cisco admite claves WEP que usen cifrado de 40 bits o de 128 bits y permanezcan estáticas en el teléfono y el punto de acceso.

Tanto la autenticación EAP como la CCKM pueden usar claves WEP para el cifrado. El servidor RADIUS administra las claves WEP y pasa una clave única al punto de acceso después de la autenticación para cifrar todos los paquetes de voz. Por consiguiente, estas claves WEP pueden cambiar en cada autenticación.

TKIP

Tanto WPA como CCKM usan el cifrado TKIP, que presenta muchas mejoras respecto a WEP. TKIP proporciona cifrado de claves por paquetes y vectores de inicialización más largos que mejoran el cifrado. Asimismo, una comprobación de integridad de mensajes (MIC) garantiza que los paquetes cifrados no se alteran. TKIP elimina la predictibilidad de WEP, que ayuda a los intrusos a descifrar las claves WEP.

AES

Un método de cifrado que se usa para la autenticación WPA2. Este estándar nacional para el cifrado usa un algoritmo simétrico que cuenta con la misma clave para el cifrado y el descifrado. AES usa el cifrado de cadena de bloqueo de código (CBC) de 128 bits de tamaño, que admite claves de 128, 192 y 256 bits, como mínimo. El teléfono IP de Cisco admite claves de 256 bits de tamaño.

Nota El teléfono IP de Cisco no admite el protocolo de integridad de claves de Cisco (CKIP) con CMIC.

Los esquemas de autenticación y cifrado se configuran dentro de la LAN inalámbrica. Las VLAN se configuran en la red y en los puntos de acceso e incluyen distintas combinaciones de autenticación y cifrado. Un SSID se asocia con una VLAN y con el esquema de autenticación y cifrado concreto. A fin de que los dispositivos cliente inalámbricos se autentiquen correctamente, debe configurar los mismos SSID con sus esquemas de autenticación y cifrado en los puntos de acceso y en el teléfono IP de Cisco.

Algunos esquemas de autenticación requieren tipos específicos de cifrado. Con la autenticación abierta, puede usar WEP estática para el cifrado a fin de aportar mayor seguridad. Pero si usa la autenticación de clave compartida, debe definir WEP estática para el cifrado y configurar una clave WEP en el teléfono.

Nota

- Si usa una clave precompartida WPA o WPA2, esta debe definirse para que permanezca estática en el teléfono. Las claves deben coincidir con las que se encuentran en el punto de acceso.
- El teléfono IP de Cisco no admite la negociación automática de EAP. Para usar el modo EAP-FAST, debe especificarlo.

En la tabla siguiente se proporciona una lista de los esquemas de autenticación y cifrado configurados en los puntos de acceso Cisco Aironet que admite el teléfono IP de Cisco. En la tabla se muestra la opción de configuración de red del teléfono que corresponde a la configuración del punto de acceso.

Tabla 17: Esquemas de autenticación y cifrado

Configuración del teléfono IP de Cisco	**Configuración del punto de acceso**			
Modo de seguridad	Seguridad	Gestión de claves	Cifrado	Itinerancia rápida
Ninguno	Ninguno	Ninguno	Ninguno	N/D
WEP	WEP estático	Estática	WEP	N/D
PSK	PSK	WPA	TKIP	Ninguna
		WPA2	AES	FT
EAP-FAST	EAP-FAST	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
EAP-TLS	EAP-TLS	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
PEAP-MSCHAPV2	PEAP-MSCHAPV2	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM

Para obtener más información sobre cómo configurar los esquemas de autenticación y cifrado en los puntos de acceso, consulte la *Guía de configuración de Cisco Aironet* de su modelo y versión en la siguiente dirección URL:

http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243

Seguridad de la LAN inalámbrica

Los teléfonos de Cisco compatibles con Wi-Fi tienen más requisitos de seguridad y requieren configuración adicional. Estos pasos adicionales incluyen la instalación de certificados y la configuración de la seguridad en los teléfonos y en Cisco Unified Communications Manager.

Para obtener información adicional, consulte la *Guía de seguridad de Cisco Unified Communications Manager*.

Página de administración del teléfono IP de Cisco

Los teléfonos Cisco compatibles con Wi-Fi tienen páginas web especiales que se diferencian de las páginas de otros teléfonos. Estas páginas especiales se utilizan para configurar la seguridad del teléfono cuando el protocolo de inscripción de certificado simple (SCEP) no está disponible. Utilice estas páginas para instalar manualmente los certificados de seguridad en un teléfono, descargar un certificado de seguridad o configurar manualmente la fecha y la hora del teléfono.

Estas páginas web también muestran la misma información que puede ver en otras páginas web del teléfono, incluida la información del dispositivo, la configuración de la red, los registros y la información estadística.

Configurar la página de administración del teléfono

La página web de administración se activa cuando el teléfono se envía de fábrica y la contraseña se establece como Cisco. Sin embargo, si un teléfono se registra con Cisco Unified Communications Manager, la página web de administración debe estar activada y la nueva contraseña configurada.

Active esta página web y establezca las credenciales de inicio de sesión antes de utilizar la página web por primera vez después de que el teléfono se haya registrado.

Una vez habilitada, se puede acceder a la página web de administración en el puerto HTTPS 8443 (**`https://x.x.x.x:8443`**, donde x.x.x.x es la dirección IP del teléfono).

Antes de empezar

Decida sobre una contraseña antes de activar la página web de administración. La contraseña puede ser cualquier combinación de letras o números, pero debe tener una longitud de entre 8 y 127 caracteres.

Su nombre de usuario se establece de forma permanente en admin.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Dispositivo** > **Teléfono**.

Paso 2 Localice su teléfono.

Paso 3 En la sección **Diseño de la configuración específica del producto**, establezca **Administrador web** en **Activado**.

Paso 4 En el campo **Contraseña del administrador**, introduzca una contraseña.

Paso 5 Seleccione **Guardar** y haga clic en **Aceptar**.

Paso 6 Seleccione **Aplicar configuración** y haga clic en **Aceptar**.

Paso 7 Reinicie el teléfono.

Acceda a la página web de administración del teléfono

Si desea acceder a las páginas web de administración, deberá especificar el puerto de administración.

Procedimiento

Paso 1 Obtener la dirección IP del teléfono:

- En Cisco Unified Communications Manager Administration, seleccione **Dispositivo** > **Teléfono** y localice el teléfono. Los teléfonos que se registran en Cisco Unified Communications Manager muestran la dirección IP en la ventana para buscar y mostrar teléfonos, en la parte superior de la ventana de configuración del teléfono.

Paso 2 Abra un navegador web e introduzca la dirección URL siguiente, donde *dirección_IP* es la dirección IP del teléfono IP de Cisco:

```
https://<IP_address>:8443
```

Paso 3 Especifique la contraseña en el campo Contraseña.

Paso 4 Haga clic en **Enviar**.

Instalación de un certificado de usuario desde la página web de administración del teléfono

Puede instalar manualmente un certificado de usuario en el teléfono si el protocolo de inscripción de certificado simple (SCEP) no está disponible.

El certificado instalado en fábrica (MIC) preinstalado puede utilizarse como certificado de usuario para EAP-TLS.

Después de que se instale el certificado de usuario, deberá agregarlo a la lista de confianza del servidor RADIUS.

Antes de empezar

Para instalar un certificado de usuario para un teléfono, debe tener:

- Un certificado de usuario guardado en su PC. El certificado debe estar en formato PKCS #12.
- La contraseña de extracción del certificado.

Procedimiento

Paso 1 En la página web de administración del teléfono, seleccione **Certificados**.

Paso 2 Busque el certificado en su PC.

Paso 3 En el campo **Extraer contraseña**, introduzca la contraseña de extracción del certificado.

Paso 4 Haga clic en **Subir**.

Paso 5 Reinicie el teléfono una vez que se complete la carga.

Instalar un certificado de servidor de autenticación desde la página web de administración del teléfono

Puede instalar manualmente un certificado de servidor de autenticación en el teléfono si el protocolo de inscripción de certificado simple (SCEP) no está disponible.

Debe instalarse el certificado de la entidad de certificación raíz que emitió el certificado de servidor RADIUS para EAP-TLS.

Antes de empezar

Para poder instalar un certificado en un teléfono, debe tener un certificado de servidor de autenticación guardado en su PC. El certificado debe estar codificado en PEM (base 64) o DER.

Procedimiento

Paso 1 En la página web de administración del teléfono, seleccione **Certificados**.

Paso 2 Localice el campo **Autoridad de certificación del servidor de autenticación (página web Admin.)** y haga clic en **Instalar**.

Paso 3 Busque el certificado en su PC.

Paso 4 Haga clic en **Subir**.

Paso 5 Reinicie el teléfono una vez que se complete la carga.

Si va a instalar más de un certificado, instale todos los certificados antes de reiniciar el teléfono.

Quitar manualmente un certificado de seguridad desde la página web de administración del teléfono

Puede quitar manualmente un certificado de seguridad desde un teléfono si el protocolo de inscripción de certificado simple (SCEP) no está disponible.

Procedimiento

Paso 1 En la página web de administración del teléfono, seleccione **Certificados**.

Paso 2 Busque el certificado en la página **Certificados**.

Paso 3 Haga clic en **Eliminar**.

Paso 4 Reinicie el teléfono cuando finalice el proceso de eliminación.

Establecer manualmente la fecha y hora del teléfono

Con la autenticación basada en certificado, el teléfono debe mostrar la fecha y hora correctas. Un servidor de autenticación comprueba la fecha y hora del teléfono en comparación con la fecha de caducidad del certificado. Si las fechas y horas del teléfono y el servidor no coinciden, el teléfono deja de funcionar.

Use este procedimiento para establecer manualmente la fecha y hora en el teléfono si el teléfono no recibe la información correcta de la red.

Procedimiento

Paso 1 En la página web de administración del teléfono, diríjase a **Fecha y hora**.

Paso 2 Lleve a cabo una de las acciones siguientes:

- Haga clic en **Establecer teléfono en fecha y hora** locales para sincronizar el teléfono con un servidor local.
- En los campos **Especificar fecha y hora**, seleccione el mes, el día, el año, la hora, los minutos y los segundos mediante los menús y haga clic en **Establecer teléfono para la fecha y hora específicas**.

Configuración SCEP

El protocolo de inscripción de certificado seguro (SCEP) es el estándar para aprovisionar y renovar certificados automáticamente. Evita la necesidad de instalar certificados manualmente en los teléfonos.

Configurar los parámetros de configuración específicos del producto SCEP

Debe configurar los siguientes parámetros SCEP en la página web del teléfono

- Dirección IP de RA
- Huella digital SHA-1 o SHA-256 del certificado de la entidad de certificación raíz del servidor SCEP

La autoridad de registro (RA) de Cisco IOS sirve como proxy para el servidor SCEP. El cliente SCEP en el teléfono usa los parámetros que se descargan de Cisco Unified Communication Manager. Después de configurar los parámetros, el teléfono envía una solicitud `SCEP getcs` para el certificado de la entidad de certificación raíz y RA que se valida mediante la huella digital definida.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Dispositivo** > **Teléfono**.

Paso 2 Localice el teléfono.

Paso 3 Diríjase al área **Diseño de la configuración específica del producto**.

Paso 4 Active la casilla de verificación **Servidor WLAN SCEP** para activar el parámetro SCEP.

Paso 5 Active la casilla de verificación **Huella digital de la entidad de certificación raíz de WLAN (SHA256 o SHA1)** para activar el parámetro SCEP QED.

Compatibilidad del servidor del protocolo de inscripción de certificado simple

Si utiliza un servidor del protocolo de inscripción de certificado simple (SCEP), el servidor puede mantener automáticamente los certificados de usuario y servidor. En el servidor SCEP, configure el agente de registro de SCEP (RA) en:

- Actuar como un punto de confianza PKI
- Actuar como un RA PKI
- Realizar la autenticación del dispositivo mediante un servidor RADIUS

Para obtener más información, consulte la documentación del servidor SCEP.

Autenticación 802.1x

Los teléfonos IP de Cisco admiten la autenticación 802.1X.

Los teléfonos IP de Cisco y los switches Cisco Catalyst usan tradicionalmente el protocolo de descubrimiento de Cisco (CDP) para identificarse entre sí y determinar parámetros tales como la asignación de VLAN y los requisitos energéticos internos.

Para la compatibilidad con la autenticación 802.1X se requieren varios componentes:

- Teléfono IP de Cisco: el teléfono inicia la solicitud para acceder a la red. Los teléfonos contienen un solicitante 802.1X. Este solicitante permite a los administradores de red controlar la conectividad de los teléfonos IP con los puertos switch de LAN. La versión actual del solicitante 802.1X del teléfono usa las opciones EAP-FAST y EAP-TLS para la autenticación de red.
- El switch Cisco Catalyst (o de otro fabricante): el switch debe ser compatible con 802.1X para poder actuar como autenticador y transferir los mensajes entre el teléfono y el servidor de autenticación. Cuando se completa el intercambio, el switch otorga o deniega el acceso del teléfono a la red.

Debe llevar a cabo las acciones siguientes para configurar 802.1X.

- Configurar los demás componentes antes de habilitar la autenticación 802.1X en el teléfono.
- Configurar VLAN de voz: dado que el estándar 802.1X no tiene en cuenta la VLAN, debe configurar este ajuste según la compatibilidad del switch.
  - Activado: si usa un switch que admita la autenticación multidominio, puede continuar usando la VLAN de voz.
  - Desactivado: si el switch no admite la autenticación multidominio, desactive la VLAN de voz y plantéese asignar el puerto a la VLAN nativa.

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

CAPÍTULO 8

Personalización del teléfono IP para conferencias de Cisco

Tonos de llamada de teléfono personalizados

El teléfono IP de Cisco incluye dos tipos de llamada predeterminados implementados en el hardware: Chirp 1 y Chirp 2. Cisco Unified Communications Manager también proporciona un juego predeterminado de tonos de llamada de teléfono adicionales que se implementan en el software como archivos de modulación de código de pulso (PCM). Los archivos PCM, junto con un archivo XML que describe las opciones de la lista de timbres disponibles en el sitio, se encuentran en el directorio TFTP de todos los servidores de Cisco Unified Communications Manager.

Atención Todos los nombres de archivo distinguen mayúsculas de minúsculas. Si no usa las mayúsculas o minúsculas correctas para el nombre del archivo, el teléfono no aplicará los cambios que realice.

Para obtener más información, consulte el capítulo sobre personalización de tonos de llamada y fondos en la Guía de configuración de características de Cisco Unified Communications Manager.

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

Configuración de un timbre del teléfono personalizado

Procedimiento

Paso 1 Cree un archivo PCM para cada timbre personalizado (un timbre por archivo).

Asegúrese de que los archivos PCM cumplen las directrices de formato descritas en la sección Formatos de archivos de timbres personalizados.

Paso 2 Cargue los nuevos archivos PCM que ha creado al servidor TFTP de Cisco para cada instancia de Cisco Unified Communications Manager del clúster.

Para obtener más datos, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Paso 3 Guarde las modificaciones que haya realizado y cierre el archivo Ringlist-wb.xml.

Paso 4 Para almacenar en caché el nuevo archivo Ringlist-wb:

- Detenga e inicie el servicio TFTP mediante Servicios Cisco Unified
- Desactive y vuelva a activar el parámetro de servicio TFTP «Habilitar almacenamiento en caché de archivos constantes y BIN al inicio» en la sección Parámetros de servicio avanzados.

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

Formatos de archivos de timbres personalizados

En el archivo Ringlist-wb.xml se define un objeto XML que contiene una lista de los tipos de timbre del teléfono. El archivo incluye hasta 50 tipos de timbre. Cada tipo contiene un puntero al archivo PCM que se usa para ese tipo de timbre y el texto que aparece en el menú Tipo de timbre correspondiente del teléfono IP de Cisco Este archivo se incluye en el servidor TFTP de Cisco de todos los Cisco Unified Communications Manager.

El objeto XML CiscoIPPhoneRinglist usa el conjunto siguiente de etiquetas simples para describir la información:

```
<CiscoIPPhoneRingList>
   <Ring>
      <DisplayName/>
      <FileName/>
   </Ring>
</CiscoIPPhoneRingList>
```

A los nombres de definición se le aplican las características siguientes. Debe incluir las etiquetas DisplayName y FileName necesarias para cada tipo de timbre de teléfono.

- DisplayName indica el nombre del timbre personalizado para el archivo PCM asociado que se muestra en el menú Tipo de timbre de teléfono IP de Cisco.
- FileName indica el nombre del archivo PCM para el timbre personalizado que se debe asociar con DisplayName.

Nota Los campos DisplayName y FileName no deben superar los 25 caracteres.

En este ejemplo se muestra un archivo Ringlist-wb.xml que define dos tipos de timbre de teléfono:

```
<CiscoIPPhoneRingList>
 <Ring>
      <DisplayName>Analog Synth 1</DisplayName>
      <FileName>Analog1.rwb</FileName>
   </Ring>
   <Ring>
```

```
      <DisplayName>Analog Synth 2</DisplayName>
      <FileName>Analog2.rwb</FileName>
   </Ring>
</CiscoIPPhoneRingList>
```

Los archivos PCM de los timbres deben cumplir los requisitos siguientes para reproducirse correctamente en los teléfonos IP de Cisco:

- PCM sin procesar (sin encabezado)
- 8000 muestras por segundo
- 8 bits por muestra
- Compresión ley Mu
- Tamaño máximo del timbre = 16 080 muestras
- Tamaño mínimo del timbre = 240 muestras
- Número de muestras en el timbre = múltiplos de 240
- El timbre se inicia y finaliza al paso por el punto cero

Para crear archivos PCM para timbres de teléfono personalizados, use cualquier paquete de edición de audio estándar que admita estos requisitos de formato.

Personalizar el tono de marcado

Puede configurar los teléfonos para que los usuarios oigan distintos tonos de marcación para las llamadas internas y externas. Dependiendo de sus necesidades, puede elegir entre tres opciones de tono de marcación:

- Valor predeterminado: un tono de marcación diferente para llamadas interiores y exteriores.
- Interior: se utiliza el tono de marcación interno para todas las llamadas.
- Exterior: se utiliza el tono de marcación externo para todas las llamadas.

Utilizar siempre el tono de marcación es un campo necesario en Cisco Unified Communications Manager.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Sistema** > **Parámetros de servicio**.

Paso 2 Seleccione el servidor adecuado.

Paso 3 Seleccione **Cisco CallManager** como servicio.

Paso 4 Desplácese hasta el panel Parámetros para todo el clúster.

Paso 5 Establezca **Utilizar siempre el tono de marcación** en una de las siguientes opciones:

- Fuera
- Dentro
- Valor predeterminado

Paso 6 Seleccione **Guardar**.

Paso 7 Reinicie los teléfonos.

CAPÍTULO 9

Configuración y características del teléfono IP para conferencias de Cisco

Asistencia para usuarios del teléfono IP de Cisco

Si es administrador del sistema, probablemente sea la fuente de información principal de los usuarios de los teléfonos IP de Cisco de su red o empresa. Es importante proporcionar información actualizada y completa a los usuarios finales.

Para usar correctamente algunas de las funciones del teléfono IP de Cisco (incluidos los servicios y las opciones del sistema de mensajes de voz), los usuarios deben recibir información de usted o del equipo de red o deben tener la capacidad de ponerse en contacto con usted para obtener asistencia. Asegúrese de proporcionar a los usuarios los nombres de las personas de contacto para recibir asistencia, así como instrucciones para hacerlo.

Se recomienda crear una página web del sitio de asistencia interno que ofrece a los usuarios finales información importante sobre sus teléfonos IP de Cisco.

Puede incluir los tipos siguientes de información en ese sitio:

- Guías de usuario de todos los modelos de teléfonos IP de Cisco que admita
- Información sobre cómo acceder al Portal de autoayuda de Cisco Unified Communications.
- Lista de las funciones admitidas.
- Guía de usuario o referencia rápida de su sistema de correo de voz.

Migración del teléfono a un teléfono multiplataforma directamente

Puede migrar su teléfono de empresa fácilmente en un solo paso sin utilizar la carga de firmware de transición. Lo único que necesita es obtener y autorizar la licencia de migración del servidor.

Para obtener más información, consulte https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/MPP/MPP-conversion/enterprise-to-mpp/cuip_b_conversion-guide-ipphone.html

Configuración de una nueva plantilla de teclas programables

Debe agregar las teclas programables a una plantilla de tecla programable para que a los usuarios tengan acceso a algunas funciones. Por ejemplo, si desea que los usuarios puedan utilizar la función no molestar, debe activar la tecla programable. Para obtener más datos, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Puede crear varias plantillas. Por ejemplo, es recomendable una plantilla para el teléfono en una sala de conferencias y otra plantilla para un teléfono en la oficina de un ejecutivo.

Este procedimiento le guía por los pasos para crear una nueva plantilla de tecla programable y asignarla a un teléfono concreto. Al igual que otras funciones del teléfono, también puede usar la plantilla en todos los teléfonos para conferencias o un grupo de teléfonos.

Procedimiento

Paso 1 Inicie sesión en Cisco Unified Communications Manager Administration como administrador.

Paso 2 Seleccione **Dispositivo** > **Configuración del dispositivo** > **Plantilla de teclas programadas**.

Paso 3 Haga clic en **Encontrar**.

Paso 4 Seleccione una de las opciones siguientes:

- Cisco Unified Communications Manager 11.5 y versiones anteriores: **usuario estándar**
- Cisco Unified Communications Manager 12.0 y versiones posteriores: **usuario de conferencia personal** o **usuario de conferencia público**.

Paso 5 Haga clic en **Copiar**.

Paso 6 Cambie el nombre de la plantilla.

Por ejemplo, Plantilla de la sala de conferencias 8832.

Paso 7 Haga clic en **Guardar**.

Paso 8 Vaya a la página **Configurar diseño de teclas programables** desde el menú de la parte superior derecha.

Paso 9 Para cada estado de llamada, defina las funciones que se mostrarán.

Paso 10 Haga clic en **Guardar**.

Paso 11 Vuelva a la **pantalla Buscar/Lista** desde el menú de la parte superior derecha.

Verá la nueva plantilla en la lista de plantillas.

Paso 12 Seleccione **Dispositivo** > **Teléfono**.

Paso 13 Busque el teléfono que tendrá la nueva plantilla y selecciónelo.

Paso 14 En el campo **Plantilla de tecla programable**, seleccione la nueva plantilla de tecla programable.

Paso 15 Haga clic en **Guardar** y **Aplicar configuración**.

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

Configuración de los servicios de telefonía para los usuarios

Puede proporcionar a los usuarios acceso a los servicios de Teléfono IP de Cisco Unified en el teléfono IP. También es posible asignar un botón a distintos servicios del teléfono. El teléfono IP administra cada servicio como una aplicación independiente.

Para que un usuario pueda acceder a cualquier servicio:

- Use Cisco Unified Communications Manager Administration para configurar los servicios que no estén presentes de forma predeterminada.
- El usuario debe usar Portal de autoayuda de Cisco Unified Communications para suscribirse a los servicios. Esta aplicación web proporciona una interfaz gráfica del usuario (GUI) para que los usuarios finales puedan configurar de forma limitada las aplicaciones del teléfono IP. Sin embargo, un usuario no puede suscribirse a ningún servicio que haya configurado como suscripción empresarial.

Para obtener más datos, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Antes de configurar los servicios, recopile las direcciones URL de los sitios que desea configurar y compruebe que los usuarios pueden acceder a esos sitios desde su red de telefonía IP empresarial. Esta actividad no se aplica a los servicios predeterminados proporcionados por Cisco.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Dispositivo** > **Configuración del dispositivo** > **Servicios de telefonía**.

Paso 2 Verifique que los usuarios pueden acceder a Portal de autoayuda de Cisco Unified Communications, desde donde pueden seleccionar los servicios configurados y suscribirse a ellos.

Consulte Descripción general del portal de autoayuda, en la página 69 para obtener un resumen de la información que debe proporcionar a los usuarios finales.

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

Configuración de funciones del teléfono

Puede configurar teléfonos para disponer de una gran variedad de funciones según las necesidades de los usuarios. Puede aplicar funciones a todos los teléfonos, a un grupo de teléfonos o a teléfonos individuales.

Al configurar las funciones, la ventana de Cisco Unified Communications Manager Administration muestra la información que es aplicable a todos los teléfonos y la información que es aplicable al modelo de teléfono. La información que es específica para el modelo de teléfono está en el área Diseño de la configuración específica del producto de la ventana.

Para obtener información sobre los campos aplicables a todos los modelos de teléfono, consulte la documentación de Cisco Unified Communications Manager.

Cuando se configure un campo, la ventana en la que establezca el campo es importante porque no existe una prioridad para las ventanas. El orden de prioridad es:

1. Teléfonos individuales (mayor prioridad)
2. Grupo de teléfonos
3. Todos los teléfonos (menor prioridad)

Por ejemplo, si no desea que un conjunto específico de usuarios acceda a las páginas web del teléfono, pero el resto de los usuarios pueda acceder a las páginas, puede:

1. Activar el acceso a las páginas web del teléfono para todos los usuarios.
2. Desactivar el acceso a las páginas web del teléfono para cada usuario individual, o configurar un grupo de usuarios y desactivar el acceso a las páginas web del teléfono para el grupo de usuarios.
3. Si un usuario específico en el grupo de usuarios precisaba acceso a las páginas web del teléfono, podía activarlo para ese usuario concreto.

Temas relacionados

Configuración de credenciales de usuario persistentes para el inicio de sesión de Expressway, en la página 123

Configuración de las funciones del teléfono para todos los teléfonos

Procedimiento

Paso 1 Inicie sesión en Cisco Unified Communications Manager Administration como administrador.

Paso 2 Seleccione **Sistema** > **Configuración de teléfono empresarial**.

Paso 3 Establezca los campos que desee cambiar.

Paso 4 Marque la casilla de verificación **Cancelar configuración empresarial** para los campos modificados.

Paso 5 Haga clic en **Guardar**.

Paso 6 Haga clic en **Aplicar configuración**.

Paso 7 Reinicie los teléfonos.

Nota Esto afectará a todos los teléfonos de la organización.

Temas relacionados

Configuración específica del producto, en la página 100

Configuración de las funciones del teléfono para un grupo de teléfonos

Procedimiento

Paso 1 Inicie sesión en Cisco Unified Communications Manager Administration como administrador.
Paso 2 Seleccione **Dispositivo** > **Configuración del dispositivo** > **Perfil de teléfono común**.
Paso 3 Busque el perfil.
Paso 4 Diríjase al panel de diseño de la configuración específica del producto y defina los campos.
Paso 5 Marque la casilla de verificación **Cancelar configuración empresarial** para los campos modificados.
Paso 6 Haga clic en **Guardar**.
Paso 7 Haga clic en **Aplicar configuración**.
Paso 8 Reinicie los teléfonos.

Temas relacionados

Configuración específica del producto, en la página 100

Configuración de las funciones del teléfono para un solo teléfono

Procedimiento

Paso 1 Inicie sesión en Cisco Unified Communications Manager Administration como administrador.
Paso 2 Seleccione **Dispositivo** > **Teléfono**.
Paso 3 Localice el teléfono asociado al usuario.
Paso 4 Diríjase al panel de diseño de la configuración específica del producto y defina los campos.
Paso 5 Active la casilla de verificación **Cancelar configuración común** para los campos modificados.
Paso 6 Haga clic en **Guardar**.
Paso 7 Haga clic en **Aplicar configuración**.
Paso 8 Reinicie el teléfono.

Temas relacionados

Configuración específica del producto, en la página 100

Configuración específica del producto

La tabla siguiente describe los campos en el panel de diseño de la configuración específica de producto. Algunos campos de esta tabla solo se muestran en la página **Dispositivo** > **Teléfono**.

Tabla 18: Campos de la configuración específica del producto

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción
Acceso a la configuración	Deshabilitado Habilitado Restringido	Habilitado	Activa, desactiva o restringe el acceso a los ajustes de configuración local en la aplicación Configuración. Con acceso restringido, se puede acceder a los menús Preferencias e Información del sistema. También están accesibles algunos ajustes en el menú Wi-Fi. Con el acceso desactivado, el menú Configuración no muestra las opciones.
ARP gratuito	Deshabilitado Habilitado	Deshabilitado	Activa o desactiva la posibilidad de que el teléfono aprenda las direcciones MAC de ARP gratuito. Esta capacidad es necesaria para supervisar o registrar flujos de voz.
Acceso vía Web	Deshabilitado Habilitado	Deshabilitado	Activa o desactiva el acceso a las páginas web del teléfono a través de un explorador web. **Precaución** Si activa este campo, puede revelar información confidencial sobre el teléfono.
Desactivar TLS 1.0 y TLS 1.1 para acceso web	Deshabilitado Habilitado	Habilitado	Controla el uso de TLS 1.2 para una conexión del servidor web. • Desactivado: un teléfono configurado para TLS1.0, TLS 1.1 o TLS1.2 puede funcionar como un servidor HTTPs. • Activado: solo un teléfono configurado para TLS1.2 puede funcionar como un servidor HTTPs.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción
Marcación en bloque	Deshabilitado Habilitado	Deshabilitado	Controla el método de marcación. • Desactivado: Cisco Unified Communications Manager espera a que el temporizador entre dígitos caduque cuando hay superposición de plan de marcación o patrón de ruta. • Activado: toda la cadena marcada se envía a Cisco Unified Communications Manager una vez completada la marcación del número. Para evitar el tiempo de espera del temporizador T.302, le recomendamos que active la marcación en bloque siempre que haya superposición de plan de marcación o patrón de ruta. Los códigos de autorización forzada (FAC) o los códigos de asunto de cliente (CMC) no son compatibles con la marcación en bloque. Si utiliza FAC o CMC para administrar el acceso a las llamadas y la contabilidad, no podrá utilizar esta función.
Luz de fondo no activa	Días de la semana		Define los días en que la luz de fondo no se enciende automáticamente a la hora especificada en el campo Activar luz de fondo. Seleccione los días oportunos en la lista desplegable. Para seleccionar más de un día, **haga clic mientras pulsa la tecla Ctrl** en cada día que desee agregar. Consulte Programación de la función de ahorro de energía para el teléfono IP de Cisco, en la página 113.
Hora de activación de luz de fondo	hh:mm		Define la hora de cada día a la que se enciende automáticamente la luz de fondo (excepto los días especificados en el campo Luz de fondo no activa). En este campo, debe introducir la hora en formato de 24 horas, donde 00:00 es la medianoche. Por ejemplo, para encender automáticamente la luz de fondo a las 7 de la mañana (0700), introduzca 07:00. Para encender automáticamente la luz de fondo a las 2 de la tarde (1400), introduzca 14:00. Si el campo está vacío, la luz de fondo se enciende automáticamente a las 0:00. Consulte Programación de la función de ahorro de energía para el teléfono IP de Cisco, en la página 113.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción
Duración de activación de luz de fondo	hh:mm		Define el período que la luz de fondo permanecerá activada tras encenderse a la hora especificada en el campo Activar luz de fondo. Por ejemplo, para que la luz de fondo siga encendida 4 horas y 30 minutos después de encenderse automáticamente, introduzca 04:30. Si el campo está vacío, el teléfono se apaga al final del día (0:00). Si la hora de activación de la luz de fondo es a las 0:00 y la duración de la luz de fondo está en blanco (o aparece como 24:00), la luz de fondo no se apagará. Consulte Programación de la función de ahorro de energía para el teléfono IP de Cisco, en la página 113.
Tiempo de espera de luz de fondo inactiva	hh:mm		Define el período que el teléfono debe estar inactivo antes de que se apague la luz de fondo. Solo se aplica si la luz de fondo estaba apagada según la programación y un usuario la enciende (pulsando un botón en el teléfono o levantando el auricular). Por ejemplo, para apagar la luz de fondo cuando el teléfono permanezca inactivo durante 1 hora y 30 minutos después de que un usuario haya encendido la luz de fondo, introduzca 01:30. Consulte Programación de la función de ahorro de energía para el teléfono IP de Cisco, en la página 113.
Luz de fondo activada si entra una llamada	Deshabilitado Habilitado	Habilitado	Enciende la luz de fondo cuando se produce una llamada entrante.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción
Activar Power Save Plus	Días de la semana		Define la programación de los días en los que el teléfono se apaga. Seleccione los días oportunos en la lista desplegable. Para seleccionar más de un día, **haga clic mientras pulsa la tecla Ctrl** en cada día que desee agregar. Si la casilla Activar Power Save Plus está activada, recibirá un mensaje de advertencia sobre los servicios de emergencia (e911). **Precaución** Con el modo Power Save Plus (el "Modo") activado, los terminales configurados con este modo tienen desactivadas las llamadas de emergencia y las llamadas entrantes. Al seleccionar este modo, acepta lo siguiente: (1) asume toda la responsabilidad de proporcionar métodos alternativos para las llamadas de emergencia y para la recepción de llamadas mientras el modo está en vigor; (2) Cisco no asume responsabilidad alguna relacionada con que seleccione este modo y toda la responsabilidad derivada de la activación del modo será suya; y (3) se compromete a informar a los usuarios sobre los efectos de este modo en las llamadas, ya sea mediante una llamada o con cualquier otro sistema. Para desactivar Power Save Plus, debe quitar la marca de la casilla de verificación Permitir anulación de EnergyWise. Si esta casilla sigue marcada pero no se selecciona ningún día en el campo Activar Power Save Plus, Power Save Plus no se desactiva. Consulte Programación de EnergyWise en el teléfono IP de Cisco, en la página 114.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción
Hora de encendido del teléfono	hh:mm		Determina la hora a la que el teléfono se enciende automáticamente los días indicados en el campo Activar Power Save Plus. En este campo, debe introducir la hora en formato de 24 horas, donde 00:00 es la medianoche. Por ejemplo, para encender automáticamente el teléfono a las 7 de la mañana (0700), introduzca 07:00. Para encender automáticamente el teléfono a las 2 de la tarde (1400), introduzca 14:00. El valor predeterminado es dejar el campo vacío, que indica las 00:00. La hora de encendido del teléfono debe ser al menos de 20 minutos después de la de apagado. Por ejemplo, si la hora de apagado del teléfono es a las 07:00, la de encendido no puede ser antes de las 07:20. Consulte Programación de EnergyWise en el teléfono IP de Cisco, en la página 114.
Hora de apagado del teléfono	hh:mm		Define la hora del día a la que el teléfono se apaga los días seleccionados en el campo Activar Power Save Plus. Si los campos Hora de encendido del teléfono y Hora de apagado del teléfono contienen el mismo valor, el teléfono no se apaga. En este campo, debe introducir la hora en formato de 24 horas, donde 00:00 es la medianoche. Por ejemplo, para apagar automáticamente el teléfono a las 7 de la mañana (0700), introduzca 7:00. Para apagar automáticamente el teléfono a las 2 de la tarde (1400), introduzca 14:00. El valor predeterminado es dejar el campo vacío, que indica las 00:00. La hora de encendido del teléfono debe ser al menos de 20 minutos después de la de apagado. Por ejemplo, si la hora de apagado del teléfono es a las 07:00, la de encendido no puede ser antes de las 07:20. Consulte Programación de EnergyWise en el teléfono IP de Cisco, en la página 114.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción
Tiempo de espera de inactividad para apagar el teléfono	hh:mm		Indica el período que el teléfono debe estar inactivo antes de que se apague. El tiempo de espera se agota si se dan las siguientes condiciones: • Si el teléfono se encuentra en el modo Power Save Plus, según la programación, y sale de dicho modo porque el usuario de teléfono pulsa la tecla Seleccionar. • Si el teléfono vuelve a recibir energía por el switch conectado. • Si se alcanza la hora de apagado del teléfono pero el teléfono está en uso. Consulte Programación de EnergyWise en el teléfono IP de Cisco, en la página 114.
Activar alerta sonora	Casilla de verificación	Desactivado	Si está activada, indica al teléfono que reproduzca una alerta sonora desde 10 minutos antes de la hora especificada en el campo Hora de apagado del teléfono. Esta casilla de verificación solo se aplica si en la lista de Activar Power Save Plus se han seleccionado uno o varios días. Consulte Programación de EnergyWise en el teléfono IP de Cisco, en la página 114.
Dominio de EnergyWise	Hasta 127 caracteres		Identifica el dominio de EnergyWise en el que se encuentra el teléfono. Consulte Programación de EnergyWise en el teléfono IP de Cisco, en la página 114.
Secreto de EnergyWise	Hasta 127 caracteres		Identifica la contraseña secreta de seguridad que se usa para comunicarse con los terminales del dominio de EnergyWise. Consulte Programación de EnergyWise en el teléfono IP de Cisco, en la página 114.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción
Permitir anulaciones de EnergyWise	Casilla de verificación	Desactivado	Determina si se permite a la directiva del controlador del dominio de EnergyWise enviar actualizaciones del nivel de energía a los teléfonos. Se aplican las condiciones siguientes: • Se deben seleccionar uno o varios días en el campo Activar Power Save Plus. • Los ajustes de Cisco Unified Communications Manager Administration surten efecto según la programación, incluso aunque EnergyWise envíe una anulación. Por ejemplo, supongamos que en Hora de apagado del teléfono se indique 22:00 (las 10 de la noche), que el valor del campo Hora de encendido del teléfono sea 06:00 (las 6 de la mañana) y que Activar Power Save Plus tenga uno o varios días seleccionados. • Si EnergyWise indica al teléfono que se apague a las 20:00 (las 8 de la tarde), esa directiva sigue en vigor (siempre que no se produzca ninguna intervención del usuario en el teléfono) hasta la hora configurada en Hora de encendido del teléfono a las 6:00. • A las 6:00, el teléfono se enciende y vuelve a recibir los cambios de nivel de energía según la configuración de la Cisco Unified Communications Manager Administration Administration. • Para volver a cambiar el nivel de energía del teléfono, EnergyWise debe emitir de nuevo un comando de cambio de nivel de energía. Para desactivar Power Save Plus, debe quitar la marca de la casilla de verificación Permitir anulación de EnergyWise. Si esta casilla sigue marcada pero no se selecciona ningún día en el campo Activar Power Save Plus, Power Save Plus no se desactiva. Consulte Programación de EnergyWise en el teléfono IP de Cisco, en la página 114.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción
Política de participación y transferencia directa	Activar en misma línea Desactivar en la misma línea	Misma línea, activar entre líneas	Controla la capacidad de un usuario de participación y transferencia de llamadas. • Activar en la misma línea: los usuarios pueden directamente transferir una llamada en la línea actual a otra llamada en la misma línea o participar en ella. • Desactivar en la misma línea: los usuarios no podrán participar en llamadas o transferirlas en la misma línea. Se desactivan las funciones de participación y transferencia, y el usuario no puede realizar la función de participación o transferencia directa.
Grabando tono	Deshabilitado Habilitado	Deshabilitado	Controla la reproducción del tono cuando un usuario está grabando una llamada.
Grabando vol. loc. de tono	Entero de 0 a 100	100	Controla el volumen del tono de grabación para el usuario local.
Volumen del tono de grabación remoto	Entero de 0 a 100	50	Controla el volumen del tono de grabación para el usuario remoto.
Grabando duración del tono	Entero, 1-3000 milisegundos		Controla la duración del tono de grabación.
Servidor de registro	Cadena de un máximo de 256 caracteres		Identifica el servidor syslog IPv4 para los resultados de depuración del teléfono. El formato de la dirección es: **dirección:<port>@@base=<0-7>;pfs=<0-1>**
Registro remoto	Deshabilitado Habilitado	Deshabilitado	Controla la capacidad de enviar registros al servidor syslog.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción
Perfil de registro	Valor predeterminado Preajuste Telefonía SIP IU Red Medios Actualizar Accesorio Seguridad EnergyWise MobileRemoteAccess	Preajuste	Especifica el perfil de registro predefinido. • Valor predeterminado: nivel de registro de depuración predeterminado. • Preajuste: no sobrescribe la configuración del registro de depuración local del teléfono. • Telefonía: registra información sobre las funciones de telefonía o llamada. • SIP: registra información sobre la señalización SIP. • Interfaz de usuario: registra información sobre la interfaz de usuario del teléfono. • Red: registra la información de red. • Medios: registra la información de medios. • Actualizar: registra la información de actualización. • Accesorio: registra la información de accesorios. • Seguridad: registra la información de seguridad. • Energywise: registra información de ahorro de energía • MobileRemoteAccess: registra el acceso móvil y remoto a través de la información de Expressway
Servidor de registro de IPv6	Cadena de un máximo de 256 caracteres		Identifica el servidor syslog IPv6 para los resultados de depuración del teléfono.
Cisco Discovery Protocol (CDP): puerto conmutador	Deshabilitado Habilitado	Habilitado	Controla Cisco Discovery Protocol en el teléfono.
Protocolo de descubrimiento de capa de enlace - Descubrimiento de terminal de medios (LLDP-MED): puerto conmutador	Deshabilitado Habilitado	Habilitado	Permite LLDP-MED en el puerto SW.
LLDP ID del dispositivo	Cadena, hasta un máximo de 32 caracteres		Identifica el ID del dispositivo asignado al teléfono para la administración del inventario.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción
Ethernet de eficacia energética (EEE): puerto de conmutador	Deshabilitado Habilitado	Deshabilitado	controla EEE en el puerto conmutador.
LLDP Prioridad energética	Desconocido Bajo. Alto. Crítico.	Desconocido	Asigna una prioridad energética del teléfono al conmutador, habilitando de esta forma el switch para que proporcione la energía oportuna a los teléfonos.
Autenticación 802.1x	Controlado por el usuario Deshabilitado Habilitado	Controlado por el usuario	Especifica el estado de la función de la autenticación 802.1X. • Usuario controlado: el usuario puede configurar 802.1X en el teléfono. • Desactivado: la autenticación 802.1x no se usa. • Habilitado: se usa la autenticación 802.1X y configura la autenticación para los teléfonos.
Cambiar configuración remota de puerto	Deshabilitado Negociación automática 10 medio 10 completo 100 medio 100 completo	Deshabilitado	Le permite configurar la velocidad y la función dúplex del puerto SW del teléfono de forma remota. Esto mejora el rendimiento en caso de grandes implementaciones con configuraciones específicas de puertos. Si los puertos SW se configuran para la configuración de puerto remota en Cisco Unified Communications Manager, los datos no se pueden cambiar en el teléfono.
Acceso SSH	Deshabilitado Habilitado	Deshabilitado	Controla el acceso al daemon SSH a través del puerto 22. El teléfono será vulnerable a los ataques de denegación de servicio (DoS) si se deja el puerto 22 abierto.
Configuración regional del timbre	Valor predeterminado Japón	Valor predeterminado	Controla el patrón de timbre.
Temporizador de reanudación de TLS	Entero de 0 a 3600 segundos	3600	Controla la capacidad de reanudar una sesión TLS sin tener que repetir todo el proceso de autenticación de TLS. Si en el campo se establece el valor 0, la reanudación de la sesión TLS está desactivada.
Modo FIPS	Deshabilitado Habilitado	Deshabilitado	Activa o desactiva el modo de estándares federales de procesamiento de la información (FIPS) de Estados Unidos en el teléfono.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción
Grabar registro de llamadas desde línea compartida	Deshabilitado Habilitado	Deshabilitado	Especifica si se va a grabar el registro de llamadas de una línea compartida.
Volumen del timbre mínimo	0: silencioso 1–15	0: silencioso	Controla el volumen del timbre mínimo para el teléfono.
Uso compartido del firmware en el grupo	Deshabilitado Habilitado	Habilitado	Permite al teléfono buscar otros teléfonos del mismo modelo en la subred y compartir archivos del firmware actualizados. Si el teléfono tiene una nueva carga de firmware, puede compartir la carga con los demás teléfonos. Si uno de los demás teléfonos tiene una nueva de firmware, el teléfono puede descargar el firmware desde el otro teléfono en lugar de hacerlo desde el servidor TFTP. Uso compartido del firmware en el grupo: • Limita la congestión de las transferencias TFTP a los servidores TFTP remotos centralizados. • Elimina la necesidad de controlar manualmente las actualización del firmware. • Reduce el tiempo de inactividad del teléfono durante las actualizaciones cuando se restauran simultáneamente grandes cantidades de teléfonos. • Ayuda con las actualizaciones del firmware en escenarios de implementación de oficinas remotas o sucursales que se produzcan en enlaces WAN con ancho de banda limitado.
Servidor de carga	Cadena de un máximo de 256 caracteres		Identifica el servidor IPv4 alternativo que usa el teléfono para obtener actualizaciones y cargas de firmware.
Servidor de carga de IPv6	Cadena de un máximo de 256 caracteres		Identifica el servidor IPv6 alternativo que usa el teléfono para obtener actualizaciones y cargas de firmware.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción
Detectar error de conexión de Unified CM	Normal Retrasada	Normal	Determina la sensibilidad que tiene el teléfono para detectar un error de conexión en Cisco Unified Communications Manager (Unified CM), que es el primer paso antes de que se produzca una conmutación por error del dispositivo en Unified CM/SRST de copia de seguridad. Los valores válidos son Normal (la detección de un error de conexión de Unified CM se produce a la velocidad estándar del sistema) o Retrasada (la detección de una conmutación por error de Unified CM se produce a una velocidad cuatro veces más lenta que la normal). Para un reconocimiento más rápido de un error de conexión de Unified CM, elija Normal. Si prefiere que la conmutación por error se retrase ligeramente para proporcionar a la conexión la posibilidad de restablecerse, elija Retrasada. La diferencia horaria precisa entre la detección de errores de la conexión Normal y Retrasada depende de muchas variables que cambian constantemente.
ID de requisito especial	Cadena		Controla las funciones personalizadas para cargas de ingeniería especiales (ES).
Servidor HTTPS	HTTP y HTTPS activados Solo https	HTTP y HTTPS activados	Controla el tipo de comunicación con el teléfono. Si selecciona solo HTTPS, la comunicación del teléfono es más segura.
Credenciales de usuario persistentes para el inicio de sesión de Expressway	Deshabilitado Habilitado	Deshabilitado	Controla si el teléfono almacena las credenciales de inicio de sesión de los usuarios. Cuando está desactivado, el usuario siempre verá el mensaje para iniciar sesión en el servidor de Expressway para Mobile and Remote Access (MRA). Si desea que el inicio de sesión de los usuarios sea más fácil, active este campo para que las credenciales de inicio de sesión de Expressway sean permanentes. El usuario solo tiene que introducir sus credenciales de inicio de sesión la primera vez. Después de eso (cuando el teléfono está encendido fuera de las instalaciones), la información de inicio de sesión se completa previamente en la pantalla de inicio de sesión. Para obtener más información, consulte el apartado Configuración de credenciales de usuario persistentes para el inicio de sesión de Expressway, en la página 123.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción
URL de carga de asistencia al cliente	Cadena, hasta un máximo de 256 caracteres		Proporciona la URL de la herramienta de informe de problemas (PRT). Si implementa dispositivos con Mobile and Remote Access mediante Expressway, también debe agregar la dirección del servidor PRT a la lista de servidores HTTP permitidos en el servidor de Expressway. Para obtener más información, consulte el apartado Configuración de credenciales de usuario persistentes para el inicio de sesión de Expressway, en la página 123.
Desactivación de los cifrados TLS	Consulte Desactivar los cifrados de seguridad de la capa de transporte, en la página 112.	Ninguno	Desactiva el cifrado TLS seleccionado. Desactive varios conjuntos de cifrado seleccionando y manteniendo pulsada la tecla **Ctrl** del teclado del ordenador.
Dedicar una línea para el aparcamiento de llamadas	Deshabilitado Habilitado	Habilitado	Controla si una llamada aparcada ocupa una línea o no. Para obtener más datos, consulte la documentación de Cisco Unified Communications Manager.

Temas relacionados

Configuración de credenciales de usuario persistentes para el inicio de sesión de Expressway, en la página 123

Desactivar los cifrados de seguridad de la capa de transporte

Puede desactivar los cifrados de seguridad de la capa de transporte (TLS) con el parámetro **Desactivar los cifrados de TTLS**. De este modo puede adaptar su seguridad a las vulnerabilidades conocidas y coordinar la red con las políticas de cifrado de su empresa.

El ajuste predeterminado es Ninguno.

Desactive varios conjuntos de cifrado seleccionando y manteniendo pulsada la tecla **Ctrl** del teclado del ordenador. Si selecciona todos los cifrados de teléfono, se verá afectado el servicio TLS del teléfono. Entre las opciones se incluyen:

- Ninguno
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Para obtener más información sobre la seguridad del teléfono, consulte el *informe técnico de descripción general de la seguridad del teléfono IP serie 7800 y 8800 de Cisco*(https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html).

Programación de la función de ahorro de energía para el teléfono IP de Cisco

A fin de ahorrar energía y garantizar la duración de la pantalla del teléfono, puede establecer que la pantalla se apague cuando no se necesite.

En Cisco Unified Communications Manager Administration es posible configurar que la pantalla se apague a una hora concreta de algunos días, además de otros días completos. Por ejemplo, puede seleccionar que la pantalla se apague al finalizar la jornada laboral durante la semana y todo el día los sábados y domingos.

Puede llevar a cabo cualquiera de estas acciones para encender la pantalla siempre que esté apagada:

- Pulse cualquier botón del teléfono.

  El teléfono realiza la acción designada por ese botón además de encender la pantalla.

- Levante el auricular.

Cuando se enciende la pantalla, sigue encendida hasta que el teléfono permanece inactivo durante un período indicado de tiempo y, entonces, se apaga automáticamente.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Dispositivo** > **Teléfono**.

Paso 2 Busque el teléfono que desea configurar.

Paso 3 Diríjase al área de configuración específica del producto y defina los campos siguientes:

- Días pantalla no activa
- Hora de activación de pantalla
- Duración actividad de pantalla
- Tiempo espera pantalla inactiva

Tabla 19: Campos de Configuración de PowerSave

Campo	Descripción
Días pantalla no activa	Los días que la pantalla no se enciende automáticamente a la hora especificada en el campo Hora de activación de pantalla. Seleccione los días oportunos en la lista desplegable. Para seleccionar más de un día, haga clic mientras pulsa la tecla Ctrl en cada día que desee agregar.

Campo	Descripción
Hora de activación de pantalla	La hora de cada día a la que se enciende automáticamente la pantalla (excepto los días especificados en el campo Días pantalla no activa). En este campo, debe introducir la hora en formato de 24 horas, donde 0:00 es la medianoche. Por ejemplo, para encender automáticamente la pantalla a las 7 de la mañana (0700), introduzca **07:00**. Para encender la pantalla a las 2 de la tarde (1400), introduzca **14:00**. Si el campo está vacío, la pantalla se enciende automáticamente a las 0:00.
Duración actividad de pantalla	El período que la pantalla permanecerá activada tras encenderse a la hora especificada en el campo Hora de activación de pantalla. Introduzca el valor en este campo con el formato *horas:minutos*. Por ejemplo, para que la pantalla siga encendida 4 horas y 30 minutos después de encenderse automáticamente, introduzca **04:30**. Si el campo está vacío, el teléfono se apaga al final del día (0:00). **Nota** Si el valor de Hora de activación de pantalla es 0:00 y el campo de duración de encendido de la pantalla está vacío (o es 24:00), la pantalla permanecerá encendida siempre.
Tiempo espera pantalla inactiva	El período que el teléfono debe estar inactivo antes de que se apague la pantalla. Solo se aplica si la pantalla estaba apagada según la programación y un usuario la enciende (pulsando un botón en el teléfono o levantando el auricular). Introduzca el valor en este campo con el formato *horas:minutos*. Por ejemplo, para apagar la pantalla cuando el teléfono permanezca inactivo durante 1 hora y 30 minutos después de que un usuario haya encendido la pantalla, introduzca **01:30**. El valor predeterminado es 01:00.

Paso 4 Seleccione **Guardar**.

Paso 5 Seleccione **Aplicar configuración**.

Paso 6 Reinicie el teléfono.

Programación de EnergyWise en el teléfono IP de Cisco

Para reducir el consumo de electricidad, configure el teléfono para que se suspenda (se apague) y se active (se encienda) si el sistema incluye un controlador de EnergyWise.

Los ajustes para activar EnergyWise y configurar las horas de suspensión y activación se realizan en Cisco Unified Communications Manager Administration. Estos parámetros están estrechamente relacionados con la configuración de la pantalla del teléfono.

Si EnergyWise está activado y se establece una hora de suspensión, el teléfono envía una solicitud al switch para que se active a la hora configurada. El switch acepta o rechaza la solicitud. Si el switch rechaza la solicitud o no responde, el teléfono no se apaga. Si el switch acepta la solicitud, el teléfono inactivo pasa a modo suspendido, reduciendo así el consumo de electricidad a un nivel predeterminado. Un teléfono que no esté

inactivo establece un temporizador de inactividad y pasa al modo de suspensión cuando el temporizador caduca.

Para activar el teléfono, pulse Seleccionar. A la hora de activación programada, el sistema restablece la energía del teléfono y lo activa.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Dispositivo** > **Teléfono**.

Paso 2 Busque el teléfono que desea configurar.

Paso 3 Diríjase al área de configuración específica del producto y defina los campos siguientes.

- Activar Power Save Plus
- Hora de encendido del teléfono
- Hora de apagado del teléfono
- Tiempo de espera de inactividad para apagar el teléfono
- Activar alerta sonora
- Dominio de EnergyWise
- Secreto de EnergyWise
- Permitir anulaciones de EnergyWise

Tabla 20: Campos de Configuración de EnergyWise

Campo	Descripción
Activar Power Save Plus	Permite programar los días en los que el teléfono se apaga. Para seleccionar varios días, pulse y mantenga pulsada la tecla Control mientras hace clic en los días de la programación. De forma predeterminada, no hay ningún día seleccionado. Si la casilla Activar Power Save Plus está marcada, recibirá un mensaje de advertencia sobre los servicios de emergencia (e911). **Precaución** Con el «modo» Power Save Plus en vigor, los terminales configurados con este modo tienen desactivadas las llamadas de emergencia y las llamadas entrantes. Al seleccionar este modo, acepta lo siguiente: (1) asume toda la responsabilidad de proporcionar métodos alternativos para las llamadas de emergencia y para la recepción de llamadas mientras el modo está en vigor; (2) Cisco no asume responsabilidad alguna relacionada con que seleccione este modo y toda la responsabilidad derivada de la activación del modo será suya; y (3) se compromete a informar a los usuarios sobre los efectos de este modo en las llamadas, ya sea mediante una llamada o con cualquier otro sistema. **Nota** Para desactivar Power Save Plus, debe quitar la marca de la casilla de verificación Permitir anulación de EnergyWise. Si esta casilla sigue marcada pero no se selecciona ningún día en el campo Activar Power Save Plus, Power Save Plus no se desactiva.

Campo	Descripción
Hora de encendido del teléfono	Determina la hora a la que el teléfono se enciende automáticamente los días indicados en el campo Activar Power Save Plus. En este campo, debe introducir la hora en formato de 24 horas, donde 00:00 es la medianoche. Por ejemplo, para encender automáticamente el teléfono a las 7 de la mañana (0700), introduzca 07:00. Para encender automáticamente el teléfono a las 2 de la tarde (1400), introduzca 14:00. El valor predeterminado es dejar el campo vacío, que indica las 00:00. **Nota** La hora de encendido del teléfono debe ser al menos de 20 minutos después de la de apagado. Por ejemplo, si la hora de apagado del teléfono es a las 07:00, la de encendido no puede ser antes de las 07:20.
Hora de apagado del teléfono	La hora del día a la que el teléfono se apaga los días seleccionados en el campo Activar Power Save Plus. Si los campos Hora de encendido del teléfono y Hora de apagado del teléfono contienen el mismo valor, el teléfono no se apaga. En este campo, debe introducir la hora en formato de 24 horas, donde 00:00 es la medianoche. Por ejemplo, para apagar automáticamente el teléfono a las 7 de la mañana (0700), introduzca 7:00. Para apagar automáticamente el teléfono a las 2 de la tarde (1400), introduzca 14:00. El valor predeterminado es dejar el campo vacío, que indica las 00:00. **Nota** La hora de encendido del teléfono debe ser al menos de 20 minutos después de la de apagado. Por ejemplo, si la hora de apagado del teléfono es a las 07:00, la de encendido no puede ser antes de las 07:20.
Tiempo de espera de inactividad para apagar el teléfono	El período que el teléfono debe estar inactivo antes de que se apague. El tiempo de espera se agota si se dan las siguientes condiciones: • Si el teléfono se encuentra en el modo Power Save Plus, según la programación, y sale de dicho modo porque el usuario pulsa la tecla **Seleccionar**. • Si el teléfono vuelve a recibir energía por el switch conectado. • Si se alcanza la hora de apagado del teléfono pero el teléfono está en uso. El intervalo para el campo es de entre 20 y 1440 minutos. El valor predeterminado es 60 minutos.

Campo	Descripción
Activar alerta sonora	Si está activada, indica al teléfono que reproduzca una alerta sonora desde 10 minutos antes de la hora especificada en el campo Hora de apagado del teléfono. La alerta sonora usa el tono de llamada del teléfono, que se reproduce brevemente en momentos específicos durante el período de alerta de 10 minutos. El tono de llamada de alerta se reproduce al volumen indicado por el usuario. La programación de la alerta sonora es la siguiente: • Diez minutos antes del apagado, el tono de llamada se reproduce cuatro veces. • Siete minutos antes del apagado, el tono de llamada se reproduce cuatro veces. • Cuatro minutos antes del apagado, el tono de llamada se reproduce cuatro veces. • Treinta segundos antes del apagado, el tono se reproduce quince veces o hasta que el teléfono se apague. Esta casilla de verificación solo se aplica si en la lista de Activar Power Save Plus se han seleccionado uno o varios días.
Dominio de EnergyWise	El dominio de EnergyWise en el que se encuentra el teléfono. La longitud máxima de este campo es de 127 caracteres.
Secreto de EnergyWise	La contraseña secreta de seguridad que se usa para comunicarse con los terminales del dominio de EnergyWise. La longitud máxima de este campo es de 127 caracteres.
Permitir anulaciones de EnergyWise	Esta casilla de verificación determina si se permite a la directiva del controlador del dominio de EnergyWise enviar actualizaciones del nivel de energía a los teléfonos. Se aplican las condiciones siguientes: • Se deben seleccionar uno o varios días en el campo Activar Power Save Plus. • Los ajustes de Cisco Unified Communications Manager Administration surten efecto según la programación, incluso aunque EnergyWise envíe una anulación. Por ejemplo, supongamos que en Hora de apagado del teléfono se indique 22:00 (las 10 de la noche), que el valor del campo Hora de encendido del teléfono sea 06:00 (las 6 de la mañana) y que Activar Power Save Plus tenga uno o varios días seleccionados. • Si EnergyWise indica al teléfono que se apague a las 20:00 (las 8 de la tarde), esa directiva sigue en vigor (siempre que no se produzca ninguna intervención del usuario en el teléfono) hasta la hora configurada en Hora de encendido del teléfono a las 6:00. • A las 6:00, el teléfono se enciende y vuelve a recibir los cambios de nivel de energía según la configuración de la administración de Unified Communications Manager. • Para volver a cambiar el nivel de energía del teléfono, EnergyWise debe emitir de nuevo un comando de cambio de nivel de energía. **Nota** Para desactivar Power Save Plus, debe quitar la marca de la casilla de verificación Permitir anulación de EnergyWise. Si esta casilla sigue marcada pero no se selecciona ningún día en el campo Activar Power Save Plus, Power Save Plus no se desactiva.

Paso 4 Seleccione **Guardar**.

Paso 5 Seleccione **Aplicar configuración**.

Paso 6 Reinicie el teléfono.

Configuración de la función No molestar

Cuando la opción No molestar (DND) está activada, el encabezado de la pantalla de teléfono para conferencias se pondrá en roja.

Para obtener más información, consulte los datos sobre la función No molestar en la documentación de su versión concreta de Cisco Unified Communications Manager.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Dispositivo** > **Teléfono**.

Paso 2 Localice el teléfono que desea configurar.

Paso 3 Establezca los parámetros siguientes.

- No molestar: esta casilla de verificación permite activar DND en el teléfono.
- Opción de DND: timbre desactivado, llamada rechazada o usar la configuración del perfil del teléfono común.
- Alerta de llamada entrante de DND: seleccione el tipo de alerta, en caso de recibir alguna, que se debe reproducir en un teléfono para las llamadas entrantes si DND está activado.

  Nota Este parámetro se encuentra en la ventana Perfil de teléfono común como en la ventana de configuración del teléfono. El valor de la ventana de configuración del teléfono tiene prioridad.

Paso 4 Seleccione **Guardar**.

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

Configuración de la notificación de desvío de llamadas

Es posible controlar la configuración del desvío de llamadas.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Dispositivo** > **Teléfono**.

Paso 2 Localice el teléfono que desea configurar.

Paso 3 Configure los campos Notificación de desvío de llamadas.

Campo	Descripción
Nombre de la persona que llama	Si esta casilla de verificación está marcada, en la ventana de notificación se muestra el nombre de la persona que llama. De forma predeterminada, esta casilla de verificación está marcada.
Número de la persona que llama	Si esta casilla de verificación está marcada, en la ventana de notificación se muestra el número de la persona que llama. De forma predeterminada, esta casilla de verificación no está marcada.
Número redirigido	Si esta casilla de verificación está marcada, en la ventana de notificación se muestra información sobre la persona que llama que desvío en último lugar la llamada. Ejemplo: si A llama a B, pero B ha desviado todas las llamadas a C y C ha desviado todas las llamadas a D, el cuadro de notificación que D ve contiene la información del teléfono de C. De forma predeterminada, esta casilla de verificación no está marcada.
Número marcado	Si esta casilla de verificación está marcada, en la ventana de notificación se muestra información sobre el destinatario original de la llamada. Ejemplo: si A llama a B, pero B ha desviado todas las llamadas a C y C ha desviado todas las llamadas a D, el cuadro de notificación que D ve contiene la información del teléfono de B. De forma predeterminada, esta casilla de verificación está marcada.

Paso 4 Seleccione **Guardar**.

Configuración de UCR 2008

Los parámetros que admite UCR 2008 se encuentran en Cisco Unified Communications Manager Administration. En la tabla siguiente se describen los parámetros se indica la ruta para cambiar la configuración.

Tabla 21: Ubicación del parámetro UCR 2008

Parámetro	Ruta de administración
Modo FIPS	**Dispositivo** > **Configuración del dispositivo** > **Perfil de teléfono común**
	Sistema > **Configuración de teléfono empresarial**
	Dispositivo > **Teléfono**
Acceso SSH	**Dispositivo** > **Teléfono**
	Dispositivo > **Configuración del dispositivo** > **Perfil de teléfono común**

Parámetro	Ruta de administración
Acceso vía Web	**Dispositivo** > **Teléfono**
	Sistema > **Configuración de teléfono empresarial**
	Dispositivo > **Configuración del dispositivo** > **Perfil de teléfono común**
Sistema > **Configuración de teléfono empresarial**	
Modo de direcciones IP	**Dispositivo** > **Configuración del dispositivo** > **Configuración de dispositivo común**
Modo de direcciones IP preferidas para señalización	**Dispositivo** > **Configuración del dispositivo** > **Configuración de dispositivo común**

Configuración de UCR 2008 en la configuración de dispositivo común

Use este procedimiento para establecer los siguientes parámetros de UCR 2008:

- Modo de direcciones IP
- Modo de direcciones IP preferidas para señalización

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Dispositivo** > **Configuración del dispositivo** > **Configuración de dispositivo común**.

Paso 2 Establezca el parámetro Modo de direcciones IP.

Paso 3 Establezca el parámetro Modo de direcciones IP preferidas para señalización.

Paso 4 Seleccione **Guardar**.

Configuración de UCR 2008 en el perfil de teléfono común

Use este procedimiento para establecer los siguientes parámetros de UCR 2008:

- Modo FIPS
- Acceso SSH
- Acceso vía Web

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Dispositivo** > **Configuración del dispositivo** > **Perfil de teléfono común**.

Paso 2 En el parámetro Modo FIPS, establezca **Activado**.

Paso 3 En el parámetro Acceso SSH, establezca **Desactivado**.

Paso 4 En el parámetro Acceso vía web, establezca **Desactivado**.

Paso 5 En el parámetro SRTCP de 80 bits, establezca **Activado**.

Paso 6 Seleccione **Guardar**.

Configuración de UCR 2008 en la configuración de teléfono empresarial

Use este procedimiento para establecer los siguientes parámetros de UCR 2008:

- Modo FIPS
- Acceso vía Web

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Sistema** > **Configuración de teléfono empresarial**.

Paso 2 En el parámetro Modo FIPS, establezca **Activado**.

Paso 3 En el parámetro Acceso vía web, establezca **Desactivado**.

Paso 4 Seleccione **Guardar**.

Configuración de UCR 2008 en el teléfono

Use este procedimiento para establecer los siguientes parámetros de UCR 2008:

- Modo FIPS
- Acceso SSH
- Acceso vía Web

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Dispositivo** > **Teléfono**.

Paso 2 En el parámetro Acceso SSH, establezca **Desactivado**.

Paso 3 En el parámetro Modo FIPS, establezca **Activado**.

Paso 4 En el parámetro Acceso vía web, establezca **Desactivado**.

Paso 5 Seleccione **Guardar**.

Mobile and Remote Access mediante Expressway

Mobile and Remote Access mediante Expressway(MRA) permite a los trabajadores remotos conectarse de forma sencilla y segura con la red corporativa mediante un túnel de cliente de una red privada virtual (VPN).

Expressway usa la seguridad de Seguridad de la capa de transporte (TLS) para asegurar el tráfico de red. Para que un teléfono pueda autenticar un certificado de Expressway y establecer una sesión de TLS, el certificado de Expressway debe estar firmado por una entidad emisora de certificados pública que sea de confianza en el firmware del teléfono. No es posible instalar ni confiar en otros certificados de CA en los teléfonos para autenticar un certificado de Expressway.

La lista de certificados de CA integrada en el firmware del teléfono está disponible en http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html.

Mobile and Remote Access mediante Expressway (MRA) funciona con Cisco Expressway. Debe estar familiarizado con la documentación de Cisco Expressway, incluida la *Guía del administrador de Cisco Expressway* y la *Guía de implementación de la configuración básica de Cisco Expressway*. La documentación de Cisco Expressway está disponible en http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html.

Para los usuarios de Mobile and Remote Access mediante Expressway, solo se admite el protocolo IPv4.

Para obtener más información sobre el trabajo con Mobile and Remote Access mediante Expressway, consulte:

- *Arquitectura preferida de Cisco para la colaboración empresarial: descripción general del diseño*
- *Arquitectura preferida de Cisco para la colaboración empresarial: CVD*
- *Guía de implementación de Mobile and Remote Access de Unified Communications mediante Cisco VCS*
- *Cisco TelePresence Video Communication Server (VCS): guías de configuración*
- *Guía de implementación de acceso móvil y remoto mediante Cisco Expressway*

Durante el proceso de registro del teléfono, este sincroniza la fecha y hora mostradas con el servidor de protocolo de hora de red (NTP). Con MRA, se usa la etiqueta 42 de la opción DHCP para localizar las direcciones IP de los servidores NTP designados para la sincronización de la fecha y la hora. Si no se encuentra esta etiqueta en los datos de configuración, el teléfono busca la etiqueta 0.tandberg.pool.ntp.org para identificar los servidores NTP.

Después del registro, el teléfono usa información del mensaje SIP para sincronizar la fecha y hora mostradas, a no ser que haya un servidor NTP configurado en los ajustes del teléfono de Cisco Unified Communications Manager.

Nota Si el perfil de seguridad de cualquiera de los teléfonos tiene marcada la opción de configuración cifrada de TFTP, no podrá usar el teléfono con Mobile and Remote Access. La solución MRA no admite la interacción con dispositivos que interactúen con CAPF (función de proxy de entidad emisora de certificados).

El modo de OAuth de SIP se admite para MRA. Este modo permite usar tokens de acceso de OAuth para la autenticación en entornos seguros.

Nota Para OAuth de SIP en el modo Mobile and Remote Access (MRA), utilice únicamente la incorporación de código de activación con Acceso móvil y remoto cuando despliegue el teléfono. No se admite la activación con un nombre de usuario y una contraseña.

El modo OAuth de SIP necesita Expressway x 14.0(1) y posterior, o Cisco Unified Communications Manager 14.0(1) y posterior.

Para obtener información adicional sobre el modo OAuth de SIP, consulte la *Guía de configuración de funciones para Cisco Unified Communications Manager*, versión 14.0(1) o posterior.

Ejemplos de implementación

En la tabla siguiente se muestran varias situaciones de implementación para Mobile and Remote Access mediante Expressway.

Situación	Acciones
El usuario que se encuentra en las instalaciones inicia sesión en la red de la empresa después de implementar Mobile and Remote Access mediante Expressway.	Se detecta la red de la empresa y el teléfono se registra en Cisco Unified Communications Manager, como sucede habitualmente.
El usuario que se encuentra fuera las instalaciones inicia sesión en la red de la empresa con Mobile and Remote Access mediante Expressway.	El teléfono detecta que se encuentra en modo externo, se abre la ventana Conectar de Mobile and Remote Access mediante Expressway y el usuario se conecta a la red corporativa. Los usuarios deben tener un nombre de servicio válido, un nombre de usuario y una contraseña para conectarse a la red. Los usuarios también deben restablecer el modo de servicio para borrar el ajuste de TFTP alternativo para poder acceder a la red de la empresa. Esto borra la configuración de servidor TFTP alternativo para que el teléfono detecte la red externa. Si se va a implementar un teléfono desde cero, los usuarios pueden omitir el requisito de restablecimiento de la configuración de red. Si los usuarios tienen la opción 150 o la opción 66 de DHCP habilitadas en el router de red, quizás no puedan iniciar sesión en la red corporativa. Deben desactivar estos ajustes de DHCP o configurar directamente su dirección IP estática.

Configuración de credenciales de usuario persistentes para el inicio de sesión de Expressway

Al iniciar sesión en la red con Mobile and Remote Access mediante Expressway, se solicita al usuario un nombre de dominio, un nombre de usuario y una contraseña. Si activa el parámetro de credenciales de usuario persistentes para el inicio de sesión de Expressway, las credenciales de inicio de sesión de los usuarios se almacenan para no tener que volver a introducir esos datos. Este parámetro está desactivado de manera predeterminada.

Puede configurar las credenciales para que se conserven en un único teléfono, un grupo de teléfonos o todos los teléfonos.

Temas relacionados

Configuración de funciones del teléfono, en la página 98
Configuración específica del producto, en la página 100

Herramienta de informe de problemas

Los usuarios le enviarán los informes de problemas con la Herramienta de informe de problemas.

Nota El servicio de asistencia técnica de Cisco necesita los registros de la Herramienta de informe de problemas para solucionar los problemas. Si reinicia el teléfono, se borrarán los registros. Recopile los registros antes de reiniciar los teléfonos.

Para emitir un informe de problema, los usuarios acceden a la Herramienta de informe de problemas y proporcionan la fecha y la hora a la que se produjo, así como una descripción del asunto.

Puede acceder al archivo PRT del teléfono desde la URL **`http://<phone-ip-address>/FS/<prt-file-name>`** si se produce un error en la carga de PRT. Esta URL se muestra en el teléfono en los casos siguientes:

- Si el teléfono se encuentra en el estado predeterminado de fábrica. Si la URL está activa durante 1 hora. Después de 1 hora, el usuario debe intentar de nuevo el envío de los registros del teléfono.
- Si se ha descargado un archivo de configuración en el teléfono y el sistema de control de llamadas permite el acceso web al teléfono.

Debe agregar la dirección de un servidor al campo **URL de carga del servicio de atención al cliente** de Cisco Unified Communications Manager.

Si va a implementar dispositivos con Mobile and Remote Access mediante Expressway, también debe agregar la dirección del servidor de la Herramienta de informe de problemas a la lista de servidores HTTP permitidos en el servidor de Expressway.

Configuración de una URL de carga del servicio de atención al cliente

Debe usar un servidor con un script de carga para recibir archivos PRT. La Herramienta de informe de problemas (PRT) usa un mecanismo POST de HTTP con los siguientes parámetros incluidos en la carga (se utiliza la codificación MIME de varias partes):

- devicename (ejemplo: «SEP001122334455»)
- serialno (ejemplo: «FCH12345ABC»)
- username (el nombre de usuario configurado en Cisco Unified Communications Manager, el propietario del dispositivo)
- prt_file (ejemplo: «probrep-20141021-162840.tar.gz»)

A continuación, se muestra un script de ejemplo. El script se proporciona solo como referencia. Cisco no ofrece asistencia para el script de carga instalado en el servidor de un cliente.

```
<?php

// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
// I used:  upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);
```

```
// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
$devicename = trim($devicename, "'\"");

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "'\"");

$username = $_POST['username'];
$username = trim($username, "'\"");

// where to put the file
$fullfilename = "/var/prtuploads/".$filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
        header("HTTP/1.0 500 Internal Server Error");
        die("Error: You must select a file to upload.");
}

?>
```

Nota Los teléfonos solo admiten direcciones URL HTTP.

Procedimiento

Paso 1 Configure un servidor que pueda ejecutar el script de carga de PRT.

Paso 2 Escriba un script que pueda manejar los parámetros indicados más arriba, o bien edite el que se proporciona de ejemplo para adaptarlo a sus necesidades.

Paso 3 Cargue su script al servidor.

Paso 4 En Cisco Unified Communications Manager, diríjase a la sección Diseño de la configuración específica de producto de la ventana de configuración del dispositivo individual, la ventana Perfil de teléfono común o la ventana Configuración de teléfono empresarial.

Paso 5 Marque la opción **URL de carga de asistencia al cliente** e introduzca la URL del servidor de carga.

Ejemplo:

http://ejemplo.com/prtscript.php

Paso 6 Guarde los cambios.

Establecimiento de la etiqueta para una línea

Puede configurar el teléfono para que muestre una etiqueta de texto en lugar del número de directorio. Use esta etiqueta para identificar la línea según el nombre o función. Por ejemplo, si el usuario comparte líneas en el teléfono, puede identificar la línea con el nombre de la persona que comparte la línea.

Al agregar una etiqueta a un módulo de expansión clave, solo se muestran los primeros 25 caracteres en una línea.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Dispositivo** > **Teléfono**.

Paso 2 Localice el teléfono que desea configurar.

Paso 3 Localice la línea y establezca el campo Texto de etiqueta de línea.

Paso 4 (Opcional) Si es preciso aplicar la etiqueta a otros dispositivos que comparten la línea, marque la casilla de verificación Actualizar configuración de dispositivo compartido y haga clic en **Propagar seleccionado**.

Paso 5 Seleccione **Guardar**.

CAPÍTULO 10

Directorio corporativo y personal

Configuración del directorio corporativo

El directorio corporativo permite a los usuarios buscar números de teléfono de los compañeros de trabajo. Para que se admita esta función, debe configurar los directorios corporativos.

Cisco Unified Communications Manager utiliza un directorio de Lightweight Directory Access Protocol (LDAP) para almacenar la información de autenticación y autorización de los usuarios de aplicaciones de Cisco Unified Communications Manager con Cisco Unified Communications Manager los que se relacionan. La autenticación establece los derechos del usuario para acceder al sistema. La autorización identifica los recursos de telefonía que un usuario tiene permitido usar, como una extensión específica del teléfono.

Para obtener más datos, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Después de completar la configuración del directorio LDAP, los usuarios pueden utilizar el servicio de directorio corporativo de su teléfono para buscar usuarios en él.

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

Configuración del directorio personal

El directorio personal permite a un usuario almacenar un conjunto de números personales.

El directorio personal incluye las siguientes funciones:

- Libreta personal de direcciones (LPD)
- Marcaciones rápidas

Los usuarios pueden usar estos métodos para acceder a las funciones del directorio personal:

- Desde un navegador web: los usuarios pueden acceder a la funciones de libreta personal de direcciones y marcación rápida desde el portal de autoayuda de Cisco Unified Communications.

- Desde el teléfono IP de Cisco: seleccione **Contactos** para buscar el directorio corporativo o la libreta personal del usuario.

Para configurar el directorio personal desde un navegador web, los usuarios deben acceder a su portal de autoayuda. Debe proporcionar a los usuarios una dirección URL e información para iniciar sesión.

PARTE IV

Solución de problemas del teléfono IP para conferencias de Cisco

CAPÍTULO 11

Sistemas de supervisión del teléfono

Descripción general de los sistemas de supervisión del teléfono

Puede ver distintos datos sobre el teléfono mediante el menú de estado y las páginas web de este. Esta información incluye lo siguiente:

- Información de dispositivo
- Información de la configuración de red
- Estadísticas de red
- Registros de dispositivos
- Estadísticas de flujo

En este capítulo se describe la información que puede conseguir en la página web del teléfono. Puede usar estos datos para supervisar de forma remota el funcionamiento de un teléfono y para prestar ayuda con la solución de problemas.

Temas relacionados

Solución de problemas del teléfono, en la página 157

Estado del teléfono IP de Cisco

En las secciones siguientes se describe cómo mostrar la información del modelo, los mensajes de estado y las estadísticas de red en los teléfonos IP de Cisco.

- Información de modelo: muestra información del hardware y el software del teléfono.
- Menú Estado: proporciona acceso a las pantallas que muestran los mensajes de estado, las estadísticas de red y las estadísticas de la llamada actual.

Puede usar la información que se muestra en estas pantallas para supervisar el funcionamiento de un teléfono y para prestar ayuda con la solución de problemas.

También puede conseguir gran parte de esta información y otros datos relacionados de forma remota a través de la página web del teléfono.

Apertura de la ventana Información del teléfono

Procedimiento

Paso 1 Presione **Configuración** > **Información del sistema**.

Paso 2 Para salir del menú, presione **Salir**.

Apertura del menú Estado

Procedimiento

Paso 1 Presione **Configuración** > **Estado**.

Paso 2 Para salir del menú, presione **Salir**.

Apertura de la ventana Mensajes de estado

Procedimiento

Paso 1 Presione **Configuración** > **Estado** > **Mensajes de estado**.

Paso 2 Para salir del menú, presione **Salir**.

Campos de Mensajes de estado

En la tabla siguiente se describen los mensajes de estado que se muestran en la pantalla correspondiente del teléfono.

Tabla 22: Mensajes de estado en el teléfono IP de Cisco

Mensaje	Descripción	Posible explicación y acción
No es posible adquirir una dirección IP desde DHCP	El teléfono no ha obtenido previamente una dirección IP de un servidor DHCP. Esto puede ocurrir cuando realiza una puesta a nuevo o una restauración de los valores de fábrica.	Confirme que el servidor DHCP está d dirección IP disponible para el teléfono

Mensaje	Descripción	Posible explicación y acción
Error tamaño TFTP	El archivo de configuración es demasiado grande para el sistema de archivos del teléfono.	Apague y encienda el teléfono.
Error de suma de comprobación de ROM	El archivo de software descargado está dañado.	Obtenga una copia nueva del firmw en el directorio de la ruta de TFTP. en este directorio cuando el softwar apagado; en caso contrario, los arch
IP duplicada	Otro dispositivo está usando la dirección IP asignada al teléfono.	Si el teléfono tiene una dirección IP ha asignado una dirección IP duplic Si utiliza DHCP, compruebe la confi
Borrando archivos CTL e ITL	Se está borrando el archivo CTL o ITL.	Ninguna. Este mensaje es únicamer
Error actual. config. regional	No se encuentran uno o varios archivos de ubicación en el directorio de la ruta de TFTP o no son válidos. No se ha cambiado la configuración regional.	En la administración del sistema op compruebe que los archivos siguier subdirectorios de la administración • Ubicado en el subdirectorio co configuración regional de la re • tones.xml • Ubicados en el subdirectorio c configuración regional del usu • glyphs.xml • dictionary.xml • kate.xml
Archivo no encontrado <Cfg File>	No se encuentra el archivo de configuración predeterminado basado en el nombre en el servidor TFTP.	El archivo de configuración de un t se agrega a la base de datos de Cisc Manager. Si el teléfono no existe en Unified Communications Manager, respuesta **`Archivo CFG no en`** • El teléfono no está registrado Communications Manager. Debe agregar manualmente el Communications Manager si n se registren automáticamente. • Si utiliza DHCP, verifique que servidor TFTP correcto. • Si usa direcciones IP estáticas, del servidor TFTP.

Mensaje	Descripción	Posible explicación y acción
Archivo no encontrado <CTLFile.tlv>	Este mensaje se muestra en el teléfono si el clúster de Cisco Unified Communications Manager no se encuentra en modo seguro.	No tiene efecto, ya que el teléfono pue Unified Communications Manager.
Dirección IP liberada	El teléfono está configurado para liberar la dirección IP.	El teléfono permanece inactivo hasta qu se restablece la dirección DHCP.
Tiempo de espera de DHCP de IPv4	El servidor DHCP IPv4 no responde.	La red está ocupada: los errores podría reduzca la carga de la red. No hay conectividad de red entre el ser teléfono: verifique las conexiones de re El servidor DHCP IPv4 está apagado: c configuración del servidor DHCP IPv4 Los errores persisten: plantéese asignar estática.
Tiempo de espera de DHCP de IPv6	El servidor DHCP IPv6 no responde.	La red está ocupada: los errores podría reduzca la carga de la red. No hay conectividad de red entre el ser teléfono: verifique las conexiones de re El servidor DHCP IPv6 está apagado: c configuración del servidor DHCP IPv6 Los errores persisten: plantéese asignar estática.
Tiempo de espera de DNS de IPv4	El servidor DNS IPv4 no responde.	La red está ocupada: los errores podría reduzca la carga de la red. No hay conectividad de red entre el ser teléfono: verifique las conexiones de re El servidor DNS IPv4 está apagado: con del servidor DNS IPv4.
Tiempo de espera de DNS de IPv6	El servidor DNS IPv6 no responde.	La red está ocupada: los errores podría reduzca la carga de la red. No hay conectividad de red entre el ser teléfono: verifique las conexiones de re El servidor DNS IPv6 está apagado: con del servidor DNS IPv6.
Host DNS de IPv4 desconocido	El servidor DNS IPv4 no puede resolver el nombre del servidor TFTP o de Cisco Unified Communications Manager.	Verifique que los nombres de host del se Unified Communications Manager está correctamente en el servidor DNS IPv4 Plantéese usar direcciones IPv4 en luga

Mensaje	Descripción	Posible explicación y acción
Host IPv6 DNS desconocido	El servidor DNS IPv6 no puede resolver el nombre del servidor TFTP o de Cisco Unified Communications Manager.	Verifique que los nombres de host d Unified Communications Manager correctamente en el servidor DNS I Plantéese usar direcciones IPv6 en
Carga rechazada HC	La aplicación descargada no es compatible con el hardware del teléfono.	Este problema se produce si intenta software en este teléfono que no adm del teléfono. Compruebe el ID de carga asignado Communications Manager, seleccio Vuelva a introducir la carga que se
No hay router predeterminado	En la configuración DHCP o estática no se especifica ningún router predeterminado.	Si el teléfono tiene una dirección IP router predeterminado está configu Si usa DHCP, el servidor DHCP no predeterminado. Compruebe la confi
Ningún servidor DNS de IPv4	Se ha especificado un nombre, pero en la configuración de DHCP o de la dirección IP estática no se especifica ninguna dirección de servidor DNS IPv4.	Si el teléfono tiene una dirección IP servidor DNS IPv4 está configurad Si usa DHCP, el servidor DHCP no h DNS IPv4. Compruebe la configura
Ningún servidor DNS de IPv6	Se ha especificado un nombre, pero en la configuración de DHCP o de la dirección IP estática no se especifica ninguna dirección de servidor DNS IPv6.	Si el teléfono tiene una dirección IP servidor DNS IPv6 está configurad Si usa DHCP, el servidor DHCP no h DNS IPv6. Compruebe la configura
Ninguna lista de confianza instalada	El archivo CTL o el archivo ITL no están instalados en el teléfono.	La lista de confianza no está config Communications Manager, que no seguridad de forma predeterminada La lista de confianza no está config Para obtener más información sobr consulte la documentación de su ve Unified Communications Manager.
Fallo al registrar el teléfono. El tamaño de clave de certificado no cumple con FIPS.	FIPS requiere que el certificado de servidor RSA sea de 2048 bits o mayor.	Actualice el certificado.
Reinicio solicitado por Cisco Unified Communications Manager	El teléfono se reinicia debido a una solicitud de Cisco Unified Communications Manager.	Es probable que se hayan realizado al teléfono en Cisco Unified Comm se haya presionado **Aplicar config** surta efecto.
Error de acceso a TFTP	El servidor TFTP dirige a un directorio que no existe.	Si utiliza DHCP, verifique que el se servidor TFTP correcto. Si usa direcciones IP estáticas, com servidor TFTP.

Mensaje	Descripción	Posible explicación y acción
Error de TFTP	El teléfono no reconoce un código de error proporcionado por el servidor TFTP.	Póngase en contacto con la asistencia t
Tiempo de espera de TFTP	El servidor TFTP no responde.	La red está ocupada: los errores podría reduzca la carga de la red. No hay conectividad de red entre el serv verifique las conexiones de red. El servidor TFTP está apagado: compru servidor TFTP.
Tiempo de espera agotado	El solicitante ha intentado realizar una transacción 802.1X, pero se ha agotado el tiempo de espera debido a la ausencia de un autenticador.	El tiempo de espera de la autenticación no está configurado en el switch.
Error al actualizar la lista de confianza	La actualización de los archivos CTL e ITL ha fallado.	El teléfono tiene archivos CTL e ITL ir actualizarlos. Posible motivo del error: • Se ha producido un error de red. • El servidor TFTP está apagado. • Se han introducido el nuevo token firmar el archivo CTL y el certifica firmar el archivo ITL, pero no esta archivos CTL e ITL actuales del t • Se ha producido un error interno c Posibles soluciones: • Compruebe la conectividad de la r • Compruebe si el servidor TFTP es normalidad. • Si el servidor TVS (servicios Vsar compatible con Cisco Unified Cor compruebe si este servidor está ac normalidad. • Verifique si el token de seguridad válidos. Si todas las soluciones anteriores fallar los archivos CTL e ITL y restablezca e Para obtener más información sobre las consulte la documentación de su versió Unified Communications Manager.
Lista de confianza actualizada	El archivo CTL, el archivo ITL o ambos están actualizados.	Ninguna. Este mensaje es únicamente i Para obtener más información sobre las consulte la documentación de su versió Unified Communications Manager.

Mensaje	Descripción	Posible explicación y acción
Error de versión	El nombre del archivo de carga del teléfono es incorrecto.	Asegúrese de que el archivo de carg nombre correcto.
XmlDefault.cnf.xml o .cnf.xml correspondiente al nombre del dispositivo del teléfono	Nombre del archivo de configuración.	Ninguna. Este mensaje indica el no configuración del teléfono.

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

Apertura de la ventana Estadísticas de red

Procedimiento

Paso 1 Presione **Configuración** > **Estado** > **Estadísticas de red**.

Paso 2 Para salir del menú, presione **Salir**.

Campos de Estadísticas de red

En la tabla siguiente se describe la información de la pantalla Estadísticas de red.

Tabla 23: Campos de Estadísticas de red

Elemento	Descripción
Fotogramas transmitidos	El número de paquetes enviados por el teléfono.
Transmitir difusiones	El número de paquetes de difusión enviados por el teléfono.
Transmisión de unidifusión	El número de paquetes de unidifusión transmitidos por el teléfono.
Fotogramas recibidos	El número de paquetes recibidos por el teléfono.
Recibir difusiones	El número de paquetes de difusión recibidos por el teléfono.
Unidifusión recibida	El número de paquetes de unidifusión recibidos por el teléfono.
ID de dispositivo vecino CDP	El identificador de un dispositivo conectado a este puerto descubierto por el protocolo CDP.
Dirección IP de vecino CDP	El identificador de un dispositivo conectado a este puerto descubierto por el protocolo CDP mediante IP.
Puerto de vecino CDP	El identificador de un dispositivo conectado a este puerto descubierto por el protocolo CDP.

Elemento	Descripción
Causa de reinicio: uno de estos valores: • Restablecimiento de hardware (restablecimiento de encendido) • Restablecimiento de software (controlador de memoria también restablecido) • Restablecimiento de software (controlador de memoria no restablecido) • Restablecimiento de guardián • Inicializado • Desconocido	Causa del último restablecimiento del teléfono.
Puerto 1	Estado de enlace y conexión del puerto de red (por ejemplo, **100 completo** significa que el puerto PC está en estado de enlace y ha negociado automáticamente una conexión de dúplex completo de 100 Mbps).
IPv4	Información sobre el estado de DHCP. Incluye los estados siguientes: • CDP BOUND • CDP INIT • DHCP BOUND • DHCP DISABLED • DHCP INIT • DHCP INVALID • DHCP REBINDING • DHCP REBOOT • DHCP RENEWING • DHCP REQUESTING • DHCP RESYNC • DHCP UNRECOGNIZED • DHCP WAITING COLDBOOT TIMEOUT • DISABLED DUPLICATE IP • SET DHCP COLDBOOT • SET DHCP DISABLED • SET DHCP FAST

Elemento	Descripción
IPv6	Información sobre el estado de DHCP. Incluye los estados siguientes: • CDP INIT • DHCP6 BOUND • DHCP6 DISABLED • DHCP6 RENEW • DHCP6 REBIND • DHCP6 INIT • DHCP6 SOLICIT • DHCP6 REQUEST • DHCP6 RELEASING • DHCP6 RELEASED • DHCP6 DISABLING • DHCP6 DECLINING • DHCP6 DECLINED • DHCP6 INFOREQ • DHCP6 INFOREQ DONE • DHCP6 INVALID • DISABLED DUPLICATE IPV6 • DHCP6 DECLINED DUPLICATE IP • ROUTER ADVERTISE • DHCP6 WAITING COLDBOOT TIMEOUT • DHCP6 TIMEOUT USING RESTORED VAL • DHCP6 TIMEOUT CANNOT RESTORE • IPV6 STACK TURNED OFF • ROUTER ADVERTISE • ROUTER ADVERTISE • UNRECOGNIZED MANAGED BY • ILLEGAL IPV6 STATE

Apertura de la ventana Estadísticas de llamadas

Procedimiento

Paso 1 Presione **Configuración** > **Estado** > **Estadísticas de llamadas**.

Paso 2 Para salir del menú, presione **Salir**.

Campos de Estadísticas de llamadas

En la tabla siguiente se describen los elementos de la pantalla de estadísticas de llamadas.

Tabla 24: Elementos de Estadísticas de llamadas

Elemento	Descripción
Códec del destinatario	Tipo de flujo de voz recibido (audio de flujo RTP desde códec): • G.729 • G.722 • G.722 AMR WB.XML • G.711 ley Mu • G.711 ley A • iLBC • OPUS
Códec del remitente	Tipo de flujo de voz transmitido (audio de flujo RTP desde códec): • G.729 • G.722 • G.722 AMR WB.XML • G.711 ley Mu • G.711 ley A • iLBC • OPUS
Tamaño del destinatario	Tamaño de los paquetes de voz, en milisegundos, en el flujo de voz de recepción (flujo RTP de audio).
Tamaño del remitente	Tamaño de los paquetes de voz, en milisegundos, en el flujo de voz de transmisión.

Elemento	Descripción
Paquetes del destinatario	El número de paquetes de voz RTP que se han recibido desde que se inició el flujo de voz. **Nota** Este número no es necesariamente idéntico al número de paquetes de voz RTP que se han recibido desde el inicio de la llamada, ya que esta podría haberse puesto en espera.
Paquetes de remitente	El número de paquetes de voz RTP que se han transmitido desde que se inició el flujo de voz. **Nota** Este número no es necesariamente idéntico al número de paquetes de voz RTP que se han transmitido desde el inicio de la llamada, ya que esta podría haberse puesto en espera.
Promedio de Jitter	La fluctuación media estimada del paquete RTP (retraso dinámico que se encuentra un paquete cuando atraviesa la red), en milisegundos, que se ha observado desde se empezó a recibir el flujo de voz.
Jitter máximo	El Jitter máximo, en milisegundos, que se ha observado desde se empezó a recibir el flujo de voz.
Destinatario descartado	El número de paquetes RTP del flujo de voz de recepción que se ha descartado (paquetes erróneos, que han llegado demasiado tarde, etc.). **Nota** El teléfono descarta los paquetes de ruido de confort de tipo de carga 19 generados por las puertas de enlace de Cisco, ya que incrementan este contador.
Paquetes perdidos destinatario	Los paquetes RTP que faltan (perdidos en el tránsito).
Mediciones de calidad de voz	
Proporción de encubrimiento acumulada	El número total de marcos de encubrimiento dividido por el número total de marcos de voz que se han recibido desde el inicio del flujo de voz.
Proporción de encubrimiento de intervalo	La proporción de marcos de encubrimiento respecto a los marcos de voz en el intervalo anterior de tres segundos de voz activa. Si se usa la detección de actividad de voz (VAD), podría necesitarse un intervalo mayor para acumular tres segundos de voz activa.
Proporción de encubrimiento máxima	La proporción mayor de encubrimiento de intervalo desde el inicio del flujo de voz.
Segundos de encubrimiento	El número de segundos que tienen eventos de encubrimiento (marcos perdidos) desde el inicio del flujo de voz (incluye los segundos con encubrimiento profundo).
Segundos de encubrimiento profundo	El número de segundos que tienen más del cinco por ciento de eventos de encubrimiento (marcos perdidos) desde el inicio del flujo de voz.

Elemento	Descripción
Latencia	Calcula la latencia de red, expresada en milisegundos. Representa una media de ejecución de la demora de ida y vuelta, medida cuando el receptor de RTCP informa de que ha recibido los bloques.

Página web del teléfono IP de Cisco

Todos los teléfonos IP de Cisco tienen una página web en la que puede observar gran variedad de información sobre el teléfono; por ejemplo:

- Información del dispositivo: muestra los ajustes del dispositivo y la información relacionada del teléfono.
- Configuración de red: muestra información de los valores de red y de otros ajustes del teléfono.
- Estadísticas de red: muestra hipervínculos con información sobre el tráfico de red.
- Registros de dispositivos: muestra hipervínculos con información que puede usar para resolver problemas.
- Estadísticas de flujo: muestra hipervínculos con distintas estadísticas del flujo.

En esta sección se describen los datos que puede conseguir en la página web del teléfono. Puede usar estos datos para supervisar de forma remota el funcionamiento de un teléfono y para prestar ayuda con la solución de problemas.

También es posible conseguir gran parte de esa información directamente en un teléfono.

Acceso a la página web del teléfono

Nota Si no puede acceder a la página web, puede que esté deshabilitada de forma predeterminada.

Procedimiento

Paso 1 Obtenga la dirección IP del teléfono IP de Cisco con uno de estos métodos:

a) Para buscar el teléfono en Cisco Unified Communications Manager Administration, seleccione **Dispositivo** > **Teléfono**. Los teléfonos que se registran en Cisco Unified Communications Manager muestran la dirección IP en la ventana para buscar y mostrar teléfonos, en la parte superior de la ventana de configuración del teléfono.

b) En el teléfono, presione **Configuración** > **Información del sistema** y, a continuación, desplácese al campo de dirección IPv4.

Paso 2 Abra un navegador web e introduzca la dirección URL siguiente, donde *dirección_IP* es la dirección IP del teléfono IP de Cisco:

http://<IP_address>

Página web Información de dispositivo

La sección Información del dispositivo de la página web del teléfono muestra los ajustes del dispositivo y la información relacionada del teléfono. En la tabla siguiente se describen estos elementos.

Para mostrar la sección Información del dispositivo, acceda a la página web del teléfono y haga clic en el hipervínculo **Información del dispositivo**.

Tabla 25: Campos de la página web Información de dispositivo

Campo	Descripción
Modo de servicio	El modo de servicio para el teléfono.
Dominio del servicio	El dominio del servicio.
Estado del servicio	El estado actual del servicio.
Dirección MAC	La dirección de control de acceso a los medios (MAC) del teléfono.
Nombre de host	Un nombre exclusivo fijo que se asigna automáticamente al teléfono según la dirección MAC.
N.º de directorio telefónico	El número de directorio que se ha asignado al teléfono.
ID de carga de la aplicación	Identifica la versión de carga de la aplicación.
ID de carga de inicio	Indica la versión de la carga de inicio.
Versión	Identificador del firmware que se está ejecutando en el teléfono.
Revisión de Hardware	Valor de revisión menor del hardware del teléfono.
N.º de serie	El número de serie exclusivo del teléfono.
N.º de modelo	El número de modelo del teléfono.
Mensaje en espera	Indica si hay un mensaje de voz en espera en la línea principal de este teléfono.
UDI	Muestra la información de identificador único de dispositivo (UDI) de Cisco sobre el teléfono: • Tipo de hardware • Nombre del modelo de teléfono • Identificador de producto • ID de versión (VID): especifica el número de versión del hardware principal. • N.º de serie
Hora	La hora del grupo de fecha y hora al que pertenece el teléfono. Esta información proviene de Cisco Unified Communications Manager.

Campo	Descripción
Zona horaria	La zona horaria del grupo de fecha y hora al que pertenece el teléfono. Esta información proviene de Cisco Unified Communications Manager.
Fecha	La fecha del grupo de fecha y hora al que pertenece el teléfono. Esta información proviene de Cisco Unified Communications Manager.
Memoria libre del sistema	Cantidad de memoria del sistema disponible.
Memoria libre de montículo de Java	Cantidad de memoria libre para el montículo de Java.
Memoria libre de grupo de Java	Cantidad de memoria libre para el grupo de Java.
Modo FIPS activado	Indica si está activado el modo de estándar federal de procesamiento de información (FIPS).

Página web Configuración de red

La sección Configuración de red de la página web de un teléfono muestra información de los valores de red y de otros ajustes del teléfono. En la tabla siguiente se describen estos elementos.

Es posible ver y establecer muchos de estos elementos en el menú Configuración de red del teléfono IP de Cisco.

Para mostrar la sección Configuración de red, acceda a la página web del teléfono y haga clic en el hipervínculo **Configuración de red**.

Tabla 26: Elementos de la sección Configuración de red

Elemento	Descripción
Dirección MAC	La dirección de control de acceso a los medios (MAC) del teléfono.
Nombre de host	El nombre de host que el servidor DHCP ha asignado al teléfono.
Nombre de dominio	El nombre del dominio del sistema de nombre de dominio (DNS) en el que se encuentra el te
Servidor DHCP	La dirección IP del servidor de protocolo de configuración de host dinámico (DHCP) desde l teléfono obtiene la dirección IP.
Servidor BOOTP	Indica si el teléfono obtiene la configuración de un servidor de protocolo de arranque-asignació o bootstrap).
DHCP	Indica si el teléfono usa DHCP.
Dirección IP	Indica la dirección del protocolo de Internet (IP) del teléfono.
Máscara de subred	La máscara de subred que usa el teléfono.
Router predeterminado 1	El router predeterminado que usa el teléfono.

Elemento	Descripción
Servidor DNS 1-3	El servidor de sistema de nombre de dominio primario (Servidor DNS 1) y los servidores D de seguridad opcionales (Servidor DNS 2 y 3) que usa el teléfono.
TFTP alternativo	Indica si el teléfono usa un servidor TFTP alternativo.
Servidor TFTP 1	El servidor de protocolo de transferencia de archivos trivial (TFTP) primario que usa el te
Servidor TFTP 2	El servidor de protocolo de transferencia de archivos trivial (TFTP) de copia de seguridad teléfono.
Dirección DHCP liberada	Indica los valores correspondientes a esa opción.
ID de VLAN operativo	La red de área local virtual (VLAN) operativa configurada en un switch Cisco Catalyst de miembro el teléfono.
ID de VLAN administrativo	La VLAN auxiliar de la que es miembro el teléfono.
Unified CM 1-5	Los nombres de host o las direcciones IP, en orden de prioridad, de los servidores de Cisc Communications Manager con los que se puede registrar el teléfono. Un elemento también mostrar la dirección IP de un router SRST capaz de proporcionar funciones limitadas de C Communications Manager, en caso de que dicho router esté disponible. Para un servidor disponible, un elemento muestra la dirección IP del servidor de Cisco Un Communications Manager y uno de los estados siguientes: • Activo: el servidor de Cisco Unified Communications Manager desde el que el teléf recibiendo los servicios de procesamiento de llamadas. • Reserva: el servidor de Cisco Unified Communications Manager al que cambia el te servidor actual deja de estar disponible. • En blanco: actualmente no hay conexión con este servidor de Cisco Unified Commu Manager. Un elemento también puede incluir la designación de Survivable Remote Site Telephony identifica un router SRST capaz de proporcionar un conjunto limitado de funciones de Ci Communications Manager. Este router asume el control del procesamiento de llamadas si demás servidores de Cisco Unified Communications Manager dejan de estar disponibles. Cisco Unified Communications Manager SRST siempre aparece el último en la lista de se incluso si está activo. La dirección del router SRST se configura en la sección Grupo de d de la ventana de configuración de Cisco Unified Communications Manager.
URL de Información	La dirección URL del texto de ayuda que aparece en el teléfono.
URL de Directorios	La dirección URL del servidor desde el que el teléfono obtiene la información de director
URL de Mensajes	La dirección URL del servidor desde el que el teléfono obtiene los servicios de mensajes.
URL de Servicios	La dirección URL del servidor desde el que el teléfono obtiene los servicios del teléfono
URL de inactividad	La dirección URL que el teléfono muestra cuando está inactivo durante el tiempo especif campo Tiempo URL de inactividad y no hay ningún menú abierto.

Elemento	Descripción
Tiempo URL de inactividad	El número de segundos que el teléfono permanece inactivo y no se abre ningún menú antes d active el servicio XML especificado en el campo URL de inactividad.
URL del servidor proxy	La dirección URL del servidor proxy que realiza las solicitudes HTTP a las direcciones de ho locales en nombre del cliente HTTP del teléfono y que proporciona respuestas desde el host r al cliente HTTP del teléfono.
URL de autenticación	La dirección URL que usa el teléfono para validar las solicitudes realizadas al servidor web del
Config. puerto switch	La velocidad y dúplex del puerto PC, donde: • A = Autonegociación • 10H = 10-BaseT/semidúplex • 10F = 10-BaseT/dúplex completo • 100H = 100-BaseT/semidúplex • 100F = 100-BaseT/dúplex completo • 1000F = 1000-BaseT/dúplex completo • No hay enlace = no hay conexión con el puerto de switch
Configuración regional de usuario	La configuración regional asociada con el usuario del teléfono. Identifica una serie de detalle compatibilidad para los usuarios, como el idioma, la fuente, el formato de fecha y hora e info sobre el teclado alfanumérico.
Config. regional de red	La configuración regional de la red asociada con el usuario del teléfono. Identifica una serie de de compatibilidad para el teléfono en una ubicación específica, como la definición de los ton cadencias utilizados por el teléfono.
Ver. config. regional usuario	La versión de la configuración regional del usuario cargada en el teléfono.
Ver. config. regional de red	La versión de la configuración regional de la red cargada en el teléfono.
Altavoz habilitado	Indica si el altavoz está activado en el teléfono.
Grupo de escucha	Indica si la función Grupo de escucha está activada en el teléfono. Grupo de escucha le permi utilizando el auricular y escuchar por el altavoz al mismo tiempo.
GARP habilitado	Indica si el teléfono recuerda las direcciones MAC de las respuestas ARP gratuitas.
Selec. línea auto. habilitada	Indica si el teléfono cambia el centro de atención de la llamada a las llamadas entrantes en to líneas.
DSCP para control llamadas	La clasificación IP DSCP para la señalización de control de llamadas.
DSCP para configuración	La clasificación IP DSCP para cualquier transferencia de configuración del teléfono.
DSCP para servicios	La clasificación IP DSCP para servicios basados en el teléfono.
Modo de seguridad	El modo de seguridad que se establece para el teléfono.

Elemento	Descripción
Acceso a web habilitado	Indica si el acceso web está habilitado (Sí) o deshabilitado (No) para el teléfono.
Acceso SSH activado	Indica si el teléfono acepta o bloquea las conexiones SSH.
CDP: puerto switch	Indica si existe compatibilidad con CDP en el puerto de switch (de forma predeterminada esta Habilite CDP en el puerto de switch para la asignación de VLAN del teléfono, la negociació la administración de QoS y la seguridad 802.1x. Habilite CDP en el puerto de switch si el teléfono se conecta a un switch de Cisco. Si CDP está deshabilitado en Cisco Unified Communications Manager, se muestra una ac que indica que CDP solo se debe deshabilitar en el puerto de switch si el teléfono se conecta que no sea de Cisco. Los valores de CDP actuales para el puerto PC y el puerto de switch se muestran en el me Configuración.
LLDP-MED: puerto switch	Indica si LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery) está h el puerto de switch.
LLDP Prioridad energética	Anuncia la prioridad energética del teléfono al switch, habilitando de esta forma el switch proporcione la energía oportuna a los teléfonos. Los valores disponibles son: • Desconocido: este es el valor predeterminado. • Bajo. • Alto. • Crítico.
LLDP ID del dispositivo	Identifica el ID del dispositivo asignado al teléfono para la administración del inventario.
Archivo CTL	Identifica el archivo CTL.
Archivo ITL	El archivo ITL contiene la lista de confianza inicial.
Firma ITL	Mejora la seguridad al usar el algoritmo hash seguro (SHA-1) en los archivos CTL e ITL
Servidor CAPF	El nombre del servidor CAPF usado por el teléfono.
TVS	El componente principal de seguridad de forma predeterminada. Los servicios de verifica confianza (TVS) permiten a los teléfonos IP de Cisco Unified autenticar los servidores de a como los servicios EM, el directorio y MIDlet durante el establecimiento de HTTPS.
Servidor TFTP	El nombre del servidor TFTP usado por el teléfono.
Sincronización de puerto automática	Sincroniza los puertos a la velocidad más reducida en la que se elimina la pérdida de paq
Cambiar configuración remota de puerto	Permite al administrador configurar la velocidad y la función del puerto de tabla de Cisco Collaboration Experience de forma remota mediante Cisco Unified Communications Ma Administration.
Configuración remota de puerto de PC	Indica si la configuración de puerto remoto de la velocidad y el modo dúplex para el puer activada o desactivada.

Elemento	Descripción
Modo de direcciones IP	Muestra el modo de direcciones IP disponible en el teléfono.
Control modo de pref. IP	Indica la versión de la dirección IP que utiliza el teléfono durante la señalización con Cisco U Communications Manager cuando tanto IPv4 como IPv6 están disponibles en el teléfono.
Modo de preferencias de IP para medios	Indica que, para los medios, el dispositivo usa una dirección IPv4 a fin de conectarse con Cisco Communications Manager.
Config. auto. de IPv6	Muestra si la configuración automática está activada o no en el teléfono.
DAD de IPv6	Verifica que la nueva dirección IPv6 de unidifusión sea exclusiva antes de que se asignen las dir a las interfaces.
Mensaje de redirección de aceptación de IPv6	Indica si el teléfono acepta los mensajes redirigidos desde el mismo router que se usó para el de destino.
Solicitud de eco de multidifusión de respuesta de IPv6	Indica que el teléfono envía un mensaje de respuesta de eco como respuesta a un mensaje del tipo enviado a una dirección IPv6.
Servidor de carga de IPv6	Se usa para optimizar el tiempo de instalación durante las actualizaciones del firmware del te descargar el tráfico de la WAN al almacenar imágenes localmente, lo que evita tener que cruz enlace WAN en cada actualización del teléfono.
Servidor de registro de IPv6	Indica la dirección IP y el puerto del equipo de registro remoto al que el teléfono envía los m de registro.
Servidor CAPF de IPv6	El nombre común (proveniente del certificado de Cisco Unified Communications Manager) d usado por el teléfono.
DHCPv6	El protocolo de configuración de host dinámico (DHCP) asigna automáticamente direcciones los dispositivos cuando se conectan a la red. En los Teléfono IP de Cisco Unified, DHCP está h de forma predeterminada.
Dirección IPv6	Muestra la dirección IPv6 actual del teléfono o permite al usuario introducir una dirección IPv
Longitud de prefijo de IPv6	Muestra la longitud actual del prefijo para la subred o permite al usuario introducir una longi prefijo nueva.
Router predeterminado 1 de IPv6	Muestra el router predeterminado usado por el teléfono o permite al usuario introducir un rou predeterminado nuevo.
Servidor DNS 1 de IPv6	Muestra el servidor DNSv6 primario usado por el teléfono o permite al usuario introducir un nuevo.
Servidor DNS 2 de IPv6	Muestra el servidor DNSv6 secundario usado por el teléfono o permite al usuario introducir un DNSv6 secundario nuevo.
TFTP alternativo de IPv6	Permite al usuario habilitar el uso de un servidor TFTP IPv6 alternativo (secundario).
Servidor TFTP 1 de IPv6	Muestra el servidor TFTP IPv6 primario usado por el teléfono o permite al usuario establecer un TFTP primario nuevo.

Elemento	Descripción
Servidor TFTP 2 de IPv6	Muestra el servidor TFTP IPv6 secundario usado en caso de que el primario no está dispo permite al usuario establecer un servidor TFTP secundario nuevo.
Dirección IPv6 liberada	Permite al usuario liberar información relacionada con IPv6.
Nivel de energía EnergyWise	Indica la medición de energía consumida por los dispositivos en una red EnergyWise.
Dominio de EnergyWise	Una agrupación administrativa de dispositivos con objeto de supervisar y controlar la ene

Página web Información de Ethernet

En la tabla siguiente se describe el contenido de la página web Información de Ethernet.

Tabla 27: Elementos de Información de Ethernet

Elemento	Descripción
Fotogramas transmitidos	El número total de paquetes que ha transmitido recibido el teléfono.
Transmitir difusiones	El número total de paquetes de difusión que transmite el teléfono.
Transmitir multidifusiones	El número total de paquetes de multidifusión que transmite el teléfono.
Transmisión de unidifusión	El número total de paquetes de unidifusión que transmite el teléfono.
Fotogramas recibidos	El número total de paquetes recibidos por el teléfono.
Recibir difusiones	El número total de paquetes de difusión que recibe el teléfono.
Recibir multidifusiones	El número total de paquetes de multidifusión que recibe el teléfono.
Unidifusión recibida	El número total de paquetes de unidifusión que recibe el teléfono.
Rx PacketNoDes	El número total de paquetes derramados que causa el descriptor que no es de acceso de memoria directa (DMA).

Páginas web de red

En la tabla siguiente se describe la información de las páginas web Área de red.

Nota Al hacer clic en el enlace **Red** situado debajo de las estadísticas de red, la página se titula «Información de puerto».

Tabla 28: Elementos de Área de red

Elemento	Descripción
Rx totalPkt	El número total de paquetes que ha recibido el teléfono.
Recibir multidifusiones	El número total de paquetes de multidifusión que ha recibido el teléfono.
Recibir difusiones	El número total de paquetes de difusión que ha recibido el teléfono.
Unidifusión recibida	El número total de paquetes de unidifusión que ha recibido el teléfono.
Rx tokenDrop	El número total de paquetes que se han interrumpido debido a falta de recursos (por ejemplo, por desbordamiento de FIFO).
Tx totalGoodPkt	El número total de paquetes correctos (multidifusión, difusión y unidifusión) que ha recibido el teléfono.
Transmitir difusiones	El número total de paquetes de difusión que ha transmitido el teléfono.
Transmitir multidifusiones	El número total de paquetes de multidifusión que ha transmitido el teléfono.
LLDP FramesOutTotal	El número total de marcos LLDP que el teléfono ha enviado.
LLDP AgeoutsTotal	El número total de marcos LLDP cuyo tiempo de espera se ha agotado en caché.
LLDP FramesDiscardedTotal	El número total de marcos LLDP que se han descargado porque faltaba alguno de los valores TLV, estaban fuera de servicio o contenían cadenas con una longitud fuera del intervalo.
Total marcos LLDP en errores	El número total de marcos LLDP que se han recibido con uno o más errores detectables.
LLDP FramesInTotal	El número total de marcos LLDP que el teléfono ha recibido.
LLDP TLVDiscardedTotal	El número total de TLV de LLDP que se han descartado.
LLDP TLVUnrecognizedTotal	El número total de TLV de LLDP que no se reconocen en el teléfono.
ID de dispositivo vecino CDP	El identificador de un dispositivo conectado a este puerto que CDP ha descubierto.
Dirección IP de vecino CDP	La dirección IP del dispositivo vecino descubierto que CDP ha descubierto.
Dirección IPv6 de vecino CDP	La dirección IPv6 del dispositivo vecino descubierto que CDP ha descubierto.
Puerto de vecino CDP	El puerto del dispositivo vecino en el que está conectado el teléfono que CDP ha descubierto.
ID de dispositivo vecino LLDP	El identificador de un dispositivo conectado a este puerto que LLDP ha descubierto.
Dirección IP de vecino LLDP	La dirección IP del dispositivo vecino descubierto que LLDP ha descubierto.

Elemento	Descripción
Dirección IPv6 de vecino LLDP	La dirección IPv6 del dispositivo vecino que CDP ha descubierto.
Puerto de vecino LLDP	El puerto del dispositivo vecino al que se conecta el teléfono que LLDP ha descubierto.
Información de puerto	La velocidad y el dúplex de la información.

Registros de consola, Volcados de memoria, Mensajes de estado y Páginas web de pantalla de depuración

En el encabezado Registros de dispositivo, los hiperenlaces Registros de consola, Volcados de memoria, Mensajes de estado y Pantalla de depuración hiperenlaces proporcionan información que ayuda a supervisar y resolver problemas del teléfono.

- Registros de consola: incluye hiperenlaces a archivos de registro individuales. Los archivos de registro de consola incluyen los mensajes de depuración y error que ha recibido el teléfono.
- Volcados de memoria: incluye hiperenlaces a archivos de volcado individuales. Los archivos de volcado de memoria incluyen datos recogidos cuando un teléfono se bloquea.
- Mensajes de estado: muestra los 10 mensajes de estado más recientes que ha generado el teléfono desde la última vez que se encendió. También puede obtener esta información en la pantalla Mensajes de estado del teléfono.
- Pantalla de depuración: muestra mensajes de depuración que podrían ser de utilidad a Cisco TAC si necesita ayuda para solucionar problemas.

Página web Estadísticas de flujo

Un teléfono IP de Cisco puede intercambiar flujos de información con hasta cinco dispositivos simultáneamente. Los teléfonos intercambian flujos de información cuando se encuentran en una llamada o cuando ejecutan un servicio que envía o recibe audio o datos.

Las secciones de estadísticas de flujo de la página web de un teléfono proporcionan información sobre estos flujos.

Para mostrar un área de estadísticas de flujo, acceda a la página web del teléfono y haga clic en uno de los hiperenlaces **Flujo**.

En la tabla siguiente se describen los elementos de las secciones de estadísticas de flujo.

Tabla 29: Campos Estadísticas de flujo

Elemento	Descripción
Dirección remota	Dirección IP y puerto UDP del destino del flujo.
Dirección local	Dirección IP y puerto UDP del teléfono.
Hora de inicio	La marca de hora interna indica cuándo solicitó Cisco Unified Communications Ma el teléfono iniciara la transmisión de los paquetes.

Elemento	Descripción
Estado de flujo	Indicación de si el flujo está activo o no.
Nombre de host	Un nombre exclusivo fijo que se asigna automáticamente al teléfono según la dirección
Paquetes de remitente	El número total de paquetes de datos de RTP que el teléfono ha transmitido desde que se la conexión. El valor es 0 si la conexión se establece en el modo de solo recepción.
Octetos de remitente	El número total de octetos de carga que el teléfono ha transmitido en paquetes de datos d desde que se inició la conexión. El valor es 0 si la conexión se establece en el modo de recepción.
Códec del remitente	El tipo de codificación de audio del flujo transmitido.
Informes remit. enviados (consulte la nota)	El número de veces que se ha enviado el informe de remitente de RTCP.
Hora de informe del remitente enviada (consulte la nota)	La marca de hora interna indica cuándo se envió por última vez el informe de remitente
Paquetes perdidos destinatario	El número total de paquetes de datos de RTP que se han perdido desde que se inició la rec de datos en esta conexión. Se define como el número de paquetes esperado menos el nú de paquetes recibidos en realidad, donde el número de paquetes recibidos incluye los q retrasan o llegan duplicados. El valor se muestra como 0 si la conexión se establece en e de solo envío.
Promedio de Jitter	Calcula la desviación media del tiempo de interarribo del paquete de datos de RTP, me milisegundos. El valor se muestra como 0 si la conexión se establece en el modo de solo
Códec del destinatario	El tipo de codificación de audio que se usa para el flujo recibido.
Informes destinatario enviados (consulte la nota)	El número de veces que se han enviado informes de receptor de RTCP.
Hora informe destinatario enviado (consulte la nota)	La marca de hora interna indica cuándo se ha enviado un informe de receptor de RTCP
Paquetes del destinatario	El número total de paquetes de datos de RTP que el teléfono ha recibido desde que se in recepción de datos en esta conexión. Incluye los paquetes que se reciben de fuentes dist se trata de una llamada de multidifusión. El valor se muestra como 0 si la conexión se es en el modo de solo envío.
Octetos del destinatario	El número total de octetos de carga que el dispositivo ha recibido en paquetes de datos d desde que se inició la conexión. Incluye los paquetes que se reciben de fuentes distintas trata de una llamada de multidifusión. El valor se muestra como 0 si la conexión se esta en el modo de solo envío.
Proporción de encubrimiento acumulada	El número total de marcos de encubrimiento dividido por el número total de marcos de v se han recibido desde el inicio del flujo de voz.

Elemento	Descripción
Proporción de encubrimiento de intervalo	La proporción de marcos de encubrimiento respecto a los marcos de voz en el interva de tres segundos de voz activa. Si la detección de actividad de voz (VAD) está en u necesitarse un intervalo mayor para acumular tres segundos de voz activa.
Proporción de encubrimiento máxima	La proporción mayor de encubrimiento de intervalo desde el inicio del flujo de voz
Segundos de encubrimiento	El número de segundos que tienen eventos de encubrimiento (marcos perdidos) desc del flujo de voz (incluye los segundos con encubrimiento profundo).
Segundos de encubrimiento profundo	El número de segundos que tienen más del cinco por ciento de eventos de encubrimien perdidos) desde el inicio del flujo de voz.
Latencia (consulte la nota)	Calcula la latencia de red, expresada en milisegundos. Representa una media de eje la demora de ida y vuelta, medida cuando el receptor de RTCP informa de que ha re bloques.
Jitter máximo	El valor máximo de fluctuación instantánea en milisegundos.
Tamaño del remitente	El tamaño del paquete de RTP, en milisegundos, del flujo transmitido.
Informes remit. recibidos (consulte la nota)	El número de veces que se han recibido informes de remitente de RTCP.
Hora de informe del remitente recibida (consulte la nota)	La hora de la última vez que se recibió un informe de remitente de RTCP.
Tamaño del destinatario	El tamaño del paquete de RTP, en milisegundos, del flujo recibido.
Destinatario descartado	Los paquetes de RTP que se han recibido de la red pero que se han descartado de lo de fluctuación.
Informes destinatario recibidos (consulte la nota)	El número de veces que se han recibido informes de receptor de RTCP.
Hora informe destinatario recibido (consulte la nota)	La hora de la última vez que se recibió un informe de receptor de RTCP.

Nota Si el protocolo de control RTP está desactivado, no se generan datos para este campo y, por lo tanto, se muestra el valor 0.

Solicitud de información del teléfono en XML

Para solucionar problemas, puede solicitar información al teléfono. La información resultante se presenta en formato XML. Hay disponible la siguiente información:

- CallInfo es la información de la sesión de llamada de una línea específica.
- LineInfo es la información de la configuración de línea del teléfono.
- ModeInfo es la información del modo del teléfono.

Antes de empezar

El acceso web debe estar activado para poder obtener la información.

El teléfono debe estar asociado con un usuario.

Procedimiento

Paso 1 Para obtener información de la llamada, introduzca la dirección URL siguiente en un navegador:
`http://<phone ip address>/CGI/Java/CallInfo<x>`

donde:

- <*phone ip address*> es la dirección IP del teléfono
- <*x*> es el número de línea sobre el que se quiere obtener información.

El comando devuelve un documento XML.

Paso 2 Para obtener información de la línea, introduzca la dirección URL siguiente en un navegador:
`http://<phone ip address>/CGI/Java/LineInfo`

donde:

- <*phone ip address*> es la dirección IP del teléfono

El comando devuelve un documento XML.

Paso 3 Para obtener información de modelo, introduzca la dirección URL siguiente en un navegador:
`http://<phone ip address>/CGI/Java/ModeInfo`

donde:

- <*phone ip address*> es la dirección IP del teléfono

El comando devuelve un documento XML.

Ejemplo de resultado del comando CallInfo

El código XML siguiente es un ejemplo del resultado del comando CallInfo.

```
<?xml version="1.0" encoding="UTF-8"?>
<CiscoIPPhoneCallLineInfo>
  <Prompt/>
  <Notify/>
  <Status/>
  <LineDirNum>1030</LineDirNum>
  <LineState>CONNECTED</LineState>
  <CiscoIPPhoneCallInfo>
     <CallState>CONNECTED</CallState>
     <CallType>INBOUND</CallType>
     <CallingPartyName/>
     <CallingPartyDirNum>9700</CallingPartyDirNum>
     <CalledPartyName/>
     <CalledPartyDirNum>1030</CalledPartyDirNum>
     <HuntPilotName/>
     <CallReference>30303060</CallReference>
     <CallDuration>12835</CallDuration>
     <CallStatus>null</CallStatus>
     <CallSecurity>UNAUTHENTICATED</CallSecurity>
     <CallPrecedence>ROUTINE</CallPrecedence>
     <FeatureList/>
   </CiscoIPPhoneCallInfo>
   <VisibleFeatureList>
     <Feature Position="1" Enabled="true" Label="End Call"/>
     <Feature Position="2" Enabled="true" Label="Show Detail"/>
   </VisibleFeatureList>
</CiscoIPPhoneCallLineInfo>
```

Ejemplo de resultado del comando LineInfo

El código XML siguiente es un ejemplo del resultado del comando LineInfo.

```
<CiscoIPPhoneLineInfo>
   <Prompt/>
   <Notify/>
   <Status>null</Status>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1028</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
     <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>ONHOOK</LineIconState>
   </CiscoIPPhoneLines>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1029</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>  <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>ONHOOK</LineIconState>
   </CiscoIPPhoneLines>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1030</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
     <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>CONNECTED</LineIconState>
   </CiscoIPPhoneLines>
   <CiscoIPPhoneLines>
     <LineType>2</LineType>
     <lineDirNum>9700</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
```

```
      <LineLabel>SD9700</LineLabel>
      <LineIconState>ON</LineIconState>
  </CiscoIPPhoneLines>
</CiscoIPPhoneLineInfo>
```

Ejemplo de resultado del comando ModeInfo

El código XML siguiente es un ejemplo del resultado del comando ModeInfo.

```
<?xml version="1.0" encoding="utf-8"?>
<CiscoIPPhoneModeInfo>
   <PlaneTitle>Applications</PlaneTitle>
   <PlaneFieldCount>12</PlaneFieldCount>
   <PlaneSoftKeyIndex>0</PlaneSoftKeyIndex>
   <PlaneSoftKeyMask>0</PlaneSoftKeyMask>
   <Prompt></Prompt>
   <Notify></Notify>
   <Status></Status>
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Call History</FieldName>
      <FieldValue></FieldValue>
   </CiscoIPPhoneFields>
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Preferences</FieldName>
      <FieldValue></FieldValue>
   </CiscoIPPhoneFields>
   ...
</CiscoIPPhoneModeInfo>
```

CAPÍTULO 12

Solución de problemas del teléfono

Información sobre la solución de problemas generales

En la tabla siguiente se proporciona información general para solucionar problemas del teléfono IP de Cisco.

Tabla 30: Solución de problemas del teléfono IP de Cisco

Resumen	Explicación
Reinicios del teléfono IP o imposibilidad de efectuar o contestar llamadas por tormentas de difusión prolongadas	Una tormenta de difusión de capa 2 prolongada (que dure varios minutos) de voz puede causar que los teléfonos IP se reinicien, que se pierda una curso o que no se pueda iniciar o contestar una llamada. Puede que los se recuperen hasta que finalice la tormenta de difusión.
Cambio de una conexión de red del teléfono a una estación de trabajo	Si alimenta el teléfono a través de la conexión de red, debe tener cuida desenchufar la conexión del red del teléfono y enchufar el cable a un e escritorio. **Precaución** La tarjeta de red del ordenador no puede recibir alimentaci de la conexión de red. Si entra alimentación a través de la tarjeta de red se destruirá. Para proteger la tarjeta de red, esp 10 segundos después de desenchufar el cable del teléfono enchufarlo a un ordenador. Este retraso da al switch tiemp para reconocer que ya no hay un teléfono en la línea y deja proporcionar alimentación al cable.

Resumen	Explicación
Cambio de la configuración del teléfono	De forma predeterminada, el ajuste de contraseña del administrador está bl para evitar que los usuarios realicen cambios que puedan afectar a su cone de red. Debe desbloquear el ajuste de contraseña de administrador para po configurarlo. Consulte Aplicación de una contraseña al teléfono, en la página 41 para ob información detallada. **Nota** Si no se define la contraseña de administrador en el perfil de t común, el usuario puede modificar los ajustes de red.
Falta de coincidencia de códecs entre el teléfono y otro dispositivo	Las estadísticas de RxType y TxType muestran el códec que se usa para la conversación entre el teléfono IP de Cisco y el otro dispositivo. Los valore estadísticas deben coincidir. Si no es así, verifique que el otro dispositivo p manejar la conversación del códec o que hay presente un transcodificador par el servicio. Consulte el apartado Apertura de la ventana Estadísticas de llar la página 140 para obtener información más detallada.
Falta de coincidencia de muestras de sonido entre el teléfono y otro dispositivo	Las estadísticas de RxSize y TxSize muestran el tamaño de los paquetes de se usan para la conversación entre el teléfono IP de Cisco y el otro disposit valores de estas estadísticas deben coincidir. Consulte el apartado Apertura ventana Estadísticas de llamadas, en la página 140 para obtener informació detallada.
Condición de bucle invertido	Si las condiciones siguientes se cumplen, se podría producir una situación invertido: • La opción de configuración del puerto de switch del teléfono está esta en 10 medio (10-BaseT/semidúplex). • El teléfono recibe energía de una fuente de alimentación externa. • El teléfono está apagado (la fuente de energía está desconectada). En este caso, el puerto de switch del teléfono puede desactivarse y se mues mensaje siguiente en el registro de la consola del switch: HALF_DUX_COLLISION_EXCEED_THRESHOLD Para resolver este problema, vuelva a habilitar el puerto desde el switch.

Problemas de inicio

Después de instalar un teléfono en la red y de agregarlo a Cisco Unified Communications Manager, el teléfono debería iniciarse como se describe en el tema relacionado indicado más abajo.

Si el teléfono no se inicia correctamente, consulte las secciones siguientes a fin de obtener instrucciones para solucionar problemas.

Temas relacionados

Verificación del inicio del teléfono, en la página 53

No se desarrolla el proceso normal de inicio en el teléfono IP de Cisco

Problema

Cuando se conecta un teléfono IP de Cisco al puerto de red, el teléfono no sigue el proceso de inicio normal descrito en el tema relacionado y la pantalla del teléfono no muestra información.

Motivo

Si el teléfono no sigue el proceso de inicio, puede deberse a que los cables estén dañados, a conexiones erróneas, a cortes de la red, a que falte alimentación o a que el teléfono no funcione correctamente.

Solución

Para determinar si el teléfono funciona correctamente, use las sugerencias siguientes para eliminar otros problemas potenciales.

- Verifique que el puerto de red funciona adecuadamente:
  - Cambie los cables Ethernet por otros cables que sepa que funcionan.
  - Desconecte un teléfono IP de Cisco que funcione de otro puerto y conéctelo a este puerto de red para comprobar que el puerto está activo.
  - Conecte el teléfono IP de Cisco que no se inicia en un puerto de red distinto que sepa que funciona correctamente.
  - Conecte el teléfono IP de Cisco que no se inicia directamente al puerto del switch, omitiendo el panel de conexiones de la oficina.
- Verifique que el teléfono recibe alimentación:
  - Si usa alimentación externa, compruebe que la toma de corriente funciona.
  - Si usa alimentación interna, use en su lugar la fuente de alimentación externa.
  - Si usa una fuente de alimentación externa, cámbiela por una unidad que sepa que funciona.
- Si el teléfono sigue sin iniciarse correctamente, enciéndalo desde la copia de seguridad de la imagen del software.
- Si el teléfono sigue sin iniciarse correctamente, realice un restablecimiento de los ajustes de fábrica.
- Después de intentar estas soluciones, si la pantalla del teléfono IP de Cisco no muestra ningún carácter después de cinco minutos, póngase en contacto con un representante del servicio técnico de Cisco para obtener más ayuda.

Temas relacionados

Verificación del inicio del teléfono, en la página 53

El teléfono IP de Cisco no se registra en Cisco Unified Communications Manager

Si el teléfono supera la primera etapa del proceso de inicio (los botones LED se encienden y se apagan de forma intermitente) pero continúa el ciclo con mensajes que se muestran en la pantalla del teléfono, el teléfono no se está iniciando correctamente. El teléfono no puede iniciarse correctamente a no ser que se conecte a la red Ethernet y se registre en un servidor de Cisco Unified Communications Manager.

Asimismo, algunos problemas de seguridad podrían impedir que el teléfono se inicie correctamente. Para obtener más información, consulte Procedimientos para solucionar problemas, en la página 169.

Se muestran mensajes de error en el teléfono

Problema

Los mensajes de estado muestran errores durante el inicio.

Solución

A medida que el teléfono pasa por el proceso de inicio, puede acceder a los mensajes de estado que proporcionan información sobre la causa de los problemas. Consulte la sección «Apertura de la ventana Mensajes de estado» para obtener instrucciones sobre cómo acceder a los mensajes de estado y para ver una lista de los errores potenciales, su explicación y sus soluciones.

Temas relacionados

Apertura de la ventana Mensajes de estado, en la página 132

El teléfono no se conecta con el servidor TFTP o con Cisco Unified Communications Manager

Problema

Si la red entre el teléfono y el servidor TFTP o Cisco Unified Communications Manager no está activa, el teléfono no se puede iniciar correctamente.

Solución

Asegúrese de que la red se está ejecutando.

El teléfono no se conecta con el servidor TFTP

Problema

Puede que la configuración del servidor TFTP no sea correcta.

Solución

Compruebe la configuración de TFTP.

Temas relacionados

Comprobación de la configuración de TFTP, en la página 169

El teléfono no se conecta con el servidor

Problema

Puede que los campos de direcciones IP y enrutado no estén configurados correctamente.

Solución

Debe verificar los ajustes de direcciones IP y enrutado en el teléfono. Si usa DHCP, el servidor DHCP debe proporcionar estos valores. Si ha asignado una dirección IP estática al teléfono, debe introducir estos valores manualmente.

Temas relacionados

Comprobación de la configuración de DHCP, en la página 170

El teléfono no se conecta mediante la DNS

Problema

Puede que la configuración de DNS sea incorrecta.

Solución

Si usa DNS para acceder al servidor TFTP o a Cisco Unified Communications Manager, debe asegurarse de especificar un servidor DNS.

Temas relacionados

Verificación de la configuración de DNS, en la página 172

Cisco Unified Communications Manager y los servicios TFTP no se ejecutan

Problema

Si Cisco Unified Communications Manager o los servicios TFTP no se ejecutan, puede que los teléfonos no puedan iniciarse correctamente. En tal caso, es probable que experimente un fallo general del sistema y que otros teléfonos y dispositivos no puedan iniciarse correctamente.

Solución

Si el servicio Cisco Unified Communications Manager no se está ejecutando, todos los dispositivos de la red que se basan en él para efectuar llamadas telefónicas se verán afectados. Si el servicio TFTP no se está ejecutando, muchos dispositivos no se podrán iniciar correctamente. Para obtener más información, consulte Inicio del servicio, en la página 172.

El archivo de configuración está dañado

Problema

Si sigue teniendo problemas con un teléfono concreto que no se resuelven con otras sugerencias de este capítulo, puede que el archivo de configuración esté dañado.

Solución

Cree un nuevo archivo de configuración del teléfono.

Temas relacionados

Creación de un archivo de configuración del teléfono, en la página 171

Registro del teléfono en Cisco Unified Communications Manager

Problema

El teléfono no está registrado en Cisco Unified Communications Manager.

Solución

Un teléfono IP de Cisco se puede registrar en un servidor de Cisco Unified Communications Manager solo si el teléfono se agrega al servidor o si el registro automático está activado. Revise la información y los procedimientos de Métodos de adición de teléfonos, en la página 60 para asegurarse de que el teléfono se ha agregado a la base de datos de Cisco Unified Communications Manager.

Para verificar si el teléfono se encuentra en la base de datos de Cisco Unified Communications Manager, seleccione **Dispositivo** > **Teléfono** en Cisco Unified Communications Manager Administration. Haga clic en **Buscar** para buscar el teléfono según su dirección MAC. Para obtener información sobre cómo determinar la dirección MAC, consulte Determinación de la dirección MAC del teléfono, en la página 60.

Si el teléfono ya está en la base de datos de Cisco Unified Communications Manager, puede que el archivo de configuración esté dañado. Consulte El archivo de configuración está dañado, en la página 161 para obtener ayuda.

El teléfono IP de Cisco no puede obtener la dirección IP

Problema

Si un teléfono puede obtener una dirección IP cuando se inicia, puede que no esté en la misma red o VLAN que el servidor DHCP, o puede que el puerto de switch con el que conecta el teléfono esté desactivado.

Solución

Asegúrese de que la red o la VLAN a la que se conecta el teléfono tienen acceso al servidor DHCP y de que el puerto de switch esté activado.

Problemas de restablecimiento del teléfono

Si los usuarios informan de que sus teléfonos se restablecen durante las llamadas o mientras se encuentran inactivos, debe investigar la causa. Si la conexión de red y la conexión de Cisco Unified Communications Manager son estables, el teléfono no debería restablecerse.

En general, un teléfono se restablece si tiene problemas al conectarse con la red o con Cisco Unified Communications Manager.

El teléfono se restablece por cortes intermitentes de la red

Problema

Puede que la red sufra cortes intermitentes.

Solución

Las interrupciones intermitentes de red afectan al tráfico de voz y datos de forma distinta. La red podría experimentar interrupciones intermitentes sin que se detecten. En ese caso, el tráfico de datos puede reenviar paquetes perdidos y verificar que los paquetes se reciben y transmiten. Sin embargo, el tráfico de voz no puede recuperar paquetes perdidos. En lugar de retransmitir una conexión de red perdida, el teléfono se restablece e intenta volver a conectarse a la red. Póngase en contacto con el administrador del sistema para obtener información sobre los problemas conocidos de la red de voz.

El teléfono se restablece por errores de configuración de DHCP

Problema

Puede que la configuración de DHCP sea incorrecta.

Solución

Compruebe que ha configurado correctamente el teléfono para usar DHCP. Compruebe que el servidor DHCP esté configurado correctamente. Compruebe la duración de liberación de DHCP. Se recomienda establecer la duración de liberación en 8 días.

Temas relacionados

Comprobación de la configuración de DHCP, en la página 170

El teléfono se restablece por una dirección IP estática incorrecta

Problema

La dirección IP estática asignada al teléfono puede ser incorrecta.

Solución

Si el teléfono tiene una dirección IP estática asignada, verifique que ha introducido los ajustes correctos.

El teléfono se restablece durante un uso intensivo de la red

Problema

Si el teléfono se restablece durante un uso intensivo de la red, es probable que no tenga una VLAN de voz configurada.

Solución

Aislar los teléfonos en una VLAN auxiliar independiente aumenta la calidad del tráfico de voz.

El teléfono se restablece de forma intencionada

Problema

Si no es el único administrador con acceso a Cisco Unified Communications Manager, debe verificar que ningún otro administrador haya restablecido de forma intencionada los teléfonos.

Solución

Puede comprobar si un teléfono IP de Cisco ha recibido un comando de Cisco Unified Communications Manager para restablecerlo presionando **Configuración** en el teléfono y seleccionando **Config. admin.** > **Estado** > **Estadísticas de red**.

- Si en el campo Causa de reinicio se muestra `Restablecer/Restablecer`, el teléfono recibe un comando Restablecer/Restablecer de Cisco Unified Communications Manager Administration.
- Si en el campo Causa de reinicio se muestra `Restaurar-Reiniciar`, el teléfono se cierra porque recibe un comando Restablecer/Reiniciar de Cisco Unified Communications Manager Administration.

El teléfono se restablece por problemas con la DNS u otros problemas de conectividad

Problema

El restablecimiento del teléfono continúa y sospecha que hay algún problema de DNS o de conectividad.

Solución

Si el teléfono continúa restableciéndose, para eliminar los errores de DNS o de conectividad, siga el procedimiento descrito en Determinación de los problemas de DNS o de conectividad, en la página 170.

El teléfono no recibe alimentación

Problema

Parece que el teléfono no recibe alimentación.

Solución

En la mayoría de los casos, el teléfono se reinicia si recibe alimentación de una fuente de alimentación externa pero pierde la conexión y cambia a PoE. Del mismo modo, el teléfono se puede reiniciar si recibe la alimentación mediante PoE y se conecta a una fuente de alimentación externa.

El teléfono no se conecta con la LAN

Problema

La conexión física con la LAN podría estar rota.

Solución

Verifique que la conexión Ethernet a la que está conectado el teléfono IP de Cisco funciona correctamente. Por ejemplo, compruebe si el puerto o switch en concreto al que esté conectado el teléfono no funciona o si el switch se está reiniciando. Asegúrese también de que no hay ningún cable roto.

Problemas de seguridad del teléfono IP de Cisco

En las secciones siguientes se proporciona información para resolver problemas de las funciones de seguridad del teléfono IP de Cisco. Para obtener información sobre las soluciones de estos problemas o para obtener instrucciones adicionales para resolver problemas de seguridad, consulte la *Guía de seguridad de Cisco Unified Communications Manager*.

Problemas con el archivo CTL

En las secciones siguientes se describe cómo solucionar problemas relacionados con el archivo CTL.

Error de autenticación, el teléfono no puede autenticar el archivo CTL

Problema

Se produce un error de autenticación del dispositivo.

Motivo

El archivo CTL no tiene un certificado de Cisco Unified Communications Manager o el certificado es incorrecto.

Solución

Instale un certificado correcto.

El teléfono no puede autenticar el archivo CTL

Problema

El teléfono no puede autenticar el archivo CTL.

Motivo

El token de seguridad que firmó el archivo CTL actualizado no existe en el archivo CTL del teléfono.

Solución

Cambie el token de seguridad en el archivo CTL e instale el archivo nuevo en el teléfono.

El archivo CTL se autentica, pero otros archivos de configuración no

Problema

El teléfono no puede autenticar ningún archivo de configuración distinto al archivo CTL.

Motivo

Hay un registro TFTP erróneo o puede que el archivo de configuración no esté firmado por el certificado correspondiente de la lista de confianza del teléfono.

Solución

Compruebe el registro TFTP y el certificado en la lista de confianza.

El archivo ITL se autentica, pero otros archivos de configuración no

Problema

El teléfono no puede autenticar ningún archivo de configuración distinto al archivo ITL.

Motivo

Puede que el archivo de configuración no esté firmado por el certificado correspondiente de la lista de confianza del teléfono.

Solución

Vuelva a firmar el archivo de configuración con el certificado correcto.

Error de autorización de TFTP

Problema

El teléfono informa de un error de autorización de TFTP.

Motivo

La dirección TFTP del teléfono no existe en el archivo CTL.

Si ha creado un archivo CTL nuevo con un registro de TFTP nuevo, el archivo CTL existente en el teléfono podría no incluir un registro para el nuevo servidor TFTP.

Solución

Compruebe la configuración de la dirección TFTP en el archivo CTL del teléfono.

El teléfono no se registra

Problema

El teléfono no se registra en Cisco Unified Communications Manager.

Motivo

El archivo CTL no contiene la información correcta del servidor de Cisco Unified Communications Manager.

Solución

Cambie la información del servidor de Cisco Unified Communications Manager en el archivo CTL.

No se solicitan los archivos de configuración firmados

Problema

El teléfono no solicita archivos de configuración firmados.

Motivo

El archivo CTL no contiene ninguna entrada TFTP con certificados.

Solución

Configure las entradas TFTP con certificados en el archivo CTL.

Problemas de sonido

En las secciones siguientes se describe cómo resolver problemas de sonido.

No hay ruta de voz

Problema

Una o varias personas de una llamada no oyen el audio.

Solución

Cuando al menos una persona en la llamada no recibe señal de audio, no se habrá establecido conectividad IP entre los teléfonos. Compruebe la configuración de los routers y los switches para asegurarse de que la conectividad IP esté configurada correctamente.

Voz entrecortada

Problema

Un usuario se queja de que escucha la voz entrecortada en una llamada.

Motivo

Puede haber un error de coincidencia en la configuración de fluctuación.

Solución

Compruebe las estadísticas AvgJtr y MaxJtr. Si estos valores son muy diferentes, podría haber un problema con la fluctuación en la red o se podrían producir tasas elevadas periódicas de actividad de la red.

Un teléfono en modo de conexión en cadena no funciona

Problema

En el modo de conexión en cadena, uno de los teléfonos de conferencia no funciona.

Solución

Compruebe que si los cables conectados al adaptador inteligente sean los correctos. Los dos cables más gruesos conectan los teléfonos con el adaptador inteligente. El cable más delgado conecta el adaptador inteligente al adaptador de alimentación.

Temas relacionados

Modo de conexión en cadena, en la página 31
Instalación del teléfono para conferencias en modo de conexión en cadena, en la página 38

Problemas generales de las llamadas telefónicas

Las secciones siguientes sirven de ayuda para solucionar problemas generales de las llamadas telefónicas.

No se puede establecer la llamada telefónica

Problema

Un usuario se queja de que no puede efectuar una llamada.

Motivo

El teléfono no dispone de una dirección IP DHCP y no puede registrarse en Cisco Unified Communications Manager. En los teléfonos con pantalla LCD, se muestra el mensaje `Configurando IP` o `Registrando`. En los teléfonos sin pantalla LCD, se reproduce el tono de reordenar (en lugar del tono de marcación) en el auricular cuando el usuario intenta efectuar una llamada.

Solución

1. Compruebe lo siguiente:
    1. Que el cable Ethernet esté conectado.
    2. Que el servicio Cisco CallManager se está ejecutando en el servidor de Cisco Unified Communications Manager.
    3. Que ambos teléfonos están registrados en la misma instancia de Cisco Unified Communications Manager.
2. La depuración del servidor de audio y los registros de captura deben estar activados en ambos teléfonos. Si fuera necesario, active la depuración de Java.

El teléfono no reconoce los dígitos DTMF o los dígitos se retrasan

Problema

El usuario se queja de que faltan números o que se retrasan cuando se usa el teclado.

Motivo

Si se presionan las teclas demasiado rápido, pueden perderse o retrasarse dígitos.

Solución

Las teclas no se deben presionar demasiado rápido.

Procedimientos para solucionar problemas

Estos procedimientos se pueden usar para identificar y corregir problemas.

Crear un informe de problemas de teléfono desde Cisco Unified Communications Manager

Puede generar un informe de problemas para los teléfonos desde Cisco Unified Communications Manager. Esta acción produce la misma información que genera la tecla programable de la herramienta de informe de problemas (PRT) en el teléfono.

El informe de problemas contiene información sobre el teléfono y los auriculares.

Procedimiento

Paso 1 En Cisco Unified CM Administration, seleccione **Dispositivo** > **Teléfono**.

Paso 2 Haga clic en **Buscar** y seleccione uno o más teléfonos IP de Cisco.

Paso 3 Haga clic en **Generar PRT para seleccionados** para recopilar registros de PRT para los auriculares utilizados en los teléfonos IP de Cisco seleccionados.

Comprobación de la configuración de TFTP

Procedimiento

Paso 1 Compruebe el campo Servidor TFTP 1.

Si ha asignado una dirección IP estática al teléfono, debe introducir manualmente un valor para la opción Servidor TFTP 1.

Si usa DHCP, el teléfono obtiene la dirección para el servidor TFTP del servidor DHCP. Compruebe que la dirección IP está configurada en DHCP opción 150.

Paso 2 También puede permitir que el teléfono use un servidor TFTP alternativo. Esa configuración es particularmente útil si el teléfono se ha trasladado de forma reciente de una ubicación a otra.

Paso 3 Si el protocolo DHCP local no ofrece la dirección TFTP correcta, permita que el teléfono use un servidor TFTP alternativo.

Esto suele ser necesario en los casos de las VPN.

Determinación de los problemas de DNS o de conectividad

Procedimiento

Paso 1 Use el menú Restablecer configuración para restablecer los ajustes predeterminados del teléfono.

Paso 2 Modifique los ajustes de DHCP e IP:

a) Desactive DHCP.
b) Asigne al teléfono los valores de IP estática. Use la misma configuración de router predeterminado que se emplee en otros teléfonos que funcionen.
c) Asigne un servidor TFTP. Use el mismo servidor TFTP que se emplee en otros teléfonos que funcionen.

Paso 3 En el servidor de Cisco Unified Communications Manager, compruebe que los archivos de host local tienen el nombre de servidor de Cisco Unified Communications Manager correcto asignado a las direcciones IP correctas.

Paso 4 En Cisco Unified Communications Manager, seleccione **Sistema** > **Servidor** y verifique que la referencia al servidor se realiza mediante la dirección IP y no con el nombre DNS.

Paso 5 El Cisco Unified Communications Manager, seleccione **Dispositivo** > **Teléfono**. Haga clic en **Buscar** para buscar este teléfono. Verifique que ha asignado la dirección MAC correcta a este teléfono IP de Cisco.

Paso 6 Apague y encienda el teléfono.

Temas relacionados

Determinación de la dirección MAC del teléfono, en la página 60
Reinicio o restablecimiento del teléfono para conferencias, en la página 175

Comprobación de la configuración de DHCP

Procedimiento

Paso 1 En el teléfono, presione **Configuración**.

Paso 2 Seleccione **Config. admin.** > **Configuración de Ethernet** > **Configuración de IPv4**.

Paso 3 Compruebe el campo del servidor DHCP.

Si ha asignado una dirección IP estática al teléfono, no necesita introducir un valor para la opción Servidor DHCP. Sin embargo, si usa un servidor DHCP, esta opción debe tener un valor. Si no se encuentra ningún valor, compruebe el enrutamiento IP y la configuración de VLAN. Consulte el documento *Solución de problemas del puerto de switch y la interfaz*, que encontrará en esta URL:

https://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html

Paso 4 Compruebe los campos Dirección IP, Máscara de subred y Router predeterminado.

Si asigna una dirección IP estática al teléfono, debe introducir manualmente la configuración de estas opciones.

Paso 5 Si utiliza DHCP, compruebe las direcciones IP que distribuye su servidor DHCP.

Consulte el documento *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks* (Conceptos y solución de problemas de DHCP en un switch Catalyst o en redes empresariales), que encontrará en esta URL:

https://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml

Creación de un archivo de configuración del teléfono

Cuando se elimina un teléfono de la base de datos de Cisco Unified Communications Manager, el archivo de configuración se borra del servidor TFTP de ese sistema. Los números de directorio del teléfono permanecen en la base de datos de Cisco Unified Communications Manager. Se denominan "números de directorio sin asignar" y se pueden usar para otros dispositivos. Si estos números sin asignar no se usan en otros dispositivos, puede eliminarlos de la base de datos de Cisco Unified Communications Manager. Puede usar el Informe de plan de enrutamiento para ver y eliminar números de referencia sin asignar. Para obtener más datos, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Si cambia los botones de una plantilla de botones de teléfono o asigna una plantilla de este tipo distinta a un teléfono, podría darse el caso de que el teléfono ya no pueda acceder a los números de directorio. Los números de directorio siguen asignados al teléfono en la base de datos de Cisco Unified Communications Manager, pero el teléfono no tienen ningún botón con el que se puedan contestar las llamadas. Estos números de directorio se deben borrar del teléfono y eliminarse, si fuera necesario.

Procedimiento

Paso 1 En Cisco Unified Communications Manager, Seleccione **Dispositivo** > **Teléfono** y haga clic en **Buscar** para localizar el teléfono con problemas.

Paso 2 Seleccione **Eliminar** para borrar el teléfono de la base de datos de Cisco Unified Communications Manager.

Nota Cuando se elimina un teléfono de la base de datos de Cisco Unified Communications Manager, el archivo de configuración se borra del servidor TFTP de ese sistema. Los números de directorio del teléfono permanecen en la base de datos de Cisco Unified Communications Manager. Se denominan "números de directorio sin asignar" y se pueden usar para otros dispositivos. Si estos números sin asignar no se usan en otros dispositivos, puede eliminarlos de la base de datos de Cisco Unified Communications Manager. Puede usar el Informe de plan de enrutamiento para ver y eliminar números de referencia sin asignar.

Paso 3 Vuelva a agregar el teléfono a la base de datos de Cisco Unified Communications Manager.

Paso 4 Apague y encienda el teléfono.

Temas relacionados

Métodos de adición de teléfonos, en la página 60
Cisco Unified Communications Manager Documentación, en la página 14

Verificación de la configuración de DNS

Procedimiento

Paso 1 En el teléfono, presione **Configuración**.

Paso 2 Seleccione **Config. admin** > **Configuración de Ethernet** > **Configuración de IPv4**.

Paso 3 Compruebe que el campo Servidor DNS 1 esté configurado correctamente.

Paso 4 También debe verificar que se ha realizado una entrada CNAME en el servidor DNS para el servidor TFTP y para el sistema Cisco Unified Communications Manager.

También debe asegurarse de que DNS se ha configurado para efectuar búsquedas inversas.

Inicio del servicio

Para que se pueda iniciar o detener, el servicio debe estar activado.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Cisco Unified Serviceability** en la lista desplegable Navegación y haga clic en **Ir**.

Paso 2 Seleccione **Herramientas** > **Centro control: página web de servicio de función**.

Paso 3 Seleccione el servidor de Cisco Unified Communications Manager principal en la lista desplegable Servidor.

La ventana muestra los nombres de los servicios del servidor que ha elegido, el estado de esos y un panel de control para iniciar o detener el servicio.

Paso 4 Si un servicio se ha detenido, seleccione el botón de opción correspondiente y haga clic en **Iniciar**.

El símbolo Estado del servicio cambia de un cuadrado a una flecha.

Control de la información de depuración desde Cisco Unified Communications Manager

Si experimenta problemas en el teléfono que no puede resolver, el servicio de asistencia técnica de Cisco puede ayudarle. Deberá activar la depuración para el teléfono, reproducir el problema, desactivar la depuración y enviar los registros al servicio de asistencia técnica para su análisis.

Dado que en la depuración se recopila información detallada, el tráfico de comunicación puede ralentizar el teléfono, haciendo que responda peor. Después de recopilar los registros, debe desactivar la depuración para asegurar el funcionamiento del teléfono.

La información de depuración puede incluir un código de un dígito que indica la gravedad de la situación. La clasificación es la siguiente:

- 0 - Emergencia
- 1 - Alerta
- 2 - Crítico
- 3 - Error
- 4 - Advertencia
- 5 - Notificación
- 6 - Información
- 7 - Depuración

Póngase en contacto con el servicio de asistencia técnica de Cisco para obtener más información y asistencia.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione una de las ventanas siguientes:

- **Dispositivo** > **Configuración del dispositivo** > **Perfil de teléfono común**
- **Sistema** > **Configuración de teléfono empresarial**
- **Dispositivo** > **Teléfono**

Paso 2 Establezca los parámetros siguientes:

- Valores de Perfil de registro: Preajuste (predeterminado), Predeterminado, Telefonía, SIP, UI, Red, Medios, Actualizar, Accesorio, Seguridad, Wi-Fi, VPN, EnergyWise, MobileRemoteAccess.
- Valores de Registro remoto: Desactivar (predeterminado), Activar.
- Servidor de registro de IPv6 o Servidor de registro - Dirección IP (dirección IPv4 o IPv6).

Nota Si no se puede acceder al servidor de registro, el teléfono deja de enviar mensajes de depuración.

- El formato de las direcciones del servidor de registro de IPv4 es `dirección:<port>@@base=<0-7>;pfs=<0-1>`

- El formato de las direcciones del servidor de registro de IPv6 es `[dirección]:<port>@@base=<0-7>;pfs=<0-1>`
- Donde:
  - La dirección IPv4 está separada por puntos (.).
  - La dirección IPv6 está separada por dos puntos (:).

Información adicional sobre solución de problemas

Si tiene más preguntas sobre la solución de problemas del teléfono, diríjase al siguiente sitio web de Cisco y busque el modelo de teléfono correspondiente:

https://www.cisco.com/cisco/web/psa/troubleshoot.html

CAPÍTULO 13

Mantenimiento

Reinicio o restablecimiento del teléfono para conferencias

Realice una restauración básica de un teléfono para recuperarlo si ha tenido un error. También puede restaurar la configuración y los ajustes de seguridad a los valores predeterminados de fábrica.

Reinicio del teléfono para conferencias

Al reiniciar el teléfono, se perderán los cambios de configuración de usuarios y de red que no están confirmados en la memoria flash en el teléfono.

Procedimiento

Presione **Configuración** > **Configuración de administración** > **Restablecer configuración** > **Restablecer dispositivo**.

Temas relacionados

Introducción de texto y opciones de menú desde el teléfono, en la página 41

Restablecimiento de la configuración de teléfono para conferencias en el menú del teléfono

Procedimiento

Paso 1 Presione **Configuración**.

Paso 2 Elija **Configuración de administración** > **Restablecer configuración**.

Paso 3 Seleccione el tipo de restablecimiento.

- **Todo**: restaura los valores de fábrica.
- **Restablecer dispositivo**: restablece el dispositivo. No cambia la configuración existente.
- **Red**: restablece la configuración de red a la configuración predeterminada.
- **Modo de servicio**: borra el modo de servicio actual, desactiva la VPN y reinicia el teléfono.
- **Seguridad**: restablece la configuración de seguridad a la configuración predeterminada. Esta opción elimina el archivo CTL.

Paso 4 Presione **Restablecer** o **Cancelar**.

Temas relacionados

Introducción de texto y opciones de menú desde el teléfono, en la página 41

Restablecimiento de los valores predeterminados de fábrica del teléfono para conferencias desde el teclado

Al restablecer el teléfono desde el teclado, el teléfono revierte a la configuración de fábrica.

Procedimiento

Paso 1 Desenchufe el teléfono:

- Si usa PoE, desenchufe el cable LAN.
- Si usa el adaptador de alimentación, desenchúfelo.

Paso 2 Espere 5 segundos.

Paso 3 Presione y mantenga presionada la tecla **#**, y vuelva a enchufar el teléfono.

Paso 4 Cuando el teléfono se inicia, se ilumina la cinta de LED. En cuanto se encienda la franja LED, pulse **123456789*0#** en secuencia.

Cuando haya presionado estos botones, el teléfono pasará por el proceso de restablecimiento de los valores de fábrica.

Si presiona los botones en una secuencia errónea, el teléfono se encenderá normalmente.

Precaución No apague el teléfono hasta que se complete el proceso de restablecimiento de los valores de fábrica y se muestre la ventana principal.

Temas relacionados

Introducción de texto y opciones de menú desde el teléfono, en la página 41

Supervisión de la calidad de voz

Para medir la calidad de voz de las llamadas que se envían o se reciben en la red, los Cisco IP Phone usan estas mediciones estadísticas basadas en eventos de encubrimiento. DSP reproduce marcos para enmascarar la pérdida de marcos en el flujo de paquetes de voz.

- Mediciones de proporción de encubrimiento: muestran la proporción de marcos de encubrimiento sobre el total de marcos de voz. La proporción de encubrimiento del intervalo se calcula cada tres segundos.
- Mediciones de segundos de encubrimiento: muestran el número de segundos en los que DSP reproduce marcos de encubrimiento debido a marcos perdidos. Un «segundo de encubrimiento» profundo es un segundo en el que DSP reproduce más del cinco por ciento de marcos de encubrimiento.

Nota La proporción de encubrimiento y los segundos de encubrimiento son mediciones primarias basadas en la pérdida de marcos. Una proporción de encubrimiento de cero indica que la red IP proporciona marcos y paquetes a tiempo y sin pérdida.

Puede acceder a las mediciones de calidad de voz desde el teléfono IP de Cisco mediante la pantalla Estadísticas de llamadas, o bien de forma remota mediante Estadísticas de flujo.

Consejos para solucionar problemas relacionados con la calidad de voz

Cuando observe cambios significativos y persistentes en las mediciones, use la tabla siguiente para obtener información general para solucionar problemas.

Tabla 31: Cambios en las mediciones de calidad de voz

Cambio de medición	Condición
La proporción de encubrimiento y los segundos de encubrimiento aumentan de forma significativa.	Problemas de red por pérdida de paquetes o fluctuación alta.
La proporción de encubrimiento es cero o casi cero, pero la calidad de la voz es pobre.	• Ruido o distorsión en el canal de audio, como eco o niveles de audio. • Llamadas tándem que sufren varias codificaciones y decodificaciones, como llamadas a una red móvil o a una red de tarjeta de llamadas. • Problemas acústicos provenientes de un altavoz, un teléfono móvil con manos libres o unos auriculares inalámbricos. Compruebe los contadores de transmisión de paquetes (TxCnt) y recepción de paquetes (RxCnt) para comprobar que los paquetes de voz fluyen.
Las puntuaciones de MOS LQK se reducen de forma significativa.	Problemas de red por pérdida de paquetes o niveles de fluctuación altos: • Las reducciones de MOS LQK promedio pueden indicar un problema extendido y uniforme. • Las reducciones MOS LQK individuales pueden indicar problemas por ráfagas. Compruebe al mismo tiempo la proporción de encubrimiento y los segundos de encubrimiento para detectar pruebas de pérdida de paquetes y fluctuación.

Cambio de medición	Condición
Las puntuaciones de MOS LQK aumentan de forma significativa.	• Compruebe si el teléfono usa un códec distinto al esperado (RxType y TxType). • Compruebe si la versión de MOS LQK ha cambiado tras una actualización del firmware.

Nota Las mediciones de calidad de voz no tienen en cuenta el ruido ni la distorsión, solo la pérdida de marcos.

Limpieza del teléfono IP de Cisco

Para limpiar el teléfono IP de Cisco y su pantalla, utilice únicamente un paño suave y seco. No aplique productos de limpieza en forma líquida o en polvo directamente sobre el teléfono. Como ocurre con todos los dispositivos electrónicos no resistentes a las condiciones atmosféricas, los productos en forma líquida o en polvo pueden dañar los componentes y provocar fallos.

Cuando el teléfono está en modo suspendido, la pantalla está en blanco y el botón Seleccionar no está iluminado. Cuando el teléfono se encuentra en este estado, puede limpiar la pantalla, siempre que sepa que el teléfono permanecerá en reposo hasta que termine de limpiarlo.

CAPÍTULO 14

Asistencia para usuarios internacionales

Instalador de configuración regional de terminales de Unified Communications Manager

De forma predeterminada, en los teléfonos IP de Cisco se usa la configuración regional en inglés (Estados Unidos). Para usar los teléfonos IP de Cisco en otras configuraciones regionales, debe instalar la versión específica del instalador de configuración regional de terminales de Unified Communications Manager en cada servidor de Cisco Unified Communications Manager del clúster. El instalador de configuración regional instala la última versión traducida del texto para la interfaz del usuario del teléfono y tonos de teléfono específicos para el país en el sistema a fin de que estén disponibles en los teléfonos IP de Cisco.

Para acceder al instalador de configuración regional necesario para una versión, visite la página de Descarga de software, diríjase al modelo de teléfono y seleccione el enlace correspondiente del instalador de configuración regional de terminales de Unified Communications Manager.

Para obtener más datos, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Nota Puede que el instalador más reciente no esté disponible de inmediato. Siga comprobando la página web para encontrar actualizaciones.

Temas relacionados

Cisco Unified Communications Manager Documentación, en la página 14

Asistencia para el registro de llamadas internacionales

Si su sistema telefónico está configurado para registrar las llamadas internacionales (normalización de la persona que llama), los registros de llamadas, las rellamadas o las entradas del directorio de llamadas podrían

mostrar el signo más (+) para representar el prefijo internacional para su ubicación. Según la configuración de su sistema telefónico, el signo más (+) podría sustituirse por el código de marcación internacional correcto, o puede ser necesario editar el número antes de marcarlo para sustituir manualmente el signo + con el prefijo internacional para su ubicación. Asimismo, aunque el registro de llamada o la entrada de directorio muestren el número internacional completo de la llamada recibida, en la pantalla del teléfono podría mostrarse solo la versión local abreviada del número, sin códigos internacionales ni de país.

Limitación de idioma

No se proporciona soporte localizado para la entrada de texto alfanumérico de teclado (KATE) para las configuraciones regionales de Asia siguientes:

- Chino (China)
- Chino (Hong Kong)
- Chino (Taiwán)
- Japonés (Japón)
- Coreano (República de Corea)

Se presenta al usuario el valor predeterminado de KATE Inglés (Estados Unidos).

Por ejemplo, la pantalla del teléfono mostrará texto en coreano, pero la tecla **2** del teclado mostrará **a b c 2 A B C**.