



Guía de administración de los teléfonos IP serie 8800 de Cisco para Cisco Unified Communications Manager

Primera publicación: 2015-07-13

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.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2015–2023 Cisco Systems, Inc. Todos los derechos reservados.



CONTENIDO

PREFACIO:

Prólogo	xiii
Descripción general	xiii
Público	xiii
Convenciones de la guía	xiii
Documentación relacionada	xv
Teléfono Cisco IP Phone serie 8800 Documentación	xv
Cisco Unified Communications Manager Documentación	xv
Cisco Business Edition 6000 Documentación	xv
Documentación, asistencia e instrucciones de seguridad	xv
Información general sobre la seguridad de productos de Cisco	xv

CAPÍTULO 1

Información nueva y modificada	1
Información nueva y modificada para la versión de firmware 14.2(1)	1
Información nueva y modificada para la versión de firmware 14.1(1)	2
Información nueva y modificada para la versión de firmware 14.0(1)	2
Información nueva y modificada para la versión de firmware 12.8(1)	3
Información nueva y modificada para la versión de firmware 12.7(1)	3
Información nueva y modificada para la versión de firmware 12.6(1)	4
Nueva información de la versión de firmware 12.5(1)SR3	4
Nueva información de la versión de firmware 12.5(1)SR1	5
Nueva información de la versión 12.1(1)SR1 del firmware	5
Nueva información de la versión 12.1(1) del firmware	6
Nueva información de la versión 12.0(1) del firmware	6
Nueva información de la versión 11.7(1) del firmware	7
Nueva información de la versión 11.5(1)SR1 del firmware	7
Nueva información de la versión 11.5(1) del firmware	8

Nueva información de la versión 11.0 del firmware 8

PARTE I: **Acerca del teléfono IP de Cisco 11**

CAPÍTULO 2 **Datos técnicos 13**

- Especificaciones físicas y ambientales de funcionamiento 13
- Especificaciones de cables 14
 - Asignación de patillas de los puertos de red y del equipo 14
 - Conector del puerto de red 14
 - Conector del puerto PC 15
- Requisitos de alimentación del teléfono 16
 - Interrupción del suministro eléctrico 17
 - Reducción del consumo eléctrico 17
 - Negociación de energía por LLDP 17
- Protocolos de red 18
- Interacción con la VLAN 22
- Interacción con Cisco Unified Communications Manager Edition 22
- Interacción con Cisco Unified Communications Manager Express 23
- Interacción con el sistema de mensajería de voz 24
- Descripción general del inicio del teléfono 24
- Dispositivos externos 26
- Información del puerto USB 26
- Archivos de configuración del teléfono 27
- Comportamiento del teléfono durante horas de congestión de red 27
- Comportamiento del teléfono en una red con dos routers de red 28
- Interfaz de programación de aplicaciones 28

CAPÍTULO 3 **Hardware del teléfono IP de Cisco 29**

- Descripción general del teléfono 29
- Teléfono IP 8811 de Cisco 31
 - 8811 de Cisco 31
- Teléfonos IP 8841 y 8845 de Cisco 32
 - Conexiones del teléfono 33
- Teléfonos IP 8851 y 8851NR de Cisco 33

IP 8851 de Cisco	34
Teléfonos IP 8861, 8865 y 8865NR de Cisco	35
Conexiones del teléfono	35
Botones y hardware	36
Teclas programables, botones de línea y de función	38
Proteger la cámara de vídeo del teléfono	39

PARTE II: **Instalación del teléfono IP de Cisco** **41**

CAPÍTULO 4 **Instalación del teléfono IP de Cisco** **43**

Verificación de la configuración de red	43
Incorporación de código de activación para los teléfonos internos	44
Incorporación de código de activación y Mobile and Remote Access	45
Activación del registro automático para los teléfonos	45
Instalación del teléfono IP de Cisco	47
Uso compartido de la conexión de red con el teléfono y el equipo	49
Configuración del teléfono en los menús	49
Aplicación de una contraseña al teléfono	50
Introducción de texto y opciones de menú desde el teléfono	50
Activar la LAN inalámbrica en el teléfono	51
Configuración de la LAN inalámbrica en Cisco Unified Communications Manager	52
Configuración de la LAN inalámbrica en el teléfono	53
Establecer el número de intentos de autenticación de WLAN	54
Habilitar el modo de mensaje de WLAN	55
Configuración de un perfil Wi-Fi mediante Cisco Unified Communications Manager	55
Configuración de un grupo Wi-Fi mediante Cisco Unified Communications Manager	58
Configuración de los ajustes de red	58
Campos de configuración de Ethernet	58
Campos de IPv4	60
Campos de IPv6	62
Configuración del teléfono para usar DHCP	64
Configuración del teléfono para no usar DHCP	64
Servidor de carga	65
Verificación del inicio del teléfono	65

Configuración de los servicios de telefonía para los usuarios 65
 Cambiar el modelo de teléfono de un usuario 66

CAPÍTULO 5

Configuración del teléfono para Cisco Unified Communications Manager 69

Configuración del teléfono IP de Cisco 69
 Determinación de la dirección MAC del teléfono 72
 Métodos de adición de teléfonos 73
 Adición de teléfonos individualmente 73
 Adición de teléfonos con una plantilla de teléfono de BAT 73
 Adición de usuarios a Cisco Unified Communications Manager 74
 Adición de usuarios desde un directorio LDAP externo 75
 Adición de un usuario directamente a Cisco Unified Communications Manager 75
 Adición de un usuario a un grupo de usuarios finales 76
 Asociación de teléfonos con usuarios 76
 Survivable Remote Site Telephony 77
 Telefonía de sitio remoto superviviente mejorada 80
 Reglas de marcación de la aplicación 80
 Configuración de las reglas de marcación de la aplicación 80

CAPÍTULO 6

Administración del portal de autoayuda 83

Descripción general del portal de autoayuda 83
 Configuración del acceso de usuario al portal de autoayuda 83
 Personalización de la presentación del portal de autoayuda 84

PARTE III:

Administración del teléfono IP de Cisco 85

CAPÍTULO 7

Seguridad del teléfono IP de Cisco 87

Mejoras de seguridad para la red del teléfono 87
 Características de seguridad admitidas 88
 Configuración de un certificado significativo local 93
 Activación del modo FIPS 94
 Seguridad de las llamadas telefónicas 95
 Identificación de llamadas de conferencia seguras 95
 Identificación de llamadas telefónicas seguras 96

Cifrado para la intrusión	97
Seguridad de WLAN	97
Configuración del modo de autenticación	100
Credenciales de seguridad inalámbrica	101
Configuración del nombre de usuario y la contraseña	101
Configuración de la clave precompartida	102
Cifrado inalámbrico	102
Exportación del certificado de CA desde ACS mediante Microsoft Certificate Services	103
Configuración PEAP	108
Seguridad de la LAN inalámbrica	109
Página de administración del teléfono IP de Cisco	109
Configuración SCEP	112
Autenticación 802.1X	113
Acceso a la autenticación 802.1X	114
Establecimiento del campo Autent. dispositivo	115

CAPÍTULO 8
Personalización del teléfono IP de Cisco 117

Personalización de timbres del teléfono	117
Imágenes de fondo personalizadas	117
Configuración del códec de banda ancha	119
Configuración de la pantalla de inactividad	120
Personalizar el tono de marcado	121

CAPÍTULO 9
Características y configuración del teléfono 123

Descripción general de las características y la configuración del teléfono	123
Asistencia para usuarios del teléfono IP de Cisco	124
Funciones del teléfono	124
Botones de función y teclas programadas	142
Configuración de funciones del teléfono	144
Configuración de las funciones del teléfono para todos los teléfonos	145
Configuración de las funciones del teléfono para un grupo de teléfonos	145
Configuración de las funciones del teléfono para un solo teléfono	146
Configuración específica del producto	146
Prácticas recomendadas de la configuración de las funciones	168

Entornos de volumen elevado de llamadas	169
Entornos de varias líneas	169
Entorno del modo de línea de sesión	169
Campo: utilizar siempre la línea principal	170
Desactivar los cifrados de seguridad de la capa de transporte	170
Activación del historial de llamadas para la línea compartida	171
Programación de la función de ahorro de energía para el teléfono IP de Cisco	171
Programación de EnergyWise en el teléfono IP de Cisco	173
Configuración de la función No molestar	176
Activación del saludo de agente	177
Configuración de las funciones de supervisión y grabación	178
Configuración de la notificación de desvío de llamadas	178
Activación de BLF para listas de llamadas	179
Configuración de Ethernet de eficacia energética para el puerto PC y de switch	180
Configuración del intervalo de puertos RTP/sRTP	181
Mobile and Remote Access mediante Expressway	182
Ejemplos de implementación	183
Rutas de medios y establecimiento interactivo de conectividad	184
Características del teléfono disponibles para Mobile and Remote Access mediante Expressway	184
Configuración de credenciales de usuario persistentes para el inicio de sesión de Expressway	186
Generación de un código QR para el inicio de sesión de MRA	186
Herramienta de informe de problemas	187
Configuración de una URL de carga del servicio de atención al cliente	187
Establecimiento de la etiqueta para una línea	189
Configuración de la información de banco doble	189
Supervisión de aparcamiento	189
Configuración de los temporizadores de supervisión de aparcamiento	190
Establecimiento de los parámetros de supervisión de aparcamiento para los números de directorio	191
Configuración de la supervisión de aparcamiento para las listas de grupos de salto	192
Configuración del intervalo de puertos de audio y vídeo	192
Configurar Cisco IP Manager Assistant	194
Configuración de Visual Voicemail	196
Configuración de Visual Voicemail para un usuario específico	197

Configuración de Visual Voicemail para un grupo de usuarios	197
Servicios garantizados SIP	197
Migración del teléfono a un teléfono multiplataforma directamente	198
Precedencia multinivel y preferencia	199
Configuración de la plantilla de teclas programadas	199
Plantillas de botones de teléfono	201
Modificación de plantillas de botones de teléfono	201
Asignación de la plantilla de botones del teléfono para todas las llamadas	202
Configuración de la libreta personal de direcciones o la marcación rápida como servicio del teléfono IP	202
Modificación de la plantilla de botones del teléfono para la libreta personal de direcciones o la marcación rápida	203
Configuración de VPN	204
Configuración de teclas de línea adicionales	205
Funciones disponibles en el modo de línea mejorado	206
Configuración del temporizador de reanudación de TLS	209
Activación de Intelligent Proximity	209
Configuración de la resolución de transmisión del vídeo	210
Administración de los auriculares en versiones anteriores de Cisco Unified Communications Manager	211
Descarga del archivo de configuración predeterminada de los auriculares	212
Modificación del archivo de configuración predeterminada de los auriculares	212
Instalación del archivo de configuración predeterminada en Cisco Unified Communications Manager	215
Reinicio del servidor Cisco TFTP	215

CAPÍTULO 10
Directorio corporativo y personal 217

Configuración del directorio corporativo	217
Configuración del directorio personal	217
Configuración de las entradas del directorio personal del usuario	218
Descarga del sincronizador de la libreta de direcciones de Cisco IP Phone	219
Implementación del sincronizador de la libreta de direcciones del teléfono IP de Cisco	219
Instalación del sincronizador	219
Configuración del sincronizador	220

PARTE IV: **Solución de problemas del teléfono IP de Cisco** 221

CAPÍTULO 11 **Sistemas de supervisión del teléfono** 223

- Estado del teléfono IP de Cisco 223
 - Apertura de la ventana Información del teléfono 223
 - Campos de Información del teléfono 224
 - Apertura del menú Estado 224
 - Apertura de la ventana Mensajes de estado 225
 - Mostrar pantalla de información de red 229
 - Apertura de la pantalla Estadísticas de red 230
 - Visualización de la pantalla Estadísticas inalámbricas 233
 - Apertura de la ventana Estadísticas de llamadas 235
 - Apertura de la ventana Punto de acceso actual 237
- Página web del teléfono IP de Cisco 239
 - Acceso a la página web del teléfono 239
 - Información del dispositivo 240
 - Configuración de la red 243
 - Estadísticas de red 248
 - Registros de dispositivos 251
 - Estadísticas de flujo 252
 - Solicitud de información del teléfono en XML 256
 - Ejemplo de resultado del comando CallInfo 257
 - Ejemplo de resultado del comando LineInfo 257
 - Ejemplo de resultado del comando ModeInfo 258

CAPÍTULO 12 **Solución de problemas** 259

- Información sobre la solución de problemas generales 259
- Problemas de inicio 260
 - No se desarrolla el proceso normal de inicio en el teléfono IP de Cisco 261
 - El teléfono IP de Cisco no se registra en Cisco Unified Communications Manager 262
 - Se muestran mensajes de error en el teléfono 262
 - El teléfono no se conecta con el servidor TFTP o con Cisco Unified Communications Manager 262

El teléfono no se conecta con el servidor TFTP	262
El teléfono no se conecta con el servidor	263
El teléfono no se conecta mediante la DNS	263
Cisco Unified Communications Manager y los servicios TFTP no se ejecutan	263
El archivo de configuración está dañado	263
Registro del teléfono en Cisco Unified Communications Manager	264
El teléfono IP de Cisco no puede obtener la dirección IP	264
Teléfono no registrado	264
Problemas de restablecimiento del teléfono	265
El teléfono se restablece por cortes intermitentes de la red	265
El teléfono se restablece por errores de configuración de DHCP	265
El teléfono se restablece por una dirección IP estática incorrecta	265
El teléfono se restablece durante un uso intensivo de la red	266
El teléfono se restablece de forma intencionada	266
El teléfono se restablece por problemas con la DNS u otros problemas de conectividad	266
El teléfono no recibe alimentación	266
El teléfono no se conecta con la LAN	267
Problemas de seguridad del teléfono IP de Cisco	267
Problemas con el archivo CTL	267
Error de autenticación, el teléfono no puede autenticar el archivo CTL	267
El teléfono no puede autenticar el archivo CTL	267
El archivo CTL se autentica, pero otros archivos de configuración no	268
El archivo ITL se autentica, pero otros archivos de configuración no	268
Error de autorización de TFTP	268
El teléfono no se registra	269
No se solicitan los archivos de configuración firmados	269
Problemas de llamadas de vídeo	269
Sin vídeo entre dos teléfonos de vídeo IP de Cisco	269
Interrupciones de vídeo o fotogramas	269
No se puede transferir una llamada de vídeo	270
Sin vídeo durante una llamada de conferencia	270
Problemas generales de las llamadas telefónicas	270
No se puede establecer la llamada telefónica	270
El teléfono no reconoce los dígitos DTMF o los dígitos se retrasan	271

Procedimientos para solucionar problemas	271
Crear un informe de problemas de teléfono desde Cisco Unified Communications Manager	271
Crear un registro de consola desde el teléfono	272
Comprobación de la configuración de TFTP	272
Determinación de los problemas de DNS o de conectividad	273
Comprobación de la configuración de DHCP	273
Creación de un archivo de configuración del teléfono	274
Identificación de problemas de autenticación 802.1X	275
Verificación de la configuración de DNS	275
Inicio del servicio	275
Control de la información de depuración desde Cisco Unified Communications Manager	276
Información adicional sobre solución de problemas	277

CAPÍTULO 13 **Mantenimiento** 279

Restauración básica	279
Restablecimiento de los valores de fábrica del teléfono desde el teclado del teléfono	280
Restablecimiento de toda la configuración desde el menú del teléfono	280
Reinicio del teléfono desde la imagen de copia de seguridad	281
Restablecimiento de la configuración de red	281
Restablecimiento de la configuración de red del usuario	281
Eliminación del archivo CTL	281
Herramienta de informes de calidad	282
Supervisión de la calidad de voz	282
Consejos para solucionar problemas relacionados con la calidad de voz	283
Limpieza del teléfono IP de Cisco	283

CAPÍTULO 14 **Asistencia para usuarios internacionales** 285

Instalador de configuración regional de terminales de Unified Communications Manager	285
Asistencia para el registro de llamadas internacionales	285
Limitación de idioma	286



Prólogo

- [Descripción general, en la página xiii](#)
- [Público, en la página xiii](#)
- [Convenciones de la guía, en la página xiii](#)
- [Documentación relacionada, en la página xv](#)
- [Documentación, asistencia e instrucciones de seguridad, en la página xv](#)

Descripción general

La *Guía de administración de los teléfonos IP serie 8800 de Cisco para Cisco Unified Communications Manager* proporciona la información que necesita para comprender, instalar, configurar, administrar y solucionar problemas de los teléfonos en una red de VoIP.

Dada la complejidad de una red de telefonía IP, en esta guía no se proporciona información completa ni detallada sobre los procedimientos que debe realizar en Cisco Unified Communications Manager ni en otros dispositivos de la red.

Público

Esta guía está dirigida a ingenieros de red, administradores del sistema e ingenieros de telecomunicaciones. En ella pueden aprender los pasos necesarios para configurar los teléfonos IP de Cisco. Las tareas descritas en este documento implican la configuración de ajustes de red que no van dirigidos a los usuarios del teléfono. Las tareas de este manual requieren que el usuario esté familiarizado con Cisco Unified Communications Manager.

Convenciones de la guía

En este documento se utilizan las siguientes convenciones:

Convenciones	Descripción
fuentes en negrita	Los comandos y las palabras clave aparecen en negrita .
fuentes en <i>cursiva</i>	Los argumentos para los que tiene que aportar valores aparecen en <i>cursiva</i> .

Convenciones	Descripción
[]	Los elementos entre corchetes son elementos optativos.
{x y z}	Las palabras clave alternativas se agrupan entre llaves y se separan mediante barras verticales.
[x y z]	Las palabras clave alternativas opcionales se agrupan entre corchetes y se separan mediante barras verticales.
Cadena	Conjunto de caracteres sin comillas. No coloque una cadena entre comillas; si lo hace, la cadena incluirá esas comillas.
Fuente de <code>pantalla</code>	Las sesiones del terminal y la información que muestra el sistema aparecen en la fuente de <code>pantalla</code> .
Fuente de entrada	La información que debe introducir aparece en la fuente de entrada .
Fuente de <i>pantalla en cursiva</i>	Los argumentos para los que tiene que aportar valores aparecen en la fuente de <i>pantalla en cursiva</i> .
^	El símbolo ^ representa la tecla Control; por ejemplo, la combinación de teclas ^D en la pantalla significa que debe mantener pulsada la tecla Control mientras pulsa la tecla D.
<>	Los caracteres que el usuario debe personalizar, como las contraseñas, aparecen entre paréntesis angulares.



Nota Indica *información que el lector debe tener en cuenta*. Las notas contienen sugerencias de gran ayuda o referencias a material que no se encuentra en el documento.



Precaución Indica que *el lector debe tener precaución*. En esta situación, es posible que realice alguna acción que provoque daños en el equipo o la pérdida de información.

En las advertencias se utilizan las siguientes convenciones:



Atención INSTRUCCIONES IMPORTANTES DE SEGURIDAD

Este símbolo de advertencia significa peligro. Puede sufrir lesiones físicas. Antes de manipular cualquier equipo, debe ser consciente de los peligros que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. Utilice el número de indicación que aparece al final de cada advertencia para localizar su traducción en las advertencias de seguridad que acompañan a este dispositivo. Indicación 1071

GUARDE ESTAS INSTRUCCIONES

Documentación relacionada

Use las secciones siguientes para obtener información relacionada.

Teléfono Cisco IP Phone serie 8800 Documentación

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.

La Guía de implementación se encuentra en la siguiente URL:

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

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 Business Edition 6000 Documentación

Consulte la *Cisco Business Edition 6000 Guía de la documentación* y otras publicaciones específicas de su versión de Cisco Business Edition 6000. Diríjase a la siguiente URL:

<https://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000/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/policiesandregulations/ear/index.htm>.



CAPÍTULO 1

Información nueva y modificada

- Información nueva y modificada para la versión de firmware 14.2(1), en la página 1
- Información nueva y modificada para la versión de firmware 14.1(1), en la página 2
- Información nueva y modificada para la versión de firmware 14.0(1), en la página 2
- Información nueva y modificada para la versión de firmware 12.8(1), en la página 3
- Información nueva y modificada para la versión de firmware 12.7(1), en la página 3
- Información nueva y modificada para la versión de firmware 12.6(1), en la página 4
- Nueva información de la versión de firmware 12.5(1)SR3, en la página 4
- Nueva información de la versión de firmware 12.5(1)SR1, en la página 5
- Nueva información de la versión 12.1(1)SR1 del firmware, en la página 5
- Nueva información de la versión 12.1(1) del firmware, en la página 6
- Nueva información de la versión 12.0(1) del firmware, en la página 6
- Nueva información de la versión 11.7(1) del firmware, en la página 7
- Nueva información de la versión 11.5(1)SR1 del firmware, en la página 7
- Nueva información de la versión 11.5(1) del firmware, en la página 8
- Nueva información de la versión 11.0 del firmware, en la página 8

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 87
Inicio de sesión de Extension Mobility simplificado con el adaptador USB de los auriculares de Cisco 730	Funciones del teléfono, en la página 124
Sincronización de silencio Bluetooth para los auriculares de Cisco de la serie 700	Funciones del teléfono, en la página 124

Función	Novedades o cambios
Nueva configuración de los auriculares de Cisco de la serie 550: Evento de base y modo Siempre encendido	Funciones del teléfono, en la página 124

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 87
Alerta de llamada mejorada para el grupo de búsqueda	Funciones del teléfono, en la página 124
Visualización del número de llamada configurable para el modo de línea mejorado	Configuración específica del producto
PLAR retrasado configurable	Funciones del teléfono, en la página 124
Compatibilidad con MRA para el inicio de sesión de Extension Mobility con auriculares de Cisco	Funciones del teléfono, en la página 124
Migración de teléfono sin carga de transición	Migración del teléfono a un teléfono multiplataforma directamente, en la página 198

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 146
Mejoras en OAuth de SIP	Mejoras de seguridad para la red del teléfono, en la página 87
Mejoras de la interfaz de usuario	Survivable Remote Site Telephony, en la página 77 Funciones del teléfono, en la página 124
Mejoras en OAuth para MRA	Mobile and Remote Access mediante Expressway, en la página 182

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 66
Mejora de la actualización de los auriculares	Información del dispositivo , en la página 240
Simplificación del inicio de sesión de Extension Mobility con auriculares de Cisco	Funciones del teléfono , en la página 124
Cambios de control de funciones	Configuración específica del producto , en la página 146 , nuevos campos Alerta para bajar la voz y Marcar llamada como spam
Cambios generales	Clarificar la conexión Wi-Fi y el puerto PC: <ul style="list-style-type: none"> • Configuración del teléfono en los menús, en la página 49 • Activar la LAN inalámbrica en el teléfono, en la página 51
Agregar información adicional sobre el campo de acceso web	Configuración específica del producto , en la página 146
Eliminación de funciones no compatibles	Funciones del teléfono , en la página 124

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

Tabla 2: Revisiones de la Guía de administración de los teléfonos IP serie 8800 de Cisco para la versión 12.7(1) del firmware.

Revisión	Sección actualizada
Se ha actualizado para la compatibilidad con el fondo de pantalla de Cisco en módulos de expansión de teclas.	Imágenes de fondo personalizadas , en la página 117

Revisión	Sección actualizada
Se ha actualizado para la compatibilidad con Auriculares Cisco 730	Información del dispositivo, en la página 240
Actualizado para Auriculares Cisco serie 500 la versión de firmware 2.0	Información del dispositivo, en la página 240 Administración de los auriculares en versiones anteriores de Cisco Unified Communications Manager, en la página 211
Actualizada para las llamadas entrantes del grupo de salto.	Funciones del teléfono, en la página 124
Se ha eliminado la información de configuración del conmutador electrónico.	Configuración específica del producto, en la página 146

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

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 3: Revisiones de la Guía de administración de los teléfonos IP serie 8800 de Cisco para la versión 11.0 del firmware.

Revisión	Sección actualizada
Actualización para revertir a la línea principal en modo de línea de sesión.	Configuración específica del producto, en la página 146 Entorno del modo de línea de sesión, en la página 169

Nueva información de 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 4: Revisiones de la Guía de administración del teléfono IP 8800 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 45
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 271

Revisión	Sección actualizada
Nuevo tema	Uso compartido de la conexión de red con el teléfono y el equipo, en la página 49
Nuevo tema	Proteger la cámara de vídeo del teléfono, en la página 39

Nueva información de la versión de firmware 12.5(1)SR1

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 5: Revisiones de la Guía de administración del teléfono IP 8800 de Cisco para la versión de firmware 12.5(1)SR1

Revisión	Sección actualizada
Compatibilidad con curva elíptica	Características de seguridad admitidas, en la página 88
Compatibilidad con las mejoras de historial de llamadas para el modo de línea mejorado con líneas de sustitución incremental	Funciones disponibles en el modo de línea mejorado, en la página 206
Compatibilidad con la mensajería silenciosa en Cisco Unified Communications Manager Express	Interacción con Cisco Unified Communications Manager Express, en la página 23
Compatibilidad con el idioma chino	Limitación de idioma, en la página 286
Compatibilidad para incorporación del código de activación	Incorporación de código de activación para los teléfonos internos, en la página 44
Compatibilidad con rutas de medios y el establecimiento interactivo de conectividad	Rutas de medios y establecimiento interactivo de conectividad, en la página 184
Compatibilidad para desactivar los cifrados TLS	Configuración específica del producto, en la página 146
Compatibilidad con la desactivación del auricular para que la ruta de audio se pueda mantener en los auriculares	Configuración específica del producto, en la página 146
Compatibilidad con la configuración remota de los parámetros de auriculares	Administración de los auriculares en versiones anteriores de Cisco Unified Communications Manager, en la página 211

Nueva información de la versión 12.1(1)SR1 del firmware

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 6: Revisiones de la Guía de administración del teléfono IP 8800 de Cisco para la versión 12.1(1)SR1 del firmware

Revisión	Sección actualizada
Marcación Enbloc para la mejora del temporizador entre dígitos T.302.	Configuración específica del producto, en la página 146

Nueva información de la versión 12.1(1) del firmware

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 7: Revisiones de la Guía de administración del teléfono IP 8800 de Cisco para la versión 12.1(1) del firmware

Revisión	Sección actualizada
Mobile and Remote Access mediante Expressway ahora admite el modo de línea mejorado.	Características del teléfono disponibles para Mobile and Remote Access mediante Expressway, en la página 184
	Mobile and Remote Access mediante Expressway, en la página 182
	Funciones disponibles en el modo de línea mejorado, en la página 206
Ahora se admite la activación o la desactivación de TLS 1.2 para el acceso del servidor web.	Configuración específica del producto, en la página 146
Ahora se admite el códec de audio G722.2 AMR-Wb.Xml.	Descripción general del teléfono, en la página 29
	Campos de Estadísticas de llamadas, en la página 235

Nueva información de la versión 12.0(1) del firmware

Todas las nuevas funciones se han agregado a [Funciones del teléfono, en la página 124](#).

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 8: Revisiones de la Guía de administración del teléfono IP 8800 de Cisco para la versión 12.0(1) del firmware

Revisión	Sección actualizada
Actualización para compatibilidad con aparcamiento de llamadas, estado de línea de aparcamiento de llamadas, captura de grupo y grupos de salto en el modo de línea mejorado	Funciones disponibles en el modo de línea mejorado, en la página 206

Nueva información de la versión 11.7(1) del firmware

No se necesitan actualizaciones de la administración para la versión de firmware 11.7(1).

Nueva información de la versión 11.5(1)SR1 del firmware

Todas las nuevas funciones se han agregado a [Funciones del teléfono](#), en la página 124.

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 9: Revisiones de la Guía de administración de los teléfonos IP serie 8800 de Cisco para la versión 11.5(1)SR1 del firmware.

Revisión	Sección actualizada
Actualización para la compatibilidad del teléfono IP 8865NR de Cisco	<ul style="list-style-type: none"> • Requisitos de alimentación del teléfono, en la página 16 • Protocolos de red, en la página 18 • Descripción general del teléfono, en la página 29 • Botones y hardware, en la página 36
Actualizado para la asistencia de grabación y supervisión en el modo de línea mejorado	Funciones disponibles en el modo de línea mejorado , en la página 206
Actualizado para la compatibilidad de la lista de análisis de WLAN.	Activar la LAN inalámbrica en el teléfono , en la página 51
	Configuración de la LAN inalámbrica en el teléfono , en la página 53
	Configuración de los ajustes de red , en la página 58
Actualizado para que No molestar sea compatible con MLPP	Configuración de la función No molestar , en la página 176
Actualizado para la compatibilidad con el timbre configurable	Configuración específica del producto , en la página 146
Seguridad mejorada	Mejoras de seguridad para la red del teléfono , en la página 87
Cambios generales	Se actualizará para Página web del teléfono IP de Cisco , en la página 239
	Nueva presentación de configuración de funciones de teléfono en Cisco Unified Communications Manager Configuración de funciones del teléfono , en la página 144

Nueva información de la versión 11.5(1) del firmware

Tabla 10: Revisiones de la Guía de administración de los teléfonos IP serie 8800 de Cisco para la versión 11.5(1) del firmware.

Revisión	Sección actualizada
Se admite el modo de línea mejorado.	Configuración de teclas de línea adicionales, en la página 205 Funciones disponibles en el modo de línea mejorado, en la página 206
Se actualizó No molestar (DND) para la nueva visualización.	Configuración de la función No molestar, en la página 176
Se admite el códec Opus.	Descripción general del teléfono, en la página 29
Se ha agregado el modo FIPS.	Activación del modo FIPS, en la página 94
Se ha actualizado la configuración de WLAN.	Configuración de la LAN inalámbrica en el teléfono, en la página 53
Se admite el perfil de WLAN para teléfonos IP 8861 y 8865 de Cisco.	Configuración de un perfil Wi-Fi mediante Cisco Unified Communications Manager, en la página 55
	Configuración de un grupo Wi-Fi mediante Cisco Unified Communications Manager, en la página 58
Se admite el conjunto de intentos de autenticación de WLAN.	Establecer el número de intentos de autenticación de WLAN, en la página 54
El modo Activar el modo de mensaje de WLAN es compatible.	Habilitar el modo de mensaje de WLAN, en la página 55
Personalizar el tono de marcación es compatible.	Personalizar el tono de marcado, en la página 121
Mostrar pantalla de información de red es compatible.	Mostrar pantalla de información de red, en la página 229

Nueva información de la versión 11.0 del firmware

Todas las nuevas funciones se han agregado a [Funciones del teléfono, en la página 124](#).

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 11: Revisiones de la Guía de administración de los teléfonos IP serie 8800 de Cisco para la versión 11.0 del firmware.

Revisión	Sección actualizada
Se han actualizado para que sean más claras y solucionar algunos defectos.	<ul style="list-style-type: none"> • Configuración de VPN, en la página 204 • Configuración de los ajustes de red, en la página 58 • Configuración de Ethernet de eficacia energética para el puerto PC y de switch, en la página 180 • Configuración de la resolución de transmisión del vídeo, en la página 210 • Telefonía de sitio remoto superviviente mejorada, en la página 80
Se ha actualizado con información mejorada sobre la opción de depuración del teléfono por secciones.	<ul style="list-style-type: none"> • Control de la información de depuración desde Cisco Unified Communications Manager, en la página 276.
Se han actualizado para mejorar la información sobre la compatibilidad de los certificados digitales EAP-TLS + SCEP, PEAP-GTC y X.509.	<ul style="list-style-type: none"> • Seguridad de WLAN, en la página 97. • Configuración del modo de autenticación, en la página 100 • Credenciales de seguridad inalámbrica, en la página 101
Se han actualizado con información mejorada sobre la Herramienta de informes de problemas (PRT).	<ul style="list-style-type: none"> • Herramienta de informe de problemas, en la página 187. • Configuración de una URL de carga del servicio de atención al cliente, en la página 187.
Se ha añadido información sobre la compatibilidad de la regla de marcación de la aplicación.	<ul style="list-style-type: none"> • Reglas de marcación de la aplicación, en la página 80
Se ha agregado la etiqueta de texto de línea.	<ul style="list-style-type: none"> • Establecimiento de la etiqueta para una línea, en la página 189.



PARTE **I**

Acerca del teléfono IP de Cisco

- [Datos técnicos, en la página 13](#)
- [Hardware del teléfono IP de Cisco, en la página 29](#)



CAPÍTULO 2

Datos técnicos

- Especificaciones físicas y ambientales de funcionamiento, en la página 13
- Especificaciones de cables, en la página 14
- Requisitos de alimentación del teléfono, en la página 16
- Protocolos de red, en la página 18
- Interacción con la VLAN, en la página 22
- Interacción con Cisco Unified Communications Manager Edition, en la página 22
- Interacción con Cisco Unified Communications Manager Express, en la página 23
- Interacción con el sistema de mensajería de voz, en la página 24
- Descripción general del inicio del teléfono, en la página 24
- Dispositivos externos, en la página 26
- Información del puerto USB, en la página 26
- Archivos de configuración del teléfono, en la página 27
- Comportamiento del teléfono durante horas de congestión de red, en la página 27
- Comportamiento del teléfono en una red con dos routers de red, en la página 28
- Interfaz de programación de aplicaciones, en la página 28

Especificaciones físicas y ambientales de funcionamiento

En la tabla siguiente se muestran las especificaciones del entorno físico y operativo para el teléfono IP serie 8800 de Cisco.

Tabla 12: 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	En funcionamiento: del 10 % al 90 % sin condensación En reposo: del 10 % al 95 % sin condensación
Temperatura de almacenamiento	De -10 a 60 °C (de 14 a 140 °F)
Alto	229,1 mm (9,02 pulg.)
Anchura	257,34 mm (10,13 pulg.)

Especificación	Valor o intervalo
Profundidad	40 mm (1,57 pulg.)
Peso	1,19 kg (2,62 libras)
Alimentación	100-240 V CA, 50-60 Hz, 0,5 A (si se usa un adaptador de CA) 48 V CC, 0,2 A (si se usa la alimentación interna por un cable de red)
Cables	Categoría 3/5/5e/6 para cables de 10 Mb/s con 4 pares Categoría 5/5e/6 para cables de 100 Mb/s con 4 pares Categoría 5e/6 para cables de 1000 Mb/s con 4 pares Nota Los cables tienen 4 pares de hilos que suman un total de 8 conductores
Requisitos de distancia	Según se indique en la especificación de Ethernet, se presupone que la longitud del cable entre cada teléfono IP de Cisco y el switch es de 100 metros (330 pies)

Especificaciones de cables

A continuación se describen las especificaciones de los cables:

- Clavija RJ-9 (4 conductores) para la conexión del auricular de mano y los auriculares
- Clavija RJ-45 para la conexión LAN 10/100/1000BaseT (puerto de red 10/100/1000 del teléfono)
- Clavija RJ-45 para una segunda conexión 10/100/1000BaseT (puerto de ordenador 10/100/1000 del teléfono)
- Clavija de 3,5 mm para la conexión del altavoz (solo teléfono IP 8861 de Cisco)
- Conector de alimentación de 48 voltios
- Puertos USB/conector: un puerto USB para el teléfono IP 8851 de Cisco y dos puertos USB para el teléfono IP 8861 de Cisco
- Tres conectores de módulos de expansión clave que se consideran como conector USB del teléfono IP 8851 y 8861 de Cisco

Asignación de patillas de los puertos de red y del equipo

Aunque para la conectividad de red se usan tanto el puerto de red como el de ordenador (acceso), ambos tienen distintas funciones y presentan patillas de los puertos distintas.

- El puerto de red es el puerto 10/100/1000 SW del teléfono IP de Cisco.
- El puerto de ordenador (acceso) es el puerto 10/100/1000 PC del teléfono IP de Cisco.

Conector del puerto de red

En la tabla siguiente se describen las patillas del conector del puerto de red.

Tabla 13: Patillas del conector del puerto de red

Número de pines	Función
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-
Nota	BI significa bidireccional. Por su parte, DA, DB, DC y DD significan Datos A, Datos B, Datos C y Datos D, respectivamente.

Conector del puerto PC

En la tabla siguiente se describen las patillas del conector del puerto del ordenador.

Tabla 14: Patillas del conector del puerto del ordenador (acceso)

Número de pines	Función
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-
Nota	BI significa bidireccional. Por su parte, DA, DB, DC y DD significan Datos A, Datos B, Datos C y Datos D, respectivamente.

Requisitos de alimentación del teléfono

El teléfono IP de Cisco puede recibir la energía de una fuente de alimentación externa o través de Ethernet (PoE). La alimentación externa se obtiene de una fuente de alimentación independiente. El switch puede proporcionar PoE a través del cable Ethernet.

Los teléfonos IP 8861 y 8865 de Cisco son dispositivos PoE de clase 4 y necesitan un conmutador o una tarjeta de línea con funciones de clase 4 para admitir las funciones adicionales.

Para obtener más información sobre los requisitos de alimentación del teléfono, consulte la hoja de datos del teléfono.

Si va a instalar un teléfono que reciba alimentación externa, conecte la fuente de alimentación antes de conectar el cable Ethernet al teléfono. Si va a retirar un teléfono que reciba alimentación externa, desconecte el cable Ethernet del teléfono antes de desconectar la fuente de alimentación.

Tabla 15: Directrices para alimentar el teléfono IP de Cisco

Tipo de alimentación	Instrucciones
Alimentación externa: proporcionada por la fuente de alimentación externa CP-PWR-CUBE-4.	El teléfono IP de Cisco usa la fuente de alimentación CP-PWR-CUBE-4.
Alimentación PoE: se proporciona mediante un switch a través del cable Ethernet conectado al teléfono.	Los teléfonos IP 8851, 8851NR, 8861, 8865 y 8865NR de Cisco admiten 802.3at PoE por uso de accesorios. Para obtener más información, consulte la hoja de datos del teléfono. El conmutador necesita una fuente de alimentación de respaldo para un funcionamiento ininterrumpido del teléfono. Asegúrese de que la versión de CatOS o IOS que se ejecuta en el switch admite la implementación prevista del teléfono. Consulte en la documentación del switch los datos de la versión de software operativo.
Alimentación universal a través de Ethernet (UPoE)	El teléfono IP 8865 y 8865NR de Cisco es compatible con UPoE.

Los documentos de esta tabla ofrecen más información sobre los temas siguiente:

- Switches de Cisco que funcionan con los teléfonos IP de Cisco
- Versiones del IOS de Cisco que admiten la negociación de energía bidireccional
- Otros requisitos y restricciones sobre la alimentación

Tabla 16: Información adicional

Temas del documento	URL
Soluciones PoE	http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html
UPoE	http://www.cisco.com/c/en/us/solutions/enterprise-networks/upoe

Temas del documento	URL
Switches Cisco Catalyst	http://www.cisco.com/c/en/us/products/switches/index.html
Routers de servicios integrados	http://www.cisco.com/c/en/us/products/routers/index.html
Software de IOS de Cisco	http://www.cisco.com/c/en/us/products/ios-nx-os-software/index.html

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 este modo durante el tiempo programado o hasta que el usuario descuelga el auricular o presiona 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.

Negociación de energía por LLDP

El teléfono y el switch negocian la energía que consume el teléfono. El teléfono IP de Cisco funciona con varios ajustes de alimentación, lo que reduce el consumo de electricidad cuando hay menos energía disponible.

Cuando un teléfono se reinicia, el switch fija un protocolo (CDP o LLDP) para la negociación energética. El switch fija el primer protocolo (que contiene un valor de límite de umbral [TLV] de energía) que el teléfono transmite. Si el administrador del sistema desactiva ese protocolo en el teléfono, este no puede alimentar ningún accesorio porque el switch no responde a las solicitudes de energía en el otro protocolo.

Cisco recomienda que la negociación de energía esté siempre activada (opción predeterminada) cuando se conecte a un switch que admita esta función.

Si la negociación de energía está desactivada, el switch podría desconectar la alimentación del teléfono. Si el switch no admite la negociación de energía, desactive la función antes de alimentar accesorios a través de

PoE. Si la función de negociación de energía está desactivada, el teléfono puede alimentar el número máximo de accesorios que permite el estándar IEEE 802.3af-2003.

**Nota**

- Si CDP y la negociación de energía están desactivadas, el teléfono puede alimentar hasta 15,4 W para los accesorios.

Protocolos de red

Los teléfonos IP serie 8800 de Cisco admiten varios estándares del sector y los protocolos de red de Cisco necesarios para la comunicación de voz. En la tabla siguiente se ofrece una descripción general de los protocolos de red admitidos por los teléfonos.

Tabla 17: Protocolos de red admitidos en los teléfonos IP serie 8800 de Cisco

Protocolo de red	Propósito	Notas de uso
Bluetooth	Bluetooth es un protocolo de red de área personal inalámbrica (WPAN) que especifica la forma que tienen los dispositivos de comunicarse en distancias cortas.	Los teléfonos IP 8845, 8865 y 8851 de Cisco admiten Bluetooth 4.1. El teléfono IP 8861 de Cisco admite Bluetooth 4.0. Los teléfonos IP 8811, 8841, 8851NR y 8865NR de Cisco no admiten Bluetooth.
Protocolo de arranque-asignación (Bootstrap o BootP)	BootP permite a un dispositivo de red, como un teléfono IP de Cisco, descubrir cierta información de inicio, como la dirección IP.	—
Túnel de sesión de audio de Cisco (CAST)	El protocolo CAST permite a los teléfonos y a las aplicaciones asociadas comunicarse con los teléfonos IP remotos sin necesidad de realizar cambios en los componentes de señalización.	El teléfono IP de Cisco usa CAST como interfaz entre Cisco Unified Video Advantage y Cisco Unified Communications Manager utilizando el teléfono como proxy SIP.
Protocolo de descubrimiento de Cisco (CDP)	CDP es un protocolo de descubrimiento de dispositivos que se ejecuta en todos los equipos fabricados por Cisco. Mediante CDP, un dispositivo puede anunciar su existencia a otros dispositivos y recibir información sobre los demás dispositivos de la red.	Los teléfonos IP de Cisco usan CDP para comunicar información como el ID de la VLAN auxiliar, detalles de administración de energía de cada puerto y datos de configuración de calidad de servicio (QoS) con el switch de Cisco Catalyst.
Protocolo de distribución entre pares de Cisco (CPPDP)	CPPDP es un protocolo propiedad de Cisco que se usa para formar una jerarquía par a par de dispositivos. Esta jerarquía se usa para distribuir archivos de firmware desde dispositivos pares a sus dispositivos vecinos.	CPPDP se usa en la función Compartir firmware en el grupo.

Protocolo de red	Propósito	Notas de uso
Protocolo de configuración dinámica de host (DHCP).	<p>DHCP asigna de forma dinámica una dirección IP a los dispositivos de red.</p> <p>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.</p>	<p>DHCP está activado de manera predeterminada. Si está desactivado, debe configurar manualmente la dirección IP, la máscara de subred, la puerta de enlace y el servidor TFTP en cada teléfono de forma local.</p> <p>Se recomienda usar la opción personalizada de DHCP 150. Con este método, se configura la dirección IP del servidor TFTP como un valor de opción. Para obtener más datos, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.</p> <p>Nota Si no puede usar la opción 150, pruebe con la opción de DHCP 66.</p>
Protocolo de transferencia de hipertexto (HTTP)	HTTP es la forma estándar para transferir información y mover documentos por Internet.	Los teléfonos IP de Cisco usan HTTP para los servicios XML y para solucionar problemas.
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 que admiten tanto HTTP como HTTPS tienen dos direcciones URL configuradas. Los teléfonos IP de Cisco que admiten HTTPS seleccionan la URL HTTPS.
IEEE 802.1X	<p>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.</p> <p>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.</p>	<p>El teléfono IP de Cisco implementa el estándar IEEE 802.1X proporcionando compatibilidad para los siguientes métodos de autenticación: EAP-FAST y EAP-TLS.</p> <p>Si la autenticación 802.1X está activada en el teléfono, debe desactivar el puerto PC y la VLAN de voz.</p>
IEEE 802.11n/802.11ac	<p>El estándar IEEE 802.11 especifica la forma en que se produce la comunicación de los dispositivos a través de una red de área local inalámbrica (WLAN).</p> <p>802.11n funciona en las bandas de 2,4 GHz y 5 GHz, mientras que 802.11ac funciona en la banda de 5 GHz.</p>	<p>La interfaz 802.11 es una opción de implementación en casos en los que el cableado Ethernet no esté disponible o no sea deseable</p> <p>Solo los teléfonos IP 8861 y 8865 de Cisco son compatibles con WLAN.</p>

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.	<p>Para comunicarse con el protocolo IP, los dispositivos de red deben tener una dirección IP, una subred y una gateway asignadas.</p> <p>Las direcciones IP, las subredes y las identificaciones de las puertas de enlace se asignan automáticamente si se usa el teléfono IP de Cisco con el protocolo de configuración dinámica de host (DHCP). Si no se usa DHCP, es preciso asignar manualmente estas propiedades a cada teléfono de forma local.</p> <p>Los teléfonos IP de Cisco admiten direcciones IPv6. Para obtener más datos, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.</p>
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 IP de Cisco 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 para los productos de voz.	<p>El teléfono IP de Cisco admite LLDP-MED en el puerto SW para comunicar información como:</p> <ul style="list-style-type: none"> • Configuración de VLAN de voz • Detección de dispositivos • Administración de la energía • Gestión de inventario.
Protocolo de transporte en tiempo real (RTP)	RTP es un protocolo estándar para el transporte en tiempo real de datos, como voz interactivo, a través de redes de datos.	Los teléfonos IP de Cisco usan el protocolo RTP para enviar y recibir tráfico de voz en tiempo real desde otros teléfonos y puertas de enlace.
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, la detección de DTMF y el ruido de confort se suelen configurar de forma global mediante Cisco Unified Communications Manager o una puerta de enlace de medios en funcionamiento. Algunos terminales SIP pueden permitir la configuración de estos parámetros en el propio terminal.

Protocolo de red	Propósito	Notas de uso
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 sirve para dirigir las funciones de señalización y administración de sesiones dentro de una red de telefonía de paquetes. La señalización permite el transporte de información de llamadas dentro de los límites de la red. La administración de sesiones aporta la capacidad de controlar los atributos de una llamada de extremo a extremo. Los teléfonos IP de Cisco admiten el protocolo SIP cuando los teléfonos funcionan en modo solo IPv6, solo IPv4 o IPv4 e IPv6.
Protocolo de control de transmisión (TCP)	TCP es un protocolo de transporte dirigido a la conexión.	Los teléfonos IP de Cisco usan TCP para conectarse a Cisco Unified Communications Manager y para acceder a los servicios XML.
Seguridad de la capa de transporte (TLS)	TLS es un protocolo estándar para asegurar y autenticar las comunicaciones.	Cuando se implementa la seguridad, los teléfonos IP de Cisco usan el protocolo TLS para registrarse de forma segura en Cisco Unified Communications Manager.
Protocolo de transferencia de archivos trivial (TFTP)	TFTP permite transferir archivos por la red. En los teléfonos IP de Cisco, 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 servidor DHCP pueda identificar de forma automática. Si desea que un teléfono use un servidor TFTP distinto al especificado por el servidor DHCP, debe asignar manualmente la dirección IP del servidor TFTP mediante el menú Configuración de red del teléfono. Para obtener más datos, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.
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 señalización SIP de los teléfonos no admite UDP.

Para obtener más información sobre la compatibilidad con LLDP-MED, consulte el documento técnico LLDP-MED and Cisco Discovery Protocol (LLDP-MED y el protocolo de descubrimiento de Cisco):

http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml

Temas relacionados

[Autenticación 802.1X](#), en la página 113

[Configuración de los ajustes de red](#)

[Verificación del inicio del teléfono](#), en la página 65

[Interacción con la VLAN](#), en la página 22

[Interacción con Cisco Unified Communications Manager Edition](#), en la página 22

[Interacción con Cisco Unified Communications Manager Express](#), en la página 23

[Configuración del intervalo de puertos de audio y vídeo](#), en la página 192

Cisco Unified Communications Manager Documentación, en la página xv

Interacción con la VLAN

El teléfono IP de Cisco incluye un switch Ethernet interno que permite el desvío de paquetes al teléfono, así como al puerto del ordenador (acceso) y al puerto de red de la parte trasera del teléfono.

Si hay un ordenador conectado al puerto del ordenador (acceso), tanto el ordenador como el teléfono comparten el mismo enlace físico al switch y el mismo puerto en este. Este enlace físico tiene las siguientes implicaciones para la configuración de la VLAN en la red:

- Las VLAN actuales se podrían configurar según una subred IP. Sin embargo, puede que las direcciones IP adicionales no estén disponibles para asignar el teléfono a la misma subred que otros dispositivos que se conectan al mismo puerto.
- El tráfico de datos presente en los teléfonos compatibles con la VLAN podría reducir la calidad del tráfico de VoIP.
- La seguridad de la red podría indicar que es necesario aislar el tráfico de voz del tráfico de datos de la VLAN.

Puede resolver estos problemas aislando el tráfico de voz en una VLAN separada. El puerto switch al que se conecta el teléfono debe configurarse para VLAN separadas a fin de transportar:

- El tráfico de voz entrante y saliente del teléfono IP (VLAN auxiliar en la serie Cisco Catalyst 6000, por ejemplo)
- El tráfico de datos entrante y saliente del PC que se conecta al switch a través del puerto del ordenador (acceso) del teléfono IP (VLAN nativa)

Al aislar los teléfonos en una VLAN auxiliar independiente, aumenta la calidad del tráfico de voz y es posible agregar un gran número de teléfonos a una red existente que no cuente con suficientes direcciones IP para cada uno de ellos.

Para obtener más datos, consulte la documentación incluida con el switch de Cisco. También puede acceder a información sobre el switch en esta dirección URL:

<http://cisco.com/en/US/products/hw/switches/index.html>

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 xv

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.

En el modo CME se admiten tanto el modo de línea de sesión como el modo de línea mejorada.

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).

Descripción general del inicio del teléfono

Al conectarse con la red de VoIP, los teléfonos IP de Cisco pasan por un proceso de inicio estándar. Según la configuración específica de su red, puede que solo algunos de estos pasos se den en su teléfono.

1. Se obtiene alimentación del switch. Si un teléfono no usa alimentación externa, el switch proporciona energía interna a través del cable Ethernet conectado al teléfono.
2. (Solo para los teléfonos IP 8861 y 8865 de Cisco en una LAN inalámbrica) Se explora en busca de un punto de acceso. Los teléfonos IP 8861 y 8865 de Cisco exploran el área de cobertura de radiofrecuencias con la radio. El teléfono busca perfiles de red y puntos de acceso que contengan un SSID y un tipo de autenticación que coincidan. El teléfono se asocia con el punto de acceso que tenga el RSSI más alto que coincida con el perfil de red.
3. (Solo para los teléfonos IP 8861 y 8865 de Cisco en una LAN inalámbrica) Se autentica con el punto de acceso. El teléfono IP de Cisco inicia el proceso de autenticación. En la tabla siguiente se describe el proceso de autenticación:

Tipo de autenticación	Opciones de administración de claves	Descripción
Abierta	Ninguno	Cualquier dispositivo puede autenticarse en el punto de acceso. Para conseguir más seguridad, se puede usar opcionalmente el cifrado de WEP estática.

Tipo de autenticación	Opciones de administración de claves	Descripción
Clave compartida	Ninguno	El teléfono cifra el texto de desafío mediante la clave WEP y el punto de acceso debe verificar la clave WEP que se usó para cifrar ese texto antes de que el acceso a la red esté disponible.
PEAP o EAP-FAST	Ninguno	El servidor RADIUS autentica el nombre de usuario y la contraseña antes de que el acceso a la red esté disponible.

4. Se carga la imagen del teléfono almacenada. En el inicio, el teléfono ejecuta un cargador de bootstrap que carga una imagen del firmware del teléfono almacenada en la memoria flash. Con esta imagen, el teléfono inicializa el software y el hardware.
5. Se configura la VLAN. Si el teléfono IP de Cisco está conectado a un switch Cisco Catalyst, este informa a continuación al teléfono de la VLAN de voz que hay definida en el switch. El teléfono debe conocer los miembros de la VLAN antes de poder continuar con la solicitud de protocolo de configuración de host dinámico (DHCP) para una dirección IP.
6. Se obtiene una dirección IP. Si el teléfono IP de Cisco usa DHCP para obtener una dirección IP, solicita al servidor DHCP que obtenga una. Si no se usa DHCP en la red, es preciso asignar direcciones IP estáticas a cada teléfono de forma local.
7. Se solicita el archivo CTL. En el servidor TFTP se almacena el archivo CTL. Este archivo contiene los certificados necesarios para establecer una conexión segura entre el teléfono y Cisco Unified Communications Manager.

Para obtener más datos, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.
8. Se solicita el archivo ITL. El teléfono solicita el archivo ITL después de solicitar el archivo CTL. El archivo ITL contiene los certificados de las entidades en las que el teléfono puede confiar. Los certificados se usan para autenticar una conexión segura con los servidores o para autenticar una firma digital firmada por los servidores. El archivo ITL se admite en Cisco Unified Communications Manager 8.5 y versiones posteriores.
9. Se accede a un servidor TFTP. Además de asignar una dirección IP, el servidor DHCP dirige al teléfono IP de Cisco a un servidor TFTP. Si el teléfono tiene una dirección IP definida estáticamente, debe configurar el servidor TFTP de forma local en el teléfono y este se conectará directamente al servidor TFTP.



Nota También puede asignar un servidor TFTP alternativo que se usará en lugar del que asigne DHCP.

10. Se solicita el archivo de configuración. El servidor TFTP tiene archivos de configuración, donde se definen los parámetros para conectarse a Cisco Unified Communications Manager y otros datos del teléfono.
11. Se establece contacto con Cisco Unified Communications Manager. El archivo de configuración define la forma en la que el teléfono IP de Cisco se comunica con Cisco Unified Communications Manager y proporciona a los teléfonos el ID de carga. Después de obtener el archivo del servidor TFTP, el teléfono

intenta establecer una conexión con la instancia de Cisco Unified Communications Manager de mayor prioridad de la lista.

Si el perfil de seguridad del teléfono está configurado para las señales seguras (está cifrado o autenticado) y Cisco Unified Communications Manager está establecido en el modo seguro, el teléfono establece una conexión TLS. En caso contrario, el teléfono establece una conexión TCP no segura.

Si el teléfono se ha agregado manualmente a la base de datos, Cisco Unified Communications Manager lo identifica. Si el teléfono se ha agregado manualmente a la base de datos y el registro automático está activado en Cisco Unified Communications Manager, el teléfono intenta registrarse automáticamente en la base de datos de Cisco Unified Communications Manager.



Nota El registro automático está desactivado si se configura el cliente CTL. En tal caso, debe agregar el teléfono a la base de datos de Cisco Unified Communications Manager manualmente.

Temas relacionados

[Cisco Unified Communications Manager Documentación](#), en la página xv

Dispositivos externos

Es recomendable usar dispositivos externos de buena calidad que cuenten con protección contra interferencias de señales de radiofrecuencia (RF) o audiofrecuencia (AF) no deseadas. Los dispositivos externos pueden ser los auriculares, los cables o los conectores.

Según la calidad de dichos dispositivos y la proximidad a otros, como teléfonos móviles o radios bidireccionales, es probable que se siga produciendo ruido. En tal caso, se aconseja llevar a cabo una o varias de estas acciones:

- Aleje el dispositivo externo de la fuente emisora de señales de radio o audiofrecuencia.
- Aparte los cables del dispositivo externo de la fuente emisora de señales de radio o audiofrecuencia.
- Utilice cables apantallados con el dispositivo externo, o bien cables con conector y blindaje más adecuados.
- Reduzca la longitud del cable del dispositivo externo.
- Aplique ferritas u otros materiales similares a los cables del dispositivo externo.

Cisco no puede garantizar el rendimiento de los conectores, cables y dispositivos externos.



Precaución En países pertenecientes a la Unión Europea, utilice únicamente altavoces, micrófonos o auriculares externos que cumplan con la Directiva EMC [89/336/CE].

Información del puerto USB

Los teléfonos IP 8851, 8851NR, 8861, 8865 y 8865NR de Cisco admiten un máximo de cinco dispositivos conectados a cada puerto USB. Cada dispositivo conectado al teléfono se incluye en el recuento del número máximo de dispositivos admitidos. Por ejemplo, el teléfono admite cinco dispositivos USB en el puerto lateral

y cinco dispositivos USB estándar más en el puerto trasero. Muchos productos USB de terceros cuentan como varios dispositivos USB. Por ejemplo, un dispositivo que contenga un concentrador y auriculares USB puede contar como dos dispositivos USB. Para obtener más información, consulte la documentación de los dispositivos USB.

**Nota**

- Los concentradores sin alimentación no se admiten, ni tampoco los concentradores con más de cuatro puertos.
- No se admiten auriculares USB que se conecten al teléfono mediante un concentrador USB.

Cada módulo de expansión clave que se conecta al teléfono cuenta como un dispositivo USB. Si hay tres módulos de expansión clave conectados al teléfono, cuentan como tres dispositivos USB.

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.

Temas relacionados

[Cisco Unified Communications Manager Documentación](#), en la página xv

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 el vídeo del teléfono 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.

Comportamiento del teléfono en una red con dos routers de red

El teléfono IP serie 8800 de Cisco usa un cortafuegos para ofrecer protección contra intrusos cibernéticos, como ataques de tipo "hombre interpuesto". Este cortafuegos no se puede desactivar. Pero podría detener el tráfico en un teléfono si configura la red con dos routers de red en la misma subred y con redirección de IP.

El cortafuegos del teléfono detiene el tráfico porque esta configuración de red es similar a un ataque de tipo "hombre interpuesto". El teléfono recibe paquetes de redirección para IP de destino distintas en una subred diferente de la del teléfono. El teléfono se encuentra en una red con más de un router, y el router predeterminado envía el tráfico a un segundo router.

Consulte los registros del teléfono si sospecha que el cortafuegos está bloqueando el tráfico. Busque una notificación del código de error 1 proveniente del sistema operativo cuando se intentó establecer una conexión. Una de las firmas es:

```
sip_tcp_create_connection: socket connect failed cpr_errno: 1.
```

Una red con dos routers de red en la misma subred y con redirección de IP no es una configuración habitual. Si usa una red de este tipo, plantéese usar solo un router en una subred. Pero si requiere dos routers de red en la misma subred, desactive el redireccionamiento de IP en el router y reinicie el teléfono.

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.



CAPÍTULO 3

Hardware del teléfono IP de Cisco

- [Descripción general del teléfono, en la página 29](#)
- [Teléfono IP 8811 de Cisco, en la página 31](#)
- [Teléfonos IP 8841 y 8845 de Cisco, en la página 32](#)
- [Teléfonos IP 8851 y 8851NR de Cisco, en la página 33](#)
- [Teléfonos IP 8861, 8865 y 8865NR de Cisco, en la página 35](#)
- [Botones y hardware, en la página 36](#)
- [Proteger la cámara de vídeo del teléfono, en la página 39](#)

Descripción general del teléfono

Los teléfonos IP serie 8800 de Cisco proporcionan comunicación de voz a través de una red IP (protocolo de Internet). Las funciones de los teléfonos IP de Cisco son muy parecidas a las de un teléfono empresarial digital: permiten realizar llamadas telefónicas, así como acceder a funciones como la puesta en silencio o en espera y la transferencia, entre otras. Además, dado que el teléfono se conecta a la red de datos, ofrece funciones avanzadas de telefonía IP, como el acceso a la información y los servicios de red o a funciones y servicios personalizables.

La pantalla LCD del teléfono IP de Cisco 8811 es en blanco y negro. La pantalla LCD de los teléfonos IP de Cisco 8841, 8845, 8851, 8851NR, 8861, 8865 y 8865NR es en color de 24 bits.

Al agregar funciones a las teclas de línea telefónica, habrá una limitación en el número de teclas de línea disponibles. No podrá agregar más funciones que el número de teclas de línea del teléfono.

Los teléfonos IP de Cisco incluyen las siguientes características:

- Botones de función programable que admiten hasta 5 líneas en el modo de línea de sesión o un máximo de 10 líneas con el modo de línea mejorado
- Capacidad completa de vídeo (solo en los teléfonos IP de Cisco 8845, 8865 y 8865NR).
- Conectividad Ethernet Gigabit.
- Compatibilidad con Bluetooth para auriculares inalámbricos (solo teléfonos IP 8845, 8851, 8861 y 8865 de Cisco). Esta función no se admite en los teléfonos IP 8811, 8841, 8851NR y 8865NR de Cisco).
- Compatibilidad con un micrófono y altavoces externos (solo en los teléfonos IP 8861, 8865 y 8865NR de Cisco).

- Conectividad de red por Wi-Fi (solo en los teléfonos IP 8861 y 8865 de Cisco). No se admite Wi-Fi en el teléfono IP 8865NR de Cisco.
- Puertos USB:
 - Un puerto USB en los teléfonos IP 8851 y 8851NR de Cisco.
 - Dos puertos USB en los teléfonos IP 8861, 8865 y 8865NR de Cisco.

Los teléfonos IP 8845, 8865 y 8865NR de Cisco admiten la función de llamadas de vídeo con la cámara integrada. Use esta función para colaborar con amigos y compañeros de trabajo o para mantener reuniones cara a cara a través del teléfono.



Nota Debe guardar la caja y el embalaje de los teléfonos IP 8845, 8865 y 8865NR de Cisco. Las cámaras de estos teléfonos son frágiles. Si mueve el teléfono, le recomendamos que lo coloque en la caja original para proteger la cámara. Para obtener más información, consulte [Proteger la cámara de vídeo del teléfono, en la página 39](#).

Las videollamadas incluyen las siguientes características:

- Imagen en imagen (PiP): seleccione una de las 4 posiciones: abajo a la derecha, arriba a la derecha, arriba a la izquierda y abajo a la izquierda. También puede desactivar la función PiP.
- Cambiar: permite intercambiar las vistas de la imagen PiP. La tecla programable Cambiar está deshabilitada si la función PIP está desactivada.
- Vídeo de vista propia: seleccione esta opción para ver su imagen tal y como aparece en el vídeo.
- Interfaz del usuario de vídeo e inicio de conferencia/transferencia: seleccione estas opciones para iniciar una conferencia.

Para obtener información adicional sobre las videollamadas, consulte la *Guía del usuario de los teléfonos IP serie 8800 de Cisco para Cisco Unified Communications Manager* y la documentación de su versión concreta de Cisco Unified Communications Manager.

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
- iSAC

**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.

Temas relacionados

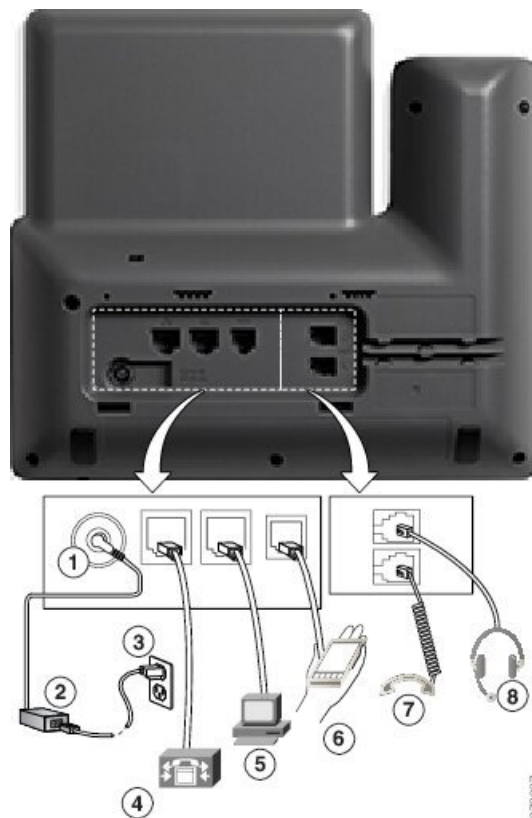
[Cisco Unified Communications Manager Documentación](#), en la página xv

Teléfono IP 8811 de Cisco

En la sección siguiente se describen los atributos de Teléfono IP 8811 de Cisco.

8811 de Cisco

Conecte el teléfono a la red de telefonía IP de su organización como se muestra en el siguiente diagrama.



1	Puerto del adaptador de CC (CC 48 V).	5	Conexión del puerto de acceso (10/100/1000 PC).
2	Fuente de alimentación CA-CC (opcional).	6	Puerto auxiliar.
3	Enchufe mural de CA (opcional).	7	Conexión del auricular.
4	Conexión del puerto de red (10/100/1000 SW). Suministro IEEE 802.3at habilitado.	8	Conexión de auriculares analógicos (opcional).



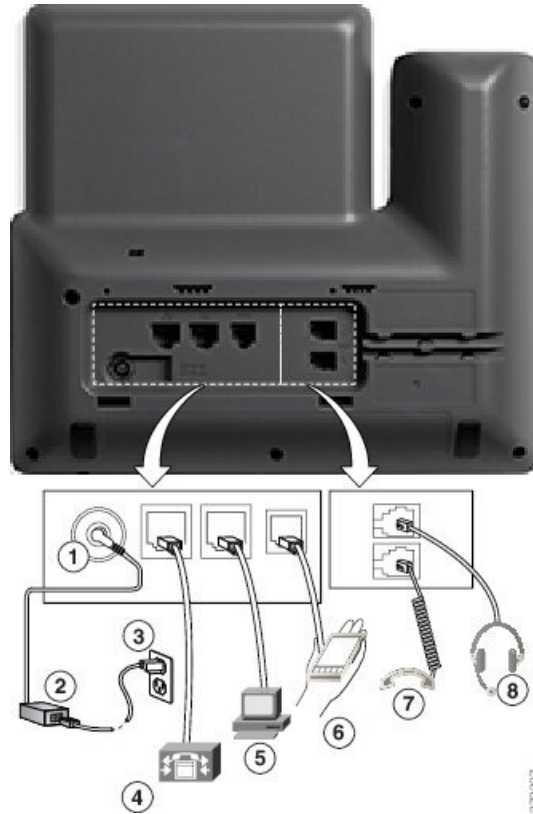
Nota El Teléfono IP 8811 de Cisco no admite un módulo de expansión clave.

Teléfonos IP 8841 y 8845 de Cisco

En la sección siguiente se describen los atributos de los teléfonos IP 8841 y 8845 de Cisco.

Conexiones del teléfono

Conecte el teléfono a la red de telefonía IP corporativa mediante el siguiente diagrama.



1	Puerto del adaptador de CC (48 V de CC).	5	Conexión del puerto de acceso (10/100/1000 PC).
2	Fuente de alimentación CA-CC (opcional).	6	Puerto auxiliar.
3	Enchufe mural de CA (opcional).	7	Conexión del auricular.
4	Conexión del puerto de red (10/100/1000 SW). Suministro IEEE 802.3at habilitado.	8	Conexión de auriculares analógicos (opcional).



Nota Los teléfonos IP 8841 y 8845 de Cisco no admiten un módulo de expansión clave.

Teléfonos IP 8851 y 8851NR de Cisco

En la sección siguiente se describen los atributos de los teléfonos IP 8851 y 8851NR de Cisco.



Nota El teléfono IP 8851NR de Cisco no admite Bluetooth. Aparte de eso, los teléfonos IP 8851 y 8851NR de Cisco admiten las mismas funciones.

IP 8851 de Cisco

Conecte el teléfono a la red de telefonía IP de la empresa como se muestra en el siguiente diagrama.



1	Puerto del adaptador de CC (48 V de CC).	6	Puerto auxiliar.
2	Fuente de alimentación CA-CC (opcional).	7	Conexión del auricular.
3	Enchufe mural de CA (opcional).	8	Conexión de auriculares analógicos (opcional).
4	Conexión del puerto de red (10/100/1000 SW). Suministro IEEE 802.3at habilitado.	9	Puerto USB.
5	Conexión del puerto de acceso (10/100/1000 PC).		



Nota Cada puerto USB admite la conexión de hasta cinco dispositivos compatibles y no compatibles. Cada dispositivo conectado al teléfono se incluye en el recuento del número máximo de dispositivos admitidos. Por ejemplo, el teléfono admite cinco dispositivos USB (por ejemplo: dos módulos de expansión clave, unos auriculares, un concentrador y otro dispositivo USB estándar) en el puerto lateral. Muchos productos USB de terceros cuentan como varios dispositivos USB. Por ejemplo, un dispositivo que contenga un concentrador y auriculares USB puede contar como dos dispositivos USB. Para obtener más información, consulte la documentación de los dispositivos USB.

Teléfonos IP 8861, 8865 y 8865NR de Cisco

En la sección siguiente se describen los atributos de los teléfonos IP 8861, 8865 y 8865NR de Cisco.

Conexiones del teléfono

Conecte el teléfono a la red de telefonía IP de la empresa como se muestra en el siguiente diagrama.



1	Puerto del adaptador de CC (48 V de CC).	7	Conexión del auricular.
---	--	---	-------------------------

2	Fuente de alimentación CA-CC (opcional).	8	Conexión de auriculares analógicos (opcional).
3	Enchufe mural de CA (opcional).	9	Puerto USB.
4	Conexión del puerto de red (10/100/1000 SW). Suministro IEEE 802.3at habilitado.	10	Puertos de E/S de audio.
5	Conexión del puerto de acceso (10/100/1000 PC).	11	Puerto USB.
6	Puerto auxiliar.		



Nota Cada puerto USB admite la conexión de hasta cinco dispositivos compatibles y no compatibles. Cada dispositivo conectado al teléfono se incluye en el recuento del número máximo de dispositivos admitidos. Por ejemplo, el teléfono admite cinco dispositivos USB (por ejemplo: tres módulos de expansión clave, un concentrador y otro dispositivo USB estándar) en el puerto lateral y cinco dispositivos USB estándar adicionales en el puerto trasero. Muchos productos USB de terceros cuentan como varios dispositivos USB. Por ejemplo, un dispositivo que contenga un concentrador y auriculares USB puede contar como dos dispositivos USB. Para obtener más información, consulte la documentación de los dispositivos USB.

Botones y hardware

Hay dos tipos de hardware distintos para el teléfono IP de la serie 8800 de Cisco:

- Los teléfonos IP 8811, 8841, 8851, 8851NR y 8861 de Cisco no tienen cámara.
- Los teléfonos IP 8845, 8865 y 8865NR de Cisco tienen una cámara incorporada.



En las ilustraciones siguientes se muestra el teléfono IP 8845 de Cisco.

Figura 1: Botones y hardware del teléfono IP 8845 de Cisco



La tabla siguiente describe los botones del teléfono IP serie 8800 de Cisco.

Tabla 18: Botones del teléfono IP serie 8800 de Cisco

1	Auricular de mano y franja de luces del auricular	Indica la existencia de una llamada entrante (luz roja intermitente) o de un nuevo mensaje de voz (luz roja fija).
2	Cámara Solo teléfonos IP 8845, 8865 y 8865NR de Cisco	Puede usar la cámara para las videollamadas.
3	Botones de funciones programables y botones de línea	<p> Acceder a las líneas de teléfono, funciones y sesiones de llamada.</p> <p>Al agregar funciones a las teclas de línea telefónica, habrá una limitación en el número de teclas de línea disponibles. No podrá agregar más funciones que el número de teclas de línea del teléfono.</p> <p>Para obtener más información, consulte la sección Teclas programables, botones de línea y de función en el capítulo "Hardware del teléfono IP de Cisco".</p>
4	Botones de teclas programadas	<p> Acceder a las funciones y servicios.</p> <p>Para obtener más información, consulte la sección Teclas programables, botones de línea y de función en el capítulo "Hardware del teléfono IP de Cisco".</p>

5	Atrás , grupo de navegación y Liberar	<p>Atrás  permite volver al menú o pantalla anteriores.</p> <p>Grupo de navegación  Anillo de navegación y botón Seleccionar: desplácese a través de los menús, resalte los elementos y seleccione el elemento resaltado.</p> <p>Liberar  finaliza una llamada conectada o una sesión.</p>
6	Espera/Reanudar , Conferencia y Transferir	<p>Espera/Reanudar  coloca una llamada activa en espera o reanuda la llamada en espera.</p> <p>Conferencia  crea una llamada de conferencia.</p> <p>Transferir  permite transferir una llamada.</p>
7	Altavoz , Silencio y Auriculares	<p>Altavoz  permite encender y apagar el altavoz. Cuando el altavoz está activado, el botón está encendido.</p> <p>Silencio  enciende o apaga el micrófono. Cuando el micrófono está silenciado, el botón está encendido.</p> <p>Auriculares  Encienda los auriculares. Cuando los auriculares están activados, el botón está encendido. Para salir del modo de auriculares, descuelgue el auricular o seleccione el Altavoz .</p>
8	Contactos , Aplicaciones y Mensajes	<p>Contactos  permite acceder a los directorios personales y corporativos.</p> <p>Aplicaciones  se usa para acceder a las llamadas recientes, las preferencias de usuario, la configuración del teléfono y la información del modelo de teléfono.</p> <p>Mensajes  permite llamar al sistema de mensajes de voz.</p>
9	Botón Volumen	<p> Permite ajustar el volumen del auricular y el teléfono con altavoz (descolgado), además del volumen del timbre (colgado).</p>







Teclas programables, botones de línea y de función

Es posible interactuar de varias formas con las funciones del teléfono:

- Las teclas programables, que se encuentran debajo de la pantalla, le proporcionan acceso a la función que se muestra en la pantalla encima de la tecla programable. Las teclas programables varían según lo que esté haciendo. La tecla **Más...** indica que hay más funciones disponibles.
- Los botones de función y de línea, situados a los lados de la pantalla, ofrecen acceso a funciones del teléfono y a las líneas.
 - Botones de función: se usan para funciones como **Marcación rápida** o **Captura de llamadas**, y para ver su estado en otra línea.

- Botones de línea: se usan para contestar una llamada o recuperar una llamada en espera. Si no se usan para una llamada activa, se pueden emplear para iniciar funciones del teléfono, como la presentación de las llamadas perdidas.

Los botones de función y de línea se iluminan para indicar el estado.

Color y estado del LED	Modo de línea normal: botones de línea	Modo de línea normal: botones de función Modo de línea mejorado
 verde, LED fijo	Llamada activa o llamada de intercomunicación bidireccional, llamada en espera, privacidad en uso.	Llamada activa o llamada de intercomunicación bidireccional, privacidad en uso.
 verde, LED intermitente	No corresponde	llamada en espera.
 ámbar, LED fijo	Llamada entrante, reversión de llamada, llamada de intercomunicación unidireccional, iniciada sesión en un grupo de salto	Llamada de intercomunicación unidireccional, iniciada sesión en un grupo de salto
 ámbar, LED intermitente	No corresponde	Llamada entrante o revertida
 rojo, LED fijo	Línea remota en uso, línea remota en espera, No molestar activa	Línea remota en uso, No molestar activa
 rojo, LED intermitente	No corresponde	línea remota en espera.

El administrador puede configurar algunas funciones como teclas programables o como botones de función. También puede acceder a algunas funciones mediante teclas programables o con el botón físico asociado.

Proteger la cámara de vídeo del teléfono

La cámara del teléfono de vídeo es frágil y podría romperse durante el transporte del teléfono.

Antes de empezar

Necesitará uno de los siguientes:

- Caja original del teléfono y material de embalaje
- Material de embalaje, como espuma o plástico de burbujas

Procedimiento

Paso 1

Si tiene la caja original:

- Sítie la espuma en la cámara de forma que la lente esté bien protegida.

b) Inserte el teléfono en su caja original.

Paso 2

Si no tiene la caja, envuelva cuidadosamente el teléfono con espuma o plástico de burbujas para proteger la cámara. Asegúrese de que la espuma protege y rodea la cámara para que nada pueda presionar contra la cámara desde cualquier dirección y para evitar que la cámara pueda dañarse durante el transporte.



PARTE **II**

Instalación del teléfono IP de Cisco

- [Instalación del teléfono IP de Cisco, en la página 43](#)
- [Configuración del teléfono para Cisco Unified Communications Manager, en la página 69](#)
- [Administración del portal de autoayuda, en la página 83](#)



CAPÍTULO 4

Instalación del teléfono IP de Cisco

- Verificación de la configuración de red, en la página 43
- Incorporación de código de activación para los teléfonos internos, en la página 44
- Incorporación de código de activación y Mobile and Remote Access, en la página 45
- Activación del registro automático para los teléfonos, en la página 45
- Instalación del teléfono IP de Cisco, en la página 47
- Configuración del teléfono en los menús, en la página 49
- Activar la LAN inalámbrica en el teléfono, en la página 51
- Configuración de los ajustes de red, en la página 58
- Verificación del inicio del teléfono, en la página 65
- Configuración de los servicios de telefonía para los usuarios, en la página 65
- Cambiar el modelo de teléfono de un usuario, en la página 66

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 xv

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**.

Instalación del teléfono IP de Cisco

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. Para terminar de instalar el teléfono, configure los ajustes de red del teléfono según si va a habilitar o deshabilitar el servicio DHCP.

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.



Nota Antes de usar dispositivos externos, lea [Dispositivos externos, en la página 26](#).

Para obtener información sobre la instalación de accesorios, consulte *Guía de accesorios del teléfono IP serie 7800 y 8800 de Cisco de Cisco Unified Communications Manager*.

Si solo dispone de un cable de LAN en su escritorio, puede conectar el teléfono a la red LAN con el puerto SW y, a continuación, conectar el ordenador en el puerto PC. Para obtener más información, consulte [Uso compartido de la conexión de red con el teléfono y el equipo, en la página 49](#).

También puede conectar en cadena dos teléfonos juntos. Conecte el puerto PC del primer teléfono al puerto SW del teléfono segundo.



Precaución No conecte los puertos SW y PC en la LAN.

Procedimiento

- Paso 1** Seleccione la fuente de alimentación del teléfono:
- Alimentación a través de Ethernet (PoE).
 - Fuente de alimentación externa

Para obtener más información, consulte [Requisitos de alimentación del teléfono, en la página 16](#).

- Paso 2** Conecte los auriculares al puerto de auriculares y encaje el cable en el canal en el teléfono.
- El auricular preparado para banda ancha está diseñado especialmente para usarse con un teléfono IP de Cisco. El auricular incluye una banda luminosa que indica cuándo hay llamadas entrantes y mensajes de voz en espera.
- Precaución** No encajar el cable en el canal del teléfono puede dañar el tablero de circuitos impreso. El canal del cable reduce la presión sobre el conector y el tablero de circuitos impreso.
- Paso 3** Conecte un auricular de mano o unos auriculares inalámbricos. Puede agregar los auriculares más tarde.
- Encaje el cable en el canal para el cable.
- Precaución** No encajar el cable en el canal del teléfono puede dañar el tablero de circuitos impreso dentro del teléfono. El canal del cable reduce la presión sobre el conector y el tablero de circuitos impreso.
- Paso 4** Conecte un cable Ethernet directo desde el switch al puerto de red con la etiqueta 10/100/1000 SW del teléfono IP de Cisco. Todos los teléfonos IP de Cisco incluyen un cable Ethernet en la caja.
- Use cableado de categoría 3, 5, 5e o 6 para las conexiones de 10 Mb/s; de categoría 5, 5e o 6 para las conexiones de 100 Mb/s y de categoría 5e o 6 para las conexiones de 1000 Mb/s. Para obtener más información, consulte [Asignación de patillas de los puertos de red y del equipo, en la página 14](#).
- Paso 5** Conecte un cable Ethernet directo desde el otro dispositivo de red, como un ordenador de escritorio, al puerto PC del teléfono IP de Cisco. Puede conectar otro dispositivo de red más tarde.
- Use cableado de categoría 3, 5, 5e o 6 para las conexiones de 10 Mb/s; de categoría 5, 5e o 6 para las conexiones de 100 Mb/s y de categoría 5e o 6 para las conexiones de 1000 Mb/s. Para obtener más información, consulte [Asignación de patillas de los puertos de red y del equipo, en la página 14](#).
- Paso 6** Si el teléfono está en un escritorio, ajuste el soporte. Con un teléfono instalado en la pared, puede que sea necesario ajustar el soporte del auricular para asegurarse de que el auricular no se caiga de la base.
- Paso 7** Supervise el proceso de encendido del teléfono. Este paso agrega números de directorio principales y secundarios, así como funciones asociadas con los números de directorio del teléfono, y verifica que el teléfono está configurado correctamente.
- Paso 8** Si va a configurar los ajustes de red en el teléfono, puede configurar una dirección IP para este mediante DHCP o introduciendo manualmente una dirección IP.
- Consulte [Configuración de los ajustes de red, en la página 58](#) y [Configuración de la red, en la página 243](#).
- Paso 9** Actualice el teléfono con la imagen de firmware actual.
- Actualizar el firmware a través de una interfaz WLAN puede tardar más que si se hace mediante una interfaz con cables, dependiendo de la calidad y el ancho de banda de la conexión inalámbrica. Algunas actualizaciones pueden tardar más de una hora.
- Paso 10** Efectúe alguna llamada con el teléfono IP de Cisco para comprobar que el teléfono y sus características funcionan correctamente.
- Consulte la *Guía del usuario del teléfono IP serie 8800 de Cisco*.
- Paso 11** Proporcione información a los usuarios finales 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 IP de Cisco.
-

Uso compartido de la conexión de red con el teléfono y el equipo

Tanto el teléfono como el equipo deben conectarse a la red para que funcionen. Si solo dispone de un puerto Ethernet, los dispositivos pueden compartir la conexión de red.

Antes de empezar

El administrador debe activar el puerto PC en Cisco Unified Communications Manager para poder utilizarlo.

Procedimiento

-
- Paso 1** Conecte el puerto del SW del teléfono a la LAN con un cable Ethernet.
- Paso 2** Conecte el equipo al puerto del PC del teléfono con un cable Ethernet.
-

Configuración del teléfono en los menús

El teléfono IP de Cisco incluye los siguientes menús de configuración:

- Configuración de red: proporciona opciones para ver y configurar ajustes de red, como solo IPv4, solo IPv6, WLAN y Ethernet.
- Configuración de Ethernet: los elementos de este submenú proporcionan opciones para configurar el teléfono IP de Cisco en una red Ethernet.
- Configuración del cliente Wi-Fi: los elementos de este submenú proporcionan opciones para configurar el teléfono IP de Cisco con la red de área local inalámbrica (WLAN). El Wi-Fi solo es compatible con los teléfonos IP 8861 y 8865 de Cisco.



Nota El puerto PC del teléfono se desactiva cuando el Wi-Fi se activa en el teléfono.

- Configuración de IPv4 y Configuración de IPv6: estos submenús de los menús Configuración de Ethernet y Configuración del cliente Wi-Fi proporcionan opciones de red adicionales.
- Configuración de seguridad: proporciona opciones para ver y configurar los ajustes de seguridad, como el modo de seguridad, la lista de confianza y la autenticación 802.1X.

Para poder cambiar los valores de la opción en el menú Configuración de red, debe desbloquear la opción para editarla.





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

- Activado: permite el acceso al menú Configuración.
- Desactivado: impide el acceso al menú Configuración.
- Restringido: permite el acceso al menú Preferencias de usuario, 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.

Procedimiento

-
- Paso 1** Presione **Aplicaciones** .
- Paso 2** Seleccione **Config. admin.**
- Paso 3** Seleccione **Configuración de red** o **Configuración de seguridad**.
- Paso 4** Introduzca su ID de usuario y la contraseña, si se solicitan, y haga clic en **Iniciar sesión**.
- 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, pulse **Salir** o la flecha atrás .
-

Aplicación de una contraseña al teléfono


Puede aplicar una contraseña para el teléfono. Si lo hace, no se podrán realizar cambios en las opciones administrativas en el teléfono sin una entrada de contraseña en la pantalla del teléfono Config. admin.

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 teclado de navegación para resaltar el campo que desea editar y pulse **Seleccionar** en ese teclado 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, pulse la tecla programada de flecha . Esta tecla programable elimina el carácter situado a la izquierda del cursor.
- Pulse **Cancelar** antes de pulsar **Guardar** para descartar los cambios que haya efectuado.
- Para introducir una dirección IP, debe introducir valores en cuatro segmentos que ya están divididos. Cuando termine de introducir los dígitos a la izquierda del primer punto, use la tecla de flecha a la derecha para desplazarse al segmento siguiente. El punto que sigue a los dígitos más a la izquierda se inserta de forma automática.
- 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.

Temas relacionados

[Restauración básica](#), en la página 279

[Aplicación de una contraseña al teléfono](#), en la página 50

Activar la LAN inalámbrica en el teléfono

Antes de configurar una LAN inalámbrica, compruebe que el teléfono admita el uso inalámbrico. Los teléfonos IP 8861 y 8865 de Cisco admiten una implementación de LAN inalámbrica. El teléfono IP 8865NR de Cisco no admite una LAN inalámbrica.

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

Si ha activado la conectividad Wi-Fi de voz y está usando el modo de seguridad PEAP o EAP-FAST, autentique la red Wi-Fi con la aplicación de inicio de sesión de WLAN. Los modos de seguridad WEP, PSK y abierto sirven para realizar la autenticación en la red Wi-Fi.

Se recomienda un método de itinerancia rápida segura para los usuarios de Wi-Fi.



Nota El puerto PC del teléfono se desactiva cuando el Wi-Fi se activa en el teléfono.

Para obtener todos los detalles sobre la configuración, consulte la *Guía de implementación en LAN inalámbrica de los teléfonos IP serie 8800 de Cisco* en esta ubicación:

<http://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 8800 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 **Aplicaciones** .
- Paso 2** Diríjase a **Config. admin. > Configuración de red > Configuración del cliente Wi-Fi > Nombre de red**. Verá una lista de puntos de acceso inalámbricos disponibles a los que se puede conectar.
- Paso 3** Active la red inalámbrica.
-

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 IP de Cisco inalámbrico.



-
- 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 en 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 El puerto PC del teléfono se desactiva cuando el Wi-Fi se activa en el teléfono.



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 del teléfono IP de serie 8800 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>.

El campo **El usuario puede modificar** del perfil de red LAN inalámbrica controla esa capacidad del usuario de configurar modos de seguridad en el teléfono. Cuando un usuario no puede cambiar algunos de los campos, estos se muestran en color gris.

Antes de empezar

Configure de la LAN inalámbrica desde Cisco Unified Communications Manager.

Procedimiento

Paso 1 Pulse **Aplicaciones** .

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 19: Opciones del menú Configuración del cliente Wi-Fi

Opción	Descripción	Para cambiarla
Nombre de red	Especifica el identificador de conjunto de servicio, un identificador único para acceder a puntos de acceso inalámbricos. Muestra la lista de puntos de acceso inalámbricos disponibles.	Consulte Configuración de los ajustes de la página 58 .
Configuración de solo IPv4	En el submenú Configuración de IPv4 puede hacer lo siguiente: <ul style="list-style-type: none"> 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 obtener más información sobre los campos de la dirección IPv4, consulte Campos de IPv4, en la página 60 .	Desplácese a Configuración de IPv4 y Seleccionar .
Configuración de solo IPv6	En el submenú Configuración de IPv6 puede hacer lo siguiente: <ul style="list-style-type: none"> 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 obtener más información sobre los campos de la dirección IPv6, consulte Campos de IPv6, en la página 62 .	Desplácese a Configuración de IPv6 y Seleccionar .
Dirección MAC	La dirección de control de acceso a los medios (MAC) única del teléfono.	Solo visualización. No es posible cambiarla.
Nombre de dominio	El nombre del dominio del sistema de nombre de dominio (DNS) en el que se encuentra el teléfono.	Consulte Configuración de los ajustes de la página 58 .

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 y 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.



Nota Los teléfonos que utilizan Mobile and Remote Access mediante Expressway para conectarse a Cisco Unified Communications Manager no pueden utilizar el perfil Wi-Fi. Debido a que no tiene el SSID, el modo de autenticación y las credenciales de inicio de sesión del teléfono del usuario, no puede configurar un perfil de red LAN inalámbrica para su teléfono.

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.

Nota El campo **Perfil de acceso a red** no es compatible con el teléfono IP 8861 y 8865 de Cisco.

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**.
-

Configuración de los ajustes de red

Procedimiento

-
- Paso 1** Pulse **Aplicaciones** .
- Paso 2** Para acceder al menú Configuración de red, seleccione **Config. admin. > Configuración de Ethernet**.
- Paso 3** Configure los campos tal y como se describe en [Campos de configuración de Ethernet, en la página 58](#).
- Paso 4** Después de configurar los campos, seleccione **Aplicar** y **Guardar**.
- Paso 5** Reinicie el teléfono.
-

Campos de configuración de Ethernet

El menú Configuración de red contiene los campos y los submenús de IPv4 e IPv6. Para modificar algunos de los campos, en primer lugar, desactive DHCP.

Al establecer una conexión VPN se sustituyen los campos de datos de Ethernet.

Tabla 20: Opciones del menú Configuración de Ethernet

Entrada	Tipo	Descripción
Configuración de IPv4	Menú	Consulte la sección de campos de IPv4. Esta opción solo se muestra si el teléfono está configurado en modo solo IPv4 o IPv6.
Configuración de IPv6	Menú	Consulte la sección de campos de IPv6.
Dirección MAC	Cadena	La dirección de control de acceso a los medios (MAC) única del teléfono. Solo visualización. No es posible configurarla.
Nombre de dominio	Cadena	El nombre del dominio del sistema de nombre de dominio (DNS) en el switch. Para cambiar este campo, desactive DHCP.
ID de VLAN operativo		La red de área local virtual (VLAN) auxiliar configurada en un switch al que pertenece el teléfono. Esta configuración se deja en blanco si no se han configurado la VLAN auxiliar o el teléfono. Si el teléfono no ha recibido una VLAN auxiliar, esta opción indica la VLAN operativa. El teléfono no hereda la VLAN operativa de VLAN administrativo si es un teléfono de protocolo de detección de nivel de vínculo-Descubrimiento de protocolo. Para asignar un ID de VLAN de forma manual, use la opción ID de VLAN auxiliar.
ID de VLAN administrativo		La VLAN auxiliar de la que es miembro el teléfono. Se usa solo si el teléfono no recibe una VLAN auxiliar del switch; en caso contrario, se omite de este valor.
VLAN de PC		Permite al teléfono interoperar con switches de terceros que no admiten VLAN administrativa. VLAN administrativa debe establecerse antes de poder cambiar esta configuración.
Config. de puerto switch	Negociación automática 1000 completo 100 medio 10 medio 10 completo	La velocidad y dúplex del puerto de red. Los valores válidos son: <ul style="list-style-type: none"> • Autonegociación (opción predeterminada) • 1000 completo: 1000-BaseT/dúplex completo • 100 medio: 100-BaseT/semidúplex • 100 completo: 100-BaseT/dúplex completo • 10 medio: 10-BaseT/semidúplex • 10 completo: 10-BaseT/dúplex completo Si el teléfono está conectado a un conmutador, configure el puerto de red con la velocidad que el teléfono; o bien configure ambos elementos para que coincidan. Desbloquee las opciones de configuración de red si desea editar este campo. Si esta opción, en la opción Configuración de puerto PC debe establecerse.

Entrada	Tipo	Descripción
Configuración de puerto PC	Negociación automática 1000 completo 100 medio 10 medio 10 completo	<p>La velocidad y dúplex del puerto de ordenador (acceso). Valores válidos:</p> <ul style="list-style-type: none"> • Autonegociación (opción predeterminada) • 1000 completo: 1000-BaseT/dúplex completo • 100 medio: 100-BaseT/semidúplex • 100 completo: 100-BaseT/dúplex completo • 10 medio: 10-BaseT/semidúplex • 10 completo: 10-BaseT/dúplex completo <p>Si el teléfono está conectado a un conmutador, configure el puerto del conmutador con la misma velocidad que el teléfono; o bien configure ambos elementos para que la velocidad sea la misma.</p> <p>Desbloquee las opciones de configuración de red si desea cambiar este campo. Si el teléfono está conectado a un conmutador, en la opción Configuración de puerto SW, debe establecer el mismo valor.</p> <p>Para configurar el ajuste en varios teléfonos de forma simultánea, active la configuración remota en la ventana Configuración de teléfono empresarial (Sistema > Configuración de teléfono empresarial).</p> <p>Si los puertos se configuran para la configuración de puerto remota en Cisco Unified Communications Manager Administration, los datos no se pueden cambiar en el teléfono.</p>

Campos de IPv4

Tabla 21: Opciones del menú de configuración de IPv4

Entrada	Descripción
DHCP habilitado	<p>Indica si el teléfono tiene DHCP habilitado o deshabilitado.</p> <p>Si DHCP está habilitado, el servidor DHCP asigna al teléfono una dirección IP. Si DHCP está deshabilitado, el administrador debe asignar una dirección IP de forma manual al teléfono.</p> <p>Para obtener más información, consulte Configuración del teléfono para usar DHCP, en la página 64 y Configuración del teléfono para no usar DHCP, en la página 64.</p>
Dirección IP	<p>Indica la dirección del protocolo de Internet (IP) del teléfono.</p> <p>Si asigna una dirección IP con esta opción, también debe asignar una máscara de subred y un router predeterminado. Consulte las opciones Máscara de subred y Router predeterminado en esta tabla.</p>
Máscara de subred	La máscara de subred que usa el teléfono.
Router predeterminado	El router predeterminado que usa el teléfono.
Servidor DNS 1 Servidor DNS 2 Servidor DNS 3	El servidor de sistema de nombre de dominio primario (Servidor DNS 1) y los servidores DNS de copia de seguridad opcionales (Servidor DNS 2 y 3) que usa el teléfono.
TFTP alternativo	Indica si el teléfono usa un servidor TFTP alternativo.

Entrada	Descripción
<p>Servidor TFTP 1</p>	<p>El servidor de protocolo de transferencia de archivos trivial (TFTP) primario que usa el teléfono. Si no usa DHCP en la red y desea cambiar este servidor, debe usar la opción Servidor TFTP 1.</p> <p>Si activa la opción TFTP alternativo, debe introducir un valor distinto a cero en la opción Servidor TFTP 1.</p> <p>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.</p> <p>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:</p> <ol style="list-style-type: none"> 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. <p>Nota Para obtener información sobre los archivos CTL e ITL, consulte la <i>Guía de seguridad de Cisco Unified Communications Manager</i>.</p>

Entrada	Descripción
Servidor TFTP 2	<p>El servidor TFTP de copia de seguridad opcional que el teléfono usa si el servidor TFTP principal no está disponible.</p> <p>Si en el archivo CTL o ITL del teléfono no aparecen ni el servidor TFTP principal ni el de copia de seguridad, debe desbloquear uno de estos archivos antes de guardar los cambios en la opción Servidor TFTP 2. En este caso, el teléfono elimina el archivo correspondiente 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.</p> <p>Si olvida desbloquear el archivo CTL o ITL, puede cambiar la dirección del servidor TFTP 2 en alguno de los archivos y luego eliminarlos pulsando la opción Borrar en el menú Configuración de seguridad. Se descarga un nuevo archivo CTL o ITL de la nueva dirección del servidor TFTP 2.</p> <p>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 el orden siguiente:</p> <ol style="list-style-type: none"> 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. <p>Nota Para obtener información sobre los archivos CTL o ITL, consulte la Guía de seguridad de Cisco Unified Communications Manager.</p>
Servidor BOOTP	Indica si el teléfono ha recibido la dirección IP de un servidor BOOTP en lugar de hacerlo de un servidor DHCP.
Dirección DHCP liberada	<p>Libera la dirección IP que DHCP ha asignado.</p> <p>Este campo se puede editar si DHCP está habilitado. Si desea eliminar el teléfono de la VLAN y liberar la dirección IP para volver a asignarla, establezca el valor Sí en esta opción y pulse Aplicar.</p>

Campos de IPv6

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 habilitadas 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 detalles acerca de la implementación de IPv6, consulte la [guía de implementación de IPv6 para la versión 12.0 de los sistemas de colaboración de Cisco](#).

Las direcciones IPv6 se configuran en uno de los menús siguientes:

- Si la comunicación Wi-Fi está desactivada: **Configuración de Ethernet > Configuración de IPv6**
- Si la comunicación Wi-Fi está activada: **Configuración del cliente Wi-Fi > Configuración de IPv6**

Utilice el teclado del teléfono para introducir o modificar una dirección IPv6. Para introducir dos puntos, presione el asterisco (*) en el teclado. Para introducir los dígitos hexadecimales a, b y c, pulse 2 en el teclado, avance para seleccionar el dígito necesario y pulse **Intro**. Para introducir los dígitos hexadecimales d, e y f, pulse 3 en el teclado, avance para seleccionar el dígito necesario y pulse **Intro**.

En la tabla siguiente se describe la información relativa a las direcciones IPv6 que hallará en el menú IPv6.

Tabla 22: Opciones del menú de configuración de IPv6


Entrada	Valor predeterminado	Descripción
DHCPv6 habilitado	Sí	Indica el método que usa el teléfono para obtener una dirección IPv6. Si DHCPv6 está habilitado, el teléfono obtiene una dirección IPv6 por el router IPv6. Si DHCPv6 está deshabilitado, el teléfono obtiene una dirección IPv6 (de SLAAC) o sin estado (de SLAAC).
Dirección IPv6	::	Muestra la dirección de solo IPv6 actual. Las direcciones IPv6 válidas tienen el siguiente formato de dirección: <ul style="list-style-type: none"> • Ocho conjuntos de dígitos hexadecimales. • Formato comprimido para conjuntos de dígitos hexadecimales por dos signos de dos puntos. Si la dirección IP se asigna con esta dirección, se muestra la dirección de solo IPv6.
Longitud de prefijo de IPv6	0	Muestra la longitud actual del prefijo de IPv6. La longitud del prefijo de subred es de 0 a 64.
Router predeterminado de IPv6	::	Muestra el router predeterminado usado para obtener una dirección IPv6 nueva.
Servidor DNS 1 de IPv6	::	Muestra el servidor DNSv6 primario usado para obtener una dirección IPv6 nueva.
Servidor DNS 2 de IPv6	::	Muestra el servidor DNSv6 secundario usado para obtener una dirección IPv6 nueva.
TFTP alternativo de IPv6	No	Permite al usuario habilitar el uso de un servidor TFTP alternativo para obtener una dirección IPv6 nueva.
Servidor TFTP 1 de IPv6	::	Muestra el servidor TFTP IPv6 primario usado para obtener una dirección IPv6 nueva.
Servidor TFTP 2 de IPv6	::	(Opcional) Muestra el servidor TFTP IPv6 secundario usado para que al usuario establecer un servidor TFTP alternativo para obtener una dirección IPv6 nueva.

Entrada	Valor predeterminado	Descripción
Dirección IPv6 liberada	No	Permite al usuario liberar información

Configuración del teléfono para usar DHCP

Para habilitar DHCP y permitir que el servidor DHCP asigne automáticamente una dirección IP al teléfono IP de Cisco y dirija el teléfono a un servidor TFTP, lleve a cabo estos pasos:


Procedimiento

-
- Paso 1** Presione **Aplicaciones** .
- Paso 2** Seleccione **Config. admin. > Configuración de red > Configuración de Ethernet > Configuración de IPv4**.
- Paso 3** Para habilitar DHCP, en DHCP habilitado indique **Sí**. DHCP está activado de manera predeterminada.
- Paso 4** Para usar un servidor TFTP alternativo, en Servidor TFTP alternativo indique **Sí** e introduzca la dirección IP del servidor TFTP.
- Nota** Pídale al administrador de red que determine si debe asignar un servidor TFTP alternativo en lugar de usar el que asigne DHCP.
- Paso 5** Pulse **Aplicar**.
-

Configuración del teléfono para no usar DHCP

Si no se usa DHCP, debe configurar la dirección IP, la máscara de subred, el servidor TFTP y el router predeterminado de forma local en el teléfono.

Procedimiento

-
- Paso 1** Presione **Aplicaciones** .
- Paso 2** Seleccione **Config. admin. > Configuración de red > Configuración de Ethernet > Configuración de IPv4**.
- Paso 3** Para desactivar DHCP y establecer manualmente una dirección IP:
- En DHCP habilitado indique **No**.
 - Introduzca una dirección IP estática para el teléfono.
 - Introduzca la máscara de subred.
 - Introduzca la dirección IP del router predeterminado.
 - En Servidor TFTP alternativo indique **Sí** e introduzca la dirección IP del servidor TFTP 1.
- Paso 4** Presione **Aplicar**.
-

Servidor de carga

El servidor de carga se usa para optimizar el tiempo de instalación de las actualizaciones del firmware del teléfono y para descargar el tráfico de la WAN al almacenar imágenes localmente, lo que evita tener que cruzar el enlace WAN en cada actualización del teléfono.

Como servidor de carga puede establecer otra dirección IP o nombre del servidor TFTP (distintos a Servidor TFTP 1 o Servidor TFTP 2) desde el que se podrá recuperar el firmware del teléfono para las actualizaciones. Cuando se establece la opción Servidor de carga, el teléfono se pone en contacto con el servidor designado para actualizar el firmware.



Nota La opción Servidor de carga permite especificar un servidor TFTP alternativo solo para las actualizaciones del teléfono. El teléfono sigue usando el servidor TFTP 1 o 2 para obtener los archivos de configuración. La opción Servidor de carga no proporciona administración para el proceso ni para los archivos, por ejemplo, para la transferencia de archivos, la compresión o la eliminación.

El servidor de carga se configura en la ventana de Configuración de teléfono empresarial. En Cisco Unified Communications Manager Administration, seleccione **Dispositivo > Teléfono > Configuración de teléfono empresarial**.

Verificación del inicio del teléfono

Cuando el teléfono IP de Cisco reciba alimentación, iniciará el proceso de diagnóstico y realizará un ciclo por los pasos siguientes.

1. Los botones de función y sesión emiten luz intermitente amarilla y luego verde durante las distintas etapas del arranque a medida que se comprueba el hardware.
2. En la pantalla principal se muestra Registro en Cisco Unified Communications Manager.

Si el teléfono completa correctamente estas fases, se ha iniciado correctamente y el botón **Seleccionar** permanece iluminado hasta que se selecciona.

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. Estos servicios incluyen aplicaciones XML y midlets Java firmados por Cisco que permiten mostrar contenido interactivo con texto y gráficos en el teléfono. El teléfono IP administra cada servicio como una aplicación independiente. Algunos ejemplos de servicios pueden ser horarios de la cartelera local, cotizaciones de acciones o previsiones meteorológicas.

Para que un usuario pueda acceder a cualquier servicio:

- Debe usar 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 [Administración del portal de autoayuda, en la página 83](#) para obtener un resumen de la información que debe proporcionar a los usuarios finales.

Temas relacionados

[Cisco Unified Communications Manager Documentación](#), en la página xv

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.

Si cambia un teléfono antiguo con el firmware de SCCP a un modelo en Teléfono Cisco IP Phone serie 8800, el nuevo teléfono se configurará para el modo de línea de sesión.

Si el teléfono antiguo tiene configurado un modelo de expansión de teclas, Unified CM copiará la información del módulo de expansión en el nuevo teléfono al mismo tiempo. Cuando el usuario conecta un módulo de expansión de teclas compatible con el nuevo teléfono, el nuevo módulo de expansión obtiene la información del módulo de expansión migrado.

Si el teléfono antiguo tiene configurado un modelo de expansión de teclas y el nuevo teléfono no admite un módulo de expansión, Unified CM no copiará la información del módulo de expansión.

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

Configuración del teléfono para Cisco Unified Communications Manager

- [Configuración del teléfono IP de Cisco, en la página 69](#)
- [Determinación de la dirección MAC del teléfono, en la página 72](#)
- [Métodos de adición de teléfonos, en la página 73](#)
- [Adición de usuarios a Cisco Unified Communications Manager, en la página 74](#)
- [Adición de un usuario a un grupo de usuarios finales, en la página 76](#)
- [Asociación de teléfonos con usuarios , en la página 76](#)
- [Survivable Remote Site Telephony, en la página 77](#)
- [Telefonía de sitio remoto superviviente mejorada, en la página 80](#)
- [Reglas de marcación de la aplicación, en la página 80](#)

Configuración del teléfono IP 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. Algunas tareas de este procedimiento son opcionales y dependen del sistema y las necesidades del usuario.

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

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.
- Dirección MAC
- 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.
- El número de líneas y de números de directorio (DN) asociados que se deben 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 botones del teléfono, las funciones del teléfono, los servicios del teléfono IP o las aplicaciones del teléfono.

La información proporciona una lista de requisitos de configuración para los teléfonos e identifica la configuración preliminar que se debe realizar antes de configurar teléfonos individuales, como las plantillas de botones del teléfono.

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

Paso 3 Personalice las plantillas de botones (si fuera necesario) cambiando el número de botones de línea, los botones de marcación rápida o los botones de URL de servicios. Seleccione **Dispositivo > Configuración del dispositivo > Plantilla de botones de teléfono** para crear y actualizar las plantillas.

Puede agregar un botón Privacidad, Todas las llamadas o Movilidad para satisfacer las necesidades de los usuarios.

Para obtener más información, consulte [Plantillas de botones de teléfono, en la página 201](#).

Paso 4 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 y hora, la plantilla de teclas programables y la información de MLPP.

Paso 5 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 6 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 7 Configure un perfil de seguridad para el tipo de dispositivo y el protocolo. Seleccione **Sistema > Seguridad > Perfil de seguridad del teléfono**.

Paso 8 Para agregar y configurar el teléfono, complete los campos necesarios de la ventana de configuración del teléfono. Un asterisco (*) junto al nombre del campo indica que es obligatorio; por ejemplo, la dirección MAC y el grupo de dispositivos.

Este paso agrega el dispositivo con la configuración predeterminada a la base de datos de Cisco Unified Communications Manager.

Para obtener información sobre los campos de configuración específicos del producto, consulte el botón de ayuda «?» en la ventana de configuración del teléfono.

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.

- Paso 9** Para agregar y configurar números de directorio (líneas) en el teléfono, complete los campos requeridos de la ventana de configuración del número de directorio. Un asterisco (*) junto al nombre del campo indica que es obligatorio; por ejemplo, el número de directorio y el grupo de presencia.
- Este paso agrega números de directorio principales y secundarios, así como funciones asociadas con los números de directorio del teléfono.
- Nota** Si no configura el número de directorio principal, el usuario verá el mensaje No suministrado en el teléfono.
- Paso 10** Configure los botones de marcación rápida y asigne los números de marcación rápida.
- Los usuarios pueden cambiar la configuración de marcación rápida en sus teléfonos mediante el portal de autoayuda de Cisco Unified Communication.
- Paso 11** Configure los servicios del teléfono IP de Cisco Unified y asigne servicios (opcional) para proporcionarlos al teléfono IP.
- Los usuarios pueden agregar o cambiar servicios en sus teléfonos mediante el portal de autoayuda de Cisco Unified Communications.
- Nota** Los usuarios solo pueden suscribirse al servicio del teléfono IP si la casilla de verificación de suscripción empresarial está sin marcar cuando el servicio del teléfono IP se configura por primera vez en Cisco Unified Communications Manager Administration.
- Nota** Algunos servicios predeterminados proporcionados por Cisco se clasifican como suscripciones empresariales, de modo que el usuario no puede agregarlos mediante el portal de autoayuda. Esos servicios se encuentran en el teléfono de forma predeterminada y solo se pueden eliminar del teléfono si se desactivan en Cisco Unified Communications Manager Administration.
- Paso 12** Asigne servicios a los botones programables (opcional) para proporcionar acceso a un servicio o una URL del teléfono IP.
- Paso 13** Agregue la información del usuario en los campos obligatorios. Un asterisco (*) junto al nombre del campo indica que se trata de un campo obligatorio; por ejemplo, ID de usuario y apellidos. Este paso añade la información del usuario al directorio global de Cisco Unified Communications Manager.
- Nota** Asigne una contraseña (para el portal de autoayuda) y un PIN (para Cisco Extension Mobility y el directorio personal).
- 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.
- 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.
- Paso 14** Asocie un usuario a un grupo de usuarios. Este paso asigna a los usuarios una lista común de funciones y permisos que se aplican 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. Por ejemplo, debe agregar usuarios al grupo de usuarios finales de Cisco CCM estándar a fin de que puedan acceder al portal de autoayuda de Cisco Unified Communications Manager.

- Paso 15** Asocie un usuario con un teléfono (opcional). Este paso proporciona a los usuarios control sobre su teléfono; por ejemplo, para que puedan desviar llamadas o agregar números de marcación rápida o servicios.
- Algunos teléfonos, como los que se encuentran en las salas de conferencias, no tienen ningún usuario asociado.
- Paso 16** Si aún no se encuentra en la ventana de configuración del usuario final, seleccione **Administración de usuarios > Usuario final** para realizar las tareas de configuración finales. Use los campos de búsqueda y la opción **Buscar** para localizar al usuario (por ejemplo, Javier García) y haga clic en el ID de usuario para acceder a la ventana de configuración del usuario final correspondiente.
- Paso 17** En la sección Asociaciones del número de directorio de la pantalla, defina la extensión primaria en la lista desplegable.
- Paso 18** En la sección de información de movilidad, marque la casilla para activar la movilidad.
- Paso 19** En la sección de información de permisos, use los botones de Grupo de usuarios 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.
- Paso 20** Para ver todos los grupos de usuarios configurados, seleccione **Administración de usuarios > Grupo de usuarios**.
- Paso 21** En la sección Extension Mobility, marque la casilla Habilitar extensión móvil entre clústeres en caso de que el usuario pueda usar este servicio.
- Paso 22** Seleccione **Guardar**.

Temas relacionados


[Cisco Unified Communications Manager Documentación](#), en la página xv

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, presione **Aplicaciones** , seleccione **Información del teléfono** y busque en 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 72](#).

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

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 xv

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 xv

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 75](#).
- 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 xv

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

La telefonía de sitio remoto superviviente (SRST) garantiza que es posible seguir accediendo a las funciones básicas del teléfono si la comunicación WAN 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 más información sobre el firmware y la versión de telefonía de sitio remoto superviviente admitida, consulte la página *Cisco Unified Survivable Remote Site Telephony Compatibility Information* (Información sobre compatibilidad de Cisco Unified Survivable Remote Site Telephony) en Cisco.com (<http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-device-support-tables-list.html>).

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

Tabla 23: Compatibilidad de funciones de SRST

Función	Compatible	Notas
Nueva llamada	Sí	
Fin llamada	Sí	
Rellamar	Sí	
Contestar	Sí	

Función	Compatible	Notas
Espera	Sí	
Continuar	Sí	
Conferencia	Sí	
Conferencia con llamadas activas (conectar)	No	No se muestra la tecla programada Llamadas activas.
Lista de conferencias	No	
Transferencia	Sí	
Transferencia a llamadas activas (transferencia directa)	No	
Contestación automática	Sí	
Llamada en espera	Sí	
Identificar a la persona que llama	Sí	
Indicador sonoro de mensaje en espera	Sí	
Tecla de línea programable Todas	Sí	
Tecla de línea programable Contestar	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.
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	

Función	Compatible	Notas
Tecla de línea programable del servicio IRL	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.
Intrusión	No	No se muestra la tecla programada Intrusión.
Indicación de mensaje en espera mejorada	No	Las señales de recuento de mensajes no aparecen en la pantalla del teléfono. Solo se muestra el icono de mensaje en espera.
Aparcamiento de llamadas dirigido	No	No se muestra la tecla programada.
BLF	Parcial	La tecla de función BLF funciona como las teclas de marcación rápida.
Reversión en espera	No	Las llamadas permanecen en espera de forma indefinida.
Espera remota	No	Las llamadas aparecen como llamadas en espera local.
Meet Me	No	No se muestra la tecla programada Meet Me.
Captura	No	La tecla no produce ninguna acción.
Captura de llamadas de grupo	No	La tecla no produce ninguna acción.
Captura de otros	No	La tecla no produce ninguna acción.
ID de llamadas maliciosas	No	La tecla no produce ninguna acción.
QRT	No	La tecla no produce ninguna acción.
Grupo de salto	No	La tecla no produce ninguna acción.
Intercomunicación	No	La tecla no produce ninguna acción.
Movilidad	No	La tecla no produce ninguna acción.
Privacidad	No	La tecla no produce ninguna acción.
Retrollamada	No	No se muestra la tecla programada Retrollamada.
Vídeo	Sí	No se admite la videoconferencia.

Función	Compatible	Notas
Vídeo	Sí	No se admite la videoconferencia.
Línea compartida	No	
Marcación rápida de BLF	Sí	

Telefonía de sitio remoto superviviente mejorada

La telefonía de sitio remoto superviviente mejorada (E-SRST) garantiza que es posible seguir accediendo a las funciones adicionales disponibles en el teléfono si la comunicación WAN se interrumpe. Además de las funciones admitidas por telefonía de sitio remoto superviviente (SRST), E-SRST admite lo siguiente:

- Línea compartida
- Busy Lamp Field (BLF, campo de luz ocupado)
- Videollamadas

Para obtener más información sobre el firmware y la versión de telefonía de sitio remoto superviviente admitida, consulte la página *Cisco Unified Survivable Remote Site Telephony Compatibility Information* (Información sobre compatibilidad de Cisco Unified Survivable Remote Site Telephony) en Cisco.com (<http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-device-support-tables-list.html>).

Reglas de marcación de la aplicación

Las reglas de marcación de la aplicación se usan para convertir números de contacto móviles compartidos en números que se pueden marcar en la red. Las reglas de marcación de la aplicación no se aplican si el usuario marca un número manualmente o si el número se ha editado antes de que el usuario efectúe la llamada.

Las reglas de marcación de la aplicación se establecen en Cisco Unified Communications Manager.

Para obtener información adicional sobre las reglas de marcación, consulte *Guía de configuración del sistema para Cisco Unified Communications Manager*, capítulo «Configurar reglas de marcación».

Configuración de las reglas de marcación de la aplicación

Procedimiento

-
- Paso 1** En Administración de Cisco Unified Communications Manager, vaya a **Enrutamiento de llamada > Reglas de marcación > Reglas de marcación de aplicación**.
- Paso 2** Seleccione **Nuevo** para crear una regla de marcación de la aplicación nueva, o bien seleccione una regla existente para modificarla.
- Paso 3** Complete los campos siguientes:

- **Nombre:** este campo incluye un nombre exclusivo para la regla de marcación que puede contener hasta 20 caracteres alfanuméricos y cualquier combinación de espacios, puntos (.), guiones (-) y guiones bajos (_).
- **Descripción:** este campo incluye una breve descripción que se introduce para la regla de marcación.
- **El número empieza por:** este campo indica los dígitos iniciales de los números de directorio a los que desea aplicar esta regla de marcación de la aplicación.
- **Número de dígitos:** este campo obligatorio indica los dígitos iniciales de los números de directorio a los que desea aplicar esta regla de marcación de la aplicación.
- **Total de dígitos que borrar:** este campo obligatorio indica el número de dígitos que desea que Cisco Unified Communications Manager elimine de los números de directorio que se aplican a esta regla de marcación.
- **Prefijo con patrón:** este campo obligatorio indica el patrón que se debe añadir al principio de los números de directorio que se aplican a esta regla de marcación de la aplicación.
- **Prioridad de regla de marcación de la aplicación:** este campo se muestra cuando se introduce la información del prefijo con patrón. El campo permite establecer el orden de prioridad de las reglas de marcación de la aplicación.

Paso 4 Reinicie Cisco Unified Communications Manager.



CAPÍTULO 6

Administración del portal de autoayuda

- [Descripción general del portal de autoayuda, en la página 83](#)
- [Configuración del acceso de usuario al portal de autoayuda, en la página 83](#)
- [Personalización de la presentación del portal de autoayuda, en la página 84](#)

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 xv

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 de Cisco

- Seguridad del teléfono IP de Cisco, en la página 87
- Personalización del teléfono IP de Cisco, en la página 117
- Características y configuración del teléfono, en la página 123
- Directorio corporativo y personal, en la página 217



CAPÍTULO 7

Seguridad del teléfono IP de Cisco

- [Mejoras de seguridad para la red del teléfono, en la página 87](#)
- [Características de seguridad admitidas, en la página 88](#)

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>).

- *Información general de 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>)
- *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>)



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.

Los teléfonos IP de Cisco serie 8800 cumplen con el estándar federal de procesamiento de información (FIPS). Para que funcione correctamente, el modo FIPS requiere un tamaño de clave de 2048 bits o mayor. Si el certificado no es de 2048 bits o superior, el teléfono no se registrará con Cisco Unified Communications Manager y se producirá un error al registrar el teléfono. El tamaño de clave de certificado no cumple con FIPS se muestra en el teléfono.

Si el teléfono tiene un LSC, deberá actualizar el tamaño de clave LSC a 2048 bits o mayor antes de activar FIPS.

En la tabla siguiente se ofrece una descripción general de las funciones de seguridad admitidas por los teléfonos. Para obtener más datos, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.


Para ver la configuración de seguridad actual en un teléfono, incluido el modo de seguridad, la lista de confianza y la autenticación 802.1X, presione **Aplicaciones**  y elija **Configuración de administración** > **Configuración de seguridad**.

Tabla 24: Descripción general de funciones de seguridad

Función	Descripción
Autenticación de imagen	Los archivos binarios firmados (con la extensión .sbn) evitan que la imagen de firmware se altere antes de que se cargue en un teléfono. Al alterar la imagen, el proceso de autenticación del teléfono falla y la nueva imagen se rechaza.
Cifrado de imagen	Los archivos binarios cifrados (con la extensión .sebn) evitan que la imagen de firmware se altere antes de que se cargue en un teléfono. Al alterar la imagen, el proceso de autenticación del teléfono falla y la nueva imagen se rechaza.
Instalación del certificado del sitio del cliente	Cada teléfono IP de Cisco requiere un certificado exclusivo para la autenticación del dispositivo. Los teléfonos incluyen un certificado instalado en fábrica (MIC), pero para aportar más seguridad, es posible especificar en Cisco Unified Communications Manager Administration que se instale un certificado mediante la función de proxy de entidad emisora de certificados (CAPF). Como alternativa, puede instalar un Locally Significant Certificate (LSC) desde el menú de configuración de seguridad del teléfono.
Autent. dispositivo	Se produce entre el servidor de Cisco Unified Communications Manager y el teléfono cuando cada entidad acepta el certificado de la otra. Determina si se debe producir una conexión segura entre el teléfono y una instancia de Cisco Unified Communications Manager y, si fuera necesario, crea una ruta de señalización segura entre las entidades mediante el protocolo TLS. Cisco Unified Communications Manager no registra los teléfonos si no puede autenticarlos.

Función	Descripción
Autenticación del archivo	Valida los archivos firmados digitalmente que descarga el teléfono. El teléfono valida la firma para asegurarse de que el archivo no se ha alterado después de su creación. Los archivos que no superan la autenticación no se escriben en la memoria flash del teléfono. El teléfono rechaza esos archivos sin procesarlos más.
Cifrado de archivo	El cifrado impide que la información confidencial se revele mientras el archivo se encuentra de camino al teléfono. Asimismo, el teléfono valida la firma para asegurarse de que el archivo no se ha alterado después de su creación. Los archivos que no superan la autenticación no se escriben en la memoria flash del teléfono. El teléfono rechaza esos archivos sin procesarlos más.
Autenticación de señalización	Se usa el protocolo TLS para validar que los paquetes de señalización no se han alterado durante la transmisión.
Certificado instalado en fábrica	Cada teléfono IP de Cisco contiene un certificado instalado en fábrica (MIC) que se usa para la autenticación del dispositivo. El MIC proporciona una prueba de identidad única permanente del teléfono y permite a Cisco Unified Communications Manager autenticarlo.
Cifrado de medios	Se usa SRTP para garantizar que los flujos de medios entre los dispositivos admitidos sean seguros y que solo el dispositivo previsto reciba y lea los datos. Incluye la creación de un par de claves principales de medios para los dispositivos, la entrega de las claves a los dispositivos y la seguridad necesaria en la entrega de las claves mientras estas se transportan.
Función proxy de entidad emisora de certificados (CAPF)	Implementa partes del procedimiento de generación del certificado que consumen demasiados recursos para el teléfono e interactúa con el teléfono para generar la clave e instalar el certificado. La función CAPF se puede configurar para que solicite certificados de autoridades emisoras especificadas por el cliente en nombre del teléfono, o bien se puede configurar para que genere los certificados de forma local.
Perfil de seguridad	Define si el teléfono no es seguro o si está autenticado, cifrado o protegido. Otras entradas de esta tabla describen las funciones de seguridad.
Archivos de configuración cifrados	Permite garantizar la privacidad de los archivos de configuración del teléfono.
Desactivación opcional del servidor web de un teléfono	Por motivos de seguridad, es posible impedir el acceso a las páginas web de un teléfono (donde se muestran diversas estadísticas de funcionamiento de este) y al portal de autoayuda.
Fortalecimiento del teléfono	<p>Opciones de seguridad adicionales que se pueden controlar desde Cisco Unified Communications Manager Administration:</p> <ul style="list-style-type: none"> • Desactivación del puerto PC • Desactivación de ARP gratuito (GARP) • Desactivación del acceso a VLAN de voz del PC • Desactivación del acceso a los menús de configuración o acceso restringido solo al menú Preferencias y para guardar cambios de volumen • Desactivación del acceso a las páginas web en un teléfono • Desactivación del puerto de accesorios Bluetooth • Restringir cifrados TLS

Función	Descripción
Autenticación 802.1X	El teléfono IP de Cisco puede usar la autenticación 802.1X para solicitar acceso a la red y acceder a ella. Para obtener más información, consulte Autenticación 802.1X, en la página 113 .
Error de SIP seguro para SRST	Después de configurar una referencia de telefonía de sitio remoto superviviente (SRST) para la seguridad y, posteriormente, restablecer los dispositivos dependientes en Cisco Unified Communications Manager Administration, el servidor TFTP agrega el certificado SRST al archivo cnf.xml del teléfono y envía este archivo al teléfono. A continuación, un teléfono seguro usa una conexión TLS para interactuar con el router SRST.
Cifrado de señales	Asegúrese de que todos los mensajes de señales SIP que se envíen entre el dispositivo y el servidor de Cisco Unified Communications Manager están cifrados.
Alarma de actualización de la lista de confianza	Cuando la lista de confianza se actualiza en el teléfono, Cisco Unified Communications Manager recibe una alarma para indicar si la actualización se ha realizado correctamente o ha fallado. Consulte la tabla siguiente para obtener más información:
Cifrado AES 256	<p>Si se conectan a la versión 10.5(2) y posteriores de Cisco Unified Communications Manager, los teléfonos admiten el cifrado AES 256 para TLS y SIP para el cifrado de las señales y los medios. Esto permite a los teléfonos iniciar y admitir conexiones TLS 1.2 mediante cifrado basado en AES-256 que cumpla los estándares SHA-2 (algoritmo hash seguro) y los estándares federales de procesamiento de la información (FIPS) de Estados Unidos. Los cifrados son:</p> <ul style="list-style-type: none"> • Para las conexiones TLS: <ul style="list-style-type: none"> • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • Para sRTP: <ul style="list-style-type: none"> • AEAD_AES_256_GCM • AEAD_AES_128_GCM <p>Para obtener más datos, consulte la documentación de Cisco Unified Communications Manager.</p>
Certificados de Elliptic Curve Digital Signature Algorithm (ECDSA).	Como parte de la certificación Common Criteria (CC), Cisco Unified Communications Manager añadió certificados ECDSA en la versión 11.0. Esto afecta a todos los productos de sistemas operativos de voz (VOS) a partir de la versión CUCM 11.5 y posteriores.

En la tabla siguiente se muestran los mensajes de alarma de actualización de la lista de confianza y su significado. Para obtener más datos, consulte la documentación de Cisco Unified Communications Manager

Tabla 25: Mensajes de alarma de actualización de la lista de confianza

Código y mensaje	Descripción
1 - TL_SUCCESS	Se ha recibido un archivo CTL o ITL nuevo.
2 - CTL_INITIAL_SUCCESS	Se ha recibido un CTL nuevo, no hay ninguna lista de confianza.

Código y mensaje	Descripción
3 - ITL_INITIAL_SUCCESS	Se ha recibido un ITL nuevo, no hay ninguna lista de confianza.
4 - TL_INITIAL_SUCCESS	Se ha recibido un CTL y un ITL nuevos, no hay ninguna lista de confianza.
5 - TL_FAILED_OLD_CTL	La actualización al nuevo CTL ha fallado, pero hay una lista de confianza anterior.
6 - TL_FAILED_NO_TL	La actualización a la nueva lista de confianza ha fallado y no hay ninguna anterior.
7 - TL_FAILED	Error genérico.
8 - TL_FAILED_OLD_ITL	La actualización al nuevo ITL ha fallado, pero hay una lista de confianza anterior.
9 - TL_FAILED_OLD_TL	La actualización a la nueva lista de confianza ha fallado, pero hay una anterior.

El menú Configuración de seguridad proporciona información sobre varios ajustes de seguridad. También proporciona acceso al menú Lista de confianza e indica si el archivo CTL o ITL está instalado en el teléfono.

En la tabla siguiente se describen las opciones del menú Configuración de seguridad.

Tabla 26: Menú Configuración de seguridad

Opción	Descripción	Para cambiar
Modo de seguridad	Muestra el modo de seguridad que se establece para el teléfono.	En Cisco Unified Communications Manager Administration, seleccione Dispositivo > Teléfono . La configuración se muestra en el apartado de información específica del protocolo de la ventana de configuración del teléfono.
LSC	Indica si se ha instalado en el teléfono el certificado significativo local que se utiliza para las funciones de seguridad (Sí) o si no se ha instalado (No).	Para obtener información sobre cómo administrar el LSC del teléfono, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Opción	Descripción	Para cambiar
Lista de confianza	<p>El menú Lista de confianza incluye submenús para los archivos CTL, ITL y de configuración firmados.</p> <p>El submenú Archivo CTL muestra el contenido del archivo CTL. El submenú Archivo ITL muestra el contenido del archivo ITL.</p> <p>El menú Lista de confianza también muestra la información siguiente:</p> <ul style="list-style-type: none"> • Firma CTL: el hash SHA1 del archivo CTL. • Unified CM/Servidor TFTP: el nombre de la instancia de Cisco Unified Communications Manager y del servidor TFTP que usa el teléfono. Muestra un icono de certificado si este se ha instalado para este servidor. • Servidor CAPF: el nombre del servidor CAPF que usa el teléfono. Muestra un icono de certificado si este se ha instalado para este servidor. • Router SRST: la dirección IP del router SRST de confianza que usa el teléfono. Muestra un icono de certificado si este se ha instalado para este servidor. 	<p>Para obtener más información, consulte Configuración de un certificado significativo local, en la página 93.</p>
Autenticación 802.1X	Permite habilitar la autenticación 802.1X para el teléfono.	Consulte Autenticación 802.1X, en la página 113 .

Temas relacionados

[Cisco Unified Communications Manager Documentación](#), en la página xv

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, presione **Aplicaciones** .

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.

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 solo en las conexiones entre dos teléfonos. Algunas funciones, como la llamada de conferencia y las líneas compartidas no se encuentran disponibles cuando se configura la llamada segura.


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 inició la llamada, los niveles de seguridad de los participantes y la disponibilidad de puentes de conferencia seguros.


Tabla 27: 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 mensaje rechazado si no cumple el nivel de seguridad, la llamada es 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. Se admiten ambos métodos de autenticación: PEAP-MSCHAPV2 y PEAP-GTC.

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 autentifiquen 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 28: Esquemas de autenticación y cifrado

Configuración del teléfono IP de Cisco	Configuración del punto de acceso			
	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
PEAP-GTC	PEAP-GTC	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>

Configuración del modo de autenticación

Para seleccionar el modo de autenticación para el perfil, siga estos pasos:

Procedimiento

Paso 1 Seleccione el perfil de red que desea configurar.

Paso 2 Seleccione el modo de autenticación.

Nota Según lo que seleccione, deberá configurar opciones adicionales en los apartados Seguridad inalámbrica o Cifrado inalámbrico. Para obtener más información, consulte [Seguridad de WLAN, en la página 97](#).

Paso 3 Haga clic en **Guardar** para aplicar el cambio.

Credenciales de seguridad inalámbrica

Si la red usa EAP-FAST y PEAP para la autenticación de usuario, debe configurar el nombre de usuario y contraseña si se requiere en el Servicio de autenticación remota de usuario por marcación (RADIUS) y en el teléfono.



Nota Si usa dominios en la red, debe introducir el nombre de usuario con el nombre de dominio con el formato: *dominio\nombreusuario*.

Las siguientes acciones podrían provocar que se borrara la contraseña Wi-Fi existente:

- Introducir un ID de usuario o contraseña no válidos
- Instalar una entidad de certificación raíz caducada cuando el tipo EAP se establece en PEAP-MSCHAPV2 o PEAP-GTC
- Desactivar el tipo EAP en el servidor RADIUS usado por el teléfono antes de cambiar un teléfono al nuevo tipo EAP

Para cambiar los tipos EAP, realice lo siguiente en el orden indicado:

- Active los nuevos tipos EAP en RADIUS.
- Cambie el tipo EAP en un teléfono para el nuevo tipo EAP.

Mantenga el tipo EAP actual configurado en el teléfono hasta que el nuevo tipo EAP esté activado en el servidor RADIUS. Una vez que el nuevo tipo EP esté activado en el servidor RADIUS, podrá cambiar el tipo EAP del teléfono. Una vez que se hayan cambiado todos los teléfonos al nuevo tipo EAP, puede desactivar el tipo EAP anterior si lo desea.

Configuración del nombre de usuario y la contraseña

Para introducir o cambiar el nombre de usuario o la contraseña del perfil de red, debe usar el mismo nombre de usuario y la misma cadena de contraseña que se han configurado en el servidor RADIUS. La longitud máxima del nombre de usuario o la entrada de contraseña es de 64 caracteres.

Para configurar el nombre de usuario y la contraseña en las credenciales de seguridad inalámbrica, siga estos pasos:

Procedimiento

-
- Paso 1** Seleccione el perfil de red.
 - Paso 2** En el campo Nombre de usuario, introduzca el nombre de usuario de red de este perfil.
 - Paso 3** En el campo Contraseña, introduzca la cadena de contraseña de red de este perfil.
 - Paso 4** Haga clic en **Guardar** para aplicar el cambio.
-

Configuración de la clave precompartida

Use las secciones siguientes como guía para configurar claves precompartidas.

Formatos de clave precompartida

El teléfono IP de Cisco admite los formatos ASCII y hexadecimal. Debe usar uno de estos formatos para configurar una clave precompartida WPA:

Hexadecimal

Para las claves hexadecimales, debe introducir 64 dígitos hexadecimales (del 0 al 9 y de la A a la F); por ejemplo, AB123456789CD01234567890EFAB123456789CD01234567890EF3456789C

ASCII

Para las claves ASCII, puede introducir una cadena de caracteres con números del 0 al 9, letras de la A a la Z (en mayúsculas y minúsculas) o símbolos. La cadena debe tener entre 8 y 63 caracteres; por ejemplo, GREG12356789ZXYW

Configuración de PSK

Para configurar una PSK en la sección de credenciales inalámbricas, siga estos pasos:

Procedimiento

-
- Paso 1** Seleccione el perfil de red que habilita la clave precompartida WPA o la clave precompartida WPA2.
 - Paso 2** En el área de tipo de clave, introduzca la clave adecuada.
 - Paso 3** Introduzca una cadena ASCII o dígitos hexadecimales en el campo de Frase de contraseña/Clave precompartida.
 - Paso 4** Haga clic en **Guardar** para aplicar el cambio.
-

Cifrado inalámbrico

Si la red inalámbrica usa cifrado WEP y como modo de autenticación establece Abierto + WEP, debe introducir una clave WEP ASCII o hexadecimal.

Las claves WEP para el teléfono deben coincidir con las que haya asignadas al punto de acceso. Tanto el teléfono IP de Cisco como los puntos de acceso Aironet de Cisco admiten claves de cifrado tanto de 40 como de 128 bits.

Formatos de teclas WEP

Debe usar uno de estos formatos para configurar una clave WEP:

Hexadecimal

Para las claves hexadecimales, se usa uno de los tamaños siguientes:

40 bits

Se introduce una cadena de clave de cifrado de 10 dígitos hexadecimales (del 0 al 9 y de la A a la F); por ejemplo, ABCD123456.

128 bits

Se introduce una cadena de clave de cifrado de 26 dígitos hexadecimales (del 0 al 9 y de la A a la F); por ejemplo, AB123456789CD01234567890EF.

ASCII

Para las claves ASCII, puede introducir una cadena de caracteres con números del 0 al 9, letras de la A a la Z (en mayúsculas y minúsculas) o cualquier símbolo, con uno de los tamaños siguientes:

40 bits

Debe introducir una cadena de 5 caracteres; por ejemplo, GREG5.

128 bits

Debe introducir una cadena de 13 caracteres; por ejemplo, GREGSSECRET13.

Configuración de teclas WEP

Para configurar claves WEP, siga estos pasos.

Procedimiento

-
- Paso 1** Seleccione el perfil de red que use Abierto+WEP o Compartido+WEP.
- Paso 2** En el área de tipo de clave, introduzca la clave adecuada.
- Paso 3** En la sección de tamaño de clave, seleccione una de las longitudes de cadena de caracteres siguientes:
- 40
 - 128
- Paso 4** En el campo Clave de cifrado, introduzca la cadena de clave adecuada según el tipo y el tamaño de clave que haya seleccionado. Consulte [Formatos de teclas WEP, en la página 103](#).
- Paso 5** Haga clic en **Guardar** para aplicar el cambio.
-

Exportación del certificado de CA desde ACS mediante Microsoft Certificate Services

Exporte el certificado CA raíz del servidor de ACS. Para obtener información adicional, consulte la documentación de entidad emisora de certificados o RADIUS.

Certificado instalado en fábrica

Cisco incluye de fábrica en el teléfono un certificado instalado de fabricación (MIC).

Durante la autenticación EAP-TLS, el servidor ACS debe verificar la confianza del teléfono y viceversa.

Para verificar el MIC, el certificado raíz de fabricación y el certificado de autoridad certificadora de fabricación deben exportarse desde un teléfono IP de Cisco e instalarse en el servidor Cisco ACS. Estos dos certificados forman parte de la cadena de certificado de confianza que el servidor Cisco ACS usa para verificar el MIC.

Para verificar el certificado Cisco ACS, se deben exportar e instalar en el teléfono un certificado subordinado de confianza (si lo hubiera) y un certificado raíz (creado por una autoridad certificadora) del servidor Cisco ACS. Estos certificados forman parte de la cadena de certificado de confianza que el servidor ACS usa para verificar la confianza del certificado.

Certificado instalado por el usuario

Para usar un certificado instalado por el usuario, se genera una solicitud de firma de certificado (CSR) y se envía para que la autoridad certificadora la apruebe. También puede generar un certificado de usuario por la CA sin un CSR.

Durante la autenticación EAP-TLS, el servidor ACS verifica la confianza del teléfono y viceversa.

Para verificar la autenticidad del certificado instalado por el usuario, debe instalar un certificado subordinado de confianza (si lo hubiera) y el certificado raíz de la autoridad certificadora que aprobó el certificado de usuario en el servidor Cisco ACS. Estos certificados forman parte de la cadena de certificado de confianza que se usa para verificar la confianza del certificado instalado por el usuario.

Para verificar el certificado Cisco ACS, se exporta e instala en el teléfono un certificado subordinado de confianza (si lo hubiera) y un certificado raíz (creado por una autoridad certificadora) del servidor Cisco ACS. Estos certificados forman parte de la cadena de certificado de confianza que el servidor ACS usa para verificar la confianza del certificado.

Instalación de certificados de autenticación EAP-TLS

Para instalar certificados de autenticación para EAP-TLS, lleve a cabo los pasos siguientes.

Procedimiento

-
- Paso 1** En la página web del teléfono, defina la fecha y la hora de Cisco Unified Communications Manager en el teléfono.
- Paso 2** Si usa el certificado instalado por el fabricante (MIC):
- En la página web del teléfono, exporte el certificado raíz de la autoridad certificadora y el certificado de autoridad certificadora de fabricación.
 - En Internet Explorer, instale los certificados en el servidor Cisco ACS y edite la lista de confianza.
 - Importe la CA raíz al teléfono.
- Para obtener más información, consulte:
- [Exportación e instalación de certificados en ACS, en la página 105](#)
 - [Exportación del certificado de CA desde ISE mediante Microsoft Certificate Services, en la página 106](#)
- Paso 3** Con la herramienta de configuración de ACS, configure la cuenta de usuario.

Para obtener más información, consulte:

- [Configuración de la cuenta de usuario de ACS e instalación del certificado, en la página 107](#)
- *Guía del usuario de Cisco Secure ACS para Windows* (<http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html>)

Definición de fecha y hora

EAP-TLS usa la autenticación basada en certificado, para la que se requiere que el reloj interno del teléfono IP de Cisco esté correctamente definido. La fecha y la hora del teléfono pueden cambiar si este se registra con Cisco Unified Communications Manager.



Nota Si se va a solicitar un certificado de autenticación de servidor nuevo y la hora local es anterior a la hora media de Greenwich (GMT), la validación del certificado de autenticación podría fallar. Cisco recomienda establecer la fecha y la hora local posterior a la hora GMT.

Para establecer la fecha y hora local correcta en el teléfono, siga estos pasos.

Procedimiento

- Paso 1** Seleccione **Fecha y hora** en el panel de navegación de la izquierda.
 - Paso 2** Si el ajuste del campo Fecha y hora actuales del teléfono es distinto al del campo Fecha y hora local, haga clic en **Definir la fecha y hora local en el teléfono**.
 - Paso 3** Haga clic en **Reinicio del teléfono** y en **Aceptar**.
-

Exportación e instalación de certificados en ACS

Para usar el MIC, exporte el certificado raíz de fabricación y el certificado de autoridad certificadora de fabricación e instálelos en el servidor Cisco ACS.

Para exportar el certificado raíz de fabricación y el certificado de autoridad certificadora de fabricación al servidor ACS, siga estos pasos.

Procedimiento

- Paso 1** En la página web del teléfono, seleccione **Certificados**.
- Paso 2** Haga clic en la opción **Exportar** situada junto al certificado raíz de fabricación.
- Paso 3** Guarde el certificado y cópielo en el servidor ACS.
- Paso 4** Repita los pasos 1 y 2 para el certificado de autoridad certificadora de fabricación.
- Paso 5** En la página de configuración del sistema del servidor ACS, introduzca la vía de cada certificado e instale los certificados.

Nota Para obtener más información sobre cómo usar la herramienta de configuración de ACS, consulte la ayuda en línea de ACS o la *Guía del usuario de Cisco Secure ACS para Windows* (<http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html>).

Paso 6 Use la página para editar la lista de certificados de confianza (CTL) para agregar los certificados de confianza de ACS.

Métodos de exportación de certificados de ACS

Según el tipo de certificado que exporte desde ACS, use uno de los métodos siguientes:

- Para exportar el certificado de CA del servidor ACS que firmó el certificado instalado por el usuario o el certificado de ACS, consulte [Exportación del certificado de CA desde ISE mediante Microsoft Certificate Services](#), en la página 106.
- Para exportar el certificado de CA desde el servidor ACS que usa el certificado autofirmado, consulte [Exportación del certificado de CA desde ACS mediante Internet Explorer](#), en la página 106.

Exportación del certificado de CA desde ISE mediante Microsoft Certificate Services

Use este método para exportar el certificado de CA del servidor ISE que firmó el certificado instalado por el usuario o el certificado de ISE.

Para exportar el certificado de CA mediante la página web Microsoft Certificate Services, siga estos pasos.

Procedimiento

- Paso 1** En la página web Microsoft Certificate Services, seleccione **Descargar certificado de CA, cadena de certificados o CRL**.
- Paso 2** En la página siguiente, resalte el certificado de CA actual en el cuadro de texto, seleccione DER en Método de codificación y haga clic en **Descargar certificado de CA**.
- Paso 3** Guarde el certificado de CA.

Exportación del certificado de CA desde ACS mediante Internet Explorer

Use este método para exportar el certificado de CA desde el servidor ACS que usa el certificado autofirmado.

Para exportar certificados desde el servidor ACS mediante Internet Explorer, siga estos pasos.

Procedimiento

- Paso 1** En Internet Explorer, seleccione **Herramientas > Opciones de Internet** y haga clic en la pestaña Contenido.
- Paso 2** En Certificados, haga clic en **Certificados** y, seguidamente, en la pestaña Entidades de certificación raíz de confianza.
- Paso 3** Resalte el certificado raíz y haga clic en **Exportar**. Se abre el Asistente para exportación de certificados.
- Paso 4** Haga clic en **Siguiente**.

- Paso 5** En la próxima ventana, seleccione **DER binario codificado X.509 (.CER)** y haga clic en **Siguiente**.
- Paso 6** Especifique un nombre para el certificado y haga clic en **Siguiente**.
- Paso 7** Guarde el certificado de CA que se va a instalar en el teléfono.
-

Solicitud e importación de certificados instalados por el usuario

Para solicitar e instalar el certificado en el teléfono, siga estos pasos.

Procedimiento

- Paso 1** En la página web del teléfono, seleccione el perfil de red que usa EAP-TLS y la opción Usuario instalado en el campo Certificado EAP-TLS.
- Paso 2** Haga clic en **Certificados**.
- En la página de instalación del certificado de usuario, el campo Nombre común debe coincidir con el nombre de usuario del servidor ACS.
- Nota** Si lo desea, puede modificar el campo Nombre común. Asegúrese de que coincide con el nombre de usuario del servidor ACS. Consulte [Configuración de la cuenta de usuario de ACS e instalación del certificado, en la página 107](#).
- Paso 3** Introduzca la información que se debe mostrar en el certificado y haga clic en **Enviar** para generar la solicitud de firma del certificado (CSR).
-

Instalación del certificado raíz del servidor de autenticación

Para instalar el certificado raíz del servidor de autenticación en el teléfono, siga estos pasos.

Procedimiento

- Paso 1** Exporte el certificado raíz del servidor de autenticación desde ACS. Consulte [Métodos de exportación de certificados de ACS, en la página 106](#).
- Paso 2** Diríjase a la página web del teléfono y seleccione **Certificados**.
- Paso 3** Haga clic en la opción **Importar** situada junto al certificado raíz del servidor de autenticación.
- Paso 4** Reinicie el teléfono.
-

Configuración de la cuenta de usuario de ACS e instalación del certificado

Para configurar el nombre de la cuenta de usuario e instalar el certificado raíz MIC para el teléfono en ACS, siga estos pasos.



- Nota** Para obtener más información sobre cómo usar la herramienta de configuración de ACS, consulte la ayuda en línea de ACS o la *Guía del usuario de Cisco Secure ACS para Windows*.
-

Procedimiento

- Paso 1** En la página Configuración del usuario de la herramienta de configuración de ACS, cree un nombre de cuenta de usuario de teléfono, en caso de que aún no se haya configurado.
- Habitualmente, el nombre de usuario incluye la dirección MAC del teléfono al final. No es necesaria una contraseña para EAP-TLS.
- Nota** Asegúrese de que el nombre de usuario coincide con el campo Nombre común de la página de instalación del certificado de usuario. Consulte [Solicitud e importación de certificados instalados por el usuario, en la página 107](#).
- Paso 2** En la página Configuración de sistema, en la sección EAP-TLS, active estos campos:
- **Permitir EAP-TLS**
 - **Comparación del nombre común del certificado**
- Paso 3** En la página de configuración de la autoridad certificadora de ACS, agregue el certificado raíz de fabricación y el certificado de autoridad certificadora de fabricación al servidor ACS.
- Paso 4** Active ambos certificados en la lista de confianza de certificados de ACS.
-

Configuración PEAP

El protocolo de autenticación ampliable protegido (PEAP) usa certificados de clave pública en el servidor para autenticar a los clientes mediante la creación de un túnel SSL/TLS cifrado entre el cliente y el servidor de autenticación.

El teléfono IP 8865 de Cisco solo es compatible con un certificado de servidor que se puede instalar a través de SCEP o el método de instalación manual, pero no ambas. El teléfono no es compatible con el método TFTP de instalación de certificados.



Nota Para activar la validación del servidor de autenticación, importe el certificado de servidor de autenticación.

Antes de comenzar

Antes de configurar la autenticación PEAP para el teléfono, asegúrese de que se cumplen estos requisitos de Cisco Secure ACS:

- El certificado raíz de ACS debe estar instalado.
- También se puede instalar un certificado para activar la validación del servidor de PEAP. Sin embargo, si está instalado un certificado de servidor se habilitará la validación del servidor.
- El ajuste Permitir EAP-MSCHAPv2 debe estar activado.
- La cuenta del usuario y la contraseña deben estar configuradas.
- Para la autenticación por contraseña, puede usar la base de datos local de ACS o una externa (como Windows o LDAP).

Habilitación de la autenticación PEAP

Procedimiento

-
- Paso 1** En la página web de configuración del teléfono, seleccione PEAP como modo de autenticación.
- Paso 2** Introduzca un nombre de usuario y contraseña.
-

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.

Temas relacionados

[Página web del teléfono IP de Cisco](#), en la página 239

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.
 - En el teléfono, pulse **Aplicaciones** , seleccione **Información del teléfono** 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:


```
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** Localice el campo Instalación del usuario y haga clic en **Instalar**.
- Paso 3** Busque el certificado en su PC.
- Paso 4** En el campo **Extraer contraseña**, introduzca la contraseña de extracción del certificado.
- Paso 5** Haga clic en **Subir**.
- Paso 6** 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. CDP no identifica localmente las estaciones de trabajo conectadas. Los teléfonos IP de Cisco proporcionan un mecanismo de pasarela EAPOL. Este mecanismo permite a una estación de trabajo conectada al teléfono IP de Cisco transferir mensajes EAPOL al autenticador 802.1X en el switch LAN. El mecanismo de pasarela garantiza que el teléfono IP actúa como switch LAN para autenticar un terminal de datos antes de acceder a la red.

Los teléfonos IP de Cisco también incluyen un mecanismo de cierre de sesión de EAPOL por proxy. En caso de que el PC conectado localmente se desconecte del teléfono IP, el switch de LAN no sufre un error de enlace físico, ya que el enlace entre este switch LAN y el teléfono IP se conserva. Para evitar poner en peligro la integridad de la red, el teléfono IP envía un mensaje de cierre de sesión de EAPOL al switch en nombre del PC conectado más adelante, lo que desencadena que el switch LAN borre la entrada de autenticación de ese PC.

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 IP de Cisco incluyen un solicitante de 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.

- Cisco Secure Access Control Server (ACS) u otro servidor de autenticación de terceros: tanto el servidor de autenticación como el teléfono deben estar configurados con un secreto compartido que autentique el teléfono.
- 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 el puerto PC: el estándar 802.1X no tiene en cuenta las VLAN y, por lo tanto, se recomienda que solo se autentique un único dispositivo en un puerto switch específico. Sin embargo, algunos switches (incluidos los switches Cisco Catalyst) admiten la autenticación multidominio. La configuración del switch determina si es posible conectar un PC al puerto PC del teléfono.
 - Activado: si usa un switch que admite la autenticación multidominio, puede activar el puerto PC y conectar en él un PC. En tal caso, los teléfonos IP de Cisco admiten el cierre de sesión de EAPOL por proxy para supervisar los intercambios de autenticación entre el switch y el PC conectado. Para obtener más información sobre la compatibilidad con IEEE 802.1X en los switches Cisco Catalyst, consulte las guías de configuración del switch Cisco Catalyst en:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
 - Desactivado: si el switch no admite varios dispositivos 802.1X en el mismo puerto, debe desactivar el puerto PC en caso de que la autenticación 802.1X esté activada. Si no desactiva este puerto e intenta conectar en él un PC, el switch deniega el acceso a red tanto del teléfono como del PC.
- 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.

Acceso a la autenticación 802.1X

Para acceder a los valores de la autenticación 802.1X, siga estos pasos:

Procedimiento

-
- Paso 1** Presione **Aplicaciones** .
 - Paso 2** Seleccione **Config. admin. > Configuración de seguridad > Autenticación 802.1X**.
 - Paso 3** Configure las opciones según se describe en [Opciones de autenticación 802.1X](#), en la página 114.
 - Paso 4** Para salir del menú, pulse **Salir**.
-

Opciones de autenticación 802.1X


En la tabla siguiente se describen las opciones de autenticación 802.1X.

Tabla 29: Opciones de autenticación 802.1X

Opción	Descripción	Para cambiarla
Autenticación del dispositivo	<p>Determina si la autenticación 802.1X está habilitada.</p> <ul style="list-style-type: none"> • Activado: el teléfono usa la autenticación 802.1X para solicitar acceso a la red. • Desactivado: valor predeterminado. El teléfono usa CDP para acceder a la VLAN y la red. 	Consulte Establecimiento del campo Autent. dispositivo , en la página 115.
Estado de transacción	<p>Estado: muestra el estado de la autenticación 802.1x.</p> <ul style="list-style-type: none"> • Desconectado: indica que la autenticación 802.1x no está configurada en el teléfono. • Autenticado: indica que el teléfono está autenticado. • En espera: indica que el proceso de autenticación está en curso. <p>Protocolo: muestra el método EAP que se usa para la autenticación 802.1x (puede ser EAP-FAST o EAP-TLS).</p>	Solo visualización. No es posible

Establecimiento del campo Autent. dispositivo

Procedimiento

-
- Paso 1** Presione **Aplicaciones** .
- Paso 2** Seleccione **Config. admin.** > **Configuración de seguridad** > **Autenticación 802.1X**
- Paso 3** Establezca la opción Autenticación del dispositivo:
- Sí
 - No
- Paso 4** Presione **Aplicar**.
-



CAPÍTULO 8

Personalización del teléfono IP de Cisco

- Personalización de timbres del teléfono, en la página 117
- Imágenes de fondo personalizadas, en la página 117
- Configuración del códec de banda ancha, en la página 119
- Configuración de la pantalla de inactividad, en la página 120
- Personalizar el tono de marcado, en la página 121

Personalización de timbres del teléfono

El teléfono incluye tres tonos de timbre implementados en el hardware: Sunshine, Chirp y Chirp1.

Cisco Unified Communications Manager también proporciona un juego predeterminado de sonidos de timbre 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 (denominado Ringlist-wb.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 usa Ringlist-wb.xml como nombre de archivo, el teléfono no aplicará los cambios que realice.

Para obtener más información, consulte el capítulo sobre personalización de tonos de llamada y fondos, [Guía de configuración de funciones de Cisco Unified Communications Manager](#) para Cisco Unified Communications Manager versión 12.0(1) o posterior.

Imágenes de fondo personalizadas

Puede personalizar una imagen de fondo de un teléfono IP de Cisco o un fondo de pantalla. Los fondos de pantalla personalizados son una forma popular de mostrar logotipos o imágenes corporativas y muchas organizaciones los utilizan para que los teléfonos destaquen.

A partir de la versión de firmware 12.7(1), se puede personalizar el fondo de pantalla tanto en los teléfonos como en los módulos de expansión de teclas. Pero necesita una imagen para el teléfono y una imagen para el módulo de expansión.

El teléfono analiza los colores del fondo de pantalla y cambia los colores de las fuentes y los iconos para que pueda leerlos. Si el fondo de pantalla es oscuro, el teléfono cambiará las fuentes e iconos a blanco. Si el fondo de pantalla es luminoso, el teléfono muestra las fuentes e iconos en color negro.

Es mejor elegir una imagen sencilla como un color sólido o un patrón para el fondo. Evite las imágenes de alto contraste.

Puede agregar un fondo de pantalla personalizado de dos maneras:

- Usando el archivo de lista
- Usando un perfil de teléfono común

Si desea que el usuario pueda seleccionar la imagen de diversos fondos de pantalla disponibles en el teléfono, modifique el archivo de lista. Sin embargo, si desea insertar la imagen en el teléfono, cree o modifique un perfil de teléfono común.

Independientemente del método, tenga en cuenta lo siguiente:

- Las imágenes deben estar en formato PNG y la imagen de tamaño completa debe tener las siguientes dimensiones:
 - Imágenes de miniatura: 139 píxeles (ancho) por 109 píxeles (alto).
 - Teléfono IP serie 8800 de Cisco: 800 por 480 píxeles
 - Módulo de expansión de teclas del teléfono IP de Cisco con una única pantalla LCD: 272 por 480 píxeles
 - Módulo de expansión de teclas del teléfono IP 8865 de Cisco con una pantalla LCD doble: 320 por 480 píxeles
 - Módulo de expansión de teclas del teléfono IP serie 8800 de Cisco con una única pantalla LCD: 272 por 480 píxeles
- Cargue las imágenes, las miniaturas y el archivo de lista en el servidor TFTP. El directorio es el siguiente:
 - Teléfono IP serie 8800 de Cisco: ordenadores de sobremesa/800x480x24
 - Módulo de expansión de teclas del teléfono IP de Cisco con una única pantalla LCD: ordenadores de sobremesa/320x480x24
 - Módulo de expansión de teclas del teléfono IP 8865 de Cisco con una pantalla LCD doble: ordenadores de sobremesa/320x480x24
 - Módulo de expansión de teclas del teléfono IP serie 8800 de Cisco con una única pantalla LCD: ordenadores de sobremesa/272x480x24

Reinicie el servidor TFTP una vez que se complete la carga.

- Si no desea que el usuario seleccione su propio fondo de pantalla, desactive **Activar acceso del usuario final a la configuración de imagen de fondo del teléfono**. Guarde y aplique el perfil del teléfono. Reinicie los teléfonos para que se apliquen los cambios.



Nota Puede aplicar las imágenes de fondo del teléfono de forma masiva con el **Perfil de teléfono común**. Sin embargo, la configuración masiva requiere desactivar la opción **Activar acceso del usuario final a imagen de fondo del teléfono**. Para obtener más información sobre la configuración masiva de imágenes de fondo, consulte el capítulo «Configuración del perfil de teléfono común» de [Mejores prácticas de fondos de pantalla personalizados del teléfono IP serie 8800 de Cisco](#).)

Para obtener más información sobre la personalización del fondo de pantalla, consulte la siguiente documentación:

- [Mejores prácticas de fondos de pantalla personalizados del teléfono IP serie 8800 de Cisco](#)).
- Capítulo sobre personalización de tonos de llamada y fondos, [Guía de configuración de funciones de Cisco Unified Communications Manager](#) para Cisco Unified Communications Manager versión 12.0(1) o posterior.
- Capítulo «Configuración» en la *Guía del usuario del teléfono IP serie 8800 de Cisco*.

Configuración del códec de banda ancha

De forma predeterminada, el códec G.722 está habilitado para el teléfono IP de Cisco. Si Cisco Unified Communications Manager se ha configurado para usar G.722 y el terminal lejano admite este códec, la llamada se conecta mediante el códec G.722 en lugar de con el G.711.

Esta situación se produce independientemente de si el usuario ha habilitado unos auriculares de banda ancha o un auricular de mano de banda ancha; pero si se han habilitado tanto un auricular de mano como unos auriculares, puede que el usuario note una mayor sensibilidad del audio durante la llamada. Una mayor sensibilidad significa más claridad del audio, pero también que el terminal lejano oírá más ruido de fondo, como el crujido de los papeles o las conversaciones cercanas. Incluso sin un auricular o unos auriculares de banda ancha, algunos usuarios pueden encontrar la sensibilidad adicional del códec G.722 molesta. Otros usuarios, sin embargo, pueden preferirla.

El parámetro de servicio Anunciar los códecs G.722 e iSAC indica si la compatibilidad con la banda ancha afecta a todos los dispositivos que se registren con este servidor de Cisco Unified Communications Manager o solo a un teléfono concreto, dependiendo de la ventana Cisco Unified Communications Manager Administration en la que se haya configurado el parámetro.

Procedimiento

Paso 1 Para configurar la compatibilidad de banda ancha para todos los dispositivos:

- a) En Cisco Unified Communications Manager Administration, seleccione **Sistema > Parámetros empresariales**.
- b) Establezca el campo Anunciar los códecs G.722 e iSAC.

El valor predeterminado para este parámetro empresarial es **Verdadero**, que indica que todos los modelos de teléfonos IP de Cisco que se registren en esta instancia de Cisco Unified Communications Manager anunciarán el códec G.722 a Cisco Unified Communications Manager. Si todos los terminales de la

llamada intentada admiten G.722 en su conjunto de capacidades, Cisco Unified Communications Manager selecciona ese códec para la llamada siempre que sea posible.

Paso 2 Para configurar la compatibilidad de banda ancha para un dispositivo específico:

- a) En Cisco Unified Communications Manager Administration, seleccione **Dispositivo > Teléfono**.
- b) Establezca el parámetro Anunciar los códec G.722 e iSAC en el área de configuración específica del producto.

El valor predeterminado para este parámetro específico del producto es usar el valor especificado en el parámetro empresarial. Si desea sustituir este valor en cada teléfono, seleccione **Activado** o **Desactivado**

Configuración de la pantalla de inactividad

Es posible especificar una pantalla de inactividad (solo de texto; el tamaño del archivo de texto no debe superar 1 millón de bytes) para que aparezca en la pantalla del teléfono. Esta pantalla es un servicio XML que el teléfono invoca cuando está inactivo (no está en uso) durante un período indicado cuando no hay ningún menú de función abierto.

Para obtener instrucciones detalladas sobre la creación y visualización de la pantalla de inactividad, consulte *Creating Idle URL Graphics on Cisco IP Phone* (Creación de gráficos de URL inactiva en el teléfono IP de Cisco) en esta URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801c0764.shtml

Consulte también en la documentación de su versión concreta de Cisco Unified Communications Manager la siguiente información:

- Especificación de la URL del servicio XML de pantalla de inactividad:
 - Para un solo teléfono: campo Inactivo de la ventana de configuración del teléfono en Cisco Unified Communications Manager Administration.
 - Para varios teléfonos simultáneamente: campo URL inactiva en la ventana de configuración de parámetros empresariales o el campo Inactivo de la Herramienta de administración por lotes (BAT)
- Especificación del período que el teléfono no debe estar en uso antes de que se invoque el servicio XML de pantalla de inactividad:
 - Para un solo teléfono: campo Tiempo de inactividad de la ventana de configuración del teléfono en Cisco Unified Communications Manager Administration.
 - Para varios teléfonos simultáneamente: campo Tiempo de inactividad de URL en la ventana de configuración de parámetros empresariales o el campo Tiempo de inactividad de la Herramienta de administración por lotes (BAT).

Procedimiento

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

Paso 2 En el campo Inactivo, introduzca la URL del servicio XML de pantalla de inactividad.

- Paso 3** En el campo Tiempo de inactividad, introduzca el tiempo que el teléfono inactivo debe esperar antes de mostrar el servicio XML de pantalla de inactividad.
- Paso 4** Seleccione **Guardar**.
-

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

Características y configuración del teléfono

- Descripción general de las características y la configuración del teléfono, en la página 123
- Asistencia para usuarios del teléfono IP de Cisco, en la página 124
- Funciones del teléfono, en la página 124
- Botones de función y teclas programadas, en la página 142
- Configuración de funciones del teléfono, en la página 144
- Configuración de la plantilla de teclas programadas, en la página 199
- Plantillas de botones de teléfono, en la página 201
- Configuración de VPN, en la página 204
- Configuración de teclas de línea adicionales, en la página 205
- Configuración del temporizador de reanudación de TLS, en la página 209
- Activación de Intelligent Proximity, en la página 209
- Configuración de la resolución de transmisión del vídeo, en la página 210
- Administración de los auriculares en versiones anteriores de Cisco Unified Communications Manager, en la página 211

Descripción general de las características y la configuración del teléfono

Después de instalar teléfonos IP de Cisco en la red, configurar sus ajustes de red y agregarlos a Cisco Unified Communications Manager, debe usar la aplicación Administración de Cisco Unified Communications Manager para configurar las características de telefonía, modificar opcionalmente las plantillas del teléfono, establecer servicios y asignar usuarios.

Puede modificar ajustes adicionales para el teléfono IP de Cisco en Administración de Cisco Unified Communications Manager. Use esta aplicación basada en web para configurar los criterios de registro del teléfono y los espacios de búsqueda de llamadas, para configurar directorios corporativos y servicios y para modificar las plantillas de botones del teléfono, entre otras tareas.

Al agregar funciones a las teclas de línea telefónica, habrá una limitación en el número de teclas de línea disponibles. No podrá agregar más funciones que el número de teclas de línea del teléfono.

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.

Funciones del teléfono

Después de agregar teléfonos IP de Cisco a Cisco Unified Communications Manager, puede agregar funciones a esos teléfonos. En la tabla siguiente se incluye una lista de las funciones de telefonía admitidas, muchas de las cuales se pueden configurar mediante Cisco Unified Communications Manager Administration.

Para obtener información sobre el uso de la mayoría de estas funciones en el teléfono, consulte la *Guía del usuario de los teléfonos IP serie 8800 de Cisco*. Consulte [Botones de función y teclas programadas](#), en la [página 142](#) para obtener una lista de las funciones que se pueden configurar como botones programables, además de como teclas programadas y botones de función.



Nota Cisco Unified Communications Manager Administration también proporciona varios parámetros de servicio que se pueden emplear para configurar diversas funciones de telefonía. Para obtener más información sobre cómo acceder y configurar los parámetros de servicio, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Para obtener más información sobre las funciones de un servicio, seleccione el nombre del parámetro o el botón de **ayuda con el signo de interrogación (?)** en la ventana de [Configuración específica del producto](#).

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

Función	Descripción e información adicional
Marcación abreviada	<p>Permite a los usuarios marcar rápidamente un número de teléfono introduciendo un código de índice asignado (del 1 al 199) en el teclado del teléfono.</p> <p>Nota Puede usar la marcación abreviada con el auricular colgado o descolgado.</p> <p>Los usuarios asignan los códigos de índice desde el portal de autoayuda.</p>
Alerta de llamada entrante con acciones	<p>Ofrece varias opciones para controlar las alertas de llamada entrante. Es posible activar o desactivar la alerta de llamada. También se puede activar o desactivar la presentación del ID de la persona que llama.</p> <p>Consulte Alerta de llamada entrante con acciones, Configuración específica del producto, en la página 146.</p>
Compatibilidad con cifrado AES 256 para teléfonos	<p>Mejora la seguridad al admitir TLS 1.2 y nuevos cifrados. Para obtener más información, consulte Características de seguridad admitidas, en la página 88.</p>
Saludo de agente	<p>Permite a un agente crear y actualizar un saludo pregrabado que se reproduce al inicio de una llamada de un cliente antes de que el agente inicie la conversación con quien ha realizado la llamada. El agente puede pregrabar un mensaje sencillo o múltiples mensajes, según sea necesario.</p> <p>Consulte Activación del saludo de agente, en la página 177.</p>
Captura de cualquier llamada	<p>Permite a los usuarios capturar una llamada en cualquier línea de su grupo de captura de llamadas, independientemente de la forma en la que esta se enrute al teléfono.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre la captura de llamadas.</p>
Reglas de marcación de la aplicación	<p>Convierte los números de los contactos móviles compartidos en números que se pueden marcar en la red.</p> <p>Consulte Reglas de marcación de la aplicación, en la página 80.</p>
Aparcamiento asistido de llamadas dirigido	<p>Permite a los usuarios aparcar una llamada presionando solo un botón mediante la función de aparcamiento directo. Los administradores deben configurar un botón de aparcamiento asistido de llamadas dirigido del campo Indicador luminoso de ocupación (BLF). Si los usuarios presionan un botón de este tipo para una llamada activa, esta se aparca en el espacio de aparcamiento directo asociado con ese botón.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el aparcamiento asistido de llamadas dirigido.</p>
Indicador sonoro de mensaje en espera	<p>Un tono intermitente en el auricular de mano, los auriculares o el altavoz indica que un usuario tiene nuevos mensajes de voz en una línea.</p> <p>Nota El tono entrecortado es específico de cada línea. Solo lo oírás cuando utilice la línea que tenga los mensajes en espera.</p>

Función	Descripción e información adicional
Contestación automática	<p>Conecta las llamadas entrantes automáticamente después de un timbre o dos.</p> <p>La función Contestación automática funciona con el altavoz o con los auriculares.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el número de directorio.</p>
Sincronización de puerto automática	<p>Sincroniza los puertos a la velocidad más baja entre los puertos de un teléfono para eliminar la pérdida de paquetes.</p> <p>Consulte Sincronización de puerto automática, Configuración específica del producto, en la página 146.</p>
Captura automática	<p>Permite a un usuario usar la característica de captura con un toque para las funciones de captura de llamadas.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre la captura de llamadas.</p>
Intrusión	<p>Permite a un usuario efectuar una intrusión en una llamada estableciendo una llamada de conferencia entre tres partes mediante el puente de conferencia integrado del teléfono de destino.</p> <p>Consulte «IntruCf» en esta tabla.</p>
Bloquear transferencia externa a externa	<p>Impide que los usuarios puedan transferir una llamada externa a otro número externo.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre la transferencia de llamadas externas.</p>
Multiconexión Bluetooth	<p>Permite al usuario vincular varios dispositivos al teléfono. El usuario puede conectar un dispositivo móvil mediante Bluetooth y unos auriculares Bluetooth al mismo tiempo.</p> <p>El teléfono IP 8851NR de Cisco no admite Bluetooth.</p>
Busy Lamp Field (BLF)	<p>Permite a un usuario supervisar el estado de la llamada de un número de directorio asociado con un botón de marcación rápida del teléfono.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre la presencia.</p>
Captura de Busy Lamp Field (BLF)	<p>Aporta mejoras para la marcación rápida de BLF. Permite configurar un número de directorio (DN) donde un usuario puede controlar si hay llamadas entrantes. Si el número de directorio recibe una llamada entrante, el sistema alerta al usuario supervisor, que puede capturar la llamada.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre la captura de llamadas.</p>
Devolver llamada	<p>Proporciona a los usuarios una alerta visual y sonora en el teléfono cuando un interviniente ocupado o no disponible vuelve a estar disponible.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre la devolución de llamadas.</p>

Función	Descripción e información adicional
Restricciones de visualización de llamadas	<p>Determina la información que se mostrará sobre las líneas de llamada o las conectadas, según las partes implicadas en la llamada.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre los planes de enrutamiento y la restricción para visualizar llamadas.</p>
Desviar una llamada	<p>Permite a los usuarios redirigir las llamadas entrantes a otro número. Las opciones de desvío de llamadas son: Desvío incondicional, Desviar si ocupado, Desvío si no hay respuesta y Desvío si no hay cobertura.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el número de directorio y Personalización de la presentación del portal de autoayuda, en la página 84.</p>
Detalles de bucles de desvío incondicional	<p>Detecta y previene los bucles del desvío incondicional. Cuando se detecta un bucle de desvío incondicional, la configuración de la función Desvío incondicional se omite y la llamada suena.</p>
Prevención de bucles de desvío incondicional	<p>Detecta y previene los bucles del desvío incondicional. Cuando se detecta un bucle de desvío incondicional, la configuración de la función Desvío incondicional se omite y la llamada suena.</p>
Visualización configurable de desvío de llamadas	<p>Evita que un usuario pueda configurar un destino de desvío incondicional directamente en el teléfono que cree un bucle de desvío incondicional o una cadena de desvíos incondicionales con más saltos que los permitidos por el parámetro de servicio Número máximo de saltos de desvío existente.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el número de directorio.</p>
Anulación de destino de desvío de llamadas	<p>Permite anular la función Desvío incondicional si el destino de ese desvío efectúa una llamada a la persona que inició el desvío incondicional. Esta función permite que el destino del desvío incondicional se ponga en contacto con la persona que inició el desvío en caso de llamadas importantes. La anulación funciona tanto si el número de teléfono del destino del desvío incondicional es interno como si es externo.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el número de directorio.</p>
Notificación de desvío de llamadas	<p>Permite configurar la información que el usuario verá al recibir una llamada desviada.</p> <p>Consulte Configuración de la notificación de desvío de llamadas, en la página 178.</p>
Historial de llamadas de una línea compartida	<p>Permite ver la actividad de la línea compartida en el historial de llamadas del teléfono. Mediante esta función es posible:</p> <ul style="list-style-type: none"> • registrar llamadas perdidas de una línea compartida, • registrar todas las llamadas contestadas y efectuadas de una línea compartida.

Función	Descripción e información adicional
Aparcamiento de llamadas	<p>Permite a los usuarios aparcar (almacenar temporalmente) una llamada y recuperarla más adelante en un teléfono distinto del sistema Cisco Unified Communications Manager.</p> <p>Puede configurar el campo Dedicar una línea para aparcar llamadas en el panel Diseño de configuración específica de producto para aparcar la llamada en la línea original o en otra línea.</p> <p>Cuando el campo está activado, la llamada aparcada permanece en la línea del usuario y puede usar la tecla programada Reanudar para capturar la llamada. El usuario verá el número de extensión de la llamada aparcada en la pantalla del teléfono.</p> <p>Cuando el campo está desactivado, la llamada aparcada se transfiere a la línea de aparcamiento de llamada. La línea del usuario volverá al estado inactivo y verá la extensión de aparcamiento de llamada en una ventana emergente. El usuario marca la extensión para capturar la llamada.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el aparcamiento de llamadas.</p>
Captura de llamadas	<p>Permite a los usuarios redirigir una llamada que está sonando en otro teléfono del mismo grupo de captura de llamada a su teléfono.</p> <p>Es posible configurar una alerta sonora y visual para la línea principal en el teléfono. Esta alerta notifica a los usuarios que hay una llamada sonando en su grupo de captura.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre la captura de llamadas.</p>
Grabación de llamadas	<p>Permite a un supervisor grabar una llamada activa. El usuario podría oír un tono de alerta de grabación durante las llamadas que se graban.</p> <p>Si una llamada está protegida, su estado de seguridad se muestra como un icono de candado en los teléfonos IP de Cisco. Las partes conectadas también podrían oír un tono de alerta que indica que la llamada está asegurada y se está grabando.</p> <p>Nota Cuando se supervisa o se graba una llamada activa, el usuario puede recibir o efectuar llamadas de intercomunicación; sin embargo, si el usuario efectúa una llamada de intercomunicación, la llamada activa se pone en pausa, lo que provoca que la sesión de grabación se interrumpa y la de supervisión se suspenda. Para reanudar la sesión de supervisión, la parte cuya llamada se está supervisando debe reanudar la llamada.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el control y la grabación.</p>
Llamada en espera	<p>Indica que suena una llamada entrante mientras se está en otra llamada (y permite a los usuarios contestarla). La información de la llamada en espera aparece en la pantalla del teléfono.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el número de directorio.</p>

Función	Descripción e información adicional
Timbre de llamada en espera	<p>Proporciona a los usuarios de la llamada en espera la opción de oír un timbre en lugar del pitido estándar.</p> <p>Las opciones son Timbre y Un timbre.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el número de directorio.</p>
ID de la persona que llama	<p>La identificación del autor de la llamada, como un número de teléfono, el nombre u otro texto descriptivo, aparece en la pantalla del teléfono.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el plan de enrutamiento, las restricciones para visualizar llamadas y el número de directorio.</p>
Bloqueo id. de llamadas	<p>Permite a un usuario bloquear su número de teléfono o la dirección de correo electrónico en los teléfonos que tienen la identificación de llamada habilitada.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el plan de enrutamiento y el número de directorio.</p>
Normalización de la persona que llama	<p>La normalización de la persona que llama presenta las llamadas telefónicas al usuario con un número de teléfono que se puede marcar. Al número se le agregan todos los códigos de escape, de forma que el usuario puede conectar fácilmente de nuevo con la persona que llama. El número que se puede marcar se guarda en el historial de llamadas y se puede guardar en la libreta personal de direcciones.</p>
CAST para SIP	<p>Establece una comunicación entre Cisco Unified Video Advantage (CUVA) y los teléfonos IP de Cisco para admitir vídeo en el PC, incluso si el teléfono IP no tiene capacidad de vídeo.</p>
IntruCf	<p>Permite a un usuario unirse a una llamada no privada en una línea de teléfono compartida. La función IntruCf agrega a un usuario a una llamada y la convierte en una conferencia, lo que permite al usuario y a otros participantes acceder a las funciones de conferencia. La llamada de conferencia se crea mediante la función de puente de conferencia de Cisco Unified Communications Manager.</p> <p>Debe activar la tecla programada y la funcionalidad de puente de conferencia para que IntruCf funcione correctamente.</p> <p>En la versión 10.2(2) y posteriores del firmware, a la función IntruCf se accede mediante la tecla programada Intru.</p> <p>Para obtener más información, consulte el capítulo sobre la irrupción en la Guía de configuración de características de Cisco Unified Communications Manager.</p>
Cargar un dispositivo móvil	<p>Permite a un usuario cargar un dispositivo móvil conectándolo al puerto USB del teléfono IP de Cisco.</p> <p>Consulte la <i>Guía del usuario del teléfono IP serie 8800 de Cisco</i>.</p>

Función	Descripción e información adicional
Cisco Extension Mobility	<p>Permite a los usuarios acceder a su configuración de teléfono IP de Cisco como apariencias de línea, servicios y marcaciones rápidas desde un teléfono IP de Cisco compartido.</p> <p>Cisco Extension Mobility puede resultar de utilidad si las personas trabajan desde distintas ubicaciones de la empresa o si comparten un espacio de trabajo con otros colegas.</p>
Cisco Extension Mobility Cross Cluster (EMCC)	<p>Permite a un usuario configurado en un clúster iniciar sesión en un teléfono IP de Cisco de otro clúster. Los usuarios de un clúster de inicio pueden iniciar sesión en un teléfono IP de Cisco en un clúster que visiten.</p> <p>Nota Debe configurar Cisco Extension Mobility en los teléfonos IP de Cisco antes de configurar EMCC.</p>
Cisco IP Manager Assistant (IPMA)	<p>Proporciona enrutamiento de llamadas y otras funciones de administración de llamadas que ayudan a que jefes y asistentes puedan manejar las llamadas de una forma más eficaz.</p> <p>Consulte Configurar Cisco IP Manager Assistant, en la página 194.</p>
<p>Módulo de expansión clave para Cisco IP Phone 8800</p> <p>Módulo de expansión clave para Cisco IP Phone 8851/8861</p> <p>Módulo de expansión clave para Cisco IP Phone 8865</p>	<p>Proporciona teclas adicionales al agregar un módulo de expansión al teléfono.</p> <p>Para obtener más información, consulte <i>Guía de accesorios del teléfono IP serie 7800 y 8800 de Cisco de Cisco Unified Communications Manager</i>.</p>
Teléfono IP 8811 de Cisco Asistencia	Proporciona compatibilidad para Teléfono IP 8811 de Cisco.
Asistencia técnica del teléfono IP 8851NR de Cisco	Proporciona asistencia técnica para el teléfono IP 8851NR de Cisco.
Negociación de versión de Cisco Unified Communications Manager Express (Unified CME)	<p>Cisco Unified Communications Manager Express usa una etiqueta especial en la información enviada al teléfono para identificarse. Esta etiqueta permite al teléfono proporcionar servicios al usuario que el switch admite.</p> <p>Consulte:</p> <ul style="list-style-type: none"> • Guía de administración del sistema Cisco Unified Communications Manager Express • Interacción con Cisco Unified Communications Manager Express, en la página 23
Cisco Unified Video Advantage (CUVA)	<p>Permite a los usuarios efectuar videollamadas mediante el teléfono IP de Cisco, un ordenador personal y una cámara de vídeo.</p> <p>Nota Configure el parámetro Capacidades de vídeo en la sección Diseño de la configuración específica de producto de la configuración del teléfono.</p> <p>Consulte la documentación de Cisco Unified Video Advantage.</p>
Cisco WebDialer	Permite a los usuarios efectuar llamadas desde aplicaciones en Internet o en el escritorio.

Función	Descripción e información adicional
Tono de llamada clásico	<p>Admite tonos de llamada integrados en el firmware del teléfono o descargados desde Cisco Unified Communications Manager. La función permite que los tonos de llamada disponibles sean comunes con los de otros teléfonos IP de Cisco.</p> <p>Consulte Personalización de timbres del teléfono, en la página 117.</p>
Conferencia	<p>Permite a un usuario hablar simultáneamente con varios participantes llamando a cada participante de forma individual. Las funciones de conferencias son: Conferencia y Meet Me.</p> <p>Permite a un usuario que no ha iniciado una conferencia estándar (ad hoc) agregar o eliminar a participantes. También permite a cualquier participante en la conferencia combinar dos conferencias estándar en la misma línea.</p> <p>El parámetro de servicio de conferencia ad hoc avanzada, desactivado de forma predeterminada en Cisco Unified Communications Manager Administration, permite activar estas funciones.</p> <p>Nota Asegúrese de informar a los usuarios en caso de que estas funciones estén activadas.</p>
Ethernet de consumo eficiente (EEE) configurable para el puerto PD y de switch	<p>Proporciona un método para controlar las funciones de EEE en los puertos PC y de switch activándolas o desactivándolas. La función controla ambos tipos de puertos de forma individual. El valor predeterminado es Activado.</p> <p>Consulte Configuración de Ethernet de eficacia energética para el puerto PC y de switch, en la página 180.</p>
Tamaño de fuente configurable	<p>Permite a los usuarios cambiar el tamaño de la fuente para aumentar o disminuir el número máximo de caracteres que el teléfono IP muestra en las pantallas de historial de llamadas y de la llamada.</p> <p>Con una fuente más pequeña, el número máximo de caracteres mostrados aumenta, mientras que con una más grande, disminuye.</p>
Aplicaciones CTI	<p>Un punto de ruta de integración de telefonía y ordenador (CTI) puede designar un dispositivo virtual para que reciba varias llamadas simultáneas para la redirección controlada por la aplicación.</p>
Decl. todas	<p>Permite al usuario transferir una llamada que suena, conectada o en espera directamente al sistema de buzón de voz. Cuando una llamada se declina, la línea estará disponible para realizar o recibir nuevas llamadas.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el desvío inmediato.</p>
Grabación invocada por el dispositivo	<p>Proporciona a los usuarios finales la capacidad de grabar sus llamadas telefónicas mediante una tecla programable.</p> <p>Además, los administradores pueden seguir grabando las llamadas telefónicas mediante la interfaz del usuario CTI.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el control y la grabación.</p>

Función	Descripción e información adicional
Aparcamiento de llamadas dirigido	<p>Permite al usuario transferir una llamada activa a un número de aparcamiento de llamadas dirigido disponible que haya marcado o para el que haya utilizado la marcación rápida. El botón Aparcamiento de llamada BLF indica si un número de aparcamiento de llamadas dirigido está ocupado y proporciona acceso mediante la marcación rápida al número de aparcamiento de llamada dirigido.</p> <p>Nota Si implementa el aparcamiento de llamadas dirigido, procure no configurar la tecla programable Aparcar. De esta forma se evita que los usuarios puedan confundir las dos funciones de aparcamiento de llamadas.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el aparcamiento de llamadas.</p>
Mostrar los iconos de carga de la batería e intensidad de la señal	<p>Muestra la batería y la intensidad de la señal del teléfono móvil en el teléfono IP cuando el primero está conectado al segundo mediante Bluetooth.</p> <p>El teléfono IP 8851NR de Cisco no admite Bluetooth.</p>
Timbre distintivo	<p>Los usuarios pueden personalizar el método que utiliza el teléfono para indicar una llamada entrante y un nuevo mensaje de buzón de voz.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre la captura de llamadas.</p>
No molestar (DND)	<p>Si la función DND está activada, no se produce ningún timbre audible mientras suena la llamada o no se producen notificaciones sonoras ni visuales de ningún tipo.</p> <p>Cuando está activada, el encabezado del teléfono se vuelve rojo y se muestra No molestar en el teléfono.</p> <p>Si se ha configurado la precedencia y prioridad multinivel (MLPP) y el usuario recibe una llamada de preferencia, el teléfono sonará con un tono de llamada especial.</p> <p>Consulte Configuración de la función No molestar, en la página 176.</p>
Activar o desactivar el control y la transferencia directa entre líneas	<p>Permite al administrador controlar las opciones Controlar entre líneas y Transferencia directa entre líneas.</p> <p>Consulte Configuración de la política de participación y transferencia directa, Configuración específica del producto, en la página 146.</p>
EnergyWise	<p>Permite que un teléfono IP se suspenda (se apague) y se active (se encienda) a horas predeterminadas para favorecer el ahorro energético.</p> <p>Consulte Programación de EnergyWise en el teléfono IP de Cisco, en la página 173.</p>
Modo de línea mejorado	<p>Permite usar los botones situados a ambos lados de la pantalla del teléfono como teclas de línea en el modo de línea mejorado.</p> <p>Consulte Configuración de teclas de línea adicionales, en la página 205</p>
Cisco Extension Mobility Cross Cluster (EMCC) seguro mejorado	<p>Mejora la función Extension Mobility Cross Cluster (EMCC) segura al conservar las configuraciones de red y de seguridad en el teléfono de inicio de sesión. Al hacer esto, las directivas de seguridad y el ancho de banda de red se conservan y se evitan errores de red dentro del clúster visitante.</p>

Función	Descripción e información adicional
Servicio de marcación veloz	<p>Permite al usuario introducir un código de marcación veloz para efectuar una llamada. Los códigos de marcación veloz se pueden asignar a números de teléfono o entradas de la libreta personal de direcciones. Consulte «Servicios» en esta tabla.</p> <p>Consulte Modificación de la plantilla de botones del teléfono para la libreta personal de direcciones o la marcación rápida, en la página 203.</p>
Captura de llamadas de grupo	<p>Permite al usuario contestar una llamada que suena en un número de directorio de otro grupo.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre la captura de llamadas.</p>
Control de tono local del auricular	<p>Permite a un administrador establecer el nivel de tono lateral de unos auriculares con cable.</p>
Reversión en espera	<p>Limita la cantidad de tiempo que una llamada puede permanecer en espera antes de que se revierta al teléfono que la puso en espera y de alertar al usuario.</p> <p>Las llamadas revertidas se distinguen de las llamadas entrantes porque solo suena un timbre (o pitido, según la configuración del indicador de llamada nueva de la línea). Esta notificación se repite a intervalos si no se reanuda.</p> <p>En las llamadas que activan la reversión en espera también se muestra un icono animado en el bocadillo de llamada. Es posible configurar la prioridad del centro de atención de la llamada para favorecer las llamadas entrantes o las de reversión.</p>
Estado de llamada en espera	<p>Permite distinguir entre las líneas local y remota que han puesto una llamada en espera en los teléfonos con una línea compartida.</p>
Espera/Continuar	<p>Permite al usuario cambiar el estado de una llamada conectada de activa a en espera.</p> <ul style="list-style-type: none"> • No se requiere configuración, a no ser que se desee usar la función Música en espera. Consulte «Música en espera» en esta tabla para obtener más información. • Consulte «Reversión en espera» en esta tabla.
Descarga HTTP	<p>Mejora el proceso de descarga de archivos en el teléfono al usar HTTP de forma predeterminada. Si la descarga HTTP falla, el teléfono vuelve a usar la descarga TFTP.</p>
Grupo de salto	<p>Permite compartir la carga de las llamadas con un número de directorio principal. Un grupo de salto contiene una serie de números de directorio que pueden contestar las llamadas entrantes. Si el primer número de directorio del grupo de salto está ocupado, el sistema saltará en una secuencia predeterminada al siguiente número de directorio disponible del grupo y dirigirá la llamada a ese teléfono.</p> <p>Puede hacer que el ID de llamada (si está configurado el ID de llamada), el Número de directorio y el Número piloto del grupo de búsqueda se muestren en la alerta de llamadas entrantes para la llamada del grupo de búsqueda. El número del grupo de búsqueda se muestra después de la etiqueta "Grupo de búsqueda".</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre grupos de salto o planes de enrutamiento.</p>

Función	Descripción e información adicional
Temporizador del mensaje emergente de llamada entrante	<p>Permite establecer el tiempo que aparece el mensaje emergente (notificación) de la llamada entrante en la pantalla de teléfono.</p> <p>Consulte Temporizador del mensaje emergente de llamada entrante, Configuración específica del producto, en la página 146.</p>
Proximidad inteligente	<p>Permite a los usuarios vincular un dispositivo móvil con el teléfono mediante Bluetooth, así como utilizar el teléfono para efectuar y recibir llamadas del móvil.</p> <p>Consulte Activación de Intelligent Proximity, en la página 209.</p> <p>Los teléfonos IP 8811, 8841 y 8851NR de Cisco no admiten Bluetooth ni la función de proximidad inteligente.</p>
Intercomunicación	<p>Permite a los usuarios efectuar y recibir llamadas de intercomunicación mediante botones de teléfono programables. Es posible configurar los botones de línea intercomunicación para:</p> <ul style="list-style-type: none"> • marcar directamente una extensión de intercomunicación específica; • iniciar una llamada de intercomunicación y solicitar al usuario que introduzca un número de intercomunicación válido. <p>Nota Si el usuario inicia sesión en el mismo teléfono a diario con el perfil de Cisco Extension Mobility, asigne a su perfil la plantilla de botones del teléfono que contiene información de intercomunicación y asigne a la línea de intercomunicación el teléfono como dispositivo de intercomunicación predeterminado.</p>
Compatibilidad solo con IPv6	<p>Proporciona compatibilidad para las direcciones IP expandidas en los teléfonos IP de Cisco. Se recomienda la configuración de IPv4 e IPv6, que es totalmente compatible. algunas funciones no se admiten en la configuración independiente. Solo se asignan direcciones IPv6.</p> <p>Consulte Configuración de los ajustes de red, en la página 58.</p>
Búfer de fluctuación	<p>La función de búfer de fluctuación controla la fluctuación entre 10 y 1000 milisegundos (ms) para los flujos de audio.</p> <p>Se ejecuta en el modo de adaptación y se ajusta de forma dinámica a la cantidad de fluctuación.</p>
Unir	<p>Permite a los usuarios combinar dos llamadas de una línea a fin de crear una llamada de conferencia y permanecer en la llamada.</p>

Función	Descripción e información adicional
Estado de línea para las listas de llamadas	<p>Permite al usuario comprobar el estado de disponibilidad del estado de línea de los números de línea supervisados en la lista Historial de llamadas. Los estados disponibles son:</p> <ul style="list-style-type: none"> • Fuera de línea • Disponible. • En uso • No molestar <p>Consulte Activación de BLF para listas de llamadas, en la página 179.</p>
Estado de línea en directorio corporativo	<p>Permite mostrar el estado de un contacto en el directorio corporativo.</p> <ul style="list-style-type: none"> • Fuera de línea • Disponible. • En uso • No molestar <p>Consulte Activación de BLF para listas de llamadas, en la página 179.</p>
Texto de etiqueta de línea	<p>Permite definir una etiqueta de texto para una línea de teléfono, en lugar de un número en directorio.</p> <p>Consulte Establecimiento de la etiqueta para una línea, en la página 189.</p>
Cierre de sesión de grupos de salto	<p>Permite a los usuarios cerrar la sesión de un grupo de salto y bloquear temporalmente las llamadas para que no suenen en los teléfonos si no están disponibles para contestar llamadas. Cerrar sesión en los grupos de salto no impedirá que otros grupos que no sean de salto llamen a su teléfono.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el plan de enrutamiento.</p>
Identificación de llamadas maliciosas (IdLIMali)	<p>Permite a los usuarios notificar al administrador del sistema sobre las llamadas sospechosas que se reciben.</p>
Conferencias Meet Me	<p>Permite a un usuario organizar una conferencia Meet Me en la que el resto de participantes tendrán que llamar a un número predeterminado a una hora programada.</p>
Mensaje en espera	<p>Define los números de directorio de los mensajes que esperan indicadores de activación o desactivación. Los sistema de mensajes de voz conectados directamente usan el número de directorio especificado para establecer o borrar una indicación de mensaje en espera para un teléfono IP de Cisco concreto.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre los mensajes en espera y el buzón de voz.</p>

Función	Descripción e información adicional
Indicador de mensaje en espera	<p>Se trata de una luz en el auricular de mano que indica que un usuario tiene nuevos mensajes de voz.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre los mensajes en espera y el buzón de voz.</p>
Volumen del timbre mínimo	<p>Establece un nivel de volumen de timbre mínimo para un teléfono IP.</p>
Registro de llamadas perdidas	<p>Permite al usuario especificar si las llamadas perdidas se registrarán en el directorio correspondiente para la apariencia de línea concreta.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el número de directorio.</p>
Mobile Connect	<p>Permite a los usuarios administrar las llamadas empresariales mediante un único número de teléfono, así como capturar las llamadas en curso en el teléfono de escritorio y en un dispositivo remoto como un teléfono móvil. Los usuarios pueden restringir el grupo de personas que llaman según el número de teléfono y la hora.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre Cisco Unified Mobility.</p>
Mobile and Remote Access mediante Expressway	<p>Permite a los trabajadores remotos conectarse de forma sencilla y segura con la red empresarial mediante un túnel de cliente de una red privada virtual (VPN).</p> <p>Consulte Mobile and Remote Access mediante Expressway, en la página 182</p>
Acceso de voz móvil	<p>Amplía las capacidades de Mobile Connect al permitir que los usuarios puedan acceder a un sistema de respuesta de voz interactiva (IVR) para originar una llamada desde un dispositivo remoto, como un teléfono móvil.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre Cisco Unified Mobility.</p>
Supervisión y grabación	<p>Permite a un supervisor controlar de forma silenciosa una llamada activa. Ninguno de los participantes en la llamada puede oír al supervisor. El usuario podría oír un tono de alerta de supervisión durante las llamadas que se controlan.</p> <p>Si una llamada está protegida, su estado de seguridad se muestra como un icono de candado en los teléfonos IP de Cisco. Las partes conectadas también podrían oír un tono de alerta que indica que la llamada está asegurada y se está supervisando.</p> <p>Nota Cuando se supervisa o se graba una llamada activa, el usuario puede recibir o efectuar llamadas de intercomunicación; sin embargo, si el usuario efectúa una llamada de intercomunicación, la llamada activa se pone en pausa, lo que provoca que la sesión de grabación se interrumpa y la de supervisión se suspenda. Para reanudar la sesión de supervisión, la parte cuya llamada se está supervisando debe reanudar la llamada.</p>
Precedencia multinivel y preferencia	<p>Permite al usuario efectuar y recibir llamadas urgentes o críticas en algunos entornos especializados, como oficinas militares o gubernamentales.</p> <p>Consulte Precedencia multinivel y preferencia, en la página 199.</p>

Función	Descripción e información adicional
Aspecto de varias llamadas por línea	<p>cada línea puede admitir varias llamadas. De forma predeterminada, el teléfono admite dos llamadas activas por línea y un máximo de seis llamadas activas por línea. Solo puede haber activa una llamada en cada momento; las llamadas restantes se pondrán en espera automáticamente.</p> <p>El sistema permite configurar el número máximo de llamadas activas/ocupadas como 6/6. Formalmente, no se admite ninguna otra configuración superior a 6/6.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el número de directorio.</p>
Música en espera	Reproduce música mientras la persona que llama está en espera.
Silencio	Silencia el micrófono del auricular de mano o los auriculares.
Sin nombre de alerta	Facilita a los usuarios finales la identificación de las llamadas transferidas al mostrar el número de teléfono de la persona que llama original. La llamada se muestra como una llamada de alerta seguida del número de teléfono de la persona que llama.
Marcación con auricular colgado	Permite al usuario marcar un número sin tener que descolgar. El usuario después puede levantar el auricular o presionar Marcar.
Captura de otro grupo	<p>Permite al usuario contestar una llamada que suena en un teléfono de otro grupo asociado al suyo.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre la captura de llamadas.</p>
Mensaje en pantalla del teléfono para usuarios de Extension Mobility	Esta función mejora la interfaz del teléfono para los usuarios de Extension Mobility al proporcionar mensajes fáciles de leer.
Notificación de lista de confianza del teléfono en Cisco Unified Communications Manager	<p>Permite al teléfono enviar una alarma a Cisco Unified Communications Manager cuando se actualice la lista de confianza.</p> <p>Consulte Características de seguridad admitidas, en la página 88.</p>
Compatibilidad PLK para las estadísticas de la cola	La función de compatibilidad PLK para las estadística de la cola permite a los usuarios consultar los detalles de la cola de llamadas sobre las cabeceras de grupo de salto. La información se muestra en la pantalla del teléfono.
Marcación con el signo más	<p>Permite al usuario marcar números E.164 con el prefijo de signo más (+).</p> <p>Para marcar el signo más +, el usuario debe presionar y mantener presionada la tecla asterisco (*) al menos 1 segundo. Esto se aplica a la marcación del primer dígito en las llamadas con el teléfono colgado (incluido el modo de edición) o con el teléfono descolgado.</p>
Negociación de energía por LLDP	<p>Permite al teléfono negociar la energía mediante el protocolo de descubrimiento de terminal de nivel de enlace (LLDP) y el Cisco Discovery Protocol (CDP).</p> <p>Consulte Negociación de energía, Configuración específica del producto, en la página 146.</p>

Función	Descripción e información adicional
Marcación predictiva	<p>Simplifica la realización de la llamada. La lista Recientes cambia para mostrar solo los números de teléfono similares al número marcado.</p> <p>La marcación predictiva está habilitada cuando el modo de línea mejorado está activado. La nueva interfaz de usuario de llamada simplificada debe estar desactivada para que funcione la marcación predictiva.</p>
Privacidad	<p>Impide que los usuarios que comparten una línea se puedan agregar a sí mismos a una llamada y puedan ver información en la pantalla del teléfono sobre la llamada del otro usuario.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre la intrusión y la privacidad.</p>
Señalización manual automática de línea privada (PLAR)	<p>El administrador de Cisco Unified Communications Manager puede configurar un número de teléfono que el teléfono IP de Cisco debe marcar en cuanto se descuelgue el auricular. Esta función puede ser útil para teléfonos designados para llamadas de emergencia o para números de «línea directa».</p> <p>El administrador puede configurar un retraso de hasta 15 segundos. Esto permite al usuario tener tiempo para realizar una llamada antes de que el teléfono pase por defecto al número de la línea directa. El temporizador se puede configurar mediante el parámetro de temporizador desde descolgado hasta el primer dígito en Dispositivo > Configuración del dispositivo > Perfil SIP.</p> <p>Para obtener más información, consulte la <i>Guía de configuración de características de Cisco Unified Communications Manager</i>.</p>
Herramienta de informe de problemas (PRT)	<p>Envía los registros del teléfono o informa sobre los problemas a un administrador.</p> <p>Consulte Herramienta de informe de problemas, en la página 187.</p>
Botones de función programables	<p>Es posible asignar a los botones de línea funciones como Nueva llamada, Devolver llamada o Desviar todas.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre las plantillas de botones de teléfono.</p>
Herramienta de generación de informes de calidad (QRT)	<p>Permite a los usuarios enviar información sobre problemas de las llamadas telefónicas presionando un botón. QRT se puede configurar para dos modos de usuario distintos, según el nivel de interacción que se desee entre el usuario y la herramienta.</p>
Recientes	<p>Permite a los usuarios ver las 150 llamadas individuales y grupos de llamadas más recientes. Puede ver los números marcados recientemente y las llamadas perdidas, así como eliminar un registro de llamada.</p>
Rellamada	<p>Permite a los usuarios llamar al número de teléfono marcado más recientemente presionando un botón o la tecla programable Rellam.</p>

Función	Descripción e información adicional
Configuración de puerto remoto	<p>Permite configurar la velocidad y la función dúplex de los puertos Ethernet del teléfono de forma remota mediante Cisco Unified Communications Manager Administration. Esto mejora el rendimiento en caso de grandes implementaciones con configuraciones específicas de puertos.</p> <p>Nota Si los puertos se configuran para la configuración de puerto remoto en Cisco Unified Communications Manager, los datos no se pueden cambiar en el teléfono.</p> <p>Consulte Configuración de puerto remoto, Configuración específica del producto, en la página 146.</p>
Redirigir llamadas directas a destino remoto a número de la empresa	<p>Redirige una llamada directa al teléfono móvil de un usuario al número de la empresa (teléfono de escritorio). En el caso de las llamadas entrantes a un destino remoto (móvil), solo suena el destino remoto, no así el teléfono de escritorio. Al contestar la llamada en el teléfono móvil, el teléfono del escritorio muestra el mensaje Remoto en uso. Durante estas llamadas, los usuarios pueden usar varias funciones en sus teléfonos móviles.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre Cisco Unified Mobility.</p>
Eliminar el temporizador del mensaje de llamada finalizada	<p>Mejora el tiempo de respuesta para finalizar la llamada al eliminar el mensaje Llamada finalizada que se muestra en la pantalla del teléfono.</p>
Configuración del tono de llamada	<p>Identifica el tipo de timbre usado para una línea cuando el teléfono tiene otra llamada activa.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el número de directorio y Personalización de timbres del teléfono, en la página 117.</p>
Espera de RTCP para SIP	<p>Garantiza que la gateway no interrumpe las llamadas en espera. La gateway comprueba el estado del puerto RTCP para determinar si una llamada está activa o no. Al mantener el puerto del teléfono abierto, la gateway no finalizará las llamadas en espera.</p>
Conferencia segura	<p>Permite que los teléfonos seguros efectúen llamadas mediante un puente de conferencia seguro. Cuando se agregan nuevos participantes con las teclas programadas Conf., Conectar o Intrus. o en conferencias Meet Me, siempre que todos los participantes usen teléfonos seguros, se mostrará el icono de llamada segura.</p> <p>En Lista de conferencia se muestra el nivel de seguridad de cada participante en la conferencia. Las personas que iniciaron la conferencia pueden eliminar a los participantes no seguros de esta lista. Los demás usuarios pueden agregar o eliminar participantes de la conferencia siempre que el parámetro de servicio de conferencia ad hoc avanzada esté activado.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager y Características de seguridad admitidas, en la página 88 la información sobre el puente de conferencia y la seguridad.</p>
EMCC seguro	<p>Mejora la función EMCC proporcionando seguridad avanzada cuando el usuario inicia sesión en su teléfono desde una oficina remota.</p>

Función	Descripción e información adicional
Servicios	<p>Permite usar el menú de configuración de servicios del teléfono IP de Cisco en Administración de Cisco Unified Communications Manager para definir y mantener la lista de servicios telefónicos a los que se pueden suscribir los usuarios.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre los servicios.</p>
Botón de URL de servicios	<p>Permite a los usuarios acceder a servicios mediante un botón programable, en lugar de usar el menú Servicios del teléfono.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre los servicios.</p>
Mostrar ID y número de llamada	<p>Los teléfonos pueden mostrar tanto el ID como el número de las llamadas entrantes. El tamaño de la pantalla LCD del teléfono IP limita la longitud mostrada del ID y del número que llama.</p> <p>La función Mostrar ID y número de llamada se aplica solo a la alerta de llamada entrante y no cambia la función de las funciones Desvío de llamadas ni Grupo de salto.</p> <p>Consulte «ID de la persona que llama» en esta tabla.</p>
Simplificación del inicio de sesión de Extension Mobility con auriculares de Cisco	<p>Permite a los usuarios iniciar sesión en Extension Mobility con sus auriculares de Cisco.</p> <p>Si el teléfono está en modo MRA, el usuario podrá utilizar los auriculares para iniciar sesión en el teléfono.</p> <p>Esta función requiere Cisco Unified Communications Manager (UCM) versión 11.5(1)SU8, 11.5(1)SU.9, 12.5(1)SU3 o posterior.</p> <p>Para obtener más información, consulte la <i>Guía de configuración de funciones del sistema para Cisco Unified Communications Manager</i>, versión 11.5(1)SU8 o posterior.</p>
Compatibilidad simplificada con tabletas	<p>Permite a los usuarios de una tableta Android o iOS vincularla al teléfono mediante Bluetooth y, a continuación, usar el teléfono para la parte de audio de una llamada en la tableta.</p> <p>Consulte Activación de Intelligent Proximity, en la página 209.</p> <p>El teléfono IP 8851NR de Cisco no admite Bluetooth.</p>
Marcación rápida	<p>Marca un número especificado que se ha guardado anteriormente.</p>
Acceso SSH	<p>Permite activar o desactivar el ajuste Acceso SSH mediante Cisco Unified Communications Manager Administration. Activar el servidor SSH permite al teléfono aceptar las conexiones SSH. Al desactivar la función de servidor SSH del teléfono, se bloquea el acceso SSH al teléfono.</p> <p>Consulte Acceso SSH, Configuración específica del producto, en la página 146.</p>
Enrutamiento de hora del día	<p>Restringe el acceso a las funciones de telefonía especificadas por un período de tiempo.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el enrutamiento por período de tiempo y hora del día.</p>

Función	Descripción e información adicional
Actualización de la zona horaria	<p>Actualiza el teléfono IP de Cisco con los cambios de las zonas horarias.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre la fecha y la hora.</p>
Transferir	<p>Permite a los usuarios redirigir las llamadas conectadas desde su teléfono a otro número.</p>
Transferencia - Transferencia directa	<p>Transferir: la primera invocación de transferencia iniciará siempre una llamada nueva con el mismo número de directorio después de poner la llamada activa en espera.</p> <p>El usuario puede transferir directamente llamadas mediante la función de transferencia de la llamada activa.</p> <p>Algunas aplicaciones JTAPI/TAPI no son compatibles con la implementación de las funciones Conectar y Transferencia directa del teléfono IP de Cisco y puede que tenga que configurar la directiva correspondiente para que se desactive la conexión y transferencia directa en la misma línea o, posiblemente, entre distintas líneas.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el número de directorio.</p>
TVS	<p>Los servicios de verificación de confianza (TVS) permiten a los teléfonos autenticar las configuraciones firmadas y autenticar otros servidores o pares sin aumentar el tamaño de la lista de certificados de confianza (CTL) y sin requerir la descarga de un archivo CTL actualizado en el teléfono. Los TVS están activados de manera predeterminada.</p> <p>El menú Configuración de seguridad del teléfono muestra la información de TVS.</p>
UCR 2013	<p>Los teléfonos IP de Cisco admiten los requisitos de capacidades unificadas (UCR) 2013, ya que proporcionan las siguientes funciones:</p> <ul style="list-style-type: none"> • Compatibilidad con el estándar federal de procesamiento de información (FIPS) 140-2 de EE. UU. • Compatibilidad para el etiquetado SRTCP de 80 bits. <p>Como administrador de un teléfono IP, debe configurar los parámetros específicos en la desinstalación de Cisco Unified Communications Manager.</p>
Notificación de línea principal no configurada	<p>Alerta al usuario si la línea principal no está configurada. El usuario verá el mensaje No suministrado en la pantalla del teléfono.</p>
Actualizaciones de la interfaz del usuario para listas, alertas y Visual Voicemail.	<p>Aumenta el tamaño de la ventana de la aplicación para reducir al mínimo el número de cadenas truncadas.</p>
Modo de vídeo	<p>Permite a un usuario seleccionar el modo de pantalla de vídeo para ver una conferencia de vídeo, dependiendo de los modos configurados en el sistema.</p> <p>Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager la información sobre el vídeo.</p> <p>Disponible en los teléfonos IP 8845, 8865 y 8865NR de Cisco.</p>

Función	Descripción e información adicional
Compatible con vídeo	Permite la compatibilidad de vídeo en el teléfono. El parámetro Capacidades de vídeo debe estar activado para las videollamadas en la ventana de configuración del teléfono de Cisco Unified Communications Manager. Está activado de manera predeterminada. Disponible en los teléfonos IP 8845, 8865 y 8865NR de Cisco.
Vídeo a través del ordenador	Permite a los usuarios efectuar videollamadas mediante el Teléfono IP de Cisco Unified, un ordenador personal y una cámara de vídeo externa. La función también permite a los usuarios efectuar videollamadas con Cisco Jabber o productos Cisco Unified Video Advantage.
Visual Voicemail	Sustituye los mensajes de audio del buzón de voz por una interfaz gráfica. Consulte la <i>Guía de instalación y configuración de Visual Voicemail</i> , que encontrará en http://www.cisco.com/en/US/partner/products/ps9829/prod_installation_guides_list.html#anchor3 .
Sistema de mensaje de voz	Permite a la persona que llama dejar mensajes en caso de que la llamada no reciba respuesta. Consulte en la documentación de su versión concreta de Cisco Unified Communications Manager y en Configuración de Visual Voicemail, en la página 196 la información sobre el correo de voz.
VPN	Mediante SSL, proporciona una conexión de red privada virtual (VPN) en el Teléfono IP de Cisco Unified si este se encuentra fuera de una red de confianza o si el tráfico de red entre el teléfono y Unified Communications Manager debe atravesar redes que no son de confianza.
Acceso vía Web deshabilitado de forma predeterminada	Mejora la seguridad al desactivar el acceso a todos los servicios web, como HTTP. Los usuarios solo pueden acceder a los servicios web si habilita el acceso web.

Temas relacionados

[Cisco Unified Communications Manager Documentación](#), en la página xv

Botones de función y teclas programadas

En la tabla siguiente se incluye información sobre las funciones que están disponibles en teclas programables, las disponibles en botones de función dedicados y las que tiene que configurar como botones de función programables. Una entrada «Compatible» en la tabla indica que la función se admite para el tipo de botón o la tecla programable correspondiente. De los dos tipos de botones y teclas programables, solo los botones de función programables requieren configuración en la administración del teléfono IP de Cisco.

Para obtener más información sobre la configuración de los botones de función programables, consulte [Plantillas de botones de teléfono, en la página 201](#).

Tabla 30: Funciones con los botones y teclas programadas correspondientes

Nombre de la función	Botón de función dedicado	Botón de función programable	Tecla programable
Llamadas en alerta	No compatible	Compatible	No compatible
Todas	No compatible	Compatible	No compatible
Contestar	No compatible	Compatible	Compatible
IntruCf	No compatible	No compatible	Compatible
Retrollamada	No compatible	Compatible	Compatible
Desvío incondicional	No compatible	No compatible	Compatible
Aparcar llamada	No compatible	Compatible	Compatible
Estado de línea de aparcamiento de llamada	No compatible	Compatible	No compatible
Captura de llamada (Capturar)	No compatible	Compatible	Compatible
Estado de línea de captura de llamada	No compatible	Compatible	No compatible
Conferencia	Compatible	No compatible	Compatible
Desviar	No compatible	No compatible	Compatible
No molestar	No compatible	Compatible	Compatible
Captura de grupo (Capt. grupo)	No compatible	Compatible	Compatible
Espera	Compatible	No compatible	Compatible
Grupos de salto	No compatible	Compatible	No compatible
Intercomunicación	No compatible	Compatible	No compatible
Identificación de llamadas maliciosas (IdLMali)	No compatible	Compatible	Compatible
Meet Me	No compatible	Compatible	Compatible
Unir	No compatible	No compatible	Compatible
Mobile Connect (Movilidad)	No compatible	Compatible	Compatible
Silencio	Compatible	No compatible	No compatible

Nombre de la función	Botón de función dedicado	Botón de función programable	Tecla programable
Captura de otros	No compatible	Compatible	Compatible
Compatibilidad PLK para estado de cola	No compatible	No compatible	Compatible
Privacidad	No compatible	Compatible	No compatible
Estado de cola	No compatible	Compatible	No compatible
Herramienta de generación de informes de calidad (QRT)	No compatible	Compatible	Compatible
Grabar	No compatible	No compatible	Compatible
Rellamar	No compatible	Compatible	Compatible
Marcación rápida	No compatible	Compatible	No compatible
Estado de línea de marcación rápida	No compatible	Compatible	No compatible
Compatibilidad con el botón de espera en auriculares USB	No compatible	No compatible	Compatible
Transferir	Compatible	No compatible	Compatible

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.

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.

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.
-

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.
-

Configuración específica del producto

La tabla siguiente describe los campos en el panel de diseño de la configuración específica de producto.

Tabla 31: Campos de la configuración específica del producto

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Desactivación del altavoz	Casilla de verificación	Desactivado	Desactiva la capacidad del teléfono con altavoz del teléfono.
Desactivar teléfono con altavoz y auriculares	Casilla de verificación	Desactivado	Desactiva la capacidad del teléfono con altavoz y los auriculares del teléfono.
Desactivar el auricular	Casilla de verificación	Desactivado	Desactiva la capacidad de auricular del teléfono.
Puerto PC	Habilitado Deshabilitado	Habilitado	Controla la capacidad para usar el puerto PC para conectar un equipo en la red LAN.
Acceso a la configuración	Deshabilitado Habilitado Restringido	Habilitado	Activa, desactiva o restringe el acceso a los ajustes de configuración del teléfono local en la aplicación Configuración. <ul style="list-style-type: none"> • Desactivado: el menú Configuración no muestra las opciones. • Habilitado: todas las entradas en el menú Configuración son accesibles. • Restringido: solo es posible acceder al menú Configuración del teléfono.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Acceso de VLAN de voz del PC	Habilitado Deshabilitado	Habilitado	Indica si el teléfono va a permitir que un dispositivo conectado al puerto PC acceda a la VLAN de voz. <ul style="list-style-type: none"> • Desactivado: el PC no puede enviar y recibir datos en la VLAN de voz o desde el teléfono. • Habilitado: el PC no puede enviar y recibir datos desde la VLAN de voz o desde el teléfono. Establezca este campo en Habilitado si se ejecuta una aplicación en el PC para supervisar el tráfico del teléfono. Estas aplicaciones pueden incluir aplicaciones de supervisión y grabación, y el uso del software de supervisión de red para fines de análisis.
Capacidades de vídeo	Habilitado Deshabilitado	8845, 8865 y 8865NR: Habilitado 8811, 8851, 8851NR y 8861: Desactivado	Permite a los usuarios efectuar videollamadas mediante el teléfono IP de Cisco, un ordenador personal y una cámara de vídeo.
Acceso vía Web	Deshabilitado Habilitado	Deshabilitado	Activa o desactiva el acceso a las páginas web del teléfono a través de un explorador web. <p>Precaución Si activa este campo, puede revelar información confidencial sobre el teléfono.</p>
Desactivar TLS 1.0 y TLS 1.1 para acceso web	Deshabilitado Habilitado	Deshabilitado	Controla el uso de TLS 1.2 para una conexión del servidor web. <ul style="list-style-type: none"> • 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 e instrucciones de uso
Marcación en bloque	Deshabilitado Habilitado	Deshabilitado	<p>Controla el método de marcación.</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
Días pantalla no activa	Días de la semana		<p>Define los días en que la pantalla no se enciende automáticamente a la hora especificada en el campo Hora de activación de pantalla.</p> <p>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.</p>
Hora de activación de pantalla	hh:mm		<p>Define la hora de cada día a la que se enciende automáticamente la pantalla (excepto los días especificados en el campo Días pantalla no activa).</p> <p>En este campo, debe introducir la hora en formato de 24 horas, donde 00:00 es la medianoche.</p> <p>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.</p> <p>Si el campo está vacío, la pantalla se enciende automáticamente a las 0:00.</p>

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Duración actividad de pantalla	hh:mm		<p>Define el período que la pantalla permanecerá activada tras encenderse a la hora especificada en el campo Hora de activación de pantalla.</p> <p>Por ejemplo, para que la pantalla siga encendida 4 horas y 30 minutos después de encenderse automáticamente, introduzca 04:30.</p> <p>Si el campo está vacío, el teléfono se apaga al final del día (0:00).</p> <p>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 no se apaga.</p>
Tiempo espera pantalla inactiva	hh:mm	01:00	<p>Define 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).</p> <p>Introduzca el valor en este campo con el formato horas:minutos.</p> <p>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.</p> <p>Para obtener más información, consulte Configuración de la pantalla de inactividad, en la página 120.</p>
Mostrar Act. en llamada entrante	Deshabilitado Habilitado	Habilitado	Enciende la pantalla de inactividad cuando se produce una llamada entrante.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Activar Power Save Plus	Días de la semana		<p>Define la programación de los días en los que el teléfono se apaga.</p> <p>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.</p> <p>Si la casilla Activar Power Save Plus está activada, recibirá un mensaje de advertencia sobre los servicios de emergencia (e911).</p> <p>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.</p> <p>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.</p>

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Hora de encendido del teléfono	hh:mm		<p>Determina la hora a la que el teléfono se enciende automáticamente los días indicados en el campo Activar Power Save Plus.</p> <p>En este campo, debe introducir la hora en formato de 24 horas, donde 00:00 es la medianoche.</p> <p>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.</p> <p>El valor predeterminado es dejar el campo vacío, que indica las 00:00.</p> <p>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.</p>
Hora de apagado del teléfono	hh:mm		<p>Identifica la hora del día en la que se apaga el teléfono 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.</p> <p>En este campo, debe introducir la hora en formato de 24 horas, donde 00:00 es la medianoche.</p> <p>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.</p> <p>El valor predeterminado es dejar el campo vacío, que indica las 00:00.</p> <p>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.</p>

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Tiempo de espera de inactividad para apagar el teléfono	De 20 a 1440 minutos	60	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: <ul style="list-style-type: none"> • 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.
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.
Dominio de EnergyWise	Hasta 127 caracteres		Identifica el dominio de EnergyWise en el que se encuentra el teléfono.
Secreto de EnergyWise	Hasta 127 caracteres		Identifica la contraseña secreta de seguridad que se usa para comunicarse con los terminales del dominio de EnergyWise.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Permitir anulaciones de EnergyWise	Casilla de verificación	Desactivado	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <ul style="list-style-type: none"> • 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. • Para volver a cambiar el nivel de energía del teléfono, EnergyWise debe emitir de nuevo un comando de cambio de nivel de energía. <p>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.</p>

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Política de participación y transferencia directa	Misma línea, activar entre líneas Activar solo en misma línea: Misma línea, desactivar entre líneas	Misma línea, activar entre líneas	Controla la capacidad de un usuario de participación y transferencia de llamadas. <ul style="list-style-type: none"> • Misma línea, activar entre líneas: los usuarios pueden transferir una llamada en la línea actual a otra llamada en otra línea o participar en una llamada de la misma línea en otra llamada de otra línea. • Activar solo en misma línea: los usuarios solo pueden transferir las llamadas o participar en ellas directamente cuando ambas llamadas están en la misma línea. • Misma línea, desactivar entre líneas: 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.
Distribuir a puerto PC	Deshabilitado Habilitado	Deshabilitado	Indica si el teléfono reenvía los paquetes transmitidos o recibidos por el puerto de red al puerto de acceso.
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>
Cisco Discovery Protocol (CDP): puerto conmutador	Deshabilitado Habilitado	Habilitado	Controla Cisco Discovery Protocol en el puerto SW del teléfono.
Cisco Discovery Protocol (CDP): puerto PC	Deshabilitado Habilitado	Habilitado	Controla Cisco Discovery Protocol en el puerto PC del teléfono.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
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.
Protocolo de descubrimiento de capa de enlace (LLDP): puerto PC	Deshabilitado Habilitado	Habilitado	Permite LLDP en el puerto PC.
LLDP ID del dispositivo	Cadena, hasta un máximo de 32 caracteres		Identifica el ID del dispositivo asignado al teléfono para la administración del inventario.
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 Habilitado Deshabilitado	Controlado por el usuario	Especifica el estado de la función de la autenticación 802.1X. <ul style="list-style-type: none"> • 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.
Sincronización de puerto automática	Deshabilitado Habilitado	Deshabilitado	Sincroniza los puertos a la velocidad más baja entre los puertos de un teléfono para eliminar la pérdida de paquetes.
Cambiar configuración remota de puerto	Deshabilitado Habilitado	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.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Configuración remota de puerto de PC	Deshabilitado Habilitado	Deshabilitado	Le permite configurar la velocidad y la función dúplex del puerto PC del teléfono de forma remota. Esto mejora el rendimiento en caso de grandes implementaciones con configuraciones específicas de puertos. Si los puertos se configuran para la configuración de puerto remoto 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.
Temporizador del mensaje emergente de llamada entrante	0, 3, 4, 5, 6, 7, 8, 9, 10, 15, 30, 60	5	Indica el tiempo, en segundos, que se muestra el mensaje emergente. El tiempo incluye los períodos de atenuación y reactivación de la ventana. 0 significa que el mensaje emergente para la llamada entrante está desactivado.
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.
Grabar registro de llamadas desde línea compartida	Deshabilitado Habilitado	Deshabilitado	Especifica si se va a grabar una llamada de línea compartida en el registro de llamadas.
Volumen del timbre mínimo	0: silencioso 1–15	0: silencioso	Controla el volumen del timbre mínimo para el teléfono. Puede configurar un teléfono para que no se puede desactivar el timbre.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Uso compartido del firmware en el grupo	Deshabilitado Habilitado	Habilitado	<p>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.</p> <p>Uso compartido del firmware en el grupo:</p> <ul style="list-style-type: none"> • Limita la congestión de las transferencias TFTP a los servidores TFTP remotos centralizados. • Elimina la necesidad de controlar manualmente las actualizaciones 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		<p>Identifica el servidor IPv4 alternativo que usa el teléfono para obtener actualizaciones y cargas de firmware.</p> <p>El formato de la dirección es: dirección: <port>@@base=<0-7>;pfs=<0-1></p>
Servidor de carga de IPv6	Cadena de un máximo de 256 caracteres		<p>Identifica el servidor IPv6 alternativo que usa el teléfono para obtener actualizaciones y cargas de firmware.</p> <p>El formato de la dirección es: [dirección]: <port>@@base=<0-7>;pfs=<0-1></p>
Control de IU de auricular de banda ancha	Deshabilitado Habilitado	Habilitado	Permite al usuario usar el códec de banda ancha para los auriculares analógicos.
Auriculares de banda ancha	Deshabilitado Habilitado	Habilitado	<p>Activa o desactiva el uso de auriculares de banda ancha en el teléfono. Se utiliza junto con los auriculares de banda ancha de control de usuario.</p> <p>Para obtener más información, consulte Configuración del códec de banda ancha, en la página 119.</p>

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Wi-Fi	Deshabilitado Habilitado	Habilitado	Permite a los teléfonos IP de Cisco 8861 y 8865 conectarse a la red Wi-Fi. Los teléfonos que no admiten esta función no muestran el campo.
Puerto USB trasero	Deshabilitado Habilitado	8861, 8865 y 8865NR: Habilitado	Controla la capacidad de usar el puerto USB en la parte posterior de los teléfonos IP de Cisco 8861 y 8865. Los teléfonos que no admiten esta función no muestran el campo.
Puerto USB lateral	Deshabilitado Habilitado	Habilitado	Controla la capacidad de usar el puerto USB en el lateral de los teléfonos IP de Cisco 8851, 8851NR, 8861, 8865 y 8865NR. Los teléfonos que no admiten esta función no muestran el campo.
Acceso a la consola	Deshabilitado Habilitado	Deshabilitado	Especifica si la consola serie está activada o desactivada.
Bluetooth	Deshabilitado Habilitado	Habilitado	Activa o desactiva la opción de Bluetooth en el teléfono. Si está desactivado, el usuario no podrá activar el Bluetooth en el teléfono. Se admiten en los teléfonos IP 8845, 8851, 8861 y 8865 de Cisco. Los teléfonos que no admiten esta función no muestran el campo.
Permitir la importación de contactos de Bluetooth	Deshabilitado Habilitado	Habilitado	Permite al usuario importar contactos desde su dispositivo móvil conectado mediante Bluetooth. Cuando está desactivado, el usuario no puede importar contactos desde su dispositivo móvil conectado en su teléfono. Se admiten en los teléfonos IP 8845, 8851, 8861 y 8865 de Cisco. Los teléfonos que no admiten esta función no muestran el campo.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Permitir el modo de manos libres móvil Bluetooth	Deshabilitado Habilitado	Habilitado	<p>Permite a los usuarios aprovechar las propiedades acústicas del teléfono con su dispositivo móvil o tableta. El usuario vincula el dispositivo móvil o la tableta al teléfono mediante Bluetooth. Cuando está desactivado, el usuario no puede vincular el dispositivo móvil o tableta con su teléfono.</p> <p>Con un dispositivo móvil vinculado, el usuario puede efectuar y recibir llamadas del móvil en el teléfono. Con una tableta, el usuario puede dirigir el audio de la tableta al teléfono.</p> <p>Los usuarios pueden vincular varios dispositivos móviles, tabletas y unos auriculares Bluetooth al teléfono. Sin embargo, solo es posible conectar un dispositivo y unos auriculares al mismo tiempo.</p> <p>Los teléfonos que no admiten esta función no muestran el campo.</p>
Perfiles Bluetooth	M. libres Dispositivo de interfaz de usuario	M. libres	<p>Indica qué perfiles Bluetooth están habilitados o deshabilitados en el teléfono.</p> <p>Los teléfonos que no admiten esta función no muestran el campo.</p>
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.
Mostrar todas las llamadas en la línea principal	Deshabilitado Habilitado	Deshabilitado	<p>Especifica si se mostrarán o no todas las llamadas presentadas al teléfono en la línea principal.</p> <p>El objetivo de este campo es que sea más fácil para el usuario final ver todas las llamadas de todas las líneas de un vistazo en lugar de tener que elegir una línea para ver las llamadas de dicha línea. Es decir, cuando hay varias líneas configuradas en el teléfono, normalmente tiene más sentido poder ver todas las llamadas en todas las líneas en una pantalla combinada. Si esta función está activada, se mostrarán todas las llamadas en la línea principal, pero podrá elegir una línea específica para filtrar la visualización y ver solo las llamadas de dicha línea específica.</p>
Servidor HTTPS	HTTP y HTTPS habilitados Solo HTTPS	HTTP y HTTPS habilitados	Controla el tipo de comunicación con el teléfono. Si selecciona solo HTTPS, la comunicación del teléfono es más segura.
Servidor de registro de IPv6	Cadena de un máximo de 256 caracteres		<p>Identifica el servidor de registro de IPv6.</p> <p>El formato de la dirección es: [dirección] : <port>@base=<0-7>;pfs=<0-1></p>

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Registro remoto	Deshabilitado Habilitado	Deshabilitado	Controla la capacidad de enviar registros al servidor syslog.
Perfil de registro	Valor predeterminado Preajuste Telefonía SIP IU Red Medios Actualizar Accesorio Seguridad Wi-Fi VPN EnergyWise MobileRemoteAc	Preajuste	<p>Especifica el perfil de registro predefinido.</p> <ul style="list-style-type: none"> • 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. • Wi-Fi: registra la información sobre Wi-Fi • VPN: registra la información de red privada virtual • Energywise: registra información de ahorro de energía • MobileRemoteAC: registra el acceso móvil y remoto a través de la información de Expressway
Anunciar códecs G.722 e iSAC	Usar configuración predeterminada del sistema Deshabilitado Habilitado	Usar configuración predeterminada del sistema	<p>Indica si el teléfono anuncia los códecs G.722 e iSAC a Cisco Unified Communications Manager.</p> <ul style="list-style-type: none"> • Usar ajustes predeterminados del sistema: pasa a la configuración especificada en el parámetro de empresa Anunciar códec G.722. • Deshabilitado: no anuncia G.722 a Cisco Unified Communications Manager. • Habilita: anuncia G.722 a Cisco Unified Communications Manager. <p>Para obtener más información, consulte la nota que sigue a la tabla.</p>

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Detectar error de conexión de Unified CM	Normal Retrasada	Normal	<p>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.</p> <ul style="list-style-type: none"> • Normal: se produce la detección de un error de conexión de Unified CM a la velocidad estándar del sistema. Elija este valor para un reconocimiento más rápido de un error de conexión de Unified CM. • Retrasada: la detección de una conmutación por error de la conexión de Unified CM es aproximadamente cuatro veces más lenta que la normal. Elija este valor si prefiere que la conmutación por error se retrase ligeramente para proporcionar a la conexión la posibilidad de reestablecerse. <p>La diferencia horaria precisa entre la detección de errores de la conexión Normal y Retrasada depende de muchas variables que cambian constantemente.</p> <p>Este campo solo se aplica a la conexión Ethernet con cables.</p>
Negociación de energía	Deshabilitado Habilitado	Habilitado	<p>Permite al teléfono negociar la energía mediante el protocolo de descubrimiento de terminal de nivel de enlace (LLDP) y el Cisco Discovery Protocol (CDP).</p> <p>La negociación de energía no se debe desactivar si el teléfono está conectado a un switch que admita esa función. Si se desactiva, el switch puede cortar la energía del teléfono.</p>
Proporcionar tono de marcación mediante el botón de liberación	Deshabilitado Habilitado	Deshabilitado	<p>Controla si el usuario oye el tono de marcado cuando se pulsa la tecla de liberación.</p> <ul style="list-style-type: none"> • Desactivado: el usuario no oye el tono de marcación. • Habilitado: el usuario oye el tono de marcación.
Imagen de fondo	Cadena, hasta un máximo de 64 caracteres		<p>Especifica el archivo de papel tapiz predeterminado. Cuando se establece un papel tapiz predeterminado, el usuario no puede cambiar el papel tapiz del teléfono.</p>

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Interfaz de usuario simplificada de nueva llamada	Deshabilitado Habilitado	Deshabilitado	<p>Controla la interfaz de usuario para la marcación con el teléfono descolgado. Cuando está activada, el usuario no puede seleccionar un número de la lista de llamadas recientes.</p> <p>Cuando está activada, este campo proporciona una ventana simplificada para que el usuario realice una llamada. El usuario no verá la ventana emergente del historial de llamadas que se muestra cuando se descuelga el teléfono. La pantalla de la ventana emergente se considera útil, por lo que se desactiva la interfaz de usuario simplificada de nueva llamada de forma predeterminada.</p>
Revertir a todas las llamadas	Deshabilitado Habilitado	Deshabilitado	<p>Especifica si el teléfono volverá a todas las llamadas después de cualquier llamada finalice o no si la llamada está en un filtro distinto a Línea principal, Todas las llamadas o Llamadas de aviso.</p>
Mostrar el historial de llamadas solo para la línea seleccionada	Deshabilitado Habilitado	Deshabilitado	<p>Controla la visualización de la lista Recientes.</p> <ul style="list-style-type: none"> • Desactivado: la lista Recientes muestra el historial de llamadas de todas las líneas. • Habilitado: la lista Recientes muestra el historial de llamadas de la línea seleccionada.
Alerta de llamada entrante con acciones	Deshabilitado Mostrar todas las llamadas entrantes Mostrar la llamada entrante invisible	Mostrar todas las llamadas entrantes	<p>Controla el tipo de alerta de llamada entrante que se muestra en la pantalla del teléfono. El objetivo de este campo es reducir el número de pulsaciones de botón necesarias para que el usuario final conteste una llamada.</p> <ul style="list-style-type: none"> • Desactivado: la alerta de llamada entrante con acciones está desactivada y el usuario ve la alerta emergente de la llamada entrante tradicional. • Mostrar todas las llamadas entrantes: se muestra la alerta de llamada entrante con acciones para todas las llamadas, sin importar la visibilidad. • Mostrar llamada entrante invisible: se muestra la alerta de llamada entrante con acciones para las llamadas que no se muestran en el teléfono. El comportamiento de este parámetro es similar a la notificación emergente de llamada entrante.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Bit DF	0 1	0	<p>Controla la forma en la que se envían los paquetes de red. Los paquetes se pueden enviar en trozos (fragmentos) de varios tamaños.</p> <p>Si el bit DF se establece en 1 en el encabezado de paquete, la carga de red no se fragmenta mientras atraviesa los dispositivos de red, como switches y routers. Si se elimina la fragmentación, se evitan análisis incorrectos en el lado receptor, pero la velocidad es ligeramente inferior.</p> <p>El ajuste de bit DF no se aplica al tráfico ICMP, VPN, VXC VPN ni DHCP.</p>
Filtro de línea predeterminado	Lista de nombres de dispositivos telefónicos separados por comas		<p>Indica la lista de teléfonos que se encuentran en el filtro predeterminado.</p> <p>Cuando se configura el filtro de línea predeterminado, los usuarios ven un filtro denominado <i>Programación diaria</i> en Notificaciones de llamada en el menú Configuración > Preferencias del teléfono. Este filtro de planificación diaria se suma al filtro <i>Todas las llamadas</i> predefinido.</p> <p>Si el filtro de línea predeterminada no está configurado, el teléfono comprueba todas las líneas aprovisionadas. Si está configurado, el teléfono comprueba las líneas establecidas en Cisco Unified Communications Manager si el usuario selecciona como filtro activo el filtro predeterminado, o en caso de que no haya ningún filtro personalizado.</p> <p>Los filtros de línea personalizados permiten filtrar líneas de alta prioridad para reducir la actividad de alertas. Puede establecer la prioridad de las notificaciones de las alertas de llamadas en un subconjunto de líneas cubierto por un filtro de alertas. El filtro personalizado genera alertas emergentes tradicionales o alertas en las que se pueden realizar acciones para las llamadas entrantes de las líneas seleccionadas. En cada filtro, solo el subconjunto de líneas cubierto generará una alerta. Esta función proporciona una forma de que los usuarios con varias líneas reduzcan la actividad de alertas filtrando y visualizando alertas solo desde líneas de alta prioridad. Los usuarios finales pueden configurar esto ellos mismos. Como alternativa, puede programar el filtro de línea predeterminado y bajar el filtro para el teléfono.</p>

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Prioridad de estado de línea de alerta más baja	Deshabilitado Habilitado	Deshabilitado	Especifica el estado de alerta cuando se utilizan líneas compartidas. <ul style="list-style-type: none"> • Desactivado: si hay una alerta de llamada entrante en la línea compartida, el icono de estado LED/de línea refleja el estado de alerta en lugar del modo Remoto en uso. • Habilitado: si hay una alerta de llamada entrante en la línea compartida, el usuario verá el icono del modo Remoto en uso.
Visualización de una columna para KEM	Deshabilitado Habilitado	Deshabilitado	Controla la visualización en el módulo de expansión clave. <ul style="list-style-type: none"> • Desactivado: el módulo de expansión utiliza el modo de dos columnas. • Habilitado: el módulo de expansión utiliza el modo de una columna. Los teléfonos que no admiten esta función no muestran el campo.
Ethernet de eficacia energética (EEE): puerto PC	Deshabilitado Habilitado	Deshabilitado	controla EEE en el puerto PC.
Ethernet de eficacia energética (EEE): puerto SW	Deshabilitado Habilitado	Deshabilitado	controla EEE en el puerto conmutador.
Puerto de vídeo inicial			Define el inicio del intervalo de puertos para las llamadas de vídeo. Los teléfonos que no admiten esta función no muestran el campo.
Puerto de vídeo final			Define el final del intervalo de puertos para las llamadas de vídeo. Los teléfonos que no admiten esta función no muestran el campo.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Credenciales de usuario persistentes para el inicio de sesión de Expressway	Deshabilitado Habilitado	Deshabilitado	<p>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).</p> <p>Si desea que sea más fácil el inicio de sesión de los usuarios, 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.</p> <p>Para obtener más información, consulte el apartado Mobile and Remote Access mediante Expressway, en la página 182.</p>
URL de carga de asistencia al cliente	Cadena, hasta un máximo de 256 caracteres		<p>Proporciona la URL de la herramienta de informe de problemas (PRT).</p> <p>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.</p> <p>Para obtener más información, consulte el apartado Mobile and Remote Access mediante Expressway, en la página 182.</p>
Administrador web	Deshabilitado Habilitado	Deshabilitado	<p>Activa o desactiva el acceso de administrador a las páginas web del teléfono a través de un explorador web.</p> <p>Para obtener más información, consulte el apartado Configurar la página de administración del teléfono, en la página 109.</p> <p>Los teléfonos que no admiten esta función no muestran el campo.</p>
Admin Password (Contraseña del administrador)	Cadena de 8–127 caracteres		<p>Define la contraseña del administrador cuando accede a las páginas web del teléfono como administrador.</p> <p>Los teléfonos que no admiten esta función no muestran el campo.</p>
Servidor SCEP de WLAN	Cadena de un máximo de 256 caracteres		<p>Especifica el servidor SCEP que usa el teléfono para obtener certificados para la autenticación WLAN. Introduzca el nombre de host o la dirección IP (con el formato estándar de dirección IP) del servidor.</p> <p>Los teléfonos que no admiten esta función no muestran el campo.</p>

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Huella digital de la entidad de certificación raíz WLAN (SHA256 o SHA1)	Cadena de un máximo de 95 caracteres		<p>Especifica la huella digital SHA256 o SHA1 de la entidad de certificación raíz que usar para la validación durante el proceso SCEP cuando se emiten certificados para la autenticación de WLAN. Le recomendamos que utilice la huella digital SHA256, que se puede obtener a través de OpenSSL (por ejemplo, openssl x509 -in rootca.cer -noout -sha256 -fingerprint) o mediante un explorador web para comprobar los detalles del certificado.</p> <p>Introduzca el valor del carácter hexadecimal 64 para la huella digital SHA256 o el valor del carácter hexadecimal 40 para la huella digital SHA1 con un separador común (dos puntos, guión, período, espacio) o sin un separador. Si utiliza un separador, este debería colocarse de forma coherente después de cada 2, 4, 8, 16 o 32 caracteres hexadecimales para una huella SHA256 o cada 2, 4 o 8 caracteres hexadecimales para una huella digital SHA1.</p> <p>Los teléfonos que no admiten esta función no muestran el campo.</p>
Intentos de autenticación de WLAN			Los teléfonos que no admiten esta función no muestran el campo.
Modo de mensaje de perfil de WLAN 1	Deshabilitado Habilitado	Deshabilitado	Los teléfonos que no admiten esta función no muestran el campo.
Modo de línea	Modo de línea de sesión Modo de línea mejorado	Modo de línea de sesión	<p>Controla la visualización de la línea en el teléfono.</p> <ul style="list-style-type: none"> • Modo de línea de sesión: los botones en un lado de la pantalla son las teclas de línea. • Modo de línea mejorado: los botones situados a ambos lados de la pantalla del teléfono son teclas de línea. Las alertas de llamada entrante con acciones y la marcación predictiva están activadas de forma predeterminada en el modo de línea mejorado.
Timbre configurable del administrador	Deshabilitado Amanecer Chirp1 Chirp2	Deshabilitado	<p>Controla el tono de llamada y la posibilidad de que los usuarios definan el tono de llamada.</p> <ul style="list-style-type: none"> • Cuando se establece en Desactivado, los usuarios pueden configurar el tono de llamada predeterminado en sus teléfonos. • Para todos los demás valores, los usuarios no pueden cambiar el tono de llamada. El elemento de menú Tono de llamada del menú Configuración está atenuado.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
Uso de atención al cliente	Cadena de un máximo de 64 caracteres	Vacío	Para uso exclusivo de Cisco TAC.
Desactivación de los cifrados TLS	Consulte Desactivar los cifrados de seguridad de la capa de transporte, en la página 170 .	Ninguno	Desactiva el cifrado TLS seleccionado. 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.
Activar la alerta Bajar la voz	Habilitado Deshabilitado	Habilitado	Controla la función para bajar la voz. <ul style="list-style-type: none"> • Desactivado: <ul style="list-style-type: none"> • El teléfono no muestra el elemento de menú Bajar la voz en el menú Configuración. • Los usuarios no verán el mensaje en la pantalla cuando hablan en voz alta. • Habilitado: <ul style="list-style-type: none"> • Los usuarios pueden controlar la función desde el elemento de menú Bajar la voz en el menú Configuración. De forma predeterminada, este campo está establecido en Activado.
Marcar llamada como spam	Habilitado Deshabilitado	Habilitado	Controla la función Marcar llamada como spam. <ul style="list-style-type: none"> • Desactivado: <ul style="list-style-type: none"> • El teléfono no muestra la tecla programable Marcar como spam. • No se muestra el elemento Lista de spam en el menú Configuración. • Si hay una lista de spam, la lista se borra y no se puede recuperar. • Habilitado: <ul style="list-style-type: none"> • El teléfono muestra la tecla programable Marcar como spam. • Se muestra la Lista de spam en el menú Configuración.

Nombre del campo	Tipo de campo u opciones	Valor predeterminado	Descripción e instrucciones de uso
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.
Visualización de etiquetas de texto en línea en ELM	Deshabilitado Habilitado	Habilitado	Controla la visualización de etiquetas de línea durante una llamada cuando se ha configurado el modo de línea mejorado <ul style="list-style-type: none"> • Habilitado <ul style="list-style-type: none"> • Si el nombre de la persona que llama está configurado, muestra el nombre en la primera línea de la sesión de llamada y la etiqueta de la línea local en la segunda línea. • Si el nombre de la persona que llama no está configurado, se muestra el número remoto en la primera línea y la etiqueta de la línea local en la segunda línea. • Deshabilitado <ul style="list-style-type: none"> • Si el nombre de la persona que llama está configurado, muestra el nombre en la primera línea de la sesión de llamada y el número en la segunda línea. • Si el nombre de la persona que llama no está configurado, muestra solo el número remoto. <p>Este campo es obligatorio.</p>



Nota La negociación del códec consta de dos pasos:

1. El teléfono anuncia el códec compatible con Cisco Unified Communications Manager. No todos los terminales admiten el mismo conjunto de códecs.
2. Cuando Cisco Unified Communications Manager obtiene la lista de códecs compatibles en todos los teléfonos involucrados en el intento de llamada, selecciona un códec admitido frecuentemente en función de diversos factores, incluida la configuración de la vinculación de la región.

Prácticas recomendadas de la configuración de las funciones

Puede configurar las funciones del teléfono para satisfacer las necesidades de los usuarios. Sin embargo, tenemos algunas recomendaciones para determinadas situaciones e implementaciones que pueden ayudarle.

Entornos de volumen elevado de llamadas

En un entorno de volumen elevado de llamadas, se recomienda configurar algunas de las funciones de una forma específica.

Campo	Área de administración	Configuración recomendada
Utilizar siempre la línea principal	Información del dispositivo	Desactivar o activar Para obtener más información, consulte Campo: utilizar siempre la línea principal, en la página 170 .
Alerta de llamada entrante con acciones	Diseño de la configuración específica del producto	Mostrar todas las llamadas entrantes
Mostrar todas las llamadas en la línea principal	Diseño de la configuración específica del producto	Habilitado
Revertir a todas las llamadas	Diseño de la configuración específica del producto	Habilitado

Entornos de varias líneas

En un entorno de varias líneas, se recomienda configurar algunas de las funciones de una forma específica.

Campo	Área de administración	Configuración recomendada
Utilizar siempre la línea principal	Información del dispositivo	Desactivado Para obtener más información, consulte Campo: utilizar siempre la línea principal, en la página 170 .
Alerta de llamada entrante con acciones	Diseño de la configuración específica del producto	Mostrar todas las llamadas entrantes
Mostrar todas las llamadas en la línea principal	Diseño de la configuración específica del producto	Habilitado
Revertir a todas las llamadas	Diseño de la configuración específica del producto	Habilitado

Entorno del modo de línea de sesión

El modo de línea mejorado es la herramienta preferida para gestionar la mayoría de entornos de llamada. Sin embargo, si el modo de línea mejorado no se ajusta a sus necesidades, puede usar el modo de línea de sesión.

Campo	Área de administración	Configuración recomendada para el modo de línea de sesión
Mostrar todas las llamadas en la línea principal	Diseño de la configuración específica del producto	Deshabilitado

Campo	Área de administración	Configuración recomendada para el modo de línea de sesión
Revertir a todas las llamadas	Diseño de la configuración específica del producto	Deshabilitado
Alerta de llamada entrante con acciones	Diseño de la configuración específica del producto	Activado de forma predeterminada (versión de firmware 11.5(1) y posterior).

Temas relacionados

[Configuración de teclas de línea adicionales](#), en la página 205

[Funciones disponibles en el modo de línea mejorado](#), en la página 206

Campo: utilizar siempre la línea principal

Este campo especifica si se elige la línea principal en un teléfono IP cuando un usuario descuelga. Si este parámetro se establece en Verdadero, cuando se descuelga el teléfono, se elige la línea principal y se convierte en la línea activa. Incluso si suena una llamada en la segunda línea del usuario, cuando el teléfono se descuelga, hace que solo la primera línea esté activa. No contesta a la llamada entrante en la segunda línea. En este caso, el usuario debe elegir la segunda línea para contestar la llamada. El valor predeterminado está establecido en Falso.

El propósito del campo Utilizar siempre la línea principal es muy similar a la combinación de Mostrar todas las llamadas en Línea principal y Revertir a todas las llamadas cuando ambas funciones están activadas. Sin embargo, la diferencia principal es que cuando Utilizar siempre la línea principal está activado, las llamadas entrantes no se contestan en la segunda línea. El tono de marcación solo se oye en la línea principal. Existen ciertos entornos de volumen elevado de llamadas en los que esta es la experiencia de usuario deseada. Por lo general, es mejor dejar este campo desactivado, excepto para los entornos de volumen elevado de llamadas que requieran esta función.

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>).

Activación del historial de llamadas para la línea compartida

Permite ver la actividad de la línea compartida en el historial de llamadas. Esta función:

- Registra llamadas perdidas de una línea compartida.
- Registra todas las llamadas contestadas y efectuadas de una línea compartida.

Antes de empezar

Desactive la función de privacidad antes de activar el historial de llamadas de una línea compartida. De lo contrario, el historial de llamadas no mostrará las llamadas a las que responden otros usuarios.

Procedimiento

-
- Paso 1** En Cisco Unified Communications Manager Administration, seleccione **Dispositivo > Teléfono**.
- Paso 2** Localice el teléfono que desea configurar.
- Paso 3** Navegue al menú desplegable Grabar registro de llamadas desde línea compartida en la sección de configuración específica del producto.
- Paso 4** Seleccione **Activado** en la lista desplegable.
- Paso 5** Seleccione **Guardar**.
-

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.

Para obtener más información, consulte [Configuración específica del producto](#), en la página 146

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 32: Campos de Configuración de PowerSave

Campo	Descripción
Días pantalla no activa	<p>Los días que la pantalla no se enciende automáticamente a la hora especificada en el campo Hora de activación de pantalla.</p> <p>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.</p>
Hora de activación de pantalla	<p>La hora de cada día a la que se enciende automáticamente la pantalla (excepto los días especificados en el campo Días pantalla no activa).</p> <p>En este campo, debe introducir la hora en formato de 24 horas, donde 0:00 es la medianoche.</p> <p>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.</p> <p>Si el campo está vacío, la pantalla se enciende automáticamente a las 0:00.</p>
Duración actividad de pantalla	<p>El período que la pantalla permanecerá activada tras encenderse a la hora especificada en el campo Hora de activación de pantalla.</p> <p>Introduzca el valor en este campo con el formato <i>horas:minutos</i>.</p> <p>Por ejemplo, para que la pantalla siga encendida 4 horas y 30 minutos después de encenderse automáticamente, introduzca 04:30.</p> <p>Si el campo está vacío, el teléfono se apaga al final del día (0:00).</p> <p>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.</p>

Campo	Descripción
Tiempo espera pantalla inactiva	<p>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).</p> <p>Introduzca el valor en este campo con el formato <i>horas:minutos</i>.</p> <p>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.</p> <p>El valor predeterminado es 01:00.</p>

- 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.

Para obtener más información, consulte [Configuración específica del producto, en la página 146](#)

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 33: Campos de Configuración de EnergyWise

Campo	Descripción
Activar Power Save Plus	<p>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.</p> <p>De forma predeterminada, no hay ningún día seleccionado.</p> <p>Si la casilla Activar Power Save Plus está marcada, recibirá un mensaje de advertencia sobre los servicios de emergencia (e911).</p> <p>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.</p> <p>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.</p>
Hora de encendido del teléfono	<p>Determina la hora a la que el teléfono se enciende automáticamente los días indicados en el campo Activar Power Save Plus.</p> <p>En este campo, debe introducir la hora en formato de 24 horas, donde 00:00 es la medianoche.</p> <p>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.</p> <p>El valor predeterminado es dejar el campo vacío, que indica las 00:00.</p> <p>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.</p>

Campo	Descripción
Hora de apagado del teléfono	<p>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.</p> <p>En este campo, debe introducir la hora en formato de 24 horas, donde 00:00 es la medianoche.</p> <p>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.</p> <p>El valor predeterminado es dejar el campo vacío, que indica las 00:00.</p> <p>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.</p>
Tiempo de espera de inactividad para apagar el teléfono	<p>El período que el teléfono debe estar inactivo antes de que se apague.</p> <p>El tiempo de espera se agota si se dan las siguientes condiciones:</p> <ul style="list-style-type: none"> • 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. <p>El intervalo para el campo es de entre 20 y 1440 minutos.</p> <p>El valor predeterminado es 60 minutos.</p>
Activar alerta sonora	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>Esta casilla de verificación solo se aplica si en la lista de Activar Power Save Plus se han seleccionado uno o varios días.</p>
Dominio de EnergyWise	<p>El dominio de EnergyWise en el que se encuentra el teléfono.</p> <p>La longitud máxima de este campo es de 127 caracteres.</p>
Secreto de EnergyWise	<p>La contraseña secreta de seguridad que se usa para comunicarse con los terminales del dominio de EnergyWise.</p> <p>La longitud máxima de este campo es de 127 caracteres.</p>

Campo	Descripción
Permitir anulaciones de EnergyWise	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <ul style="list-style-type: none"> • 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. <p>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.</p>

Paso 4 Seleccione **Guardar**.

Paso 5 Seleccione **Aplicar configuración**.

Paso 6 Reinicie el teléfono.

Configuración de la función No molestar

Si la función No molestar (DND) está activada, no se produce ningún timbre audible mientras suena la llamada o no se producen notificaciones sonoras ni visuales de ningún tipo.

Si No molestar (DND) está activado, la sección de encabezado de la pantalla del teléfono cambia de color y se muestra el mensaje `No molestar` en el teléfono.

Puede configurar el teléfono con una plantilla de botones de teléfono que tenga DND como una de las funciones seleccionadas.

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.
No elija Rechazo de llamada si desea que las llamadas de prioridad (MLPP) suenen en este teléfono cuando se active DND.
- 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 xv

Activación del saludo de agente

La función Saludo de agente permite a un agente crear y actualizar un saludo pregrabado que se reproduce al inicio de una llamada, como por ejemplo, la llamada de un cliente, antes de que el agente inicie la conversación con quien ha realizado la llamada. El agente puede pregrabar uno o varios saludos, según se precise, así como crear y actualizar los saludos.

Cuando llama un cliente, tanto el agente como el cliente escuchan el saludo pregrabado. El agente puede permanecer en silencio hasta que finalice el mensaje o contestar la llamada mientras se reproduce.

Todos los códecs admitidos por el teléfono se admiten en las llamadas de saludo de agente.

Para obtener más información, consulte los datos sobre intrusión y privacidad 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 Busque el teléfono IP que desea configurar.

Paso 3 Diríjase al panel de diseño de la información del dispositivo y en **Puente integrado** establezca Activar o Predeterminado.

Paso 4 Seleccione **Guardar**.

Paso 5 Compruebe la configuración del puente:

- a) Seleccione **Sistema > Parámetros de servicio**.
- b) Seleccione el servidor y el servicio apropiados.
- c) Diríjase al panel de parámetros para todo el clúster (Dispositivo - Teléfono) y en **Puente integrado** establezca Activar.

d) Seleccione **Guardar**.

Temas relacionados

[Cisco Unified Communications Manager Documentación](#), en la página xv

Configuración de las funciones de supervisión y grabación

Las funciones Supervisión y Grabación permiten a un supervisor controlar en silencio una llamada activa. Ninguna de las partes de la llamada podrá oír al supervisor. El usuario podría recibir una alerta sonora durante las llamadas que se controlan.

Si una llamada es segura, se muestra un icono de candado. La persona que llama también puede recibir una alerta sonora para indicar que la llamada se está supervisando. Las partes conectadas también podrían recibir una alerta sonora que indica que la llamada está asegurada y se está supervisando.

Cuando se supervisa o se graba una llamada activa, el usuario puede recibir o efectuar llamadas de intercomunicación; sin embargo, si el usuario efectúa una llamada de intercomunicación, la llamada activa se pone en pausa. Esto provoca que la sesión de grabación se interrumpa y la de supervisión se suspenda. Para reanudar la sesión de supervisión, la persona cuya llamada se está supervisando debe reanudar la llamada.

Para obtener más información, consulte los datos sobre cómo supervisar y grabar en la documentación de su versión concreta de Cisco Unified Communications Manager.

Mediante el procedimiento siguiente se agrega a un usuario a los grupos de usuarios de supervisión estándar.

Antes de empezar

Cisco Unified Communications Manager debe estar configurado para admitir las funciones de supervisión y grabación.

Procedimiento

-
- Paso 1** En Cisco Unified Communications Manager Administration, seleccione **Administración de usuarios > Usuario de aplicación**.
 - Paso 2** Marque los grupos de usuarios de permiso de supervisión de llamadas estándar CTI y los grupos de usuarios de permiso de grabación de llamadas estándar CTI.
 - Paso 3** Haga clic en **Agregar seleccionados**.
 - Paso 4** Haga clic en **Agregar a grupo de usuarios**.
 - Paso 5** Agregue los teléfonos del usuario a la lista de dispositivos controlados por los usuarios de la aplicación.
 - Paso 6** Seleccione **Guardar**.

Temas relacionados

[Cisco Unified Communications Manager Documentación](#), en la página xv

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 desvió 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**.

Activación de BLF para listas de llamadas

El campo BLF para listas de llamadas también controla la función Estado de línea del directorio corporativo.

Procedimiento

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

Paso 2 En el campo BLF para listas de llamadas, active o desactive la función.

Esta función está desactivada de forma predeterminada.

Los parámetros que se establecen en la sección Configuración específica de producto también pueden aparecer en la ventana de configuración de diversos dispositivos, así como en la ventana Configuración de teléfono empresarial. Si establece estos mismos parámetros también en esas otras ventanas, el ajuste que tendrá precedencia se determinará en el orden siguiente:

1. Los ajustes de la ventana Configuración del dispositivo
2. Los ajustes de la ventana Perfil de teléfono común
3. Los ajustes de la ventana Configuración de teléfono empresarial

Paso 3 Seleccione **Guardar**.

Configuración de Ethernet de eficacia energética para el puerto PC y de switch

La Ethernet de eficacia energética (EEE) IEEE 802.3az es una extensión del estándar IEEE 802.3 que proporciona un método para reducir el consumo de energía sin reducir las funciones vitales de las interfaces de red. La EEE configurable permite al administrador controlar las funciones de EEE en los puertos PC y de switch.



Nota Los administradores deben confirmar que la casilla de verificación Sobrescribir está marcada en todas las páginas aplicables de UCM o EEE no funcionará.

El administrador controla las funciones de EEE con los dos parámetros siguientes:

- **Ethernet de consumo eficiente.** Puerto PC: proporciona una conexión sin pérdida con ordenadores personales. El administrador puede seleccionar las opciones Activado o Desactivado para controlar la función.
- **Ethernet de consumo eficiente.** Puerto switch: proporciona una conexión sin pérdida.

Para obtener más información, consulte [Configuración específica del producto, en la página 146](#)

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione una de las ventanas siguientes:

- **Dispositivo > Teléfono**
- **Dispositivo > Configuración del dispositivo > Perfil de teléfono común**
- **Sistema > Configuraciones del teléfono empresarial**

Si configura el parámetro en varias ventanas, el orden de precedencia es el siguiente:

1. **Dispositivo > Teléfono**
2. **Dispositivo > Configuración del dispositivo > Perfil de teléfono común**
3. **Sistema > Configuraciones del teléfono empresarial**

- Paso 2** Si fuera necesario, localice el teléfono.
- Paso 3** Configure los campo **Ethernet de consumo eficiente: puerto PC** y **Configuración de la Ethernet de consumo eficiente para el puerto y el switch: puerto switch**.
- Ethernet de eficacia energética: puerto PC
 - Ethernet de eficacia energética: puerto switch
- Paso 4** Seleccione **Guardar**.
- Paso 5** Seleccione **Aplicar configuración**.
- Paso 6** Reinicie el teléfono.
-

Configuración del intervalo de puertos RTP/sRTP

Puede configurar los valores de los puertos del protocolo de transporte en tiempo real (RTP) y del protocolo seguro de transporte en tiempo real (sRTP) en el perfil SIP. Los valores de los puertos RTP y sRTP van de 2048 a 65535, con un rango predeterminado de 16384 a 32764. Algunos valores de puerto dentro del rango de puertos RTP y sRTP están designados para otros servicios telefónicos. No es posible configurar esos puertos para RTP ni sRTP.

Para obtener más información, consulte los datos sobre el perfil SIP en la documentación de su versión concreta de Cisco Unified Communications Manager.

Procedimiento

- Paso 1** Seleccione **Dispositivo > Configuración del dispositivo > Perfil SIP**.
- Paso 2** Seleccione los criterios de búsqueda que desea usar y haga clic en **Buscar**.
- Paso 3** Seleccione el perfil que desea modificar.
- Paso 4** Establezca los valores de Puerto de medios inicial y Puerto de medios final para indicar el intervalo de puertos correspondiente.

En la lista siguiente se identifican los puertos UDP que se usan para otros servicios del teléfono y que, por tanto, no están disponibles para usarse en los protocolos RTP y sRTP:

Puerto 4051

Se usa para la función Compartir firmware en el grupo (PFS).

Puerto 5060

Se usa para el transporte de SIP por UDP.

Intervalo de puertos del 49152 al 53247

Se usa para los puertos efímeros locales.

Intervalo de puertos del 53248 al 65535

Se usa para la función de VPN de túnel sencillo VxC.

- Paso 5** Haga clic en **Guardar**.

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

Temas relacionados

[Cisco Unified Communications Manager Documentación](#), en la página xv

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).

Mobile and Remote Access mediante Expressway admite el modo de línea mejorado.

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 las secciones siguientes se muestran varias situaciones de implementación para Mobile and Remote Access mediante Expressway.

El usuario que se encuentra en las instalaciones inicia sesión en la red empresarial

Después de implementar Mobile and Remote Access mediante Expressway, inicie sesión en la red empresarial cuando esté en las instalaciones. El teléfono detecta la red y se registra con Cisco Unified Communications Manager.

El usuario que se encuentra fuera de las instalaciones inicia sesión en la red empresarial

Cuando esté fuera de la oficina, el teléfono detectará que se encuentra en el modo externo. Se mostrará la ventana de inicio de sesión Mobile and Remote Access mediante Expressway y se conectará a la red corporativa.

Tenga en cuenta los siguientes aspectos:

- Usted debe tener un dominio de servicio válido, un nombre de usuario y una contraseña para conectarse a la red.
- Restablezca el modo de servicio para borrar el ajuste de TFTP alternativo para poder acceder a la red de la empresa. De esta forma, se borra el ajuste de Servidor TFTP alternativo para garantizar que el teléfono detecte la red externa y no realice una conexión VPN. Omitir este paso si se va a implementar un teléfono por primera vez.
- Si tiene la opción 150 o la opción 66 de DHCP habilitadas en el router de red, quizás no pueda iniciar sesión en la red corporativa. Restablezca su modo de servicio para entrar en el modo de MRA.

El usuario que se encuentra fuera de las instalaciones inicia sesión en la red empresarial con una VPN

Cuando se encuentre fuera de las instalaciones, inicie en la red de la empresa mediante VPN después de implementar Mobile and Remote Access mediante Expressway.

Lleve a cabo un restablecimiento básico para restablecer las configuraciones de teléfono si produce un error en el teléfono.

Debe configurar el ajuste de TFTP alternativo (**Config. admin.** > **Ajustes de red** > **IPv4**, campo **Servidor TFTP alternativo 1**).

Temas relacionados

[Restauración básica](#), en la página 279

Rutas de medios y establecimiento interactivo de conectividad

Es posible implementar el establecimiento interactivo de conectividad (ICE) para mejorar la fiabilidad de Mobile and Remote Access (MRA) de las llamadas que pasan a un servidor de seguridad o la traducción de direcciones de red (NAT). ICE es una implementación opcional que utiliza el túnel de serie y transversal utilizando retransmisiones alrededor de servicios NAT para seleccionar la mejor ruta de medios para una llamada.

No se admite la conmutación por error de servidor Turn secundario ni la conmutación por error de servidor Turn.

Para obtener más información sobre MRA e ICE, consulte *Guía de configuración del sistema para Cisco Unified Communications Manager, versión 12.0(1)* o posterior. También puede encontrar información adicional en la solicitud de Internet Engineering Task Force (IETF) para los documentos de comentario:

- *Traversal Usando Relés alrededor de NAT (TURN): Extensiones de Relé a Utilidades de Traversal de Sesión para NAT (STUN)*(RFC 5766)
- *Establecimiento interactivo de conectividad (ICE): Un protocolo de traducción de dirección de red NAT (traductor) transversal para protocolos de oferta/respuesta* (RFC 5245)

Características del teléfono disponibles para Mobile and Remote Access mediante Expressway

Mobile and Remote Access mediante Expressway proporciona acceso seguro sin VPN a los servicios de colaboración Cisco para los usuarios móviles y remotos. Pero, para proteger la seguridad de la red, limita el acceso a determinadas características del teléfono.

En la lista siguiente se muestran las características del teléfono disponibles con Mobile and Remote Access mediante Expressway.

Tabla 34: Compatibilidad de funciones y Mobile and Remote Access mediante Expressway

Característica del teléfono	Versión de firmware del teléfono
Marcación abreviada	10.3 (1) y posterior
Contestar más antigua	11.5 (1)SR1 y posterior
Aparcamiento asistido de llamadas dirigido	10.3 (1) y posterior
Contestación automática	11.5 (1)SR1 y posterior
Intrusión e IntruCf	11.5 (1)SR1 y posterior
Campo Indicador luminoso de ocupación (BLF)	10.3 (1) y posterior
Captura del campo Indicador luminoso de ocupación (BLF)	10.3 (1) y posterior
Marcación rápida de Busy Lamp Field (BLF)	10.3 (1) y posterior
Retrollamada	10.3 (1) y posterior

Característica del teléfono	Versión de firmware del teléfono
Desviar una llamada	10.3 (1) y posterior
Notificación de desvío de llamadas	10.3 (1) y posterior
Aparcar llamada	10.3 (1) y posterior
Captura de llamadas	10.3 (1) y posterior
Nivel de servicio de Cisco Unified	11.5 (1)SR1 y posterior
Licencia de acceso de cliente (CAL)	11.5 (1)SR1 y posterior
Conferencia	10.3 (1) y posterior
Lista de la conferencia/Eliminar al participante	11.5 (1)SR1 y posterior
Directorio corporativo	11.5 (1)SR1 y posterior
Aplicaciones CTI (con control CTI)	11.5 (1)SR1 y posterior
Transferencia directa	10.3 (1) y posterior
Aparcamiento de llamadas dirigido	10.3 (1) y posterior
Timbre distintivo	11.5 (1)SR1 y posterior
Desviar	10.3 (1) y posterior
Modo de línea mejorado	12.1 (1) y posterior
Desviar	10.3 (1) y posterior
Códigos de acceso forzoso y códigos de asunto de cliente	11.5 (1)SR1 y posterior
Captura de llamadas de grupo	10.3 (1) y posterior
Espera/Continuar	10.3 (1) y posterior
Reversión en espera	10.3 (1) y posterior
Desvío inmediato	10.3 (1) y posterior
Conexión	10.3 (1) y posterior
Identificación de llamadas maliciosas (IdLMali)	11.5 (1)SR1 y posterior
Conferencias Meet Me	10.3 (1) y posterior
Indicador de mensaje en espera	10.3 (1) y posterior
Mobile Connect	10.3 (1) y posterior
Acceso de voz móvil	10.3 (1) y posterior

Característica del teléfono	Versión de firmware del teléfono
Servicio de precedencia multinivel y de preferencia (MLPP)	11.5 (1)SR1 y posterior
Multilínea	11.5 (1)SR1 y posterior
Música en espera	10.3 (1) y posterior
Silencio	10.3 (1) y posterior
Perfiles de red (automáticos)	11.5 (1)SR1 y posterior
Marcación con el auricular descolgado	10.3 (1) y posterior
marcar con el auricular colgado	10.3 (1) y posterior
Marcación con el signo más	10.3 (1) y posterior
Privacidad	11.5 (1)SR1 y posterior
Señalización manual automática de línea privada (PLAR)	11.5 (1)SR1 y posterior
Rellamar	10.3 (1) y posterior
Marcación rápida (no es compatible con una pausa)	10.3 (1) y posterior
Botón de URL de servicios	11.5 (1)SR1 y posterior
Transferir	10.3 (1) y posterior
Marcación con identificador uniforme de recursos (URI)	10.3 (1) y posterior

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 144

[Configuración específica del producto](#), en la página 146

Generación de un código QR para el inicio de sesión de MRA

Los usuarios que tengan un teléfono con cámara pueden escanear un código QR para iniciar sesión en MRA, en lugar de introducir el dominio del servicio y su nombre de usuario de forma manual.

Procedimiento

-
- Paso 1** Use un generador de código QR para generar un código de este tipo con el dominio del servicio o bien con el dominio del servicio y el nombre de usuario separados por una coma. Por ejemplo: mra.ejemplo.com o mra.ejemplo.com,nombreusuario.
- Paso 2** Imprima el código QR y proporciónese lo al usuario.
-

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 compartan la línea, marque la casilla de verificación Actualizar configuración de dispositivo compartido y haga clic en **Propagar seleccionado**.
 - Paso 5** Seleccione **Guardar**.
-

Configuración de la información de banco doble

Para configurar la información de banco doble, siga estos pasos:

Procedimiento

- Paso 1** En Cisco Unified Communications Manager Administration, seleccione **Dispositivo > Valores predeterminados de dispositivo**.
 - Paso 2** Compruebe la información de carga en el campo de información de carga inactiva.
 - Paso 3** Seleccione **Administración masiva > Importar/Exportar > Exportar > Valores predeterminados de dispositivo** y programe un trabajo de exportación.
 - Paso 4** Descargue el archivo tar exportado y descomprímalo.
 - Paso 5** Compruebe el formato del archivo CSV exportado y compruebe que tiene una columna de información de carga inactiva con el valor correcto.
- Nota** El valor del archivo CSV debe coincidir con el valor predeterminado del dispositivo de la ventana Cisco Unified Communications Manager Administration.
-

Supervisión de aparcamiento

La supervisión de aparcamiento solo se admite si un teléfono IP de Cisco aparca una llamada. Esta función controla el estado de una llamada aparcada. El bocadillo de llamada de supervisión de aparcamiento no se borra hasta que la llamada aparcada se recupera o se abandona. Esta llamada aparcada se puede recuperar mediante el propio bocadillo de llamada en el teléfono desde el que se aparcó.

Configuración de los temporizadores de supervisión de aparcamiento

Cisco Unified Communications Manager Administration proporciona tres parámetros de servicio para todo el clúster destinados al control del aparcamiento: temporizador de reversión de supervisión de aparcamiento, temporizador de reversión periódica de supervisión de aparcamiento y temporizador sin recuperación de desvío de supervisión de aparcamiento. Cada parámetro de servicio incluye un valor predeterminado y no requiere configuración especial alguna. Estos parámetros de temporizador solo sirven para la supervisión del aparcamiento; el temporizador de visualización de aparcamiento de llamada y el temporizador de reversión de aparcamiento de llamada no se usan para la supervisión del aparcamiento. Consulte la tabla siguiente para ver las descripciones de estos parámetros.

Configure los temporizadores en la página de parámetro de servicio de Cisco Unified Communications Manager.

Procedimiento

- Paso 1** En Cisco Unified Communications Manager Administration, seleccione **Sistema > Parámetros de servicio**.
- Paso 2** Actualice los campos de temporizador de reversión de supervisión de aparcamiento, temporizador de reversión periódica de supervisión de aparcamiento y temporizador sin recuperación de desvío de supervisión de aparcamiento en el panel de parámetros para todo el clúster (Funciones-General).

Tabla 35: Parámetros de servicio para la supervisión de aparcamiento

Campo	Descripción
Temporizador de reversión de supervisión de aparcamiento	<p>El valor predeterminado es 60 segundos. Este parámetro determina el número de segundos que Cisco Unified Communications Manager espera antes de solicitar al usuario que recupere una llamada aparcada. El temporizador se inicia cuando el usuario pulsa Aparcar en el teléfono y se abre un recuadro de diálogo cuando el temporizador llega a su fin.</p> <p>Es posible sustituir el valor especificado en este parámetro de servicio en cada línea de la sección de supervisión de aparcamiento de la ventana de configuración del número de directorio (en Cisco Unified Communications Manager Administration, seleccione Llamada en espera > Número de directorio). Especifique el valor 0 para utilizar de inmediato el intervalo de reversión periódica especificado en el parámetro de servicio de temporizador de reversión periódica de supervisión de aparcamiento (consulte la descripción siguiente). Por ejemplo, si este parámetro tiene el valor cero y el temporizador de reversión periódica de supervisión de aparcamiento tiene el valor 15, el usuario recibe un aviso inmediato de llamada aparcada cada 15 segundos hasta que el temporizador sin recuperación de desvío de supervisión de aparcamiento (consulte la descripción más abajo) llega a su fin.</p>
Temporizador de reversión periódica de supervisión de aparcamiento	<p>El valor predeterminado es 30 segundos. Este parámetro determina el intervalo (en segundos) que Cisco Unified Communications Manager espera antes de volver a recordar al usuario que hay una llamada aparcada. Para conectar con la llamada aparcada, el usuario solo tiene que descolgar durante unos segundos. Cisco Unified Communications Manager sigue avisando al usuario sobre la llamada aparcada mientras esta permanezca en ese estado y hasta que llega la hora indicada en el temporizador sin recuperación de desvío de supervisión de aparcamiento (consulte la descripción a continuación). Especifique el valor de 0 para desactivar los avisos periódicos sobre la llamada aparcada.</p>

Campo	Descripción
Temporizador sin recuperación de desvío de supervisión de aparcamiento	El valor predeterminado es 300 segundos. Este parámetro determina el número de segundos transcurrir para que se produzcan las notificaciones de recordatorio de aparcamiento antes de que una llamada que se ha aparcado se desvíe al destino de no recuperación de desvío de supervisión de aparcamiento, que se especifica en la ventana de configuración del número de directorio del usuario que ha aparcado la llamada (si el usuario proporciona ningún destino en Cisco Unified Communications Manager Administration, la llamada se desvía a la línea desde la que se aparcó). Este parámetro se inicia cuando se alcanza la hora especificada en el parámetro de servicio de temporizador de reversión de supervisión de aparcamiento. Cuando el temporizador de supervisión de aparcamiento sin recuperación de desvío de supervisión de aparcamiento llega a su fin, la llamada se elimina del estado de aparcamiento y se desvía al destino especificado o vuelve a la línea del usuario que la aparcó.

Establecimiento de los parámetros de supervisión de aparcamiento para los números de directorio

La ventana de configuración Número de directorio contiene una sección de supervisión de aparcamiento donde puede configurar tres parámetros.

Procedimiento

- Paso 1** En Cisco Unified Communications Manager Administration, seleccione **Llamada en espera > Número de directorio**.
- Paso 2** Configure los campos de supervisión de aparcamiento como se describe en la tabla siguiente.

Tabla 36: Parámetros de supervisión de aparcamiento

Campo	Descripción
Destino externo sin recuperación de desvío de supervisión de aparcamiento	Si el destino del aparcamiento es una parte externa, la llamada se desvía al destino especificado en el parámetro Destino externo sin recuperación de desvío de supervisión de aparcamiento del usuario que realizó el aparcamiento. Si el valor del campo Destino externo sin recuperación de desvío está vacío, el destinatario del aparcamiento se redirige a la línea del usuario que realizó el aparcamiento.
Destino interno sin recuperación de desvío de supervisión de aparcamiento	Si el destino del aparcamiento es una parte interna, la llamada se desvía al destino especificado en el parámetro Destino interno sin recuperación de desvío de supervisión de aparcamiento del usuario que realizó el aparcamiento. Si el valor del campo Destino interno sin recuperación de desvío está vacío, el destinatario del aparcamiento se redirige a la línea del usuario que realizó el aparcamiento.

Campo	Descripción
Temporizador de reversión de supervisión de aparcamiento	<p>Este parámetro determina el número de segundos que Cisco Unified Communications Manager espera antes de solicitar al usuario que recupere una llamada que ha aparcado. El temporizador se inicia cuando el usuario pulsa Aparcar en el teléfono y se abre un recordatorio cuando el temporizador llega a su fin.</p> <p>El valor predeterminado es de 60 segundos.</p> <p>Si configura un valor distinto a cero, este sustituye al valor establecido para este parámetro en la ventana Parámetros de servicio. Sin embargo, si configura aquí un valor 0, entonces se usa el valor presente en la ventana Parámetros de servicio.</p>

Configuración de la supervisión de aparcamiento para las listas de grupos de salto

Cuando se aparca una llamada que se aparcó mediante la lista de grupo de salto, se usa el valor del parámetro de destino sin recuperación de desvío de supervisión de aparcamiento de cabecera de grupo de salto (a no ser que esté vacío) cuando el temporizador sin recuperación de desvío de supervisión de aparcamiento llega a su fin.

Procedimiento

Paso 1 En Cisco Unified Communications Manager Administration, seleccione **Llamada en espera > Ruta/Grupo de salto > Cabecera de grupo de salto**.

Paso 2 Establezca el parámetro de destino sin recuperación de desvío de supervisión de aparcamiento de cabecera de grupo de salto.

Si el valor de ese parámetro está vacío, la llamada se desvía al destino configurado en la ventana de configuración Número de directorio cuando el temporizador sin recuperación de desvío de supervisión de aparcamiento llega a su fin.

Configuración del intervalo de puertos de audio y vídeo

El tráfico de audio y vídeo se puede enviar a distintos intervalos de puertos RTP a fin de mejorar la calidad del servicio (QoS).

Los campos siguientes controlan los intervalos de puertos en Cisco Unified Communications Manager Administration:

- Puertos de audio
 - Puerto de medios inicial (predeterminado: 16384)
 - Puerto de medios final (predeterminado: 32766)
- Puertos de vídeo

- Vídeo inicial (se usa para definir el puerto de vídeo inicial)
 - Mínimo: 2048
 - Máximo: 65535
- Vídeo final (se usa para definir el puerto de vídeo final)
 - Mínimo: 2048
 - Máximo: 65535

Las reglas siguientes se aplican a la hora de configurar los campos de puertos de vídeo:

Después de configurar el puerto RTP de vídeo inicial y final, el teléfono usa puertos del intervalo para el tráfico de vídeo. El tráfico de audio usa los puertos de medios.

Si los intervalos de puertos de audio y de vídeo se solapan, los puertos superpuestos portarán tanto tráfico de audio como de vídeo. Si el intervalo de puertos de vídeo no se configura correctamente, el teléfono usa los puertos de audio configurados tanto para el tráfico de audio como para el de vídeo.

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

Procedimiento

- Paso 1** En Cisco Unified Communications Manager Administration, seleccione **Dispositivo > Configuración del dispositivo > Perfil de SIP**.
- Paso 2** Establezca los valores de los campos Puerto de medios inicial y Puerto de medios final para indicar el intervalo de puertos de audio.
- Paso 3** Seleccione **Guardar**.
- Paso 4** Seleccione una de las ventanas siguientes:
- **Sistema > Configuración de teléfono empresarial**
 - **Dispositivo > Configuración del dispositivo > Perfil de teléfono común**
 - **Dispositivo > Teléfono > Configuración del teléfono**
- Paso 5** Establezca los valores de los campos Puerto RTP de vídeo inicial y Puerto RTP de vídeo final para indicar el intervalo de puertos necesario.
- Las reglas siguientes se aplican a la hora de configurar los campos de puertos de vídeo:
- El valor del campo Puerto RTP de vídeo final debe ser mayor que el del campo Puerto RTP de vídeo inicial.
 - La diferencia entre los campos debe ser de al menos 16.
- Paso 6** Seleccione **Guardar**.

Temas relacionados

[Cisco Unified Communications Manager Documentación](#), en la página xv

Configurar Cisco IP Manager Assistant

Cisco IP Manager Assistant (Cisco IPMA) ofrece enrutamiento de llamadas y otras funciones de administración de llamadas que ayudan a que jefes y asistentes puedan manejar las llamadas de una forma más eficaz.

Los servicios IPMA deben estar configurados en Cisco Unified Communications Manager para que pueda acceder a ellos. Para obtener información detallada sobre cómo configurar IPMA, consulte la *Guía de configuración de funciones de Cisco Unified Communications Manager*.

IPMA consta de tres componentes principales:

Jefe

Un administrador tiene llamadas interceptadas por el servicio de enrutamiento de llamadas.

Asistente

El asistente administra las llamadas en nombre de un administrador.

Assistant Console

Assistant Console es una aplicación de escritorio que pueden usar los asistentes para realizar tareas y administrar la mayoría de las funciones.

IPMA admite dos modos de funcionamiento: compatibilidad de línea proxy y compatibilidad de línea compartida. Ambos modos admiten varias llamadas por línea para el jefe. El servicio IPMA admite tanto la compatibilidad de línea proxy como de línea compartida en un clúster.

En el modo de línea compartida, el jefe y el asistente comparten un número de directorio y las llamadas se controlan en la línea compartida. Tanto el teléfono del jefe como el del asistente suenan cuando se recibe una llamada en la línea compartida. El modo de línea compartida no admite la selección de asistente por defecto, vigilancia de asistente, el filtrado de llamadas ni la función para desviar todas las llamadas.

Si configura Cisco IPMA en modo de línea compartida, el gestor y el asistente comparten un número de directorio; por ejemplo, 1701. El asistente gestiona las llamadas del gestor en el número de directorio compartido. Si un jefe recibe una llamada en el número de directorio 1701, sonarán tanto su teléfono como el del asistente.

No todas las funciones de Cisco IPMA están disponibles en el modo de línea compartida, como la selección predeterminada de asistente, vigilancia de asistente, el filtrado de llamadas y el desvío de todas las llamadas. Los asistentes no pueden ver ni tener acceso a estas funciones en la aplicación Assistant Console. El teléfono del asistente no cuenta con la tecla programada correspondiente a la función Desviar todas. El teléfono del jefe no cuenta con las teclas programables de vigilancia de asistente, interceptación de llamadas ni la función Desviar todas.

Para poder acceder a la compatibilidad de línea compartida en los dispositivos de usuario, primero debe usar Cisco Unified Communications Manager Administration para configurar e iniciar el servicio Cisco IP Manager Assistant.

En el modo de línea proxy, el asistente controla las llamadas de un jefe mediante un número de proxy. El modo de línea proxy admite todas las funciones de IPMA.

Si configura Cisco IPMA en el modo de línea proxy, el jefe y el asistente no comparten número de directorio. El asistente controla las llamadas de un jefe mediante un número de proxy. El número de proxy no es el número de directorio del jefe. Es un número alternativo elegido por el sistema y que el asistente utiliza para manejar las llamadas del jefe. En modo de línea proxy, jefes y asistentes tienen acceso a todas las funciones disponibles en IPMA, entre las que se incluyen la selección de asistente predeterminado, vigilancia de asistente, el filtrado de llamadas y el desvío de todas las llamadas.

Para poder acceder a la compatibilidad de línea proxy en los dispositivos de usuario, primero debe usar Cisco Unified Communications Manager Administration para configurar e iniciar el servicio Cisco IP Manager Assistant.

Acceda a las funciones de IPMA mediante teclas programables y a través de los servicios telefónicos. La plantilla de teclas programables se configura en Cisco Unified Communications Manager. IPMA admite las plantillas de teclas programables estándar siguientes:

Jefe estándar

Para el jefe en modo proxy.

Jefe en modo compartido estándar

Para el jefe en modo compartido.

Asistente estándar

Para el asistente tanto en modo proxy como compartido.

En la tabla siguiente se describen las teclas programables disponibles en las plantillas de teclas programables.

Tabla 37: Teclas programables de IPMA

Tecla programable	Estado de la llamada	Descripción
Redirigir	Llamando, Conectada, En espera	Desvía la llamada seleccionada a un destino preconfigurado.
Interceptar	Todos los estados	Desvía una llamada del teléfono del asistente al de un jefe y la contesta automáticamente.
EstabActiv.	Todos los estados	Permite ver el estado de una llamada administrada por un asistente.
TrnsfBu	Llamando, Conectada, En espera	Redirige la llamada seleccionada al buzón de voz del jefe.
Desviar todas	Todos los estados	Desvía todas las llamadas que se enrutan al jefe a un destino preconfigurado.



Nota Interceptar, EstabActiv. y Desviar todas solo se pueden configurar para el teléfono de un jefe en el modo de línea proxy.

El procedimiento siguiente es una descripción general de los pasos necesarios.

Procedimiento

- Paso 1** Configure los teléfonos y usuarios.
- Paso 2** Asocie los teléfonos a los usuarios.
- Paso 3** Active el servicio Cisco IP Manager Assistant en la ventana Activación del servicio.

- Paso 4** Configure los parámetros de administración del sistema.
- Paso 5** Si fuera necesario, configure los parámetros de servicios para todo el clúster de IPMA.
- Paso 6** (Opcional) Configure el perfil CAPF del usuario.
- Paso 7** (Opcional) Configure los parámetros de servicio de IPMA relativos a la seguridad.
- Paso 8** Detenga y reinicie el servicio IPMA.
- Paso 9** Configure los parámetros del teléfono y la configuración del jefe y del asistente, incluidas las plantillas de teclas programables.
- Paso 10** Configure la aplicación Assistant de Cisco Unified Communications Manager.
- Paso 11** Configure las reglas de marcación.
- Paso 12** Instale la aplicación Assistant Console.
- Paso 13** Configure las aplicaciones de consola del jefe y del asistente.

Configuración de Visual Voicemail

Visual Voicemail se configura para todos los teléfonos IP de Cisco o para usuarios o grupos de usuarios individuales desde Administración de Cisco Unified Communications Manager.



Nota Para obtener datos sobre la configuración, consulte la documentación de Cisco Visual Voicemail en <http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html>.

El cliente de buzón de voz visual no es compatible como un midlet en cualquiera de los teléfonos IP 8800 de Cisco.

Procedimiento

- Paso 1** En Cisco Unified Communications Manager Administration, seleccione **Dispositivo > Configuración del dispositivo > Servicios de telefonía**.
- Paso 2** Seleccione **Nuevo** para crear un servicio nuevo para Visual Voicemail.
- Paso 3** En la ventana de configuración del servicio del teléfono IP, introduzca los datos siguientes en los campos respectivos:

- Nombre del servicio: escriba **VisualVoiceMail**.
- Nombre del servicio ASCII: escriba **VisualVoiceMail**.
- URL de servicio: escriba **Application: Cisco/VisualVoiceMail**.
- Categoría del servicio: seleccione **Servicio XML** en el menú desplegable.
- Tipo de servicio: seleccione **Mensajes** en el menú desplegable.

- Paso 4** Marque **Activar** y haga clic en **Guardar**.

Nota Asegúrese de que no se ha marcado **Suscripción empresarial**.

- Paso 5** En la ventana de información Parámetro de servicio, haga clic en **Nuevo parámetro** e introduzca los datos siguientes en los campos respectivos:

- Nombre del parámetro: escriba voicemail_server.
- Nombre para mostrar del parámetro: escriba voicemail_server.
- Valor predeterminado: introduzca el nombre del host del servidor Unity principal.
- Descripción del parámetro.

Paso 6 Marque **El parámetro es obligatorio** y haga clic en **Guardar**.

Nota Asegúrese de que no se ha marcado **El parámetro es una contraseña (contenido de máscara)**.

Paso 7 Cierre la ventana y seleccione de nuevo **Guardar** en la ventana de configuración del servicio del teléfono.

Configuración de Visual Voicemail para un usuario específico

Use el procedimiento siguiente para configurar Visual Voicemail para un usuario específico.



Nota Para obtener datos sobre la configuración, consulte la documentación de Cisco Visual Voicemail en <http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html>.

Procedimiento

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

Paso 2 Seleccione el dispositivo asociado al usuario que busca.

Paso 3 En la lista desplegable Enlaces relacionados, seleccione **Suscribirse o anular suscripción de servicios** y haga clic en **Ir**.

Paso 4 Seleccione el servicio de Visual Voicemail que ha creado y seleccione **Siguiente > Suscribirse**.

Configuración de Visual Voicemail para un grupo de usuarios

Para agregar un lote de teléfonos IP de Cisco a Cisco Unified Communications Manager con Visual Voicemail suscrito, cree una plantilla de teléfono en la herramienta BAT para cada tipo de teléfono y en cada plantilla de teléfono. A continuación, puede suscribirse al servicio Visual Voicemail y usar la plantilla para insertar los teléfonos.

Si ya ha registrado teléfonos IP de Cisco y desea suscribirlos al servicio Visual Voicemail, cree una plantilla de teléfono en BAT, suscríbese al servicio Visual Voicemail en la plantilla y use la herramienta BAT para actualizar los teléfonos.

Para obtener más información, consulte <http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html>.

Servicios garantizados SIP

Servicios SIP(AS-SIP) garantizados es un conjunto de funciones y protocolos que ofrecen un flujo de llamada de alta seguridad para teléfonos IP de Cisco y de otros fabricantes. Las siguientes funciones se conocen colectivamente como AS-SIP:

- Servicio de precedencia multinivel y de preferencia (MLPP)
- Punto de código de servicios diferenciados (DSCP)
- Seguridad de la capa de transporte (TLS) y Protocolo de transporte seguro en tiempo real (SRTP)
- Protocolo de Internet versión 6 (IPv6)

AS-SIP se suele usar con precedencia multinivel y de preferencia (MLPP) para establecer la prioridad de llamadas durante una emergencia. Con MLPP, asigne un nivel de prioridad a las llamadas salientes, entre 1 (baja) y 5 (alta). Cuando reciba una llamada, aparecerá un icono de nivel de prioridad en el teléfono que muestra la prioridad de la llamada.

Para configurar AS-SIP, realice las siguientes tareas en Cisco Unified Communications Manager:

- Configure un usuario implícito: configuración del usuario final para usar la autenticación implícita para las solicitudes SIP.
- Configure el puerto de SIP teléfono seguro: Cisco Unified Communications Manager utiliza este puerto para escuchar teléfonos SIP para registros de línea SIP sobre TLS.
- Reinicio de servicios: después de configurar el puerto seguro, reinicie Cisco Unified Communications Manager y los servicios de proveedor de Cisco CTL. Configure perfil de SIP para AS-SIP configure un perfil de SIP con la configuración de SIP para los terminales AS-SIP y para los troncales SIP. Los parámetros específicos del teléfono no se descargan en un teléfono AS-SIP de terceros. Solo los utiliza Cisco Unified Manager. Los teléfonos de terceros deben establecer localmente la misma configuración.
- Configurar el perfil de seguridad para AS-SIP: puede utilizar el perfil de seguridad para asignar la configuración de seguridad, como la autenticación implícita, TLS y SRTP.
- Configurar el Terminal de AS-SIP: configure un teléfono IP de Cisco o un terminal de terceros con asistencia AS-SIP.
- Asociar el dispositivo con el uso final: asocie un usuario al punto final.
- Configurar el perfil de seguridad de troncal SIP de AS-SIP: puede utilizar el perfil de seguridad de troncal sip para asignar funciones de seguridad, como la autenticación TLS o implícita a un troncal SIP.
- Configurar el troncal SIP de AS-SIP: configure un troncal SIP con asistencia AS-SIP.
- Configurar las funciones de AS-SIP: configure las funciones de AS-SIP adicionales, como MLPP, TLS, V.150 y IPv6.

Para obtener información detallada sobre la configuración de AS-SIP, consulte el capítulo "Configurar terminales AS-SIP", *Guía de configuración del sistema para Cisco Unified Communications Manager*.

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

Precedencia multinivel y preferencia

Servicio de precedencia multinivel y de preferencia (MLPP) le permite dar prioridad a llamadas durante emergencias o en otras situaciones de crisis. Usted asigna una prioridad a sus llamadas salientes que va de 1 a 5. Las llamadas entrantes muestran un icono que indica la prioridad de la llamada. Los usuarios autenticados pueden evitar llamadas a estaciones específicas o a través de troncales TDM totalmente suscritas.

Esta capacidad garantiza al personal de alto rango la comunicación con organizaciones y personal críticos.

El MLPP se utiliza a menudo con Assured Services SIP (AS-SIP). Para obtener información detallada sobre la configuración de MLPP, consulte el capítulo "Configurar varios niveles de precedencia y prioridad", *Guía de configuración del sistema para Cisco Unified Communications Manager*.

Configuración de la plantilla de teclas programadas

Mediante Cisco Unified Communications Manager Administration, puede asociar un máximo de 18 teclas programables con aplicaciones compatibles con el teléfono. Cisco Unified Communications Manager admite las plantillas de teclas programables de usuario estándar y de características estándar.

Una aplicación que admita teclas programables tiene una o varias plantillas de teclas programables asociadas. Para modificar una plantilla de teclas programables estándar, debe copiarla, cambiarle el nombre y actualizar la nueva plantilla. También puede modificar una plantilla de teclas programables no estándar.

El parámetro Control de teclas programables muestra si las teclas programables de un teléfono se controlan mediante la función Plantilla de tecla programable. El parámetro Control de teclas programables es obligatorio.

Para obtener más información sobre cómo configurar esta función, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Los teléfonos IP de Cisco no admiten todas las teclas programadas que se pueden configurar en la página de configuración de la plantilla de teclas programadas de Administración de Cisco Unified Communications Manager. Cisco Unified Communications Manager permite habilitar o deshabilitar algunas teclas programables en los ajustes de configuración de la política de control. En la tabla siguiente se muestran las funciones y las teclas programadas que se pueden configurar en la plantilla, y se indica si se admite en el teléfono IP de Cisco.



Nota Cisco Unified Communications Manager permite configurar cualquier tecla programable de una plantilla de teclas programadas, pero las que no se admiten no se muestran en el teléfono.

Tabla 38: Teclas programables configurables

Función	Teclas programables configurables en la plantilla de teclas programables	Admitida como tecla programada
Contestar	Contestar (Contest.)	Compatible
Retro llamada	RetroLla (RetroLla)	Compatible
Desvío incondicional	Desv. todas (DsvInc)	Compatible
Aparcar llamada	Ap. llam. (Aparcar)	Compatible
Captura de llamadas	Capturar (Capturar)	Compatible

Función	Teclas programables configurables en la plantilla de teclas programables	Admitida como tecla programada
Intrusión	Intrusión	Compatible
IntruCf	Intrusión de conferencia	Compatible
Conferencia	Conferencia (Conf.)	Compatible
Lista de conferencias	Lista de conferencia (ListCnf)	Compatible
Desviar	Desvío inmediato (Desviar)	Compatible
No molestar	Alternar No molestar (DND)	Compatible
Fin llamada	FinLlam. (FinLlam)	Compatible
Captura de llamadas de grupo	Captura de grupo (CaptGr)	Compatible
Espera	Espera (Espera)	Compatible
Grupo de salto	ConGrupo (ConGrupo)	Compatible
Conexión	Conectar (Conectar)	No compatible
Identificar llamadas maliciosas	Alternar identificación de llamadas maliciosas (IdLIMali)	Compatible
Meet Me	Meet Me (MeetMe)	Compatible
Mobile Connect	Movilidad (Movilid.)	Compatible
Nueva llamada	Nueva llamada (NvaLlam)	Compatible
Captura de otros	Captura de otros (CaptOtr)	Compatible
Compatibilidad PLK para las estadísticas de la cola	Estado de cola	No compatible
Herramienta de generación de informes de calidad	Herramienta de generación de informes de calidad (QRT)	Compatible
Rellamar	Rellamada (Rellam.)	Compatible
Eliminar al último participante de la conferencia	Eliminar al último participante de la conferencia (Quitar)	No compatible
Continuar	Continuar (Cont.)	Compatible
Seleccionar	Seleccionar (Selec.)	No compatible
Marcación rápida	Marcación abreviada (MarcAbr)	Compatible
Transferir	Transferir (Trnsf.)	Compatible

Función	Teclas programables configurables en la plantilla de teclas programables	Admitida como tecla programable
Comando de modo de vídeo	Comando de modo de vídeo (ModoVid)	No compatible

Procedimiento

- Paso 1** En Cisco Unified Communications Manager Administration, seleccione una de las ventanas siguientes:
- Para configurar plantillas de teclas programables, seleccione **Dispositivo > Configuración del dispositivo > Plantilla de teclas programables**.
 - Para asignar una plantilla de teclas programables a un teléfono, seleccione **Dispositivo > Teléfono** y configure el campo Plantilla de teclas programables.
- Paso 2** Guarde los cambios.

Temas relacionados

[Cisco Unified Communications Manager Documentación](#), en la página xv

Plantillas de botones de teléfono

Las plantillas de botones de teléfono permiten asignar funciones de marcación rápida y administración de llamadas a los botones programables. Las funciones de administración de llamadas que se pueden asignar a los botones son Contestar, Movilidad y Todas.

Lo ideal es modificar las plantillas antes de registrar los teléfonos en la red. De esta forma, podrá acceder a las opciones de la plantilla de botones de teléfono personalizada desde Cisco Unified Communications Manager durante el registro.

Modificación de plantillas de botones de teléfono

Para obtener más información sobre los servicios del teléfono IP y la configuración de los botones de línea, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Procedimiento

- Paso 1** En Cisco Unified Communications Manager Administration, seleccione **Dispositivo > Configuración del dispositivo > Plantilla de botones de teléfono**.
- Paso 2** Haga clic en **Encontrar**.
- Paso 3** Seleccione el modelo de teléfono.
- Paso 4** Seleccione **Copiar**, introduzca un nombre de la nueva plantilla y seleccione **Guardar**.
Se abre la ventana de configuración de la plantilla de botones del teléfono.
- Paso 5** Identifique el botón que desea asignar y seleccione **URL de servicio** en la lista desplegable Funciones asociada con la línea.

- Paso 6** Seleccione **Guardar** para crear una plantilla de botones de teléfono que use la URL de servicio.
- Paso 7** Seleccione **Dispositivo > Teléfono** y abra la ventana de configuración del teléfono.
- Paso 8** Seleccione la nueva plantilla de botones de teléfono en la lista desplegable correspondiente.
- Paso 9** Seleccione **Guardar** para guardar el cambio y en **Aplicar configuración** para implementarlo.
- El usuario del teléfono puede acceder ahora al portal de autoayuda y asociar el servicio a un botón del teléfono.

Temas relacionados

[Cisco Unified Communications Manager Documentación](#), en la página xv

Asignación de la plantilla de botones del teléfono para todas las llamadas

Es posible asignar un botón Todas las llamadas de la plantilla de teléfono para los usuarios con varias líneas compartidas.

Si configura un botón Todas las llamadas en el teléfono, los usuarios podrán usarlo para lo siguiente:

- Ver una lista consolidada de las llamadas actuales de todas las líneas del teléfono.
- Ver (en el historial de llamadas) una lista de todas las llamadas perdidas de todas las líneas del teléfono.
- Efectuar una llamada en la línea principal del usuario cuando este descuelgue. El botón Todas las llamadas toma de forma predeterminada la línea principal del usuario para las llamadas salientes.

Procedimiento

- Paso 1** Modifique la plantilla de botones del teléfono para incluir el botón Todas las llamadas.
- Paso 2** Asigne la plantilla al teléfono.
-

Configuración de la libreta personal de direcciones o la marcación rápida como servicio del teléfono IP

Es posible modificar una plantilla de botones del teléfono para asociar una URL de servicio a un botón programable. De esta forma, los usuarios dispondrán de un acceso con un solo botón a la libreta personal de direcciones y a las marcaciones rápidas. Antes de modificar la plantilla de botones del teléfono, debe configurar la libreta personal de direcciones o las marcaciones rápidas como un servicio del teléfono IP. Para obtener más datos, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Para configurar la libreta personal de direcciones o las marcaciones rápidas como servicio del teléfono IP (si aún no lo son), siga estos pasos:

Procedimiento

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

Se abre la ventana de búsqueda y lista de servicios del teléfono IP.

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

Se abre la ventana de configuración de servicios del teléfono IP.

Paso 3 Introduzca los ajustes siguientes:

- Nombre del servicio: introduzca **Libreta personal de direcciones**.
- Descripción del servicio: introduzca una descripción opcional del servicio.
- URL de servicio

Para la libreta personal de direcciones, introduzca la URL siguiente:

http://<Unified CM-server-name>:8080/ccmpd/login.do?name=#DEVICENAME#&service=pab

Para la marcación rápida, introduzca la URL siguiente:

http://<Unified-CM-server-name>:8080/ccmpd/login.do?name=#DEVICENAME#&service=fd

- URL de servicio seguro

Para la libreta personal de direcciones, introduzca la URL siguiente:

https://<Unified CM-server-name>:8443/ccmpd/login.do?name=#DEVICENAME#&service=pab

Para la marcación rápida, introduzca la URL siguiente:

https://<Unified-CM-server-name>:8443/ccmpd/login.do?name=#DEVICENAME#&service=fd

- Categoría del servicio: seleccione **Servicio XML**.
- Tipo de servicio: seleccione **Directorios**.
- Activar: marque la casilla de verificación.

http://<IP_address> o *https://<IP_address>* (depende del protocolo que admita el teléfono IP de Cisco).

Paso 4 Seleccione **Guardar**.

Nota Si cambia la URL del servicio, elimine el parámetro de servicio del teléfono IP, o si cambia el nombre del parámetro de servicio de un teléfono de un servicio al que los usuarios estén suscritos, debe hacer clic en **Actualizar suscripciones** para actualizar todos los usuarios suscritos actualmente con los cambios. Si no lo hace, los usuarios deberán volver a suscribirse para reconstruir la URL correcta.

Temas relacionados

[Cisco Unified Communications Manager Documentación](#), en la página xv

Modificación de la plantilla de botones del teléfono para la libreta personal de direcciones o la marcación rápida

Es posible modificar una plantilla de botones del teléfono para asociar una URL de servicio a un botón programable. De esta forma, los usuarios dispondrán de un acceso con un solo botón a la libreta personal de

direcciones y a las marcaciones rápidas. Antes de modificar la plantilla de botones del teléfono, debe configurar la libreta personal de direcciones o las marcaciones rápidas como un servicio del teléfono IP.

Para obtener más información sobre los servicios del teléfono IP y la configuración de los botones de línea, consulte la documentación de su versión concreta de Cisco Unified Communications Manager.

Procedimiento

-
- Paso 1** En Cisco Unified Communications Manager Administration, seleccione **Dispositivo > Configuración del dispositivo > Plantilla de botones de teléfono**.
- Paso 2** Haga clic en **Encontrar**.
- Paso 3** Seleccione el modelo de teléfono.
- Paso 4** Seleccione **Copiar**, introduzca un nombre de la nueva plantilla y seleccione **Guardar**.
Se abre la ventana de configuración de la plantilla de botones del teléfono.
- Paso 5** Identifique el botón que desea asignar y seleccione **URL de servicio** en la lista desplegable Funciones asociada con la línea.
- Paso 6** Seleccione **Guardar** para crear una plantilla de botones de teléfono que use la URL de servicio.
- Paso 7** Seleccione **Dispositivo > Teléfono** y abra la ventana de configuración del teléfono.
- Paso 8** Seleccione la nueva plantilla de botones de teléfono en la lista desplegable correspondiente.
- Paso 9** Seleccione **Guardar** para guardar el cambio y en **Aplicar configuración** para implementarlo.
El usuario del teléfono puede acceder ahora al portal de autoayuda y asociar el servicio a un botón del teléfono.
-

Temas relacionados

[Cisco Unified Communications Manager Documentación](#), en la página xv

Configuración de VPN

La función de VPN de Cisco ayuda a mantener la seguridad de la red y aporta a los usuarios un método seguro y fiable para conectarse a la red corporativa. Use esta función en estas circunstancias:

- Un teléfono está ubicado fuera de una red de confianza.
- El tráfico de red entre el teléfono y Cisco Unified Communications Manager cruza una red que no es de confianza.

Con una VPN, hay tres enfoques habituales para la autenticación del cliente:

- Certificados digitales
- Contraseñas
- Nombre de usuario y contraseña

Cada método tiene sus ventajas. Pero si la política de seguridad de su empresa lo permite, se recomienda utilizar un enfoque basado en certificado, ya que estos permiten realizar el inicio de sesión sin problemas y sin intervención alguna del usuario. Se admiten tanto certificados LSC como MIC.

Para configurar cualquier función de VPN, aprovisiona primero el dispositivo de forma local y, a continuación, impleméntelo de forma externa.

Para obtener más datos sobre la autenticación de la certificación y sobre el trabajo con redes VPN, consulte la nota técnica *AnyConnect VPN Phone with Certificate Authentication on an ASA Configuration Example* (Ejemplo de configuración de teléfono VPN AnyConnect con autenticación de certificado en un ASA). La dirección URL de este documento es

<http://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/115785-anyconnect-vpn-00.html>

Con el enfoque de contraseña o de nombre de usuario y contraseña, se pide al usuario sus credenciales de inicio de sesión. Establezca las credenciales de inicio de sesión del usuario de acuerdo con la política de seguridad de su empresa. También puede configurar el ajuste para activar la persistencia de contraseña que permite guardar la contraseña del usuario en el teléfono. La contraseña del usuario se guarda hasta que se produce un intento de inicio de sesión erróneo, un usuario la borra manualmente o el teléfono se restablece o pierde la alimentación.

Otra herramienta útil es el ajuste de detección automática de la red. Si marca la casilla de verificación correspondiente, el cliente de VPN solo se puede ejecutar cuando detecta que se encuentra fuera de la red corporativa. Este ajuste está desactivado de manera predeterminada.

El teléfono de Cisco es compatible con la versión de cliente de Cisco SVC IPPhone 1.0 como tipo de cliente.

Para obtener más información sobre el mantenimiento, la configuración y el funcionamiento de una red privada virtual con VPN, consulte el capítulo "Configuración de la red privada virtual" en la *Guía de seguridad de Cisco Unified Communications Manager*. La dirección URL de este documento es

<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>

La función VPN de Cisco usa la capa de zócalos seguros (SSL) para mantener la seguridad de la red.



Nota Introduzca el valor del servidor TFTP alternativo cuando vaya a configurar un teléfono externo para la VPN SSL en ASA mediante el cliente integrado.

Configuración de teclas de línea adicionales

Permite usar los botones situados a ambos lados de la pantalla del teléfono como teclas de línea en el modo de línea mejorado. Las alertas de llamada entrante con acciones y la marcación predictiva están activadas de forma predeterminada en el modo de línea mejorado.

Antes de empezar

Debe crear una nueva plantilla de botones de teléfono personalizada.

Procedimiento

-
- Paso 1** En Cisco Unified Communications Manager Administration, seleccione **Dispositivo > Teléfono**.
 - Paso 2** Busque el teléfono que desea configurar.
 - Paso 3** Diríjase al apartado de configuración específica del producto y en el campo **Modo de línea** establezca **Modo de línea mejorada**.

- Paso 4** Diríjase al área de información del dispositivo y establezca el campo **Plantilla de botones de teléfono** en una plantilla personalizada.
- Paso 5** Seleccione **Aplicar configuración**.
- Paso 6** Seleccione **Guardar**.
- Paso 7** Reinicie el teléfono.

Temas relacionados

[Entorno del modo de línea de sesión](#), en la página 169

Funciones disponibles en el modo de línea mejorado

El modo de línea mejorado (ELM) se puede usar con Mobile and Remote Access mediante Expressway.

También puede utilizarse ELM con una línea de sustitución incremental, una configuración de enrutamiento de llamada en el que las llamadas se desvían a otra línea compartida si la línea compartida inicial está ocupada. Cuando se usa ELM con una línea de sustitución incremental, las llamadas recientes a las líneas compartidas se consolidan en un único número de directorio. Para obtener más información sobre líneas de sustitución incremental, consulte la *Guía de configuración de funciones de Cisco Unified Communications Manager* para Cisco Unified Communications Manager versión 12.0(1) o posterior.

ELM es compatible con la mayoría de las funciones, pero no todas. La activación de la función no implica soporte. Lea la tabla siguiente para confirmar que se admite una función.

Tabla 39: Compatibilidad de funciones y modo de línea mejorado

Función	Compatible	Versión de firmware
Contestar	Sí	11.5 (1) y posterior
Contestación automática de llamadas	Sí	11.5 (1) y posterior
Intrusión/IntruCf	Sí	11.5 (1) y posterior
Aparcamiento de llamadas dirigido con BLF	Sí	12.0 (1) y posterior
Integración de teléfono inteligente Bluetooth	No	-
Auriculares USB Bluetooth	Sí	11.5 (1) y posterior
Retrollamada	Sí	11.5 (1) y posterior
Supervisión de llamadas	No	-
Desvío incondicional	Sí	11.5 (1) y posterior
Aparcar llamada	Sí	12.0 (1) y posterior
Estado de línea de aparcamiento de llamada	Sí	12.0 (1) y posterior

Función	Compatible	Versión de firmware
Captura de llamadas	Sí	11.5 (1) y posterior
Estado de línea de captura de llamada	Sí	11.5 (1) y posterior
Desvío de todas las llamadas en varias líneas	Sí	11.5 (1) y posterior
Extensión móvil entre clústeres de Cisco	Sí	12.0(1) y posterior admite esta función.
Cisco IP Manager Assistant (IPMA)	No	-
Cisco Unified Communications Manager Express	No	-
Conferencia	Sí	11.5 (1) y posterior
Aplicaciones de integración de telefonía y ordenador (CTI)	Sí	11.5 (1) y posterior
Rechazar	Sí	11.5 (1) y posterior
Grabación invocada por el dispositivo	Sí	11.5 (1)SR1 y posterior
No molestar	Sí	11.5 (1) y posterior
SRST mejorado	No	-
Extension Mobility	Sí	11.5 (1) y posterior
Captura de llamadas de grupo	Sí	12.0(1) y posterior admite esta función.
Espera	Sí	11.5 (1) y posterior
Grupos de salto	Sí.	12.0 (1) y posterior
Alerta de llamada entrante con el temporizador configurable	No	-
Intercomunicación	Sí	11.5 (1) y posterior
Módulo de expansión clave	El módulo de expansión clave de teléfono IP 8851/8861 de Cisco y el módulo de expansión clave de teléfono IP 8865 de Cisco admiten el modo de línea mejorado	12.0 (1) y posterior
Identificación de llamadas maliciosas (IdLIMali)	Sí	11.5 (1) y posterior

Función	Compatible	Versión de firmware
Meet Me	Sí	11.5 (1) y posterior
Mobile Connect	Sí	11.5 (1) y posterior
Precedencia multinivel y preferencia	No	-
Silencio	Sí	11.5 (1) y posterior
Captura de otros	Sí	12.0 (1) y posterior
Compatibilidad con tecla de línea programable (PLK) para el estado de cola	Sí	11.5 (1) y posterior
Privacidad	Sí	11.5 (1) y posterior
Estado de cola	Sí	11.5 (1) y posterior
Herramienta de generación de informes de calidad (QRT)	Sí	11.5 (1) y posterior
Soporte regional de derecha a izquierda	No	-
Rellamar	Sí	11.5 (1) y posterior
Supervisión y grabación silenciosas	Sí	11.5 (1)SR1 y posterior
Marcación rápida	Sí	11.5 (1) y posterior
Telefonía en sitio remoto a prueba de fallos (SRST)	Sí	11.5 (1) y posterior
Transferir	Sí	11.5 (1) y posterior
Marcación con identificador uniforme de recursos (URI)	Sí	11.5 (1) y posterior
Videollamadas	Sí	11.5 (1) y posterior
Visual Voicemail	Sí	11.5 (1) y posterior
Correo de voz	Sí	11.5 (1) y posterior

Temas relacionados

[Entorno del modo de línea de sesión](#), en la página 169

Configuración del temporizador de reanudación de TLS

La reanudación de la sesión TLS permite reanudar una sesión TLS sin tener que repetir todo el proceso de autenticación. Puede reducir de forma significativa el tiempo empleado por la conexión TLS para intercambiar datos.

Aunque los teléfonos admiten sesiones TLS, no todas las sesiones TLS admiten la reanudación de TLS. En la lista siguiente se describen las distintas sesiones y la compatibilidad con la reanudación de TLS:

- Sesión TLS para señales SIP: admite la reanudación.
- Cliente HTTPs: admite la reanudación.
- CAPF: admite la reanudación.
- TVS: admite la reanudación.
- EAP-TLS: no admite la reanudación.
- EAP-FAST: no admite la reanudación.
- Cliente VPN: no admite la reanudación.

Para obtener más datos, consulte 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 Establezca el parámetro del temporizador de reanudación de TLS.

El rango para el temporizador es de 0 a 3600 segundos. El valor por defecto es 3600. Si el campo está a 0, la reanudación de sesión TLS está desactivada.

Temas relacionados

[Cisco Unified Communications Manager Documentación](#), en la página xv

Activación de Intelligent Proximity



Nota Este procedimiento solo se aplica a los teléfonos compatibles con Bluetooth. Los teléfonos IP 8811, 8841, 8851NR y 8865NR de Cisco no admiten Bluetooth.

Intelligent Proximity permite a los usuarios aprovechar las propiedades acústicas del teléfono con su dispositivo móvil o tableta. El usuario vincula el dispositivo móvil o la tableta al teléfono mediante Bluetooth.

Con un dispositivo móvil vinculado, el usuario puede efectuar y recibir llamadas del móvil en el teléfono. Con una tableta, el usuario puede dirigir el audio de la tableta al teléfono.

Los usuarios pueden vincular varios dispositivos móviles, tabletas y unos auriculares Bluetooth al teléfono. Sin embargo, solo es posible conectar un dispositivo y unos auriculares al mismo tiempo.

Procedimiento

-
- Paso 1** En Cisco Unified Communications Manager Administration, seleccione **Teléfono > Dispositivo**.
 - Paso 2** Localice el teléfono que desea modificar.
 - Paso 3** Localice el campo Bluetooth y establezca el valor **Activado**.
 - Paso 4** Localice el campo para permitir el modo de manos libres en el móvil Bluetooth y establezca el valor **Activado**.
 - Paso 5** Guarde los cambios y aplíquelos al teléfono.
-

Configuración de la resolución de transmisión del vídeo

Los teléfonos IP 8845, 8865 y 8865NR de Cisco admiten los siguientes formatos de vídeo:

- 720p (1280 x 720)
- WVGA (800 x 480)
- 360p (640 x 360)
- 240p (432 x 240)
- VGA (640 x 480)
- CIF (352 x 288)
- SIF (352 x 240)
- QCIF (176 x 144)

Los teléfonos IP de Cisco con capacidad de vídeo negocian la mejor resolución para la banda ancha según los límites de configuración o resolución del teléfono. Ejemplo: en una llamada directa de 88 x 5 a 88 x 5, los teléfonos no envían realmente resolución 720p, sino 800 x 480. Este límite se debe meramente a que la resolución de pantalla WVGA de 5 pulgadas de 88 x 5 es de 800 x 480.

Tipo de vídeo	Resolución de vídeo	Fotogramas por segundo (mps)	Intervalo de velocidad de bits de vídeo
720p	1280 x 720	30	De 1360 a 2500 kb/s
720p	1280 x 720	15	De 790 a 1359 kb/s
WVGA	800 x 480	30	De 660 a 789 kb/s
WVGA	800 x 480	15	De 350 a 399 kb/s
360p	640 x 360	30	De 400 a 659 kb/s
360p	640 x 360	15	De 210 a 349 kb/s

Tipo de vídeo	Resolución de vídeo	Fotogramas por segundo (mps)	Intervalo de velocidad de bits de vídeo
240p	432 x 240	30	De 180 a 209 kb/s
240p	432 x 240	15	De 64 a 179 kb/s
VGA	640 x 480	30	De 520 a 1500 kb/s
VGA	640 x 480	15	De 280 a 519 kb/s
CIF	352 x 288	30	De 200 a 279 kb/s
CIF	352 x 288	15	De 120 a 199 kb/s
SIF	352 x 240	30	De 200 a 279 kb/s
SIF	352 x 240	15	De 120 a 199 kb/s
QCIF	176 x 144	30	De 94 a 119 kb/s
QCIF	176 x 144	15	De 64 a 93 kb/s

Administración de los auriculares en versiones anteriores de Cisco Unified Communications Manager

Si tiene una versión de Cisco Unified Communications Manager anterior a 12.5(1)SU1, puede configurar de forma remota la configuración de los auriculares Cisco para su uso con teléfonos locales.

La configuración remota de los auriculares en las versiones 10.5(2), 11.0(1), 11.5(1), 12.0(1) y 12.5(1) de Cisco Unified Communication Manager requiere que se descargue un archivo del sitio web [Descargas de software de Cisco](#), se edite el archivo y, a continuación, se cargue el archivo al servidor TFTP de Cisco Unified Communications Manager. El archivo es un archivo de notificación de objetos JavaScript (JSON). La configuración actualizada de los auriculares se aplica a los auriculares de la empresa en un período de 10 a 30 minutos para evitar un retraso de tráfico en el servidor TFTP.



Nota Los auriculares se pueden administrar y configurar mediante Cisco Unified Communications Manager Administration, versión 11.5(1)SU7.

Observe lo siguiente mientras trabaja con el archivo JSON:

- Los ajustes no se aplican si falta un paréntesis o paréntesis en el código. Utilice una herramienta en línea como JSON Formatter y compruebe el formato.
- Establezca la configuración **updatedTime** a la hora actual de la época o no se aplicará la configuración. Como alternativa, puede aumentar el valor de **updatedTime** por +1 para que sea mayor que la versión anterior.
- No cambie el nombre del parámetro o no se aplicará la configuración.

Para más información sobre el servicio TFTP, consulte el capítulo "Administrar firmware del dispositivo" de la *Guía de administración de Cisco Unified Communications Manager, IM y el Servicio de presencia*.

Actualice los teléfonos a la última versión de firmware antes de aplicar el archivo `defaultheadsetconfig.json`. En la tabla siguiente se describen los ajustes predeterminados que puede ajustar con el archivo JSON.

Descarga del archivo de configuración predeterminada de los auriculares

Antes de configurar los parámetros de los auriculares de forma remota, debe descargar el archivo de ejemplo de anotación de objeto JavaScript (JSON) más reciente.

Procedimiento

-
- Paso 1** Diríjase a la siguiente dirección URL: <https://software.cisco.com/download/home/286320550>.
 - Paso 2** Seleccione **Auriculares serie 500**.
 - Paso 3** Seleccione la serie de sus auriculares.
 - Paso 4** Seleccione la carpeta de una versión y seleccione el archivo zip.
 - Paso 5** Haga clic en el botón **Descargar** o **Agregar al carrito** y siga las indicaciones.
 - Paso 6** Descomprima el archivo en un directorio del PC.
-

Qué hacer a continuación

[Modificación del archivo de configuración predeterminada de los auriculares, en la página 212](#)

Modificación del archivo de configuración predeterminada de los auriculares

Tenga en cuenta lo siguiente al trabajar con el archivo de anotación de objeto JavaScript (JSON):

- Los ajustes no se aplican si falta un paréntesis o paréntesis en el código. Utilice una herramienta en línea como JSON Formatter y compruebe el formato.
- Establezca la configuración "**updatedTime**" a la hora actual de la época o no se aplica la configuración.
- Confirme que **firmwareName** es el **MÁS RECIENTE** o no se aplicará la configuración.
- No cambie el nombre de ningún parámetro o no se aplicará la configuración.

Procedimiento

-
- Paso 1** Abra el archivo `defaultheadsetconfig.json` con un editor de texto.
 - Paso 2** Edite **updatedTime** y los valores de los parámetros de los auriculares que desea modificar.

A continuación, se muestra un script de ejemplo. El script se proporciona solo como referencia. Utilícelo como guía para configurar los parámetros de los auriculares. Use el archivo JSON incluido con la carga del firmware.

```

{
  "headsetConfig": {
    "templateConfiguration": {
      "configTemplateVersion": "1",
      "updatedTime": 1537299896,
      "reportId": 3,
      "modelSpecificSettings": [
        {
          "modelSeries": "530",
          "models": [
            "520",
            "521",
            "522",
            "530",
            "531",
            "532"
          ],
          "modelFirmware": [
            {
              "firmwareName": "LATEST",
              "latest": true,
              "firmwareParams": [
                {
                  "name": "Speaker Volume",
                  "access": "Both",
                  "usageId": 32,
                  "value": 7
                },
                {
                  "name": "Microphone Gain",
                  "access": "Both",
                  "usageId": 33,
                  "value": 2
                },
                {
                  "name": "Sidetone",
                  "access": "Both",
                  "usageId": 34,
                  "value": 1
                },
                {
                  "name": "Equalizer",
                  "access": "Both",
                  "usageId": 35,
                  "value": 3
                }
              ]
            }
          ]
        }
      ]
    },
    {
      "modelSeries": "560",
      "models": [
        "560",
        "561",
        "562"
      ],
      "modelFirmware": [
        {
          "firmwareName": "LATEST",
          "latest": true,
          "firmwareParams": [
            {
              "name": "Speaker Volume",

```


Instalación del archivo de configuración predeterminada en Cisco Unified Communications Manager

Después de editar el archivo `defaultheadsetconfig.json`, instálelo en Cisco Unified Communications Manager mediante la herramienta de administración de archivos TFTP.

Procedimiento

- Paso 1** En Cisco Unified OS Administration, seleccione **Actualizaciones de software** > **Administración de archivos TFTP**.
 - Paso 2** Seleccione **Cargar archivo**.
 - Paso 3** Seleccione **Seleccionar archivo** y diríjase al archivo `defaultheadsetconfig.json`.
 - Paso 4** Seleccione **Cargar archivo**.
 - Paso 5** Haga clic en **Cerrar**.
-

Reinicio del servidor Cisco TFTP

Después de cargar el archivo `defaultheadsetconfig.json` en el directorio TFTP, reinicie el servidor TFTP de Cisco y restablezca los teléfonos. Transcurridos unos 10 o 15 minutos, el proceso de descarga se iniciará y se aplicarán las nuevas configuraciones a los auriculares. La configuración tarda de 10 a 30 minutos más en aplicarse.

Procedimiento

- Paso 1** Inicie sesión en Cisco Unified Serviceability y seleccione **Herramientas** > **Centro de control - Servicios de la característica**.
 - Paso 2** En el cuadro de lista desplegable **Servidor**, seleccione el servidor en el que se está ejecutando el servicio TFTP de Cisco.
 - Paso 3** Haga clic en el botón de opción que corresponda al servicio **TFTP de Cisco**.
 - Paso 4** Haga clic en **Reiniciar**.
-



CAPÍTULO 10

Directorio corporativo y personal

- [Configuración del directorio corporativo, en la página 217](#)
- [Configuración del directorio personal, en la página 217](#)
- [Configuración de las entradas del directorio personal del usuario, en la página 218](#)

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.

Los teléfonos IP de Cisco utilizan asignación dinámica para SecureApp tanto en el cliente como en los servidores. Esto garantiza que su teléfono pueda leer certificados de más de 4 KB y reduce la frecuencia de los mensajes de error `Host no encontrado` cuando un usuario accede a su directorio.

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 xv

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
- Herramienta de sincronización de la libreta de direcciones (TABSynch)

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.
- En una aplicación de Microsoft Windows: Los usuarios pueden utilizar la herramienta TABSynch para sincronizar sus PAB con la Libreta de direcciones de Microsoft Windows. Los clientes que deseen utilizar la libreta de direcciones de Microsoft Outlook, deberían comenzar por importar los datos de dicha libreta a la libreta de direcciones de Microsoft Windows. A continuación, puede utilizarse TabSync para sincronizar la Libreta de direcciones de Windows con el Directorio personal. Para obtener información acerca de TABSync, consulte [Descarga del sincronizador de la libreta de direcciones de Cisco IP Phone, en la página 219](#) y [Configuración del sincronizador, en la página 220](#).

Los teléfonos IP de Cisco utilizan asignación dinámica para SecureApp tanto en el cliente como en los servidores. Esto garantiza que su teléfono pueda leer certificados de más de 4 KB y reduce la frecuencia de los mensajes de error `Host no encontrado` cuando un usuario accede a su directorio.

Para asegurarse de que los usuarios del sincronizador de la libreta de direcciones de teléfono IP de Cisco solo acceden a sus datos de usuario final, active el servicio web de Cisco UXL en Cisco Unified Serviceability.

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.

Configuración de las entradas del directorio personal del usuario

Los usuarios pueden configurar las entradas del directorio personal en el teléfono IP de Cisco. Para configurar un directorio personal, los usuarios deben tener acceso a lo siguiente:

- Al portal de autoayuda: asegúrese de que los usuarios saben cómo acceder a su portal de autoayuda. Consulte el apartado [Configuración del acceso de usuario al portal de autoayuda, en la página 83](#) para obtener información más detallada.
- Al sincronizador de la libreta de direcciones del teléfono IP de Cisco: asegúrese de proporcionar a los usuarios el instalador. Consulte [Descarga del sincronizador de la libreta de direcciones de Cisco IP Phone, en la página 219](#).



Nota El sincronizador de la libreta de direcciones de teléfono IP de Cisco solo es compatible con versiones de Windows no compatibles (por ejemplo, Windows XP y anteriores). La herramienta no es compatible con las versiones más recientes de Windows. En el futuro, se eliminará de la lista de complementos de Cisco Unified Communications Manager.

Descarga del sincronizador de la libreta de direcciones de Cisco IP Phone

Para descargar una copia del sincronizador que se debe enviar a los usuarios, siga estos pasos:

Procedimiento

-
- Paso 1** Para obtener el instalador, seleccione **Aplicación > Complementos** en Cisco Unified Communications Manager Administration.
 - Paso 2** Seleccione la opción **Descargar**, situada junto al nombre del complemento Sincronizador de la libreta de direcciones del teléfono IP de Cisco.
 - Paso 3** Cuando se muestre el cuadro de diálogo de descarga, seleccione **Guardar**.
 - Paso 4** Envíe el archivo TabSyncInstall.exe y las instrucciones de [Implementación del sincronizador de la libreta de direcciones del teléfono IP de Cisco, en la página 219](#) a todos los usuarios que requieran esta aplicación.
-

Implementación del sincronizador de la libreta de direcciones del teléfono IP de Cisco

El sincronizador de libreta de direcciones del teléfono IP de Cisco sincroniza datos almacenados en la libreta de direcciones de Microsoft Windows con el directorio de Cisco Unified Communications Manager y la libreta de direcciones personales del portal de autoayuda.



-
- Consejo** Para sincronizar correctamente la libreta de direcciones de Windows con la libreta personal de direcciones, todos los usuarios de la libreta de Windows deben introducirse en dicha libreta antes de realizar los procedimientos siguientes.
-

Instalación del sincronizador

Para instalar el sincronizador de la libreta de direcciones del teléfono IP de Cisco, siga estos pasos:

Procedimiento

-
- Paso 1** Obtenga el archivo de instalación del sincronizador de la libreta de direcciones del teléfono IP de Cisco del administrador del sistema.
 - Paso 2** Haga doble clic en el archivo TabSyncInstall.exe que le ha proporcionado el administrador.
 - Paso 3** Seleccione **Ejecutar**.
 - Paso 4** Seleccione **Siguiente**.
 - Paso 5** Lea la información del acuerdo de licencia y seleccione **Acepto**. Seleccione **Siguiente**.
 - Paso 6** Seleccione el directorio donde desea instalar la aplicación y haga clic en **Siguiente**.
 - Paso 7** Seleccione **Instalar**.
 - Paso 8** Seleccione **Finalizar**.

Paso 9 Para completar el proceso, siga los pasos descritos en [Configuración del sincronizador, en la página 220](#).

Configuración del sincronizador

Para configurar el sincronizador de la libreta de direcciones del teléfono IP de Cisco, siga estos pasos:

Procedimiento

- Paso 1** Abra el sincronizador de la libreta de direcciones de teléfono IP de Cisco.
Si ha aceptado el directorio de instalación predeterminado, puede abrir la aplicación seleccionando **Inicio > Todos los programas > Cisco Systems > TabSync**.
- Paso 2** Para configurar la información del usuario, seleccione **Usuario**.
- Paso 3** Introduzca el nombre de usuario y la contraseña del teléfono IP de Cisco y seleccione **Aceptar**.
- Paso 4** Para configurar la información del servidor de Cisco Unified Communications Manager, seleccione **Servidor**.
- Paso 5** Introduzca la dirección IP o el nombre de host y el número de puerto del servidor de Cisco Unified Communications Manager y seleccione **Aceptar**.
Si no dispone de esta información, póngase en contacto con el administrador del sistema.
- Paso 6** Para iniciar el proceso de sincronización del directorio, seleccione **Sincronizar**.
La ventana Estado de sincronización proporciona el estado de la sincronización de la libreta de direcciones. Si selecciona la intervención del usuario para la regla de entradas duplicadas y tiene entradas duplicadas en la libreta de direcciones, se mostrará la ventana Duplicar selección.
- Paso 7** Seleccione la entrada que desea incluir en la libreta personal de direcciones y seleccione **Aceptar**.
- Paso 8** Cuando se complete la sincronización, seleccione **Salir** para cerrar el sincronizador de la libreta de direcciones de Cisco Unified CallManager.
- Paso 9** Para verificar si la sincronización ha funcionado, inicie sesión en el portal de autoayuda y seleccione **Libreta personal de direcciones**. Deben aparecer los usuarios de la libreta de direcciones de Windows.
-



PARTE **IV**

Solución de problemas del teléfono IP de Cisco

- [Sistemas de supervisión del teléfono, en la página 223](#)
- [Solución de problemas, en la página 259](#)
- [Mantenimiento, en la página 279](#)
- [Asistencia para usuarios internacionales, en la página 285](#)



CAPÍTULO 11

Sistemas de supervisión del teléfono

- [Estado del teléfono IP de Cisco, en la página 223](#)
- [Página web del teléfono IP de Cisco, en la página 239](#)
- [Solicitud de información del teléfono en XML, en la página 256](#)

Estado del teléfono IP de Cisco

En esta sección se describe cómo mostrar la información del modelo, los mensajes de estado y las estadísticas de red en el teléfono IP serie 8800 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.

Para obtener más información sobre la solución de problemas, consulte [Solución de problemas, en la página 259](#).

Apertura de la ventana Información del teléfono

Para abrir la pantalla Información del modelo, lleve a cabo estos pasos:

Procedimiento

Paso 1 Pulse **Aplicaciones** .

Paso 2 Seleccione **Información del teléfono**.

Si el usuario está conectado a un servidor seguro o autenticado, se muestra el icono correspondiente (candado o certificado) en la pantalla Información del teléfono, a la derecha de la opción de servidor. Si el usuario no está conectado a un servidor seguro o autenticado, no aparece ningún icono.

Paso 3 Para salir de la pantalla Información del modelo, presione **Salir**.

Campos de Información del teléfono

En la tabla siguiente se describen la configuración de información del teléfono.

Tabla 40: Configuración de Información del teléfono

Opción	Descripción
Número del modelo	El número de modelo del teléfono.
Dirección IPv4	La dirección IP del teléfono.
Nombre de host	El nombre de host del teléfono.
Carga activa	La versión del firmware que hay instalada en el teléfono. El usuario puede pulsar Detalles para obtener más información.
Carga inactiva	<p>La carga inactiva solo aparece si hay una descarga en curso. También se muestran un icono de descarga y el estado «Actualización en curso» o «Error al actualizar». Si un usuario pulsa Detalles durante una actualización, se muestran el nombre de archivo y los componentes de la descarga.</p> <p>Es posible establecer que se descargue una imagen de firmware nueva por adelantado de una ventana de mantenimiento. Por lo tanto, en lugar de esperar a que todos los teléfonos descarguen el firmware, el sistema cambia con más rapidez entre restablecer una carga existente al estado Inactivo e instalar la nueva carga.</p> <p>Cuando se completa la descarga, el icono cambia para indicar el estado completado; se muestra una marca de comprobación en caso de una descarga correcta o una «X» si la descarga falla. Si es posible, el resto de las cargas siguen descargándose.</p>
Última actualización	Fecha de la actualización del firmware más reciente.
Servidor activo	Nombre de dominio del servidor en el que está registrado el teléfono.
Servidor de reserva	Nombre de dominio del servidor de reserva.

Apertura del menú Estado


El menú Estado incluye las opciones siguientes que proporcionan información sobre el teléfono y su funcionamiento:

- Mensajes de estado: muestra la pantalla correspondiente, donde se muestra un registro de mensajes importantes del sistema.
- Estadísticas de Ethernet: muestra la pantalla correspondiente, donde se muestran estadísticas del tráfico de Ethernet.

- Estadísticas inalámbricas: muestra la pantalla correspondiente, si fuera aplicable.
- Estadísticas de llamadas: muestra varios contadores y estadísticas sobre la llamada actual.
- Punto de acceso actual: muestra la pantalla correspondiente, si fuera aplicable.

Para mostrar el menú Estado, lleve a cabo los pasos siguientes:


Procedimiento

-
- Paso 1** Para mostrar el menú Estado, presione **Aplicaciones** .
- Paso 2** Seleccione **Config. admin. > Estado**.
- Paso 3** Para salir del menú Estado, pulse **Salir**.
-

Apertura de la ventana Mensajes de estado

La ventana Mensajes de estado muestra los 30 mensajes de estado más recientes que ha generado el teléfono. Puede acceder a esta pantalla en cualquier momento, incluso aunque el teléfono no haya terminado de iniciarse.

Procedimiento

-
- Paso 1** Pulse **Aplicaciones** .
- Paso 2** Seleccione **Config. admin. > Estado > Mensajes de estado**.
- Paso 3** Para eliminar los mensajes de estado actuales, pulse **Borrar**.
- Paso 4** Para salir de la pantalla Mensajes de estado, pulse **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 41: Mensajes de estado del teléfono IP de Cisco Unified

Mensaje	Descripción	Posible explicación y acción
Error tamaño TFTP de CFG	El archivo de configuración es demasiado grande para el sistema de archivos del teléfono.	Apague y encienda el teléfono.
Error de checksum	El archivo de software descargado está dañado.	Obtenga una copia nueva del firmware, colóquela en el directorio de la memoria flash y copie los archivos en este directorio. Asegurese de que el servidor TFTP esté apagado; en caso contrario, podrían dañarse.

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 es una dirección IP disponible para el teléfono.
CTL e ITL instalados	Los archivos CTL o ITL no están instalados en el teléfono.	Ninguna. Este mensaje es únicamente informativo. El archivo CTL ni el archivo ITL se han instalado.
CTL instalado	Hay instalado un archivo de lista de confianza de certificados (CTL) en el teléfono.	Ninguna. Este mensaje es únicamente informativo. El archivo CTL no se ha instalado por error.
Error al actualizar la CTL	El teléfono no ha podido actualizar el archivo de lista de certificados de confianza (CTL).	Hay un problema con el archivo CTL. Verifique que el archivo CTL es el correcto y que el teléfono tiene acceso a él.
Tiempo de espera de DHCP	El servidor DHCP no responde.	La red está ocupada: los errores pueden reducirse si se reduce la carga de la red. No hay conectividad de red entre el teléfono y el servidor DHCP: verifique las conexiones de red. El servidor DHCP está apagado: confirme que el servidor DHCP está encendido. Los errores persisten: plantéese usar direcciones IP estáticas.
Tiempo de espera de DNS	El servidor DNS no responde.	La red está ocupada: los errores pueden reducirse si se reduce la carga de la red. No hay conectividad de red entre el teléfono y el servidor DNS: verifique las conexiones de red. El servidor DNS está apagado: confirme que el servidor DNS está encendido.
Host DNS desconocido	El servidor DNS no puede resolver el nombre del servidor TFTP o de Cisco Unified Communications Manager.	Verifique que los nombres de host de los servidores TFTP o de Cisco Unified Communications Manager estén configurados correctamente en el servidor DNS. Plantéese usar direcciones IP en lugar de nombres de host.
IP duplicada	Otro dispositivo está usando la dirección IP asignada al teléfono.	Si el teléfono tiene una dirección IP estática, asegúrese de que no ha asignado una dirección IP duplicada. Si utiliza DHCP, compruebe la configuración del servidor DHCP.
Borrando archivos CTL e ITL	Se está borrando el archivo CTL o ITL.	Ninguna. Este mensaje es únicamente informativo.

Mensaje	Descripción	Posible explicación y acción
Error al actualizar la configuración regional	No se encuentran uno o varios archivos de ubicación en el directorio TFTPPath o no son válidos. No se ha cambiado la configuración regional.	<p>En la administración del sistema compruebe que los archivos sigan en los subdirectorios de la administración de la configuración regional:</p> <ul style="list-style-type: none"> • Ubicados en el subdirectorios de la configuración regional <ul style="list-style-type: none"> • tones.xml • Ubicados en el subdirectorios de la configuración regional <ul style="list-style-type: none"> • 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.	<p>El archivo de configuración de este se agrega a la base de datos de Cisco Unified Communications Manager. Si el archivo no se encuentra en la base de datos de Cisco Unified Communications Manager, el servidor TFTP genera la respuesta archivo no encontrado.</p> <ul style="list-style-type: none"> • El teléfono no está registrado en Cisco Unified Communications Manager. Debe agregar manualmente el archivo de configuración de Cisco Unified Communications Manager. Para obtener información sobre cómo los teléfonos se registren automáticamente, consulte el apartado Métodos de adición de teléfonos 73 para obtener información. • Si utiliza DHCP, verifique que el servidor DHCP sea el correcto. • Si usa direcciones IP estáticas, verifique la configuración del servidor TFTP.
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 no se encuentra en Cisco Unified Communications Manager.
Dirección IP liberada	El teléfono está configurado para liberar la dirección IP.	El teléfono permanece inactivo hasta que se restablece la dirección IP.
ITL instalado	El archivo ITL no está instalado en el teléfono.	Ninguna. Este mensaje es único porque el archivo ITL no se ha instalado.

Mensaje	Descripción	Posible explicación y acción
Carga rechazada HC	La aplicación descargada no es compatible con el hardware del teléfono.	Este problema se produce si intenta instalar software en este teléfono que no es compatible con el hardware del teléfono. Compruebe el ID de carga asignado al teléfono (Cisco Unified Communications Manager, Teléfono). Vuelva a introducir la carga en el teléfono.
No hay router predeterminado	En la configuración DHCP o estática no se especifica ningún router predeterminado.	Si el teléfono tiene una dirección IP predeterminada, el router predeterminado está configurado. Si usa DHCP, el servidor DHCP no tiene un router predeterminado. Compruebe la configuración del servidor DHCP.
Sin IP de servidor DNS	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.	Si el teléfono tiene una dirección IP predeterminada, el servidor DNS está configurado. Si usa DHCP, el servidor DHCP no tiene un servidor DNS. Compruebe la configuración del servidor DHCP.
Ninguna lista de confianza instalada	El archivo CTL o el archivo ITL no están instalados en el teléfono.	La lista de confianza no está configurada en Cisco Unified Communications Manager, que no puede garantizar la seguridad de forma predeterminada.
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 cambios en la configuración al teléfono en Cisco Unified Communications Manager y que se haya pulsado Aceptar para surta efecto.
Error de acceso a TFTP	El servidor TFTP dirige a un directorio que no existe.	Si utiliza DHCP, verifique que el servidor TFTP sea el correcto. Si usa direcciones IP estáticas, compruebe la dirección del servidor TFTP.
Error de TFTP	El teléfono no reconoce un código de error proporcionado por el servidor TFTP.	Póngase en contacto con la asistencia técnica.
Tiempo de espera de TFTP	El servidor TFTP no responde.	La red está ocupada: los errores pueden disminuir si se reduce la carga de la red. No hay conectividad de red entre el teléfono y el servidor TFTP: verifique las conexiones de red. El servidor TFTP está apagado: compruebe que el servidor TFTP esté encendido.

Mensaje	Descripción	Posible explicación y acción
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 802.1X no está configurado en el teléfono.
Error al actualizar la lista de confianza	La actualización de los archivos CTL e ITL ha fallado.	<p>El teléfono tiene archivos CTL e ITL que no se pudieron actualizar.</p> <p>Posible motivo del error:</p> <ul style="list-style-type: none"> • Se ha producido un error de conexión con el servidor TFTP. • El servidor TFTP está apagado. • Se han introducido el nuevo archivo CTL o ITL para firmar el archivo CTL o ITL, pero no se usó para firmar el archivo correspondiente disponible en los archivos de configuración del teléfono. • Se ha producido un error de configuración. <p>Posibles soluciones:</p> <ul style="list-style-type: none"> • Compruebe la conectividad con el servidor TFTP. • Compruebe si el servidor TFTP está funcionando con normalidad. • Si el servidor TVS (servicio de verificación de firmas) es compatible con Cisco Unified Communications Manager, compruebe si está funcionando con normalidad. • Verifique si el token de seguridad de los archivos CTL e ITL son válidos. <p>Si todas las soluciones anteriores no funcionan, actualice manualmente los archivos CTL e ITL en el teléfono.</p>
Lista de confianza actualizada	El archivo CTL, el archivo ITL o ambos están actualizados.	Ninguna. Este mensaje es único.
Error de versión	El nombre del archivo de carga del teléfono es incorrecto.	Asegúrese de que el archivo de carga tiene el nombre correcto.
XmlDefault.cnf.xml o .cnf.xml correspondiente al nombre del dispositivo del teléfono	Nombre del archivo de configuración.	Ninguna. Este mensaje indica la configuración del teléfono.

Temas relacionados


[Cisco Unified Communications Manager Documentación](#), en la página xv

Mostrar pantalla de información de red

Utilice la información mostrada en la pantalla de información de red para resolver los problemas de conexión en un teléfono.

Si un usuario tiene problemas al conectarse a una red telefónica, se muestra un mensaje en el teléfono.

Procedimiento


- Paso 1** Para mostrar el menú Estado, presione **Aplicaciones** .
 - Paso 2** Seleccione **Config. admin. > Estado > Mensajes de estado**.
 - Paso 3** Seleccione **Información de red**.
 - Paso 4** Para salir de Información de red, pulse **Salir**.
-

Apertura de la pantalla Estadísticas de red

La pantalla Estadísticas de red muestra información sobre el rendimiento del teléfono y de la red.

Para abrir la pantalla Estadísticas de red, lleve a cabo estos pasos:

Procedimiento

- Paso 1** Presione **Aplicaciones** .
 - Paso 2** Seleccione **Config. admin.>Estado>Estadísticas de red**.
 - Paso 3** Para restablecer las estadísticas de marcos recibidos, marcos transmitidos y difusiones recibidas a 0, presione **Borrar**.
 - Paso 4** Para salir de la pantalla Estadísticas de red, pulse **Salir**.
-

Información de estadísticas de Ethernet

En las tablas siguientes se describe la información de la pantalla Estadísticas de Ethernet.

Tabla 42: Información de estadísticas de Ethernet

Elemento	Descripción
Fotogramas recibidos	El número de paquetes que ha recibido el teléfono.
Fotogramas transmitidos	El número de paquetes que ha enviado el teléfono.
Recibir difusiones	El número de paquetes de difusión que ha recibido el teléfono.

Elemento	Descripción
Causa de reinicio	Causa del último restablecimiento del teléfono. Se especifica uno de los siguientes valores: <ul style="list-style-type: none"> • Inicializado • TCP-timeout • CM-cerrado-TCP • TCP-Bad-ACK • CM-reset-TCP • CM-aborted-TCP • CM-NAKed • KeepaliveTO • Failback • Phone-Keypad • Phone-Re-IP • Reset-Reset • Reset-Restart • Phone-Reg-Rej • Carga rechazada HC • CM-ICMP-Unreach • Phone-Abort
Tiempo transcurrido	Cantidad de tiempo que ha transcurrido desde que el teléfono se reinició por última vez.
Puerto 1	Estado de enlace y conexión del puerto de red. Por ejemplo, Auto 100 Mb dúplex completo significa que el puerto de red está en estado de enlace y ha negociado automáticamente una conexión de dúplex completo de 100 Mb/s.
Puerto 2	Estado de enlace y conexión del puerto PC.
Estado de DHCP (IPv4/IPv6)	<ul style="list-style-type: none"> • En modo solo IPv4, muestra únicamente el estado de DHCPv4, como DHCP BOUND. • En modo IPv6, muestra solo el estado de DHCPv6, como ROUTER ADVERTISE. • Se muestra información de estado de DHCPv6.

En las tablas siguientes se describen los mensajes que aparecen para los mensajes de DHCPv4 y de DHCPv6.

Tabla 43: Mensajes de estadísticas de Ethernet de DHCPv4

Estado de DHCPv4	Descripción
CDP INIT	CDP no está vinculado o la WLAN no está en servicio.
DHCP BOUND	DHCPv4 está vinculado.

Estado de DHCPv4	Descripción
DHCP DISABLED	DHCPv4 está deshabilitado.
DHCP INIT	DHCPv4 está inicializado.
DHCP INVALID	DHCPv4 no es válido; este es el estado inicial.
DHCP RENEWING	DHCPv4 se está renovando.
DHCP REBINDING	DHCPv4 se está reuniendo.
DHCP REBOOT	DHCPv4 está inicializando el reinicio.
DHCP REQUESTING	DHCPv4 está realizando una solicitud.
DHCP RESYNC	DHCPv4 se está resincronizando.
DHCP WAITING COLDBOOT TIMEOUT	DHCPv4 se está reiniciando.
DHCP UNRECOGNIZED	Estado de DHCPv4 no reconocido.
DISABLED DUPLICATE IP	Dirección IPv4 duplicada.
DHCP TIMEOUT	Tiempo agotado para DHCPv4.
IPV4 STACK TURNED OFF	El teléfono está en modo de solo IPv6 con la pila IPv4 desactivada.
ILLEGAL IPV4 STATE	Estado de IPv4 ilegal que no debería ocurrir.

Tabla 44: Mensajes de estadísticas de Ethernet de DHCPv6

Estado de DHCPv6	Descripción
CDP INIT	CDP se está inicializando.
DHCP6 BOUND	DHCPv6 está vinculado.
DHCP6 DISABLED	DHCPv6 está deshabilitado.
DHCP6 RENEW	DHCPv6 se está renovando.
DHCP6 REBIND	DHCPv6 se está reuniendo.
DHCP6 INIT	DHCPv6 se está inicializando.
DHCP6 SOLICIT	DHCPv6 está realizando una petición.
DHCP6 REQUEST	DHCPv6 está realizando una solicitud.
DHCP6 RELEASING	DHCPv6 se está liberando.
DHCP6 RELEASED	DHCPv6 se ha liberado.
DHCP6 DISABLING	DHCPv6 se está deshabilitando.


Estado de DHCPv6	Descripción
DHCP6 DECLINING	DHCPv6 se está rechazando.
DHCP6 DECLINED	DHCPv6 se ha rechazado.
DHCP6 INFOREQ	DHCPv6 está solicitando información.
DHCP6 INFOREQ DONE	DHCPv6 ha finalizado de solicitar información
DHCP6 INVALID	DHCPv6 no es válido; este es el estado inicial.
DISABLED DUPLICATE IPV6	DHCP6 está deshabilitado, pero se ha detectado una IPv6 duplicada.
DHCP6 DECLINED DUPLICATE IP	DHCP6 se ha rechazado. Se ha detectado una IPv6 duplicada.
ROUTER ADVERTISE., (DUPLICATE IP)	Dirección IPv6 configurada automáticamente duplicada.
DHCP6 WAITING COLDBOOT TIMEOUT	DHCPv6 se está reiniciando.
DHCP6 TIMEOUT USING RESTORED VAL	Tiempo agotado para DHCPv6, se va a usar el valor guardado en la memoria flash.
DHCP6 TIMEOUT CANNOT RESTORE	Tiempo agotado para DHCP6 y no hay copia de seguridad en la memoria flash.
IPV6 STACK TURNED OFF	El teléfono está en modo de solo IPv4 con la pila IPv6 desactivada.
ROUTER ADVERTISE., (GOOD IP)	
ROUTER ADVERTISE., (BAD IP)	
UNRECOGNIZED MANAGED BY	La dirección IPv6 no es del router o del servidor DHCPv6.
ILLEGAL IPV6 STATE	Estado de IPv6 ilegal que no debería ocurrir.

Visualización de la pantalla Estadísticas inalámbricas

Este procedimiento se aplica únicamente al teléfono IP 8861 inalámbrico de Cisco.

Para abrir la pantalla Estadísticas inalámbricas, lleve a cabo estos pasos:

Procedimiento

- Paso 1** Pulse **Aplicaciones** .
- Paso 2** Seleccione **Config. admin.** > **Estado** > **Estadísticas inalámbricas**.
- Paso 3** Para restablecer a 0 los valores de las estadísticas inalámbricas, pulse **Borrar**.

Paso 4 Para salir de la pantalla Estadísticas inalámbricas, pulse **Salir**.

Estadísticas de WLAN

En la tabla siguiente se describen las estadísticas de WLAN del teléfono.

Tabla 45: Estadísticas de WLAN del Teléfono IP de Cisco Unified

Elemento	Descripción
bytes transmitidos	El número de bytes que ha transmitido el teléfono.
bytes recibidos	El número de bytes que ha recibido el teléfono.
paquetes transmitidos	El número de paquetes que ha transmitido el teléfono.
paquetes recibidos	El número de paquetes que ha recibido el teléfono.
paquetes transmitidos eliminados	El número de paquetes eliminados durante la transmisión.
paquetes recibidos eliminados	El número de paquetes eliminados durante la recepción.
errores de paquetes transmitidos	El número de paquetes erróneos que ha transmitido el teléfono.
errores de paquetes recibidos	El número de paquetes erróneos que ha recibido el teléfono.
Fotogramas transmitidos	El número de MSDU transmitidas correctamente.
fotogramas de multidifusión transmitidos	El número de MSDU de multidifusión transmitidas correctamente.
reintento de transmisión	El número de MSDU que se han transmitido correctamente después de una o varias retransmisiones.
reintento múltiple de transmisión	El número de MSDU de multidifusión que se han transmitido correctamente después de una o varias retransmisiones.
error de transmisión	El número de MSDU que no se han transmitido correctamente debido a que se ha superado el límite de reintentos de transmisión.
rts correcta	Este contador aumenta cuando se recibe una CTS en respuesta a una RTS.
error de RTS	Este contador aumenta cuando no se recibe una CTS en respuesta a una RTS.
error de ataque	Este contador aumenta cuando no se recibe una ACK cuando se esperaba.
fotogramas duplicados recibidos	El número de fotogramas recibidos que el campo Control de secuencia indica que son duplicados.
paquetes fragmentados recibidos	El número de MPDU de tipo Datos o Administración recibidos correctamente.

Elemento	Descripción
recuento de itinerancia	El número de itinerancias correctas.

Apertura de la ventana Estadísticas de llamadas

Puede acceder a la ventana Estadísticas de llamadas en el teléfono para mostrar contadores, estadísticas y mediciones de calidad de la voz de la llamada más reciente.



Nota También es posible ver de forma remota información de estadísticas de llamadas accediendo mediante un navegador web a la página web Estadísticas de flujo. Esta página contiene estadísticas adicionales de RTCP no disponibles en el teléfono.

Una sola llamada puede usar varios flujos de voz, pero los datos solo se recopilan del último flujo. Un flujo de voz es un flujo de paquetes entre dos terminales. Si un terminal se pone en espera, el flujo de voz se detiene aunque la llamada siga conectada. Cuando la llamada se reanuda, se inicia un nuevo flujo de paquetes de voz y los datos de la nueva llamada sustituyen a los de la antigua.

Procedimiento

- Paso 1** Presione **Aplicaciones** .
- Paso 2** Seleccione **Config. admin.** > **Estado** > **Estadísticas de llamadas**.
- Paso 3** Para salir de la pantalla Estadísticas de llamadas, pulse **Salir**.

Campos de Estadísticas de llamadas

En la tabla siguiente se describen los elementos de la pantalla de estadísticas de llamadas.

Tabla 46: Elementos de Estadísticas de llamadas del teléfono de Cisco Unified

Elemento	Descripción
Códec del destinatario	Tipo de flujo de voz recibido (audio de flujo RTP desde códec): <ul style="list-style-type: none"> • G.729 • G.722 • G722.2 AMR-WB • G.711 ley Mu • G.711 ley A • iLBC • Opus • iSAC


Elemento	Descripción
Códec del remitente	Tipo de flujo de voz transmitido (audio de flujo RTP desde códec): <ul style="list-style-type: none"> • G.729 • G.722 • G722.2 AMR-WB • G.711 ley Mu • G.711 ley A • iLBC. • Opus • iSAC
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.
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 del 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.

Elemento	Descripción
Paquetes perdidos del 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.
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.

Apertura de la ventana Punto de acceso actual

La pantalla Punto de acceso actual muestra estadísticas sobre el punto de acceso que usa el teléfono IP 8861 de Cisco para las comunicaciones inalámbricas.

Procedimiento

-
- Paso 1** Presione **Aplicaciones** .
- Paso 2** Seleccione **Config. admin. > Estado > Punto de acceso actual**.
- Paso 3** Para salir de la pantalla Punto de acceso actual, pulse **Salir**.
-

Campos de Punto de acceso actual

En la tabla siguiente se describen los campos de la pantalla Punto de acceso actual.

Tabla 47: Elementos de Punto de acceso actual

Elemento	Descripción
Nombre de AP	Nombre del punto de acceso, si es compatible con CCX; en caso contrario, aquí se muestra la dirección MAC.

Elemento	Descripción
Dirección MAC	Dirección MAC del punto de acceso.
Frecuencia	La última frecuencia en la que se observó este punto de acceso.
Canal actual	El último canal en el que se observó este punto de acceso.
RSSI último	El último RSSI en el que se observó este punto de acceso.
Intervalo de señal	Número de unidades de tiempo entre señales. Una unidad de tiempo es 1,024 ms.
Capacidad	Este campo contiene varios campos secundarios que se usan para indicar capacidades opcionales solicitadas o anunciadas.
Velocidades básicas	Velocidades de datos que requiere el punto de acceso y el punto de acceso en el que la estación debe ser capaz de funcionar.
Velocidades opcionales	Velocidades de datos que admite el punto de acceso y el punto de acceso opcional en el que puede funcionar la estación.
Velocidades de VHT (rx) compatibles	Conjunto RX MCS compatibles con VHT recibido del punto de acceso.
Velocidades de VHT (tx) compatibles	Conjunto TX MCS compatibles con VHT recibido del punto de acceso.
HT MCS compatible	Conjunto MCS compatibles con HT recibido del punto de acceso.
Periodo DTIM	Cada enésima señal es un periodo de tiempo (dtime). Después de cada señal DTIM, el punto de acceso envía paquetes de difusión o de multidifusión que se ponen en cola en los dispositivos con ahorro de energía.
Código del país	Un código de país de dos dígitos. Si el elemento de información del país (IE) no está presente en la señal, la información del país podría no mostrarse.
Canales	Una lista de canales admitidos (del IE de país).
Restricción de potencia	La cantidad de potencia que debe reducir la transmisión máxima de energía respecto al límite de dominio regulador.
Límite de alimentación	Energía de transmisión máxima en dBm que se permite para el canal.
Utilización de canal	El porcentaje de tiempo, redondeado a 255, en el que el punto de acceso detectó que el medio estaba ocupado, como indica el mecanismo de sentido de portadora (CS) física o virtual.
Número de estaciones	El número total de STA asociadas actualmente a este punto de acceso.
Capacidad de admisión	Un número entero sin firmar que especifica la cantidad restante de tiempo del medio disponible mediante el control de admisión explícito, en unidades de 32 microsegundos por segundo. Si el valor es 0, el punto de acceso no admite este elemento de información y se desconoce la capacidad.

Elemento	Descripción
WMM compatible	Compatibilidad para las extensiones multimedia Wi-Fi.
UAPSD compatible	El punto de acceso admite la entrega de ahorro de energía automático sin programar. Podría estar disponible solo si se admite WMM. Esta función es fundamental para el tiempo de conversación y para conseguir la máxima densidad de llamada en el teléfono IP inalámbrico.
Proxy ARP	Los puntos de acceso compatibles con CCX admiten la respuesta a solicitudes ARP de IP en nombre de la estación asociada. Esta función es fundamental para el tiempo de reserva en el teléfono IP inalámbrico.
Versión de CCX	Si el punto de acceso es compatible con CCX, este campo muestra la versión de CCX.
Mayor esfuerzo	Contiene información relacionada con la cola de mejor esfuerzo.
Información de referencia	Contiene información relacionada con la cola de fondo.
Vídeo	Contiene información relacionada con la cola de vídeo.
Voz	Contiene información relacionada con la cola de voz.

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.
- Sistema: muestra un hipervínculo para reiniciar el teléfono.

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

Para acceder a la página web de un teléfono, siga estos pasos:



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:
- 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.
 - En el teléfono IP de Cisco, pulse **Aplicaciones** , seleccione **Config. admin. > Configuración de red > Configuración de Ethernet > Configuración de IPv4** y diríjase al campo Dirección IP.
- 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://Dirección_IP**

Información del 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.



Nota Algunos de los elementos de la tabla siguiente no se aplican a todos los modelos de teléfonos.

Para mostrar el área **Información del dispositivo**, acceda a la página web del teléfono como se describe en [Acceso a la página web del teléfono, en la página 239](#) y, a continuación, haga clic en el hipervínculo **Información del dispositivo**.

Tabla 48: Elementos de la sección Información del dispositivo

Elemento	Descripción
Modo de servicio	El modo de servicio para el teléfono.
Nombre de 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.

Elemento	Descripción
ID de carga de la aplicación	La versión del firmware de la aplicación que se está ejecutando en el teléfono.
ID de carga de inicio	Versión de firmware de inicio.
Versión	Identificador del firmware que se está ejecutando en el teléfono.
Módulo de expansión clave 1	Identificador del primer módulo de expansión clave, si fuera aplicable. Aplicable al teléfono IP 8851, 8851NR, 8861, 8865 y 8865NR de Cisco.
Módulo de expansión clave 2	Identificador del segundo módulo de expansión clave, si fuera aplicable. Aplicable al teléfono IP 8851, 8851NR, 8861, 8865 y 8865NR de Cisco.
Módulo de expansión clave 3	Identificador del tercer módulo de expansión clave, si fuera aplicable. Aplicable al teléfono IP 8851, 8851NR, 8861, 8865 y 8865NR de Cisco.
Revisión de hardware	Valor de revisión menor del hardware del teléfono.
N.º de serie	El número de serie exclusivo del teléfono.
Número del 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: <ul style="list-style-type: none"> • Tipo de dispositivo: indica el tipo de hardware. Por ejemplo, para todos los modelos de teléfonos se muestra que es un teléfono. • Descripción del dispositivo: muestra el nombre del teléfono asociado al tipo de modelo indicado. • Identificador de producto: especifica el modelo de teléfono. • ID de versión (VID): especifica el número de versión del hardware principal. • N.º de serie: muestra el número de serie exclusivo del teléfono.
UDI del módulo de expansión clave	Identificador único de dispositivo (UDI) de Cisco del módulo de expansión clave. Aplicable al teléfono IP 8851, 8851NR, 8861, 8865 y 8865NR de Cisco.

Elemento	Descripción
Nombre de los auriculares	<p>Muestra en la columna de la izquierda el nombre de los auriculares de Cisco conectados. La columna de la derecha contiene la siguiente información:</p> <ul style="list-style-type: none"> • Puerto: muestra cómo se conectan los auriculares al teléfono. <ul style="list-style-type: none"> • USB • AUXILIAR • Versión: muestra la versión del firmware de los auriculares. • Intervalo de radio: muestra la intensidad configurada para el aparato de radio DECT. Aplicable solo a Auriculares Cisco serie 560. • Ancho de banda: se muestra si los auriculares utilizan banda ancha o banda estrecha. Aplicable solo a Auriculares Cisco serie 560. • Bluetooth: muestra si Bluetooth está activado o desactivado. Aplicable solo a Auriculares Cisco serie 560. • Conferencia: muestra si la función de conferencia está activada o desactivada. Aplicable solo a Auriculares Cisco serie 560. • Origen de firmware: muestra el método de actualización de firmware permitido: <ul style="list-style-type: none"> • Restringir a solo UCM • Permitir desde UCM o Cisco Cloud <p>Aplicable solo a Auriculares Cisco serie 560.</p>
Hora	La hora del grupo de fecha y hora al que pertenece el teléfono. Esta información proviene de Cisco Unified Communications Manager.
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 sin utilizar en el teléfono
Memoria libre de montículo de Java	Cantidad libre de memoria en montón de Java interna
Memoria libre de grupo de Java	Cantidad libre de memoria agrupada de Java interna
Modo FIPS habilitado	Indica si está activado el modo de estándar federal de procesamiento de información (FIPS).

Configuración de la 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.



Nota Algunos de los elementos de la tabla siguiente no se aplican a todos los modelos de teléfonos.

Para mostrar el área **Configuración de red**, acceda a la página web del teléfono que se describe en [Acceso a la página web del teléfono, en la página 239](#) y, a continuación, haga clic en el hipervínculo **Configuración de red**.

Tabla 49: 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 teléfono.
Servidor DHCP	La dirección IP del servidor de protocolo de configuración de host dinámico (DHCP) del que el teléfono obtiene la dirección IP.
Servidor BOOTP	Indica si el teléfono obtiene la configuración de un servidor de protocolo de arranque-asignación (BOOTP o bootstrap).
DHCP	Indica si el teléfono usa DHCP.
Dirección IP	Indica la dirección del protocolo de Internet (IPv4) del teléfono.
Máscara de subred	La máscara de subred que usa el teléfono.
Router predet.	El router predeterminado que usa el teléfono.
Servidor DNS 1-3	El servidor de sistema de nombre de dominio primario (Servidor DNS 1) y los servidores 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 teléfono.
Servidor TFTP 2	El servidor de protocolo de transferencia de archivos trivial (TFTP) de copia de seguridad que usa el teléfono.
Dirección DHCP liberada	Indica el valor de la opción Dirección DHCP liberada en el menú Configuración de red del teléfono.
ID de VLAN operativo	La red de área local virtual (VLAN) operativa configurada en un switch Cisco Catalyst del que es miembro el teléfono.

Elemento	Descripción
ID de VLAN administrativo	La VLAN auxiliar de la que es miembro el teléfono.
Servidor CUCM 1-5	<p>Los nombres de host o las direcciones IP, en orden de prioridad, de los servidores de Cisco Unified Communications Manager con los que se puede registrar el teléfono. Un elemento también puede mostrar la dirección IP de un router SRST capaz de proporcionar funciones limitadas de Cisco Unified Communications Manager, en caso de que dicho router esté disponible.</p> <p>Para un servidor disponible, un elemento muestra la dirección IP del servidor de Cisco Unified Communications Manager y uno de los estados siguientes:</p> <ul style="list-style-type: none"> • Activo: el servidor de Cisco Unified Communications Manager desde el que el teléfono está recibiendo los servicios de procesamiento de llamadas. • Reserva: el servidor de Cisco Unified Communications Manager al que cambia el teléfono cuando el servidor actual deja de estar disponible. • En blanco: actualmente no hay conexión con este servidor de Cisco Unified Communications Manager. <p>Un elemento también puede incluir la designación de Survivable Remote Site Telephony (SRST) que identifica un router SRST capaz de proporcionar un conjunto limitado de funciones de Cisco Unified Communications Manager. Este router asume el control del procesamiento de llamadas si todos los demás servidores de Cisco Unified Communications Manager dejan de estar disponibles. El primer router SRST de Cisco Unified Communications Manager siempre aparece el último en la lista de servidores de Cisco Unified Communications Manager, incluso si está activo. La dirección del router SRST se configura en la sección Grupo de dispositivos de la ventana de configuración de Cisco Unified Communications Manager.</p>
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 directorio.
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 IP de Cisco Unified.
URL de inactividad	La dirección URL que el teléfono muestra cuando está inactivo durante el tiempo especificado en el campo Tiempo URL de inactividad y no hay ningún menú abierto.
Tiempo URL de inactividad	El número de segundos que el teléfono permanece inactivo y no se abre ningún menú antes de que se 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 hosts locales en nombre del cliente HTTP del teléfono y que proporciona respuestas desde el host proxy al cliente HTTP del teléfono.
URL de autenticación	La dirección URL que usa el teléfono para validar las solicitudes realizadas al servidor web del

Elemento	Descripción
Config. de puerto switch	La velocidad y dúplex del puerto PC, donde: <ul style="list-style-type: none"> • 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 de puerto PC	La velocidad y dúplex del puerto PC, donde: <ul style="list-style-type: none"> • 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 PC
Puerto PC deshabilitado	Indica si el puerto PC del teléfono está activado o desactivado.
Configuración regional de usuario	La configuración regional asociada con el usuario del teléfono. Identifica una serie de compatibilidad para los usuarios, como el idioma, la fuente, el formato de fecha y hora e sobre el teclado alfanumérico.
Configuración regional de red	La configuración regional de la red asociada con el usuario del teléfono. Identifica una serie de compatibilidad para el teléfono en una ubicación específica, como la definición de los cadencias utilizados por el teléfono.
Versión de configuración regional de usuario	La versión de la configuración regional del usuario cargada en el teléfono.
Versión de configuración 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.
GARP habilitado	Indica si el teléfono recuerda las direcciones MAC de las respuestas ARP gratuitas.
Distribuir a puerto PC	Indica si el teléfono reenvía los paquetes transmitidos o recibidos por el puerto de red al p acceso.
Capacidad de vídeo habilitada	Indica si el teléfono puede participar en videollamadas si se equipa una cámara apropiada
VLAN de voz habilitada	Indica si el teléfono permite que un dispositivo conectado al puerto PC pueda acceder a la voz.
VLAN de PC activado	La VLAN que identifica y elimina las etiquetas 802.1P/Q de los paquetes que se envían a

Elemento	Descripción
Selección de línea automática habilitada	Identifica si el teléfono selecciona automáticamente una línea cuando se descuelga el teléfono.
Control de protocolo DSCP	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 (no seguro)	El modo de seguridad que se establece para el teléfono.
Acceso vía Web habilitado	Indica si el acceso web está habilitado (Sí) o deshabilitado (No) para el teléfono.
Acceso SSH activado	Indica si el puerto SSH se ha activado o desactivado.
CDP: puerto switch	<p>Indica si existe compatibilidad con CDP en el puerto de switch (de forma predeterminada está habilitado).</p> <p>Habilite CDP en el puerto de switch para la asignación de VLAN del teléfono, la negociación de QoS y la seguridad 802.1x.</p> <p>Habilite CDP en el puerto de switch si el teléfono se conecta a un switch de Cisco.</p> <p>Si CDP está deshabilitado en Cisco Unified Communications Manager, se muestra una advertencia que indica que CDP solo se debe deshabilitar en el puerto de switch si el teléfono se conecta a un switch que no sea de Cisco.</p> <p>Los valores de CDP actuales para el puerto PC y el puerto de switch se muestran en el menú Configuración.</p>
CDP: puerto PC	<p>Indica si existe compatibilidad con CDP en el puerto PC (de forma predeterminada está habilitado).</p> <p>Si CDP está deshabilitado en Cisco Unified Communications Manager, se muestra una advertencia que indica que al deshabilitar CDP en el puerto PC se impide que CVTA funcione.</p> <p>Los valores de CDP actuales para el puerto PC y el puerto switch se muestran en el menú Configuración.</p>
LLDP-MED: puerto SW	Indica si LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery) está habilitado en el puerto de switch.
LLDP-MED: puerto PC	Indica si LLDP-MED está activado en el puerto PC.
LLDP Prioridad energética	<p>Prioridad energética del teléfono al conmutador, activando de esta forma el conmutador para que proporcione la energía oportuna a los teléfonos. Los valores disponibles son:</p> <ul style="list-style-type: none"> • Desconocido: este es el valor predeterminado. • Bajo. • Alto. • Crítico.
LLDP ID del dispositivo	ID del dispositivo asignado al teléfono para la administración del inventario.
Archivo CTL	Hash MD5 del archivo CTL.

Elemento	Descripción
Archivo ITL	El archivo ITL contiene la lista de confianza inicial.
Firma ITL	Hash MD5 del archivo ITL
Servidor CAPF	Servidor CPF en uso
TVS	El componente principal de seguridad de forma predeterminada. Los servicios de verificación de confianza (TVS) permiten a los teléfonos IP de Cisco Unified autenticar los servidores de confianza como los servicios EM, el directorio y MIDlet durante el establecimiento de HTTPS.
Servidor TFTP	El nombre del servidor TFTP usado por el teléfono.
Servidor TFTP	El nombre del servidor TFTP usado por el teléfono.
Sincronización de puerto automática	Indica si el teléfono sincroniza automáticamente la velocidad del puerto para eliminar la pérdida de paquetes.
Cambiar configuración remota de puerto	Indica si el puerto SW se controla de forma remota.
Configuración remota de puerto PC	Indica si el puerto PC se controla de forma remota.
Modo de direcciones IP	Identifica el modo de dirección: <ul style="list-style-type: none"> • Solo IPv4 • IPv4 y IPv6 • Solo IPv6
Control del modo de preferencias de IP	Indica la versión de la dirección IP que utiliza el teléfono durante la señalización con Cisco Communications Manager cuando tanto IPv4 como IPv6 están disponibles en el teléfono.
Modo de preferencias de IP para medios	
Configuración de IPv6 automática	Indica que, para los medios, el dispositivo usa una dirección IPv4 a fin de conectarse con Cisco Communications Manager.
Protección de direcciones IPv6 duplicadas	
Mensaje de redirección de aceptación de IPv6	Indica si el teléfono acepta los mensajes redirigidos desde el mismo router que se usó para el 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 de eco enviado a una dirección solo IPv6.
Servidor de carga de IPv6	Se usa para optimizar el tiempo de instalación durante las actualizaciones del firmware de descargar el tráfico de la WAN al almacenar imágenes localmente, lo que evita tener que enlazar WAN en cada actualización del teléfono.

Elemento	Descripción
Servidor de registro de IPv6	
Servidor CAPF de IPv6	Indica la dirección IP y el puerto del equipo de registro remoto al que el teléfono envía los mensajes de registro.
DHCPv6	Indica el método que usa el teléfono para obtener la dirección de solo IPv6. Si DHCPv6 está habilitado, el teléfono obtiene la dirección IPv6 del servidor DHCPv6 o de SLAAC con el RA enviado por el router IPv6. Si DHCPv6 está deshabilitado, el teléfono no tendrá ni dirección IPv6 con estado (del servidor DHCPv6) o sin estado (de SLAAC). Nota A diferencia de DHCPv4, aunque DHCPv6 esté deshabilitado, el teléfono podrá obtener una dirección SLAAC si la configuración automática está activada.
Dirección IPv6	Muestra la dirección solo IPv6 actual del teléfono. Se admiten dos formatos de dirección: <ul style="list-style-type: none"> • Ocho conjuntos de dígitos hexadecimales separados por dos puntos (X:X:X:X:X:X:X:X) • Formato comprimido para contraer una única sección de grupos de ceros consecutivos en un grupo representado por dos signos de dos puntos.
Longitud de prefijo de IPv6	Muestra la longitud del prefijo solo IPv6 actual de la subred.
Router predeterminado de IPv6	Muestra el router de IPv6 predeterminado usado por el teléfono.
Servidor DNS 1 de IPv6 1-2	Muestra el servidor DNSv6 primario y secundario usado por el teléfono
TFTP alternativo de IPv6	Indica si se usa un servidor TFTP IPv6 alternativo.
Servidor TFTP de IPv6 1-2	Muestra el servidor TFTP de IPv6 principal y secundario usado por el teléfono.
Dirección IPv6 liberada	Indica si el usuario ha publicado la información relacionada con IPv6.
Nivel de energía EnergyWise	El nivel de energía que se utiliza cuando el teléfono está inactivo.
Dominio de EnergyWise	El dominio de EnergyWise en el que se encuentra el teléfono.
DF_BIT	Indica el ajuste de bit DF de los paquetes.

Estadísticas de red

Los siguientes hipervínculos de estadísticas de red de la página web de un teléfono proporcionan información sobre el tráfico de red del teléfono.

- Información Ethernet: muestra información sobre el tráfico Ethernet.

- Acceso: muestra información sobre el tráfico de red que entra y sale del puerto PC del teléfono.
- Red: muestra información sobre el tráfico de red que entra y sale del puerto de red del teléfono.

Para mostrar la sección de estadísticas de red, acceda a la página web del teléfono y haga clic en los hipervínculos **Información Ethernet**, **Acceso** o **Red**.

Página web Información de Ethernet

En la tabla siguiente se describe el contenido de la página web Información de Ethernet.

Tabla 50: 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 acceso y red

En la tabla siguiente se describe la información de las páginas web Acceso y Red.

Tabla 51: Campos de Acceso y Red

Elemento	Descripción
Rx totalPkt	El número total de paquetes que ha recibido el teléfono.
Rx crcErr	El número total de paquetes recibidos con errores de CRC.
Rx alignErr	El número total de paquetes de entre 64 y 1522 bytes de longitud que se han recibido y que tenían una secuencia de comprobación de marcos (FCS) errónea.

Elemento	Descripción
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 shortErr	El número total de paquetes de error de FCS o de error de alineación recibidos de menos de 64 bytes de tamaño.
Rx shortGood	El número total de paquetes correctos recibidos de menos de 64 bytes de tamaño.
Rx longGood	El número total de paquetes correctos recibidos de más de 1522 bytes de tamaño.
Rx longErr	El número total de paquetes de error de FCS o de error de alineación recibidos de más de 1522 bytes de tamaño.
Rx size64	El número total de paquetes recibidos, incluidos los paquetes incorrectos, de entre 0 y 64 bytes de tamaño.
Rx size65to127	El número total de paquetes recibidos, incluidos los paquetes incorrectos, de entre 65 y 127 bytes de tamaño.
Rx size128to255	El número total de paquetes recibidos, incluidos los paquetes incorrectos, de entre 128 y 255 bytes de tamaño.
Rx size256to511	El número total de paquetes recibidos, incluidos los paquetes incorrectos, de entre 256 y 511 bytes de tamaño.
Rx size512to1023	El número total de paquetes recibidos, incluidos los paquetes incorrectos, de entre 512 y 1023 bytes de tamaño.
Rx size1024to1518	El número total de paquetes recibidos, incluidos los paquetes incorrectos, de entre 1024 y 1518 bytes de tamaño.
Rx tokenDrop	El número total de paquetes que se han interrumpido debido a falta de recursos (por ejemplo, por desbordamiento de FIFO).
Tx excessDefer	El número total de paquetes cuya transmisión se ha retrasado debido a medios ocupados.
Tx lateCollision	El número de veces que se han producido colisiones después de las veces de 512 bit tras el inicio de la transmisión del paquete.
Tx totalGoodPkt	El número total de paquetes correctos (multidifusión, difusión y unidifusión) que ha recibido el teléfono.
Tx Collisions	El número total de colisiones que se han producido mientras se transmitía un paquete.
Tx excessLength	El número total de paquetes que no se han transmitido porque el paquete ha experimentado 16 intentos de transmisión.

Elemento	Descripción
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 IPv6 de vecino CDP	La dirección IP del dispositivo vecino descubierto que el protocolo CDP ha descubierto.
Puerto de vecino CDP	El puerto del dispositivo vecino en el que está conectado el teléfono descubierto por el protocolo CDP.
ID de dispositivo vecino LLDP	El identificador de un dispositivo conectado a este puerto que el protocolo LLDP ha descubierto.
Dirección IPv6 de vecino LLDP	La dirección IP del dispositivo vecino descubierto que el protocolo LLDP ha descubierto.
Puerto de vecino LLDP	El puerto del dispositivo vecino al que se conecta el teléfono que el protocolo LLDP ha descubierto.
Información de puerto	La velocidad y el dúplex de la información.

Registros de dispositivos

Los hipervínculos de registro de dispositivo siguientes de una página web proporcionan información que ayuda a supervisar el teléfono y a solucionar problemas.

- Registros de consola: incluye hipervínculos 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 hipervínculos 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. La pantalla Mensajes de estado del teléfono también muestra esta información.
- Pantalla de depuración: muestra mensajes de depuración que podrían ser de utilidad al servicio de asistencia técnica de Cisco si necesita ayuda para solucionar problemas.

Estadísticas de flujo

Los teléfonos Teléfono IP de Cisco Unified pueden intercambiar flujos de información con hasta tres 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.

En la tabla siguiente se describen los elementos de las secciones de estadísticas de flujo.

Tabla 52: Elementos de la sección de 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 Manager al teléfono iniciara la transmisión de los paquetes.
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 del remitente	El número total de paquetes de datos de RTP que el teléfono ha transmitido desde que se estableció la conexión. El valor es 0 si la conexión se establece en el modo de solo recepción.
Octetos del remitente	El número total de octetos de carga que el teléfono ha transmitido en paquetes de datos de RTP desde que se inició la conexión. El valor es 0 si la conexión se establece en el modo de solo recepción.
Códec del remitente	El tipo de codificación de audio del flujo transmitido.
Informes del remitente enviados (consulte la nota)	El número de veces que se ha enviado el informe de remitente de RTCP.
Hora de envío del informe del remitente (consulte la nota)	La marca de hora interna indica cuándo se envió por última vez el informe de remitente de RTCP.
Paquetes perdidos del destinatario	El número total de paquetes de datos de RTP que se han perdido desde que se inició la conexión. Se define como el número de paquetes esperado menos el número de paquetes recibidos en realidad, donde el número de paquetes recibidos incluye los que se retrasan o llegan duplicados. El valor se muestra como 0 si la conexión se establece en el modo de solo envío.

Elemento	Descripción
Promedio de Jitter	Calcula la desviación media del tiempo de interarribo del paquete de datos de RTP, milisegundos. El valor se muestra como 0 si la conexión se establece en el modo de solo envío.
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 de envío de informe del destinatario (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 inició la recepción de datos en esta conexión. Incluye los paquetes que se reciben de fuentes distintas si se trata de una llamada de multidifusión. El valor se muestra como 0 si la conexión se establece 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 desde que se inició la conexión. Incluye los paquetes que se reciben de fuentes distintas si se trata de una llamada de multidifusión. El valor se muestra como 0 si la conexión se establece en el modo de solo envío.
MOS LQK	<p>La puntuación es un cálculo objetivo de la puntuación de opinión media (MOS) de escucha (LQK) que varía entre 5 (excelente) y 1 (mala). Esta puntuación se basa en los eventos de encubrimiento audibles que se producen en la pérdida de marcos del intervalo de ocho segundos precedente al flujo de voz. Para obtener más información, consulte Solución de problemas de la calidad de voz, en la página 282.</p> <p>Nota La puntuación de LQK de MOS puede variar debido al tipo de códec que se usa en el teléfono IP de Cisco Unified.</p>
MOS LQK Promedio	La puntuación media de LQK de MOS observada para todo el flujo de voz.
LQK de MOS mínimo	La puntuación de LQK de MOS más baja observada desde el inicio del flujo de voz.
LQK de MOS máximo	<p>La línea base o la puntuación de LQK de MOS más alta observada desde el inicio del flujo de voz.</p> <p>Estos códecs proporcionan la siguiente puntuación de LQK de MOS máxima en condiciones normales sin pérdida de marcos:</p> <ul style="list-style-type: none"> • G.711 produce 4,5. • G.729 A /AB produce 3,7.
Versión MOS LQK	Versión del algoritmo propiedad de Cisco que se usa para calcular las puntuaciones de MOS.
Proporción de encubrimiento acumulada	El número total de marcos de encubrimiento dividido por el número total de marcos que 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 intervalo a de tres segundos de voz activa. Si la detección de actividad de voz (VAD) está en uso, p 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 e 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 (perdidos) desde el inicio del flujo de voz.
Latencia (consulte la nota)	Calcula la latencia de red, expresada en milisegundos. Representa una media de ejecu la demora de ida y vuelta, medida cuando el receptor de RTCP informa de que ha recib 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 del remitente recibidos (consulte la nota)	El número de veces que se han recibido informes de remitente de RTCP.
Hora de recepción del informe del remitente (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 los b de fluctuación.
Informes destinatario recibidos (consulte la nota)	El número de veces que se han recibido informes de receptor de RTCP.
Hora de recepción de informe del destinatario (consulte la nota)	La hora de la última vez que se recibió un informe de receptor de RTCP.
Destinatario cifrado	Indica si el destinatario está utilizando el cifrado.
Remitente cifrado	Indica si el remitente está utilizando el cifrado.
Marcos de remitente	Número de fotogramas enviados.
Marcos parciales de remitente	Número de fotogramas parciales enviados.
Fotogramas I de remitente	Número de fotogramas I enviados. Los fotogramas I se utilizan en la transmisión de ví

Elemento	Descripción
IFrames de remitente	Número de fotogramas de actualización de descodificador instantáneo (IDR) enviados. Los fotogramas IDR se utilizan en la transmisión de vídeo.
Velocidad de marcos del remitente	Velocidad a la que el remitente envía fotogramas.
Ancho de banda del remitente	Ancho de banda para el remitente.
Resolución del remitente	Resolución de vídeo del remitente.
Marcos del destinatario	Número de fotogramas recibidos
Marcos parciales del destinatario	Número de fotogramas parciales recibidos
Fotogramas I del destinatario	Número de fotogramas I recibidos.
IFrames del destinatario	Número de fotogramas IDR recibidos.
Solicitud de IFrames del destinatario	Número de fotogramas IDR solicitados recibidos.
Velocidad de marcos del destinatario	Velocidad a la que el receptor recibe los fotogramas.
Marcos perdidos del destinatario	Número de fotogramas que no se han recibido.
Errores de marcos del destinatario	Número de fotogramas que no se han recibido.
Ancho de banda del destinatario	Ancho de banda del receptor.
Resolución del destinatario	Resolución de vídeo del receptor.
Dominio	Dominio en el que se encuentra el teléfono.
Conexiones del remitente	Número de veces que se unió el remitente.
Conexiones del destinatario	Número de veces que se unió el receptor.
Secuencias detenidas	Número de fotogramas de «secuencias detenidas»
Hora de inicio del remitente	Hora en la que el remitente inició la operación.
Hora de inicio del destinatario	Hora en la que el receptor inició la operación.
Estado de fila	Si el teléfono está transmitiendo
Herramienta del remitente	Tipo de codificación de audio utilizado para la secuencia
Informes del remitente	Informes del remitente RTCP
Hora de informe del remitente	Última vez que se envió el informe del remitente RTCP.
Fluctuación del destinatario	Fluctuación máxima de secuencia

Elemento	Descripción
Herramienta del destinatario	Tipo de codificación de audio utilizado para la secuencia
Informes del destinatario	Número de veces que se ha accedido a este informe de estadísticas de transmisión desde página web.
Hora de informe del destinatario	Marca de tiempo interna que indica cuándo se ha generado este informe de estadísticas de transmisión
Es un vídeo	Indica si la llamada era una llamada de vídeo o solo de audio.
ID de llamada	Identificación de la llamada
ID de grupo	Identificación del grupo en el que está el teléfono.



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 ModelInfo

El código XML siguiente es un ejemplo del resultado del comando ModelInfo.

```

<?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

- [Información sobre la solución de problemas generales, en la página 259](#)
- [Problemas de inicio, en la página 260](#)
- [Problemas de restablecimiento del teléfono, en la página 265](#)
- [El teléfono no se conecta con la LAN, en la página 267](#)
- [Problemas de seguridad del teléfono IP de Cisco, en la página 267](#)
- [Problemas de llamadas de vídeo, en la página 269](#)
- [Problemas generales de las llamadas telefónicas, en la página 270](#)
- [Procedimientos para solucionar problemas, en la página 271](#)
- [Control de la información de depuración desde Cisco Unified Communications Manager, en la página 276](#)
- [Información adicional sobre solución de problemas, en la página 277](#)

Información sobre la solución de problemas generales

En la tabla siguiente se proporciona información general para solucionar problemas del teléfono IP de Cisco.

Tabla 53: Solución de problemas del teléfono IP de Cisco

Resumen	Explicación
Conexión de un teléfono IP de Cisco a otro	Cisco no admite la conexión de un teléfono IP a otro a través del puerto de un teléfono IP. El teléfono IP debe conectarse directamente a un puerto switch. Si los teléfonos se conectan juntos en una línea mediante el puerto PC, no funcionan.
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 un curso o que no se pueda iniciar o contestar una llamada. Puede que los teléfonos se recuperen hasta que finalice la tormenta de difusión.

Resumen	Explicación
Cambio de una conexión de red del teléfono a una estación de trabajo	<p>Si alimenta el teléfono a través de la conexión de red, debe tener cuidado s desenchufar la conexión del red del teléfono y enchufar el cable a un equip escritorio.</p> <p>Precaución La tarjeta de red del ordenador no puede recibir alimentación de la conexión de red. Si entra alimentación a través de la conexión de red, la tarjeta de red se destruirá. Para proteger la tarjeta de red, espere 10 segundos después de desenchufar el cable del teléfono antes de enchufarlo a un ordenador. Este retraso da al switch tiempo suficiente para reconocer que ya no hay un teléfono en la línea y dejar de proporcionar alimentación al cable.</p>
Cambio de la configuración del teléfono	<p>De forma predeterminada, las opciones de configuración de red están bloqueadas para evitar que los usuarios realicen cambios que puedan afectar a su conexión de red. Debe desbloquear las opciones de configuración de red para poder configurarlas. Consulte el apartado Aplicación de una contraseña al teléfono en la página 50 para obtener información más detallada.</p> <p>Nota Si no se define la contraseña de administrador en el perfil de configuración del teléfono, el usuario puede modificar la configuración de red.</p>
Falta de coincidencia de códecs entre el teléfono y otro dispositivo	<p>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 valores de estas estadísticas deben coincidir. Si no es así, verifique que el otro dispositivo puede manejar la conversación del códec o que hay presente un transcodificador para el servicio.</p>
Falta de coincidencia de muestras de sonido entre el teléfono y otro dispositivo	<p>Las estadísticas de RxSize y TxSize muestran el tamaño de los paquetes de voz que se usan para la conversación entre el teléfono IP de Cisco y el otro dispositivo. Los valores de estas estadísticas deben coincidir.</p>
Condición de bucle invertido	<p>Si las condiciones siguientes se cumplen, se podría producir una situación de bucle invertido:</p> <ul style="list-style-type: none"> • La opción de configuración del puerto switch del menú Configuración de red del teléfono está establecida 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). <p>En este caso, el puerto de switch del teléfono puede desactivarse y se muestra el siguiente mensaje en el registro de la consola del switch:</p> <pre>HALF_DUX_COLLISION_EXCEED_THRESHOLD</pre> <p>Para resolver este problema, vuelva a habilitar el puerto desde el switch.</p>

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 65

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 65

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 271](#).

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.

Temas relacionados

[Apertura de la ventana Mensajes de estado](#), en la página 225

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 272

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.

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.

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 275](#).

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.

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 73](#) 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 72](#).

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 263](#) 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.

Teléfono no registrado

Problema

La pantalla del teléfono muestra el mensaje "Introducir código de activación o dominio de servicio".

Solución

Falta la dirección TFTP en el teléfono. Compruebe que el servidor DHCP proporcione la opción 150 o que se haya configurado manualmente un TFTP alternativo.

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.

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 **Aplicaciones**  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 273](#).

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 llamadas de vídeo

Sin vídeo entre dos teléfonos de vídeo IP de Cisco

Problema

El vídeo no se está transmitiendo entre dos teléfonos de vídeo IP de Cisco.

Solución

Marque esta casilla para asegurarse de que no se está usando ningún Media Termination Point (MTP) en el flujo de llamadas.

Interrupciones de vídeo o fotogramas

Problema

Cuando estoy en una llamada de vídeo, el vídeo se almacena en búfer o interrumpe los fotogramas.

Solución

La calidad de la imagen depende del ancho de banda de la llamada. Si se eleva la velocidad de bits, aumenta la calidad del vídeo, pero se requieren recursos de red adicionales. Utilice siempre la velocidad de bits más adecuada para el tipo de vídeo. Una llamada de vídeo de 720p y 15 fotogramas por segundo requiere una velocidad de bits de 790 kbps o superior. Una llamada de vídeo de 720p y 30 fotogramas por segundo requiere una velocidad de bits de 1360 kbps o superior.

Para obtener información adicional sobre el ancho de banda, consulte la sección Configuración de la resolución de transmisión del vídeo del capítulo "Funciones y configuración del teléfono".

Solución

Confirme que el parámetro de Velocidad de bits de sesión máxima para llamadas de vídeo sea al menos el intervalo de velocidad de bits de audio mínimo. En Cisco Unified Communications Manager, vaya a **Sistema > Información de la región > Región**.

No se puede transferir una llamada de vídeo

Problema

No puedo transferir una llamada de vídeo desde mi teléfono de escritorio a mi dispositivo móvil.

Solución

Cisco Unified Mobility no se amplía a las llamadas de vídeo. No se puede descolgar una llamada de vídeo recibida en el teléfono de escritorio en el teléfono móvil.

Sin vídeo durante una llamada de conferencia

Problema

Una llamada de vídeo pasa a una llamada de audio cuando agrego dos o más personas a la llamada.

Debe usar un puente de conferencia de vídeo para las conferencias de vídeo ad hoc y Meet-Me.

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.
-


Crear un registro de consola desde el teléfono

Puede generar un registro de consola cuando el teléfono no se conecte a la red y no pueda acceder a la herramienta de informe de problemas (PRT).

Antes de empezar


Conecte un cable de la consola al puerto auxiliar de la parte posterior del teléfono.

Procedimiento

- Paso 1** En el teléfono, presione **Aplicaciones** .
 - Paso 2** Vaya a **Configuración de administración > Puerto auxiliar**.
 - Paso 3** Seleccione **Recopilar registro de consola** para recopilar registros de dispositivos.
-

Comprobación de la configuración de TFTP

Procedimiento

- Paso 1** En el teléfono IP de Cisco, pulse **Aplicaciones** , seleccione **Config. admin > Configuración de red > Configuración de Ethernet > Configuración de IPv4 > Servidor TFTP 1**.
- Paso 2** Si ha asignado una dirección IP estática al teléfono, debe introducir manualmente un valor para la opción Servidor TFTP 1.
- Paso 3** 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 4** 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 5** 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 el caso 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:
- Desactive DHCP.
 - Asigne al teléfono los valores de IP estática. Use la misma configuración de router predeterminado que se emplee en otros teléfonos que funcionen.
 - 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

[Restauración básica](#), en la página 279

[Determinación de la dirección MAC del teléfono](#), en la página 72

Comprobación de la configuración de DHCP

Procedimiento

- Paso 1** En el teléfono, presione **Aplicaciones** .
- Paso 2** Seleccione **Wi-Fi > Configuración de red > Configuración de IPv4** y fijese en las opciones siguientes:
- Servidor DHCP: si ha asignado una dirección IP estática al teléfono, debe introducir manualmente 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:
http://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html
 - Dirección IP, Máscara de subred y Router predeterminado: si ha asignado una dirección IP estática al teléfono, debe introducir la configuración manualmente para estas opciones.
- Paso 3** 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:

http://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

[Cisco Unified Communications Manager Documentación](#), en la página xv

[Métodos de adición de teléfonos](#), en la página 73

Identificación de problemas de autenticación 802.1X


Procedimiento

- Paso 1** Compruebe que ha configurado correctamente los componentes necesarios.
- Paso 2** Confirme que el secreto compartido se ha configurado en el teléfono.
- Si el secreto compartido está configurado, verifique que tiene el mismo secreto compartido en el servidor de autenticación.
 - Si el secreto compartido no está configurado en el teléfono, introdúzcalo y asegúrese de que coincide con que está presente en el servidor de autenticación.
-

Verificación de la configuración de DNS

Para verificar la configuración de DNS, lleve a cabo los pasos siguientes:

Procedimiento

- Paso 1** Presione **Aplicaciones** .
- Paso 2** Seleccione **Configuración del administrador > Configuración de red > Configuración de IPv4 > Servidor DNS 1**.
- Paso 3** 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, IU, Red, Medios, Actualizar, Accesorio, Seguridad, Wi-Fi, VPN, EnergyWise, MobileRemoteAccess.

Nota Para implementar la compatibilidad de los parámetros en varios niveles y secciones, marque la casilla de verificación Perfil de registro.

- 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




- Restauración básica, en la página 279
- Restablecimiento de la configuración de red, en la página 281
- Restablecimiento de la configuración de red del usuario, en la página 281
- Eliminación del archivo CTL, en la página 281
- Herramienta de informes de calidad, en la página 282
- Supervisión de la calidad de voz, en la página 282
- Limpieza del teléfono IP de Cisco, en la página 283

Restauración básica

Realizar una restauración básica de un teléfono IP de Cisco ofrece una forma de recuperación en caso de que el teléfono tenga un error. También es un método de restablecer y recuperar diversos ajustes de configuración y seguridad.

En la tabla siguiente se describen las formas de realizar una restauración básica. Puede restaurar un teléfono con cualquiera de estas operaciones después de iniciarlo. Seleccione la operación adecuada a su caso.

Tabla 54: Métodos de restauración básica

Funcionamiento	Acción	Expli
Reiniciar el teléfono	Pulse Aplicaciones  . Vaya a Config. admin > Restaurar configuración > Restaurar dispositivo .	Resta el tele y, a c
Restablecer configuración	Para restaurar la configuración, pulse Aplicaciones  y elija Configuración del administrador > Restaurar configuración > Red .	Es po como
	Para restaurar el archivo CTL, pulse Aplicaciones  y elija Configuración del administrador > Restaurar configuración > Seguridad .	Se re

Restablecimiento de los valores de fábrica del teléfono desde el teclado del teléfono

Es posible restablecer los valores de fábrica del teléfono. El restablecimiento borra todos los parámetros del teléfono.

Procedimiento

Paso 1 Retire la alimentación del teléfono de una de estas formas:

- Desenchufe el adaptador de alimentación.
- Desenchufe el cable de LAN.

Paso 2 Espere 5 segundos.

Paso 3 Pulse y mantenga pulsada la tecla # y vuelva a enchufar el teléfono. Suelte # solo cuando los botones **Auriculares** y **Altavoz** estén iluminados.

Nota En algunas versiones de hardware, el botón **Silenciar** también se ilumina con los botones **Auriculares** y **Altavoz** cuando vuelve a enchufar el teléfono. En ese caso, espere a que se apaguen todos y suelte # solo cuando los botones **Auriculares** y **Altavoz** vuelvan a estar iluminados.

Paso 4 Introduzca la secuencia de teclas siguiente:

123456789*0#

La luz del botón **Auriculares** se apaga después de pulsar la tecla **1**. Después de introducir la secuencia de teclas, el botón **Silencio** se ilumina.


Precaución No apague el teléfono hasta que se complete el proceso de restablecimiento de los valores de fábrica y se muestre la ventana principal.

El teléfono se restablece.

Restablecimiento de toda la configuración desde el menú del teléfono

Realice esta tarea si desea restablecer los valores predeterminados de configuración de usuario y de red.

Procedimiento

Paso 1 Presione **Aplicaciones** .

Paso 2 Seleccione **Configuración del administrador > Restablecer configuración > Toda la configuración**.

Si es necesario, desbloquee las opciones del teléfono.

Reinicio del teléfono desde la imagen de copia de seguridad

Su teléfono IP 8832 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** Desconecte la alimentación.
 - Paso 2** Pulse y mantenga pulsada la tecla asterisco (*).
 - Paso 3** Vuelva a conectar la alimentación. Siga pulsando la tecla asterisco hasta que el LED de silencio se desactive.
 - Paso 4** Suelte la tecla asterisco.
El teléfono se reiniciará desde la imagen de copia de seguridad.
-

Restablecimiento de la configuración de red

Es posible restaurar los valores predeterminados de la configuración de red y restablecer el teléfono. Este método provoca que el protocolo DHCP reconfigure la dirección IP del teléfono.

Procedimiento

- Paso 1** En el menú Configuración del administrador, si se requiere, desbloquee las opciones del teléfono.
 - Paso 2** Seleccione **Restablecer configuración** > **Configuración de red**.
-

Restablecimiento de la configuración de red del usuario

Restaura cualquier cambio de configuración de usuario y de red que haya realizado pero que el teléfono aún no haya guardado en su memoria flash a los valores guardados anteriormente.

Procedimiento

- Paso 1** En el menú Configuración del administrador, si se requiere, desbloquee las opciones del teléfono.
 - Paso 2** Seleccione **Restaurar configuración** > **Restablecer dispositivo**.
-

Eliminación del archivo CTL

Solo se elimina el archivo CTL del teléfono.

Procedimiento

-
- Paso 1** En el menú Configuración del administrador, si se requiere, desbloquee las opciones del teléfono.
- Paso 2** Seleccione **Restablecer configuración > Configuración de seguridad**.
-

Herramienta de informes de calidad

La Herramienta de informes de calidad (QRT) es una herramienta para generar informes de problemas generales y de calidad de la voz para el teléfono IP de Cisco. QRT se incluye en la instalación de Cisco Unified Communications Manager.

Es posible configurar los teléfonos IP de Cisco de los usuarios con QRT. De esta forma, los usuarios pueden informar sobre los problemas con las llamadas telefónicas pulsando Informar de calidad. Esta tecla programada o botón solo está disponible si el teléfono IP de Cisco está en los estados Conectado, Conferencia conectada, Transferencia conectada o Colgado.

Cuando un usuario pulsa Informar de calidad, aparece una lista de categorías de problemas. El usuario selecciona la categoría de problema apropiada y sus comentarios se registran en un archivo XML. La información real que se registra depende de lo que haya seleccionado el usuario y de si el dispositivo de destino es un teléfono IP de Cisco.

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

Temas relacionados

[Cisco Unified Communications Manager Documentación](#), en la página xv

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 55: 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.	<ul style="list-style-type: none"> • 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. <p>Compruebe los contadores de transmisión de paquetes (TxCnt) y recepción de paquetes (RxCnt) para comprobar que los paquetes de voz fluyen.</p>
Las puntuaciones de MOS LQK se reducen de forma significativa.	<p>Problemas de red por pérdida de paquetes o niveles de fluctuación altos:</p> <ul style="list-style-type: none"> • Las reducciones de MOS LQK promedio pueden indicar un problema extendido y uniforme. • Las reducciones MOS LQK individuales pueden indicar problemas por ráfagas. <p>Compruebe al mismo tiempo la proporción de encubrimiento y los segundos de encubrimiento para detectar pruebas de pérdida de paquetes y fluctuación.</p>
Las puntuaciones de MOS LQK aumentan de forma significativa.	<ul style="list-style-type: none"> • 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, en la página 285](#)
- [Asistencia para el registro de llamadas internacionales, en la página 285](#)
- [Limitación de idioma, en la página 286](#)

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 xv

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 (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.

La entrada en chino funciona de forma similar a la de los PC y teléfonos móviles en chino. Para que la entrada en chino funcione, se requiere el instalador de configuración regional para chino.