Guia de administração do Telefone IP Cisco de conferência 8832 para o Cisco Unified Communications Manager

Primeira publicação: 2017-09-15

Última modificação: 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

AS ESPECIFICAÇÕES E INFORMAÇÕES COM RELAÇÃO AOS PRODUTOS DESTE MANUAL ESTÃO SUJEITAS A ALTERAÇÕES SEM PRÉVIO AVISO. TODAS AS DECLARAÇÕES, INFORMAÇÕES E RECOMENDAÇÕES DESTE GUIA SÃO PRECISAS, MAS SÃO APRESENTADAS SEM NENHUM TIPO DE GARANTIA EXPLÍCITA OU IMPLÍCITA. OS USUÁRIOS DEVEM ASSUMIR A RESPONSABILIDADE TOTAL DA APLICAÇÃO DE QUALQUER PRODUTO.

A LICENÇA DE SOFTWARE E A GARANTIA LIMITADA PARA O PRODUTO QUE ACOMPANHA ESTE MANUAL SÃO DEFINIDAS NO PACOTE DE INFORMAÇÕES ENVIADO COM O PRODUTO E SÃO AQUI INCORPORADAS POR ESTA REFERÊNCIA. SE VOCÊ NÃO CONSEGUIR LOCALIZAR A LICENÇA DE SOFTWARE OU A GARANTIA LIMITADA, ENTRE EM CONTATO COM O REPRESENTANTE DA CISCO PARA SOLICITAR UMA CÓPIA.

As seguintes informações são para dispositivos de classe A em conformidade com a FCC: Este equipamento foi testado e atende aos limites de um dispositivo digital Classe A, de acordo com a Parte 15 das regras da FCC (Comissão Federal das Comunicações dos EUA). Esses limites têm o objetivo de proporcionar uma proteção razoável contra interferências prejudiciais ocorridas quando o equipamento é operado em um ambiente comercial. O equipamento gera, utiliza e pode irradiar energia de radiofrequência e, se não for instalado e usado conforme as instruções, podem causar interferência prejudicial às comunicações de rádio. A operação deste equipamento em um ambiente residencial poderá causar interferência prejudicial, caso em que o usuário será obrigado a corrigir a interferência às suas próprias custas.

As seguintes informações são para dispositivos de classe B em conformidade com a FCC: Este equipamento foi testado e atende aos limites de um dispositivo digital Classe B, de acordo com a Parte 15 das regras da FCC (Comissão Federal das Comunicações dos EUA). Esses limites foram estabelecidos para oferecer proteção razoável contra interferência prejudicial em instalações residenciais. Este equipamento gera, utiliza e pode irradiar energia de radiofrequência e, se não for instalado e usado em conformidade com as instruções, pode causar interferência prejudicial às comunicações de rádio. No entanto, não há garantias de que não haverá interferência em uma instalação específica. Se este equipamento causar interferência prejudicial na recepção de rádio ou televisão, o que pode ser identificado ao ligar ou desligar o equipamento, recomenda-se que o usuário tente eliminar a interferência ao adotar uma das seguintes medidas:

- Reorientar ou reposicionar a antena de recepção.
- Aumentar a distância entre o equipamento e o receptor.
- Conectar o equipamento em uma tomada de um circuito diferente daquele no qual o receptor está conectado.
- Consultar o revendedor ou um técnico com experiência em rádio/televisão para obter ajuda.

Modificações a este produto que não tiverem sido autorizadas pela Cisco poderão constituir violação da aprovação da FCC e invalidar a sua autorização para operar o equipamento.

A implementação da compactação de cabeçalho TCP pela Cisco é uma adaptação de um programa desenvolvido pela Universidade da Califórnia, Berkeley (UCB), como parte de uma versão de domínio público da UCB do sistema operacional UNIX. Todos os direitos reservados. Copyright © 1981, Membros da Universidade da Califórnia.

SEM CONTRARIAR NENHUMA OUTRA GARANTIA AQUI DESCRITA, TODOS OS ARQUIVOS DE DOCUMENTOS E SOFTWARE DESSES FORNECEDORES SÃO FORNECIDOS “COMO ESTÃO”, COM TODOS OS SEUS POSSÍVEIS PROBLEMAS. A CISCO E OS FORNECEDORES ACIMA MENCIONADOS SE ISENTAM DE TODAS AS GARANTIAS, EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÃO, AS GARANTIAS DE COMERCIABILIDADE, ADEQUAÇÃO A UM DETERMINADO OBJETIVO E NÃO VIOLAÇÃO OU ORIUNDAS DE UM CURSO DE NEGOCIAÇÃO, USO OU PRÁTICA COMERCIAL.

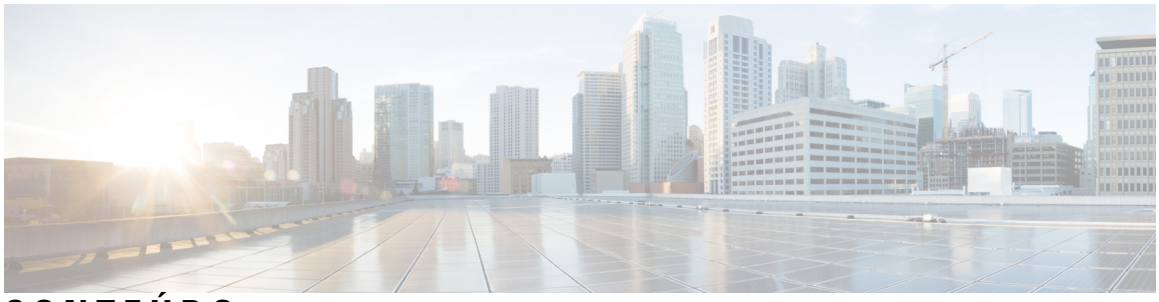
SOB NENHUMA CIRCUNSTÂNCIA A CISCO OU SEUS FORNECEDORES SERÃO RESPONSÁVEIS POR DANOS INDIRETOS, ESPECIAIS, CONSEQUENCIAIS OU INCIDENTAIS, INCLUINDO, MAS NÃO SE LIMITANDO A, PERDA DE LUCROS OU DANOS A DADOS RESULTANTES DO USO OU INCAPACIDADE DE USO DESTE GUIA, MESMO QUE A CISCO OU SEUS FORNECEDORES TENHAM ADVERTIDO SOBRE A POSSIBILIDADE DE TAIS DANOS.

Quaisquer números de telefone e endereços IP (Internet Protocol – Protocolo de Internet) usados neste documento não se destinam a ser endereços e números de telefone reais. Todos os exemplos, saída de exibição de comando, diagramas de topologia de rede e outras figuras incluídas no documento são mostrados apenas para fins ilustrativos. O uso de endereços IP ou números de telefone reais no conteúdo ilustrativo não é intencional e deve ser considerado uma coincidência.

Todas as cópias impressas e as duplicatas digitais deste documento são consideradas cópias sobre as quais não temos controle. Consulte a versão on-line atual para obter a versão mais recente.

A Cisco possui mais de 200 escritórios em todo o mundo. Os endereços, números de telefone e fax estão disponíveis no site www.cisco.com/go/offices.

Cisco e o logotipo da Cisco são marcas comerciais ou registradas da Cisco e/ou de suas afiliadas nos Estados Unidos e em outros países. Para visualizar uma lista de marcas comerciais da Cisco, acesse o URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Todas as marcas de terceiros citadas pertencem a seus respectivos detentores. O uso da palavra "parceiro" não significa um relacionamento de parceria entre a Cisco e qualquer outra empresa. (1721R)



CONTEÚDO

CAPÍTULO 1

Informações novas e alteradas

Informações novas e alteradas da versão de firmware 14.2(1)

As seguintes informações são novas ou alteradas para o firmware versão 14.2(1).

Recurso	Novas ou alteradas
Suporte a SIP OAuth em SRST	Aprimoramentos de segurança para sua rede de telefonia, na página 76

Informações novas e alteradas da versão de firmware 14.1(1)

As informações a seguir são novas ou alteradas para o firmware versão 14.1(1).

Recurso	Novas ou alteradas
Suporte a SIP OAuth para proxy TFTP	Aprimoramentos de segurança para sua rede de telefonia, na página 76
Migração de telefone sem carga de transição	Migração do seu telefone diretamente para um telefone multiplataforma, na página 98

Informações novas e alteradas da versão de firmware 14.0(1)

Tabela 1: Informações novas e alteradas

Recurso	Novas ou alteradas
Melhoria no monitoramento do estacionamento de chamada	Configuração específica do produto, na página 102
Aprimoramentos do SIP OAuth	Aprimoramentos de segurança para sua rede de telefonia, na página 76
Aprimoramentos do OAuth para MRA	Acesso móvel e remoto através do Expressway, na página 123
Aprimoramentos da interface do usuário	SRST (Survivable Remote Site Telephony), na página 66

A partir da versão de firmware 14.0, os telefones suportam DTLS 1.2. O DTLS 1.2 requer o Cisco Adaptive Security Appliance (ASA) versão 9.10 ou posterior. Você configura a versão mínima do DTLS para uma conexão VPN no ASA. Para obter mais informações, consulte o *Livro 3 de ASDM: guia de configuração do Cisco ASA Series VPN ASDM* em https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

Informações novas e alteradas da versão de firmware 12.8(1)

As seguintes informações são novas ou alteradas para o firmware versão 12.8(1).

Recurso	Conteúdo novo ou alterado
Migração de dados do telefone	Alterar o modelo de telefone de um usuário, na página 55
Adicionar informações adicionais sobre o campo de acesso à Web	Configuração específica do produto, na página 102

Informações novas e alteradas da versão de firmware 12.7(1)

Nenhuma atualização do guia de administração foi exigida no Firmware versão 12.7(1).

Informações novas e alteradas da versão de firmware 12.6(1)

Nenhuma atualização do guia de administração foi exigida na versão de firmware 12.6(1).

Informações novas e alteradas da versão de firmware 12.5(1)SR3

Todas as referências à documentação do Cisco Unified Communications Manager foram atualizadas para oferecer suporte a todas as versões do Cisco Unified Communications Manager.

Tabela 2: Revisões do Guia de administração do Telefone IP Cisco 8832 para a versão de firmware 12.5(1)SR3

Revisão	Seção atualizada
Suporte para integração de códigos de ativação e Mobile and Remote Access	Integração de código de ativação e Mobile and Remote Access, na página 31
Suporte para utilização da ferramenta de relatório de problemas a partir do Cisco Unified Communications Manager.	Criar um relatório de problemas de telefone a partir do Cisco Unified Communications Manager, na página 171

Informações novas e alteradas da versão de firmware 12.5(1)SR2

Nenhuma atualização do guia de administração foi necessária na versão de firmware 12.5(1)SR2.

A versão de firmware 12.5(1)SR2 substitui as versões de firmware 12.5(1) e 12.5(1)SR1. As versões de firmware 12.5(1) e 12.5(1)SR1 foram adiadas em favor da versão de firmware 12.5(1)SR2.

Informações novas e alteradas da versão de firmware 12.5(1)SR1

A tabela a seguir inclui as alterações efetuadas ao *Guia de administração do Telefone IP Cisco de conferência 8832 para o Cisco Unified Communications Manager* para suportar a versão de firmware 12.5(1)SR1.

Tabela 3: Revisões do Guia de administração do Telefone IP Cisco de conferência 8832 para o Firmware versão 12.5(1)SR1

Revisão	Seção nova ou atualizada
Suporte para curva elíptica	Recursos de segurança suportados, na página 77

Informações novas e alteradas da versão de firmware 12.5(1)

A tabela a seguir inclui as alterações efetuadas ao *Guia de administração do Telefone IP Cisco de conferência 8832 para o Cisco Unified Communications Manager* para suportar a versão de firmware 12.5(1).

Tabela 4: Revisões do Guia de administração do Telefone IP Cisco de conferência 8832 para a versão de firmware 12.5(1)

Revisão	Seção nova ou atualizada
Suporte para página confidencial sobre o suporte do Cisco Unified Communications Manager Express	Interação com o Cisco Unified Communications Manager Express, na página 23

Revisão	Seção nova ou atualizada
Suporte para desativar codificações de TLS	Configuração específica do produto, na página 102
Suporte para discagem Enbloc para aprimoramento do temporizador entre dígitos T.302.	Configuração específica do produto, na página 102

Informações novas e alteradas da versão de firmware 12.1(1)

A tabela a seguir descreve as alterações do *Guia de administração do telefone do Telefone IP Cisco de conferência 8832 para o Cisco Unified Communications Manager* para suportar o Firmware versão 12.1 (1).

Revisão	Seção nova ou atualizada
Compatível com Injetor PoE do Telefone IP Cisco de conferência 8832	• Requisitos de energia do telefone, na página 18 • Maneiras de fornecer energia para o telefone de conferência, na página 35 • Instalar o telefone de conferência, na página 33
Compatível com microfones sem fio	• Telefone IP Cisco de conferência 8832, na página 9 • Microfone de expansão sem fio (somente 8832), na página 13 • Instalar microfones de expansão sem fio, na página 38 • Instalar o gancho de carregamento do microfone sem fio, na página 39
Compatível com Daisy Chain	• Telefone IP Cisco de conferência 8832, na página 9 • Modo Daisy Chain, na página 33 • Instalar o telefone de conferência no modo Daisy Chain, na página 40 • Um telefone no modo Daisy Chain não funciona, na página 170
Compatível com Telefone IP Cisco de conferência 8832 injetor Ethernet não PoE	• Instalar o telefone de conferência, na página 33 • Maneiras de fornecer energia para o telefone de conferência, na página 35

Revisão	Seção nova ou atualizada
Compatível com Wi-Fi	• Instalar o telefone de conferência, na página 33 • Maneiras de fornecer energia para o telefone de conferência, na página 35 • Definir o campo Nome de domínio, na página 48 • Ativar a LAN sem fio do telefone, na página 48 • Configurar a LAN sem fio no Cisco Unified Communications Manager, na página 49 • Configurar a LAN sem fio usando o telefone, na página 50 • Definir o número de tentativas de autenticação WLAN, na página 51 • Ativar o modo de prompt de WLAN, na página 52 • Configurar um perfil de Wi-Fi usando o Cisco Unified Communications Manager, na página 52 • Definir um grupo de Wi-Fi usando o Cisco Unified Communications Manager, na página 54
Suporte para Mobile and Remote Access através do Expressway	• Acesso móvel e remoto através do Expressway, na página 123 • Cenários de implantação, na página 125 • Configurar credenciais do usuário persistentes para o início de sessão no Expressway, na página 125
Suporte para ativar ou desativar TLS 1.2 para acesso ao servidor Web.	Configuração específica do produto, na página 102
Suporte para codec de áudio G722.2 AMR-WB	• Telefone IP Cisco de conferência 8832, na página 9 • Campos de estatísticas da chamada, na página 142

PARTE I

Sobre o Cisco IP Conference Phone

CAPÍTULO 2

Hardware do Telefone IP Cisco de conferência

Telefone IP Cisco de conferência 8832

O Telefone IP Cisco de conferência 8832 e 8832NR otimizam comunicações centralizadas em pessoas. Ele combina desempenho de áudio de alta definição (HD) e cobertura de 360 graus para salas de conferência de média e grande dimensão e para escritórios executivos. Ele fornece uma experiência sonora digna de um aficionado em sistemas de som de alta qualidade juntamente com um alto-falante de áudio bidirecional full-duplex de banda larga (G.722) que dispensa o uso das mãos. Este telefone é uma solução simples que atende os desafios das mais diversas salas.

Figura 1: Telefone IP Cisco de conferência 8832

O telefone de conferência tem microfones sensíveis com cobertura de 360 graus. Esta cobertura permite que você fale em uma voz normal e seja ouvido claramente a uma distância de até 10 pés (3 m). O telefone também possui tecnologia que resiste à interferência de telefones celulares e outros dispositivos sem fio, o que garante

o suprimento de comunicações claras sem distrações. O telefone possui uma tela a cores e teclas programáveis para acessar as funções do usuário. Com a unidade base isolada, o telefone fornece cobertura para uma sala de 20 x 20 pés (6,1 x 6,1 m) e até 10 pessoas.

Dois microfones de expansão com fio estão disponíveis para uso com o telefone. Colocar os microfones de expansão afastados da unidade base otimiza a cobertura em salas de conferência maiores. Com a unidade base e microfones de expansão com fio, o telefone de conferência fornece cobertura para uma sala de 20 x 34 pés (6,1 x 10 m) e até 22 pessoas.

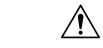
O telefone também é compatível com um conjunto opcional de dois microfones de expansão com fio. Com a unidade base e microfones de expansão sem fio, o telefone de conferência fornece cobertura para uma sala de 20 x 40 pés (6,1 x 12,2 m) e até 26 pessoas. Para cobrir uma sala de 20 x 40 pés (6,1 x 12,2 m), recomendamos que você coloque cada microfone a uma distância máxima de 10 pés (3 m) da base.

Você pode conectar duas unidades base para aumentar a cobertura para uma sala. Esta configuração requer o kit de Daisy Chain opcional e pode oferecer suporte a dois microfones de expansão (com fio ou sem fio, mas não uma combinação mista). Se você estiver usando microfones com fio com o kit de Daisy Chain, a configuração fornece cobertura para uma sala de até 6,1 x 15,2 m (20 x 50 pés) e com um máximo de 38 pessoas. Se você estiver usando microfones sem fio com o kit de Daisy Chain, a configuração fornece cobertura para uma sala de até 6,1 x 17,4 m (20 x 57 pés) e com um máximo de 42 pessoas.

A versão (não rádio) do Telefone IP Cisco de conferência 8832NR não é compatível com Wi-Fi, com microfones de expansão sem fio ou Bluetooth.

Como outros dispositivos, um Telefone IP Cisco deve ser configurado e gerenciado. Esses telefones codificam e descodificam os seguintes codecs:

- G.711 a-law
- G.711 mu-law
- G.722
- G722.2 AMR-WB
- G.729a/G.729ab
- G.726
- iLBC
- Opus



Cuidado Usar um telefone celular, móvel ou GSM, ou um rádio bidirecional em estreita proximidade a um Telefone IP Cisco pode causar interferência. Para obter mais informações, consulte a documentação do fabricante do dispositivo que interfere.

Os Telefones IP Cisco oferecem funcionalidade de telefonia tradicional, como encaminhamento e transferência de chamadas, rediscagem, discagem rápida, chamada de conferência e acesso ao sistema de mensagens de voz. Os Telefones IP Cisco também fornecem uma variedade de outros recursos.

Assim como em outros dispositivos de rede, você deve configurar os Telefones IP Cisco de modo a prepará-los para acessar o Cisco Unified Communications Manager e o restante da rede IP. Ao usar DHCP, você tem menos configurações para definir em um telefone. No entanto, se sua rede exigi-lo, você poderá configurar manualmente informações como: endereço IP, servidor TFTP e informações de sub-rede.

Os Telefones IP Cisco podem interagir com outros serviços e dispositivos na sua rede IP para fornecer funcionalidade aprimorada. Por exemplo, é possível integrar o Cisco Unified Communications Manager ao diretório padrão LDAP3 corporativo a fim de permitir que os usuários pesquisem informações de contato de colegas de trabalho diretamente em seus telefones IP. Você também pode usar XML para permitir que os usuários acessem informações como previsão do tempo, bolsa de valores, citação do dia e outras informações baseadas na Web.

Por fim, como o Telefone IP Cisco é um dispositivo de rede, é possível obter informações detalhadas de status diretamente dele. Essas informações podem ajudar na solução de problemas que os usuários podem encontrar ao usar os respectivos telefones IP. Você também pode obter estatísticas sobre uma chamada ativa ou versões de firmware no telefone.

Para funcionar na rede de telefonia IP, o Telefone IP Cisco deve ser conectado a um dispositivo de rede, como o switch do Cisco Catalyst. Você também deve registrar o Telefone IP Cisco em um sistema Cisco Unified Communications Manager antes de enviar e receber chamadas.

Hardware e botões do Telefone IP Cisco de conferência 8832

A figura a seguir mostra o Telefone IP Cisco de conferência 8832.

Figura 2: Recursos e teclas do Telefone IP Cisco de conferência 8832

A tabela a seguir descreve os botões do Telefone IP Cisco de conferência 8832.

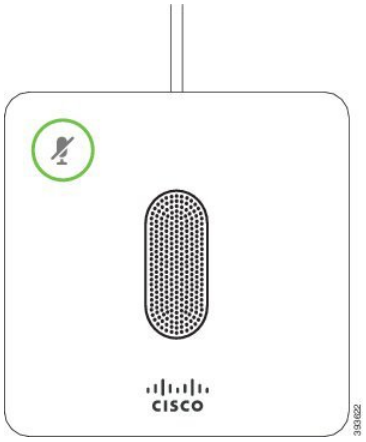
Tabela 5: Botões do Telefone IP Cisco de conferência 8832

1	Barra de LED	Indica estados de chamada: • Verde, aceso — Chamada ativa • Verde, intermitente — Chamada recebida • Verde, pulsando — Chamada em espera • Vermelho, aceso — Chamada com som desativado
2	Porta do microfone de expansão	O cabo do microfone de expansão com fio é conectado à porta.
3	Barra **Silenciar**	Liga e desliga o microfone. Quando silenciar o microfone, a barra de LED acende em vermelho.
4	Botões de função	Acesse funções e serviços.
5	Barra de navegação e botão **Selecionar**	 Navegue pelos menus, realce itens e selecione o item realçado.
6	Tecla **Volume**	 Ajusta o volume do alto-falante (fora do gancho) e o volume do toque (no gancho). Quando você altera o volume, a barra de LED fica branca para mostrar a alteração de volume.

Microfone de expansão com fio (somente 8832)

O Telefone IP Cisco de conferência 8832 suporta dois microfones de expansão com fio, disponíveis em um kit opcional. Use os microfones de expansão em salas maiores ou em um uma sala muito cheia. Para obter melhores resultados, recomendamos que coloque os microfones entre 0,91 m e 2,1 m de distância do telefone.

Figura 3: Microfone de expansão com fio



Quando você está em uma chamada, o LED do microfone de expansão ao redor do botão **Silenciar** fica verde.

Quando o microfone é silenciado, o LED fica verde. Quando você pressiona o botão **Silenciar**, o telefone e os microfones de expansão são silenciados.

Tópicos relacionados

Instalar microfones de expansão com fio, na página 37

Microfone de expansão sem fio (somente 8832)

O Telefone IP Cisco de conferência 8832 suporta dois microfones de expansão sem fio, disponíveis com um gancho de carregamento em um kit opcional. Quando o microfone sem fio for colocado no gancho de carregamento para carregamento, o LED no gancho acende com uma luz branca.

Figura 4: Microfone sem fio

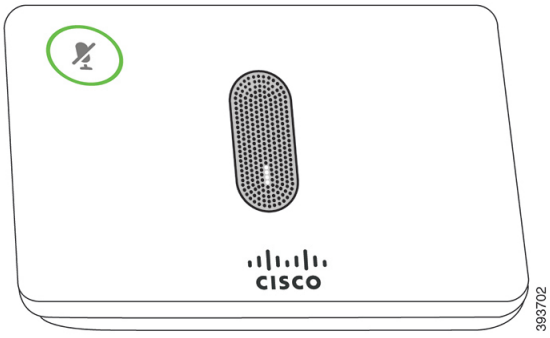
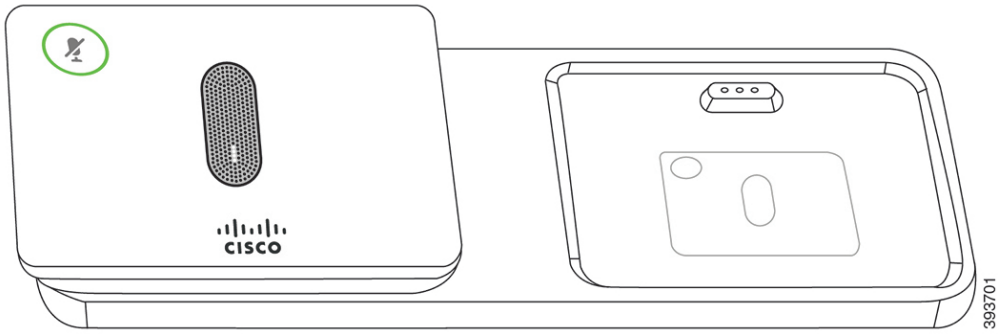


Figura 5: Microfone sem fio montado no gancho de carregamento



Quando o telefone de conferência está em uma chamada, o LED do microfone de expansão ao redor do botão **Silenciar** fica aceso em verde.

Quando o microfone está com o som desativado, o LED fica aceso em vermelho. Quando você pressiona o botão **Silenciar**, o telefone e os microfones de expansão são silenciados.

Se o telefone está emparelhado com um microfone sem fio (por exemplo, microfone sem fio 1) e você conectar o microfone sem fio a um carregador, pressionar a tecla programável **Mostrar detalhes** indica o nível de carregamento para esse microfone.

Quando o telefone está emparelhado com um microfone sem fio e você conectar um microfone com fio, o microfone sem fio é desemparelhado e o telefone é emparelhado com o microfone com fio. Uma notificação será exibida na tela do telefone indicando se o microfone com fio está conectado.

Tópicos relacionados

Instalar microfones de expansão sem fio, na página 38
Instalar o gancho de carregamento do microfone sem fio, na página 39

Documentação relacionada

Use as seções a seguir para obter informações relacionadas.

Documentação do Telefone IP Cisco de conferência 8832

Localize a documentação específica do seu idioma, modelo de telefone e sistema de controle de chamadas na página de suporte ao produto do Cisco IP Phone 7800 series.

Documentação do Cisco Unified Communications Manager

Consulte o *Guia de documentação do Cisco Unified Communications Manager* e outras publicações que são específicas de sua versão do Cisco Unified Communications Manager. Navegue até o seguinte URL de documentação:

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

Documentação do Cisco Unified Communications Manager Express

Consulte as publicações que são específicas ao seu idioma, modelo do telefone e versão do Cisco Unified Communications Manager Express. Navegue até o seguinte URL de documentação:

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

Documentação do Cisco Hosted Collaboration Service

Consulte o *Guia de documentação do Cisco Hosted Collaboration Solution* e outras publicações que são específicas de sua versão do Cisco Hosted Collaboration Solution. Navegue no seguinte URL:

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

Documentação do Cisco Business Edition 4000

Consulte o *Guia de documentação do Cisco Business Edition 4000* e outras publicações que são específicas de sua versão do Cisco Business Edition 4000. Navegue no seguinte URL:

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

Documentação, suporte e instruções de segurança

Para obter informações sobre como obter documentação, obter suporte, fornecer feedback sobre a documentação, revisar instruções de segurança e também recomendar aliases e documentos gerais da Cisco, consulte *What's New in Cisco Product Documentation* mensalmente, que também relaciona toda a documentação técnica nova e revisada da Cisco, em:

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

Assine o feed RSS do *What's New in Cisco Product Documentation* e defina o conteúdo a ser entregue diretamente no seu desktop usando um aplicativo de leitura. Os feeds RSS são um serviço gratuito e a Cisco também trabalha no momento com RSS versão 2.0.

Visão geral da segurança dos produtos Cisco

Este produto contém funções criptografadas e está sujeito às leis locais e dos EUA que regulamentam a importação, exportação, transferência e utilização. O fornecimento de produtos criptografados pela Cisco não implica que terceiros tenham autoridade para importar, exportar, distribuir ou utilizar criptografia. Importadores, exportadores, distribuidores e usuários são responsáveis pelo cumprimento das leis americanas e locais. Ao utilizar este produto, você concorda em cumprir as leis e regulamentações aplicáveis. Se não for possível cumprir as leis dos Estados Unidos e locais, devolva este produto imediatamente.

Mais informações sobre as regulamentações de exportação dos EUA podem ser encontradas em https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear.

Diferenças de terminologia

Neste documento, o termo *Telefone IP Cisco* inclui o Telefone IP Cisco de conferência 8832.

A tabela a seguir destaca algumas diferenças de terminologia entre o *Guia do usuário do Telefone IP Cisco de conferência 8832*, o *Guia de administração do Telefone IP Cisco de conferência 8832 para Cisco Unified Communications Manager* e a documentação do Cisco Unified Communications Manager.

Tabela 6: Diferenças de terminologia

Manual do usuário	Guia de administração
Indicadores de mensagens	Indicador de mensagem em espera (MWI)
Sistema de correio de voz	Sistema de mensagens de voz

CAPÍTULO 3

Detalhes técnicos

Especificações físicas e do ambiente operacional

A tabela a seguir mostra as especificações físicas e do ambiente operacional do telefone de conferência.

Tabela 7: Especificações físicas e operacionais

Especificação	Valor ou intervalo
Temperatura de operação	0° a 40°C
Umidade relativa de operação	De 10% a 90% (sem condensação)
Temperatura de armazenamento	14° a 140°F (–10° a 60°C)
Altura	278 mm (10,9 pol.)
Largura	278 mm (10,9 pol.)
Profundidade	61,3 mm (2,4 pol.)
Peso	1852 g (4,07 lb)
Energia	IEEE PoE Classe 3 por meio de um injetor PoE. O telefone é comp Discovery Protocol e o Link Layer Discovery Protocol – Power ov Outras opções incluem um injetor Ethernet não PoE, se os switche necessário um adaptador de energia do Telefone IP Cisco de confe

Especificação	Valor ou intervalo
Funções de segurança	Inicialização segura
Cabos	USB-C
Requisitos de distância	A especificação Ethernet pressupõe que o comprimento máximo do ca

Para obter mais informações, consulte *Folha de dados do Telefone IP Cisco de conferência 8832*: https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/datasheet-listing.html

Requisitos de energia do telefone

O Telefone IP Cisco de conferência 8832 pode usar as seguintes fontes de alimentação:

- Implantação Power over Ethernet (PoE) com um Injetor PoE do Telefone IP Cisco de conferência 8832
- Implantação não PoE Ethernet deployment com um Telefone IP Cisco de conferência 8832 injetor Ethernet não PoE
- Implantação Wi-Fi com um adaptador de energia do Telefone IP Cisco de conferência 8832

Tabela 8: Diretrizes de alimentação do Telefone IP Cisco de conferência

Tipo de alimentação	Diretrizes
Alimentação PoE — Fornecida pelo Injetor PoE do Telefone IP Cisco de conferência 8832 ou Injetor de Ethernet do Telefone IP Cisco de conferência 8832 por meio do cabo USB-C conectado ao telefone.	Se você estiver usando o Injetor PoE do Telefone IP Cisco de conferência 8832 ou Injetor de Ethernet do Telefone IP Cisco de conferência 8832, verifique se o switch tem uma fonte de alimentação de backup para garantir uma operação ininterrupta do telefone. Verifique se a versão CatOS ou IOS que é executada em seu switch aceita a implantação do telefone pretendido. Consulte a documentação do seu switch para obter informações de versão do sistema operacional. Quando você instalar um telefone que é alimentado por PoE, conecte o injetor à LAN antes de conectar o cabo USB-C ao telefone. Quando você remover um telefone que usa PoE, desconecte o cabo USB-C do telefone antes de desconectar o adaptador da alimentação.

Tipo de alimentação	Diretrizes
Alimentação externa • Implantação não PoE Ethernet deployment com um Telefone IP Cisco de conferência 8832 injetor Ethernet não PoE • Implantação Wi-Fi com um adaptador de energia do Telefone IP Cisco de conferência 8832 • Implantação não PoE com um Injetor de Ethernet do Telefone IP Cisco de conferência 8832 e um adaptador de energia do Telefone IP Cisco de conferência 8832	Quando você instala um telefone que é alimentado externamente, conecte o injetor à energia elétrica e à Ethernet antes de conectar o cabo USB-C ao telefone. Quando você remover um telefone que é alimentado externamente, desconecte o cabo USB-C do telefone antes de desconectar o adaptador da alimentação.

Interrupção de energia

O seu acesso aos serviços de emergência através do telefone requer que o telefone receba energia. Se ocorrer uma interrupção da energia, o serviço ou a discagem para o serviço de chamadas de emergência não funcionará até a energia ser restaurada. Se ocorrer uma falha ou interrupção da energia, talvez seja necessário redefinir ou reconfigurar o equipamento antes de poder usar o serviço ou a discagem para o serviço de chamadas de emergência.

Redução do consumo de energia

Você pode reduzir a quantidade de energia que o Telefone IP Cisco consome usando o modo Economia de energia ou EnergyWise (Economia de energia Plus).

Economia de energia

No modo Economia de energia, a luz de fundo na tela não acende quando o telefone não está em uso. O telefone permanece no modo Economia de energia pelo tempo programado ou até que o usuário pressione algum botão.

Economia de energia Plus (EnergyWise)

O Telefone IP Cisco é compatível com o modo Cisco EnergyWise (Economia de energia Plus). Quando sua rede contém um controlador EW (EnergyWise) (por exemplo, um switch Cisco com o recurso EnergyWise ativado), você pode configurar esses telefones para repousar (desligar) e despertar (ligar) de acordo com uma programação para reduzir ainda mais o consumo de energia.

Configure cada telefone para ativar ou desativar as configurações de EnergyWise. Se o EnergyWise for ativado, configure uma hora de repouso e despertar, bem como outros parâmetros. Esses parâmetros são enviados ao telefone como parte do arquivo XML da configuração do telefone.

Tópicos relacionados

Agendar economia de energia para o Telefone IP Cisco, na página 115
Programar EnergyWise no Telefone IP Cisco, na página 116

Protocolos de rede

O Telefone IP Cisco de conferência 8832 é compatível com vários protocolos de rede Cisco e padrão do setor que são exigidos na comunicação por voz. A tabela a seguir fornece uma visão geral dos protocolos de rede que são compatíveis com os telefones.

Tabela 9: Protocolos de rede compatíveis com o Telefone IP Cisco de conferência

Protocolo de rede	Objetivo	Notas de uso
BootP (Protocolo Bootstrap)	O BootP permite que um dispositivo de rede, como o telefone, descubra determinadas informações de inicialização, como o endereço IP.	—
CDP (Cisco Discovery Protocol)	O CDP é um protocolo de descoberta de dispositivo que é executado em todos os equipamentos fabricados pela Cisco. Um dispositivo pode usar o CDP para anunciar sua existência para outros dispositivos e receber informações sobre outros dispositivos na rede.	O telefone usa o CDP para comunicar informações, de energia, e informações de configuração de QoS (
Protocolo de Configuração Dinâmica de Host (DHCP)	O DHCP aloca e atribui dinamicamente um endereço IP aos dispositivos de rede. O DHCP permite conectar um telefone IP na rede e fazer com que ele funcione sem a necessidade de atribuir manualmente um endereço IP ou configurar parâmetros de rede adicionais.	O DHCP é ativado por padrão. Se desativado, você d e um servidor TFTP em cada telefone localmente. É recomendável usar a opção 150 personalizada do como o valor de opção. Para obter mais configuraçõ do Cisco Unified Communications Manager. **Observação** Se não for possível usar a opção 150, u
Protocolo HTTP	O HTTP é o protocolo padrão para transferência de informações e movimentação de documentos pela Internet e Web.	Os telefones usam o HTTP para serviços XML, pro
HTTPS (Secure Hypertext Transfer Protocol - Protocolo de Transferência de Hipertexto Seguro)	O protocolo HTTPS (Hypertext Transfer Protocol Secure) é uma combinação dos protocolos HTTP com SSL/TLS para fornecer criptografia e identificação segura de servidores.	Aplicativos da Web com suporte a HTTP e HTTPS tê o URL HTTPS. Um ícone de cadeado será exibido ao usuário se a c
IEEE 802.1x	O padrão IEEE 802.1X define um controle de acesso baseado em cliente-servidor e o protocolo de autenticação que restringe a conexão com uma LAN por meio de portas que podem ser acessadas publicamente por clientes não autorizados. Até que o cliente seja autenticado, o controle de acesso 802.1X permite apenas o tráfego do protocolo EAPOL por LAN por meio da porta à qual o cliente está conectado. Depois da autenticação bem-sucedida, o tráfego normal pode passar pela porta.	O telefone implementa o padrão IEEE 802.1X por m EAP-TLS. Quando a autenticação 802.1X é ativada no telefone

Protocolo de rede	Objetivo	Notas de uso
Protocolo IP	IP é um protocolo de troca de mensagens que envia pacotes pela rede.	Para se comunicar com IP, os dispositivos de rec As identificações de endereços IP, sub-redes e g o protocolo DHCP. Se não estiver usando DHCP, Os telefones são compatíveis com o endereço IPv do Cisco Unified Communications Manager.
LLDP (Link Layer Discovery Protocol)	O LLDP é um protocolo de descoberta de rede padronizado (semelhante ao CDP) que é compatível com alguns dispositivos Cisco e de terceiros.	O telefone é compatível com o LLDP na porta d
LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Devices)	O LLDP-MED é uma extensão do padrão LLDP desenvolvido para produtos de voz.	O telefone é compatível com o LLDP-MED na p • Configuração da VLAN de voz • Descoberta de dispositivo • Gerenciamento de energia • Gerenciamento de estoque Para obter mais informações sobre o suporte ao *Protocol* nesse URL: https://www.cisco.com/en/US/tech/tk652/tk701/
Real-Time Transport Protocol (RTP)	O RTP é um protocolo padrão para transporte de dados em tempo real, como voz e vídeo interativos por redes de dados.	Os telefones usam o protocolo RTP para enviar
RTCP (Real-Time Control Protocol)	O RTCP trabalha em conjunto com o RTP para fornecer dados de QoS (como instabilidade, latência e atraso na resposta) em fluxos RTP.	O RTCP é ativado por padrão.
Protocolo SDP	O SDP é a parte do protocolo SIP que determina quais parâmetros estão disponíveis durante uma conexão entre dois dispositivos. Conferências são estabelecidas usando apenas os recursos do SDP aos quais todos os dispositivos da conferência oferecem suporte.	Os recursos do SDP, como tipos de codec, detec pelo Cisco Unified Communications Manager ou a configuração desses parâmetros no próprio dis
SIP (Session Initiation Protocol)	O protocolo SIP é o padrão IETF (Internet Engineering Task Force) para conferência de multimídia por IP. O SIP é um protocolo de controle na camada de aplicativo baseado em ASCII (definido no RFC 3261) que pode ser usado para estabelecer, manter e encerrar chamadas entre dois ou mais dispositivos.	Como outros protocolos VoIP, o SIP é designado de telefonia de pacote. A sinalização permite que de sessão permite controlar os atributos de uma
Protocolo SRTP (Secure Real-Time Transfer)	O SRTP é uma extensão do Perfil de áudio/vídeo RTP (Real-Time Protocol) e garante a integridade dos pacotes de RTP e RTCP (Real-Time Control Protocol) fornecendo autenticação, integridade e criptografia de pacotes de mídia entre dois dispositivos.	Os telefones usam SRTP para criptografia de mí
Protocolo TCP	O TCP é um protocolo de transporte orientado por conexão.	Os telefones usam o TCP para se conectar ao Ci

Protocolo de rede	Objetivo	Notas de uso
Segurança da camada de transporte (TLS)	O TLS é um protocolo padrão para proteger e autenticar comunicações.	Quando a segurança é implementada, os telefones u Communications Manager. Para obter mais informa Communications Manager.
Protocolo de Transferência Trivial de Arquivo (TFTP)	O TFTP permite transferir arquivos pela rede. No telefone, o TFTP permite obter um arquivo de configuração específico ao tipo de telefone.	O TFTP exige um servidor TFTP na sua rede, que p telefone use um servidor TFTP diferente do especif do servidor TFTP usando o menu Configuração da Para obter mais informações, consulte a documenta
Protocolo UDP (User Datagram Protocol)	O UDP é um protocolo de troca de mensagens sem conexão para entrega de pacotes de dados.	O UDP é usado somente para fluxos RTP. A sinaliz

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

Interação com o Cisco Unified Communications Manager

O Cisco Unified Communications Manager é um sistema aberto de processamento de chamadas padrão do setor. O software Cisco Unified Communications Manager configura e derruba ligações entre telefones, integrando a funcionalidade PBX tradicional à rede IP corporativa. O Cisco Unified Communications Manager gerencia os componentes do sistema de telefonia, como os telefones, os gateways de acesso e os itens necessários para recursos como conferência de chamada e planejamento de rota. O Cisco Unified Communications Manager também fornece:

- Firmware para telefones
- Arquivos CTL (Lista de certificados confiáveis) e ITL (Lista de confiança de identidade) usando os serviços TFTP e HTTP
- Registro de telefone
- Preservação de chamada, para que uma sessão de mídia continue se a sinalização for perdida entre o Communications Manager primário e o telefone.

Para obter informações sobre como configurar o Cisco Unified Communications Manager para trabalhar com os telefones descritos neste capítulo, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Observação Se o modelo do telefone que você deseja configurar não aparecer na lista suspensa Tipo de telefone na Administração do Cisco Unified Communications Manager, instale o pacote de dispositivo mais recente para sua versão do Cisco Unified Communications Manager de Cisco.com.

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

Interação com o Cisco Unified Communications Manager Express

Quando o telefone trabalha com o Cisco Unified Communications Manager Express (Unified CME), ele deve entrar no modo CME.

Quando um usuário chama o recurso de conferência, a marca permite que o telefone use um recurso de conferência de hardware de rede ou local.

Os telefones não oferecem suporte às seguintes ações:

- Transferir — permitida somente no cenário de transferência de chamadas conectadas.
- Conferência — permitida somente no cenário de transferência de chamadas conectadas.
- Unir — permitida usando o botão Conferência ou o acesso ao Hookflash.
- Espera — permitida usando o botão Espera.
- Intercalar e mesclar — não suportado.
- Transferência direta — não suportado.
- Selecionar — não suportado.

Os usuários não podem criar chamadas de conferência e transferência entre diferentes linhas.

O Unified CME suporta chamadas de intercomunicador, também conhecidas como paginação confidencial. Mas, a página será rejeitada pelo telefone durante as chamadas.

Interação com o sistema de mensagens de voz

O Cisco Unified Communications Manager permite que você faça a integração com diferentes sistemas de mensagens de voz, incluindo o sistema de mensagens de voz Cisco Unity Connection. Como você pode fazer a integração com vários sistemas, é preciso fornecer aos usuários informações sobre como usar seu sistema específico.

Para habilitar a capacidade de um usuário transferir para correio de voz, é preciso configurar um padrão de discagem *xxxxx e configurá-lo como Encaminhar todas as chamadas para Correio de voz. Para obter mais informações, consulte a documentação do Cisco Unified Communications Manager.

Forneça as seguintes informações para cada usuário:

- Como acessar a conta do sistema de mensagens de voz.

  Certifique-se de que você tenha usado o Cisco Unified Communications Manager para configurar o botão Mensagens no Telefone IP Cisco.

- Senha inicial para acessar o sistema de mensagens de voz.

  Configure uma senha padrão para o sistema de mensagens de voz para todos os usuários.

- Como o telefone indica que há mensagens de voz em espera.

Use o Cisco Unified Communications Manager para configurar um método de indicador de mensagem em espera (MWI).

Arquivos de configuração do telefone

Os arquivos de configuração para um telefone são armazenados no servidor TFTP e definem parâmetros de conexão ao Cisco Unified Communications Manager. Em geral, sempre que você fizer uma alteração no Cisco Unified Communications Manager que exija a redefinição do telefone, uma alteração será feita automaticamente no arquivo de configuração do telefone.

Os arquivos de configuração também contêm informações sobre qual carregamento de imagem o telefone está executando. Se esse carregamento de imagem for diferente daquele atualmente carregado em um telefone, o telefone contatará o servidor TFTP para solicitar os arquivos de carregamento necessários.

Se você definir configurações relacionadas à segurança no Administração do Cisco Unified Communications Manager, o arquivo de configuração do telefone conterá informações confidenciais. Para garantir a privacidade de um arquivo de configuração, você deve configurá-lo para criptografia. Para obter mais informações, consulte a documentação da sua versão específica do Cisco Unified Communications Manager. Um telefone solicita um arquivo de configuração sempre que é redefinido e registrado com o Cisco Unified Communications Manager.

Um telefone acessa um arquivo de configuração padrão denominado XmlDefault.cnf.xml do servidor TFTP quando as seguintes condições são verdadeiras:

- Você ativou o registro automático no Cisco Unified Communications Manager
- O telefone não foi adicionado ao banco de dados do Cisco Unified Communications Manager
- O telefone está se registrando pela primeira vez

Comportamento do telefone em momentos de congestionamento da rede

Qualquer coisa que prejudique o desempenho da rede pode afetar o áudio do telefone e, em alguns casos, pode fazer com que uma chamada caia. As fontes de degradação da rede podem incluir, mas não se limitam, às atividades a seguir:

- Tarefas administrativas, como verificação de porta interna ou verificação de segurança.
- Ataques que ocorrem na rede, como o Ataque de negação de serviço.

Application Programming Interface, interface de programação de aplicativos

A Cisco suporta a utilização da API do telefone por aplicativos de terceiros que foram testados e certificados pela Cisco pelo desenvolvedor de aplicativos de terceiros. Os problemas de telefone relacionados à interação de aplicativos não certificado devem ser tratados pelo terceiro e não serão tratados pela Cisco.

Para obter suporte do modelo de aplicativos/soluções de terceiros certificados pela Cisco, consulte o site do Cisco Solution Partner Program para obter detalhes.

PARTE II

Instalação do Telefone IP Cisco de conferência

CAPÍTULO 4

Instalação do telefone

Verificar configuração da rede

Ao implantarem um novo sistema de telefonia IP, os administradores de sistemas e de redes devem executar várias tarefas de configuração inicial para preparar a rede para o serviço de telefonia IP. Para obter informações e uma lista de verificação para instalar e configurar uma rede de telefonia IP da Cisco, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Para que o telefone funcione corretamente como um dispositivo em sua rede, ela deve atender a requisitos específicos. Um requisito é a largura de banda apropriada. Os telefones exigem mais largura de banda do que os 32 kbps recomendados quando eles são registrados no Cisco Unified Communications Manager. Quando você configurar sua largura de banda QoS, considere este requisito de largura de banda maior. Para obter mais informações, consulte *Designs de rede de referência da solução (SRND) do Cisco Collaboration System 12.x* ou posterior (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.html).

Observação O telefone exibe a data e a hora de Cisco Unified Communications Manager. A hora exibida no telefone pode diferir da hora do Cisco Unified Communications Manager em até 10 segundos.

Procedimento

Etapa 1 Configure uma Rede VoIP para atender aos seguintes requisitos:

- O VoIP está configurado em seus roteadores e gateways.
- Cisco Unified Communications Manager está instalado em sua rede e está configurado para tratar do processamento de chamadas.

Etapa 2 Configure a rede para suportar um dos seguintes:

- DHCP
- Atribuição manual de endereço IP, gateway e máscara de sub-rede

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

Integração de código de ativação para os telefones no local

Você pode usar a integração de código de ativação para configurar rapidamente a novos telefones sem registro automático. Com essa abordagem, é possível controlar o processo de integração de telefone usando um dos seguintes:

- Bulk Administration Tool (BAT) do Cisco Unified Communications Manager
- Interface de administração do Cisco Unified Communications Manager
- Serviço Web XML administrativo (AXL)

Ative esse recurso a partir da seção **Informações do dispositivo** da página de configuração do telefone. Selecione **Necessário código de ativação para integração** se deseja que esse recurso se aplique a um telefone único no local.

Os usuários devem inserir um código de ativação para que seus telefones possam se registrar. A integração de código de ativação pode ser aplicada a telefones individuais, a um grupo de telefones ou em toda a rede.

Isso é uma forma fácil para usuários integrarem seus telefones, porque eles somente digitam um código de ativação de 16 dígitos. Os códigos são inseridos manualmente ou com um código QR, se um telefone tiver uma câmera de vídeo. Recomendamos que você use um método seguro para fornecer essas informações aos usuários. Mas se um usuário estiver atribuído a um telefone, essa informação estará disponível no Portal de ajuda. Os registros de log de auditoria quando um usuário acessa o código do portal.

Os códigos de ativação podem ser usados apenas uma vez e eles expirarem após 1 semana por padrão. Se um código expirar, você terá que fornecer um novo ao usuário.

Você descobrirá que essa abordagem é uma forma fácil de manter sua rede segura, porque um telefone não pode ser registrado até que o Certificado de instalação de origem (MIC) e o código de ativação sejam verificados. Esse método também é uma maneira conveniente de integrar telefones em massa, porque ele não usa a Ferramenta de suporte para telefones registrados automaticamente (TAPS) ou o registro automático. A taxa de integração é um telefone por segundo ou aproximadamente 3600 telefones por hora. Os telefones podem ser adicionados com a Administração do Cisco Unified Communications Manager, com o Serviço Web XML administrativo (AXL) ou com a BAT.

Os telefones existentes são redefinidos após serem configurados para integração de código de ativação. Eles não são registrados até que o código de ativação seja inserido e o MIC do telefone verificado. Informe os usuários atuais que se está movendo para a integração de código de ativação antes de você implementá-lo.

Para obter mais informações, consulte o *Guia de administração do Cisco Unified Communications Manager e serviço de IM e Presença, versão 12.0(1)* ou posterior.

Integração de código de ativação e Mobile and Remote Access

Você pode usar a integração de código de ativação com Mobile and Remote Access ao implantar os Telefones IP Cisco para usuários remotos. Esse recurso é uma maneira segura de implantar telefones remotos quando o registro automático não é necessário. Mas você pode configurar um telefone para registro automático quando estiver no local e códigos de ativação quando estiver fora do local. Esse recurso é semelhante a integração de código de ativação para telefones no local, mas torna o código de ativação disponível também para telefones remotos.

A integração de código de ativação para Mobile and Remote Access requer o Cisco Unified Communications Manager 12.5(1)SU1 ou posterior e o Cisco Expressway X12.5 ou posterior. O licenciamento inteligente também deve ser ativado.

Você ativa este recurso na administração do Cisco Unified Communications Manager, mas observe o seguinte:

- Ative esse recurso a partir da seção **Informações do dispositivo** da página de configuração do telefone.
- Selecione **Necessário código de ativação para integração** se deseja que esse recurso se aplique a um telefone único no local.
- Selecione **Permitir código de ativação via MRA** e **Necessário código de ativação para integração** se desejar usar a integração de ativação para um único telefone remoto. Se o telefone estiver no local, ele muda para o modo de Mobile and Remote Access e usa o Expressway. Se o telefone não conseguir acessar o Expressway, ele somente será registrado quando ficar fora do local.

Para obter mais informações, consulte os seguintes documentos:

- *Guia de administração do Cisco Unified Communications Manager e serviço de IM e Presença, versão 12.0(1)*
- *Mobile and Remote Access através do Cisco Expressway* para Cisco Expressway X12.5 ou posterior

Ativar o registro automático de telefones

O Telefone IP Cisco exige o Cisco Unified Communications Manager para lidar com o processamento de chamadas. Consulte a documentação da sua versão específica do Cisco Unified Communications Manager ou a ajuda contextual na Administração do Cisco Unified Communications Manager a fim de garantir que o Cisco Unified Communications Manager esteja configurado corretamente para gerenciar o telefone, bem como rotear e processar as chamadas corretamente.

Antes de instalar o Telefone IP Cisco, você deve escolher um método para adicionar telefones ao banco de dados do Cisco Unified Communications Manager.

Ao ativar o registro automático antes de instalar os telefones, você pode:

- Adicionar telefones sem antes coletar os endereços MAC dos telefones.
- Adicionar automaticamente um Telefone IP Cisco ao banco de dados do Cisco Unified Communications Manager quando você conecta fisicamente o telefone à sua rede de telefonia IP. Durante o registro

automático, o Cisco Unified Communications Manager atribui o próximo número de diretório sequencial disponível ao telefone.

- Inserir rapidamente telefones no banco de dados do Cisco Unified Communications Manager e modificar todas as configurações, como os números de diretório, no Cisco Unified Communications Manager.
- Mover telefones registrados automaticamente para novos locais e atribuí-los a diferentes pools de dispositivos sem afetar os respectivos números de diretório.

O registro automático está desativado por padrão. Em alguns casos, talvez você não queira usar o registro automático; por exemplo, se desejar atribuir um número de diretório específico ao telefone ou usar uma conexão segura com o Cisco Unified Communications Manager. Para obter informações sobre como ativar o registro automático, consulte a documentação da sua versão específica do Cisco Unified Communications Manager. Quando você configura o cluster para o modo misto por meio do cliente CTL da Cisco, o registro automático é desativado automaticamente; no entanto, você pode ativá-lo. Quando você configura o cluster para o modo não seguro por meio do cliente CTL da Cisco, o registro automático não é ativado automaticamente.

Você pode adicionar telefones com o registro automático e a TAPS, a Ferramenta para suporte a telefones registrados automaticamente, sem ter que coletar antes os endereços MAC dos telefones.

A TAPS trabalha com a BAT (Bulk Administration Tool) para atualizar um lote de telefones que já foram adicionados ao banco de dados do Cisco Unified Communications Manager com endereços MAC falsos. Use a TAPS para atualizar endereços MAC e baixar configurações predefinidas para telefones.

A Cisco recomenda usar o registro automático e a TAPS para adicionar menos de 100 telefones à sua rede. Para adicionar mais de 100, use a BAT (Bulk Administration Tool).

Para implementar a TAPS, você ou o usuário final disca um número de diretório da TAPS e segue os prompts de voz. Após a conclusão do processo, o telefone contém o número de diretório e outras configurações, além de ser atualizado na Administração do Cisco Unified Communications Manager com o endereço MAC correto.

Verifique se o registro automático está ativado e corretamente configurado na Administração do Cisco Unified Communications Manager antes de você conectar qualquer Telefone IP Cisco à rede. Para obter informações sobre como ativar e configurar o registro automático, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

O registro automático deve ser ativado na Administração do Cisco Unified Communications Manager para que a TAPS funcione.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, clique em **Sistema** > **Cisco Unified CM**.

Etapa 2 Clique em **Localizar** e selecione o servidor necessário.

Etapa 3 Em **Informações de registro automático**, configure esses campos.

- **Modelo de dispositivo universal**
- **Modelo de linha universal**
- **Número de diretório inicial**
- **Número de diretório final**

Etapa 4 Desmarque a caixa de seleção **Registro automático desativado nesse Cisco Unified Communications Manager**.

Etapa 5 Clique em **Save** (Salvar).

Etapa 6 Clique em **Aplicar config.**

Modo Daisy Chain

Você pode conectar dois telefones de conferência usando um Adaptador Inteligente e os cabos USB-C fornecidos no kit de daisy chain para expandir a área de cobertura de áudio em uma sala.

No modo daisy chain, ambas as unidades ecebem energia por meio do adaptador inteligente que está conectado a um adaptador de energia. Você pode usar apenas um microfone externo por unidade. Você pode usar um par de microfones com fio com as unidades ou um par de microfones sem fio com as unidades, mas não uma combinação mista dos microfones. Quando um microfone com fio estiver conectado a uma das unidades, ele desemparelha quaisquer microfones sem fio que estejam conectados à mesma unidade. Sempre que houver uma chamada ativa, os LEDs e as opções de menu na tela do telefone de ambas as unidades são sincronizados.

Tópicos relacionados

Instalar o telefone de conferência no modo Daisy Chain, na página 40
Um telefone no modo Daisy Chain não funciona, na página 170

Instalar o telefone de conferência

Depois que o telefone se conecta à rede, o processo de inicialização do telefone é iniciado e o telefone é registrado no Cisco Unified Communications Manager. Se você desativar o serviço DHCP, você terá de definir as configurações de rede no telefone.

Se você usou o registro automático, você terá de atualizar as informações de configuração específicas do telefone, como associar o telefone a um usuário, alterar a tabela de botões ou o número de diretório.

Depois que o telefone se conecta, ele determina se uma nova carga de firmware tem de ser instalada no telefone.

Se você estiver usando o telefone de conferência no modo daisy chain, consulte Instalar o telefone de conferência no modo Daisy Chain, na página 40.

Antes de Iniciar

Certifique-se de que você tem a versão de firmware mais recente instalada em seu Cisco Unified Communications Manager. Verifique os pacotes de dispositivos atualizados aqui:

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

Procedimento

Etapa 1 Escolha a fonte de alimentação para o telefone:

- Implantação Power over Ethernet (PoE) com um Injetor PoE do Telefone IP Cisco de conferência 8832
- Implantação não PoE Ethernet deployment com um Telefone IP Cisco de conferência 8832 injetor Ethernet não PoE

- Implantação Wi-Fi com um adaptador de energia do Telefone IP Cisco de conferência 8832

Para obter mais informações, consulte Maneiras de fornecer energia para o telefone de conferência, na página 35

Etapa 2 Conecte o telefone ao switch.

- Se você usar PoE:
  1. Conecte o cabo Ethernet na porta LAN.
  2. Conecte a outra extremidades do cabo Ethernet ao Injetor PoE do Telefone IP Cisco de conferência 8832 ou ao Injetor de Ethernet do Telefone IP Cisco de conferência 8832.
  3. Conecte o injetor ao telefone de conferência com o cabo USB-C.
- Se você não usar PoE:
  1. Se você estiver usando o Injetor de Ethernet do Telefone IP Cisco de conferência 8832, conecte o adaptador de energia a uma tomada elétrica.
  2. Conecte o adaptador de energia ao injetor de Ethernet usando um cabo USB-C.

     OR

     Se você estiver usando o Telefone IP Cisco de conferência 8832 injetor Ethernet não PoE, conecte-o uma tomada elétrica.
  3. Conecte o cabo Ethernet ao injetor de Ethernet não PoE ou ao injetor de Ethernet.
  4. Conecte o cabo Ethernet na porta LAN.
  5. Conecte o injetor de Ethernet não PoE ou o injetor de Ethernet ao telefone de conferência usando um cabo USB-C.
- Se você usar Wi-Fi:
  1. Conecte o adaptador de energia do Telefone IP Cisco de conferência 8832 à tomada elétrica.
  2. Conecte o adaptador de energia ao telefone de conferência usando um cabo USB-C.

     Observação Em vez do adaptador de energia, você pode usar o injetor de Ethernet não PoE para obter energia para o telefone. No entanto, você deve desconectar o cabo de LAN. O telefone apenas se conecta à rede Wi-Fi quando a conexão Ethernet não está disponível.

Etapa 3 Monitore o processo de inicialização do telefone. Essa etapa verifica se o telefone está configurado corretamente.

Etapa 4 Se você não usar o registro automático, defina manualmente as configurações de segurança no telefone.

Etapa 5 Permita que o telefone atualize para a imagem de firmware atual que é armazenada em seu Cisco Unified Communications Manager.

Etapa 6 Faça chamadas com o telefone para verificar se o telefone e os recursos funcionam corretamente.

Etapa 7 Forneça informações aos usuários sobre como usar seus telefones e como configurar as opções do telefone. Essa etapa garante que os usuários tenham informações adequadas para usar com êxito seus telefones Cisco.

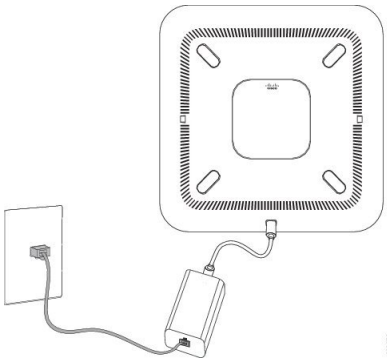
Maneiras de fornecer energia para o telefone de conferência

Seu telefone de conferência precisa de energia de uma destas fontes:

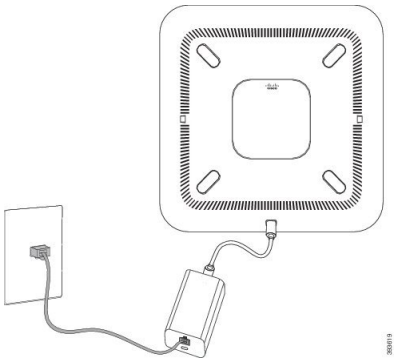
- Alimentação pela Ethernet (PoE – Power over Ethernet)
  - América do Norte
    - Injetor PoE do Telefone IP Cisco de conferência 8832
    - Injetor de Ethernet do Telefone IP Cisco de conferência 8832
  - Fora da América do Norte —Injetor PoE do Telefone IP Cisco de conferência 8832
- Não PoE Ethernet
  - América do Norte
    - Telefone IP Cisco de conferência 8832 injetor Ethernet não PoE
    - Injetor de Ethernet do Telefone IP Cisco de conferência 8832 com um adaptador de energia do Telefone IP Cisco de conferência 8832 conectado a uma tomada elétrica.
  - Fora da América do Norte —Telefone IP Cisco de conferência 8832 injetor Ethernet não PoE
- WiFi — Usar o adaptador de energia do Telefone IP Cisco de conferência 8832 conectado a uma tomada elétrica.

Figura 6: Opções de energia PoE do telefone de conferência

A figura a seguir mostra as duas opções de energia PoE.



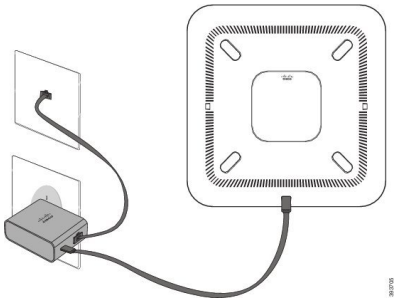
Injetor PoE do Telefone IP Cisco de conferência 8832 com a opção de energia PoE



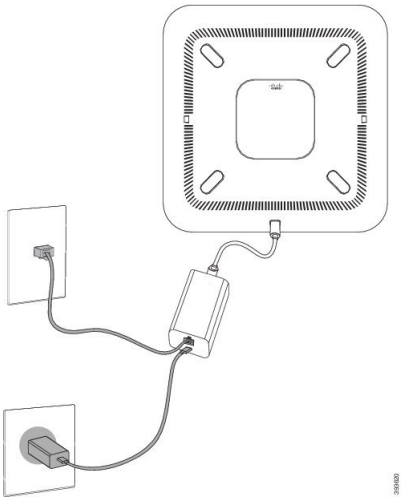
Injetor de Ethernet do Telefone IP Cisco de conferência 8832 com a opção de energia PoE

Figura 7: Opções de energia Ethernet do telefone de conferência

A figura a seguir mostra as duas opções de energia Ethernet.



Telefone IP Cisco de conferência 8832 injetor Ethernet não PoE com a opção de energia Ethernet



Injetor de Ethernet do Telefone IP Cisco de conferência 8832 com a opção de energia Ethernet

Figura 8: Opção de energia de telefone de conferência quando conectado a uma rede Wi-Fi

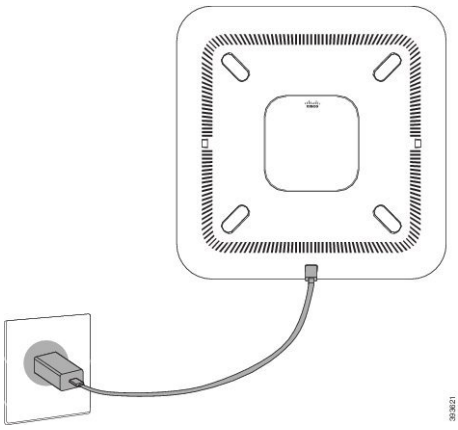
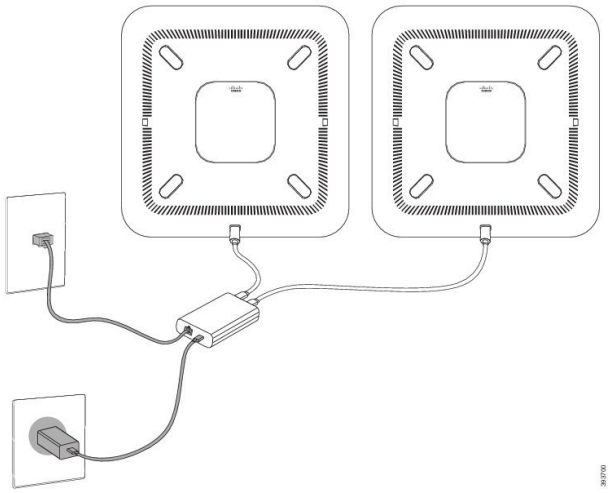


Figura 9: Opção de energia do telefone de conferência no modo Daisy Chain

A figura a seguir mostra a opção de energia quando o telefone está conectado no modo daisy chain.



Instalar microfones de expansão com fio

O telefone é compatível com um kit opcional com dois microfones de expansão com fio. Você pode estender os microfones até 2,13 m (7 pés) de distância do telefone. Para obter melhores resultados, recomendamos que coloque os microfones entre 0,91 m (3 pés) e 2,1 m (7 pés) de distância do telefone.

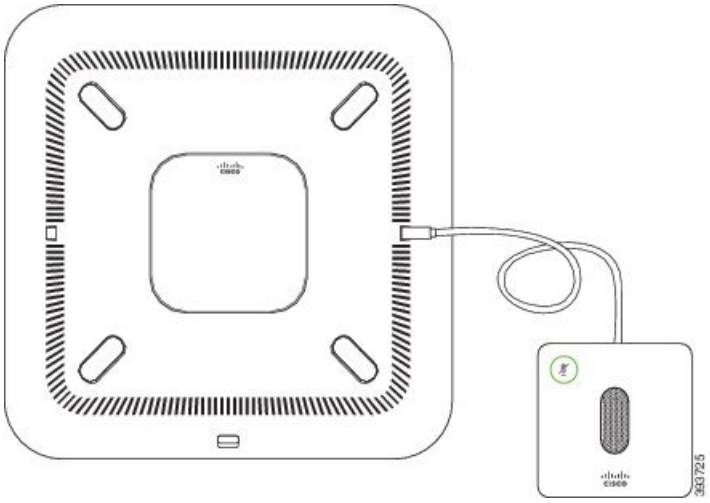
Procedimento

Etapa 1 Conecte a extremidade do cabo do microfone à porta lateral do telefone.

Etapa 2 Estenda o cabo do microfone para a posição desejada.

A figura a seguir mostra a instalação de um microfone de expansão com fio.

Figura 10: Instalação de microfones de expansão com fio



Instalar microfones de expansão sem fio

O telefone de conferência oferece a opção de conexão de dois microfones de expansão sem fio.

Observação Você deve usar dois microfones com fio ou dois microfones sem fio com o telefone, mas não uma combinação mista.

Quando o telefone está em uma chamada, o LED do microfone de expansão fica aceso em verde. Para silenciar o microfone de expansão, pressione a tecla **Silenciar**. Quando o microfone está com o som desativado, o LED fica aceso em vermelho. Quando a bateria no microfone estiver baixa, o LED de indicação da bateria pisca rapidamente.

Antes de Iniciar

Desconecte os microfones de expansão com fio antes de instalar microfones de expansão sem fio. Você não pode usar os dois microfones de expansão com e sem fio ao mesmo tempo.

Procedimento

Etapa 1 Posicione a placa de montagem na superfície da mesa onde deseja colocar o microfone.

Etapa 2 Remova o adesivo para a fita dupla face na parte inferior da placa de montagem da mesa. Posicione a placa de montagem de modo a que seja fixada à superfície da mesa.

Etapa 3 Prenda o microfone na placa de montagem da mesa. Ímãs estão incorporados no microfone para fixar a unidade no seu devido lugar.

Você pode mover o microfone e a placa de montagem para um local diferente na superfície da mesa, conforme necessário. Mova a unidade com cautela para protegê-la.

Tópicos relacionados

Microfone de expansão sem fio (somente 8832), na página 13
Instalar o gancho de carregamento do microfone sem fio, na página 39

Instalar o gancho de carregamento do microfone sem fio

Você usa o gancho de carregamento para carregar a bateria do microfone sem fio.

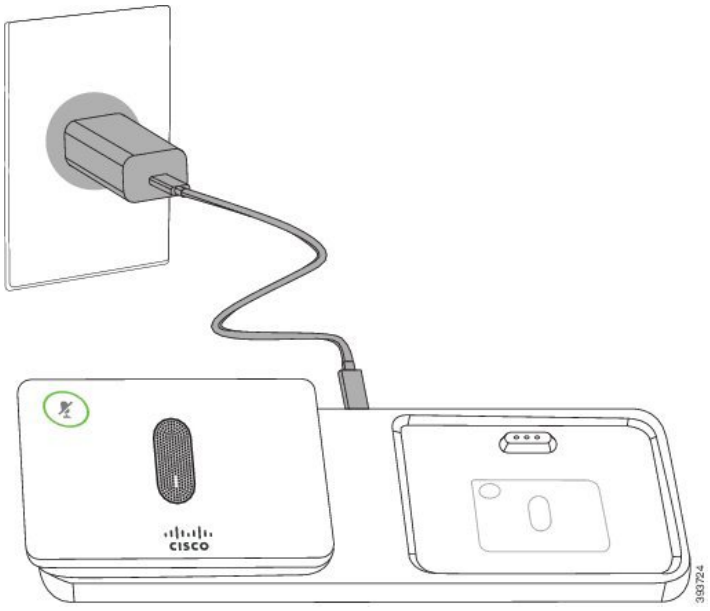
Procedimento

Etapa 1 Conecte o adaptador de energia do gancho de carregamento a uma tomada elétrica.

Etapa 2 Conecte uma extremidade do cabo USB-C ao gancho de carregamento e a outra extremidade ao adaptador de energia.

A figura a seguir mostra a instalação de um gancho de carregamento de microfone sem fio.

Figura 11: Instalação do gancho de carregamento de microfone sem fio



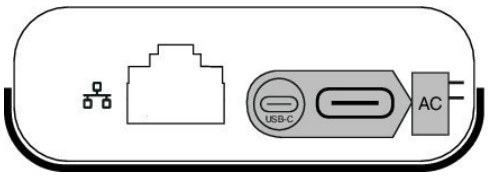
Tópicos relacionados

Microfone de expansão sem fio (somente 8832), na página 13
Instalar microfones de expansão sem fio, na página 38

Instalar o telefone de conferência no modo Daisy Chain

O kit de daisy chain contém um Adaptador Inteligente, um cabo de LAN curto, dois cabos USB-C longos mais grossos e um cabo USB-C mais curto e fino. No modo daisy chain, os telefones de conferência necessitam de alimentação externa de uma tomada elétrica. Você deve usar o Adaptador Inteligente para ligar os telefones juntos. Os cabos USB-C longos são ligados ao telefone e o curto é ligado ao adaptador de energia. Consulte a figura a seguir ao ligar o adaptador de energia e a porta LAN ao Adaptador Inteligente.

Figura 12: Porta do adaptador de energia inteligente e porta LAN



Você pode usar apenas um microfone por unidade.

Observação Você deve usar dois microfones com fio ou dois microfones sem fio com o telefone, mas não uma combinação mista.

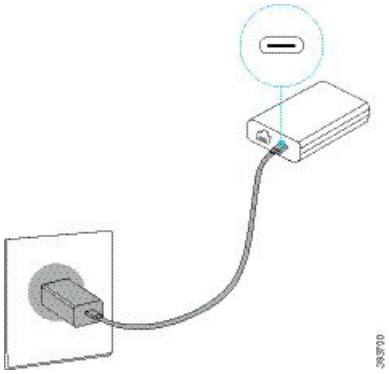
O cabo USB-C para o adaptador de energia é mais fino que os cabos USB-C que se conectam ao telefone.

Procedimento

Etapa 1 Conecte o adaptador de energia à tomada elétrica.

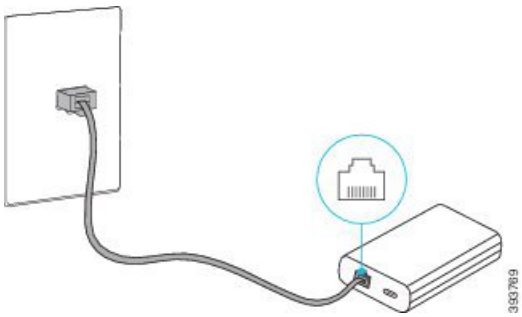
Etapa 2 Conecte o cabo USB-C curto e mais fino do adaptador de energia ao Adaptador Inteligente.

Figura 13: Porta USB do adaptador inteligente conectada à tomada elétrica



Etapa 3 Necessário: Conecte o cabo Ethernet ao Adaptador Inteligente e à porta LAN.

Figura 14: Porta LAN do adaptador inteligente conectada à porta LAN na tomada de parede

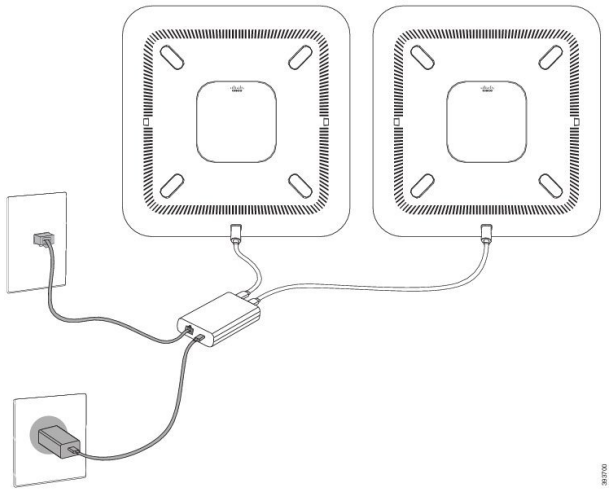


Etapa 4 Conecte o telefone primeiro ao Adaptador Inteligente usando o cabo USB-C mais longo e fino.

Etapa 5 Conecte o segundo telefone ao Adaptador Inteligente usando um cabo USB-C.

A figura a seguir mostra a instalação do telefone de conferência no modo daisy chain.

Figura 15: Instalação do telefone de conferência no modo Daisy Chain



Tópicos relacionados

Modo Daisy Chain, na página 33
Um telefone no modo Daisy Chain não funciona, na página 170

Reinicializar o telefone de conferência da imagem de backup

O Telefone IP Cisco de conferência 8832 tem uma segunda imagem de backup que permite que você recupere o telefone quando a imagem padrão tiver sido comprometida.

Para reinicializar o telefone com a imagem de backup, execute o procedimento a seguir.

Procedimento

Etapa 1 Mantenha a tecla * pressionada enquanto conecta a energia ao telefone de conferência.

Etapa 2 Após a luz da barra de LED ACENDER a verde e, depois, DESLIGAR, você poderá liberar a tecla *.

Etapa 3 O telefone de conferência reinicializa com a imagem de backup.

Configurar o telefone nos menus de configuração

O telefone inclui muitas definições de rede configuráveis que talvez você precise modificar para que o telefone funcione para os usuários. Você pode acessar essas configurações e alterar algumas delas usando os menos do telefone.

O telefone inclui os seguintes menus de configuração:

- Configuração de rede: fornece opções para visualizar e definir várias configurações de rede.
  - Configuração do IPv4: esse submenu fornece opções de rede adicionais.
  - Configuração do IPv6: esse submenu fornece opções de rede adicionais.
- Configuração de segurança: fornece opções para visualizar e definir várias configurações de segurança.

Observação Você pode controlar se um telefone tem acesso ao menu Configurações ou às opções neste menu. Use o campo **Acesso às configurações** na janela Administração do Cisco Unified Communications Manager Configuração do telefone para controlar o acesso. O campo **Acesso às configurações** aceita estes valores:

- Ativado: permite acesso ao menu Configurações.
- Desativado: impede o acesso à maioria das entradas no menu Configurações. O usuário ainda pode acessar a **Configurações** > **Status**.
- Restrito: Permite o acesso a itens do menu Preferências do usuário e Status e permite salvar as alterações ao volume. Impede o acesso a outras opções no menu Configurações.

Se não for possível acessar uma opção no menu Configurações do administrador, verifique o campo **Acesso às configurações**.

Você configura as definições que são somente exibição no Administração do Cisco Unified Communications Manager do telefone.

Procedimento

Etapa 1 Pressione **Configurações**.

Etapa 2 Selecione **Definições do admin.**

Etapa 3 Insira a senha, se necessário, e clique em **Iniciar sessão**.

Etapa 4 Selecione **Configuração de rede** ou **Configuração de segurança**.

Etapa 5 Execute uma destas ações para exibir o menu desejado:

- Use as setas de navegação para selecionar o menu desejado e pressione **Selecionar**.
- Use o teclado numérico do telefone para inserir o número que corresponde ao menu.

Etapa 6 Para exibir um submenu, repita a etapa 5.

Etapa 7 Para sair de um menu, pressione **Voltar**.

Tópicos relacionados

Reinicializar ou redefinir o telefone de conferência, na página 177
Definir as configurações de rede, na página 44
Definir as Configurações de Segurança

Aplicar uma senha ao telefone

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, navegue até a janela de configuração de Perfil de telefone comum (**Dispositivo** > **Configurações do dispositivo** > **Perfil de telefone comum**).

Etapa 2 Insira uma senha na opção Senha de desbloqueio de telefone local.

Etapa 3 Aplique a senha ao perfil de telefone comum usado pelo telefone.

Entrada de menu e texto no telefone

Ao editar o valor de uma configuração de opção, siga estas diretrizes:

- Use as setas no painel de navegação para realçar o campo que deseja editar. Pressione **Selecionar** no painel de navegação para ativar o campo. Depois que o campo estiver ativado, você poderá inserir valores.
- Use as teclas no teclado numérico para inserir números e letras.
- Para inserir letras usando o teclado numérico, use uma tecla de número correspondente. Pressione a tecla uma ou mais vezes para exibir uma letra em particular. Por exemplo, pressione a tecla **2** uma vez para "a," duas vezes rapidamente para "b" e três vezes rapidamente para "c." Depois de pausar, o cursor avança automaticamente para permitir que você insira a próxima letra.
- Pressione a tecla programável caso faça um erro. Essa tecla programável exclui o caractere à esquerda do cursor.
- Pressione **Reverter** antes de pressionar **Aplicar** para descartar quaisquer alterações feitas.
- Para inserir um ponto (por exemplo, em um endereço IP), pressione ***** no teclado numérico.
- Para inserir um ponto-e-vírgula para um endereço IPv6, pressione ***** no teclado numérico.

Observação O Telefone IP Cisco fornece vários métodos para redefinir ou restaurar configurações de opções, se necessário.

Definir as configurações de rede

Procedimento

Etapa 1 Pressione **Configurações**.

Etapa 2 Selecione **Configurações de administração** > **Configuração de rede** > **Configuração Ethernet**.

Etapa 3 Configure os campos conforme descrito em Campos de configuração de rede, na página 44.
Depois que você configurar os campos, talvez seja necessário reinicializar o telefone.

Campos de configuração de rede

O menu Configuração de rede contém campos e submenus para IPv4 e IPv6.

Para alterar alguns dos campos, você precisa desativar o DHCP.

Tabela 10: Menu de configuração de rede

Entrada	Tipo	Padrão	Descrição
Configuração de IPv4	Menu		Consulte a tabela "Submenu de configuração de IPv4". Esta opção é exibida somente no modo de pilha dupla.
Configuração de IPv6	Menu		Consulte a tabela "Submenu de configuração de IPv6".
Nome do host	String		Nome do host do telefone. Se estiver usando DHCP, esse nome é automaticamente atribuído.
Nome de domínio	String		Nome do domínio DNS (Sistema de nome de domínio) no qual o telefone reside. Para alterar esse campo, desative o DHCP.
ID da VLAN operacional			VLAN (Rede local virtual) operacional que é configurada em um switch do Cisco Catalyst do qual o telefone é um membro.
ID da VLAN administrativa			VLAN auxiliar do qual o telefone é um membro.

Entrada	Tipo	Padrão	Descrição
Config. porta do switch	Negociação automática 10 Meio 10 Todo 100 Meio 100 Todo	Negociação automática	Velocidade e duplex da porta do switch, onde: • 10 Meio = 10-BaseT/half-duplex • 10 Todo = 10-BaseT/full-duplex • 100 Meio = 100-BaseT/half-duplex • 100 Todo = 100-BaseT/full-duplex
LLDP-MED: Porta do switch	Desativado Habilitado	Habilitado	Indica se o protocolo LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) está ativado na porta do switch.

Tabela 11: Submenu de configuração de IPv4

Entrada	Tipo	Padrão	Descrição
DHCP	Desativado Habilitado	Habilitado	Ativa ou desativa o uso de DHCP.
Endereço IP			Endereço IP versão 4 (IPv4) do telefone. Para alterar esse campo, desative o DHCP.
Máscara de sub-rede			Máscara de sub-rede usada pelo telefone. Para alterar esse campo, desative o DHCP.
Roteador padrão 1			O roteador padrão que o telefone usa. Para alterar esse campo, desative o DHCP.
Servidor DNS 1			Servidor DNS (Domain Name System) primário (Servidor DNS 1) usado pelo telefone. Para alterar esse campo, desative o DHCP.
Servidor DNS 2			Servidor DNS (Domain Name System) primário (Servidor DNS 2) usado pelo telefone.
Servidor DNS 3			Servidor DNS (Domain Name System) primário (Servidor DNS 3) usado pelo telefone.

Entrada	Tipo	Padrão	Descrição
TFTP alternativo	Não Sim	Não	Indica se o telefone está usando um servidor TFTP alternativo.
Servidor TFTP 1			Servidor TFTP (Trivial File Transfer Protocol) primário utilizado pelo telefone. Se você definir a opção TFTP alternativo como Ligado, deverá inserir um valor diferente de zero para a opção Servidor TFTP 1. Se nem o servidor TFTP primário nem o servidor TFTP de reserva estiver listado no arquivo CTL ou ITL no telefone, você deverá desbloquear o arquivo antes de salvar as alterações para a opção Servidor TFTP 1. Nesse caso, o telefone excluirá o arquivo quando você salvar as alterações para a opção Servidor TFTP 1. Um novo arquivo CTL ou ITL será baixado do novo endereço de Servidor TFTP 1. Consulte as notas de TFTP após a tabela final.
Servidor TFTP 2			Servidor TFTP secundário usado pelo telefone. Se nem o servidor TFTP primário nem o servidor TFTP de reserva estiver listado no arquivo CTL ou ITL no telefone, você deverá desbloquear o arquivo antes de salvar as alterações para a opção Servidor TFTP 2. Nesse caso, o telefone excluirá o arquivo quando você salvar as alterações para a opção Servidor TFTP 2. Um novo arquivo CTL ou ITL será baixado do novo endereço de Servidor TFTP 2. Consulte a seção de notas de TFTP após a tabela final.
Endereço DHCP liberado	Não Sim	Não	

Tabela 12: Submenu de configuração de IPv6

Entrada	Tipo	Padrão	Descrição
DHCPv6 ativado	Desativado Habilitado	Habilitado	Ativa ou desativa o uso de DHCP IPv6.
Endereço IPv6			O endereço IPv6 do telefone. Para alterar esse campo, desative o DHCP.
Tamanho do prefixo IPv6			Comprimento do endereço IPv6. Para alterar esse campo, desative o DHCP.
Roteador padrão IPv6 1			Roteador IPv6 padrão. Para alterar esse campo, desative o DHCP.
Servidor DNS IPv6 1			Servidor DNS IPv6 primário Para alterar esse campo, desative o DHCP.
TFTP alternativo de IPv6	Não Sim	Não	Indica se o telefone está usando um servidor TFTP IPv6 alternativo.
Servidor TFTP 1 de IPv6			Servidor TFTP IPv6 primário usado pelo telefone. Consulte a seção de notas de TFTP após esta tabela.
Servidor TFTP 2 de IPv6			Servidor TFTP IPv6 secundário usado pelo telefone. Consulte a seção de notas de TFTP após esta tabela.
Endereço IPv6 liberado	Não Sim	Não	

Para poder configurar as opções de IPv6 em seu dispositivo, o IPv6 deve ser ativado e configurado na Administração do Cisco Unified Communication. Os campos de configuração de dispositivo a seguir se aplicam à configuração de IPv6:

- Modo de endereçamento IP
- Preferência do modo de endereçamento IP para sinalização

Se o IPv6 estiver ativado no cluster Unified, a configuração padrão do modo de endereçamento IP será IPv4 e IPv6. Nesse modo de endereçamento, o telefone vai adquirir e usar um endereço IPv4 e um endereço IPv6.

Ele pode usar o IPv4 e o endereço IPv6 conforme exigido pela mídia. O telefone usa o endereço IPv4 ou IPv6 para sinalização de controle de chamadas.

Para obter mais informações sobre IPv6, consulte:

- seção sobre "Configuração comum para dispositivos" no *Cisco Unified Communications Manager Feature and Services Guide*, capítulo "IPv6 Support in Cisco Unified Communications Devices".
- *Guia de implantação do IPv6 para sistemas Cisco Collaboration versão 12.0*, localizado aqui: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html

Notas TFTP

Quando o telefone procura pelo servidor TFTP, dá prioridade aos servidores TFTP atribuídos manualmente, independentemente do protocolo. Se a sua configuração incluir servidores TFTP IPv6 e IPv4, o telefone priorizará a ordem em que procura pelo servidor TFTP dando prioridade a servidores TFTP IPv6 e IPv4 atribuídos manualmente. O telefone procura pelo servidor TFTP nesta ordem:

1. Todos os servidores TFTP IPv4 atribuídos manualmente
2. Todos os servidores IPv6 atribuídos manualmente
3. Servidores TFTP atribuídos pelo DHCP
4. Servidores TFTP atribuídos pelo DHCPv6

Para obter informações sobre o arquivo CTL e ITL, consulte o *Guia de segurança do Cisco Unified Communications Manager*.

Definir o campo Nome de domínio

Procedimento

Etapa 1 Defina a opção DHCP ativado como **Não**.

Etapa 2 Role até a opção Nome de domínio, pressione **Selecionar** e insira um novo nome de domínio.

Etapa 3 Pressione **Aplicar**.

Ativar a LAN sem fio do telefone

Verifique se a cobertura de Wi-Fi no local em que a LAN sem fio está implementada é adequada para a transmissão de pacotes de voz.

Um método de roaming rápido e seguro é recomendado para usuários de Wi-Fi. Recomendamos que você use 802.11r (FT).

Para obter informações detalhadas de configuração, consulte o *Guia de implantação de LAN de Telefone IP sem fio Cisco 8832* neste local:

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

O *Guia de implantação de LAN do Telefone IP sem fio Cisco 8832* inclui as seguintes informações de configuração:

- Configuração da rede sem fio
- Configuração da rede sem fio na Administração do Cisco Unified Communications Manager
- Configuração da rede sem fio no Telefone IP Cisco

Antes de Iniciar

Verifique se a rede Wi-Fi está ativada no telefone e se o cabo Ethernet está desconectado.

Procedimento

Etapa 1 Para ativar o aplicativo, pressione **Configurações**.

Etapa 2 Navegue para **Configurações do administrador** > **Configuração de rede** > **Configuração de cliente Wi-Fi** > **Sem fio**.

Etapa 3 Pressione **Lig**.

Configurar a LAN sem fio no Cisco Unified Communications Manager

Na Administração do Cisco Unified Communications Manager, você deve ativar um parâmetro chamado "Wi-Fi" para o telefone de conferência.

Observação Na janela Configuração do telefone na Administração do Cisco Unified Communications Manager (**Dispositivo** > **Telefone**), use o endereço MAC de linha com fio quando configurar o endereço MAC. O registro do Cisco Unified Communications Manager não usa o endereço MAC sem fio.

Execute o procedimento a seguir na Administração do Cisco Unified Communications Manager.

Procedimento

Etapa 1 Para ativar a LAN sem fio em um telefone específico, execute as seguintes etapas:

a) Selecione **Dispositivo** > **Telefone**.
b) Localize o telefone necessário.
c) Selecione a configuração **Ativado** para ativar o parâmetro Wi-Fi na seção Layout de configuração específica do produto.
d) Marque a caixa de seleção **Substituir definições comuns**.

Etapa 2 Para ativar a LAN sem fio para um grupo de telefones,

a) Selecione **Dispositivo** > **Definições do dispositivo** > **Perfil de telefone comum**.

b) Selecione a configuração **Ativado** para ativar o parâmetro Wi-Fi.

Observação Para garantir que a configuração nesta etapa funciona, desmarque a caixa de seleção **Substituir configurações comuns** mencionada na etapa 1d.

c) Marque a caixa de seleção **Substituir definições comuns**.
d) Associe os telefones com esse perfil de telefone comum usando **Dispositivo** > **Telefone**.

Etapa 3 Para ativar a LAN sem fio para todos os telefones compatíveis com WLAN na rede,

a) Selecione **Sistema** > **Configuração do telefone da empresa**.
b) Selecione a configuração **Ativado** para ativar o parâmetro Wi-Fi.

Observação Para garantir que a configuração nesta etapa funciona, desmarque a caixa de seleção **Substituir configurações comuns** mencionada nas etapas 1d e 2c.

c) Marque a caixa de seleção **Substituir definições comuns**.

Configurar a LAN sem fio usando o telefone

Antes que o Telefone IP Cisco possa ser conectado à WLAN, você deve configurar o perfil de rede para o telefone com as configurações apropriadas da WLAN. Você pode usar o menu **Configuração de rede** no telefone para acessar o submenu **Configuração do cliente Wi-Fi** e definir a configuração da WLAN.

Observação A opção **Configuração do cliente Wi-Fi** não é exibida no menu **Configuração de rede** quando o Wi-Fi está desativado no Cisco Unified Communications Manager.

Para obter mais informações, consulte o *Guia de implementação de WLAN do Telefone IP Cisco de conferência 8832*, localizado aqui: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html

Antes de Iniciar

Configure a LAN sem fio usando o Cisco Unified Communications Manager.

Procedimento

Etapa 1 Pressione **Configurações**.

Etapa 2 Selecione **Definições do admin.** > **Configuração de rede** > **Configuração do cliente Wi-Fi**.

Etapa 3 Defina a configuração sem fio conforme descrito na tabela a seguir.

Tabela 13: Opções do menu Configuração do cliente Wi-Fi

Opção	Descrição	Para alterar
Sem fio	Ativa ou desativa o rádio sem fio no Telefone IP Cisco.	Role até a opção **Sem fio** e use a opçã alternância para ativar e desativar a cor

Opção	Descrição	Para alterar
Nome da rede	Permite que você se conecte a uma rede sem fio usando a janela **Escolher uma rede**. Essa janela tem duas teclas programáveis - **Voltar** e **Outros**.	Na janela **Escolher uma rede**, sel a que você deseja se conectar.
Login de acesso Wi-Fi	Ativa a exibição da janela de login de acesso Wi-Fi.	Role até a opção **Login de acesso** opção de alternância para ativar e configuração.
Configuração de IPv4	No submenu Configuração de IPv4, é possível fazer o seguinte: • Ativar ou desativar o telefone para usar o endereço IP que o servidor DHCP atribui. • Definir manualmente o endereço IP, a máscara de sub-rede, os roteadores padrão, o servidor DNS e os servidores TFTP alternativos. Para obter mais informações sobre os campos de endereço IPv4, consulte a tabela "Submenu de configuração IPv4".	Role até **Configuração de IPv4** e **Selecionar**.
Configuração de IPv6	No submenu Configuração de IPv6, é possível fazer o seguinte: • Ativar ou desativar o telefone para usar o endereço IPv6 que é atribuído pelo servidor DHCPv6 ou adquirido pelo SLAAC por meio de um roteador ativado por IPv6. • Definir manualmente o endereço IPv6, o comprimento do prefixo, os roteadores padrão, o servidor DNS e os servidores TFTP alternativos. Para obter mais informações sobre os campos de endereço IPv6, consulte a tabela "Submenu de configuração IPv6".	Role até **Configuração de IPv6** e **Selecionar**.
endereço MAC	Endereço MAC (Controle de acesso à mídia) exclusivo do telefone.	Somente para exibição. Não é possí
Nome de domínio	Nome do domínio DNS (Sistema de nome de domínio) no qual o telefone reside.	Consulte Definir o campo Nome d página 48.

Etapa 4 Pressione **Salvar** para fazer alterações ou **Reverter** para descartar a conexão.

Definir o número de tentativas de autenticação WLAN

Uma solicitação de autenticação é uma confirmação das credenciais de entrada do usuário. Ela ocorre sempre que um telefone que já ingressou em uma rede Wi-Fi tenta se reconectar ao servidor Wi-Fi. Exemplos incluem

quando o limite de tempo de uma sessão de Wi-Fi é esgotado ou quando uma conexão é perdida e, em seguida, readquirida.

Você pode configurar o número de vezes que um telefone Wi-Fi envia uma solicitação de autenticação ao servidor Wi-Fi. O número padrão de tentativas é 2, mas você pode definir esse parâmetro de 1 a 3. Se um telefone falhar na autenticação, o usuário será solicitado a fazer login novamente.

Você pode aplicar tentativas de autenticação da WLAN a telefones individuais, a um conjunto de telefones ou a todos os telefones Wi-Fi de sua rede.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, selecione **Dispositivo** > **Telefone** e localize o telefone.

Etapa 2 Navegue até a área Configuração específica do produto e defina o campo de **Tentativas de autenticação da WLAN**.

Etapa 3 Selecione **Salvar**.

Etapa 4 Selecione **Aplicar config.**

Etapa 5 Reinicie o telefone.

Ativar o modo de prompt de WLAN

Ative o modo de prompt de perfil WLAN 1 se desejar que um usuário entre na rede Wi-Fi quando o telefone dele for ligado ou redefinido.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, selecione **Dispositivo** > **Telefone**.

Etapa 2 Localize o telefone que você precisa configurar.

Etapa 3 Navegue até a área Configuração específica do produto e defina o campo **Modo de prompt de perfil WLAN 1** para **Ativar**.

Etapa 4 Selecione **Salvar**.

Etapa 5 Selecione **Aplicar config.**

Etapa 6 Reinicie o telefone.

Configurar um perfil de Wi-Fi usando o Cisco Unified Communications Manager

Você pode configurar um perfil de Wi-Fi e depois atribuir um perfil aos telefones compatíveis com Wi-Fi. O perfil contém os parâmetros necessários para os telefones se conectarem ao Cisco Unified Communications Manager com Wi-Fi. Ao criar e usar um perfil de Wi-Fi, você ou seus usuários não precisam configurar a rede sem fio para telefones individuais.

Os perfis de Wi-Fi são compatíveis com o Cisco Unified Communications Manager versão 10.5(2) ou posterior. EAP-FAST, PEAP-GTC e PEAP-MSCHAPv2 são compatíveis com o Cisco Unified Communications Manager

versão 10.0 e posterior. O EAP-TLS é compatível com o Cisco Unified Communications Manager versão 11.0 e posterior.

Um perfil de Wi-Fi permite impedir ou limitar as alterações na configuração de Wi-Fi no telefone pelo usuário.

É recomendável usar um perfil seguro com criptografia TFTP ativada para proteger chaves e senhas quando você usar um perfil de Wi-Fi.

Quando você configurar os telefones para usar a autenticação EAP-FAST, PEAP-MSCHAPv2 ou PEAP-GTC, seus usuários precisarão de IDs de usuário e senhas individuais para entrar no telefone.

Os telefones são compatíveis apenas com um certificado de servidor que pode ser instalado com SCEP ou o método de instalação manual, mas não com ambos os métodos. O telefone não suporta o método de TFTP de instalação do certificado.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, selecione **Dispositivo** > **Definições do dispositivo** > **Perfil de rede local sem fio**.

Etapa 2 Clique em **Adicionar novo**.

Etapa 3 Na seção **Informações do perfil de rede local sem fio**, defina os parâmetros:

- **Nome** — insira um nome exclusivo para o perfil de Wi-Fi. Esse nome é exibido no telefone.
- **Descrição** — insira uma descrição para o perfil de Wi-Fi para ajudar a identificar esse perfil de outros perfis de Wi-Fi.
- **Modificável pelo usuário** — selecione uma opção:
  - **Permitido** — indica que o usuário pode fazer alterações nas configurações de Wi-Fi do telefone. Essa opção é selecionada por padrão.
  - **Não permitido** — indica que o usuário não pode fazer alterações nas configurações de Wi-Fi do telefone.
  - **Restrito** — indica que o usuário pode alterar o nome de usuário e a senha do Wi-Fi no telefone. Mas, os usuários não têm permissão para fazer alterações em outras configurações de Wi-Fi no telefone.

Etapa 4 Na seção **Configurações sem fio**, defina os parâmetros:

- **SSID (nome da rede)** — insira o nome da rede disponível no ambiente de usuário ao qual o telefone pode estar conectado. Esse nome é exibido na lista de redes disponíveis no telefone, e o telefone pode se conectar a essa rede sem fio.
- **Faixa de frequência** — as opções disponíveis são Automático, 2,4 GHz e 5 GHz. Esse campo determina a faixa de frequência que usa a conexão sem fio. Se você selecionar Automático, o telefone tentará usar a faixa de 5 GHz primeiro e usará somente a faixa de 2,4 GHz quando 5 GHz não estiver disponível.

Etapa 5 Na seção **Configurações de autenticação**, defina o **Método de autenticação** para um destes métodos de autenticação: EAP-FAST, EAP-TLS, PEAP-MSCHAPv2, PEAP-GTC, PSK, WEP e Nenhum.

Depois de configurar esse campo, você poderá ver os campos adicionais que precisam ser configurados.

- **Certificado do usuário** — necessário para autenticação EAP-TLS. Selecione **Instalado pela fabricação** ou **Instalado pelo usuário**. O telefone exige a instalação de um certificado, quer automaticamente a partir do SCEP ou manualmente a partir da página de administração do telefone.
- **Senha PSK** — necessária para autenticação PSK. Insira a senha ASCII de 8-63 caracteres ou de 64 caracteres HEX.
- **Chave WEP** — necessária para autenticação WEP. Insira a chave WEP ASCII ou HEX 40/102 ou 64/128.
  - A chave ASCII 40/104 tem 5 caracteres.
  - A chave ASCII 64/128 tem 13 caracteres.
  - A chave HEX 40/104 tem 10 caracteres.
  - A chave HEX 64/128 tem 26 caracteres.
- **Fornecer credenciais compartilhadas**: necessário para autenticação EAP-FAST, PEAP-MSCHAPv2 e PEAP-GTC.
  - Se o usuário gerencia o nome de usuário e a senha, deixe os campos **Nome de usuário** e **Senha** em branco.
  - Se todos os usuários compartilham o mesmo nome de usuário e senha, você pode inserir as informações nos campos **Nome de usuário** e **Senha**.
  - Digite uma descrição no campo **Descrição de senha**.

Observação Se você precisar atribuir cada usuário um nome de usuário e uma senha exclusivos, crie um perfil para cada usuário.

Etapa 6 Clique em **Save** (Salvar).

O que Fazer Depois

Aplique o grupo de perfil de WLAN a um pool de dispositivos (**Sistema** > **Pool de dispositivos**) ou diretamente ao telefone (**Dispositivo** > **Telefone**).

Definir um grupo de Wi-Fi usando o Cisco Unified Communications Manager

Você pode criar um grupo de perfis de LAN sem fio e adicionar qualquer perfil de LAN sem fio a esse grupo. O grupo de perfis pode, então, ser atribuído ao telefone quando você configurar o telefone.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, selecione **Dispositivo** > **Definições do dispositivo** > **Grupo de perfil de rede local sem fio**.

Você também pode definir um grupo de perfis de LAN sem fio em **sistema** > **Pool de dispositivos**.

Etapa 2 Clique em **Adicionar novo**.

Etapa 3 Na seção de **Informações do Grupo de perfil de rede local sem fio**, digite um nome e uma descrição para o grupo.

Etapa 4 Na seção de **Perfis para este Grupo de perfil de rede local sem fio**, selecione um perfil disponível na lista de **Perfis disponíveis** e mova o perfil selecionado para a lista de **Perfis selecionados**.

Quando mais de um perfil de LAN sem fio for selecionado, o telefone usará somente o primeiro perfil de LAN sem fio.

Etapa 5 Clique em **Save** (Salvar).

Verificar a inicialização do telefone

Depois que o telefone for ligado à energia elétrica, ele iniciará automaticamente o processo de diagnóstico na inicialização.

Procedimento

Ligue o telefone.

Quando a tela principal for exibida, significa que ele foi corretamente inicializado.

Alterar o modelo de telefone de um usuário

Você ou o usuário pode alterar o modelo de telefone de um usuário. A alteração pode ser necessária por vários motivos, por exemplo:

- Você atualizou o Cisco Unified Communications Manager (Unified CM) para uma versão do software que não é compatível com o modelo do telefone.
- O usuário deseja um modelo de telefone diferente do modelo atual.
- O telefone exige reparo ou substituição.

O Unified CM identifica o telefone antigo e usa o endereço MAC do telefone antigo para identificar a configuração do telefone antigo. O Unified CM copia a configuração do telefone antigo para a entrada do novo telefone. O novo telefone tem a mesma configuração do telefone antigo.

Limitação: se o telefone antigo tiver mais linhas ou botões de linha do que o novo telefone, o novo telefone não terá linhas ou botões de linha extras configurados.

O telefone é reinicializado quando a configuração é concluída.

Antes de Iniciar

Configure o Cisco Unified Communications Manager de acordo com as instruções do *Guia de configuração do recurso do Cisco Unified Communications Manager*.

Você precisa de um telefone novo e não utilizado que vem pré-instalado com a versão do firmware 12.8(1) ou posterior.

Procedimento

Etapa 1 Desligue o telefone antigo.

Etapa 2 Ligue o novo telefone.

Etapa 3 No novo telefone, selecione **Substituir um telefone existente**.

Etapa 4 Insira a extensão principal do telefone antigo.

Etapa 5 Se o telefone antigo tiver um PIN atribuído, digite o PIN.

Etapa 6 Pressione **Enviar**.

Etapa 7 Se houver mais de um dispositivo para o usuário, selecione o dispositivo a ser substituído e pressione **Continuar**.

CAPÍTULO 5

Instalação de telefones no Cisco Unified Communications Manager

Configurar um Telefone IP Cisco de conferência

Se o registro automático não estiver ativado e o telefone não existir no banco de dados do Cisco Unified Communications Manager, você deverá configurar manualmente o Telefone IP Cisco na Administração do Cisco Unified Communications Manager. Algumas tarefas nesse procedimento são opcionais, dependendo do seu sistema e das necessidades do usuário.

Para obter mais informações sobre qualquer uma das etapas, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Execute as etapas de configuração no procedimento a seguir usando a Administração do Cisco Unified Communications Manager.

Procedimento

Etapa 1 Colete as seguintes informações sobre o telefone:

- Modelo do telefone
- Endereço MAC: consulte Determinar o endereço MAC do telefone, na página 62
- Local físico do telefone
- Nome ou ID do usuário de telefonia
- Pool de dispositivos

- Partição, espaço de pesquisa de chamada e informações de local
- Número de diretório (DN) para atribuir ao telefone
- Usuário do Cisco Unified Communications Manager a ser associado ao telefone
- Informações de uso do telefone que afetam o modelo de tecla programável, os recursos do telefone, os serviços de telefonia IP ou os aplicativos do telefone

Para obter mais informações, consulte a documentação da sua versão específica do Cisco Unified Communications Manager e veja os links relacionados.

Etapa 2 Verifique se você tem licenças de unidade suficientes para seu telefone.

Para obter mais informações, consulte o documento de licenciamento da sua versão específica do Cisco Unified Communications Manager.

Etapa 3 Defina os Pools de dispositivos. Selecione **Sistema** > **Pool de dispositivos**.

Os Pools de dispositivos definem características comuns para dispositivos, como região, grupo de data/hora e modelo de tecla programável.

Etapa 4 Defina o Perfil de telefone comum. Selecione **Dispositivo** > **Definições do dispositivo** > **Perfil de telefone comum**.

Os perfis de telefone comuns fornecem dados exigidos pelo servidor TFTP da Cisco, bem como configurações do telefone, como o recurso Não perturbar e as opções de controle de recurso.

Etapa 5 Defina um Espaço de pesquisa de chamada. Na Administração do Cisco Unified Communications Manager, clique em **Roteamento de chamadas** > **Classe do controle** > **Espaço de pesquisa de chamada**.

Um Espaço de pesquisa de chamada é um conjunto de partições que são pesquisadas para determinar como um número discado é roteado. O espaço de pesquisa de chamada para o dispositivo e o espaço de pesquisa de chamada para o número de diretório são usados juntos. A CSS do número de diretório tem precedência sobre a CSS do dispositivo.

Etapa 6 Configure um perfil de segurança para o protocolo e o tipo de dispositivo. Selecione **Sistema** > **Segurança** > **Perfil de segurança do telefone**.

Etapa 7 Configure o telefone. Selecione **Dispositivo** > **Telefone**.

a) Localize o telefone que deseja modificar ou adicione um novo telefone.
b) Configure o telefone preenchendo os campos obrigatórios no painel Informações sobre dispositivo da janela Configuração do telefone.
    - Endereço MAC (obrigatório): certifique-se de que o valor contenha 12 caracteres hexadecimais.
    - Descrição: insira uma descrição útil para ajudar caso precise pesquisar informações sobre o usuário.
    - Pool de dispositivos (obrigatório)
    - Perfil de telefone comum
    - Espaço de Pesquisa de Chamada
    - LOCAL
    - Proprietário (Usuário ou Anônimo); se selecionar Usuário, a ID de usuário de proprietário

O dispositivo com suas configurações padrão é adicionado ao banco de dados do Cisco Unified Communications Manager.

Para obter informações sobre os campos Configuração específica do produto, consulte a Ajuda do botão "?" Botão Ajuda na janela Configuração do telefone e o link relacionado.

Observação Se desejar adicionar o telefone e o usuário ao banco de dados do Cisco Unified Communications Manager ao mesmo tempo, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

c) Na área Informações específicas do protocolo dessa janela, escolha um Perfil de segurança do dispositivo e defina o modo de segurança.

Observação Escolha um perfil de segurança com base na estratégia geral de segurança da empresa. Se o telefone não oferecer suporte à segurança, escolha um perfil não seguro.

d) Na área Extension Information (Informações de ramal), marque a caixa de seleção Enable Extension Mobility (Ativar Extension Mobility) se esse telefone for compatível com o Cisco Extension Mobility.
e) Clique em **Save** (Salvar).

Etapa 8 Selecione **Dispositivo** > **Configurações do dispositivo** > **Perfil SIP** para configurar os parâmetros SIP.

Etapa 9 Selecione **Dispositivo** > **Telefone** para configurar os números de diretório (linhas) no telefone preenchendo os campos obrigatórios na janela Configuração do Número de diretório.

a) Localize o telefone.
b) Na janela Configuração do telefone, clique em Linha 1 no painel esquerdo da janela.

Os telefones de conferência só têm uma linha.

c) No campo Número de diretório, insira um número válido que possa ser discado.

Observação Esse campo deve conter o mesmo número que aparece no campo Número de telefone na janela Configuração de usuário final.

d) Na lista suspensa Partição de rota, escolha a partição à qual o número de diretório pertence. Se não desejar restringir o acesso ao número de diretório, escolha <None> para a partição.
e) Na lista suspensa Espaço de pesquisa de chamada, escolha o espaço apropriado. O valor que você escolhe se aplica a todos os dispositivos que estão usando esse número de diretório.
f) Na área Configurações de Captura de chamadas e Encaminhamento de chamadas, escolha os itens (por exemplo, Encaminhar todas, Encaminhar internas ocupadas) e os destinos correspondentes aos quais as chamadas devem ser enviadas.

Exemplo:

Se desejar que as chamadas recebidas externas e internas que recebem um sinal de ocupado sejam encaminhadas para o correio de voz da linha, marque a caixa de seleção Correio de voz ao lado dos itens Encaminhar internas ocupadas e Encaminhar externas ocupadas na coluna esquerda da área Configurações de Captura de chamadas e Encaminhamento de chamadas.

g) Na Linha 1 do painel Dispositivo, configure os seguintes campos:

- Exibição (campo ID do autor da chamada interna): você pode inserir o nome e o sobrenome do usuário desse dispositivo para que esse nome seja exibido para todas as chamadas internas. Deixe esse campo em branco para que o sistema exiba o ramal telefônico.
- Máscara de número de telefone externo: indica o número de telefone (ou máscara) que é usado para enviar informações sobre o ID do autor da chamada quando uma chamada é realizada nessa linha.

Você pode inserir um máximo de 24 caracteres numéricos e "X". Os Xs representam o número de diretório e devem aparecer no fim do padrão.

Exemplo:

Se você especificar uma máscara de 408902XXXX, uma chamada externa do ramal 6640 exibirá um número de ID do autor da chamada de 4089026640.

Essa configuração se aplica apenas ao dispositivo atual, a menos que você marque a caixa de seleção à direita (Update Shared Device Settings [Atualizar configurações compartilhadas de dispositivo]) e clique em **Propagate Selected (Propagar selecionados)**. A caixa de seleção à direita será exibida somente se outros dispositivos compartilharem esse número de diretório.

h) Selecione **Salvar**.

Para obter mais informações sobre números de diretório, consulte a documentação da sua versão específica do Cisco Unified Communications Manager e veja os links relacionados.

Etapa 10 (Opcional) Associe o usuário a um telefone. Clique em **Associar usuários finais** na parte inferior da janela Configuração do telefone para associar um usuário à linha que está sendo configurada.

a) Use **Localizar** em conjunto com os campos Pesquisar para localizar o usuário.
b) Marque a caixa ao lado do nome do usuário e clique em **Adicionar selecionados**.

O nome e a ID de usuário aparecem no painel Users Associated With Line (Usuários associados à linha) da janela Configuração do número de diretório.

c) Selecione **Salvar**.

O usuário agora está associado à Linha 1 no telefone.

Etapa 11 (Opcional) Associe o usuário ao dispositivo:

a) Escolha **Gerenciamento de usuários** > **Usuário final**.
b) Use as caixas de pesquisa e **Localizar** para encontrar o usuário que você adicionou.
c) Clique na ID de usuário.
d) Na área Associações do número de diretório da tela, defina o Ramal principal na lista suspensa.
e) (Opcional) Na área Informações sobre mobilidade, marque a caixa Ativar mobilidade.
f) Na área Informações sobre permissões, use os botões **Adicionar ao grupo de controle de acesso** para adicionar esse usuário a qualquer grupo de usuários.

Por exemplo, talvez você queira adicionar o usuário a um grupo que esteja definido como um Grupo de usuários finais do CCM padrão.

g) Para visualizar os detalhes de um grupo, selecione o grupo e clique em **Ver detalhes**.
h) Na área Extension Mobility, marque a caixa Ativar Extension Mobility entre Clusters se o usuário puder usar esse serviço.
i) Na área Informações sobre dispositivo, clique em **Associações do dispositivo**.
j) Use os campos Pesquisar e **Localizar** para encontrar o dispositivo que deseja associar ao usuário.
k) Selecione o dispositivo e clique em **Salvar selecionados/alterações**.
l) Clique em **Ir** ao lado do link relacionado "Voltar para usuário" no canto superior direito da tela.
m) Selecione **Salvar**.

Etapa 12 Personalize os modelos de tecla programável. Selecione **Dispositivo** > **Configurações do dispositivo** > **Modelo de tecla programável**.

Use a página para adicionar, excluir ou alterar a ordem dos recursos de tecla programável que são exibidos no telefone do usuário para atender às necessidades de uso do recurso.

O telefone de conferência tem requisitos especiais de tecla programável. Consulte os links relacionados para obter mais informações.

Etapa 13 Configure os serviços do Telefone IP Cisco e atribua serviços. Selecione **Dispositivo** > **Configurações do dispositivo** > **Serviços de telefonia**.

Forneça os serviços de telefonia IP ao telefone.

Observação Os usuários podem adicionar ou alterar serviços nos respectivos telefones usando o Cisco Unified Communications Self Care Portal.

Etapa 14 (Opcional) Adicione informações sobre usuário ao diretório global do Cisco Unified Communications Manager. Selecione **Gerenciamento de usuários** > **Usuário final**, clique em **Adicionar novo** e configure os campos obrigatórios. Campos obrigatórios são indicados por um asterisco (*).

Observação Se sua empresa usa um diretório Lightweight Directory Access Protocol (LDAP) para armazenar informações sobre usuários, você poderá instalar e configurar o Cisco Unified Communications para usar seu diretório LDAP existente. Consulte Configuração do diretório corporativo, na página 129. Depois que o campo Ativar a sincronização no servidor LDAP for ativado, você não poderá adicionar mais usuários na Administração do Cisco Unified Communications Manager.

a) Defina os campos ID de usuário e sobrenome.
b) Atribua uma senha (para Self Care Portal).
c) Atribua um PIN (para Cisco Extension Mobility e Diretório pessoal).
d) Associe o usuário a um telefone.

   Forneça aos usuários controle sobre o respectivo telefone, como encaminhamento de chamadas ou adição de serviços ou números de discagem rápida.

   Observação Alguns telefones, como os da sala de conferência, não têm um usuário associado.

Etapa 15 (Opcional) Associe um usuário a um grupo de usuários. Selecione **Gerenciamento de usuários** > **Configurações do usuário** > **Grupo de controle de acesso**.

Atribua aos usuários uma lista comum de funções e permissões que se aplicam a todos os usuários em um grupo de usuários. Os administradores podem gerenciar grupos de usuários, funções e permissões para controlar o nível de acesso (e, portanto, o nível de segurança) dos usuários do sistema.

Para que os usuários finais acessem o Cisco Unified Communications Portal de Ajuda, você deverá adicionar usuários ao grupo padrão Usuários finais do Cisco Communications Manager.

Tópicos relacionados

Configuração específica do produto, na página 102
Recursos e configuração do Cisco IP Conference Phone, na página 97
Documentação do Cisco Unified Communications Manager, na página 14
Configurar um novo modelo de tecla programável, na página 98

Determinar o endereço MAC do telefone

Para adicionar telefones ao Cisco Unified Communications Manager, você deve determinar o endereço MAC de um telefone.

Procedimento

Efetue uma das seguintes ações:

- No telefone, selecione **Configurações** > **Informações do telefone** e observe o campo Endereço MAC.
- Observe o rótulo MAC na parte de trás do telefone.
- Exiba a página da Web do telefone e clique em **Informações sobre dispositivo**.

Métodos de adição de telefone

Depois de instalar o Telefone IP Cisco, você pode escolher uma das opções a seguir para adicionar telefones ao banco de dados do Cisco Unified Communications Manager.

- Adicionar telefones individualmente com a Administração do Cisco Unified Communications Manager
- Adicionar vários telefones com a Bulk Administration Tool (BAT)
- Registro automático
- BAT e a ferramenta de suporte para telefones registrados automaticamente (TAPS)

Antes de você adicionar telefones individualmente ou com a BAT, você precisa obter o endereço MAC do telefone. Para obter mais informações, consulte Determinar o endereço MAC do telefone, na página 62.

Para obter mais informações sobre a Bulk Administration Tool, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

Adicionar telefones individualmente

Colete o endereço MAC e as informações do telefone que você adicionará ao Cisco Unified Communications Manager.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, escolha **Dispositivo** > **Telefone**.

Etapa 2 Clique em **Adicionar novo**.

Etapa 3 Selecione o tipo de telefone.

Etapa 4 Selecione **Avançar**.

Etapa 5 Complete as informações sobre o telefone, incluindo o endereço MAC.

Para obter instruções completas e informações conceituais sobre o Cisco Unified Communications Manager, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Etapa 6 Selecione **Salvar**.

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

Adicionar telefones com um modelo de telefonia BAT

A Cisco Unified Communications Bulk Administration Tool (BAT) permite executar operações em lote, incluindo o registro de vários telefones.

Para adicionar telefones usando apenas a BAT (não em conjunto com a TAPS), você deve obter o endereço MAC apropriado de cada telefone.

Para obter mais informações sobre o uso da BAT, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, escolha **Administração em massa** > **Telefones** > **Modelo de telefone**.

Etapa 2 Clique em **Adicionar novo**.

Etapa 3 Escolha um Tipo de telefone e clique em **Avançar**.

Etapa 4 Insira os detalhes dos parâmetros específicos do telefone, como Pool de dispositivos, Modelo de tecla do telefone e Perfil de segurança do telefone.

Etapa 5 Clique em **Save** (Salvar).

Etapa 6 Selecione **Dispositivo** > **Telefone** > **Adicionar novo** para adicionar um telefone usando o modelo de telefonia BAT.

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

Adicionar usuários ao Cisco Unified Communications Manager

Você pode exibir e manter informações sobre os usuários registrados no Cisco Unified Communications Manager. O Cisco Unified Communications Manager também permite que cada usuário execute estas tarefas:

- Acessar o diretório corporativo e outros diretórios personalizados de um Telefone IP Cisco.
- Criar um diretório pessoal.
- Configurar números de discagem rápida e encaminhamento de chamadas.

- Inscrever-se em serviços que podem ser acessados de um Telefone IP Cisco.

Procedimento

Etapa 1 Para adicionar usuários individualmente, consulte Adicionar um usuário diretamente ao Cisco Unified Communications Manager, na página 64.

Etapa 2 Para adicionar usuários em lotes, use a Bulk Administration Tool. Esse método também permite que você defina uma senha padrão idêntica para todos os usuários.

Para obter mais informações, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

Adicionar um usuário de um diretório LDAP externo

Se tiver adicionado um usuário a um Diretório LDAP (um diretório que não pertence ao servidor Cisco Unified Communications), você poderá sincronizar imediatamente o diretório LDAP com o Cisco Unified Communications Manager no qual está adicionando o usuário e o telefone do usuário.

Observação Se você não sincronizar o Diretório LDAP com o Cisco Unified Communications Manager imediatamente, a Agenda de sincronização do Diretório LDAP na janela Diretório LDAP determinará quando a próxima sincronização automática será agendada. A sincronização deve ocorrer antes de você associar um novo usuário a um dispositivo.

Procedimento

Etapa 1 Entre na Administração do Cisco Unified Communications Manager.

Etapa 2 Selecione **Sistema** > **LDAP** > **Diretório LDAP**.

Etapa 3 Use **Localizar** para encontrar o diretório LDAP.

Etapa 4 Clique no nome do diretório LDAP.

Etapa 5 Clique em **Executar sincronização completa agora**.

Adicionar um usuário diretamente ao Cisco Unified Communications Manager

Se não estiver usando um diretório LDAP, você poderá adicionar um usuário diretamente com a Administração do Cisco Unified Communications Manager seguindo as etapas abaixo.

Observação Se o LDAP estiver sincronizado, você não poderá adicionar um usuário com a Administração do Cisco Unified Communications Manager.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, escolha **Gerenciamento de usuários** > **Usuário final**.

Etapa 2 Clique em **Adicionar novo**.

Etapa 3 No painel Informações do usuário, insira o seguinte:

- ID de usuário: insira o nome de identificação do usuário final. O Cisco Unified Communications Manager não permite modificar a ID de usuário após sua criação. Você pode usar os seguintes caracteres especiais: =, +, <, >, #,;, \,, “” e espaços em branco. **Exemplo**: johndoe
- Senha e Confirmar senha: insira cinco ou mais caracteres alfanuméricos ou especiais para a senha do usuário final. Você pode usar os seguintes caracteres especiais: =, +, <, >, #, ;, \, , “” e espaços em branco.
- Sobrenome: insira o sobrenome do usuário final. Você pode usar os seguintes caracteres especiais: =, +, <, >, #, ;, \, , “” e espaços em branco. **Exemplo**: doe
- Número de telefone: insira o número de diretório primário do usuário final. Os usuários finais podem ter várias linhas em seus telefones. **Exemplo**: 26640 (número de telefone interno da empresa de John Doe)

Etapa 4 Clique em **Save** (Salvar).

Adicionar um usuário a um Grupo de usuários finais

Para adicionar um usuário ao Grupo de usuários finais do Cisco Unified Communications Manager padrão, execute estas etapas:

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, escolha **Gerenciamento de usuários** > **Configurações do usuário** > **Grupo de controle de acesso**.

A janela para localizar e listar usuários será exibida.

Etapa 2 Insira os critérios de pesquisa apropriados e clique em **Localizar**.

Etapa 3 Selecione o link **Usuários finais do CCM padrão** link. A janela de configuração do grupo de usuários para os usuários finais do CCM padrão aparecerá.

Etapa 4 Selecione **Adicionar usuários finais a grupo**. A janela para localizar e listar usuários será exibida.

Etapa 5 Use as caixas da lista suspensa Procurar usuário para localizar os usuários que você quer adicionar e clique em **Localizar**.

A lista de usuários que correspondem aos seus critérios de pesquisa será exibida.

Etapa 6 Na lista de registros exibida, clique na caixa de seleção ao lado dos usuários que você quer adicionar a esse grupo de usuários. Se a lista for longa, use os links no final dela para ver mais resultados.

Observação A lista de resultados da pesquisa não exibe os usuários que já pertencem ao grupo de usuários.

Etapa 7 Escolha **Adicionar selecionado**.

Associar telefones a usuários

Você associa telefones a usuários na janela Usuário final do Cisco Unified Communications Manager.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, escolha **Gerenciamento de usuários** > **Usuário final**.

A janela para localizar e listar usuários será exibida.

Etapa 2 Insira os critérios de pesquisa apropriados e clique em **Localizar**.

Etapa 3 Na lista de registros que aparecem, selecione o link para o usuário.

Etapa 4 Selecione **Associação do dispositivo**.

A janela Associação do dispositivo do usuário é exibida.

Etapa 5 Insira os critérios de pesquisa apropriados e clique em **Localizar**.

Etapa 6 Escolha o dispositivo que você deseja associar ao usuário marcando a caixa à esquerda do dispositivo.

Etapa 7 Escolha **Salvar selecionados/alterações** para associar o dispositivo ao usuário.

Etapa 8 Na lista suspensa Links relacionados no canto superior direito da janela, selecione **Voltar para usuário** e clique em **Ir**.

A janela de Configuração de usuários finais é exibida e os dispositivos associados que você escolheu são exibidos no painel Dispositivos controlados.

Etapa 9 Escolha **Salvar selecionados/alterações**.

SRST (Survivable Remote Site Telephony)

A SRST (Surviveable Remote Site Telephony) garante que as funções básicas do telefone permaneçam acessíveis quando as comunicações com o Cisco Unified Communications Manager de controle são interrompidas. Nesse cenário, o telefone pode manter uma chamada em andamento ativa e o usuário pode acessar um subconjunto dos recursos disponíveis. Quando ocorre o failover, o usuário recebe uma mensagem de alerta no telefone.

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

A tabela a seguir descreve a disponibilidade dos recursos durante o failover.

Tabela 14: Suporte ao recurso SRST

Recurso	Com suporte	Notas
NovaCh.	Sim	
Terminar chamada	Sim	
Discar novamente	Sim	
Resposta	Sim	
Espera	Sim	
Continuar	Sim	
Conferência	Sim	Apenas 3 vias e apenas combinação local.
Lista de conferência	Não	
Transferir	Sim	Apenas consulta.
Transferência para chamadas ativas (transferência direta)	Não	
Resposta automática	Sim	
Chamada em espera	Sim	
ID do chamador	Sim	
Apresentação de sessão unificada	Sim	Conferência é o único recurso aceito devido a outras limitações de recurso.
Correio de voz	Sim	O Correio de voz não será sincronizado com outros usuários no cluster do Cisco Unified Communications Manager.

Recurso	Com suporte	Notas
Encaminhar todas as chamadas	Sim	O estado de encaminhamento está disponível somente no telefone que define o encaminhamento, pois não há ocorrência de linha compartilhada no modo SRST. As configurações Encaminhar todas as chamadas não são preservadas no failover do Cisco Unified Communications Manager para o SRST ou do failback do SRST para o Communications Manager. Qualquer configuração original Encaminhar todas as chamadas ainda ativa no Communications Manager deverá ser indicada quando o dispositivo se reconectar ao Communications Manager após o failover.
Discagem rápida	Sim	
Para o correio de voz (DesvIme)	Não	A tecla programável DesvIme não é exibida.
Filtros de linha	Parcial	As linhas são suportadas, mas não podem ser compartilhadas.
Monitoramento de estacionamento	Não	A tecla programável Estacionar não é exibida.
Indicação aprimorada de mensagem em espera	Sim	Os emblemas de contagem de mensagens são exibidos na tela do telefone.
Estac. chamada direcionado	Não	A tecla programável não é exibida.
Reversão de espera	Sim	
Espera remota	Não	As chamadas são exibidas como chamadas em espera local.
Meet Me	Não	A tecla programável Meet Me não é exibida.
Captura	Sim	
GrupoCap	Não	A tecla programável não é exibida.
OutrCap	Não	A tecla programável não é exibida.
ID de chamada maliciosa	Sim	
QRT	Sim	
Grupo de busca	Não	A tecla programável não é exibida.
Mobilidade	Não	A tecla programável não é exibida.
Privacidade	Não	A tecla programável não é exibida.

Recurso	Com suporte	Notas
Retorno de Chamada	Não	A tecla programável Retorno de chamada não é exibida.
URL de serviço	Sim	Não é exibida a chave de linha programável com uma URL de serviço atribuída.

CAPÍTULO 6

Gerenciamento do Portal de Ajuda

Visão geral do Portal de Ajuda

No Cisco Unified Communications Self Care Portal, os usuários podem personalizar e controlar recursos e configurações do telefone.

Como administrador, você controla o acesso ao Portal de Ajuda. Você também deve fornecer informações a seus usuários para que eles possam acessar o Portal de Ajuda.

Para que um usuário possa acessar o Cisco Unified Communications Self Care Portal, você precisa usar a Administração do Cisco Unified Communications Manager para adicioná-lo a um grupo padrão de usuários finais do Cisco Unified Communications Manager.

Você também deve fornecer as seguinte informações aos usuários finais sobre o Portal de Ajuda:

- O URL para acessar o aplicativo. Esse URL é:

  `https://<server_name:portnumber>/ucmuser/`, onde server_name é o host no qual o servidor Web está instalado e portnumber é o número da porta nesse host.

- Um ID de usuário e uma senha padrão para acessar o aplicativo.

- Uma visão geral das tarefas que os usuários podem realizar com o portal.

Essas configurações correspondem aos valores inseridos durante a adição do usuário ao Cisco Unified Communications Manager.

Para obter mais informações, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

Configurar o acesso do usuário ao Portal de Ajuda

Para que um usuário possa acessar o Portal de Ajuda, você precisa autorizar o acesso.

Procedimento

Etapa 1 Em Administração do Cisco Unified Communications Manager, selecione **Gerenciamento de usuários** > **Usuário final**.

Etapa 2 Pesquise o usuário.

Etapa 3 Clique no link ID de usuário.

Etapa 4 Garanta que o usuário tenha uma senha e um PIN configurados.

Etapa 5 Na seção Informações de permissão, assegure-se de que a lista Grupos inclua **Usuários finais do CCM padrão**.

Etapa 6 Selecione **Salvar**.

Personalizar a exibição do Portal de Ajuda

A maioria das opções é exibida no Portal de Ajuda. No entanto, você deve configurar as seguintes opções usando as definições de configuração dos Parâmetros corporativos na Administração do Cisco Unified Communications Manager:

- Mostrar configurações de toque
- Mostrar configurações do rótulo da linha

Observação As configurações se aplicam a todas as páginas do Portal de Ajuda em seu site.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, selecione **Sistema** > **Parâmetros corporativos**.

Etapa 2 Na área Portal de Ajuda, defina o campo **Servidor padrão do Portal de Ajuda**.

Etapa 3 Ative ou desative os parâmetros que os usuários podem acessar no portal.

Etapa 4 Selecione **Salvar**.

PARTE III

Administração do Telefone IP Cisco de conferência

CAPÍTULO 7

Segurança do Cisco IP Conference Phone

Visão geral da segurança do Telefone IP Cisco

Os recursos de segurança protegem contra várias ameaças, incluindo ameaças à identidade do telefone e aos dados. Os recursos estabelecem e mantêm fluxos de comunicação autenticados entre o telefone e o servidor Cisco Unified Communications Manager, além de garantir que o telefone use apenas arquivos assinados digitalmente.

O Cisco Unified Communications Manager versão 8.5(1) e posterior inclui a opção Segurança por padrão, que fornece os seguintes recursos de segurança para Telefones IP Cisco sem executar o cliente CTL:

- Assinatura dos arquivos de configuração do telefone
- Criptografia dos arquivos de configuração do telefone
- HTTPS com Tomcat e outros serviços Web

Observação Os recursos de mídia e sinalização segura ainda exigem que você execute o cliente CTL e use eTokens físicos.

Para obter mais informações sobre os recursos de segurança, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Um LSC (Locally Significant Certificate) é instalado nos telefones depois que você executa as tarefas necessárias associadas à função de proxy de autoridade de certificação (CAPF). Você pode usar a Administração do Cisco Unified Communications Manager para configurar um LSC. Para obter mais informações, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Um LSC não pode ser usado como o certificado do usuário para EAP-TLS com autenticação WLAN.

Opcionalmente, você pode iniciar a instalação de um LSC no menu Configuração de segurança do telefone. Este menu também permite atualizar ou remover um LSC.

O Telefone IP Cisco de conferência 8832 está em conformidade com a norma FIPS (Federal Information Processing Standard). Para funcionar corretamente, o modo FIPS requer uma chave RSA de 2048 bits ou

mais. Se o certificado do servidor RSA não tiver 2048 bits ou mais, o telefone não será registrado no Cisco Unified Communications Manager e a mensagem `Falha ao registrar o telefone. O tamanho da chave do certificado não é compatível com FIPS` é exibida em mensagens de status do telefone.

Você não pode usar chaves privadas (LSC ou MIC) no modo FIPS.

Se o telefone tiver uma chave LSC existente menor do que 2048 bits, você precisa atualizar o tamanho da chave LSC para 2048 bits ou mais antes de ativar FIPS.

Tópicos relacionados

Configurar um certificado localmente significativo, na página 79
Documentação do Cisco Unified Communications Manager, na página 14

Aprimoramentos de segurança para sua rede de telefonia

Você pode ativar o Cisco Unified Communications Manager 11.5(1) e 12.0(1) para operar em um ambiente de segurança avançada. Com esses aprimoramentos, sua rede de telefonia opera sob um conjunto de controles rígidos de gerenciamento de segurança e riscos para proteger você e seus usuários.

O Cisco Unified Communications Manager 12.5(1) não é compatível com um ambiente de segurança optimizada. Desative FIPS antes de atualizar para o Cisco Unified Communications Manager 12.5(1) ou seu TFTP e outros serviços não funcionará corretamente.

O ambiente de segurança optimizada inclui os seguintes recursos:

- Autenticação de pesquisa de contatos.
- O TCP como o protocolo padrão para o registro em log de auditoria remota.
- Modo FIPS.
- Uma política de credenciais aprimorada.
- Suporte à família SHA-2 de hashes para assinaturas digitais.
- Suporte para uma chave RSA de 512 e 4096 bits.

Com o Cisco Unified Communications Manager versão 14.0 e o firmware do Telefone IP Cisco versão 14.0 e posterior, os telefones suportam autenticação SIP OAuth.

O OAuth é compatível com proxy trivial File Transfer Protocol (TFTP) com Cisco Unified Communications Managerversão 14.0(1)SU1 ou posterior e Cisco IP Phone firmware versão 14.1(1). Proxy TFTP e OAuth para proxy TFTP não são compatíveis com o Mobile Remote Access (MRA).

Para obter informações adicionais sobre a segurança, consulte o seguinte:

- *Guia de configuração do sistema do Cisco Unified Communications Manager, versão 12.0(1)* ou posterior (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html).
- *Guia de segurança para o Cisco Unified Communications Manager* (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html)

- SIP OAuth: *Guia de configuração de recursos do Cisco Unified Communications Manager* (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html)

Observação O Telefone IP Cisco só pode armazenar um número limitado de arquivos Identity Trust List (ITL). Os arquivos ITL não podem exceder o limite de 64K no limite, por isso, limite o número de arquivos que o Cisco Unified Communications Manager envia para o telefone.

Recursos de segurança suportados

Os recursos de segurança protegem contra várias ameaças, incluindo ameaças à identidade do telefone e aos dados. Os recursos estabelecem e mantêm fluxos de comunicação autenticados entre o telefone e o servidor Cisco Unified Communications Manager, além de garantir que o telefone use apenas arquivos assinados digitalmente.

O Cisco Unified Communications Manager versão 8.5(1) e posterior inclui a opção Segurança por padrão, que fornece os seguintes recursos de segurança para Telefones IP Cisco sem executar o cliente CTL:

- Assinatura dos arquivos de configuração do telefone
- Criptografia dos arquivos de configuração do telefone
- HTTPS com Tomcat e outros serviços Web

Observação Os recursos de mídia e sinalização segura ainda exigem que você execute o cliente CTL e use eTokens físicos.

Implementar a segurança no sistema Cisco Unified Communications Manager impede o roubo de identidade do telefone e do servidor Cisco Unified Communications Manager, impede a violação de dados e impede a adulteração da sinalização de chamadas do fluxo de mídia.

Para minimizar essas ameaças, a rede de telefonia IP da Cisco estabelece e mantém fluxos de comunicação seguros (criptografados) entre um telefone e o servidor, assina digitalmente os arquivos antes de serem transferidos para um telefone e criptografa fluxos de mídia e a sinalização de chamadas entre Telefones IP Cisco.

Um LSC (Locally Significant Certificate) é instalado nos telefones depois que você executa as tarefas necessárias associadas à função de proxy de autoridade de certificação (CAPF). Você pode usar a Administração do Cisco Unified Communications Manager para configurar um LSC, conforme descrito no Guia de segurança do Cisco Unified Communications Manager. Opcionalmente, você pode iniciar a instalação de um LSC no menu Configuração de segurança do telefone. Este menu também permite atualizar ou remover um LSC.

Um LSC não pode ser usado como o certificado do usuário para EAP-TLS com autenticação WLAN.

Os telefones usam o perfil de segurança do telefone, que define se o dispositivo está seguro ou não. Para obter informações sobre como aplicar o perfil de segurança ao telefone, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Se você definir configurações de segurança na Administração do Cisco Unified Communications Manager, o arquivo de configuração do telefone conterá informações confidenciais. Para garantir a privacidade de um

arquivo de configuração, você deve configurá-lo para criptografia. Para obter informações detalhadas, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Implementar a segurança no sistema Cisco Unified Communications Manager impede o roubo de identidade do telefone e do servidor Cisco Unified Communications Manager, impede a violação de dados e impede a adulteração da sinalização de chamadas do fluxo de mídia.

A tabela a seguir fornece uma visão geral dos recursos de segurança que são compatíveis com o Telefone IP Cisco de conferência 8832. Para obter mais informações sobre esses recursos, o Cisco Unified Communications Manager e a segurança do Telefone IP Cisco, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Tabela 15: Visão geral dos recursos de segurança

Recurso	Descrição
Autenticação de imagem	Arquivos binários assinados (com a extensão .sbn) impedem a telefone. A falsificação com a imagem causa falha no processo
Instalação de certificado no site do cliente	Cada telefone exige um certificado exclusivo para autenticaçã fabricante), mas para segurança adicional, você pode especific certificado seja instalado usando a CAPF (Função de proxy de (Certificado localmente significativo) no menu Configuração d
Autenticação do dispositivo	Ocorre entre o servidor Cisco Unified Communications Manag Determina se uma conexão segura entre o telefone e um Cisco caminho de sinalização seguro entre as entidades usando o proto a menos que possa autenticá-los.
Autenticação de arquivo	Valida arquivos assinados digitalmente baixados pelo telefone. ocorreu depois da criação do arquivo. Os arquivos que falham rejeita tais arquivos sem outro processamento.
Autenticação de sinalização	Usa o protocolo TLS para confirmar que não houve falsificaçã
Certificado instalado pelo fabricante	Cada telefone contém um MIC (certificado instalado pelo fabri de identidade exclusiva permanente do telefone e permite que
Referência SRST segura	Depois de configurar uma referência SRST para segurança e re Communications Manager, o servidor TFTP adiciona o certific telefone seguro usa uma conexão TLS para interagir com o rot
Criptografia de mídia	Usa SRTP para garantir que os fluxos de mídia entre dispositiv receba e leia os dados. Inclui criação de um par de chaves prim protegendo a entrega das chaves enquanto são transportadas.
CAPF (Função de proxy de autoridade de certificação)	Implementa partes do procedimento de geração do certificado geração de chave e instalação do certificado. A CAPF pode ser co pelo cliente em nome do telefone ou pode ser configurada para
Perfis de segurança	Define se o telefone não é seguro e se está autenticado ou cript
Arquivos de configuração criptografados	Permite que você assegure a privacidade dos arquivos de confi

Recurso	Descrição
Desativação opcional da funcionalidade do servidor Web para um telefone	Você pode impedir o acesso à página da Web de um telefon
Proteção do telefone	Opções de segurança adicionais, que você controla na Adm • Desativar acesso a páginas da Web de um telefone **Observação** Você pode visualizar as configurações atuais d menu Configuração do telefone.
Autenticação 802.1X	O telefone pode usar autenticação 802.1X para solicitar e c
Criptografia AES 256	Quando conectados ao Cisco Unified Communications Ma para TLS e SIP para sinalização e criptografia de mídia. Iss baseadas em AES-256 em conformidade com os padrões SH Processing Standards). As novas cifras são: • Para conexões TLS: • TLS_ECDHE_RSA_WITH_AES_256_GCM_S • TLS_ECDHE_RSA_WITH_AES_128_GCM_S • Para sRTP: • AEAD_AES_256_GCM • AEAD_AES_128_GCM Para obter mais informações, consulte a documentação do
Certificados Elliptic Curve Digital Signature Algorithm (ECDSA)	Como parte da certificação Common Criteria (CC), o Cisco Isso afeta todos os produtos de Voice Operating System (V

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

Configurar um certificado localmente significativo

Essa tarefa se aplica à configuração de um LSC com o método de cadeia de autenticação.

Antes de Iniciar

Verifique se configurações de segurança apropriadas do Cisco Unified Communications Manager e da CAPF (Função de proxy de autoridade de certificação) foram concluídas:

- O arquivo CTL ou ITL tem um certificado CAPF.
- Na Administração do sistema operacional do Cisco Unified Communications, verifique se o certificado CAPF está instalado.
- A CAPF está em execução e foi configurada.

Para obter mais informações sobre essas configurações, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Procedimento

Etapa 1 Obtenha o código de autenticação da CAPF que foi definido quando a CAPF foi configurada.

Etapa 2 No telefone, escolha **Configurações**.

Etapa 3 Selecione **Configurações do administrador** > **Configurações de segurança**.

Observação Você pode controlar o acesso ao menu Configurações usando o campo Acesso às configurações na janela Configuração do telefone da Administração do Cisco Unified Communications Manager.

Etapa 4 Escolha **LSC** e pressione **Selecionar** ou **Atualizar**.

O telefone solicita uma string de autenticação.

Etapa 5 Insira o código de autenticação e pressione **Enviar**.

O telefone começa a instalar, atualizar ou remover o LSC, dependendo de como a CAPF foi configurada. Durante o procedimento, uma série de mensagens aparecerá no campo Opção de LSC no menu Configuração de segurança para que você possa monitorar o andamento. Quando o procedimento estiver concluído, será exibida a mensagem Instalado ou Não instalado no telefone.

O processo de instalação, atualização ou remoção do LSC pode demorar bastante para ser concluído.

Quando o procedimento de instalação do telefone for bem-sucedido, a mensagem `Instalado` será exibida. Se o telefone exibir `Não instalado`, a string de autorização pode estar incorreta ou a atualização do telefone pode não estar ativada. Se a operação de CAPF excluir o LSC, o telefone exibirá `Não instalado` para indicar que a operação foi bem-sucedida. O servidor CAPF registra em log as mensagens de erro. Consulte a documentação do servidor CAPF para localizar os logs e entender o significado das mensagens de erro.

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

Ativar modo FIPS

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, selecione **Dispositivo** > **Telefone** e localize o telefone.

Etapa 2 Navegue até a área Configuração específica do produto.

Etapa 3 Defina o campo **Modo FIPS** como Ativado.

Etapa 4 Selecione **Aplicar config.**

Etapa 5 Selecione **Salvar**.

Etapa 6 Reinicie o telefone.

Segurança da chamada telefônica

Quando a segurança é implementada para um telefone, você pode identificar chamadas telefônicas seguras por ícones na tela do telefone. Também será possível determinar se o telefone conectado está seguro e protegido se um tom de segurança for tocado no início da chamada.

Em uma chamada segura, todos os fluxos de mídia e sinalização de chamada são criptografados. Uma chamada segura oferece um alto nível de segurança, fornecendo integridade e privacidade à chamada. Quando uma chamada em andamento é criptografada, o ícone de andamento da chamada à direita do temporizador de duração da chamada na tela do telefone muda para o seguinte ícone: 

Observação Se a chamada for roteada por meio de segmentos de chamada não IP, por exemplo, o PSTN, ela poderá não ser segura, mesmo que esteja criptografada na rede IP e tenha um ícone de cadeado associado a ela.

Em uma chamada segura, um tom de segurança é tocado no início para indicar que o outro telefone conectado também está recebendo e transmitindo áudio seguro. Se a chamada se conectar a um telefone não seguro, o tom de segurança não será tocado.

Observação A chamada segura é permitida entre dois telefones. A conferência segura, o Cisco Extension Mobility e as linhas compartilhadas podem ser configurados por um recurso de conferência seguro.

Quando um telefone é configurado como seguro (criptografado e confiável) no Cisco Unified Communications Manager, ele pode receber o status de "protegido". Depois disso, se desejado, o telefone protegido pode ser configurado para tocar um tom indicativo no início de uma chamada:

- Dispositivo protegido: para alterar o status de um telefone seguro para protegido, marque a caixa de seleção Dispositivo protegido na janela Configuração do telefone na Administração do Cisco Unified Communications Manager (**Dispositivo** > **Telefone**).
- Tocar tom indicativo de seguro: para permitir que o telefone protegido toque um tom indicativo de seguro ou não seguro, defina a configuração Play Secure Indication Tone (Tocar tom indicativo de seguro) como Verdadeiro. Por padrão, a opção Tocar tom indicativo de seguro é definida como Falso. Você define essa opção na Administração do Cisco Unified Communications Manager (**Sistema** > **Parâmetros de serviço**). Selecione o servidor e, em seguida, o serviço do Unified Communications Manager. Na janela Configuração de parâmetro de serviço, selecione a opção na área Recurso - Tom de seguro. O padrão é Falso.

Identificação de chamada de conferência segura

Você pode iniciar uma chamada de conferência segura e monitorar o nível de segurança dos participantes. Uma chamada de conferência segura é estabelecida por este processo:

1. Um usuário inicia a conferência de um telefone seguro.
2. O Cisco Unified Communications Manager atribui um recurso de conferência seguro à chamada.
3. Conforme os participantes são adicionados, o Cisco Unified Communications Manager verifica o modo de segurança de cada telefone e mantém o nível seguro para a conferência.

4. O telefone exibe o nível de segurança da chamada de conferência. Uma conferência segura exibe o ícone de proteção à direita da **Conferência** na tela do telefone.

Observação A chamada segura é permitida entre dois telefones. Em telefones protegidos, alguns recursos, como a chamada de conferência, as linhas compartilhadas e o Extension Mobility, não estão disponíveis quando a chamada segura é configurada.

A tabela a seguir fornece informações sobre alterações nos níveis de segurança da conferência, de acordo com o nível de segurança do telefone do iniciador, os níveis de segurança dos participantes e a disponibilidade dos recursos de conferência seguros.

Tabela 16: Restrições de segurança com chamadas de conferência

Nível de segurança do telefone do iniciador	Recurso usado	Nível de segurança dos participantes	Resultados da ação
Não seguro	Conferência	Seguro	Recurso de conferência não seguro Conferência não segura
Seguro	Conferência	Pelo menos um membro não seguro.	Recurso de conferência seguro Conferência não segura
Seguro	Conferência	Seguro	Recurso de conferência seguro Conferência de nível criptografado seguro
Não seguro	Meet Me	Nível mínimo de segurança é criptografado.	O iniciador recebe a mensagem `Does not m Security Level, call rejected ( atende ao Nível de segurança, c rejeitada).`
Seguro	Meet Me	Nível mínimo de segurança é não seguro.	Recurso de conferência seguro A conferência aceita todas as chamadas.

Identificação de chamada telefônica segura

Uma chamada segura é estabelecida quando seu telefone, assim como o telefone na outra ponta, é configurado para chamada segura. O outro telefone pode estar na mesma rede IP Cisco ou em uma rede fora da rede IP. As chamadas seguras podem ser feitas apenas entre dois telefones. As chamadas de conferência devem dar suporte à chamada segura após a configuração do recurso de conferência protegida.

Uma chamada segura é estabelecida usando este processo:

1. Um usuário inicia a chamada de um telefone seguro (modo de segurança protegido).
2. O ícone de proteção é exibido na tela do telefone. Esse ícone indica que o telefone está configurado para chamadas seguras, mas isso não significa que o outro telefone conectado também está protegido.

3. O usuário ouve um tom de segurança se a chamada se conectar a outro telefone protegido, indicando que ambas as extremidades da conversa estão criptografadas e protegidas. Se a chamada se conectar a um telefone não seguro, o usuário não ouvirá o tom de segurança.

Observação A chamada segura é permitida entre dois telefones. Em telefones protegidos, alguns recursos, como a chamada de conferência, as linhas compartilhadas e o Extension Mobility, não estão disponíveis quando a chamada segura é configurada.

Somente os telefones protegidos tocam esses tons indicativos de telefones seguros ou não seguros. Os telefones não protegidos nunca tocam tons. Se o status geral da chamada mudar durante a chamada, o tom indicativo também mudará e o telefone protegido tocará o tom apropriado.

Um telefone protegido toca um tom ou não sob estas circunstâncias:

- Quando a opção Play Secure Indication Tone (Tocar tom indicativo de seguro) estiver ativada:
  - Quando uma mídia segura de ponta a ponta for estabelecida e o status da chamada for seguro, o telefone tocará o tom indicativo seguro (três bipes longos com pausas).
  - Quando uma mídia não segura de ponta a ponta for estabelecida e o status da chamada for não seguro, o telefone tocará o tom indicativo não seguro (seis bipes curtos com pausas rápidas).

Se a opção Play Secure Indication Tone (Tocar tom indicativo de seguro) estiver desativada, nenhum tom será tocado.

Fornecer criptografia para intercalação

O Cisco Unified Communications Manager verifica o status de segurança do telefone quando são estabelecidas conferências e muda a indicação de segurança da conferência ou bloqueia a conclusão da chamada para manter a segurança e a integridade do sistema.

Um usuário não pode entrar em uma chamada criptografada se o telefone usado para isso não está configurado para criptografia. Quando a intercalação falha nesse caso, é reproduzido um tom de reordenação (sinal de ocupado) no telefone em que a intercalação foi iniciada.

Se o telefone do iniciador estiver configurado para criptografia, o iniciador da intercalação poderá entrar em uma chamada não segura do telefone criptografado. Depois que acontece a intercalação, o Cisco Unified Communications Manager classifica a chamada como não segura.

Se o telefone do iniciador estiver configurado para criptografia, o iniciador da intercalação poderá entrar em uma chamada criptografada e o telefone indicará que a chamada está criptografada.

Segurança na WLAN

Como todos os dispositivos de WLAN que estão no intervalo podem receber todo o tráfego da WLAN, proteger a comunicação por voz é algo essencial nessas redes. Para garantir que intrusos não manipulem nem interceptem o tráfego de voz, a arquitetura do Cisco SAFE Security oferece suporte para os APs do Telefone IP Cisco e do Cisco Aironet. Para obter mais informações sobre a segurança em redes, consulte http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html.

A solução de telefonia IP sem fio da Cisco fornece segurança de rede sem fio que impede inícios de sessão não autorizados e comunicações comprometidas usando os seguintes métodos de autenticação aceitos pelo Telefone IP sem fio Cisco:

- Autenticação aberta: qualquer dispositivo sem fio pode solicitar autenticação em um sistema aberto. O AP que recebe a solicitação pode conceder autenticação para qualquer solicitante ou apenas para solicitantes encontrados em uma lista de usuários. A comunicação entre o dispositivo sem fio e o AP pode não estar criptografada ou os dispositivos podem usar chaves WEP para fornecer segurança. Os dispositivos que usam WEP só tentam se autenticar com um ponto de acesso que está usando WEP.
- Autenticação EAP-FAST: essa arquitetura de segurança de cliente-servidor criptografa transações EAP dentro de um túnel TLS entre o AP e o servidor RADIUS, como o Cisco Access Control Server (ACS).

  O túnel TLS usa credenciais de acesso protegido (PACs) para autenticação entre o cliente (telefone) e o servidor RADIUS. O servidor envia um ID de autoridade (AID) para o cliente (telefone), que por sua vez seleciona a PAC apropriada. O cliente (telefone) retorna uma PAC-Opaque para o servidor RADIUS. O servidor descriptografa a PAC com a chave primária. Agora s dois pontos de extremidade contêm a chave PAC, e um túnel TLS é criado. O EAP-FAST oferece suporte para provisionamento automático de PAC, mas você precisa ativá-lo no servidor RADIUS.

Observação No Cisco ACS, por padrão, a PAC expira em uma semana. Se a PAC do telefone tiver expirado, a autenticação no servidor RADIUS será mais demorada enquanto o telefone obtém uma nova PAC. Para evitar atrasos no provisionamento da PAC, defina o período de expiração para 90 dias ou mais no servidor ACS ou RADIUS.

- Autenticação Extensible Authentication Protocol-Transport Layer Security (EAP-TLS): o EAP-TLS exige um certificado de cliente para autenticação e acesso à rede. Para EAP-TLS com fio, o certificado de cliente pode ser o MIC ou LSC do telefone. O LSC é o certificado de autenticação de cliente recomendado para EAP-TLS com fio.
- Protocolo de autenticação extensível protegido (PEAP): esquema de autenticação mútua baseada em senha e proprietário da Cisco entre o cliente (telefone) e um servidor RADIUS. O Telefone IP Cisco pode usar PEAP para autenticação na rede sem fio. Somente o PEAP MSCHAPV2 é compatível. O PEAP-GTC não é compatível.

Os seguintes esquemas de autenticação usam o servidor RADIUS para gerenciar chaves de autenticação:

- WPA/WPA2: usa informações do servidor RADIUS para gerar chaves exclusivas para autenticação. Como essas chaves são geradas no servidor RADIUS centralizado, o WPA/WPA2 oferece que mais segurança do que as chaves pré-compartilhadas WPA que são armazenadas no AP e no telefone.
- Roaming rápido e seguro: usa informações do servidor RADIUS e de um servidor de domínio sem fio (WDS) para gerenciar e autenticar as chaves. O WDS cria um cache de credenciais de segurança para dispositivos cliente ativados para o CCKM, para uma nova autenticação rápida e segura. O Telefone IP Cisco série 8800 oferece suporte para 802.11r (FT). 11r (FT) e CCKM são compatíveis para permitir roaming rápido e seguro. Mas a Cisco recomenda altamente a utilização do método pelo ar 802.11r (FT).

Com o WPA/WPA2 e o CCKM, as chaves de criptografia não são inseridas no telefone, mas derivadas automaticamente entre o AP e o telefone. Porém, o nome do usuário EAP e a senha que são usados para autenticação devem ser inseridos em cada telefone.

Para garantir que o tráfego de voz esteja seguro, o Telefone IP Cisco oferece suporte para WEP, TKIP e padrões de criptografia avançada (AES) para criptografia. Quando esses mecanismos são usados para criptografia, tanto os pacotes SIP de sinalização quanto os pacotes RTP (Real-Time Transport Protocol) de voz são criptografados entre o AP e o Telefone IP Cisco.

WEP

Com o uso do WEP na rede sem fio, a autenticação acontece no AP usando a autenticação de chave aberta ou de chave compartilhada. A chave WEP configurada no telefone deve corresponder à chave WEP que está configurada no AP para que as conexões sejam bem-sucedidas. O Telefone IP Cisco oferece suporte para chaves WEP que usam criptografia de 40 bits ou uma criptografia de 128 bits e permanecem estáticas no telefone e no AP.

A autenticação EAP e do CCKM pode usar chaves WEP para criptografia. O servidor RADIUS gerencia a chave WEP e passa uma chave exclusiva para o AP depois da autenticação para criptografar todos os pacotes de voz; consequentemente, essas chaves WEP podem mudar a cada autenticação.

TKIP

WPA e CCKM usam criptografia TKIP, que tem diversas melhorias em relação ao WEP. TKIP fornece vetores de inicialização (IVs) mais longos e criptografia de chave por pacote que reforçam a criptografia. Além disso, uma verificação de integridade das mensagens (MIC) garante que os pacotes criptografados não estejam sendo alterados. O TKIP remove a capacidade de previsão do WEP que ajuda os invasores a decifrar a chave WEP.

AES

Um método de criptografia usado para autenticação WPA2. Esse padrão nacional de criptografia usa um algoritmo simétrico que tem a mesma chave para criptografia e descriptografia. O AES usa criptografia CBC de 128 bits, que suporta tamanhos de chave de pelo menos 128, 192 e 256 bits. O Telefone IP Cisco suporta um tamanho de chave de 256 bits.

Observação O Telefone IP Cisco não oferece suporte para o protocolo de integridade de chave Cisco (CKIP) com CMIC.

Esquemas de autenticação e criptografia são configuradas na LAN sem fio. As VLANs configuradas na rede e nos APs e especificam diferentes combinações de autenticação e criptografia. Um SSID é associado a uma VLAN e ao esquema de autenticação e criptografia específico. Para que os dispositivos cliente sem fio sejam autenticados corretamente, você deve configurar os mesmos SSIDs com os esquemas de autenticação e criptografia deles nos APs e no Telefone IP Cisco.

Alguns esquemas de autenticação exigem tipos específicos de criptografia. Com a autenticação aberta, você pode usar WEP estático para criptografia para aumentar a segurança. Mas se você estiver usando autenticação de chave compartilhada, deve configurar o WEP estático para criptografia e uma chave WEP no telefone.

Observação

- Quando você usa uma chave pré-compartilhada WPA ou WPA2, a chave pré-compartilhada deve ser definida de forma estática no telefone. Essas chaves devem coincidir com as chaves que estão no AP.
- O Telefone IP Cisco não oferece suporte para negociação automática de EAP; para usar o modo EAP-FAST, você deve especificá-lo.

A tabela a seguir mostra uma lista de esquemas de autenticação e criptografia configurados nos APs do Cisco Aironet que são suportados pelo Telefone IP Cisco. A tabela mostra a opção de configuração de rede para o telefone que corresponde à configuração do AP.

Tabela 17: Esquemas de autenticação e criptografia

Configuração do Telefone IP Cisco	Configuração do AP			
Modo de segurança	Segurança	Gerenciamento de tecla	Criptografia	Roaming rápido
Nenhuma	Nenhuma	Nenhuma	Nenhuma	N/A
WEP	WEP estático	Static	WEP	N/A
PSK	PSK	WPA	TKIP	Nenhuma
		WPA2	AES	FT
EAP-FAST	EAP-FAST	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
EAP-TLS	EAP-TLS	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
PEAP-MSCHAPV2	PEAP-MSCHAPV2	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM

Para obter mais informações sobre como configurar esquemas de autenticação e criptografia em APs, consulte o *Cisco Aironet Configuration Guide* do seu modelo e versão no seguinte URL:

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

Segurança da LAN sem fio

Os telefones Cisco compatíveis com Wi-Fi têm mais requisitos de segurança e exigem configuração extra. Essas etapas extras incluem instalar certificados e configurar a segurança nos telefones e no Cisco Unified Communications Manager.

Para obter mais informações, consulte o *Guia de segurança do Cisco Unified Communications Manager*.

Página de administração do Telefone IP Cisco

Os telefones Cisco que oferecem suporte de Wi-Fi possuem páginas da Web especiais diferentes das páginas de outros telefones. Você utiliza essas páginas da Web especiais para configuração de segurança do telefone quando o SCEP (Simple Certificate Enrollment Protocol) não estiver disponível. Use essas páginas para instalar manualmente certificados de segurança em um telefone, para baixar um certificado de segurança ou para configurar manualmente a data e hora do telefone.

Essas páginas da Web também mostram as mesmas informações que você vê em páginas da Web de outros telefones, incluindo informações do dispositivo, configuração de rede, registros e informações estatísticas.

Configurar a página de administração do telefone

A página da Web de administração é ativada quando o telefone é enviado pela fábrica, e a senha é definida como Cisco. Mas, se um telefone for registrado no Cisco Unified Communications Manager, será preciso ativar a página da Web de administração e configurar uma nova senha.

Ative essa página da Web e defina as credenciais de acesso antes de usar a página da Web pela primeira vez depois que o telefone for registrado.

Uma vez ativada, a página da Web de administração estará acessível na porta HTTPS 8443 (`https://x.x.x.x:8443`, onde x.x.x.x é o endereço IP do telefone).

Antes de Iniciar

Defina uma senha antes de ativar a página da Web de administração. A senha pode ser formada por qualquer combinação de letras ou números, mas deve conter entre 8 e 127 caracteres.

Seu nome de usuário é permanentemente definido como admin.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, selecione **Dispositivo** > **Telefone**.

Etapa 2 Localize seu telefone.

Etapa 3 Na seção **Layout da configuração específica do produto**, defina **Administrador Web** como **Ativado**.

Etapa 4 No campo **Senha do administrador**, insira uma senha.

Etapa 5 Selecione **Salvar** e clique em **OK**.

Etapa 6 Selecione **Aplicar config.** e clique em **OK**.

Etapa 7 Reinicie o telefone.

Acessar a página da Web de administração do telefone

Quando você quiser acessar as páginas da Web de administração, terá de especificar a porta de administração.

Procedimento

Etapa 1 Obtenha o endereço IP do telefone:

- Na Administração do Cisco Unified Communications Manager, selecione **Dispositivo** > **Telefone** e localize o telefone. Os telefones registrados no Cisco Unified Communications Manager exibem o endereço IP na janela **Localizar e listar telefones** e na parte superior da janela **Configuração do telefone**.

Etapa 2 Abra um navegador da Web e insira o seguinte URL, onde *endereço_IP* é o endereço IP do Telefone IP Cisco:

`https://<IP_address>:8443`

Etapa 3 Digite a senha no campo Senha.

Etapa 4 Clique em **Enviar**.

Instalar um certificado de usuário na página da Web de administração do telefone

Você pode instalar manualmente um certificado de usuário no telefone se o protocolo SCEP (Simple Certificate Enrollment Protocol) não estiver disponível.

O Certificado instalado pelo fabricante (MIC) pré-instalado pode ser usado como o certificado do usuário para EAP-TLS.

Depois de instalar o certificado do usuário, você precisa adicioná-lo à lista de confiança do servidor RADIUS.

Antes de Iniciar

Para poder instalar um certificado de usuário para um telefone, você precisa ter:

- Um certificado de usuário salvo em seu PC. O certificado deve estar no formato PKCS #12.
- A senha de extração do certificado.

Procedimento

Etapa 1 Na página da Web de administração do telefone, selecione **Certificados**.
Etapa 2 Navegue até o certificado em seu PC.
Etapa 3 No campo **Extrair senha**, insira a senha de extração do certificado.
Etapa 4 Clique em **Carregar**.
Etapa 5 Reinicie o telefone depois que o upload terminar.

Instalar um certificado de autenticação de servidor usando a página da Web de administração do telefone

Você pode instalar manualmente um certificado de servidor de autenticação no telefone se o protocolo SCEP (Simple Certificate Enrollment Protocol) não estiver disponível.

O certificado raiz de CA que emitiu o certificado de servidor RADIUS deve estar instalado para o EAP-TLS.

Antes de Iniciar

Antes de instalar um certificado em um telefone, você deve ter um certificado de servidor de autenticação salvo no PC. O certificado deve ser codificado no PEM (Base 64) ou DER.

Procedimento

Etapa 1 Na página da Web de administração do telefone, selecione **Certificados**.
Etapa 2 Localize o campo **CA (página da Web de administração) do servidor de autenticação** e clique em **Instalar**.
Etapa 3 Navegue até o certificado em seu PC.
Etapa 4 Clique em **Carregar**.
Etapa 5 Reinicie o telefone depois que o upload terminar.

Se estiver instalando mais de um certificado, instale todos os certificados antes de reiniciar o telefone.

Remover manualmente um certificado de segurança da página da Web de administração do telefone

Você pode remover manualmente um certificado de segurança de um telefone se o protocolo SCEP (Simple Certificate Enrollment Protocol) não estiver disponível.

Procedimento

Etapa 1 Na página da Web de administração do telefone, selecione **Certificados**.

Etapa 2 Localize o certificado na página **Certificados**.

Etapa 3 Clique em **Excluir**.

Etapa 4 Reinicie o telefone depois que o processo de exclusão for concluído.

Definir manualmente a data e a hora do telefone

Com a autenticação baseada em certificados, o telefone deve exibir a data e a hora corretas. Um servidor de autenticação verifica a data e a hora do telefone em relação à data de expiração do certificado. Se as datas e horas do telefone e do servidor não coincidirem, o telefone deixará de funcionar.

Use este procedimento para definir manualmente a data e a hora do telefone se ele não estiver recebendo as informações corretas de sua rede.

Procedimento

Etapa 1 Na página da Web de administração do telefone, role até **Data e hora**.

Etapa 2 Realize uma das seguintes opções:

- Clique em **Definir telefone para Data e hora local** para sincronizar o telefone com um servidor local.
- Nos campos **Data e hora específica**, selecione mês, dia, ano, hora, minuto e segundo usando os menus e clique em **Definir telefone para data e hora específica**.

Configuração do SCEP

O protocolo SCEP (Simple Certificate Enrollment Protocol) é o padrão para fornecimento e renovação automática de certificados. Evite a instalação manual de certificados em seus telefones.

Definir os parâmetros de configuração específicos do produto SCEP

Você deve configurar os seguintes parâmetros do SCEP na página da Web do telefone

- Endereço IP do RA
- Impressão digital SHA-1 ou SHA-256 do certificado raiz da CA para o servidor SCEP

A Autoridade de registro (RA) do Cisco IOS atua como um proxy para o servidor SCEP. O cliente SCEP no telefone usa os parâmetros que são baixados do Cisco Unified Communication Manager. Depois que você configura os parâmetros, o telefone envia uma solicitação `SCEP getcs` para o RA, e o certificado raiz da CA é validado usando a impressão digital definida.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, selecione **Dispositivo** > **Telefone**.

Etapa 2 Localize o telefone.

Etapa 3 Role até a área **Layout da configuração específica do produto**.

Etapa 4 Marque a caixa de seleção **Servidor WLAN SCEP** para ativar o parâmetro SCEP.

Etapa 5 Marque a caixa de seleção **Impr. digital CA de raiz WLAN (SHA256 ou SHA1)** para ativar o parâmetro QED SCEP.

Suporte ao servidor SCEP (Simple Certificate Enrollment Protocol)

Se você estiver usando um servidor SCEP (Simple Certificate Enrollment Protocol), o servidor poderá manter automaticamente seus certificados de usuário e de servidor. No servidor SCEP, configure o agente de registro (RA) SCEP para:

- Agir como um ponto de confiança PKI
- Agir como um RA PKI
- Executar a autenticação de dispositivos usando um servidor RADIUS

Para obter mais informações, consulte a documentação do servidor SCEP.

Autenticação 802.1x

Os Telefones IP Cisco são compatíveis com a Autenticação 802.1X.

Os Telefones IP Cisco e os switches do Cisco Catalyst tradicionalmente usam o CDP (Cisco Discovery Protocol) para identificar um ao outro e determinar parâmetros como a alocação de VLAN e os requisitos de potência embutida.

O suporte à autenticação 802.1X exige vários componentes:

- Telefone IP Cisco: o telefone inicia a solicitação para acessar a rede. Os telefones contêm um suplicante 802.1X. Esse suplicante permite aos administradores de rede controlar a conectividade dos telefones IP para as portas de switch da LAN. A versão atual do suplicante 802.1X do telefone usa as opções EAP-FAST e EAP-TLS para autenticação de rede.
- Switch do Cisco Catalyst (ou outro switch de terceiros): o switch deve ser compatível com 802.1X para que possa atuar como o autenticador e passar as mensagens entre o telefone e o servidor de autenticação. Após a conclusão da troca, o switch concede ou nega o acesso do telefone à rede.

Você deve executar as ações a seguir para configurar a 802.1X.

- Configure os outros componentes antes de ativar a Autenticação 802.1X no telefone.

- Configure a VLAN de voz — Como o padrão 802.1X não considera as VLANs, você deve definir essa configuração com base no suporte ao switch.
  - Ativado — Se você estiver usando um switch que aceita a autenticação de vários domínios, você poderá continuar usando a VLAN de voz.
  - Desativado — Se o switch não aceitar a autenticação de vários domínios, desative a VLAN de voz e considere a atribuição da porta à VLAN nativa.

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

CAPÍTULO 8

Personalização do Cisco IP Conference Phone

Toques de telefone personalizados

O Telefone IP Cisco apresenta dois toques padrão que são implementados no hardware: Chirp1 e Chirp2. O Cisco Unified Communications Manager também fornece um conjunto padrão de toques adicionais de telefone que são implementados no software como arquivos PCM (modulação de código de pulso). Os arquivos PCM, junto com um arquivo XML que descreve as opções da lista de toques disponíveis em seu site, estão localizados no diretório TFTP em cada servidor Cisco Unified Communications Manager.

Atenção Todos os nomes de arquivo diferenciam maiúsculas de minúsculas. Se você usar o tamanho de letra errado para o nome de arquivo, o telefone não aplicará suas alterações.

Para obter mais informações, consulte o capítulo "Toques e fundos personalizados do telefone" no Guia de configuração de recursos para o Cisco Unified Communications Manager.

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

Configurar um toque personalizado do telefone

Procedimento

Etapa 1 Crie um arquivo PCM para cada toque personalizado (um toque por arquivo).

Assegure-se de que os arquivos PCM cumpram as diretrizes de formato listadas na seção Formatos de arquivo de toque personalizado.

Etapa 2 Carregue os novos arquivos PCM que você criou no servidor TFTP da Cisco para cada Cisco Unified Communications Manager no seu cluster.

Para obter mais informações, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Etapa 3 Salve suas modificações e feche o arquivo Ringlist-wb.

Etapa 4 Para colocar o novo arquivo Ringlist-wb no cache:

- Pare e inicie o serviço TFTP usando o Cisco Unified Serviceability
- Desative e reative o parâmetro de serviço TFTP "Ativar o armazenamento em cache de arquivos de binários e constantes na inicialização", localizado na área Parâmetros de serviço avançados.

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

Formatos de arquivo de toque personalizado

O arquivo Ringlist-wb.xml define um objeto XML que contém uma lista de tipos de toque de telefone. Esse arquivo inclui até 50 tipos de toque. Cada tipo de toque contém um ponteiro para o arquivo PCM que é usado para esse tipo de toque e o texto que é exibido no menu Tipo de toque de um Telefone IP Cisco para esse toque. O servidor TFTP da Cisco para cada Cisco Unified Communications Manager contém esse arquivo.

O objeto XML CiscoIPPhoneRinglist usa o seguinte conjunto de marcas simples para descrever as informações:

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

As seguintes características se aplicam aos nomes de definições. Você deve incluir o DisplayName e o FileName necessários para cada tipo de toque de telefone.

- DisplayName especifica o nome do toque personalizado para o arquivo PCM associado que é exibido no menu Tipo de toque do Telefone IP Cisco.
- FileName especifica o nome do arquivo PCM que o toque personalizado deve associar a DisplayName.

Observação Os campos DisplayName e FileName não devem exceder 25 caracteres.

Este exemplo mostra um arquivo Ringlist-wb.xml que define dois tipos de toque de telefone:

```
<CiscoIPPhoneRingList>
 <Ring>
      <DisplayName>Analog Synth 1</DisplayName>
      <FileName>Analog1.rwb</FileName>
   </Ring>
   <Ring>
      <DisplayName>Analog Synth 2</DisplayName>
      <FileName>Analog2.rwb</FileName>
   </Ring>
</CiscoIPPhoneRingList>
```

Os arquivos PCM para os toques devem atender aos seguintes requisitos para a reprodução apropriada em Telefones IP Cisco:

- PCM bruto (sem cabeçalho)
- 8.000 amostras por segundo

- 8 bits por amostra
- Compactação Mu-law
- Tamanho máximo do toque = 16080 amostras
- Tamanho mínimo do toque = 240 amostras
- Número de amostras no toque = múltiplos de 240.
- Início e término do toque em cruzamento zero.

Para criar arquivos PCM para toques de telefone personalizados, use qualquer pacote padrão de edição de áudio que suporte esses requisitos de formato de arquivo.

Personalizar o tom de discagem

Você pode configurar seus telefones para que os usuários ouçam diferentes tons de discagem para chamadas internas e externas. Dependendo das suas necessidades, você pode escolher dentre três opções de tom de discagem:

- Padrão: um tom de discagem diferente para chamadas internas e externas.
- Interno: o tom de discagem interno é usado para todas as chamadas.
- Externo: o tom de discagem externo é usado para todas as chamadas.

Always Use Dial Tone (Sempre usar tom de discagem) é um campo obrigatório no Cisco Unified Communications Manager.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, selecione **Sistema** > **Parâmetros de serviço**.

Etapa 2 Selecione o servidor apropriado.

Etapa 3 Selecione **Cisco CallManager** como o serviço.

Etapa 4 Role até o painel Parâmetros gerais de cluster.

Etapa 5 Defina **Sempre usar tom de discagem** para um destes valores:

- Externo
- Interno
- Padrão

Etapa 6 Selecione **Salvar**.

Etapa 7 Reinicie os telefones.

CAPÍTULO 9

Recursos e configuração do Cisco IP Conference Phone

Suporte para usuários do Telefone IP Cisco

Se você for um administrador do sistema, provavelmente é a fonte principal de informações dos usuários do Telefone IP Cisco em sua rede ou empresa. É importante fornecer informações atuais e detalhadas aos usuários finais.

Para usar alguns dos recursos do Telefone IP Cisco (incluindo Serviços e opções de sistema de mensagens de voz), os usuários devem receber informações de você ou de sua equipe de rede ou devem poder entrar em contato com você para obter assistência. Forneça aos usuários os nome das pessoas de contato para assistência e as instruções de como entrar em contato com essas pessoas.

Recomendamos que você crie uma página da Web em seu site de suporte interno que forneça aos usuários finais informações importantes sobre os Telefones IP Cisco deles.

É recomendável incluir os seguintes tipos de informações nesse site:

- Guias do usuário de todos os modelos de Telefone IP Cisco para os quais você oferece suporte
- Informações sobre como acessar o Cisco Unified Communications Portal de Ajuda
- Lista de recursos com suporte
- Guia do usuário ou referência rápida de seu sistema de correio de voz

Migração do seu telefone diretamente para um telefone multiplataforma

Você pode migrar o telefone de sua empresa para um telefone multiplataforma facilmente em uma etapa sem usar a carga do firmware de transição. Tudo o que você precisa é obter e autorizar a licença de migração a partir do servidor.

Para obter mais informações, 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

Configurar um novo modelo de tecla programável

Você precisa adicionar teclas programáveis a um modelo de tecla programável para fornecer aos usuários o acesso a alguns recursos. Por exemplo, se você desejar que os usuários usem o recurso Não perturbar, você precisa ativar a tecla programável. Para obter mais informações, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Talvez seja útil criar vários modelos. Por exemplo, talvez você queira um modelo para o telefone em uma sala de conferência e outro modelo para um telefone no escritório de um executivo.

Este procedimento leva você através das etapas para criar um novo modelo de tecla programável e atribuí-lo a um telefone específico. Semelhante a outros recursos do telefone, você também pode usar o modelo para todos os seus telefones de conferência ou para um grupo de telefones.

Procedimento

Etapa 1 Inicie uma sessão na Administração do Cisco Unified Communications Manager como um administrador.

Etapa 2 Selecione **Dispositivo** > **Configurações do dispositivo** > **Modelo de tecla programável**.

Etapa 3 Clique em **Localizar**.

Etapa 4 Selecione uma das opções a seguir:

- Cisco Unified Communications Manager 11.5 e versões anteriores — **Usuário padrão**
- Cisco Unified Communications Manager 12.0 e versões posteriores — **Usuário de conferência pessoal** ou **Usuário de conferência pública**.

Etapa 5 Clique em **Copiar**.

Etapa 6 Altere o nome do modelo.

Por exemplo, Modelo de sala de conferência 8832.

Etapa 7 Clique em **Save** (Salvar).

Etapa 8 Vá para a página **Configurar layout da tecla programável** do menu superior direito.

Etapa 9 Para cada estado de chamada, defina os recursos a exibir.

Etapa 10 Clique em **Save** (Salvar).

Etapa 11 Volte para a **tela Localizar/listar** do menu superior direito.

Você verá o novo modelo na lista de modelos.

Etapa 12 Selecione **Dispositivo** > **Telefone**.

Etapa 13 Localize o telefone ao qual deseja atribuir o novo modelo e selecione-o.

Etapa 14 No campo **Modelo de tecla programável**, selecione o novo modelo de tecla programável.

Etapa 15 Clique em **Salvar** e **Aplicar config.**

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

Configurar serviços de telefonia para usuários

Você pode fornecer aos usuários acesso aos serviços do Telefone IP Cisco no telefone IP. Também é possível atribuir um botão a diferentes serviços de telefonia. O telefone IP gerencia cada serviço como um aplicativo distinto.

Para que um usuário possa acessar qualquer serviço:

- Use a Administração do Cisco Unified Communications Manager to configurar serviços que não estão presentes por padrão.
- O usuário tem que se inscrever nos serviços usando o Portal de autoatendimento do Cisco Unified Communications. Esse aplicativo baseado na Web fornece uma GUI (interface gráfica do usuário) para configuração limitada dos aplicativos do telefone IP pelo usuário final. No entanto, um usuário não pode se inscrever em qualquer serviço que você configura como uma assinatura corporativa.

Para obter mais informações, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Antes de configurar serviços, colete os URLs dos sites que você deseja configurar e verifique se os usuários podem acessá-los pela rede de telefonia IP corporativa. Essa atividade não se aplica aos serviços padrão fornecidos pela Cisco.

Procedimento

Etapa 1 Em Administração do Cisco Unified Communications Manager, escolha **Dispositivo** > **Configurações do dispositivo** > **Serviços de telefonia**.

Etapa 2 Verifique se os usuários podem acessar Portal de autoatendimento do Cisco Unified Communications, no qual eles podem selecionar e se inscrever nos serviços configurados.

Consulte Visão geral do Portal de Ajuda, na página 71 para obter um resumo das informações que devem ser fornecidas aos usuários finais.

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

Configuração de recursos do telefone

Você pode configurar telefones para que tenham uma variedade de recursos, de acordo com as necessidades dos usuários. É possível aplicar recursos a todos os telefones, um grupo de telefones ou a telefones individuais.

Quando você configura recursos, a janela Administração do Cisco Unified Communications Manager exibe informações que são aplicáveis a todos os telefones e informações que são aplicáveis ao modelo do telefone. As informações específicas ao modelo do telefone estão na área Layout de configuração específica do produto da janela.

Para obter informações sobre os campos aplicáveis a todos os modelos de telefone, consulte a documentação do Cisco Unified Communications Manager.

Quando você define um campo, a janela na qual o campo é definido é importante, pois há uma precedência para as janelas. A ordem de precedência é:

1. Telefones individuais (precedência mais alta)
2. Grupo de telefones
3. Todos os telefones (precedência mais baixa)

Por exemplo, se você não quiser que um conjunto específico de usuários acesse as páginas da Web do telefone, mas sim o restante dos usuários, você:

1. Ativa o acesso às páginas da Web do telefone para todos os usuários.
2. Desativa o acesso às páginas da Web do telefone para cada usuário individual ou configura um grupo de usuários e desativa o acesso às páginas da Web do telefone para o grupo de usuários.
3. Se um usuário específico do grupo precisar de acesso às páginas da Web do telefone, você poderá ativá-lo para o usuário em questão.

Tópicos relacionados

Configurar credenciais do usuário persistentes para o início de sessão no Expressway, na página 125

Configurar recursos do telefone para todos os telefones

Procedimento

Etapa 1	Entre na administração do Cisco Unified Communications Manager como administrador.
Etapa 2	Selecione **Sistema** > **Configuração do telefone da empresa**.
Etapa 3	Defina os campos que você deseja alterar.
Etapa 4	Marque a caixa de seleção **Substituir configurações da empresa** para os campos alterados.
Etapa 5	Clique em **Save** (Salvar).
Etapa 6	Clique em **Aplicar config.**
Etapa 7	Reinicie os telefones.

Observação Isso afetará todos os telefones de sua organização.

Tópicos relacionados

Configuração específica do produto, na página 102

Configurar recursos do telefone para um grupo de telefones

Procedimento

Etapa 1 Entre na administração do Cisco Unified Communications Manager como administrador.
Etapa 2 Selecione **Dispositivo** > **Definições do dispositivo** > **Perfil de telefone comum**.
Etapa 3 Localize o perfil.
Etapa 4 Navegue até o painel Layout da configuração específica do produto e defina os campos.
Etapa 5 Marque a caixa de seleção **Substituir configurações da empresa** para os campos alterados.
Etapa 6 Clique em **Save** (Salvar).
Etapa 7 Clique em **Aplicar config.**
Etapa 8 Reinicie os telefones.

Tópicos relacionados

Configuração específica do produto, na página 102

Configurar recursos do telefone para um único telefone

Procedimento

Etapa 1 Entre na administração do Cisco Unified Communications Manager como administrador.
Etapa 2 Selecione **Dispositivo** > **Telefone**
Etapa 3 Localize o telefone associado ao usuário.
Etapa 4 Navegue até o painel Layout da configuração específica do produto e defina os campos.
Etapa 5 Marque a caixa de seleção **Substituir definições comuns** para os campos alterados.
Etapa 6 Clique em **Save** (Salvar).
Etapa 7 Clique em **Aplicar config.**
Etapa 8 Reinicie o telefone.

Tópicos relacionados

Configuração específica do produto, na página 102

Configuração específica do produto

A tabela a seguir descreve os campos do painel Layout de configuração específica do produto. Alguns campos nesta tabela são exibidos apenas na página **Dispositivo** > **Telefone**.

Tabela 18: Campos de configuração específica do produto

Nome do campo	Tipo de campo Ou opções	Padrão	Descrição
Acesso às Configurações	Desativado Habilitado Restrito	Habilitado	Ativa, desativa ou restringe o acesso às configurações locais do telefone no app Configurações. Com o acesso restringido, os menus Preferências e Informações do sistema podem ser acessados. Algumas configurações no menu Wi-Fi também são acessíveis. Com o acesso desativado, o menu Configurações não exibe opções.
ARP Gratuito	Desativado Habilitado	Desativado	Ativa ou desativa a capacidade do telefone de identificar endereços MAC do ARP Gratuito. Esse recurso é necessário para monitorar ou gravar fluxos de voz.
Acesso à Web	Desativado Habilitado	Desativado	Ativa ou desativa o acesso às páginas da Web do telefone por meio de um navegador da Web. **Cuidado** Se você ativar este campo, poderá expor informações confidenciais sobre o telefone.
Desativar o TLS 1.0 e TLS 1.1 para WebAccess	Desativado Habilitado	Habilitado	Controla o uso de TLS 1.2 para uma conexão de servidor Web. • Desabilitado — um telefone configurado para TLS1.0, TLS 1.1 ou TLS1.2 pode funcionar com um servidor HTTPs. • Habilitado — somente um telefone configurado para TLS1.2 pode funcionar com um servidor HTTPs.

Nome do campo	Tipo de campo Ou opções	Padrão	Descrição
Discagem enbloc	Desativado Habilitado	Desativado	Controla o método de discagem. • Desativado — o Cisco Unified Communications Manager aguarda até que o temporizador interdígito expire quando houver sobreposição do padrão de rota ou plano de discagem. • Ativado — a cadeia discada completa é enviada para o Cisco Unified Communications Manager quando a discagem estiver concluída. Para evitar o limite de tempo esgotado do temporizador T.302, recomendamos que você ative a discagem Enbloc sempre que houver uma sobreposição do padrão de rota ou plano de discagem. Os códigos de autorização forçados (FAC) ou códigos de assunto de cliente (CMC) não são compatíveis com a discagem enbloc. Se você usar o FAC ou CMC para gerenciar o acesso de chamada e contabilidade, não é possível usar esse recurso.
Dias de inatividade da luz de fundo	Dias da semana		Define os dias que a luz de fundo não será ativada automaticamente no horário especificado no campo Tempo de ativação da luz de fundo. Escolha o dia ou os dias na lista suspensa. Para escolher mais de um dia, pressione **Ctrl+clique** em cada dia que desejar. Consulte Agendar economia de energia para o Telefone IP Cisco, na página 115.
Tempo de ativação da luz de fundo	hh:mm		Define o horário de cada dia em que a luz de fundo será ativada automaticamente (exceto nos dias especificados no campo Luz de fundo da tela não ativa). Insira a hora neste campo no formato 24 horas, onde 0:00 corresponde a meia-noite. Por exemplo, para ativar a luz de fundo automaticamente às 7 horas da manhã (0700), insira 07:00. Para ativar a luz de fundo às 2 horas da tarde (1400), insira 14:00. Se esse campo for deixado em branco, a luz de fundo será ativada automaticamente à meia-noite (0:00). Consulte Agendar economia de energia para o Telefone IP Cisco, na página 115.

Nome do campo	Tipo de campo Ou opções	Padrão	Descrição
Duração da ativação da luz de fundo	hh:mm		Define por quanto tempo a luz de fundo permanecerá ativada após a ativação no horário especificado no campo Tempo de ativação da luz de fundo. Por exemplo, para manter a luz de fundo ativada por 4 horas e 30 minutos depois que ela for ativada automaticamente, insira 04:30. Se esse campo for deixado em branco, o telefone se apagará no fim do dia (0:00). Se o tempo de ativação da luz de fundo for definido para 0:00 e a duração da luz de fundo ativada for deixada em branco (ou 24:00), a luz de fundo não será desativada. Consulte Agendar economia de energia para o Telefone IP Cisco, na página 115.
Tempo limite ocioso da luz de fundo	hh:mm		Define por quanto tempo o telefone permanece ocioso antes de a luz de fundo se apagar. Aplica-se somente quando a luz de fundo estava desativada conforme programado e foi ativada por um usuário (pressionando um botão no telefone ou levantando o monofone). Por exemplo, para desativar a luz de fundo quando o telefone estiver ocioso por 1 hora e 30 minutos depois que o usuário ativar a luz de fundo, insira 01:30. Consulte Agendar economia de energia para o Telefone IP Cisco, na página 115.
Luz de fundo ligada em chamada de entrada	Desativado Habilitado	Habilitado	Ativa a luz de fundo quando há uma chamada recebida.

Nome do campo	Tipo de campo Ou opções	Padrão	Descrição
Ativar Economia de energia adicional	Dias da semana		Define a programação de dias nos quais o telefone será desligado. Escolha o dia ou os dias na lista suspensa. Para escolher mais de um dia, pressione **Ctrl+clique** em cada dia que desejar. Quando Ativar Economia de energia adicional estiver ativado, você receberá uma mensagem que alerta sobre problemas de emergência (e911). **Cuidado** Quando o Modo Economia de energia adicional (o "Modo") está ativado, os dispositivos que estão configurados para o modo são desativados para chamadas de emergência e para receber chamadas. Ao selecionar esse modo, você concorda com o seguinte: (i) Você assume total responsabilidade por fornecer métodos alternativos para chamadas de emergência e para receber chamadas enquanto o modo está ativo; (ii) A Cisco não tem responsabilidade em relação à sua seleção do modo, e é inteiramente de responsabilidade a ativação do modo; e (iii) Você informará totalmente aos usuários os efeitos do modo sobre as chamadas, como efetuar chamadas e tudo mais. Para desativar a Economia de energia adicional, você deve desmarcar a caixa de seleção Permitir substituições de EnergyWise. Se a caixa Permitir substituições de EnergyWise permanecer desmarcada, mas nenhum dia for selecionado no campo Ativar Economia de energia adicional, a Economia de energia adicional não será desativada. Consulte Programar EnergyWise no Telefone IP Cisco, na página 116.

Nome do campo	Tipo de campo Ou opções	Padrão	Descrição
Tempo de telefone ligado	hh:mm		Determina quando o telefone será ligado automaticamente nos dias que estão no campo Ativar Economia de energia adicional. Insira a hora neste campo no formato 24 horas, onde 00:00 corresponde a meia-noite. Por exemplo, para ativar o telefone automaticamente às 7 horas da manhã (0700), insira 07:00. Para ativar o telefone às 2 horas da tarde (1400), insira 14:00. O valor padrão é em branco, o que significa 00:00. O Tempo de telefone ligado deve ser pelo menos 20 minutos depois do Tempo de telefone desligado. Por exemplo, se o Tempo de telefone desligado for 07:00, o Tempo de telefone ligado deverá ser no mínimo 07:20. Consulte Programar EnergyWise no Telefone IP Cisco, na página 116.
Tempo de telefone desligado	hh:mm		Define a hora do dia em que o telefone é desligado nos dias que estão selecionados no campo Ativar Economia de energia adicional. Se os campos Tempo de telefone ligado e Tempo de telefone desligado contiverem o mesmo valor, o telefone não será desligado. Insira a hora neste campo no formato 24 horas, onde 00:00 corresponde a meia-noite. Por exemplo, para desativar o telefone automaticamente às 7 horas da manhã (0700), insira 7:00. Para desativar o telefone às 2 horas da tarde (1400), insira 14:00. O valor padrão é em branco, o que significa 00:00. O Tempo de telefone ligado deve ser pelo menos 20 minutos depois do Tempo de telefone desligado. Por exemplo, se o Tempo de telefone desligado for 7:00, o Tempo de telefone ligado deverá ser no mínimo 7:20. Consulte Programar EnergyWise no Telefone IP Cisco, na página 116.

Nome do campo	Tipo de campo Ou opções	Padrão	Descrição
Tempo limite de ociosidade de telefone desligado	hh:mm		Indica por quanto tempo o telefone deve estar ocioso antes de o telefone ser desligado. O limite de tempo esgotado ocorre nas seguintes condições: • Quando o telefone estava no modo Economia de energia adicional, conforme programado, e foi retirado desse modo porque o usuário do telefone pressionou a tecla Selecionar. • Quando o telefone é religado pelo switch conectado. • Quando o Tempo de telefone desligado é atingido, mas o telefone está em uso. Consulte Programar EnergyWise no Telefone IP Cisco, na página 116.
Ativar alerta sonoro	Caixa de Seleção	Desmarcada	Quando ativado, instrui o telefone a reproduzir um alerta sonoro a partir de 10 minutos antes do tempo especificado no campo Tempo de telefone desligado. Essa caixa de seleção é aplicável somente quando a caixa de lista Ativar Economia de energia adicional tem um ou mais dias selecionados. Consulte Programar EnergyWise no Telefone IP Cisco, na página 116.
Domínio do EnergyWise	Até 127 caracteres		Identifica o domínio do EnergyWise em que o telefone está. Consulte Programar EnergyWise no Telefone IP Cisco, na página 116.
Segredo do EnergyWise	Até 127 caracteres		Identifica a senha secreta de segurança que é usada para se comunicar com os dispositivos no domínio do EnergyWise. Consulte Programar EnergyWise no Telefone IP Cisco, na página 116.

Nome do campo	Tipo de campo Ou opções	Padrão	Descrição
Permitir substituições de EnergyWise	Caixa de seleção	Desmarcada	Determina se você permite que a política do controlador do domínio do EnergyWise envie atualizações de nível de potência para os telefones. As seguintes condições se aplicam: • Um ou mais dias devem ser selecionados no campo Ativar Economia de energia adicional. • As configurações na Administração do Cisco Unified Communications Manager entram em vigor conforme programado, mesmo que o EnergyWise enviar uma substituição. Por exemplo, supondo-se que a opção Tempo de telefone desligado esteja definida como 22:00, o valor no campo Tempo de telefone ligado seja 06:00 e Ativar economia de energia adicional tenha um ou mais dias selecionados. • Se o EnergyWise instruir o telefone para desligar às 20:00, essa diretiva permanecerá em vigor (presumindo que não ocorra intervenção do usuário do telefone) até o Tempo de telefone ligado às 06:00. • Às 06:00, o telefone é ligado e recomeça a receber as alterações de nível de potência das configurações da Administração do Cisco Unified Communications Manager. • Para alterar o nível de potência no telefone novamente, o EnergyWise deve reemitir um novo comando de alteração de nível de energia. Para desativar a Economia de energia adicional, você deve desmarcar a caixa de seleção Permitir substituições de EnergyWise. Se a caixa Permitir substituições de EnergyWise permanecer desmarcada, mas nenhum dia for selecionado no campo Ativar Economia de energia adicional, a Economia de energia adicional não será desativada. Consulte Programar EnergyWise no Telefone IP Cisco, na página 116.

Nome do campo	Tipo de campo Ou opções	Padrão	Descrição
Política de registro e transferência direta	Ativar na mesma linha Desativar na mesma linha	Mesma linha, ativação de linha cruzada	Controla a capacidade de um usuário unir e transferir chamadas. • Ativar na mesma linha — Os usuários podem transferir ou unir diretamente uma chamada na linha atual a outra chamada na mesma linha. • Desativar na mesma linha — Os usuários não podem unir ou transferir chamadas na mesma linha. Os recursos para unir e transferir chamadas são desativados, e o usuário não pode executar a função de transferência direta ou união.
Tom da gravação	Desativado Habilitado	Desativado	Controla a reprodução do tom quando um usuário está gravando uma chamada
Volume local do tom da gravação	Inteiro 0–100	100	Controla o volume do tom de gravação para o usuário local.
Volume remoto do tom de gravação	Inteiro 0–100	50	Controla o volume do tom de gravação para o usuário remoto.
Duração do tom da gravação	Inteiro 1–3000 milissegundos		Controla a duração do tom de gravação.
Servidor de registro	String de até 256 caracteres		Identifica o servidor de log do sistema IPv4 para a saída de depuração do telefone. O formato do endereço é: **address:<port>@@base=<0-7>;pfs=<0-1>**
Registro remoto	Desativado Habilitado	Desativado	Controla a capacidade de enviar registros para o servidor de log do sistema.

Nome do campo	Tipo de campo Ou opções	Padrão	Descrição
Perfil de registro	Padrão Predefinição Telefonia SIP UI Rede Mídia Atualização Acessório Segurança EnergyWise AcessoRemotoMóvel	Predefinição	Especifica o perfil de registro em log predefinido. • Padrão — nível de registro em log de depuração padrão • Predefinição — não substitui a configuração de registro em log de depuração local do telefone • Telefonia — registra informações sobre recursos de telefonia ou chamada • SIP — registra informações sobre a sinalização SIP • UI — registra informações sobre a interface do usuário do telefone • Rede — registra informações da rede • Mídia — registra informações da mídia • Atualização — registra informações da atualização • Acessório — registra informações do acessório • Segurança — registra informações de segurança • Energywise — registra informações de economia de energia • MobileRemoteAccess – Registra informações de Acesso remoto e móvel por meio do Expressway
Servidor de registro IPv6	String de até 256 caracteres		Identifica o servidor de log do sistema IPv6 para a saída de depuração do telefone.
Cisco Discovery Protocol (CDP): Porta do switch	Desativado Habilitado	Habilitado	Controla o Cisco Discovery Protocol no telefone.
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Porta do switch	Desativado Habilitado	Habilitado	Ativa LLDP-MED na porta do SW.
ID do ativo LLDP	String, até 32 caracteres		Identifica o ID do ativo atribuído ao telefone para gerenciamento de inventário.
Energy Efficient Ethernet (EEE): Porta do switch	Desativado Habilitado	Desativado	Controla o EEE na porta do switch.

Nome do campo	Tipo de campo Ou opções	Padrão	Descrição
Prioridade da potência LLDP	Desconhecido Baixo Alta Crítico	Desconhecido	Atribui uma propriedade de potência do telefone para o switch, o que permite que o switch forneça energia adequadamente para os telefones.
Autenticação 802.1x	Controlado pelo usuário Desativado Habilitado	Controlado pelo usuário	Especifica o status do recurso de autenticação 802.1x. • Controlado pelo usuário — o usuário pode configurar a autenticação 802.1x no telefone. • Desativado — A autenticação 802.1x não é usada. • Habilitado — A autenticação 802.1x é usada, e você configura a autenticação para os telefones.
Configuração remota da porta do switch	Desativado Negociação automática 10 Meio 10 Todo 100 Meio 100 Todo	Desativado	Permite configurar a velocidade e a função duplex da porta do SW do telefone remotamente. Isso melhora o desempenho para implantações grandes com configurações de porta específicas. Se as portas do SW forem configuradas para Configuração remota de portas no Cisco Unified Communications Manager, os dados não poderão ser alterados no telefone.
Acesso ao SSH	Desativado Habilitado	Desativado	Controla o acesso ao daemon SSH por meio da porta 22. Deixar a porta 22 aberta deixa o telefone vulnerável a ataques de negação de serviço (DoS).
Código de idioma em anéis	Padrão Japão	Padrão	Controla o padrão de toque.
TLS reinício do cronômetro	Inteiro 0–3600 segundos	3600	Controla a capacidade de retomar uma sessão TLS sem repetir todo o processo de autenticação TLS. Se o campo for definido como 0, a retomada de sessão TLS será desativada.
Modo FIPS	Desativado Habilitado	Desativado	Ativa ou desativa o modo FIPS (Federal Information Processing Standards) no telefone.
Registrar log de chamadas a partir de linha compartilhada	Desativado Habilitado	Desativado	Especifica se você deseja registrar o log de chamadas de uma linha compartilhada.
Volume mínimo do toque	0 - Silencioso 1–15	0 - Silencioso	Controla o volume de toque mínimo para o telefone.

Nome do campo	Tipo de campo Ou opções	Padrão	Descrição
Compart. firmware corresp.	Desativado Habilitado	Habilitado	Permite que o telefone localize outros telefones do mesmo modelo na sub-rede e compartilhe arquivos de firmware atualizados. Se o telefone tiver uma nova carga de firmware, ele poderá compartilhar essa carga com os outros telefones. Se um dos outros telefones tiver uma nova carga de firmware, o telefone poderá baixar o firmware do outro telefone, em vez do servidor SMTP. Compart. firmware corresp.: • Limita o congestionamento de transferências TFTP aos servidores TFTP remotos centralizados. • Elimina a necessidade de controlar manualmente as atualizações de firmware. • Reduz o tempo de inatividade do telefone durante as atualizações quando muitos telefones são redefinidos ao mesmo tempo. • Ajuda nas atualizações de firmware em cenários de implantação em filiais ou escritórios remotos que trabalham com links de WAN de largura de banda limitada.
Servidor de carregamento	String de até 256 caracteres		Identifica o servidor IPv4 alternativo que o telefone usa para obter cargas e atualizações de firmware.
Servidor de carregamento de IPv6	String de até 256 caracteres		Identifica o servidor IPv6 alternativo que o telefone usa para obter cargas e atualizações de firmware.

Nome do campo	Tipo de campo Ou opções	Padrão	Descrição
Detectar falha no Unified CM Connection	Normal Atrasado	Normal	Determina a sensibilidade que o telefone tem para detectar uma falha de conexão com o Cisco Unified Communications Manager (Unified CM), o que é o primeiro passo antes de ocorrer o failover do dispositivo para um Unified CM/SRST de reserva. Os valores válidos especificam Normal (a detecção de uma falha de conexão do Unified CM ocorre à velocidade padrão do sistema) ou Atrasada (a detecção de um failover de conexão do Unified CM ocorre aproximadamente quatro vezes mais lentamente do que o Normal). Para um reconhecimento mais rápido de uma falha de conexão do Unified CM, escolha Normal. Se você preferir que o failover seja ligeiramente atrasado para dar a oportunidade para restabelecer a conexão, escolha Atrasada. A diferença de tempo precisa entre a detecção de falha de conexão Normal e Atrasada depende de muitas variáveis que mudam constantemente.
ID do requisito especial	String		Controla recursos personalizados de cargas de engenharia especial (ES).
Servidor HTTPS	http e https ativados Apenas https	http e https ativados	Controla o tipo de comunicação com o telefone. Se você selecionar Apenas HTTPS, a comunicação com o telefone é mais segura.
As credenciais do usuário persistem para o login no Expressway	Desativado Habilitado	Desativado	Controla se o telefone armazena as credenciais de login dos usuários. Quando desativado, o usuário sempre vê a mensagem para entrar no servidor Expressway para Mobile and Remote Access (MRA). Se desejar facilitar o login para os usuários, ative esse campo para que as credenciais de login do Expressway sejam persistentes. Assim, o usuário terá de inserir as credenciais de login apenas na primeira vez. Nos acessos subsequentes (quando o telefone estiver ligado fora do local), as informações de login serão preenchidas previamente na tela Iniciar sessão. Para obter mais informações, consulte Configurar credenciais do usuário persistentes para o início de sessão no Expressway, na página 125.

Nome do campo	Tipo de campo Ou opções	Padrão	Descrição
URL de carregamento do suporte ao cliente	String, até 256 caracteres		Fornece o URL da ferramenta Relatório de problemas (PRT). Se você implantar dispositivos com Mobile and Remote Access através do Expressway, também deverá adicionar o endereço do servidor PRT à lista de permissões do servidor HTTP no servidor Expressway. Para obter mais informações, consulte Configurar credenciais do usuário persistentes para o início de sessão no Expressway, na página 125.
Desativar codificações de TLS	Consulte Desativar codificações de TLS (Transport Layer Security), na página 114.	Nenhuma	Desativa a codificação de TLS selecionada. Desative mais de um conjunto de codificação, selecionando e mantendo a tecla **Ctrl** pressionada no teclado do computador.
Dedicar uma linha para estacionamento de chamada	Desativado Habilitado	Habilitado	Controla se uma chamada estacionada ocupa uma linha ou não. Para obter mais informações, consulte a documentação do Cisco Unified Communications Manager.

Tópicos relacionados

Configurar credenciais do usuário persistentes para o início de sessão no Expressway, na página 125

Desativar codificações de TLS (Transport Layer Security)

Você pode desativar codificações de TLS (Transport Layer Security) com o parâmetro **Desativar codificações de TLS**. Isso permite personalizar sua segurança para vulnerabilidades conhecidas e alinhar sua rede com políticas da empresa para codificações.

Nenhum é a configuração padrão.

Desative mais de um conjunto de codificação, selecionando e mantendo a tecla **Ctrl** pressionada no teclado do computador. Se você selecionar todas as codificações de telefone, o serviço de telefone de TLS será afetado. Suas opções são:

- Nenhuma
- 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 obter mais informações sobre a segurança do telefone, consulte *White Paper da Visão geral de segurança de Telefones IP Cisco série 7800 e 8800*(https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html).

Agendar economia de energia para o Telefone IP Cisco

Para conservar energia e garantir a longevidade da exibição da tela do telefone, você pode definir a exibição para desligar quando não for necessária.

É preciso configurar as definições na Administração do Cisco Unified Communications Manager para desligar a exibição em uma hora designada em alguns dias e todo o dia em outros dias. Por exemplo, você pode optar por desligar a exibição após o horário comercial em dias da semana e todo o dia aos sábados e domingos.

Você pode executar qualquer uma destas ações para ativar a tela a qualquer momento que ela estiver desativada:

- Pressione qualquer botão no telefone.

  O telefone executa a ação designada por esse botão além de ativar a tela.

- Pegue o monofone.

Quando você ativa a tela, ela permanece ativa até que o telefone permaneça ocioso por um período designado e, em seguida, ela é desativada automaticamente.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, selecione **Dispositivo** > **Telefone**.

Etapa 2 Localize o telefone que você precisa configurar.

Etapa 3 Navegue até a área Configuração específica do produto e defina os campos a seguir:

- Exibição de Dias Não Ativos
- Exibir Tempo
- Exibir Duração
- Tempo inativid. visor excedido

Tabela 19: Campos de configuração de economia de energia

Campo	Descrição
Exibição de Dias Não Ativos	Dias que a tela não será ativada automaticamente no horário especificado no campo Hora de ligação do visor. Escolha o dia ou os dias na lista suspensa. Para escolher mais de um dia, pressione Ctrl+clique em cada dia que desejar.

Campo	Descrição
Exibir Tempo	O horário de cada dia em que a tela será ativada automaticamente (exceto nos dias especificados no campo Dias de inatividade do visor). Insira a hora neste campo no formato 24 horas, onde 0:00 corresponde a meia-noite. Por exemplo, para ativar a tela automaticamente às 7 horas da manhã (0700), insira **07:00**. Para ativar a tela às 2 horas da tarde (1400), insira **14:00**. Se esse campo for deixado em branco, a tela será ativada automaticamente à meia-noite (0:00).
Exibir Duração	Por quanto tempo a tela permanecerá ativada após a ativação no horário especificado no campo Hora de ligação do visor. Insira o valor nesse campo no formato *horas:minutos*. Por exemplo, para manter a tela ativada por 4 horas e 30 minutos depois que ela for ativada automaticamente, insira **04:30**. Se esse campo for deixado em branco, o telefone a desativará no fim do dia (0:00). **Observação** Se a Hora de ligação do visor for 0:00 e a duração da ativação da tela estiver em branco (ou 24:00), a tela permanecerá ativa continuamente.
Tempo inativid. visor excedido	Por quanto tempo o telefone permanece ocioso antes de a tela ser desativada. Aplica-se somente quando a tela estava desativada conforme programado e foi ativada por um usuário (pressionando um botão no telefone ou levantando o monofone). Insira o valor nesse campo no formato *horas:minutos*. Por exemplo, para desativar a tela quando o telefone estiver ocioso por 1 hora e 30 minutos depois que o usuário ativar a tela, insira **01:30**. O valor padrão é 01:00.

Etapa 4 Selecione **Salvar**.

Etapa 5 Selecione **Aplicar config.**

Etapa 6 Reinicie o telefone.

Programar EnergyWise no Telefone IP Cisco

Para reduzir o consumo de energia, configure o telefone para entrar em repouso (desligar) e despertar (ligar) se seu sistema contiver um controlador EnergyWise.

Você define as configurações em Administração do Cisco Unified Communications Manager para ativar o EnergyWise e configurar os horários de suspensão e despertar. Esses parâmetros estão fortemente ligados aos parâmetros de configuração da tela do telefone.

Quando o EnergyWise é ativado e um horário de suspensão é definido, o telefone envia uma solicitação ao switch para despertá-lo no horário configurado. O switch retorna uma aceitação ou rejeição da solicitação. Se o switch rejeitar a solicitação ou não responder, o telefone não será desligado. Se o switch aceitar a solicitação, o telefone ocioso entrará em suspensão, reduzindo o consumo de energia a um nível predeterminado. Um

telefone que não está ocioso define um temporizador de ociosidade e entra em suspensão quando esse temporizador expira.

Para despertar o telefone, pressione Selecionar. Na hora agendada para despertar, o sistema restaura a energia ao telefone, despertando-o.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, selecione **Dispositivo** > **Telefone**.

Etapa 2 Localize o telefone que você precisa configurar.

Etapa 3 Navegue até a área Configuração específica do produto e defina os campos a seguir.

- Ativar Economia de energia adicional
- Tempo de telefone ligado
- Tempo de telefone desligado
- Tempo limite de ociosidade de telefone desligado
- Ativar alerta sonoro
- Domínio do EnergyWise
- Segredo do EnergyWise
- Permitir substituições de EnergyWise

Tabela 20: Campos de configuração do EnergyWise

Campo	Descrição
Ativar Economia de energia adicional	Seleciona a programação de dias nos quais o telefone será desligado. Selecione vários dias pressionando e mantendo pressionada a tecla Control enquanto clica nos dias para a agenda. Por padrão, nenhum dia é selecionado. Quando a opção Ativar Economia de energia adicional estiver ativada, você receberá uma mensagem que alerta sobre problemas de emergência (e911). **Cuidado** Quando o Modo Economia de energia adicional (o "Modo") estiver ativado, os dispositivos que estiverem configurados para o modo serão desativados para chamadas de emergência e para receber chamadas. Ao selecionar esse modo, você concorda com o seguinte: (i) Você assume total responsabilidade por fornecer métodos alternativos para chamadas de emergência e para receber chamadas enquanto o modo está ativo; (ii) A Cisco não tem responsabilidade em relação à sua seleção do modo, e é inteiramente de responsabilidade a ativação do modo; e (iii) Você informará totalmente aos usuários os efeitos do modo sobre as chamadas, como efetuar chamadas e tudo mais. **Observação** Para desativar a Economia de energia adicional, você deve desmarcar a caixa de seleção Permitir substituições de EnergyWise. Se a caixa Permitir substituições de EnergyWise permanecer desmarcada, mas nenhum dia for selecionado no campo Ativar Economia de energia adicional, a Economia de energia adicional não será desativada.

Campo	Descrição
Tempo de telefone ligado	Determina quando o telefone será ligado automaticamente nos dias que estão no campo Ativar Economia de energia adicional. Insira a hora neste campo no formato 24 horas, onde 00:00 corresponde a meia-noite. Por exemplo, para ativar o telefone automaticamente às 7 horas da manhã (0700), insira 07:00. Para ativar o telefone às 2 horas da tarde (1400), insira 14:00. O valor padrão é em branco, o que significa 00:00. **Observação** O Tempo de telefone ligado deve ser pelo menos 20 minutos depois do Tempo de telefone desligado. Por exemplo, se o Tempo de telefone desligado for 07:00, o Tempo de telefone ligado deverá ser no mínimo 07:20.
Tempo de telefone desligado	A hora do dia em que o telefone é desligado nos dias que estão selecionados no campo Ativar Economia de energia adicional. Se os campos Tempo de telefone ligado e Tempo de telefone desligado contiverem o mesmo valor, o telefone não será desligado. Insira a hora neste campo no formato 24 horas, onde 00:00 corresponde a meia-noite. Por exemplo, para desativar o telefone automaticamente às 7 horas da manhã (0700), insira 7:00. Para desativar o telefone às 2 horas da tarde (1400), insira 14:00. O valor padrão é em branco, o que significa 00:00. **Observação** O Tempo de telefone ligado deve ser pelo menos 20 minutos depois do Tempo de telefone desligado. Por exemplo, se o Tempo de telefone desligado for 7:00, o Tempo de telefone ligado deverá ser no mínimo 7:20.
Tempo limite de ociosidade de telefone desligado	Quanto tempo o telefone deve estar ocioso antes de ser desligado. O limite de tempo esgotado ocorre nas seguintes condições: • Quando o telefone estava no modo Economia de energia adicional, conforme programado, e foi retirado desse modo porque o usuário do telefone pressionou a tecla **Selecionar**. • Quando o telefone é religado pelo switch conectado. • Quando o Tempo de telefone desligado é atingido, mas o telefone está em uso. O intervalo do campo é de 20 a 1440 minutos. O valor padrão é de 60 minutos.

Campo	Descrição
Ativar alerta sonoro	Quando ativado, instrui o telefone a reproduzir um alerta sonoro a partir de 10 minutos antes do tempo especificado no campo Tempo de telefone desligado. O alerta sonoro usa o toque do telefone, que é reproduzido brevemente em momentos específicos durante o período de alerta de 10 minutos. O toque de alerta é reproduzido no nível de volume designado pelo usuário. A programação do alerta sonoro é: • 10 minutos antes de desligar, o toque é reproduzido quatro vezes. • 7 minutos antes de desligar, o toque é reproduzido quatro vezes. • 4 minutos antes de desligar, o toque é reproduzido quatro vezes. • 30 segundos antes de desligar, o toque é reproduzido 15 vezes ou até o telefone desligar. Essa caixa de seleção é aplicável somente quando a caixa de lista Ativar Economia de energia adicional tem um ou mais dias selecionados.
Domínio do EnergyWise	O domínio do EnergyWise em que o telefone está. O comprimento máximo deste campo é de 127 caracteres.
Segredo do EnergyWise	A senha secreta de segurança que é usada para se comunicar com os dispositivos no domínio do EnergyWise. O comprimento máximo deste campo é de 127 caracteres.
Permitir substituições de EnergyWise	Esta caixa de seleção determina se você permite que a política do controlador do domínio do EnergyWise envie atualizações de nível de potência para os telefones. As seguintes condições se aplicam: • Um ou mais dias devem ser selecionados no campo Ativar Economia de energia adicional. • As configurações na Administração do Cisco Unified Communications Manager entram em vigor conforme programado, mesmo que o EnergyWise enviar uma substituição. Por exemplo, supondo-se que a opção Tempo de telefone desligado esteja definida como 22:00, o valor no campo Tempo de telefone ligado seja 06:00 e Ativar economia de energia adicional tenha um ou mais dias selecionados. • Se o EnergyWise instruir o telefone para desligar às 20:00, essa diretiva permanecerá em vigor (presumindo que não ocorra intervenção do usuário do telefone) até o Tempo de telefone ligado às 06:00. • Às 06:00, o telefone é ligado e recomeça a receber as alterações de nível de potência das configurações da Administração do Unified Communications Manager. • Para alterar o nível de potência no telefone novamente, o EnergyWise deve reemitir um novo comando de alteração de nível de energia. **Observação** Para desativar a Economia de energia adicional, você deve desmarcar a caixa de seleção Permitir substituições de EnergyWise. Se a caixa Permitir substituições de EnergyWise permanecer desmarcada, mas nenhum dia for selecionado no campo Ativar Economia de energia adicional, a Economia de energia adicional não será desativada.

Etapa 4 Selecione **Salvar**.

Etapa 5 Selecione **Aplicar config.**

Etapa 6 Reinicie o telefone.

Configurar o recurso Não perturbar

Quando o recurso Não perturbar (NãoPtb) está ativado, o cabeçalho na tela do telefone de conferência fica vermelho.

Para obter mais informações, consulte as informações de não perturbar na documentação da sua versão específica do Cisco Unified Communications Manager.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, selecione **Dispositivo** > **Telefone**.

Etapa 2 Localize o telefone a ser configurado.

Etapa 3 Configure os parâmetros a seguir.

- Não perturbar: essa caixa de seleção permite ativar o DND no telefone.
- Opção de DND: Toque desligado, Rejeição de chamada ou Usar configuração do perfil de telefone comum.
- Alerta de chamada recebida em DND: escolha o tipo de alerta, se houver, para reproduzir em um telefone para chamadas recebidas quando o DND estiver ativo.

  Observação Esse parâmetro está localizado na janela Perfil de telefone comum e na janela Configuração do telefone. O valor na janela Configuração do telefone tem precedência.

Etapa 4 Selecione **Salvar**.

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

Configurar notificação de encaminhamento de chamadas

Você pode controlar as configurações de encaminhamento de chamadas.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, selecione **Dispositivo** > **Telefone**.

Etapa 2 Localize o telefone a ser configurado.

Etapa 3 Configure os campos de notificação de encaminhamento de chamadas.

Campo	Descrição
Nome da pessoa que realizou a chamada	Quando essa caixa de seleção é marcada, o nome do autor da chamada é exibido na janela de notificação. Por padrão, essa caixa de seleção está marcada.
Número do chamador	Quando essa caixa de seleção é marcada, o número do autor da chamada é exibido na janela de notificação. Por padrão, essa caixa de seleção não está marcada.
Número redirecionado	Quando essa caixa de seleção é marcada, as informações sobre o autor da chamada que encaminhou a chamada pela última vez são exibidas na janela de notificação. Exemplo: se o Autor da chamada A ligar para B, mas B tiver encaminhado todas as chamadas para C e C encaminhado todas as chamadas para D, a caixa de notificação que D visualiza conterá as informações do telefone do autor da chamada C. Por padrão, essa caixa de seleção não está marcada.
Número Discado	Quando essa caixa de seleção é marcada, as informações sobre o destinatário original da chamada são exibidas na janela de notificação. Exemplo: se o Autor da chamada A ligar para B, mas B tiver encaminhado todas as chamadas para C e C encaminhado todas as chamadas para D, a caixa de notificação que D visualiza conterá as informações do telefone do autor da chamada B. Por padrão, essa caixa de seleção está marcada.

Etapa 4 Selecione **Salvar**.

Configuração do UCR 2008

Os parâmetros que dão suporte ao UCR 2008 estão localizados na Administração do Cisco Unified Communications Manager. A tabela a seguir descreve os parâmetros e indica o caminho para alterar a configuração.

Tabela 21: Local do parâmetro do UCR 2008

Parâmetro	Caminho da administração
Modo FIPS	**Dispositivo** > **Configurações do dispositivo** > **Perfil de telefone comum**
	Sistema > **Configuração do telefone da empresa**
	Dispositivo > **Telefones**
Acesso ao SSH	**Dispositivo** > **Telefone**
	Dispositivo > **Configurações do dispositivo** > **Perfil de telefone comum**

Parâmetro	Caminho da administração
Acesso à Web	**Dispositivo** > **Telefone**
	Sistema > **Configuração do telefone da empresa**
	Dispositivo > **Configurações do dispositivo** > **Perfil de telefone comum**
Sistema > **Configuração do telefone da empresa**	**Dispositivo** > **Configurações do dispositivo** > **Configuração comum do dispositivo**
Modo de endereçamento IP	
Preferência do modo de endereçamento IP para sinalização	**Dispositivo** > **Configurações do dispositivo** > **Configuração comum do dispositivo**

Configurar o UCR 2008 em Configuração comum do dispositivo

Use este procedimento para definir os seguintes parâmetros do UCR 2008:

- Modo de endereçamento IP
- Preferência do modo de endereçamento IP para sinalização

Procedimento

Etapa 1 Em Administração do Cisco Unified Communications Manager, escolha **Dispositivo** > **Configurações de dispositivo** > **Configuração comum do dispositivo**.

Etapa 2 Defina o parâmetro Modo de endereçamento IP.

Etapa 3 Defina o parâmetro Preferência do modo de endereçamento IP para sinalização.

Etapa 4 Selecione **Salvar**.

Configurar o UCR 2008 em Perfil comum de telefone

Use este procedimento para definir os seguintes parâmetros do UCR 2008:

- Modo FIPS
- Acesso ao SSH
- Acesso à Web

Procedimento

Etapa 1 Em Administração do Cisco Unified Communications Manager, escolha **Dispositivo** > **Configurações de dispositivo** > **Perfil de telefone comum**.

Etapa 2 Defina o parâmetro Modo FIPS como **Ativado**.

Etapa 3 Defina o parâmetro Acesso SSH como **Desativado**.

Etapa 4 Defina o parâmetro Acesso à Web como **Desativado**.

Etapa 5 Defina o parâmetro SRTCP de 80 bits como **Ativado**.

Etapa 6 Selecione **Salvar**.

Configurar o UCR 2008 em Configuração do telefone da empresa

Use este procedimento para definir os seguintes parâmetros do UCR 2008:

- Modo FIPS
- Acesso à Web

Procedimento

Etapa 1 Em Administração do Cisco Unified Communications Manager, escolha **Sistema** > **Configuração do telefone da empresa**.

Etapa 2 Defina o parâmetro Modo FIPS como **Ativado**.

Etapa 3 Defina o parâmetro Acesso à Web como **Desativado**.

Etapa 4 Selecione **Salvar**.

Configurar o UCR 2008 no telefone

Use este procedimento para definir os seguintes parâmetros do UCR 2008:

- Modo FIPS
- Acesso ao SSH
- Acesso à Web

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, escolha **Dispositivo** > **Telefone**.

Etapa 2 Defina o parâmetro Acesso SSH como **Desativado**.

Etapa 3 Defina o parâmetro Modo FIPS como **Ativado**.

Etapa 4 Defina o parâmetro Acesso à Web como **Desativado**.

Etapa 5 Selecione **Salvar**.

Acesso móvel e remoto através do Expressway

Acesso móvel e remoto através do Expressway(MRA) permite que funcionários remotos conectem-se de forma fácil e segura à rede corporativa sem usar um túnel cliente da rede virtual privada (VPN). O Expressway

usa TLS (Transport Layer Security) para proteger o tráfego de rede. Para um telefone autenticar um certificado Expressway e estabelecer uma sessão TLS, um certificado Expressway deve ser assinado por uma autoridade de certificação (Certificate Authority) pública considerada confiável pelo firmware do telefone. Não é possível instalar ou confiar em outros certificados da autoridade de certificação em telefones para autenticar um certificado Expressway.

A lista de certificados da autoridade de certificação inseridos no firmware do telefone está disponível em http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html.

Acesso móvel e remoto através do Expressway (MRA) funciona com Cisco Expressway. Você deve já deve estar familiarizado com a documentação do Cisco Expressway, incluindo o *Guia do administrador do Cisco Expressway* e o *Guia de implantação de configuração básica do Cisco Expressway*. A documentação do Cisco Expressway está disponível em http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html.

Somente o protocolo IPv4 é suportado para usuários do Acesso móvel e remoto através do Expressway.

Para obter mais informações sobre como trabalhar com o Acesso móvel e remoto através do Expressway, consulte:

- *Cisco Preferred Architecture for Enterprise Collaboration, Design Overview*
- *Cisco Preferred Architecture for Enterprise Collaboration, CVD*
- *Guia de implantação de Unified Communications Mobile and Remote Access via Cisco VCS*
- *Cisco TelePresence Video Communication Server (VCS), guias de configuração*
- *Guia de implantação de Mobile and Remote Access por meio do Cisco Expressway*

Durante o processo de registro do telefone, o telefone sincroniza a data e a hora exibidas com o servidor NTP (Network Time Protocol). Com o MRA, a marca da opção 42 do DHCP é usada para localizar os endereços IP dos servidores NTP designados para sincronização de data e hora. Se a marca da opção 42 do DHCP não for encontrada nas informações de configuração, o telefone procurará a marca 0.tandberg.pool.ntp.org para identificar os servidores NTP.

Após o registro, o telefone usa informações da mensagem SIP para sincronizar a data e a hora exibidas, a menos que um servidor NTP esteja configurado na configuração do telefone no Cisco Unified Communications Manager.

Observação Se o perfil de segurança de qualquer um de seus telefones tiver Config. criptografada TFTP marcada, você não poderá usar o telefone com Mobile and Remote Access. A solução MRA não é compatível com a interação de dispositivos com a função de proxy de autoridade de certificação (CAPF).

O modo SIP OAuth é suportado para MRA. Esse modo permite usar tokens de acesso OAuth para autenticação em ambientes seguros.

Observação Para SIP OAuth no modo de acesso móvel e remoto (MRA), use apenas o integração do código de ativação com o acesso móvel e remoto quando você implantar o telefone. Não há suporte para a ativação com um nome do usuário e senha.

O modo SIP OAuth exige o Expressway x14.0(1) e posterior ou o Cisco Unified Communications Manager 14.0(1) e posterior.

Para obter informações adicionais sobre o modo SIP OAuth, consulte o *Guia de configuração de recursos para o Cisco Unified Communications Manager*, versão 14.0(1) ou posterior.

Cenários de implantação

A tabela a seguir mostra vários cenários de implantação do Acesso móvel e remoto através do Expressway.

Cenário	Ações
O usuário local entra na rede da empresa, após a implantação do Acesso móvel e remoto através do Expressway.	A rede da empresa é detectada e o telefone é registrado no Cisco Unified Communications Manager como acontece normalmente.
O usuário remoto entra na rede da empresa com o Acesso móvel e remoto através do Expressway.	O telefone detecta que está no modo remoto, a janela Iniciar ses. do Acesso móvel e remoto através do Expressway é aberta e o usuário se conecta à rede corporativa. Os usuários devem ter um nome de serviço, um nome de usuário e uma senha válidos para se conectar à rede. Os usuários também devem redefinir o modo de serviço para limpar a configuração de TFTP alternativo para poder acessar a rede da empresa. Isso limpa a configuração do Servidor TFTP alternativo para que o telefone possa detectar a rede remota. Se um telefone estiver sendo implantado imediatamente, os usuários poderão ignorar o requisito de redefinição das Configurações de rede. Se os usuários tiverem a opção 150 ou a opção 66 do DHCP ativada no respectivo roteador de rede, talvez eles não consigam fazer login na rede corporativa. Os usuários deverão desativar essas configurações do DHCP ou configurar o endereço IP estático diretamente.

Configurar credenciais do usuário persistentes para o início de sessão no Expressway

Quando um usuário entrar na rede com o Acesso móvel e remoto através do Expressway, ele é solicitado a especificar um domínio de serviço, nome de usuário e senha. Se você ativar o parâmetro de Credenciais do usuário persistentes para o login no Expressway, as credenciais de login dos usuários são armazenadas para que eles não precisem inserir novamente essas informações. Esse parâmetro é desativado por padrão.

Você pode configurar credenciais para persistir para um único telefone, um grupo de telefones ou todos os telefones.

Tópicos relacionados

Configuração de recursos do telefone, na página 100

Configuração específica do produto, na página 102

Ferramenta Relatório de problemas

O usuário envia relatórios de problemas para você com a ferramenta Relatório de problemas.

Observação Os logs da ferramenta Relatório de problemas são exigidos pelo Cisco TAC para solucionar problemas. Os registros são limpos se você reiniciar o telefone. Colete os registros antes de reiniciar os telefones.

Para enviar um relatório de problema, os usuários acessam a ferramenta Relatório de problemas e fornecem a data e a hora em que o problema ocorreu e uma descrição do problema.

Se o carregamento do PRT falhar, você poderá acessar o arquivo PRT para o telefone a partir do URL **`http://<phone-ip-address>/FS/<prt-file-name>`**. Esse URL é exibido no telefone nos seguintes casos:

- Se o telefone estiver no estado padrão de fábrica. O URL fica ativo por 1 hora. Após 1 hora, o usuário deve tentar enviar os logs do telefone novamente.
- Se o telefone tiver baixado um arquivo de configuração e o sistema de controle de chamadas permite o acesso via Web ao telefone.

Você deve adicionar um endereço do servidor ao campo **URL de carregamento do suporte ao cliente** no Cisco Unified Communications Manager.

Se você for implantar dispositivos com Mobile and Remote Access através do Expressway, também deverá adicionar o endereço do servidor PRT à lista de permissões do servidor HTTP no servidor Expressway.

Configurar um URL de carregamento do suporte ao cliente

Você deve usa rum servidor com um script de carregamento para receber arquivos PRT. O PRT usa um mecanismo HTTP POST, com os seguintes parâmetros incluídos no carregamento (utilizando codificação MIME de várias partes):

- devicename (exemplo: “SEP001122334455”)
- serialno (exemplo: “FCH12345ABC”)
- username (o nome do usuário configurado no Cisco Unified Communications Manager, o proprietário do dispositivo)
- prt_file (exemplo: “probrep-20141021-162840.tar.gz”)

Um script de exemplo é mostrado abaixo. Esse script é fornecido apenas para referência. A Cisco não fornece suporte ao script de carregamento instalado em um servidor do 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.");
}

?>
```

Observação Os telefones são compatíveis apenas com URLs HTTP.

Procedimento

Etapa 1 Configure um servidor que possa executar o script de carregamento PRT.

Etapa 2 Escreva um script que possa tratar dos parâmetros listados acima ou edite o script de exemplo fornecido para adequá-lo às suas necessidades.

Etapa 3 Carregue o script no servidor.

Etapa 4 No Cisco Unified Communications Manager, vá para área Layout de configuração específica do produto da janela de configuração do dispositivo individual, janela Perfil de telefone comum ou janela Configuração do telefone da empresa.

Etapa 5 Marque **URL de carregamento de suporte ao cliente** e insira o URL de servidor de carregamento.

Exemplo:

http://example.com/prtscript.php

Etapa 6 Salvar suas alterações.

Definir o rótulo de uma linha

Você pode configurar um telefone para exibir um rótulo de texto em vez do número de diretório. Use esse rótulo para identificar a linha por nome ou função. Por exemplo, se o usuário compartilhar linhas no telefone, você poderá identificar a linha com o nome da pessoa que compartilha a linha.

Ao adicionar um rótulo para um módulo de expansão de teclas, somente os primeiros 25 caracteres são exibidos em uma linha.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, selecione **Dispositivo** > **Telefone**.

Etapa 2 Localize o telefone a ser configurado.

Etapa 3 Localize a instância da linha e defina o campo Etiqueta de texto de linha.

Etapa 4 (Opcional) Se o rótulo precisar ser aplicado a outros dispositivos que compartilham a linha, marque a caixa de seleção Atualizar configurações de dispositivo compartilhado e clique em **Propagar selecionado**.

Etapa 5 Selecione **Salvar**.

CAPÍTULO 10

Diretório pessoal e corporativo

Configuração do diretório corporativo

O Diretório corporativo permite a um usuário procurar números de telefone dos colegas de trabalho. Para usar esse recurso, é preciso configurar diretórios corporativos.

Cisco Unified Communications Manager usa um diretório Lightweight Directory Access Protocol (LDAP) para armazenar informações de autenticação e autorização sobre os usuários de aplicativos Cisco Unified Communications Manager que fazem interface com Cisco Unified Communications Manager. A autenticação estabelece os direitos do usuário para acessar o sistema. A autorização identifica os recursos de telefonia que um usuário tem permissão para usar, como um ramal telefônico específico.

Para obter mais informações, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Depois de concluir a configuração do diretório LDAP, os usuários podem usar o serviço de Diretório corporativo no respectivo telefone para procurar os usuários no diretório corporativo.

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

Configuração do diretório pessoal

O Diretório pessoal permite que o usuário armazene um conjunto de números pessoais.

O Diretório pessoal consiste nos seguintes recursos:

- Lista de endereços pessoal (PAB)
- Discagens rápidas

Os usuários podem usar estes métodos para acessar os recursos do Diretório pessoal:

- Em um navegador da Web — os usuários podem acessar os recursos PAB e Discagem rápida do Cisco Unified Communications Portal de Ajuda.

- No Telefone IP Cisco: escolha **Contatos** para pesquisar no diretório corporativo ou na lista de endereços pessoal do usuário.

Para configurar o Diretório pessoal usando um navegador da Web, os usuários devem acessar o Portal de Ajuda. Você deve fornecer aos usuários um URL e as informações para entrar no sistema.

PARTE IV

Solução de problemas do Telefone IP Cisco de conferência

CAPÍTULO 11

Monitoramento de sistemas de telefonia

Visão geral do monitoramento de sistemas de telefonia

É possível visualizar uma variedade de informações sobre o telefone usando o menu de status do telefone no próprio telefone e nas páginas da Web do telefone. Essas informações incluem:

- Informações sobre o dispositivo
- Informações de configuração da rede
- Estatísticas de rede
- Registros do dispositivo
- Estatísticas de transmissão

Este capítulo descreve as informações que você pode obter na página da Web do telefone. É possível usar essas informações para monitorar remotamente a operação de um telefone e auxiliar com a solução de problemas.

Tópicos relacionados

Solução de problemas do telefone, na página 159

Status do Telefone IP Cisco

As seções a seguir descrevem como visualizar informações do modelo, mensagens de status e estatísticas de rede no Telefone IP Cisco.

- Informações do modelo: exibe informações do hardware e do software do telefone.
- Menu Status: fornece acesso a telas que exibem as mensagens de status, as estatísticas de rede e as estatísticas da chamada atual.

É possível usar as informações exibidas nessas telas para monitorar a operação de um telefone e auxiliar com a solução de problemas.

Também é possível obter grande parte dessas informações, além de outras informações relacionadas, remotamente pela página da Web do telefone.

Exibir a janela Informações do telefone

Procedimento

Etapa 1 Pressione **Configurações** > **Informações do sistema**.

Etapa 2 Para sair do menu, pressione **Sair**.

Exibir o menu Status

Procedimento

Etapa 1 Pressione **Configurações** > **Status**.

Etapa 2 Para sair do menu, pressione **Sair**.

Exibir a janela Mensagens de status

Procedimento

Etapa 1 Pressione **Configurações** > **Status** > **Mensagens de status**.

Etapa 2 Para sair do menu, pressione **Sair**.

Campos de mensagens de status

A tabela a seguir descreve as mensagens de status que exibem a tela Mensagens de status do telefone.

Tabela 22: Mensagens de status no Telefone IP Cisco

Mensagem	Descrição	Explicação possível e ação
Não foi possível adquirir um endereço IP a partir do DHCP	O telefone não obteve previamente um endereço IP do servidor DHCP. Isso pode ocorrer quando você faz uma restauração da configuração inicial ou de fábrica.	Confirme se o servidor DHCP está disp IP está disponível para o telefone.

Mensagem	Descrição	Explicação possível e ação
Erro de tamanho de TFTP	O arquivo de configuração é muito grande para o sistema de arquivos do telefone.	Desligue e religue o telefone.
Erro de soma de verificação ROM	O arquivo de software baixado está corrompido.	Obtenha uma nova cópia do firmwa no diretório TFTPPath. Você deve co somente quando o software do servi caso contrário, os arquivos serão co
IP duplicado	Outro dispositivo está usando o endereço IP que está atribuído ao telefone.	Se o telefone tiver um endereço IP não atribuiu um endereço IP duplic Se você estiver usando DHCP, veri servidor DHCP.
Apagando arquivos CTL e ITL	Apagando arquivo CTL ou ITL.	Nenhuma. Essa mensagem é apena
Erro ao atualizar localização	Um ou mais arquivos de localização não foram encontrados no diretório do caminho do TFTP ou não são válidos. A localidade não foi alterada.	Na Administração do sistema opera verifique se os seguintes arquivos e subdiretórios no Gerenciamento de • Localizados no subdiretório co localidade da rede: • tones.xml • Localizados no subdiretório co localidade do usuário: • glyphs.xml • dictionary.xml • kate.xml
Arquivo não encontrado <Cfg File>	O arquivo de configuração padrão baseado em nome não foi encontrado no servidor TFTP.	O arquivo de configuração de um te telefone é adicionado ao banco de c Communications Manager. Se o tel de dados do Cisco Unified Commun TFTP gera uma resposta **Arquivo** • O telefone não está registrado Communications Manager. Você deverá adicionar manual Unified Communications Man os telefones sejam registrados • Se você estiver usando DHCP, DHCP está apontando para o s • Se você estiver usando endere configuração do servidor TFT

Mensagem	Descrição	Explicação possível e ação
Arquivo não encontrado <CTLFile.tlv>	Esta mensagem é exibida no telefone quando o cluster do Cisco Unified Communications Manager não está no modo seguro.	Não há impacto; o telefone ainda pode Unified Communications Manager.
Endereço IP liberado	O telefone está configurado para liberar o endereço IP.	O telefone permanece ocioso até ser de você redefinir o endereço DHCP.
Tempo esgotado p/DHCP de IPv4	O servidor DHCP IPv4 não respondeu.	A rede está ocupada: os erros deverão s quando a carga da rede diminuir. Não há conectividade de rede entre o s telefone: verifique as conexões de rede O servidor DHCP IPv4 está fora do ar: do servidor DHCP IPv4. Erro persistente: é recomendável atribu estático.
Tempo esgotado p/DHCP de IPv6	O servidor DHCP IPv6 não respondeu.	A rede está ocupada: os erros deverão s quando a carga da rede diminuir. Não há conectividade de rede entre o s telefone: verifique as conexões de rede O servidor DHCP IPv6 está fora do ar: do servidor DHCP IPv6. Erro persistente: é recomendável atribu estático.
Tempo esgotado p/DNS de IPv4	O servidor DNS IPv4 não respondeu.	A rede está ocupada: os erros deverão s quando a carga da rede diminuir. Não há conectividade de rede entre o s telefone: verifique as conexões de rede O servidor DNS IPv4 está fora do ar: v do servidor DNS IPv4.
Tempo esgotado p/DNS de IPv6	O servidor DNS IPv6 não respondeu.	A rede está ocupada: os erros deverão s quando a carga da rede diminuir. Não há conectividade de rede entre o s telefone: verifique as conexões de rede O servidor DNS IPv6 está fora do ar: v do servidor DNS IPv6.
Host IPv4 desconhecido para DNS	O DNS IPv4 não pôde resolver o nome do servidor TFTP ou do Cisco Unified Communications Manager.	Verifique se os nomes de host do servi Unified Communications Manager estã corretamente no DNS IPv4. É recomendável usar endereços IPv4 e

Mensagem	Descrição	Explicação possível e ação
Host IPv6 desconhecido para DNS	O DNS IPv6 não pôde resolver o nome do servidor TFTP ou do Cisco Unified Communications Manager.	Verifique se os nomes de host do se Unified Communications Manager corretamente no DNS IPv6. É recomendável usar endereços IPv
Carregamento rejeitado HC	O aplicativo baixado não é compatível com o hardware do telefone.	Ocorre se você tentar instalar uma telefone que não suporta alterações Verifique o ID de carga atribuído ac Communications Manager, escolha Reinsira a carga que é exibida no te
Sem roteador padrão	A configuração DHCP ou estática não especificou um roteador padrão.	Se o telefone tiver um endereço IP roteador padrão está configurado. Se você estiver usando DHCP, o se um roteador padrão. Verifique a conf
Sem servidor DNS de IPv4	Um nome foi especificado, mas a configuração de IP DHCP ou estático não especificou um endereço de servidor DNS IPv4.	Se o telefone tiver um endereço IP servidor DNS IPv4 está configurad Se você estiver usando DHCP, o se um servidor DNS IPv4. Verifique a DHCP.
Sem servidor DNS de IPv6	Um nome foi especificado, mas a configuração de IP DHCP ou estático não especificou um endereço de servidor DNS IPv6.	Se o telefone tiver um endereço IP servidor DNS IPv6 está configurad Se você estiver usando DHCP, o se um servidor DNS IPv6. Verifique a DHCP.
Não há lista de certificados credíveis instalada	O arquivo CTL ou o arquivo ITL não está instalado no telefone.	A lista de confiança não está config Communications Manager, que não por padrão. A lista de confiança não está config Para obter mais informações sobre as a documentação da sua versão espe Communications Manager.
Falha ao registrar o telefone. O tamanho da chave do certificado não é compatível com FIPS.	A norma FIPS exige que o certificado do servidor RSA seja de no mínimo 2048 bits.	Atualize o certificado.
Reinicialização solicitada pelo Cisco Unified Communications Manager	O telefone está sendo reiniciado devido a uma solicitação do Cisco Unified Communications Manager.	Provavelmente foram feitas alteraçõ telefone no Cisco Unified Commun **config.** foi pressionado para que as
Erro de acesso ao TFTP	O servidor TFTP está apontando para um diretório que não existe.	Se você estiver usando DHCP, veri está apontando para o servidor TFT Se você estiver usando endereços I configuração do servidor TFTP.

Mensagem	Descrição	Explicação possível e ação
Erro de TFTP	O telefone não reconhece um código de erro que o servidor TFTP forneceu.	Entre em contato com o Cisco TAC.
Tempo esgotado de TFTP	O servidor TFTP não respondeu.	A rede está ocupada: os erros deverão s quando a carga da rede diminuir. Não há conectividade de rede entre o ser verifique as conexões de rede. O servidor TFTP está fora do ar: verifi servidor TFTP.
Limite de tempo esgotado	O suplicante tentou a transação 802.1X, mas o limite de tempo se esgotou devido à ausência de um autenticador.	A autenticação normalmente atinge o t 802.1X não está configurado no switch
Falha na atualização da lista de certificados credíveis	A atualização dos arquivos CTL e ITL falhou.	O telefone tem arquivos CTL e ITL ins os novos arquivos CTL e ITL. Possíveis motivos da falha: • Ocorreu uma falha na rede. • O servidor TFTP estava fora do ar • O novo token de segurança que fo arquivo CTL e o certificado TFTP c o arquivo ITL foram introduzidos disponíveis nos arquivos CTL e IT • Ocorreu uma falha interna no tele Soluções possíveis: • Verifique a conectividade de rede. • Verifique se o servidor TFTP está normalmente. • Se o servidor TVS (Transactional compatível com o Cisco Unified Co verifique se o servidor TVS está a normalmente. • Verifique se o token de segurança válidos. Exclua manualmente os arquivos CTL e anteriores falharem; restaure o telefone Para obter mais informações sobre as list a documentação da sua versão específi Communications Manager.
Lista de certificados credíveis atualizada	O arquivo CTL, o arquivo ITL ou os dois arquivos estão atualizados.	Nenhuma. Essa mensagem é apenas in Para obter mais informações sobre as list a documentação da sua versão específi Communications Manager.

Mensagem	Descrição	Explicação possível e ação
Erro de versão	O nome do arquivo de carga do telefone está incorreto.	Certifique-se de que o arquivo de ca correto.
XmlDefault.cnf.xml, ou .cnf.xml correspondente ao nome do dispositivo telefônico	Nome do arquivo de configuração.	Nenhuma. Essa mensagem indica o configuração do telefone.

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

Exibir a janela Estatísticas da rede

Procedimento

Etapa 1 Pressione **Configurações** > **Status** > **Estatísticas da rede**.

Etapa 2 Para sair do menu, pressione **Sair**.

Campos de estatísticas de rede

A tabela a seguir descreve as informações da tela Estatísticas de rede.

Tabela 23: Campos de estatísticas de rede

Item	Descrição
quadros Tx	Número de pacotes enviados pelo telefone
Tx broadcast	Número de pacotes broadcast enviados pelo telefone
Tx unicast	Número total de pacotes unicast transmitidos pelo telefone
Quadros Rx	Número de pacotes recebidos pelo telefone
Rx broadcast	Número de pacotes broadcast recebidos pelo telefone
Rx unicast	Número total de pacotes unicast recebidos pelo telefone
ID de dispositivo de vizinho de CDP	Identificador de um dispositivo conectado a essa porta descoberto pelo protocolo CDP.
Endereço IP de vizinho de CDP	Identificador de um dispositivo conectado a essa porta descoberto pelo protocolo CDP usando IP.
Porta de vizinho de CDP	Identificador de um dispositivo conectado a essa porta descoberto pelo protocolo CDP.

Item	Descrição
Causa do reinício: um destes valores: • Redefinição de hardware (redefinição para ativação) • Redefinição de software (o controlador de memória também é redefinido) • Redefinição de software (o controlador de memória não é redefinido) • Redefinição do watchdog • Initialized • Desconhecido	Causa da última redefinição do telefone
porta 1	Estado do link e conexão da porta de rede (por exemplo, **100 Todo** significa que a porta do PC está em um estado de link ativo e tem uma conexão de 100 Mbps full-duplex negociada automaticamente)
IPv4	Informações sobre o status do DHCP. Isso inclui os seguintes estados: • CDP BOUND • CDP INIT • DHCP BOUND • DHCP DISABLED • DHCP INIT • DHCP INVALID • DHCP REBINDING • DHCP REBOOT • DHCP RENEWING • DHCP REQUESTING • DHCP RESYNC • DHCP UNRECOGNIZED • DHCP WAITING COLDBOOT TIMEOUT • DISABLED DUPLICATE IP • SET DHCP COLDBOOT • SET DHCP DISABLED • SET DHCP FAST

Item	Descrição
IPv6	Informações sobre o status do DHCP. Isso inclui os seguintes estados: • CDP INIT • DHCP6 BOUND • DHCP6 DISABLED • DHCP6 RENEW • DHCP6 REBIND • DHCP6 INIT • DHCP6 SOLICIT • DHCP6 REQUEST • DHCP6 RELEASING • DHCP6 RELEASED • DHCP6 DISABLING • DHCP6 DECLINING • DHCP6 DECLINED • DHCP6 INFOREQ • DHCP6 INFOREQ DONE • DHCP6 INVALID • DISABLED DUPLICATE IPV6 • DHCP6 DECLINED DUPLICATE IP • ROUTER ADVERTISE • DHCP6 WAITING COLDBOOT TIMEOUT • DHCP6 TIMEOUT USING RESTORED VAL • DHCP6 TIMEOUT CANNOT RESTORE • IPV6 STACK TURNED OFF • ROUTER ADVERTISE • ROUTER ADVERTISE • UNRECOGNIZED MANAGED BY • ILLEGAL IPV6 STATE

Exibir a janela Estatísticas da chamada

Procedimento

Etapa 1 Pressione **Configurações** > **Status** > **Estatísticas da chamada**.

Etapa 2 Para sair do menu, pressione **Sair**.

Campos de estatísticas da chamada

A tabela a seguir descreve os itens na tela de Estatísticas da chamada.

Tabela 24: Itens de estatísticas da chamada

Item	Descrição
Codec do receptor	Tipo de fluxo de voz recebido (áudio de fluxo RTP de codec): • G0.729 • G.722 • 722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS
Codec do emissor	Tipo de fluxo de voz transmitido (áudio de fluxo RTP de codec): • G0.729 • G.722 • 722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS
Tamanho do receptor	Tamanho de pacotes de voz, em milissegundos, no fluxo de voz recebido (áudio de fluxo RTP).
Tamanho do emissor	Tamanho de pacotes de voz, em milissegundos, no fluxo de voz transmitido (áudio de fluxo RTP).

Item	Descrição
Pacotes do receptor	Número de pacotes de voz RTP que foram recebidos desde a abertura do fluxo de voz. **Observação** Esse número não é necessariamente idêntico ao número de pacotes de voz RTP que foram recebidos desde o início da chamada porque a chamada pode ter sido colocada em espera.
Pacotes do emissor	Número de pacotes de voz RTP que foram transmitidos desde a abertura do fluxo de voz. **Observação** Esse número não é necessariamente idêntico ao número de pacotes de voz RTP que foram transmitidos desde o início da chamada porque a chamada pode ter sido colocada em espera.
Instabilidade média	Instabilidade média estimada dos pacotes RTP (atraso dinâmico que um pacote encontra ao passar pela rede), em milissegundos, observada desde a abertura do fluxo de voz recebido.
Instabilidade máxima	Instabilidade máxima, em milissegundos, observada desde a abertura do fluxo de voz recebido.
Receptor abandonado	Número de pacotes RTP no fluxo de voz recebido que foram descartados (pacotes inválidos, atrasados, etc.). **Observação** O telefone descarta os pacotes de ruído confortável de carga tipo 19 gerados pelos Gateways da Cisco porque eles incrementam esse contador.
Pacotes perdidos do receptor	Pacotes RTP perdidos (em trânsito).
Métricas de qualidade da voz	
Taxa ocult. cumulativa	Número total de quadros de ocultação dividido pelo número total de quadros de fala que foram recebidos desde o início do fluxo de voz.
Taxa ocultação do intervalo	Taxa de quadros de ocultação para quadros de fala no intervalo anterior de 3 segundos da fala ativa. Se a VAD (detecção de atividade de voz) estiver em uso, talvez seja necessário um intervalo mais longo para acumular 3 segundos de fala ativa.
Taxa ocultação máxima	Taxa mais alta de ocultação do intervalo desde o início do fluxo de voz.
Ocultar segs.	Número de segundos que tem eventos de ocultação (quadros perdidos) desde o início do fluxo de voz (inclui segundos severamente ocultados).
Ocultar segs. estritamente	Número de segundos que tem mais de 5% de eventos de ocultação (quadros perdidos) desde o início do fluxo de voz.
Latência	Estimativa da latência da rede, expressa em milissegundos. Representa a média de execução do atraso na resposta, medida quando os blocos de relatório do receptor RTCP são recebidos.

Página da Web do Telefone IP Cisco

Cada Telefone IP Cisco tem uma página da Web na qual é possível ver uma variedade de informações sobre o telefone, incluindo:

- Informações sobre dispositivo: exibem configurações do dispositivo e informações relacionadas do telefone.
- Configuração de rede: exibe informações de configuração de rede e informações sobre outras configurações do telefone.
- Estatísticas de rede: exibem hiperlinks que fornecem informações sobre o tráfego da rede.
- Logs de dispositivo: exibem hiperlinks que fornecem informações que você pode usar para solução de problemas.
- Estatísticas de transmissão: exibem hiperlinks para uma variedade de estatísticas de transmissão.

Essa seção descreve as informações que você pode obter na página da Web do telefone. É possível usar essas informações para monitorar remotamente a operação de um telefone e auxiliar com a solução de problemas.

Também é possível obter muito dessas informações diretamente de um telefone.

Acessar página da Web do telefone

Observação Se não for possível acessar a página da Web, talvez ela esteja desativada por padrão.

Procedimento

Etapa 1 Obtenha o endereço IP do Telefone IP Cisco usando um destes métodos:

a) Procure o telefone em Administração do Cisco Unified Communications Manager escolhendo **Dispositivo** > **Telefone**. Os telefones registrados no Cisco Unified Communications Manager exibem o endereço IP na janela Localizar e listar telefones e na parte superior da janela Configuração do telefone.

b) No telefone, pressione **Configurações** > **Informações do sistema** e, em seguida, role até ao campo Endereço IPv4.

Etapa 2 Abra um navegador da Web e insira o seguinte URL, onde *endereço_IP* é o endereço IP do Telefone IP Cisco:

http://<IP_address>

Página da Web Informações sobre o dispositivo

A área Informações sobre dispositivo em uma página da Web do telefone exibe configurações do dispositivo e informações relacionadas do telefone. A tabela a seguir descreve esses itens.

Para exibir a área Informações sobre dispositivo, acesse a página da Web do telefone e clique no hiperlink **Informações sobre dispositivo**.

Tabela 25: Campos da página da Web de Informações sobre o dispositivo

Campo	Descrição
Modo de serviço	O modo de serviço do telefone.
Domínio do serviço	O domínio do serviço.
Estado do serviço	O estado atual do serviço.
Endereço MAC	Endereço MAC (Controle de acesso à mídia) do telefone.
Nome de host	Nome exclusivo e fixo que é atribuído automaticamente ao telefone com base no endereço MAC.
Número do telefone	Número de diretório que é atribuído ao telefone.
Firmware de aplicação	Identifica a versão de carga do aplicativo.
Boot Load ID	Indica a versão da carga de inicialização.
Versão	Identificador do firmware que está em execução no telefone.
Revisão do hardware	Valor de revisão secundária do hardware do telefone.
Número de série	Número de série exclusivo do telefone.
Número do modelo	Número do modelo do telefone.
Mensagem em espera	Indica se uma mensagem de voz está aguardando na linha principal do telefone.
UDI	Exibe as seguintes informações UDI (Identificador exclusivo do dispositivo) da Cisco sobre o telefone: • Tipo de hardware • Nome do modelo do telefone • Identificador do produto • ID da versão (VID): especifica o número da versão do hardware principal. • Número de série
Hora	Hora do Grupo de data/hora ao qual o telefone pertence. Essas informações são extraídas do Cisco Unified Communications Manager.
Fuso Horário	Fuso horário do Grupo de data/hora ao qual o telefone pertence. Essas informações são extraídas do Cisco Unified Communications Manager.
Data	Data do Grupo de data/hora ao qual o telefone pertence. Essas informações são extraídas do Cisco Unified Communications Manager.
Memória livre do sistema	Quantidade de memória disponível no sistema.

Campo	Descrição
Memória livre do heap do Java	Quantidade de memória livre para o heap do Java.
Memória livre do pool de Java	Quantidade de memória livre para o pool do Java.
Modo FIPS ativado	Indica se o Modo FIPS (Federal Information processing Standard) está ativado.

Página da Web de configuração de rede

A área Configuração de rede na página da Web de um telefone exibe informações de configuração de rede e sobre outras configurações do telefone. A tabela a seguir descreve esses itens.

Você pode visualizar e definir muitos desses itens no menu Configuração de rede no Telefone IP Cisco.

Para exibir a área Configuração de rede, acesse a página da Web do telefone e clique no hiperlink **Configuração de rede**.

Tabela 26: Itens da área Configuração de rede

Item	Descrição
Endereço MAC	Endereço MAC (Controle de acesso à mídia) do telefone.
Nome de host	Nome do host que o servidor DHCP atribuiu ao telefone.
Nome do domínio	Nome do domínio DNS (Sistema de nome de domínio) no qual o telefone reside.
Servidor DHCP	Endereço IP do servidor do protocolo DHCP (Dynamic Host Configuration Protocol) do qual o obtém o endereço IP.
Servidor BOOTP	Indica se o telefone obtém a configuração de um servidor do protocolo BootP (Booststrap Pr
DHCP	Indica se o telefone usa DHCP.
Endereço IP	Endereço IP do telefone.
Máscara de sub-rede	Máscara de sub-rede usada pelo telefone.
Roteador padrão 1	O roteador padrão que o telefone usa.
Servidor DNS de 1 a 3	Servidor DNS (Domain Name System) primário (Servidor DNS 1) e servidores DNS opcion reserva (Servidor DNS 2) utilizados pelo telefone.
TFTP alternativo	Indica se o telefone está usando um servidor TFTP alternativo.
Servidor TFTP 1	Servidor do protocolo TFTP (Trivial File Transfer Protocol) primário que o telefone usa.
Servidor TFTP 2	Servidor do protocolo TFTP (Trivial File Transfer Protocol) de backup que o telefone usa.
Endereço DHCP liberado	Indica a configuração da opção Endereço DHCP liberado.

Item	Descrição
ID da VLAN operacional	VLAN (Rede local virtual) operacional que é configurada em um switch do Cisco Cataly telefone é um membro.
ID da VLAN administrativa	VLAN auxiliar do qual o telefone é um membro.
Unified CM 1 a 5	Nomes de host ou endereços IP, em ordem de prioridade, dos servidores Cisco Unified Com Manager nos quais o telefone pode se registrar. Um item também pode mostrar o endereç roteador SRST que é capaz de fornecer funcionalidade limitada do Cisco Unified Commu Manager, se tal roteador estiver disponível. Em um servidor disponível, um item mostra o endereço IP do servidor Cisco Unified Com Manager e um dos seguintes estados: • Ativo: o servidor Cisco Unified Communications Manager do qual o telefone está at recebendo serviços de processamento de chamadas. • Suspensão: o servidor Cisco Unified Communications Manager para o qual o telefor o servidor atual ficar indisponível • Em branco: sem conexão atual com esse servidor Cisco Unified Communications M Um item também pode incluir a designação SRST (Survivable Remote Site Telephony), q um roteador SRST capaz de fornecer funcionalidade do Cisco Unified Communications M um conjunto de recursos limitado. Esse roteador assume o controle de todo o processamento se todos os outros servidores Cisco Unified Communications Manager ficarem indisponív Unified Communications Manager SRST sempre aparece por último na lista de servidore estiver ativo. Você configura o endereço do roteador SRST na seção Pool de dispositivos Configuração do Cisco Unified Communications Manager.
URL das Informações	URL do texto de ajuda que aparece no telefone.
URL de diretórios	URL do servidor do qual o telefone obtém informações do diretório.
URL de Mensagens	URL do servidor do qual o telefone obtém serviços de mensagens.
URL de Serviços	URL do servidor do qual o telefone obtém serviços do Telefone IP Cisco.
URL Ociosa	URL que o telefone exibe quando está ocioso pelo tempo especificado no campo Tempo de e nenhum menu está aberto.
Tempo de inatividade do URL	Número de segundos pelo qual o telefone está ocioso e nenhum menu é aberto antes da at serviço XML que o URL ocioso especifica.
URL do Servidor Proxy	URL do servidor proxy, que faz solicitações HTTP a endereços de host não locais em nom HTTP do telefone e fornece respostas do host não local ao cliente HTTP do telefone.
URL de autenticação	URL que o telefone usa para validar solicitações que são feitas ao servidor Web do telefo

Item	Descrição
Config. porta do switch	Velocidade e duplex da porta do switch, onde: • A = Negociação automática • 10H = 10-BaseT/half-duplex • 10F = 10-BaseT/full-duplex • 100H = 100-BaseT/half-duplex • 100F = 100-BaseT/full-duplex • 1000F = 1000-BaseT/full-duplex • Sem link = nenhuma conexão com a porta do switch
Localidade do Usuário	Localidade do usuário associada ao usuário de telefonia. Identifica um conjunto de informaç detalhadas para oferecer suporte aos usuários, incluindo idioma, fonte, formatação de data e l informações de texto de teclado alfanumérico.
Localidade da Rede	Localidade da rede associada ao usuário de telefonia. Identifica o conjunto de informações de para oferecer suporte ao telefone em um local específico, incluindo definições dos tons e cad usadas pelo telefone.
Versão localização usuário	Versão da localidade do usuário que é carregada no telefone.
Versão de localização de rede	Versão da localidade da rede que é carregada no telefone.
Alto-falante ativado	Indica se o alto-falante está ativado no telefone.
Escuta em grupo	Indica se o recurso de escuta em grupo está ativado no telefone. A escuta em grupo permite c usando o monofone e ouvir no alto-falante ao mesmo tempo.
GARP ativado	Indica se o telefone aprende endereços MAC de respostas ARP gratuitas.
Seleção linha auto. ativada	Indica se o telefone muda o foco da chamada para chamadas recebidas em todas as linhas.
DSCP para controle chamada	Classificação de IP DSCP para sinalização do controle de chamadas.
DSCP para configuração	Classificação de IP DSCP para qualquer transferência de configuração do telefone.
DSCP para serviços	Classificação de IP DSCP para serviços baseados no telefone.
Modo de segurança	Modo de segurança que é definido para o telefone.
Acesso à Web ativado	Indica se o acesso à Web está ativado (Sim) ou desativado (Não) para o telefone.
Acesso ao SSH ativado	Indica se o telefone aceita ou bloqueia as conexões SSH.

Item	Descrição
CDP: Porta do switch	Indica se há suporte ao CDP na porta do switch (o padrão é ativado). Ative o CDP na porta do switch para atribuição de VLAN do telefone, negociação de ene gerenciamento de QoS e segurança 802.1x. Ative o CDP na porta do switch quando o telefone se conectar a um switch da Cisco. Quando o CDP é desativado no Cisco Unified Communications Manager, um aviso é exibid que o CDP deverá ser desativado na porta do switch somente se o telefone se conectar a un não seja da Cisco. Os valores atuais de CDP da porta do switch e do PC são mostrados no menu Configuraç
LLDP-MED: Porta do switch	Indica se o protocolo LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Disc ativado na porta do switch.
Prioridade da potência LLDP	Informa a prioridade de potência do telefone para o switch, permitindo que o switch forne adequadamente para os telefones. As configurações incluem: • Desconhecido: esse é o valor padrão. • Baixo • Alta • Crítico
ID do ativo LLDP	Identifica o ID do ativo atribuído ao telefone para gerenciamento de inventário.
Arquivo CTL	Identifica o arquivo CTL.
Arquivo ITL	O arquivo ITL contém a lista de confiança inicial.
Assinatura ITL	Aprimora a segurança usando o algoritmo de hash seguro (SHA-1) nos arquivos CTL e I
Servidor CAPF	O nome do servidor CAPF usado pelo telefone.
TVS	O principal componente da Segurança por Padrão. O TVS (Trust Verification Services) p Telefones IP Cisco Unified autenticar servidores de aplicativos, como serviços do EM, di MIDlet, durante a definição do HTTPS.
Servidor TFTP	O nome do servidor TFTP usado pelo telefone.
Sincronização automática da porta	Sincroniza as portas com a velocidade inferior que elimina a perda de pacotes.
Configuração remota da porta do switch	Permite ao administrador configurar a velocidade e a função da porta de tabela do Cisco I Collaboration Experience remotamente usando a Administração do Cisco Unified Comm Manager.
Configuração remota da porta do computador	Indica se a configuração da porta remota do modo duplex e da velocidade da porta do PC ou desativada.
Modo de endereçamento IP	Exibe o modo de endereçamento IP que está disponível no telefone.

Item	Descrição
Controle de modo de preferências IP	Indica a versão do endereço IP que o telefone usa durante a sinalização com o Cisco Unified Communications Manager quando o IPv4 e IPv6 estão disponíveis no telefone.
Modo de preferências IP para mídia	Indica que a mídia do dispositivo usa um endereço IPv4 para se conectar ao Cisco Unified Communications Manager.
Configuração de IPv6 auto	Exibe se a configuração automática está ativada ou desativada no telefone.
IPv6 DAD	Verifica a exclusividade dos novos endereços IPv6 unicast antes da atribuição dos endereços às in
IPv6 Aceitar mensagem de redirecionamento	Indica se o telefone aceita as mensagens de redirecionamento do mesmo roteador que é usad número de destino.
IPv6 Responder à solicitação de eco de multicast	Indica se o telefone envia uma mensagem de Resposta de eco na resposta a uma mensagem de So de eco enviada a um endereço IPv6.
Servidor de carregamento de IPv6	Usado para otimizar o tempo de instalação das atualizações de firmware do telefone e descar WAN armazenando imagens localmente, eliminando a necessidade de desviar o link de WAN cada atualização do telefone.
Servidor de registro IPv6	Indica o endereço IP e a porta da máquina de registro em log remoto para a qual o telefone en mensagens de log.
Servidor CAPF IPv6	Nome comum (no Certificado do Cisco Unified Communications Manager) da CAPF usado telefone.
DHCPv6	O protocolo DHCP atribui automaticamente o endereço IPv6 a dispositivos quando você os c rede. Os Telefones IP Cisco Unified ativam o DHCP por padrão.
Endereço IPv6	Exibe o endereço IPv6 atual do telefone ou permite que o usuário insira um novo endereço IP
Tamanho do prefixo IPv6	Exibe o comprimento do prefixo atual para a sub-rede ou permite que o usuário insira um no comprimento de prefixo.
Roteador padrão IPv6 1	Exibe o roteador padrão usado pelo telefone ou permite ao usuário inserir um novo roteador IPv6.
Servidor DNS IPv6 1	Exibe o servidor DNSv6 primário usado pelo telefone ou permite que o usuário insira um novo
Servidor DNS IPv6 2	Exibe o servidor DNSv6 secundário usado pelo telefone ou permite que o usuário defina um servidor DNSv6 secundário.
TFTP alternativo de IPv6	Permite ao usuário ativar o uso de um servidor TFTP IPv6 alternativo (secundário).
Servidor TFTP 1 de IPv6	Exibe o servidor TFTP IPv6 primário usado pelo telefone ou permite que o usuário defina un servidor TFTP primário.
Servidor TFTP 2 de IPv6	Exibe o servidor TFTP IPv6 secundário usado se o servidor TFTP IPv6 primário ficar indispo permite que o usuário defina um novo servidor TFTP secundário.
Endereço IPv6 liberado	Permite que o usuário libere informações relacionadas ao IPv6.

Item	Descrição
Nível de potência do Energywise	A medida da energia consumida por dispositivos em uma rede EnergyWise.
Domínio do Energywise	Um agrupamento administrativo de dispositivos com a finalidade de monitoramento e co

Página da Web Informações sobre a Ethernet

A tabela a seguir descreve o conteúdo da página da Web Informações sobre a Ethernet.

Tabela 27: Itens de Informações sobre a Ethernet

Item	Descrição
quadros Tx	Número total de pacotes que o telefone transmite.
Tx broadcast	Número total de pacotes broadcast que o telefone transmite.
Tx multicast	Número total de pacotes multicast que o telefone transmite.
Tx unicast	Número total de pacotes unicast que o telefone transmite.
Quadros Rx	Número total de pacotes recebidos pelo telefone.
Rx broadcast	Número total de pacotes broadcast que o telefone recebe.
Rx multicast	Número total de pacotes multicast que o telefone recebe.
Rx unicast	Número total de pacotes unicast que o telefone recebe.
Rx PacketNoDes	Número total de pacotes dispersos gerados pelo descritor sem DMA (Acesso direto à memória).

Páginas da Web de rede

A tabela a seguir descreve as informações nas páginas da Web Área de rede.

Observação Quando você clica no link **Rede** abaixo de Estatísticas da rede, a página é intitulada “Informações sobre a porta”.

Tabela 28: Itens da área de rede

Item	Descrição
Rx totalPkt	Número total de pacotes que o telefone recebeu.
Rx multicast	Número total de pacotes multicast que o telefone recebeu.
Rx broadcast	Número total de pacotes broadcast que o telefone recebeu.

Item	Descrição
Rx unicast	Número total de pacotes unicast que o telefone recebeu.
Rx tokenDrop	Número total de pacotes que foram descartados devido à falta de recursos (por exemplo, excedente de FIFO).
Tx totalGoodPkt	Número total de pacotes em boas condições (multicast, broadcast e unicast) que o telefone recebeu.
Tx broadcast	Número total de pacotes broadcast que o telefone transmitiu.
Tx multicast	Número total de pacotes multicast que o telefone transmitiu.
LLDP FramesOutTotal	Número total de quadros LLDP que o telefone enviou.
LLDP AgeoutsTotal	Número total de quadros LLDP com tempo limite esgotado no cache.
LLDP FramesDiscardedTotal	Número total de quadros LLDP que foram descartados quando qualquer um dos TLVs obrigatórios esteve ausente, fora de ordem ou continha comprimento de string fora do intervalo.
LLDP FramesInErrorsTotal	Número total de quadros LLDP que foram recebidos com um ou mais erros detectáveis.
LLDP FramesInTotal	Número total de quadros LLDP que o telefone recebe.
LLDP TLVDiscardedTotal	Número total de TLVs LLDP que são descartados.
LLDP TLVUnrecognizedTotal	Número total de TLVs LLDP que não são reconhecidos no telefone.
ID de dispositivo de vizinho de CDP	Identificador de um dispositivo conectado a essa porta descoberto pelo CDP.
Endereço IP de vizinho de CDP	Endereço IP do dispositivo vizinho descoberto pelo CDP.
Endereço IPv6 de vizinho de CDP	Endereço IPv6 do dispositivo vizinho descoberto pelo CDP.
Porta de vizinho de CDP	Porta do dispositivo vizinho à qual o telefone está conectado descoberta pelo CDP.
ID de dispositivo de vizinho de LLDP	Identificador de um dispositivo conectado a essa porta descoberto pelo LLDP.
Endereço IP de vizinho de LLDP	Endereço IP do dispositivo vizinho descoberto pelo LLDP.
Endereço IPv6 de vizinho de LLDP	Endereço IPv6 do dispositivo vizinho descoberto pelo CDP.
Porta de vizinho de LLDP	Porta do dispositivo vizinho à qual o telefone se conecta descoberta pelo LLDP.
Informações sobre a porta	Informações de velocidade e duplex.

Páginas da Web de logs do console, dumps do core, mensagens de status e exibição de depuração

Sob o título de Logs de dispositivo, os hiperlinks de Logs do console, Dumps do core, Mensagens de status e Exibição de depuração fornecem informações que ajudam a monitorar e solucionar problemas do telefone.

- Logs do console — inclui hiperlinks para arquivos de log individuais. O arquivos de log do console incluem mensagens de erro e depuração que o telefone recebeu
- Dumps do core — inclui hiperlinks para arquivos de dump individuais. Os arquivos de dump do core incluem dados da falha de um telefone.
- Mensagens de status — exibe as 10 mensagens de status mais recentes que o telefone gerou desde a última vez em que foi ligado. Você também pode ver essas informações na tela Mensagens de status no telefone.
- Exibição de depuração — exibe mensagens de depuração que podem ser úteis para o Cisco TAC caso você necessite de assistência com a solução de problemas.

Página da Web de estatísticas de transmissão

Um Telefone IP Cisco pode transmitir informações bidirecionalmente para até cinco dispositivos em simultâneo. Um telefone transmite informações quando está em uma chamada ou executando um serviço que envia ou recebe áudio ou dados.

As áreas de estatísticas de transmissão em uma página da Web do telefone fornecem informações sobre os fluxos.

Para exibir uma área de Estatísticas de transmissão, acesse a página da Web do telefone e clique em um hiperlink **Fluxo**.

A tabela a seguir descreve os itens nas áreas Estatísticas de transmissão.

Tabela 29: Campos de estatísticas de transmissão

Item	Descrição
Endereço Remoto	Endereço IP e porta UDP do destino do fluxo.
Endereço local	Endereço IP e porta UDP do telefone.
Hora Inicial	O carimbo de data/hora interno indica quando o Cisco Unified Communications Ma solicitou que o telefone iniciasse a transmissão dos pacotes.
Status da sequência	Indica se a transmissão está ativa ou não.
Nome de host	Nome exclusivo e fixo que é atribuído automaticamente ao telefone com base no en MAC.
Pacotes do emissor	Número total de pacotes de dados RTP que o telefone transmitiu desde que iniciou O valor será 0 se a conexão for definida para o modo somente recebimento.

Item	Descrição
Octetos do emissor	Número total de octetos de carga que o telefone transmitiu nos pacotes de dados RTP d que iniciou a conexão. O valor será 0 se a conexão for definida para o modo somente recebimento.
Codec do emissor	Tipo de codificação de áudio para o fluxo transmitido.
Relatórios do emissor enviados (veja a nota)	Número de itens que o Relatório do emissor RTCP enviou.
Hora de envio do relatório do emissor (veja a nota)	Indicação de carimbo de data/hora interno do último Relatório do emissor RTCP que foi en
Pacotes perdidos do receptor	Número total de pacotes de dados RTP que foram perdidos desde que a recepção de da iniciou nesta conexão. Definido como o número de pacotes esperado menos o número de p recebidos, em que o número de pacotes recebidos inclui os atrasados ou duplicados. O será 0 se a conexão tiver sido definida para o modo somente envio.
Instabilidade média	Estimativa de desvio médio da hora de chegada do pacote de dados RTP, medido em milissegundos. O valor será 0 se a conexão tiver sido definida para o modo somente en
Codec do receptor	Tipo de codificação de áudio usado para o fluxo recebido.
Relatórios do receptor enviados (veja a nota)	Número de vezes que os Relatórios do receptor RTCP foram enviados.
Hora de envio do relatório do receptor (veja a nota)	Indicação de carimbo de data/hora interno de quando um Relatório do receptor RTCP f enviado.
Pacotes do receptor	Número total de pacotes de dados RTP que o telefone recebeu desde que a recepção de iniciou nesta conexão. Inclui pacotes que foram recebidos de diferentes fontes, caso ess uma chamada multicast. O valor será 0 se a conexão tiver sido definida para o modo so envio.
Octetos do receptor	Número total de octetos de carga que o dispositivo recebeu nos pacotes de dados RTP d que a recepção iniciou na conexão. Inclui pacotes que foram recebidos de diferentes fo caso essa seja uma chamada multicast. O valor será 0 se a conexão tiver sido definida p modo somente envio.
Taxa ocult. cumulativa	Número total de quadros de ocultação dividido pelo número total de quadros de fala que recebidos desde o início do fluxo de voz.
Taxa ocultação do intervalo	Taxa de quadros de ocultação para quadros de fala no intervalo anterior de 3 segundos ativa. Se a VAD (detecção de atividade de voz) estiver em uso, talvez seja necessário u intervalo mais longo para acumular três segundos de fala ativa.
Taxa ocultação máxima	Taxa mais alta de ocultação do intervalo desde o início do fluxo de voz.

Item	Descrição
Ocultar segs.	Número de segundos que tem eventos de ocultação (quadros perdidos) desde o iníci de voz (inclui segundos severamente ocultados).
Ocultar segs. estritamente	Número de segundos que tem mais de 5% de eventos de ocultação (quadros perdido início do fluxo de voz.
Latência (veja a nota)	Estimativa da latência da rede, expressa em milissegundos. Representa a média de e do atraso na resposta, medida quando os blocos de relatório do receptor RTCP são r
Instabilidade máxima	Valor máximo de instabilidade instantânea, em milissegundos.
Tamanho do emissor	Tamanho do pacote RTP, em milissegundos, para o fluxo transmitido.
Relatórios do emissor recebidos (veja a nota)	Número de vezes que os Relatórios do emissor RTCP foram recebidos.
Hora de recebimento do relatório do emissor (veja a nota)	Hora mais recente em que um Relatório do emissor RTCP foi recebido.
Tamanho do receptor	Tamanho do pacote RTP, em milissegundos, para o fluxo recebido.
Receptor abandonado	Pacotes RTP que foram recebidos da rede, mas foram descartados dos buffers de ins
Relatórios do receptor recebidos (veja a nota)	Número de vezes que os Relatórios do receptor RTCP foram recebidos.
Hora de recebimento do relatório do receptor (veja a nota)	Hora mais recente em que um Relatório do receptor RTCP foi recebido.

Observação Quando o Protocolo de controle RTP é desativado, nenhum dado é gerado para esse campo que, portanto, exibe 0.

Solicitar informações do telefone em XML

Para solução de problemas, você pode solicitar informações do telefone. As informações resultantes são em formato XML. As seguintes informações estão disponíveis:

- CallInfo são informações de sessão de chamada para uma linha específica.
- LineInfo são informações de configuração de linha para o telefone.
- ModeInfo são informações de modo do telefone.

Antes de Iniciar

O acesso à Web precisa ser ativado para obter as informações.

O telefone deve ser associado a um usuário.

Procedimento

Etapa 1 Para Informações de chamada, insira o seguinte URL em um navegador: **http://<phone ip address>/CGI/Java/CallInfo<x>**

onde

- <*phone ip address*> é o endereço IP do telefone
- <*x*> é o número da linha da qual obter informações.

O comando retorna um documento XML.

Etapa 2 Para Informações de linha, insira o seguinte URL em um navegador: **http://<phone ip address>/CGI/Java/LineInfo**

onde

- <*phone ip address*> é o endereço IP do telefone

O comando retorna um documento XML.

Etapa 3 Para Informações de modo, insira o seguinte URL em um navegador: **http://<phone ip address>/CGI/Java/ModeInfo**

onde

- <*phone ip address*> é o endereço IP do telefone

O comando retorna um documento XML.

Exemplo de saída de CallInfo

O código XML a seguir é um exemplo da saída do 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>
```

Exemplo de saída de LineInfo

O código XML a seguir é um exemplo da saída do 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>
```

Exemplo de saída de ModeInfo

O código XML a seguir é um exemplo da saída do comando ModeInfo.

```
<?xml version="1.0" encoding="utf-8"?>
<CiscoIPPhoneModeInfo>
   <PlaneTitle>Applications</PlaneTitle>
```

```
   <PlaneFieldCount>12</PlaneFieldCount>
   <PlaneSoftKeyIndex>0</PlaneSoftKeyIndex>
   <PlaneSoftKeyMask>0</PlaneSoftKeyMask>
   <Prompt></Prompt>
   <Notify></Notify>
   <Status></Status>
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Call History</FieldName>
      <FieldValue></FieldValue>
   </CiscoIPPhoneFields>
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Preferences</FieldName>
      <FieldValue></FieldValue>
   </CiscoIPPhoneFields>
   ...
</CiscoIPPhoneModeInfo>
```

CAPÍTULO 12

Solução de problemas do telefone

Informações gerais sobre solução de problemas

A tabela a seguir fornece informações gerais sobre solução de problemas para o Telefone IP Cisco.

Tabela 30: Solução de problemas do Telefone IP Cisco

Resumo	Explicação
As tempestades de difusão prolongadas redefinem os telefones IP ou os impossibilitam de efetuar uma chamada ou responder a uma.	Uma tempestade de difusão prolongada (com duração de muitos minutos 2 na VLAN de voz pode fazer com que os telefones IP sejam redefinid uma chamada ativa ou não possam iniciar nem responder a uma chamada. ficarão inativos até o fim de uma tempestade de difusão.
Transferência de uma conexão de rede do telefone para uma estação de trabalho	Se você carrega seu telefone por meio da conexão de rede, é preciso ter decida desconectar a conexão de rede do telefone e conectar o cabo em um desktop. **Cuidado** A placa de rede no computador não pode receber energia p conexão de rede; se a energia for fornecida por meio da cone de rede poderá ser destruída. Para proteger uma placa de r 10 segundos ou mais depois de desconectar o cabo do telef de conectá-lo a um computador. Esse intervalo dá ao switc suficiente para reconhecer que não há mais um telefone na interromper o fornecimento de energia para o cabo.

Resumo	Explicação
Alteração da configuração do telefone	Por padrão, as configurações da senha do administrador são bloqueadas par que os usuários façam alterações que possam afetar a conectividade de red deve desbloquear as configurações da senha do administrador para poder c Consulte Aplicar uma senha ao telefone, na página 43 para obter mais deta **Observação** Se a senha do administrador não estiver definida no perfil de t comum, o usuário poderá modificar as configurações de rede.
Incompatibilidade do codec entre o telefone e outro dispositivo	As estatísticas RxType e TxType mostram o codec que é usado para uma c entre o Telefone IP Cisco e o outro dispositivo. Os valores dessas estatístic corresponder. Se não corresponderem, verifique se o outro dispositivo pode a conversa do codec ou se um transcodificador está definido para processar Consulte Exibir a janela Estatísticas da chamada, na página 142 para obter detalhes.
Incompatibilidade da amostra de som entre o telefone e outro dispositivo	As estatísticas RxSize e TxSize mostram o tamanho dos pacotes de voz qu usados em uma conversa entre o Telefone IP Cisco e o outro dispositivo. C dessas estatísticas devem corresponder. Consulte Exibir a janela Estatística chamada, na página 142 para obter mais detalhes.
Condição de loopback	Uma condição de loopback pode ocorrer quando as seguintes condições fo atendidas: • A opção Configuração da porta do switch no telefone está definida co meio (10-BaseT/half duplex). • O telefone recebe energia de uma fonte de alimentação externa. • O telefone é desligado (a fonte de alimentação é desconectada). Nesse caso, a porta do switch no telefone pode ser desativada e a seguinte m é exibida no log do console do switch: HALF_DUX_COLLISION_EXCEED_THRESHOLD Para resolver esse problema, reative a porta no switch.

Problemas de inicialização

Depois de instalar um telefone na sua rede e adicioná-lo ao Cisco Unified Communications Manager, o telefone deverá iniciar conforme descrito no tópico relacionado abaixo.

Se o telefone não iniciar corretamente, consulte as seções a seguir para obter informações sobre como solucionar problemas.

Tópicos relacionados

Verificar a inicialização do telefone, na página 55

O Telefone IP Cisco não passa pelo processo normal de inicialização

Problema

Quando você conecta um Telefone IP Cisco à porta de rede, o telefone não passa pelo processo normal de inicialização, conforme descrito no tópico relacionado, e a tela do telefone não exibe informações.

Razão

Se o telefone não passar pelo processo de inicialização, a causa pode estar em cabos com defeito, conexões incorretas, interrupções de rede, falta de energia ou o telefone não está funcionando.

Solução

Para determinar se o telefone está funcionando, use as sugestões a seguir para eliminar outros possíveis problemas.

- Verifique se a porta da rede está funcionando:
  - Troque os cabos Ethernet por outros que você saiba que estejam funcionando.
  - Desconecte um Telefone IP Cisco em funcionamento de outra porta e conecte-o a essa porta de rede para verificar se a porta está ativa.
  - Conecte o Telefone IP Cisco que não inicia a outra porta de rede que esteja em boas condições.
  - Conecte o Telefone IP Cisco que não inicia diretamente à porta no switch, eliminando a conexão do painel de patch no escritório.
- Verifique se o telefone está recebendo energia:
  - Se você estiver usando energia externa, verifique se a tomada elétrica está funcionando.
  - Se você estiver usando energia embutida, use a fonte de alimenta externa.
  - Se estiver usando a fonte de alimentação externa, troque-a por uma unidade que você saiba que esteja funcionando.
- Se o telefone ainda não iniciar corretamente, ligue-o a partir do backup de imagem de software.
- Se o telefone ainda não iniciar corretamente, execute uma redefinição de fábrica.
- Depois de tentar essas soluções, se a tela do Telefone IP Cisco não exibir qualquer caractere decorridos pelo menos cinco minutos, entre em contato com o representante do suporte técnico da Cisco para obter mais ajuda.

Tópicos relacionados

Verificar a inicialização do telefone, na página 55

O Telefone IP Cisco não é registrado no Cisco Unified Communications Manager

Se o telefone passa da primeira fase do processo de inicialização (botões de LED piscando), mas continua passando pelas mensagens que são exibida na tela do telefone, o telefone não está inicializando corretamente.

O telefone não pode inicializar com êxito até que seja conectado à rede Ethernet e registrado em um servidor Cisco Unified Communications Manager.

Além disso, problemas com a segurança podem impedir o telefone de inicializar corretamente. Consulte Procedimentos da solução de problemas, na página 171 para obter mais informações.

O telefone exibe mensagens de erro

Problema

As mensagens de status exibem erros durante a inicialização.

Solução

Enquanto o telefone passa pelo processo de inicialização, você pode acessar as mensagens de status que podem fornecer informações sobre a causa de um problema. Veja a seção “Exibir janela Mensagens de status” para obter instruções sobre como acessar mensagens de status e obter uma lista de possíveis erros, suas explicações e suas soluções.

Tópicos relacionados

Exibir a janela Mensagens de status, na página 134

O telefone não pode se conectar ao Servidor TFTP ou ao Cisco Unified Communications Manager

Problema

Se a rede estiver desativada entre o telefone e o servidor TFTP ou o Cisco Unified Communications Manager, o telefone não poderá inicializar corretamente.

Solução

Garanta que a rede esteja atualmente em execução.

O telefone não consegue se conectar ao servidor TFTP

Problema

As configurações do servidor TFTP podem estar incorretas.

Solução

Verifique as configurações de TFTP.

Tópicos relacionados

Verificar configurações de TFTP, na página 171

O telefone não consegue se conectar ao servidor

Problema

Os campos de endereço IP e roteamento podem não estar configurados corretamente.

Solução

Você deve verificar as configurações de endereço IP e roteamento no telefone. Se você estiver usando DHCP, o servidor DHCP deverá fornecer esses valores. Se você tiver atribuído um endereço IP estático ao telefone, insira esses valores manualmente.

Tópicos relacionados

Verificar configurações de DHCP, na página 172

O telefone não pode se conectar usando DNS

Problema

As configurações DNS podem estar incorretas.

Solução

Se você usar DNS para acessar o servidor TFTP ou o Cisco Unified Communications Manager, será preciso garantir a especificação de um servidor DNS.

Tópicos relacionados

Verificar configurações de DNS, na página 174

O Cisco Unified Communications Manager e os Serviços TFTP não estão funcionando

Problema

Se o Cisco Unified Communications Manager e os serviços TFTP não estiverem em execução, os telefones talvez não possam inicializar corretamente. Nesse caso, é provável que você esteja enfrentando uma falha em todo o sistema e outros telefones e serviços não estão aptos a inicializar corretamente.

Solução

Se o serviço do Cisco Unified Communications Manager não estiver em execução, todos os dispositivos na rede que dependem dele para fazer chamadas serão afetados. Se o serviço TFTP não estiver em execução, muitos dispositivos não poderão ser inicializados com êxito. Para obter mais informações, consulte Iniciar serviço, na página 174.

Corrupção do arquivo de configuração

Problema

Se você continuar tendo problemas com um determinado telefone que outras sugestões neste capítulo não resolveram, o arquivo de configuração pode estar corrompido.

Solução

Crie um novo arquivo de configuração do telefone.

Tópicos relacionados

Criar um novo arquivo de configuração do telefone, na página 173

Registro de telefones no Cisco Unified Communications Manager

Problema

O telefone não está registrado no Cisco Unified Communications Manager

Solução

Um Telefone IP Cisco pode ser registrado em um servidor Cisco Unified Communications Manager somente se o telefone for adicionado ao servidor ou se o registro automático estiver ativado. Consulte as informações e os procedimentos em Métodos de adição de telefone, na página 62 para garantir que o telefone seja adicionado ao banco de dados do Cisco Unified Communications Manager.

Para verificar se o telefone está no banco de dados do Cisco Unified Communications Manager, escolha **Dispositivo** > **Telefone** em Administração do Cisco Unified Communications Manager. Clique em **Localizar** para pesquisar o telefone com base no endereço MAC. Para obter informações sobre como determinar um endereço MAC, consulte Determinar o endereço MAC do telefone, na página 62.

Se o telefone já estiver no banco de dados do Cisco Unified Communications Manager, o arquivo de configuração pode estar danificado. Consulte Corrupção do arquivo de configuração, na página 163 para obter assistência.

O Telefone IP Cisco não pode obter o endereço IP

Problema

Se um telefone não puder obter um endereço IP quando iniciado, talvez ele não esteja na mesma rede ou VLAN que o servidor DHCP ou a porta do switch à qual o telefone se conecta pode estar desativada.

Solução

Verifique se a rede ou VLAN à qual o telefone se conecta tem acesso ao servidor DHCP e se a porta do switch está ativada.

Problemas com a redefinição do telefone

Se os usuários relatarem que seus telefones estão sendo redefinidos durante as chamadas ou enquanto estão ociosos, você deverá investigar a causa. Se a conexão de rede e a conexão do Cisco Unified Communications Manager estiverem estáveis, um telefone não deverá ser redefinido.

Normalmente, um telefone será redefinido se tiver problemas ao se conectar à rede ou ao Cisco Unified Communications Manager.

O telefone é redefinido devido a interrupções de rede intermitentes

Problema

Talvez sua rede esteja enfrentando interrupções intermitentes.

Solução

Interrupções de rede intermitentes afetam os dados e o tráfego de voz de modo diferente. Talvez sua rede esteja enfrentando interrupções intermitentes sem detecção. Se for isso, o tráfego dos dados pode reenviar pacotes perdidos e verificar se esses pacotes estão sendo recebidos e transmitidos. Entretanto, o tráfego de voz não pode recapturar pacotes perdidos. Em vez de retransmitir uma conexão de rede perdida, o telefone é redefinido e tentar se reconectar à rede. Entre em contato com o administrador do sistema para obter informações sobre problemas conhecidos na rede de voz.

O telefone é redefinido devido a erros de configuração do DHCP

Problema

As configurações DHCP podem estar incorretas.

Solução

Verifique se você configurou corretamente o telefone para usar DHCP. Verifique se o servidor DHCP está configurado corretamente. Verifique a duração da concessão de DHCP. Recomendamos definir a duração da concessão para 8 dias.

Tópicos relacionados

Verificar configurações de DHCP, na página 172

O telefone é redefinido devido ao endereço IP estático incorreto

Problema

O endereço IP estático atribuído ao telefone pode estar incorreto.

Solução

Se o telefone estiver atribuído a um endereço IP estático, verifique se você inseriu as configurações corretas.

O telefone é redefinido durante o uso intenso da rede

Problema

Se o telefone parecer redefinir durante o uso intenso da rede, é provável que você não tenha uma VLAN de voz configurada.

Solução

Isolar os telefones em uma VLAN auxiliar separada aumenta a qualidade do tráfego de voz.

O telefone é redefinido intencionalmente

Problema

Se você não for o único administrador com acesso ao Cisco Unified Communications Manager, verifique se ninguém mais redefiniu intencionalmente os telefones.

Solução

Você pode verificar se um Telefone IP Cisco recebeu um comando de redefinição do Cisco Unified Communications Manager, pressionando **Configurações** no telefone e escolhendo **Configurações do administrador** > **Status** > **Estatísticas da rede**.

- Se o campo Reinicializar causa exibir `Reset-Reset`, o telefone recebeu um comando Reset/Reset da Administração do Cisco Unified Communications Manager.
- Se o campo Reinicializar causa exibir `Reset-Restart`, o telefone foi encerrado porque recebeu um comando Reset/Restart da Administração do Cisco Unified Communications Manager.

O telefone é redefinido devido ao DNS ou outros problemas de conectividade

Problema

A redefinição do telefone continua, e você suspeita de problemas com o DNS ou de outros problemas de conectividade.

Solução

Se o telefone continuar a ser redefinido, elimine os erros de DNS ou outros erros de conectividade seguindo o procedimento descrito em Determinar problemas de DNS ou conectividade, na página 172.

O telefone não liga

Problema

O telefone parece não estar ligado.

Solução

Na maioria dos casos, um telefone é reiniciado se ele for ligado usando energia externa, mas perder essa conexão e alternar para PoE. Da mesma forma, um telefone pode ser reiniciado se ele for ligado usando PoE e depois se conectar a uma fonte de alimentação externa.

O telefone não consegue se conectar à LAN

Problema

A conexão física com a LAN pode estar interrompida.

Solução

Verifique se a conexão Ethernet do Telefone IP Cisco está ativa. Por exemplo, verifique se a porta ou o switch em particular ao qual o telefone se conecta está inativo e se o switch não está sendo reinicializado. Verifique também se não há cabos danificados.

Problemas de segurança do Telefone IP Cisco

As seções a seguir fornecem informações para solução de problemas dos recursos de segurança no Telefone IP Cisco. Para obter informações sobre as soluções para qualquer um desses problemas, bem como informações adicionais para solução de problemas de segurança, consulte o *Guia de segurança do Cisco Unified Communications Manager*.

Problemas com o arquivo CTL

As seções a seguir descrevem a solução de problemas com o arquivo CTL.

Erro de autenticação, o telefone não pode autenticar o arquivo CTL

Problema

Ocorre um erro de autenticação do dispositivo.

Razão

O arquivo CTL não tem um certificado Cisco Unified Communications Manager ou tem um certificado incorreto.

Solução

Instale um certificado correto.

O telefone não pode autenticar o arquivo CTL

Problema

O telefone não pode autenticar o arquivo CTL.

Razão

O token de segurança que assinou o arquivo CTL atualizado não existe no arquivo CTL do telefone.

Solução

Altere o token de segurança no arquivo CTL e instale o novo arquivo no telefone.

O arquivo CTL é autenticado, mas outros arquivos de configuração não são autenticados

Problema

O telefone não pode autenticar qualquer arquivo de configuração que não seja o arquivo CTL.

Razão

Há um registro de TFTP incorreto ou o arquivo de configuração pode não estar assinado pelo certificado correspondente na Lista de confiança do telefone.

Solução

Verifique o registro de TFTP e o certificado na Lista de confiança.

O arquivo ITL é autenticado, mas outros arquivos de configuração não são autenticados

Problema

O telefone não pode autenticar qualquer arquivo de configuração que não seja o arquivo ITL.

Razão

O arquivo de configuração pode não estar assinado pelo certificado correspondente na Lista de confiança do telefone.

Solução

Assine o arquivo de configuração novamente usando o certificado correto.

Falha na autorização de TFTP

Problema

O telefone reporta falha na autorização de TFTP.

Razão

O endereço TFTP para o telefone não existe no arquivo CTL.

Se você criou um novo arquivo CTL com um novo registro TFTP, o arquivo CTL existente no telefone pode não conter um registro para o novo servidor TFTP.

Solução

Verifique a configuração do endereço TFTP no arquivo CTL do telefone.

O telefone não é registrado

Problema

O telefone não é registrado no Cisco Unified Communications Manager.

Razão

O arquivo CTL não contém as informações corretas para o servidor Cisco Unified Communications Manager.

Solução

Altere as informações do servidor Cisco Unified Communications Manager no arquivo CTL.

Arquivos de configuração assinados não são solicitados

Problema

O telefone não solicita arquivos de configuração assinados.

Razão

O arquivo CTL não contém entradas TFTP com certificados.

Solução

Configure entradas TFTP com certificados no arquivo CTL.

Problemas de áudio

As seções a seguir descrevem como resolver problemas de áudio.

Sem caminho de fala

Problema

Uma ou mais pessoas em uma chamada não ouvem qualquer áudio.

Solução

Quando pelo menos uma pessoa em uma chamada não está recebendo o áudio, a conectividade IP entre os telefones não está estabelecida. Verifique a configuração dos roteadores e switches para garantir que a conectividade IP esteja configurada corretamente.

Fala irregular

Problema

Um usuário reclama de fala irregular em uma chamada.

Razão

Pode haver uma incompatibilidade na configuração de instabilidade.

Solução

Verifique as estatísticas de AvgJtr e MaxJtr. Uma grande variação entre essas estatísticas pode indicar um problema de instabilidade na rede ou altas taxas periódicas de atividade da rede.

Um telefone no modo Daisy Chain não funciona

Problema

No modo daisy chain, um dos telefones de conferência não funciona.

Solução

Verifique se os cabos conectados ao adaptador inteligente são os corretos. Os dois cabos mais grossos conectam os telefones ao adaptador inteligente. O cabo mais fino conecta o adaptador inteligente ao adaptador de energia.

Tópicos relacionados

Modo Daisy Chain, na página 33
Instalar o telefone de conferência no modo Daisy Chain, na página 40

Problemas gerais com chamadas telefônicas

As seções a seguir ajudam a solucionar problemas gerais de chamada telefônica.

Não é possível estabelecer a chamada telefônica

Problema

Um usuário reclama por não conseguir efetuar uma chamada.

Razão

O telefone não tem um endereço IP DHCP e, portanto, não pode ser registrado no Cisco Unified Communications Manager. Os telefones com tela LCD mostram a mensagem `Configurando IP` ou `Registrando`. Os telefones sem tela LCD reproduzem o tom de reordenação (em vez do tom de discagem) no monofone quando o usuário tenta efetuar uma chamada.

Solução

1. Tente o seguinte:
    1. O cabo Ethernet está conectado.
    2. O serviço Cisco CallManager está em execução no servidor Cisco Unified Communications Manager.
    3. Os dois telefones estão registrados no mesmo Cisco Unified Communications Manager.
2. Os logs de depuração e captura do servidor de áudio estão ativados nos dois telefones. Se necessário, ative a depuração do Java.

O telefone não reconhece dígitos DTMF ou os dígitos são atrasados

Problema

O usuário reclama que os números são perdidos ou atrasados quando o teclado numérico é usado.

Razão

Pressionar as teclas muito rapidamente pode resultar em dígitos perdidos ou atrasados.

Solução

As teclas não devem ser pressionadas rapidamente.

Procedimentos da solução de problemas

Esses procedimentos podem ser usados para identificar e corrigir problemas.

Criar um relatório de problemas de telefone a partir do Cisco Unified Communications Manager

Você pode gerar um relatório de problemas para os telefones do Cisco Unified Communications Manager. Essa ação resulta na mesma informação que a tecla programável da ferramenta de relatório de problemas (PRT) gera no telefone.

O relatório de problemas contém informações sobre o telefone e os fones de ouvido.

Procedimento

Etapa 1 Na Administração do Cisco Unified CM, selecione **Dispositivo** > **Telefone**.

Etapa 2 Clique em **Localizar** e selecione um ou mais Telefones IP Cisco.

Etapa 3 Clique em **Gerar PRT para selecionados** para coletar registros de PRT para os fones de ouvido usados em Telefones IP Cisco selecionados.

Verificar configurações de TFTP

Procedimento

Etapa 1 Verifique o campo Servidor TFTP 1.

Se você tiver atribuído um endereço IP estático ao telefone, insira manualmente uma configuração para a opção Servidor TFTP 1.

Se você estiver usando DHCP, o telefone obterá o endereço para o servidor TFTP do servidor DHCP. Verifique se o endereço IP está configurado na Opção 150.

Etapa 2 Você também pode ativar o telefone para usar um servidor TFTP alternativo. Essa configuração é particularmente útil se o telefone foi movido de um local para outro recentemente.

Etapa 3 Se o DHCP local não oferece o endereço SFTP correto, ative o telefone para usar um servidor TFTP alternativo.

Isso é geralmente necessário em cenários de VPN.

Determinar problemas de DNS ou conectividade

Procedimento

Etapa 1 Use o menu Redefinir configurações para redefinir as configurações do telefone para seus valores padrão.

Etapa 2 Modifique as configurações de DHCP e IP:

a) Desative o DHCP.
b) Atribua valores IP estáticos ao telefone. Use a mesma configuração de roteador padrão usada por outros telefone em funcionamento.
c) Atribua um servidor TFTP. Use o mesmo servidor TFTP usado por outros telefones em funcionamento.

Etapa 3 No servidor Cisco Unified Communications Manager, verifique se os arquivos host locais têm o nome do servidor Cisco Unified Communications Manager correto mapeado para o endereço IP correto.

Etapa 4 No Cisco Unified Communications Manager, escolha **Sistema** > **Servidor** e verifique se a referência ao servidor é feita pelo endereço IP e não pelo nome DNS.

Etapa 5 No Cisco Unified Communications Manager, escolha **Dispositivo** > **Telefone**. Clique em **Localizar** para procurar esse telefone. Verifique se você atribuiu o endereço MAC correto ao Telefone IP Cisco.

Etapa 6 Desligue e religue o telefone.

Tópicos relacionados

Determinar o endereço MAC do telefone, na página 62
Reinicializar ou redefinir o telefone de conferência, na página 177

Verificar configurações de DHCP

Procedimento

Etapa 1 No telefone, pressione **Configurações**.

Etapa 2 Selecione **Configurações do administrador** > **Configuração de Ethernet** > **Configuração de IPv4**.

Etapa 3 Marque o campo Servidor DHCP.

Se tiver atribuído um endereço IP estático ao telefone, você não precisará inserir um valor para a opção Servidor DHCP. No entanto, se você estiver usando um servidor DHCP, essa opção deverá ter um valor. Se

nenhum valor for encontrado, verifique a configuração da VLAN e do roteamento IP. Consulte o documento *Troubleshooting Switch Port and Interface Problems*, disponível neste URL:

https://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html

Etapa 4 Marque os campos Endereço IP, Máscara de sub-rede e Roteador padrão.

Se você atribuir um endereço IP estático ao telefone, você deve inserir manualmente as configurações para essas opções.

Etapa 5 Se estiver usando o DHCP, verifique os endereços IP distribuídos pelo servidor DHCP.

Consulte o documento *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks*, disponível neste URL:

https://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml

Criar um novo arquivo de configuração do telefone

Quando você remove um telefone do banco de dados do Cisco Unified Communications Manager, o arquivo de configuração é excluído do servidor TFTP do Cisco Unified Communications Manager. Os números de diretório do telefone permanecem no banco de dados do Cisco Unified Communications Manager. Eles são chamados de DNs não atribuídos e podem ser usados para outros dispositivos. Se DNs não atribuídos não forem usados por outros dispositivos, exclua-os do banco de dados do Cisco Unified Communications Manager. Você pode usar o Relatório de plano de rota para visualizar e excluir números de referência não atribuídos. Para obter mais informações, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Alterar os botões em um modelo de botão do telefone, ou atribuir outro modelo de botão a um telefone, pode resultar na inacessibilidade de números de diretório no telefone. Os números de diretório continuam sendo atribuídos ao telefone no banco de dados do Cisco Unified Communications Manager, mas não há botão no telefone com o qual as chamadas possam ser atendidas. Esses números de diretório devem ser removidos do telefone e excluídos, se necessário.

Procedimento

Etapa 1 No Cisco Unified Communications Manager, escolha **Dispositivo** > **Telefone** e clique em **Localizar** para encontrar o telefone que está com problemas.

Etapa 2 Escolha **Excluir** para remover o telefone do banco de dados do Cisco Unified Communications Manager.

Observação Quando você remove um telefone do banco de dados do Cisco Unified Communications Manager, o arquivo de configuração é excluído do servidor TFTP do Cisco Unified Communications Manager. Os números de diretório do telefone permanecem no banco de dados do Cisco Unified Communications Manager. Eles são chamados de DNs não atribuídos e podem ser usados para outros dispositivos. Se DNs não atribuídos não forem usados por outros dispositivos, exclua-os do banco de dados do Cisco Unified Communications Manager. Você pode usar o Relatório de plano de rota para visualizar e excluir números de referência não atribuídos.

Etapa 3 Adicione o telefone de volta ao banco de dados do Cisco Unified Communications Manager.

Etapa 4 Desligue e religue o telefone.

Tópicos relacionados

Métodos de adição de telefone, na página 62
Documentação do Cisco Unified Communications Manager, na página 14

Verificar configurações de DNS

Procedimento

Etapa 1 No telefone, pressione **Configurações**.

Etapa 2 Selecione **Configurações do administrador** > **Configuração de Ethernet** > **Configuração de IPv4**

Etapa 3 Verifique se o campo Servidor DNS 1 está definido corretamente.

Etapa 4 Você também deve verificar se uma entrada de CNAME foi feita no servidor DNS para o servidor TFTP e para o sistema Cisco Unified Communications Manager.

Você também deve garantir que o DNS seja configurado para fazer consultas reversas.

Iniciar serviço

Um serviço deve ser ativado para que possa ser iniciado ou parado.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, escolha **Cisco Unified Serviceability** na lista suspensa Navegação e clique em **Ir**.

Etapa 2 Escolha **Ferramentas** > **Centro controle - Página da Web Serviços de função**.

Etapa 3 Escolha o servidor Cisco Unified Communications Manager principal na lista suspensa Servidor.

A janela exibe os nomes de serviços do servidor escolhido, o status dos serviços e um painel de controle de serviços para iniciar ou parar um serviço.

Etapa 4 Se um serviço estiver parado, clique no botão de opção correspondente e clique em **Iniciar**.

O símbolo de Status do serviço muda de um quadrado para uma seta.

Controlar informações de depuração no Cisco Unified Communications Manager

Se você estiver com problemas no telefone que não é capaz de resolver, o Cisco TAC poderá ajudá-lo. Você precisará ativar a depuração para o telefone, reproduzir o problema, desativar a depuração e enviar os logs para o TAC para análise.

Como a depuração captura informações detalhadas, o tráfego de comunicação poderá deixar o telefone mais lento, menos responsivo. Depois que você capturar os logs, desative a depuração para garantir o funcionamento do telefone.

As informações de depuração podem incluir um código de um dígito que reflete a gravidade do problema. Os problemas são classificados da seguinte forma:

- 0 - Emergência
- 1 - Alerta
- 2 - Crítico
- 3 - Erro
- 4 - Avisar
- 5 - Notificação
- 6 - Informações
- 7 - Depuração

Entre em contato com o Cisco TAC para obter mais informações e assistência.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, selecione uma das seguintes janelas:

- **Dispositivo** > **Configurações do dispositivo** > **Perfil de telefone comum**
- **Sistema** > **Configuração do telefone da empresa**
- **Dispositivo** > **Telefone**

Etapa 2 Configure os seguintes parâmetros:

- Perfil de registro - valores: Predefinição (padrão), Padrão, Telefonia, SIP, IU, Rede, Mídia, Atualização, Acessório, Segurança, EnergyWise, AcessoRemotoMóvel
- Registro remoto - valores: Desativar (padrão), Ativar
- Servidor de log IPv6 ou Servidor de log - Endereço IP (endereço IPv4 ou IPv6)

Observação Quando não é possível contatar o Servidor de registro, o telefone para de enviar mensagens de depuração.

- O formato do endereço do Servidor de registro IPv4 é **endereço:<port>@@base=<0-7>;pfs=<0-1>**
- O formato do endereço do Servidor de registro IPv6 é **[endereço]:<port>@@base=<0-7>;pfs=<0-1>**
- Em que:
  - o endereço IPv4 é separado por ponto (.)
  - o endereço IPv6 é separado por dois-pontos (:)

Informações adicionais sobre solução de problemas

Se você tiver perguntas adicionais sobre a solução de problemas do seu telefone, vá para o seguinte website e navegue até o modelo de telefone desejado:

https://www.cisco.com/cisco/web/psa/troubleshoot.html

CAPÍTULO 13

Manutenção

Reinicializar ou redefinir o telefone de conferência

Você executa uma redefinição básica de um telefone para recuperar de um erro no telefone. Você também pode restaurar as configurações de segurança para as configurações padrão de fábrica.

Reinicializar o telefone de conferência

Quando você reinicia o telefone, quaisquer alterações de configuração de usuário e rede que não são confirmadas para a memória flash no telefone serão perdidas.

Procedimento

Pressione **Configurações** > **Configurações do administrador** > **Redefinir configurações** > **Redefinir dispositivo**.

Tópicos relacionados

Entrada de menu e texto no telefone, na página 43

Redefinir as configurações do telefone de conferência no menu do telefone

Procedimento

Etapa 1 Pressione **Configurações**.

Etapa 2 Escolha **Configurações do administrador** > **Redefinir configurações**.

Etapa 3 Selecione o tipo de redefinição.

- **Tudo** — Restaura as configurações de fábrica.

- **Redefinir dispositivo** — O dispositivo é redefinido. As configurações existentes não são alteradas.
- **Rede** — Restaura a configuração de rede para as configurações padrão.
- **Modo de serviço** — Limpa o modo de serviço atual, desativa a conexão com a VPN e reinicia o telefone.
- **Segurança** — Restaura a configuração de segurança para as configurações padrão. Esta opção exclui o arquivo CTL.

Etapa 4 Pressione **Redefinir** ou **Cancelar**.

Tópicos relacionados

Entrada de menu e texto no telefone, na página 43

Redefinir o telefone de conferência para os padrões de fábrica usando o teclado numérico

Quando você redefine o telefone no teclado numérico, o telefone é revertido para as configurações de fábrica.

Procedimento

Etapa 1 Desconecte o telefone:

- Se estiver usando PoE, desconecte o cabo da LAN.
- Se estiver usando o adaptador de energia, desconecte-o.

Etapa 2 Aguarde 5 segundos.

Etapa 3 Pressione e segure a tecla **#** e reconecte o telefone.

Etapa 4 Quando o telefone inicializa, a faixa de LED acende. Assim que a faixa de LED acender, pressione **123456789*0#** em sequência.

Depois de pressionar esses botões, o telefone passa pelo processo de redefinição de fábrica.

Se você pressionar os botões fora da sequência, o telefone ligará normalmente.

Cuidado Não desligue o telefone até que o processo de redefinição de fábrica seja concluído e a tela principal seja exibida.

Tópicos relacionados

Entrada de menu e texto no telefone, na página 43

Monitoramento da qualidade de voz

Para medir a qualidade da voz das chamadas enviadas e recebidas na rede, os Cisco IP Phones usam estas métricas estatísticas baseadas em eventos de ocultação. O DSP reproduz quadros de ocultação para mascarar a perda de quadros no fluxo de pacotes de voz.

- Métrica de taxa de ocultação – Mostra a taxa de quadros de ocultação sobre o total de quadros de fala. Uma taxa de ocultação por intervalo é calculada a cada 3 segundos.

- Métrica de segundos ocultados – Mostra o número de segundos nos quais o DSP reproduz quadros de ocultação devido à perda de quadros. Um "segundo severamente ocultado" é um segundo em que o DSP reproduz mais do que cinco por cento dos quadros de ocultação.

Observação A taxa e os segundos de ocultação são medidas primárias baseadas na perda de quadros. Uma taxa de ocultação igual a zero indica que a rede IP está entregando quadros e pacotes a tempo e sem perdas.

Você pode acessar as métricas de qualidade da voz do Telefone IP Cisco usando a tela de Estatísticas da chamada ou remotamente, usando as Estatísticas de transmissão.

Dicas para solução de problemas da qualidade de voz

Quando você observar alterações significativas e persistentes nas métricas, use a tabela a seguir para obter informações gerais de solução de problemas.

Tabela 31: Alterações nas métricas de qualidade da voz

Alteração na métrica	Condição
A Taxa de ocultação e Ocultar segs aumentam significativamente	Deficiência da rede por perda de pacotes ou alta instabilidade.
A Taxa de ocultação está próxima de ou é igual a zero, mas a qualidade da voz está baixa.	• Ruído ou distorção no canal de áudio, como níveis de áudio ou eco. • Chamadas em tandem que passam por várias codificações/decodificações, como chamadas para uma rede celular ou de cartão de chamada. • Problemas acústicos vindos de um alto-falante, telefone celular com viva-voz ou fone de ouvido sem fio. Verifique os contadores de transmissão de pacotes (TxCnt) e recepção de pacotes (RxCnt) para confirmar se os pacotes estão fluindo.
As pontuações de MOS LQK caem significativamente	Deficiência da rede por perda de pacotes ou altos níveis de instabilidade: • Reduções de MOS LQK em média podem indicar deficiência geral e uniforme. • Reduções individuais de MOS LQK podem indicar deficiência intermitente. Faça a verificação cruzada da Taxa de ocultação e de Ocultar segs para procurar por evidências de perda de pacotes e instabilidade.

Alteração na métrica	Condição
As pontuações de MOS LQK aumentam significativamente	• Verifique se o telefone está usando um codec diferente do esperado (RxType e TxType). • Verifique se a versão de MOS LQK mudou após uma atualização de firmware.

Observação As métricas de qualidade da voz não levam em conta ruídos ou distorções, apenas a perda de quadros.

Limpeza do Telefone IP Cisco

Para limpar o Telefone IP Cisco, use apenas um pano limpo e seco no telefone e na tela do telefone. Não aplique líquidos nem pós diretamente no telefone. Assim como em todos os aparelhos eletrônicos que não são à prova de intempéries, líquidos e pós podem danificar os componentes e causar falhas.

Quando o telefone está no modo de repouso, a tela fica em branco e o botão Selecionar não acende. Quando o telefone está nessa condição, você pode limpar a tela, desde que saiba que o telefone permanecerá no estado de suspensão até que você termine de limpar.

CAPÍTULO 14

Suporte para usuário internacional

Instalador de localidade dos dispositivos do Unified Communications Manager

Por padrão, os Telefones IP Cisco são configurados para a localidade inglesa (Estados Unidos). Para usar os Telefones IP Cisco em outras localidades, é preciso instalar a versão específica da localidade do Instalador de localidade dos dispositivos do Unified Communications Manager em cada servidor Cisco Unified Communications Manager no cluster. O Instalador de localidade instala o texto convertido mais recente da interface do usuário de telefonia e os tons de telefone específicos do país no seu sistema para que eles estejam disponíveis para os Telefones IP Cisco.

Para acessar o Instalador de localidade necessário para uma versão, acesse a página Download de software, navegue até o modelo do telefone e selecione o link Instalador de localidade dos dispositivos do Unified Communications Manager.

Para obter mais informações, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Observação O Instalador de localidade mais recente pode não estar prontamente disponível; continue verificando o website em busca de atualizações.

Tópicos relacionados

Documentação do Cisco Unified Communications Manager, na página 14

Suporte para registro em log de chamadas internacionais

Se seu sistema de telefonia estiver configurado para registro em log de chamadas internacionais (normalização do originador da chamada), os logs de chamadas, a rediscagem ou as entradas do diretório de chamadas podem exibir o símbolo de adição (+) para representar o código de escape internacional de seu local. Dependendo

da configuração de seu sistema de telefonia, o + pode ser substituído pelo código de discagem internacional correto, ou talvez seja necessário editar o número antes de discar para substituir manualmente o + pelo código de escape internacional de seu local. Além disso embora o log de chamadas ou a entrada do diretório possam exibir o número internacional inteiro da chamada recebida, a tela do telefone pode mostrar a versão local abreviada do número, sem códigos internacionais ou do país.

Limitação de idioma

Não há suporte para entrada de texto alfanumérico por teclado (KATE) localizada para as seguintes localidades asiáticas:

- Chinês (China)
- Chinês (Hong Kong)
- Chinês (Taiwan)
- Japonês (Japão)
- Coreano (República da Coreia)

O padrão KATE Inglês (Estados Unidos) é apresentado ao usuário.

Por exemplo, a tela do telefone mostrará o texto em coreano, mas a tecla **2** do teclado exibirá **a b c 2 A B C**.

Sobre a tradução

A Cisco pode fornecer traduções no idioma local deste conteúdo em alguns locais. Observe que essas traduções são fornecidas apenas para fins informativos e, se houver alguma inconsistência, a versão em inglês deste conteúdo prevalecerá.