Guide de l'utilisateur des téléphones IP Cisco série 8800 pour Cisco Unified Communications Manager.

Première publication : 13 juillet 2015

Dernière modification : 16 juin 2023

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

LES SPÉCIFICATIONS ET INFORMATIONS SUR LES PRODUITS PRÉSENTÉS DANS CE MANUEL PEUVENT ÊTRE MODIFIÉES SANS PRÉAVIS. TOUTES LES DÉCLARATIONS, INFORMATIONS ET RECOMMANDATIONS FOURNIES DANS CE MANUEL SONT EXACTES À NOTRE CONNAISSANCE, MAIS SONT PRÉSENTÉES SANS GARANTIE D'AUCUNE SORTE, EXPRESSE OU IMPLICITE. LES UTILISATEURS ASSUMENT L'ENTIÈRE RESPONSABILITÉ DE L'APPLICATION DE TOUT PRODUIT.

LA LICENCE DE LOGICIEL ET LA GARANTIE LIMITÉE DU PRODUIT CI-JOINT SONT DÉFINIES DANS LES INFORMATIONS FOURNIES AVEC LE PRODUIT ET SONT INTÉGRÉES AUX PRÉSENTES SOUS CETTE RÉFÉRENCE. SI VOUS NE TROUVEZ PAS LA LICENCE LOGICIELLE OU LA LIMITATION DE GARANTIE, DEMANDEZ-EN UN EXEMPLAIRE À VOTRE REPRÉSENTANT CISCO.

Les informations qui suivent concernent la conformité FCC des périphériques de classe A : cet appareil a été testé et reconnu conforme aux limites relatives aux appareils numériques de classe A, conformément à la section 15 du règlement de la FCC. Ces limites ont pour but de fournir une protection raisonnable contre les interférences nuisibles susceptibles de se produire lorsque l'équipement est utilisé dans un environnement commercial. Cet équipement génère, utilise et peut émettre des fréquences radio et, s'il n'est pas installé et utilisé conformément au manuel de l'utilisateur, peut causer des interférences susceptibles de perturber les communications radio. L'utilisation de cet équipement en zone résidentielle est susceptible de causer du brouillage nuisible, auquel cas les utilisateurs devront corriger le brouillage à leurs propres frais.

Les informations suivantes sont relatives aux appareils de classe B et leur respect de la norme de la FCC : cet appareil a été testé et est conforme aux limites des appareils numériques de classe B, conformément à l'article 15 de la réglementation de la FCC. Ces limites sont destinées à fournir une protection raisonnable contre les interférences nuisibles causées lorsque l'équipement est utilisé en environnement résidentiel. Cet équipement génère, utilise et peut émettre des fréquences radio et, s'il n'est pas installé et utilisé conformément aux instructions, peut causer des interférences susceptibles de perturber les communications radio. Toutefois, nous ne pouvons en aucun cas garantir l’absence d’interférences dans une installation donnée. Si l'équipement provoque des interférences au niveau de la réception d’émissions radio ou télévisées, ce qui peut être constaté en l'allumant et en l'éteignant, l'utilisateur est invité à essayer de remédier à ces interférences à l'aide d'une ou de plusieurs mesures :

- Réorientez ou déplacez l'antenne de réception.
- Augmentez la distance entre l'équipement et le récepteur.
- Branchez l'équipement dans la prise d’un autre circuit que celui auquel le récepteur est raccordé.
- Sollicitez l’aide du distributeur ou d’un technicien radio/télévision expérimenté.

Toute modification de ce produit effectuée sans l'autorisation de Cisco est susceptible d'annuler l'autorisation accordée par la FCC et de rendre caduc votre droit d'utiliser ce produit.

La mise en œuvre Cisco de la compression d'en-tête TCP est l'adaptation d'un programme développé par l'Université de Californie, Berkeley (UCB), dans le cadre de la mise au point, par l'UCB, d'une version gratuite du système d'exploitation UNIX. Tous droits réservés. Copyright © 1981, Regents of the University of California.

NONOBSTANT TOUTE AUTRE GARANTIE CONTENUE DANS LES PRÉSENTES, TOUS LES DOSSIERS DE DOCUMENTATION ET LES LOGICIELS PROVENANT DE CES FOURNISSEURS SONT FOURNIS « EN L'ÉTAT », TOUS DÉFAUTS INCLUS. CISCO ET LES FOURNISSEURS SUSMENTIONNÉS DÉCLINENT TOUTE GARANTIE EXPLICITE OU IMPLICITE, NOTAMMENT CELLES DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER ET D'ABSENCE DE CONTREFAÇON, AINSI QUE TOUTE GARANTIE EXPLICITE OU IMPLICITE LIÉE À DES NÉGOCIATIONS, À UN USAGE OU À UNE PRATIQUE COMMERCIALE.

EN AUCUN CAS CISCO OU SES FOURNISSEURS NE SAURAIENT ÊTRE TENUS POUR RESPONSABLES DE DOMMAGES INDIRECTS, SPÉCIAUX, CONSÉQUENTS OU ACCIDENTELS, Y COMPRIS ET SANS LIMITATION, LA PERTE DE PROFITS OU LA PERTE OU LES DOMMAGES DE DONNÉES CONSÉCUTIVES À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISER CE MANUEL, MÊME SI CISCO OU SES FOURNISSEURS ONT ÉTÉ AVERTIS DE LA POSSIBILITÉ DE TELS DOMMAGES.

Les adresses IP (Internet Protocol) et les numéros de téléphone utilisés dans ce document ne sont pas censés correspondre à des adresses ni à des numéros de téléphone réels. Tous les exemples, résultats d'affichage de commandes, schémas de topologie du réseau et autres illustrations inclus dans ce document sont donnés à titre indicatif uniquement. L'utilisation d'adresses IP ou de numéros de téléphone réels à titre d'exemple est non intentionnelle et fortuite.

Les exemplaires imprimés et les copies numériques de ce document peuvent être obsolètes. La version originale en ligne constitue la version la plus récente.

Cisco compte plus de 200 agences à travers le monde. Les adresses et les numéros de téléphone sont indiqués sur le site web Cisco, à l'adresse suivante : www.cisco.com/go/offices.

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

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

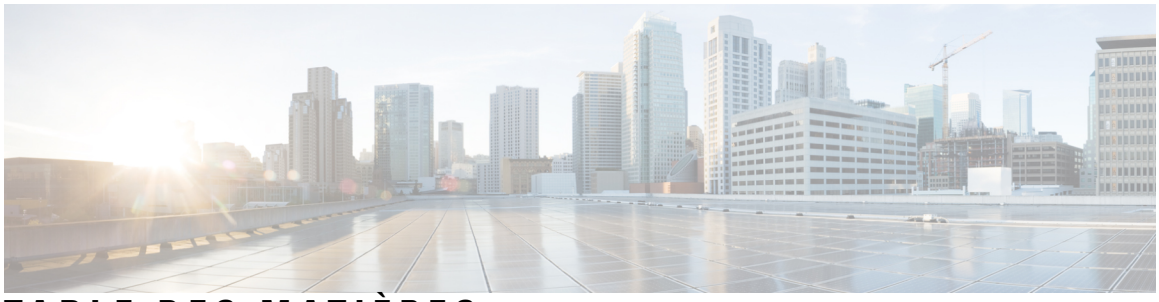


TABLE DES MATIÈRES

Préface

Vue d'ensemble

Le *Guide d'administration des Téléphones IP Cisco série 8800 pour téléphone Cisco Unified Communications Manager (SIP)* fournit les informations nécessaires pour comprendre, installer, configurer, gérer et dépanner les téléphones sur un réseau VoIP.

En raison de la complexité d'un réseau de téléphonie IP, ce guide ne présente pas les informations complètes et détaillées relatives aux procédures nécessaires dans Cisco Unified Communications Manager ou sur d'autres périphériques réseau.

Public visé

Les ingénieurs réseau, les administrateurs système et les ingénieurs en télécommunications doivent consulter ce guide pour connaître les étapes nécessaires à la configuration des téléphones IP Cisco. Les tâches décrites dans le présent document font intervenir la configuration de paramètres réseau qui ne concernent pas les utilisateurs du téléphone. Les tâches abordées dans le présent manuel nécessitent une bonne connaissance de Cisco Unified Communications Manager.

Conventions utilisées dans ce guide

Le présent document a recours aux conventions suivantes :

Convention	Description
police en **gras**	Les commandes et les mots-clés apparaissent en **gras**.
Police *italique*	Les arguments pour lesquels vous pouvez définir une valeur s'affichent en *italique*s.

Convention	Description
[]	Les éléments entre crochets droits sont facultatifs.
{x | y | z}	Les mots-clés alternatifs sont regroupés entre accolades et séparés par des barres verticales.
[x | y | z]	Les mots-clés alternatifs facultatifs sont regroupés entre crochets et séparés par des barres verti
chaîne	Un jeu de caractères sans guillemets. N'utilisez pas de guillemets autour de la chaîne, sinon seront inclus dans la chaîne.
police `écran`	Les informations et sessions de terminal affichées par le système apparaissent en police `écr`
police **`d'entrée`**	Les informations que vous devez saisir apparaissent en police de **`saisie`**.
police *écran italique*	Les arguments pour lesquels vous pouvez définir une valeur s'affichent en police *écran itali*
^	Le symbole ^ représente la touche CTRL : par exemple, la combinaison de touches ^D qui s'af sur un écran signifie que vous devez maintenir la touche CTRL enfoncée tout en appuyant s touche D.
<>	Les caractères invisibles, tels que les mots de passe, se trouvent entre crochets pointus.

Remarque Introduit une *remarque à l'attention du lecteur*. Les remarques contiennent des suggestions et des références utiles pour le matériel qui n'est pas couvert par la présente documentation.

Avertissement Invite le *lecteur à être prudent*. Dans cette situation, vous pourriez effectuer une opération risquant d'endommager l'équipement ou d'entraîner une perte de données.

Ce manuel utilise les conventions suivantes pour les avertissements :

Attention CONSIGNES DE SÉCURITÉ IMPORTANTES

Ce symbole d'avertissement indique un danger. Vous êtes dans une situation susceptible d'entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements qui figurent dans les consignes de sécurité accompagnant cet appareil, reportez-vous au numéro de l'instruction situé à la fin de chaque avertissement. Instruction 1071

CONSERVEZ CES INSTRUCTIONS.

Documentation associée

Consultez les sections suivantes pour obtenir des informations associées.

Documentation des Téléphone IP Cisco série 8800

Recherchez de la documentation spécifique à votre langue, au modèle de votre téléphone et à votre système de contrôle d'appel sur la page d'assistance produit du téléphone IP Cisco série 7800.

Le Guide de déploiement se trouve à l'adresse suivante :

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

Documentation des Cisco Unified Communications Manager

Consultez le Guide sur la documentation *Cisco Unified Communications Manager* et les autres publications propres à votre version de Cisco Unified Communications Manager. Naviguez à partir de l'URL de documentation suivante :

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

Documentation des Cisco Business Edition 6000

Consultez le Guide sur la documentation *Cisco Business Edition 6000* et les autres publications propres à votre version de Cisco Business Edition 6000. Naviguez à partir de l'URL suivante :

https://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000/tsd-products-support-series-home.html

Documentation, assistance technique et consignes de sécurité

Pour savoir comment obtenir de la documentation ou de l'assistance, nous faire part de votre avis sur la documentation, vous renseigner sur les consignes de sécurité ou encore pour en savoir plus sur les pseudonymes recommandés et les documents Cisco généraux, reportez-vous à la publication mensuelle *What's New in Cisco Product Documentation*, qui répertorie également les nouveautés et les révisions en matière de documentation technique Cisco, à l'adresse suivante :

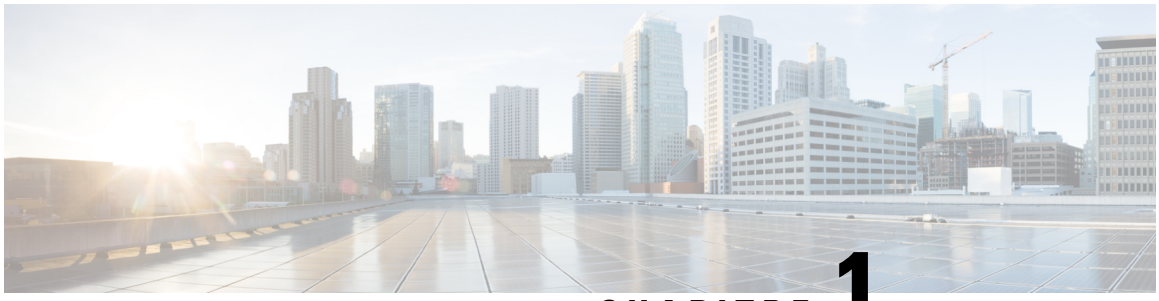
http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Abonnez-vous au flux RSS *What's New in Cisco Product Documentation* et programmez l'envoi direct de contenus vers votre bureau, à l'aide d'une application de type lecteur. Les flux RSS constituent un service gratuit ; Cisco prend actuellement en charge RSS version 2.0.

Présentation de la sécurité des produits Cisco

Ce produit, qui contient des fonctions cryptographiques, est soumis aux lois des États-Unis et d'autres pays, qui en régissent l'importation, l'exportation, le transfert et l'utilisation. La fourniture de produits cryptographiques Cisco n'autorise pas un tiers à importer, à exporter, à distribuer ou à utiliser le chiffrement. Les importateurs, exportateurs, distributeurs et utilisateurs sont responsables du respect des lois des États-Unis et des autres pays. En utilisant ce produit, vous acceptez de vous conformer aux lois et aux réglementations en vigueur. Si vous n'êtes pas en mesure de respecter les lois des États-Unis et celles des autres pays, renvoyez-nous ce produit immédiatement.

Pour en savoir plus sur les réglementations américaines sur les exportations, reportez-vous à l'adresse https://www.bis.doc.gov/policiesandregulations/ear/index.htm.



CHAPITRE 1

Nouveautés et mises à jour

Nouveautés et modifications des informations de la version 14.2(1) du micrologiciel

Les informations suivantes sont nouvelles ou modifiées pour le micrologiciel version 14.2 (1).

Nouveautés et modifications des informations de la version 14.1(1) du micrologiciel

Les informations suivantes sont nouvelles ou modifiées pour la version du micrologiciel 14.1(1).

Fonctionnalité	Nouveautés et mises à jour
Prise en charge du protocole TFTP SIP OAuth pour proxy	Renforcement de la sécurité pour votre réseau téléphonique, à la page 89

Fonctionnalité	Nouveautés et mises à jour
Alerte d'appel améliorée pour le groupe de recherche	Fonctionnalités du téléphone, à la page 126
Affichage des numéros d'appel configurables pour le mode ligne étendue	Configuration spécifique au produit
PLAR différés configurables	Fonctionnalités du téléphone, à la page 126
Prise en charge de MRA pour la connexion Extension Mobility avec les casques Cisco	Fonctionnalités du téléphone, à la page 126
Migration du téléphone sans utiliser de version de transition	Migration de votre téléphone vers un téléphone multiplateforme directement, à la page 200

Nouveautés et modifications des informations de la version 14.0(1) du micrologiciel

Tableau 1 : Nouveautés et mises à jour

Fonctionnalité	Nouveautés et mises à jour
Amélioration de la surveillance du parcage d'appels	Configuration spécifique au produit, à la page 149
Améliorations SIP OAuth	Renforcement de la sécurité pour votre réseau téléphonique, à la page 89
Améliorations de l'interface utilisateur	Survivable Remote Site Telephony (SRST), à la page 79 Fonctionnalités du téléphone, à la page 126
Améliorations de Oauth pour MRA	Mobile and Remote Access Through Expressway, à la page 183

Depuis la version 14.0 du micrologiciel, les téléphones prennent en charge DTLS 1.2. DTLS 1.2 nécessite l'appliance de sécurité adaptatif Cisco (ASA) version 9.10 ou ultérieure. Vous configurez la version DTLS minimale pour une connexion VPN dans ASA. Pour plus d'informations, reportez-vous à *Livre ASDM 3 : Guide de configuration du ASDM VPN Cisco série ASA* à l'adresse https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

Nouveautés et modifications des informations de la version 12.8 (1) du micrologiciel

Les informations suivantes sont nouvelles ou modifiées pour le micrologiciel version 12.8 (1).

Fonctionnalité	Nouveautés et modifications du contenu
Migration des données des téléphones	Modifier le modèle de téléphone d'un utilisateur, à la page 69
Amélioration de la mise à jour du casque	Informations sur le périphérique, à la page 242
Simplification de la connexion Extension Mobility avec les casques Cisco	Fonctionnalités du téléphone, à la page 126
Modifications de contrôles de fonctionnalité	Configuration spécifique au produit, à la page 149, les nouveaux champs **Baisser le son de votre alerte vocale** et **Marquer l'appel comme indésirable**
Modifications générales	Clarifier le Wi-Fi et le port PC : • Configuration du téléphone depuis les menus de configuration, à la page 51 • Activer le réseau local sans fil sur le téléphone, à la page 54
Ajouter des informations supplémentaires au champ d'accès au Web	Configuration spécifique au produit, à la page 149
Supprimer les fonctionnalités non prises en charge	Fonctionnalités du téléphone, à la page 126

Nouveautés et modifications des informations de la version 12.7 (1) du micrologiciel

Tableau 2 : Révisions apportées au Guide d'administration du téléphone IP Cisco 8800, relatives à la version 12.7(1) du micrologiciel.

Révision	Section mise à jour
Mise à jour relative à la prise en charge du fond d'écran sur les modules d'extension de touches.	Images d'arrière-plan personnalisées, à la page 119
Mise à jour pour la prise en charge de la fonction Casque Cisco 730	Informations sur le périphérique, à la page 242
Mise à jour pour le micrologiciel version 2.0 du Casque Cisco série 500	Informations sur le périphérique, à la page 242 Gestion des casques sur les versions antérieures de Cisco Unified Communications Manager, à la page 213
Mise à jour pour les appels entrants de groupe de recherche.	Fonctionnalités du téléphone, à la page 126
Les informations de configuration de la commutation électronique ont été supprimées.	Configuration spécifique au produit, à la page 149

Nouveautés et modifications des informations de la version 12.6(1) du micrologiciel

Toutes les références à la documentation Cisco Unified Communications Manager correspondent aux plus récentes versions de Cisco Unified Communications Manager.

Tableau 3 : Révisions apportées au guide d'administration du téléphone IP Cisco 8800, relatives à la version 12.6 du micrologiciel

Révision	Section mise à jour
Mise à jour de la prise en charge du retour à la ligne principale en mode ligne de session.	Configuration spécifique au produit, à la page 149 Environnement de mode ligne Session, à la page 170

Nouveautés de la version 12.5(1) SR3 du micrologiciel

Toutes les références à la documentation Cisco Unified Communications Manager correspondent aux plus récentes versions de Cisco Unified Communications Manager.

Tableau 4 : Révisions apportées au Guide d'administration du téléphone IP Cisco 8800, relatives à la version 12.5(1) SR3 du micrologiciel.

Révision	Section mise à jour
Prise en charge de l'intégration par code d'activation et de Mobile and Remote Access	Intégration par code d'activation et Mobile and Remote Access, à la page 47
Prise en charge de l'outil de rapport de problème utilisé à partir de Cisco Unified Communications Manager.	Créer un rapport sur les problèmes téléphoniques à partir de Cisco Unified Communications Manager, à la page 274
Nouvelle rubrique	Partager une connexion réseau avec votre téléphone et votre ordinateur, à la page 51
Nouvelle rubrique	Protéger la caméra de votre téléphone vidéo, à la page 41

Nouveautés de la version 12.5(1) SR1 du micrologiciel

Toutes les références à la documentation Cisco Unified Communications Manager correspondent aux plus récentes versions de Cisco Unified Communications Manager.

Tableau 5 : Révisions apportées au Guide d'administration du téléphone IP Cisco 8800, relatives à la version 12.5(1)SR1 du micrologiciel.

Révision	Section mise à jour
Prise en charge de la courbe elliptique	Fonctionnalités de sécurité prises en charge, à la page 90

Révision	Section mise à jour
Prise en charge des améliorations de l'historique des appels pour le mode ligne renforcée avec les lignes de substitution	Fonctions disponibles en mode ligne renforcée, à la page 207
Prise en charge de la radiomessagerie de chuchotement sur Cisco Unified Communications Manager Express	Interaction avec Cisco Unified Communications Manager Express, à la page 23
Prise en charge de la prise en charge linguistique du chinois	Limitation de langue, à la page 288
Prise en charge de l'intégration du code d'activation	Intégration par code d'activation pour les téléphones sur site, à la page 46
Prise en charge des chemins de média et de l'établissement de la connectivité interactive	Chemins de média et établissement de la connectivité Interactive, à la page 185
Prise en charge de la désactivation des codes de chiffrement TLS	Configuration spécifique au produit, à la page 149
Prise en charge de la désactivation du combiné pour que le chemin audio puisse être conservé vers le casque	Configuration spécifique au produit, à la page 149
Prise en charge de la configuration à distance des paramètres de casque	Gestion des casques sur les versions antérieures de Cisco Unified Communications Manager, à la page 213

Nouveautés de la version 12.1(1) SR1 du micrologiciel

Toutes les références à la documentation Cisco Unified Communications Manager correspondent aux plus récentes versions de Cisco Unified Communications Manager.

Tableau 6 : Révisions apportées au Guide d'administration du téléphone IP Cisco 8800, relatives à la version 12.1(1) SR1 du micrologiciel.

Révision	Section mise à jour
Composition Enbloc pour l'amélioration de la minuterie de délai entre chiffres T.302.	Configuration spécifique au produit, à la page 149

Nouveautés de la version 12.1(1) du micrologiciel

Toutes les références à la documentation Cisco Unified Communications Manager correspondent aux plus récentes versions de Cisco Unified Communications Manager.

Tableau 7 : Révisions apportées au Guide d'administration du téléphone IP Cisco 8800, relatives à la version 12.1(1) du micrologiciel.

Révision	Section mise à jour
Mobile and Remote Access Through Expressway prend désormais en charge le mode ligne renforcée.	Fonctionnalités téléphoniques disponibles pour Mobile and Remote Access Through Expressway, à la page 185
	Mobile and Remote Access Through Expressway, à la page 183
	Fonctions disponibles en mode ligne renforcée, à la page 207
L'activation ou la désactivation de TLS 1.2 pour l'accès au serveur web est désormais prise en charge.	Configuration spécifique au produit, à la page 149
Le codec audio G722.2 AMR-WB est désormais pris en charge.	Présentation des téléphones, à la page 31
	Champs relatifs aux statistiques d'appel, à la page 237

Nouveautés de la version 12.0(1) du micrologiciel

Toutes les nouvelles fonctionnalités sont présentées à la section Fonctionnalités du téléphone, à la page 126.

Toutes les références à la documentation Cisco Unified Communications Manager correspondent aux plus récentes versions de Cisco Unified Communications Manager.

Tableau 8 : Révisions apportées au Guide d'administration du téléphone IP Cisco 8800, relatives à la version 12.0(1) du micrologiciel.

Révision	Section mise à jour
Mise à jour pour le parcage d'appels, état de la ligne de parcage d'appels, interception d'appels de groupe et prend en charge les groupes de recherche en Mode ligne Avancé	Fonctions disponibles en mode ligne renforcée, à la page 207

Nouveautés de la version 11.7(1) du micrologiciel

Aucune révision n'a été apportée à l'administration, relative à la version 11.7(1) du micrologiciel.

Nouveautés de la version 11.5(1)SR1 du micrologiciel

Toutes les nouvelles fonctionnalités sont présentées à la section Fonctionnalités du téléphone, à la page 126.

Toutes les références à la documentation Cisco Unified Communications Manager correspondent aux plus récentes versions de Cisco Unified Communications Manager.

Tableau 9 : Révisions apportées au Guide d'administration du téléphone IP Cisco 8800, relatives à la version 11.5(1)SR1 du micrologiciel.

Révision	Section mise à jour
Mise à jour pour téléphone IP Cisco 8865NR	• Conditions requises pour l'alimentation du téléphone, à la page 16 • Protocoles réseau, à la page 18 • Présentation des téléphones, à la page 31 • Boutons et matériel du, à la page 38
Mise à jour pour la prise en charge d'enregistrement et de surveillance en mode ligne renforcée	Fonctions disponibles en mode ligne renforcée, à la page 207
Mise à jour pour la prise en charge de la liste de recherche de réseau local sans fil	Activer le réseau local sans fil sur le téléphone, à la page 54
	Configuration d'un réseau LAN sans fil depuis le téléphone, à la page 56
	Configurer des paramètres réseau, à la page 61
Mise à jour pour la prise en charge du mode MLPP avec Ne pas déranger	Configuration de la fonctionnalité Ne pas déranger, à la page 177
Mise à jour pour la prise en charge de la sonnerie configurable	Configuration spécifique au produit, à la page 149
Sécurité renforcée	Renforcement de la sécurité pour votre réseau téléphonique, à la page 89
Modifications générales	Mises à jour Page web du téléphone IP Cisco, à la page 241 Nouvelle présentation de la configuration des fonctions téléphoniques dans Cisco Unified Communications Manager Configuration des fonctionnalités téléphoniques, à la page 147

Nouveautés de la version 11.5(1) du micrologiciel

Tableau 10 : Révisions apportées au Guide d'administration du téléphone IP Cisco 8800, relatives à la version 11.5(1)SR1 du micrologiciel.

Révision	Section mise à jour
Le mode ligne renforcée est pris en charge.	Configuration des touches de ligne supplémentaires, à la page 207 Fonctions disponibles en mode ligne renforcée, à la page 207

Révision	Section mise à jour
Ne pas déranger (NPD) a été mis à jour pour les nouveaux écrans.	Configuration de la fonctionnalité Ne pas déranger, à la page 177
Le codec Opus est pris en charge.	Présentation des téléphones, à la page 31
Le mode FIPS a été ajouté.	Activer le mode FIPS, à la page 96
La configuration WLAN a été mise à jour.	Configuration d'un réseau LAN sans fil depuis le téléphone, à la page 56
Le profil WLAN pour les Téléphones IP Cisco 8861 et 8865 est pris en charge.	Définir un profil Wifi à l'aide de Cisco Unified Communications Manager, à la page 58
	Définir un groupe Wifi à l'aide de Cisco Unified Communications Manager, à la page 60
Le paramètre Définir les tentatives d'authentification WLAN est pris en charge.	Définir le nombre de tentatives d'authentification de réseau local sans fil (WLAN), à la page 57
Le paramètre Activer le Mode invite WLAN est pris en charge.	Activer le Mode invite du réseau local sans fil, à la page 58
Le paramètre Personnaliser la tonalité est pris en charge.	Personnaliser la tonalité, à la page 123
Le paramètre Afficher l'écran des informations de réseau est pris en charge.	Afficher l'écran Informations réseau, à la page 231

Nouveautés de la version 11.0 du micrologiciel

Toutes les nouvelles fonctionnalités sont présentées à la section Fonctionnalités du téléphone, à la page 126.

Toutes les références à la documentation Cisco Unified Communications Manager correspondent aux plus récentes versions de Cisco Unified Communications Manager.

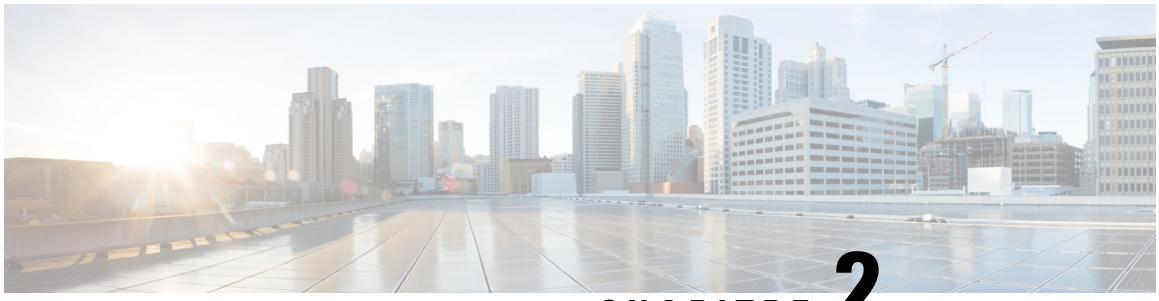
Tableau 11 : Révisions apportées au guide d'administration du téléphone IP Cisco 8800, relatives à la version 11.0 du micrologiciel

Révision	Section mise à jour
Mise à jour pour clarification et pour corriger les déficiences	• Configuration du réseau privé virtuel, à la page 206 • Configurer des paramètres réseau, à la page 61 • Configuration de Energy Efficient Ethernet (EEC) pour les ports SW et PC, à la page 181 • Configuration de la résolution de transmission vidéo, à la page 211 • Solution E-SRST (Enhanced Survivable Remote Site Telephony), à la page 82

Révision	Section mise à jour
Mise à jour pour l'amélioration de la prise en charge de l'option de débogage téléphonique de la section	• Contrôle des informations de débogage à l'aide de Cisco Unified Communications Manager, à la page 278.
Mise à jour pour l'amélioration de la prise en charge des certificats numériques EAP-TLS + SCEP, PEAP-GTC et X.509	• Sécurité WLAN, à la page 99. • Configurer le mode d'authentification, à la page 102 • Informations d'identification de sécurité sans fil, à la page 103
Mise à jour pour l'amélioration de la prise en charge de l'Outil de rapport de problème (PRT)	• Outil de rapport de problème, à la page 188. • Configuration d'une URL de téléchargement de l'assistance utilisateurs, à la page 188.
Ajout de la prise en charge des Règles de numérotation de l'application	• Règles de numérotation de l'application, à la page 82
Ajouté pour le Libellé de ligne	• Définition du libellé d'une ligne, à la page 190.

SECTION I

À propos des téléphones IP Cisco



CHAPITRE 2

Caractéristiques techniques

Spécifications physiques et environnementales

Le tableau suivant présente les caractéristiques physiques et l'environnement de fonctionnement des téléphones IP Cisco de la série 8800.

Tableau 12 : Caractéristiques environnementales et physiques

Spécification	Valeur ou plage
Température de fonctionnement	De 0 à 40 °C (de 32 à 104 °F)
Humidité relative en fonctionnement	En fonctionnement : de 10 à 90 % (sans condensation) Hors fonctionnement : de 10 à 95 % (sans condensation)
Température de stockage	De –10 °C à 60° C (de 14° à 114° F)
Hauteur	229,1 mm
Largeur	257,34 mm

Spécification	Valeur ou plage
Profondeur	40 mm
Poids	1,19 kg
Alimentation	100-240 VCA, 50-60 Hz, 0,5-0,2 A si utilisé avec l'adaptateur secteur 48 VDC, 0,2 A lorsqu'une alimentation est utilisée sur le câble réseau
Câbles	Catégorie 3/5/5e/6 pour des câbles 10 Mbits/s avec 4 paires Catégorie 5/5e/6 pour câbles 100 Mbits/s avec 4 paires Catégorie 5e/6 pour des câbles 1000 Mbits/s avec 4 paires **Remarque** Les câbles présentent 4 paires de fils pour un total de 8 conducteu
Exigences relatives à la distance	Comme stipulé par la spécification Ethernet, la longueur du câble reliant chaque IP Cisco au commutateur doit être de 100 mètres maximum.

Spécifications relatives aux câbles

Les informations suivantes répertorient les caractéristiques des câbles :

- Jack RJ-9 (4 conducteurs) pour la connexion des combiné et casque
- Jack RJ-45 pour la connexion LAN 10/100/1000BaseT (port réseau 10/100/1000 sur le téléphone)
- Jack RJ-45 pour une deuxième connexion 10/100/1000BaseT compatible (port ordinateur 10/100/1000 sur le téléphone)
- Jack de 3,5 mm pour la connexion du haut-parleur (uniquement sur les Téléphones IP Cisco 8861)
- Connecteur d'alimentation 48 volts
- Ports et connecteur USB : un port USB pour les Téléphones IP Cisco 8851 et deux ports USB pour les Téléphones IP Cisco 8861
- 3 connecteurs de module d'extension de touches qui est considéré comme le connecteur USB pour les Téléphones IP Cisco 8851 et 8861

Brochage des ports réseau et PC

Bien que les ports réseau et ordinateur (accès) soient tous deux utilisés pour la connectivité réseau, ils répondent à des objectifs différents et présentent plusieurs brochages de port.

- Le port réseau est le port SW 10/100/1000 sur le téléphone IP Cisco.
- Le port de l'ordinateur (accès) est le port PC 10/100/1000 sur le téléphone IP Cisco.

Connecteur pour port réseau

Le tableau suivant décrit le brochage de connecteur pour port réseau.

Tableau 13 : Brochage du connecteur pour port réseau

Numéro de broche	Fonction
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-
Remarque	BI signifie bidirectionnel, et DA, DB, DC et DD signifient respectivement Données A, Données B, Données C et Données D.

Connecteur de port d'ordinateur

Le tableau suivant décrit le brochage du connecteur pour port d'ordinateur.

Tableau 14 : Brochage du connecteur de port PC

Numéro de broche	Fonction
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-
Remarque	BI signifie bidirectionnel, et DA, DB, DC et DD signifient respectivement Données A, Données B, Données C et Données D.

Conditions requises pour l'alimentation du téléphone

Le téléphone IP Cisco peut fonctionner sur alimentation externe ou sur PoE (Power Over Ethernet). Un bloc d'alimentation distinct fournit l'alimentation externe. Le commutateur peut fournir l'alimentation PoE au moyen du câble Ethernet du téléphone.

Les Téléphones IP Cisco 8861 et 8865 sont des périphériques de classe PoE 4 et nécessitent une carte ligne ou commutateur avec des fonctionnalités de classe 4 pour prendre en charge des fonctionnalités supplémentaires.

Pour plus d'informations sur les exigences d'alimentation de votre téléphone, consultez la fiche technique de votre téléphone.

Lorsque vous installez un téléphone alimenté par une alimentation externe, connectez l'alimentation électrique avant de connecter le câble Ethernet au téléphone. Lorsque vous retirez un téléphone qui fonctionne sur alimentation externe, débranchez le câble Ethernet du téléphone avant de débrancher le bloc d'alimentation.

Tableau 15 : Directives relatives à l'alimentation du téléphone IP Cisco

Type d'alimentation	Directives
Alimentation externe : assurée par le bloc d'alimentation externe CP-PWR-CUBE-4=.	Le téléphone IP Cisco utilise le bloc d'alimentation externe CP-PWR-CUBE-4.
Alimentation PoE : fournie par un commutateur par le biais du câble Ethernet raccordé au téléphone.	Les Téléphones IP Cisco 8851, 8851NR, 8861, 8865 et 8865NR prennent en charge PoE pour l'utilisation d'accessoires. Pour plus d'informations, consultez la fiche techn votre téléphone. Le commutateur nécessite un bloc d'alimentation de secours pour assurer un fonctior ininterrompu du téléphone Vérifiez que la version de CatOS ou d'IOS qui est installée sur le commutateur prend le déploiement de votre téléphone. Reportez-vous à la documentation de votre comm pour connaître les exigences relatives à la version du système d'exploitation.
Alimentation UPoE (Universal Power-over-Ethernet)	Les Téléphones IP Cisco 8865 et 8865NR prennent en charge UPoE.

Les documents du tableau ci-dessous fournissent plus d'informations sur les sujets suivants :

- Les commutateurs Cisco compatibles avec les téléphones IP Cisco
- Les versions IOS Cisco prenant en charge la négociation bidirectionnelle de l'alimentation
- Autres exigences et restrictions concernant l'alimentation

Tableau 16 : Informations complémentaires

Sujets du document	URL
Solutions PoE	http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html
UPoE	http://www.cisco.com/c/en/us/solutions/enterprise-networks/upoe

Sujets du document	URL
Commutateurs Catalyst Cisco	http://www.cisco.com/c/en/us/products/switches/index.html
Routeurs à services intégrés	http://www.cisco.com/c/en/us/products/routers/index.html
Logiciel Cisco IOS	http://www.cisco.com/c/en/us/products/ios-nx-os-software/inc

Coupure de courant

Pour accéder au service d'urgence, votre téléphone doit être sous tension. En cas de coupure de courant, vous ne pourrez pas appeler le service d'appel en cas d'urgence ou de réparation tant que le courant n'aura pas été rétabli. En cas de coupure de courant, vous devrez peut-être réinitialiser ou reconfigurer votre téléphone pour pouvoir appeler le service d'appel d'urgence ou de réparation.

Réduction de l'alimentation

Vous pouvez réduire la quantité d'énergie consommée par le téléphone IP Cisco, grâce au mode Économies d'énergie ou EnergyWise (Économies d'énergie Plus).

Économies d'énergie

En mode Économies d'énergie, le rétroéclairage de l'écran n'est pas activé lorsque le téléphone n'est pas en cours d'utilisation. Le téléphone reste en mode Économies d'énergie pour la durée planifiée ou jusqu'à ce que l'utilisateur décroche le combiné ou appuie sur n'importe quel bouton.

Économies d'énergie Plus (EnergyWise)

Le téléphone IP Cisco prend en charge le mode EnergyWise (Économies d'énergie Plus) de Cisco. Lorsque votre réseau comporte un contrôleur EnergyWise (par exemple, un commutateur Cisco sur lequel la fonctionnalité EnergyWise est activée), vous pouvez configurer ces téléphones pour qu'ils se mettent en veille (arrêt) ou quittent leur veille (mise en marche) à des horaires donnés pour réduire encore plus la consommation électrique.

Configurez chaque téléphone pour activer ou désactiver les paramètres du mode EnergyWise. Si le mode EnergyWise est activé, configurez une heure de mise en veille, une heure de sortie de veille et d'autres paramètres. Ces paramètres sont envoyés au téléphone dans le cadre de la configuration du fichier XML.

Gestion de l'énergie sur LLDP

Le téléphone et le commutateur gèrent l'énergie consommée par le téléphone. Le téléphone IP Cisco peut fonctionner à plusieurs niveaux d'alimentation, ce qui réduit la consommation électrique lorsqu'il y a moins d'énergie disponible.

Après le redémarrage d'un téléphone, le commutateur choisit un protocole (CDP ou LLDP) pour la gestion de l'énergie. Le commutateur choisit le premier protocole (qui contient une TLV (Threshold Limit Value) d'énergie) que le téléphone transmet. Si l'administrateur système désactive ce protocole sur le téléphone, le téléphone ne peut plus alimenter d'accessoires car le commutateur ne répond pas aux requêtes d'énergie envoyées avec l'autre protocole.

Cisco vous conseille d'activer par défaut la fonctionnalité Gestion de l'énergie lorsque vous connectez un téléphone à un commutateur qui prend en charge la gestion de l'énergie.

Si la fonctionnalité Gestion de l'énergie est désactivée, il est possible que le commutateur déconnecte l'alimentation du téléphone. Si le commutateur ne prend pas en charge la gestion de l'énergie, désactivez la fonctionnalité Gestion de l'énergie avant d'alimenter les accessoires via PoE. Lorsque la fonctionnalité Gestion de l'énergie est désactivée, le téléphone peut alimenter les accessoires jusqu'au maximum permis par la norme IEEE 802.3af-2003.

Remarque

- Lorsque CDP et la fonctionnalité Gestion de l'énergie sont désactivés, le téléphone peut alimenter les accessoires jusqu'à 15,4 W.

Protocoles réseau

Le téléphone IP Cisco série 8800 prend en charge plusieurs protocoles réseaux Cisco et métier requis pour la communication vocale. Le tableau suivant présente les protocoles réseaux pris en charge par ces téléphones.

Tableau 17 : Protocoles réseaux pris en charge par le téléphone IP Cisco série 8800

Protocole réseau	Rôle	Notes sur l'utilisation
Bluetooth	Bluetooth est un protocole de réseau personnel sans fil (WPAN) qui spécifie la méthode de communication entre appareils sur de courtes distances.	Les Téléphones IP Cisco 8845, 8865 et 8851 prennent en charge Bluetooth 4.1. Les Téléphones IP Cisco 8861 prennent en charge Bluetooth 4.0. Les Téléphones IP Cisco 8811, 8841, 8851NR et 8865NR ne prennent pas en charge Bluetooth.
Protocole de démarrage (BootP)	BootP permet à un appareil réseau, comme un téléphone IP Cisco, de détecter certaines informations de démarrage, comme l'adresse IP.	-
Protocole CAST (Cisco Audio Session Tunnel)	Le protocole CAST permet à vos téléphones et aux applications associées de communiquer avec les téléphones IP distants sans demander de modifications des composants de signalisation.	Le téléphone IP Cisco utilise le protocole CAST en tant qu'interface entre CUVA et Cisco Unified Communications Manager ; dans ce cas, le téléphone IP Cisco fait office de proxy SIP.
Cisco Discovery Protocol (CDP)	CDP est un protocole de détection de périphériques qui est intégré à tous les équipements fabriqués par Cisco. Grâce au protocole CDP, un périphérique peut annoncer sa présence à d'autres périphériques et recevoir des informations sur d'autres périphériques du réseau.	Les téléphones IP Cisco utilisent CDP pour communiquer des informations comme l'ID VLAN auxiliaire, les détails du power management pour chaque port ainsi que les informations de configuration de la qualité de service (QoS) grâce au commutateur Catalyst Cisco.

Protocole réseau	Rôle	Notes sur l'utilisation
Protocole CPPDP (Cisco Peer-to-Peer Distribution Protocol)	CPPDP est un protocole propriétaire Cisco utilisé pour organiser une hiérarchie homologue-à-homologue des périphériques. Cette hiérarchie est utilisée pour distribuer les fichiers de micrologiciel depuis les périphériques pairs jusqu'aux périphériques voisins.	CPPDP est utilisé par la fonctionnalité de partage d'image.
Protocole DHCP (Dynamic Host Configuration Protocol)	Le protocole DHCP alloue dynamiquement une adresse IP qu'il affecte aux périphériques réseau. Le protocole DHCP vous permet de connecter un téléphone IP au réseau et de le rendre opérationnel sans avoir besoin d'attribuer manuellement une adresse IP ni de configurer des paramètres réseau supplémentaires.	Le protocole DHCP est activé par défaut. S'il est désactivé, vous devez configurer manuellement l'adresse IP, le masque de sous-réseau, la passerelle et un serveur TFTP sur chaque téléphone. Il est recommandé d'utiliser l'option personnalisée DHCP 150. Cette méthode permet de configurer l'adresse IP du serveur TFTP en tant que valeur de l'option. Pour plus d'informations, reportez-vous à la documentation relative à votre version particulière de Cisco Unified Communications Manager. **Remarque** Si vous ne pouvez pas utiliser l'option n°150, vous pouvez essayer d'utiliser l'option DHCP n°66.
Protocole HTTP (HyperText Transfer Protocol)	Le protocole HTTP est la méthode standard de transmission des informations et de déplacement de documents via Internet et le web.	Les téléphones IP Cisco utilisent le protocole HTTP pour les services XML et à des fins de dépannage.
Protocole HTTPS (Hypertext Transfer Protocol Secure)	Le protocole HTTPS (Hypertext Transfer Protocol Secure) est une combinaison du protocole de transfert hypertexte (HTTP) et du protocole SSL/TLS, qui permet le chiffrement et l'identification sécurisée des serveurs.	Deux URL sont configurées pour les applications web qui prennent en charge à la fois HTTP et HTTPS. Les téléphones IP Cisco qui prennent en charge HTTPS utilisent l'URL HTTPS.
IEEE 802.1x	La norme IEEE 802.1x définit un contrôle d'accès de type client-serveur et un protocole d'authentification qui empêche les clients non autorisés de se connecter à un réseau LAN via des ports accessibles publiquement. Tant que le client n'est pas authentifié, le contrôle d'accès 802.1X autorise uniquement le protocole EAPOL (Extensible Authentication Protocol over LAN) sur le trafic via le port auquel le client est connecté. Une fois l'authentification réussie, le trafic normal peut traverser le port.	Le téléphone IP Cisco implémente la norme IEEE 802.1x en prenant en charge les méthodes d'authentification suivantes : EAP-FAST et EAP-TLS. Lorsque l'authentification 802.1x est activée sur le téléphone, il est recommandé de désactiver le port PC et le VLAN voix.

Protocole réseau	Rôle	Notes sur l'utilisation
IEEE 802.11n/802.11ac	La norme IEEE 802.11 spécifie la méthode de communication entre appareils via un réseau local sans fil (WLAN). 802.11n fonctionne sur la bande des 2,4 GHz et celle des 5 GHz. 802.11ac fonctionne sur la bande des 5 GHz.	L'interface 802.11 est une option de déploiement pour les situations dans lesquelles le câblage Ethernet est impossible ou indésirable. Seuls les Téléphones IP Cisco 8861 et 8865 prennent en charge WLAN.
Protocole IP	Le protocole IP est un protocole de messagerie qui adresse et envoie des paquets sur le réseau.	Pour communiquer via IP, les périphériques réseau doivent se voir attribuer une adresse IP, un sous-réseau ainsi qu'une passerelle. Les adresses IP, les sous-réseaux et les passerelles sont attribués automatiquement si vous utilisez un téléphone IP Cisco avec le protocole DHCP (Dynamic Host Configuration Protocol). Si vous n'utilisez pas DHCP, vous devez affecter manuellement ces propriétés à chaque téléphone, localement. Les téléphones IP Cisco prennent en charge les adresses IPv6. Pour obtenir plus d'informations, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.
Protocole LLDP (Link Layer Discovery Protocol)	LLDP est un protocole standardisé de détection de réseau (similaire au protocole CDP) qui est pris en charge par certains périphériques Cisco et de fabricants tiers.	LLDP est pris en charge sur le port PC des téléphones IP Cisco.
LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Devices)	LLDP-MED est une extension de la norme LLDP pour les produits de communication vocale.	LLDP-MED est pris en charge sur le port de commutation des téléphones IP Cisco, pour communiquer des informations telles que : • La configuration du VLAN • La détection de périphériques • La gestion de l'alimentation • La gestion de l'inventaire
Protocole RTP (Real-Time Transport Protocol)	RTP est un protocole standard pour le transfert de données en temps réel via des réseaux de données, comme la voix interactive.	Les téléphones IP Cisco utilisent le protocole RTP pour envoyer et recevoir le trafic audio en temps réel provenant d'autres téléphones et passerelles.
Protocole RTCP (Real-Time Control Protocol)	Le protocole RTCP fonctionne en conjonction avec le protocole RTP pour fournir des données QoS (comme la gigue, la latence et le délai aller-retour) sur les flux RTP.	Le protocole RTCP est activé par défaut.

Protocole réseau	Rôle	Notes sur l'utilisation
Protocole SDP (Session Description Protocol)	SDP est la partie du protocole SIP qui permet de déterminer quels paramètres sont disponibles pendant une connexion entre deux terminaux. Les conférences sont créées en utilisant uniquement les fonctionnalités SDP prises en charge par tous les terminaux dans la conférence.	Les fonctionnalités SDP, comme les types de codec, la détection DTMF et le bruit de confort, sont habituellement configurées à un niveau global par Cisco Unified Communications Manager ou la passerelle multimédia en fonction. Certains terminaux SIP peuvent permettre la configuration de ces paramètres directement sur le terminal.
Protocole SIP (Session Initiation Protocol)	Le protocole SIP est la norme de groupe de travail (IETF, Internet Engineering Task Force) pour la conférence multimédia sur IP. SIP est un protocole ASCII de contrôle de couche application (défini dans la norme RFC 3261), qui peut être utilisé pour établir, gérer et interrompre des appels entre plusieurs terminaux.	Comme les autres protocoles VoIP, le protocole SIP se charge du signalement et de la gestion des sessions dans un réseau de téléphonie par paquets. Le signalement permet le transport des informations d'appel au-delà des limites d'un réseau. La gestion des sessions permet de contrôler les attributs d'un appel de bout en bout. Les téléphones IP Cisco prennent en charge le protocole SIP lorsqu'ils fonctionnent uniquement en IPv6, uniquement en IPv4 ou à la fois en IPv6 et IPv4.
Protocole TCP (Transmission Control Protocol)	Le protocole TCP est un protocole de transport orienté connexion.	Les téléphones IP Cisco utilisent TCP pour se connecter à Cisco Unified Communications Manager et pour accéder aux services XML.
Transport Layer Security (Protocole TLS, Sécurité des couches de transport)	TLS est un protocole standard de sécurisation et d'authentification des communications.	Dès l'implémentation de la sécurité, les téléphones IP Cisco utilisent le protocole TLS lorsqu'ils s'enregistrent de manière sécurisée auprès de Cisco Unified Communications Manager.
Protocole TFTP (Trivial File Transfer Protocol)	Le protocole TFTP permet de transférer des fichiers sur le réseau. Sur un téléphone IP Cisco, le protocole TFTP vous permet d'obtenir un fichier de configuration propre au modèle du téléphone.	Le protocole TFTP nécessite la présence dans votre réseau d'un serveur TFTP que le serveur DHCP peut identifier automatiquement. Si vous voulez qu'un téléphone utilise un serveur TFTP autre que celui spécifié par le serveur DHCP, vous devez attribuer manuellement l'adresse IP du serveur TFTP souhaité en utilisant le menu Configuration réseau sur le téléphone. Pour obtenir plus d'informations, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.
Protocole UDP (Utilisateur Datagram Protocol)	Le protocole UDP est un protocole de communication sans connexion pour l'envoi des paquets de données.	Le protocole UDP est uniquement utilisé par les flux RTP. Le signalement SIP sur les téléphones ne prend pas en charge le protocole UDP.

Pour plus d'informations sur la prise en charge de LLDP-MED, consultez le livre blanc LLDP-MED and Cisco Discovery Protocol :

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

Rubriques connexes

Authentification 802.1x, à la page 115
Configurer des paramètres réseau
Vérification du démarrage du téléphone, à la page 68
Interaction VLAN, à la page 22
Interaction avec Cisco Unified Communications Manager, à la page 22
Interaction avec Cisco Unified Communications Manager Express, à la page 23
Configuration de la plage des ports audio et vidéo, à la page 193
Documentation des Cisco Unified Communications Manager, à la page xv

Interaction VLAN

Le téléphone IP Cisco contient un commutateur Ethernet interne, qui permet la transmission de paquets au téléphone, au port PC et au port réseau situés à l'arrière du téléphone.

Si un ordinateur est connecté au port (d'accès au) PC, l'ordinateur et le téléphone partagent la même liaison physique au commutateur et le même port sur le commutateur. Ce lien physique commun présente les implications suivantes pour la configuration VLAN du réseau :

- Les VLAN actuels peuvent être configurés par sous-réseau IP. Toutefois, des adresses IP supplémentaires risquent de ne pas être disponibles pour affecter le téléphone au même sous-réseau que d'autres périphériques connectés au même port.
- Le trafic de données du réseau VLAN qui prend en charge les téléphones peut réduire la qualité du trafic VoIP.
- La sécurité du réseau peut indiquer qu'il est nécessaire d'isoler le trafic voix du trafic de données VLAN.

Pour résoudre ces problèmes, isolez le trafic voix en l'hébergeant sur un VLAN distinct. Le port de commutation auquel le téléphone est connecté doit être configuré pour des VLAN distincts pour transporter :

- Le trafic voix en direction et en provenance du téléphone IP (VLAN auxiliaire sur le téléphone Cisco Catalyst série 6000, par exemple)
- Le trafic voix en direction et en provenance de l'ordinateur qui est connecté à ce commutateur au moyen du port PC du téléphone IP (VLAN natif)

Le fait d'isoler les téléphones sur un VLAN auxiliaire distinct améliore la qualité du trafic voix et permet l'ajout d'un grand nombre de téléphones sur un réseau qui ne dispose pas de suffisamment d'adresses IP pour tous les téléphones.

Pour obtenir plus d'informations, reportez-vous à la documentation relative aux commutateurs Cisco. Vous pouvez également accéder aux informations relatives aux commutateurs à l'adresse suivante :

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

Interaction avec Cisco Unified Communications Manager

Cisco Unified Communications Manager est un système de traitement d'appels ouvert reconnu comme un des meilleurs du marché. Le logiciel Cisco Unified Communications Manager organise les appels entre les téléphones et intègre les fonctionnalités PABX habituelles au réseau IP de l'entreprise. Cisco Unified

Communications Manager gère les éléments d'un système de téléphonie IP, comme les téléphones, les passerelles d'accès et les ressources indispensables aux fonctionnalités comme la téléconférence et la planification du routage. Cisco Unified Communications Manager fournit également :

- Des micrologiciels pour les téléphones
- Les fichiers CTL (Certificate Trust List) et ITL (Identify Trust List) utilisant les services TFTP et HTTP
- L'enregistrement des téléphones
- La conservation d'appel, afin qu'une session multimédia puisse continuer en cas de perte de signal entre l'instance principale de Communications Manager et un téléphone

Pour plus d'informations sur la configuration de Cisco Unified Communications Manager pour qu'il interagisse avec les téléphones IP décrits dans ce chapitre, consultez la documentation relative à votre version spécifique de Cisco Unified Communications Manager.

Remarque Si le modèle de téléphone IP Cisco que vous souhaitez configurer n'apparaît pas dans la liste déroulante Type de téléphone de Cisco Unified Communications Manager Administration, installez le dernier package du périphérique pour votre version de Cisco Unified Communications Manager à partir du site Cisco.com.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Interaction avec Cisco Unified Communications Manager Express

Lorsque le téléphone IP Cisco utilise Cisco Unified Communications Manager Express (Unified CME), les téléphones doivent entrer en mode CME.

Lorsqu'un utilisateur requiert la fonctionnalité de conférence, la balise permet au téléphone d'utiliser un pont de conférence matériel local ou en réseau.

Les téléphones ne prennent pas en charge les actions suivantes :

- Transfert : uniquement pris en charge dans le scénario de transfert d'appels connecté.
- Conférence : uniquement prise en charge dans le scénario de transfert d'appels connecté.
- Jointure : prise en charge à l'aide du bouton Conférence ou de l'accès au crochet commutateur.
- Attente : prise en charge à l'aide de la touche de mise en attente.
- Insertion et fusion : non prises en charge.
- Transfert direct : non pris en charge.
- Sélectionner : non pris en charge.

Les utilisateurs ne peuvent pas créer de conférences ni transférer des appels sur différentes lignes.

Unified CME prend en charge les appels intercom, également connus sous le nom de radiomessagerie de chuchotement. Mais la radiomessagerie est rejetée par le téléphone lors des appels.

Le mode ligne de session et le mode ligne étendue sont tous deux pris en charge en mode CME.

Interaction du système de messagerie vocale

Cisco Unified Communications Manager vous permet d'intégrer différents systèmes de messagerie vocale, y compris le système de messagerie vocale Cisco Unity Connection. Comme il est possible d'intégrer plusieurs systèmes, vous devez fournir aux utilisateurs des informations sur l'utilisation de votre système spécifique.

Pour permettre à un utilisateur de transférer vers la messagerie vocale, configurez un modèle de numérotation *xxxxx et configurez-le comme Renvoi de tous les appels vers la messagerie vocale. Pour plus d'informations, reportez-vous à la documentation de Cisco Unified Communications Manager.

Fournissez les informations suivantes à chaque utilisateur :

- Comment accéder à son compte du système de messagerie vocale.

  Assurez-vous que vous avez utilisé Cisco Unified Communications Manager pour configurer le bouton Messages sur le téléphone IP Cisco.

- Mot de passe initial pour accéder au système de messagerie vocale.

  Configurez un mot de passe par défaut pour le système de messagerie vocale pour tous les utilisateurs.

- Comment le téléphone indique la présence de messages vocaux en attente.

  Utilisez Cisco Unified Communications Manager pour configurer une méthode MWI (indicateur de message en attente).

Présentation du démarrage du téléphone

Lorsque les téléphones IP Cisco se connectent au réseau VoIP, ils entament un processus de démarrage standard. En fonction de votre configuration réseau, seules certaines de ces étapes peuvent avoir lieu pour votre téléphone IP Cisco.

1. Branchez l'alimentation du téléphone sur le commutateur. Si le téléphone n'utilise pas d'alimentation externe, le commutateur assure une alimentation via le câble Ethernet relié au téléphone.
2. (Pour les téléphones IP Cisco 8861 et 8865 dans un réseau WLAN uniquement) Cherchez un point d'accès. Les téléphones IP Cisco 8861 et 8865 parcourent la zone de couverture RF via radio. Le téléphone recherche les profils réseau et cherche des points d'accès contenant un SSID et un type d'authentification correspondant à ces profils. Le téléphone s'associe avec le point d'accès ayant le RSSI le plus élevé qui correspond au profil réseau.
3. (Pour les téléphones IP Cisco 8861 et 8865 dans un réseau WLAN uniquement) Authentifiez le téléphone auprès du point d'accès. Le téléphone IP Cisco entame le processus d'authentification. Le tableau suivant décrit le processus d'authentification :

Type d'authentification	Options de gestion des clés	Description
Ouverte	Aucun	N'importe quel périphérique peut s'authentifier auprès du point d'accès. Pour plus de sécurité, un chiffrement statique WEP peut être éventuellement utilisé.
Clé partagée	Aucun	Le téléphone chiffre le texte de test à l'aide la clé WEP. Le point d'accès doit vérifier la clé WEP utilisée pour chiffrer le texte de test avant d'autoriser l'accès au réseau.
PEAP ou EAP-FAST	Aucun	Le serveur RADIUS authentifie le nom d'utilisateur et le mot de passe avant d'autoriser l'accès au réseau.

4. Chargez le fichier image stocké du téléphone. Pendant le démarrage, le téléphone exécute un chargeur d'amorçage qui charge un fichier d'image de micrologiciel de téléphone stockée dans la mémoire flash. Grâce à cette image, le téléphone initialise le logiciel et le matériel.
5. Configurez le réseau virtuel VLAN. Si le téléphone IP Cisco est connecté à un commutateur Cisco Catalyst, le commutateur informe ensuite le téléphone du VLAN vocal défini sur le commutateur. Le téléphone doit connaître les appartenances au VLAN avant de procéder à la requête DHCP (Dynamic Host Configuration Protocol) pour une adresse IP.
6. Obtenez une adresse IP. Si le téléphone IP Cisco utilise DHCP pour obtenir une adresse IP, il envoie une requête d'obtention au serveur DHCP. Si vous n'utilisez pas de DHCP dans votre réseau, vous devez attribuer localement une adresse IP statique à chaque téléphone.
7. Effectuez une requête de fichier CTL. Le fichier CTL est stocké sur le serveur TFTP. Ce fichier contient les certificats nécessaires à l'établissement d'une connexion sécurisée entre le téléphone et Cisco Unified Communications Manager.

   Pour plus d'informations, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
8. Effectuez une requête de fichier ITL. Le téléphone effectue une requête de fichier ITL après la requête de fichier CTL. Le fichier ITL contient les certificats des entités auxquelles le téléphone peut faire confiance. Ces certificats sont utilisés pour authentifier une connexion sécurisée avec les serveurs ou pour authentifier une signature numérique provenant des serveurs. Cisco Unified Communications Manager 8.5 et versions ultérieures prennent en charge le fichier ITL.
9. Accédez à un serveur TFTP. En plus d'attribuer une adresse IP, le serveur DHCP guide le téléphone IP Cisco vers un serveur TFTP. Si le téléphone a une adresse IP statique, vous devez configurer localement le serveur TFTP sur le téléphone ; il contactera ensuite le serveur TFTP directement.

Remarque Vous pouvez également attribuer un serveur TFTP alternatif, à utiliser à la place de celui proposé par le serveur DHCP.

10. Effectuez une requête de fichier de configuration. Le serveur TFTP contient des fichiers de configuration, qui définissent les paramètres de connexion à Cisco Unified Communications Manager ainsi que d'autres informations pour le téléphone.

11. Contactez Cisco Unified Communications Manager. Le fichier de configuration détermine la manière dont le téléphone IP Cisco communique avec Cisco Unified Communications Manager et fournit au téléphone une ID de chargement. Une fois que le téléphone a obtenu le fichier depuis le serveur TFTP, il va essayer d'établir une connexion au Cisco Unified Communications Manager ayant la priorité la plus haute de la liste.

    Si le profil de sécurité ou le téléphone est paramétré pour le signalement sécurisé (chiffré ou authentifié) et que Cisco Unified Communications Manager est paramétré en mode sécurisé, le téléphone établit alors une connexion TLS. Sinon, le téléphone établit une connexion TCP non sécurisée.

    Si le téléphone a été ajouté manuellement à la base de données, Cisco Unified Communications Manager identifie le téléphone. Si le téléphone n'a pas été ajouté manuellement à la base de données et que l'enregistrement automatique est activé dans Cisco Unified Communications Manager, le téléphone tente de s'enregistrer automatiquement dans la base de données de Cisco Unified Communications Manager.

Remarque L'enregistrement automatique est désactivé lorsque vous configurez le client CTL. Dans ce cas, vous devez ajouter manuellement le téléphone à la base de données de Cisco Unified Communications Manager.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Périphériques externes

Il est recommandé d'utiliser des périphériques externes de bonne qualité, blindés contre les interférences émises par les signaux de fréquences radio (RF) ou audio (AF). Les périphériques externes comprennent les casques, les câbles et les connecteurs.

Selon la qualité de ces périphériques et leur proximité par rapport à d'autres périphériques, tels que des téléphones portables ou des radios bidirectionnelles, des parasites sonores sont toujours susceptibles de se produire. Dans ce cas, il est recommandé d'appliquer une ou plusieurs des mesures ci-dessous :

- Éloigner le périphérique externe de la source émettrice des signaux de fréquences radio ou audio.
- Maintenir les câbles du périphérique externe éloignés de la source émettrice des signaux de fréquences radio ou audio.
- Utiliser des câbles blindés pour le périphérique externe ou des câbles dotés d'un blindage supérieur et d'un meilleur connecteur.
- Raccourcir le câble du périphérique externe.
- Utiliser des structures en ferrite ou d'autres dispositifs de ce type pour les câbles du périphérique externe.

Cisco ne peut pas garantir les performances des périphériques, des câbles et des connecteurs externes.

Avertissement Dans les pays de l'Union européenne, utilisez uniquement des haut-parleurs, des microphones et des casques externes conformes à la Directive 89/336/CE sur la compatibilité électromagnétique (CEM).

Informations port USB

Les Téléphones IP Cisco 8851, 8851NR, 8861, 8865 et 8865NR prennent en charge un maximum de cinq périphériques se connectant à chaque port USB. Chaque périphérique qui se connecte au téléphone est inclus dans le nombre maximum de périphériques. Par exemple, votre téléphone peut prendre en charge cinq périphériques USB sur le port latéral et cinq périphériques USB supplémentaires sur le port arrière. Un grand nombre de produits USB tiers peuvent compter comme plusieurs périphériques USB. Par exemple, un périphérique contenant un concentrateur USB ainsi qu'un casque peut compter comme deux périphériques USB. Pour en savoir plus, reportez-vous à la documentation du périphérique USB.

Remarque

- Les concentrateurs non alimentés ne sont pas pris en charge et les concentrateurs alimentés disposant de plus de quatre ports ne sont pas pris en charge.
- Les casques USB se connectant au téléphone via un concentrateur USB ne sont pas pris en charge.

Chaque module d'extension de touches qui est raccordé au téléphone compte comme un périphérique USB. Si trois modules d’extension de touches sont raccordés au téléphone, ils comptent comme trois périphériques USB.

Fichiers de configuration du téléphone

Les fichiers de configuration d'un téléphone sont stockés sur le serveur TFTP et définissent les paramètres de connexion à Cisco Unified Communications Manager. De manière générale, lorsque vous modifiez un paramètre de Cisco Unified Communications Manager qui nécessite la réinitialisation du téléphone, le fichier de configuration du téléphone est automatiquement modifié.

Les fichiers de configuration contiennent également des informations sur l'image de chargement que le téléphone doit utiliser. Si cette image de chargement est différente de celle actuellement chargée sur un téléphone, le téléphone contacte le serveur TFTP et envoie une requête pour les fichiers de chargement requis.

Si vous configurez des paramètres de sécurité dans Cisco Unified Communications Manager Administration, le fichier de configuration du téléphone contiendra des informations sensibles. Pour garantir la confidentialité d'un fichier de configuration, vous devez configurer son chiffrement. Pour obtenir plus d'informations, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager. Un téléphone envoie une requête de fichier de configuration à chaque fois qu'il se réinitialise et qu'il s'enregistre auprès de Cisco Unified Communications Manager.

Un téléphone accède au fichier de configuration par défaut nommé XmlDefault.cnf.xml situé sur le serveur TFTP lorsque les conditions suivantes sont remplies :

- Vous avez activé l'enregistrement automatique dans Cisco Unified Communications Manager
- Le téléphone n'a pas été ajouté à la base de données de Cisco Unified Communications Manager

- Le téléphone s'enregistre pour la première fois

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Comportement du téléphone pendant les périodes de congestion du réseau

Tout élément susceptible de dégrader la performance du réseau risque d'affecter la qualité téléphonique audio et vidéo, et dans certains cas, d'entraîner l'abandon d'un appel. Parmi les sources de dégradation du réseau figurent, de manière non exhaustive, les activités suivantes :

- Les tâches administratives telles qu'une analyse de port interne ou une analyse de sécurité.
- Les attaques se produisant sur le réseau, telles que les attaques de déni de service.

Comportement téléphonique sur un réseau avec deux routeurs réseau

Le téléphone IP Cisco série 8800 utilise un pare-feu pour assurer sa protection contre les intrusions via internet, comme les attaques HDM (homme du milieu) ou MITM (man in the middle). Ce pare-feu ne peut pas être désactivé. Cependant, il peut bloquer le trafic sur un téléphone, si vous configurez votre réseau avec deux routeurs dans le même sous-réseau et avec une redirection IP.

Le pare-feu du téléphone bloque le trafic, car cette configuration réseau est similaire à une attaque HDM. Le téléphone reçoit des paquets de redirection de destinations IP différentes dans un autre sous-réseau. Le téléphone est dans un réseau comportant plusieurs routeurs et le routeur par défaut envoie du trafic à un deuxième routeur.

Consultez l'historique d'activité du téléphone si vous pensez que le pare-feu bloque le trafic. Vérifiez si une notification de code d'erreur 1 est présente, envoyée par le système d'exploitation lorsqu'il a tenté d'établir une connexion. L'une des signatures est

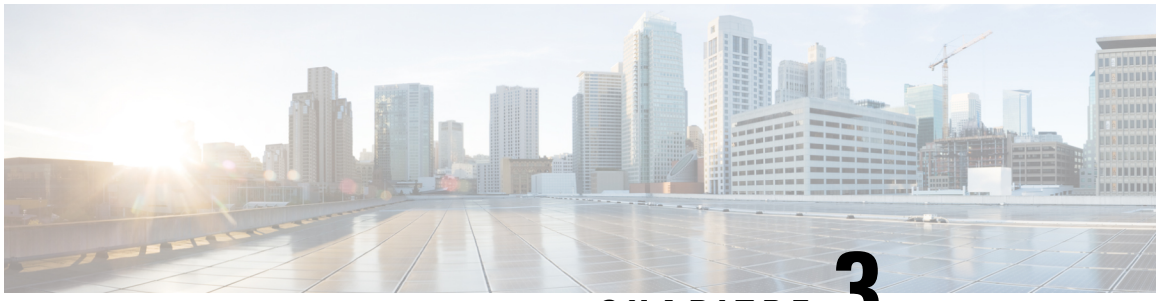
```
sip_tcp_create_connection: socket connect failed cpr_errno: 1.
```

Un réseau ayant deux routeurs dans le même sous-réseau et une redirection IP est une configuration inhabituelle. Si vous utilisez une telle configuration réseau, envisagez de n'utiliser qu'un seul routeur par sous-réseau. Cependant, si vous avez besoin de deux routeurs dans un même sous-réseau, désactivez la redirection IP sur le routeur et redémarrez le téléphone.

Application Programming Interface – Interface de programmation d'applications

Cisco prend en charge l'utilisation des API de téléphone par les applications tierces qui ont été testées et certifiées via Cisco par le développeur de l'application tierce. Tout problème de téléphone lié à l'interaction d'une application non certifiée doit être traité par le tiers et ne sera pas pris en considération par Cisco.

Pour obtenir des informations sur les modèle pris en charge par les applications/solutions tierces certifiées par Cisco, reportez-vous au site Web du programme des partenaires Solution de Cisco.



CHAPITRE 3

Matériel du téléphone IP Cisco

Présentation des téléphones

Les téléphones IP Cisco série 8800 permettent la communication vocale via un réseau IP (Internet Protocol). Le téléphone IP Cisco fonctionne comme tout téléphone professionnel numérique, vous permettant de passer des appels ainsi que d'accéder à des fonctionnalités comme le mode muet, la mise en attente, le transfert et bien plus encore. De plus, du fait que le téléphone se connecte à votre réseau de données, il offre des fonctions avancées de téléphonie sur IP, y compris l'accès aux informations sur le réseau et les services, ainsi que des fonctions et des services personnalisables.

Le téléphone IP Cisco 8811 dispose d'un écran LCD en nuances de gris. Les Téléphones IP Cisco 8841, 8845, 8851, 8851NR, 8861, 8865 et 8865NR disposent d'un écran LCD couleur 24 bits.

Lors de l'ajout des fonctionnalités aux touches de ligne téléphonique, vous êtes limité par le nombre de touches de ligne disponibles. Vous ne pouvez pas ajouter plus de fonctionnalités que le nombre de touches de ligne sur votre téléphone.

Les téléphones IP Cisco présentent les fonctionnalités suivantes :

- Boutons de fonction programmables qui prennent en charge jusqu'à 5 lignes en mode ligne de session ou jusqu'à 10 lignes en mode ligne renforcée
- Capacités vidéo complètes (téléphones IP Cisco 8845, 8865 et 8865NR uniquement)
- Connectivité Gigabit Ethernet
- Prise en charge Bluetooth pour les casques sans fil (Téléphones IP Cisco 8845, 8851, 8861 et 8865 uniquement). Cette fonctionnalité n'est pas prise en charge sur les Téléphones IP Cisco 8811, 8841, 8851NR et 8865NR).
- Prise en charge d'un microphone et de haut-parleurs externes (Téléphones IP Cisco 8861, 8865 et 8865NR uniquement)

- Connectivité réseau via Wi-Fi (Téléphones IP Cisco 8861 et 8865 uniquement). La Wi-Fi n'est pas prise en charge sur les Téléphones IP Cisco 8865NR).
- Ports USB :
  - Un port USB pour les Téléphones IP Cisco 8851 et 8851NR
  - Deux ports USB pour les Téléphones IP Cisco 8861, 8865 et 8865NR

Les téléphones IP Cisco 8845, 8865 et 8865NR prennent en charge les appels vidéo avec caméra intégrée. Utilisez cette fonctionnalité pour collaborer avec des amis ou des collègues ou pour tenir des conférences en face à face sur le téléphone.

Remarque Vous devez mettre de côté la boîte et l'emballage des téléphones IP Cisco 8845, 8865 et 8865NR. Les caméras de ces téléphones sont fragiles. Si vous devez déplacer le téléphone, nous vous recommandons de l'emballer dans la boîte d'origine pour protéger la caméra. Pour obtenir plus d'informations, reportez-vous à Protéger la caméra de votre téléphone vidéo, à la page 41.

Les appels vidéo incluent les fonctionnalités suivantes :

- PIP : sélectionnez l'une des quatre positions disponibles : En bas à droite, En haut à droite, En haut à gauche et En bas à gauche. Vous pouvez également désactiver l'incrustation d'image (PIP).
- Permuter : permet de basculer entre les vues PIP. La touche dynamique Permuter est désactivée lorsque l'incrustation d'image est désactivée.
- Retour d'image vidéo : sélectionnez Retour d'image vidéo pour visualiser votre image telle qu'elle apparaît sur la vidéo.
- IU Vidéo et initiation de Conférence/transfert : sélectionnez pour démarrer une conférence.

Pour plus d'informations sur les appels vidéo, consultez le *Guide de l'utilisateur du téléphone IP Cisco série 8800 pour téléphone Cisco Unified Communications Manager* et la documentation relative à votre version particulière de Cisco Unified Communications Manager.

Comme les autres appareils, un téléphone IP Cisco doit être configuré et géré. Ces téléphones chiffrent et décodent les codes suivants :

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

Avertissement L'utilisation d'un téléphone cellulaire, portable ou GSM, ainsi que d'une radio bidirectionnelle à proximité immédiate d'un téléphone IP Cisco, peut engendrer des interférences. Pour obtenir plus d'informations, reportez-vous à la documentation du fabricant du périphérique produisant les interférences.

Les téléphones IP Cisco donnent accès aux fonctionnalités de téléphonie traditionnelles, comme le renvoi et le transfert d'appels, le rappel (bis), la numérotation rapide, la téléconférence et l'accès aux systèmes de messagerie vocale. Les téléphones IP Cisco offrent également diverses autres fonctionnalités.

Comme c'est le cas pour d'autres périphériques réseau, vous devez configurer les téléphones IP Cisco pour qu'ils puissent accéder à Cisco Unified Communications Manager et au reste du réseau IP. Si vous utilisez DHCP, vous aurez moins de paramètres à configurer sur le téléphone. Toutefois, si cela est nécessaire sur votre réseau, vous pouvez configurer manuellement des informations telles qu'une adresse IP, un serveur TFTP ou un masque de sous-réseau.

Les téléphones IP Cisco peuvent interagir avec d'autres services et périphériques de votre réseau IP afin d'améliorer certaines fonctionnalités. Par exemple, vous pouvez intégrer Cisco Unified Communications Manager à l'annuaire LDAP3 (Lightweight Directory Access Protocol 3) standard de l'entreprise, pour permettre aux utilisateurs de rechercher les informations de contact de leurs collègues directement sur leur téléphone IP. Vous pouvez également utiliser XML pour permettre aux utilisateurs d'accéder aux informations comme la météo, la bourse, la citation du jour et d'autres informations provenant du Web.

Enfin, comme le téléphone IP Cisco est un périphérique réseau, vous pouvez obtenir des informations d'état détaillées directement sur le téléphone. Ces informations pourront vous aider à résoudre les éventuels problèmes rencontrés par les utilisateurs sur leurs téléphones IP. Vous pouvez aussi obtenir des statistiques sur un appel en cours ou sur les versions des microprogrammes du téléphone.

Pour pouvoir fonctionner dans un réseau de téléphonie IP, le téléphone IP Cisco doit être connecté à un périphérique réseau, comme un commutateur Cisco Catalyst. Vous devez également enregistrer le téléphone IP Cisco auprès d'un système Cisco Unified Communications Manager avant de pouvoir passer et recevoir des appels.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Téléphone IP Cisco 8811

La section suivante décrit les attributs du Téléphone IP Cisco 8811.

IP Cisco 8811

Connectez votre téléphone au réseau de téléphonie IP de votre entreprise, comme illustré dans le diagramme suivant.

1	Port d’adaptateur secteur (48 V CC).	5	Connexion au port d'accès (10/100/1000 PC).
2	Alimentation CA vers CC (en option).	6	Port auxiliaire.
3	Prise murale CA (en option).	7	Raccordement du combiné.
4	Raccordement au port réseau (10/100/1000 SW). Compatible IEEE 802.3at.	8	Raccordement du casque analogique (en option).

Remarque Le Téléphone IP Cisco 8811 ne prend pas en charge un module d'extension de touches.

Téléphones IP Cisco 8841 et 8845

La section suivante décrit les attributs des téléphones IP Cisco 8841 et 8845.

Raccordement du téléphone

Connectez votre téléphone au réseau de téléphonie IP de votre entreprise, à l'aide du diagramme suivant.

1	Port d'adaptateur secteur (48 V CC).	5	Connexion au port d'accès (10/100/1000 PC).
2	Alimentation CA vers CC (en option).	6	Port auxiliaire.
3	Prise murale CA (en option).	7	Raccordement du combiné.
4	Raccordement au port réseau (10/100/1000 SW). Compatible IEEE 802.3at.	8	Raccordement du casque analogique (en option).

Remarque Les Téléphones IP Cisco 8841 et 8845 ne prennent pas en charge de module d'extension de touches.

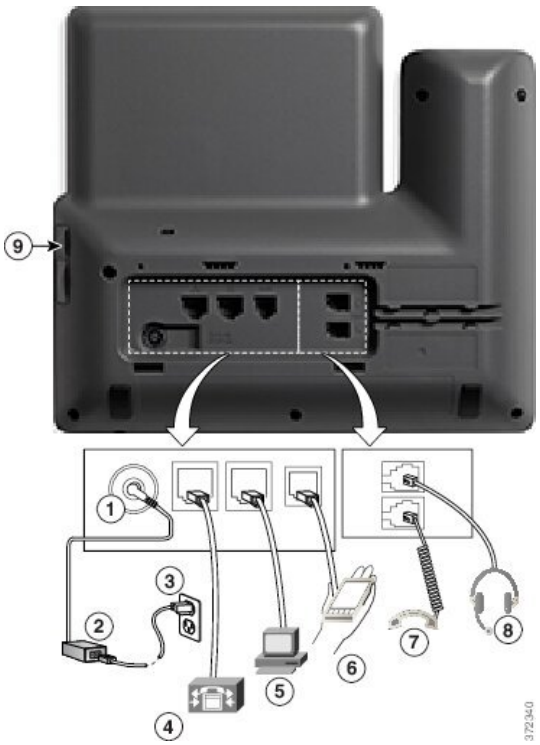
Téléphones IP Cisco 8851 et 8851NR

La section suivante décrit les attributs des téléphones IP Cisco 8851 et 8851NR.

Remarque Le téléphone IP Cisco 8851NR ne prend pas en charge Bluetooth. Sinon, les téléphones IP Cisco 8851 et 8851NR prennent en charge les mêmes fonctionnalités.

Raccordements du téléphone

Connectez votre téléphone au réseau de téléphonie IP de votre entreprise, comme illustré dans le diagramme suivant.



1	Port d'adaptateur secteur (48 V CC).	6	Port auxiliaire.
2	Alimentation CA vers CC (en option).	7	Raccordement du combiné.
3	Prise murale CA (en option).	8	Raccordement du casque analogique (en option).
4	Raccordement au port réseau (10/100/1000 SW). Compatible IEEE 802.3at.	9	Port USB
5	Connexion au port d'accès (10/100/1000 PC).		

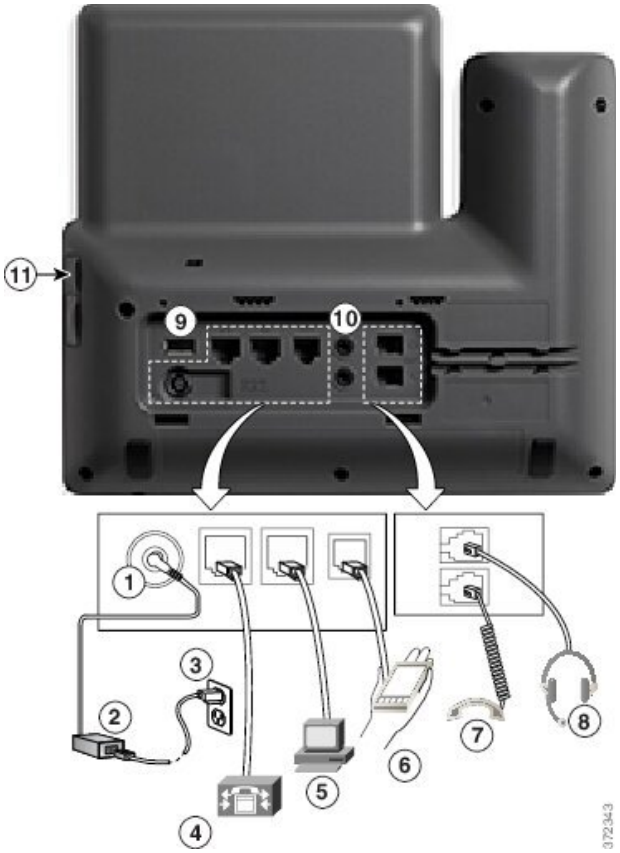
Remarque Chaque port USB prend en charge la connexion d'un maximum de cinq périphériques pris en charge et non pris en charge. Chaque périphérique connecté au téléphone est inclus dans le nombre maximum. Par exemple, votre téléphone peut prendre en charge cinq périphériques USB (par exemple, deux modules d'extension de touches , un casque, un concentrateur et un autre périphérique USB standard) sur le port latéral. Un grand nombre de produits USB tiers comptent comme plusieurs périphériques USB, par exemple, un périphérique contenant un concentrateur et un casque USB peuvent compter comme deux périphériques USB. Pour en savoir plus, reportez-vous à la documentation du périphérique USB.

Téléphones IP Cisco 8861, 8865 et 8865NR

La section suivante décrit les attributs des téléphones IP Cisco 8861, 8865 et 8865NR.

Raccordement du téléphone

Connectez votre téléphone au réseau de téléphonie IP de votre entreprise, comme illustré dans le diagramme suivant.



1	Port d'adaptateur secteur (48 V CC).	7	Raccordement du combiné.
2	Alimentation CA vers CC (en option).	8	Raccordement du casque analogique (en option).
3	Prise murale CA (en option).	9	Port USB
4	Raccordement au port réseau (10/100/1000 SW). Compatible IEEE 802.3at.	10	Ports audio d'entrée et de sortie
5	Connexion au port d'accès (10/100/1000 PC).	11	Port USB
6	Port auxiliaire.		

Remarque Chaque port USB prend en charge la connexion d'un maximum de cinq périphériques pris en charge et non pris en charge. Chaque périphérique connecté au téléphone est inclus dans le nombre maximum. Par exemple, votre téléphone peut prendre en charge cinq périphériques USB (tels que trois modules d'extension de touches , un concentrateur et un autre périphérique USB standard) sur le port latéral et cinq périphériques USB standard supplémentaires sur le port arrière. Un grand nombre de produits USB tiers comptent comme plusieurs périphériques USB, par exemple, un périphérique contenant un concentrateur et un casque USB peuvent compter comme deux périphériques USB. Pour en savoir plus, reportez-vous à la documentation du périphérique USB.

Boutons et matériel du

Les téléphones IP Cisco série 8800 sont équipés de deux types de matériel distincts :

- Les téléphones IP Cisco 8811, 8841, 8851, 8851NR et 8861 ne sont pas équipés de caméra.
- Les téléphones IP Cisco 8845, 8865 et 8865NR sont équipés d'une caméra intégrée.

La figure suivante illustre le téléphone IP Cisco 8845.

Illustration 1 : Boutons et matériel du téléphone IP Cisco 8845

Le tableau suivant décrit les boutons du téléphone IP Cisco série 8800.

Tableau 18 : Boutons du téléphone IP Cisco série 8800

1	Combiné et bande lumineuse du combiné	Indique si vous avez un appel entrant (rouge clignotant) ou un nouveau message vocal (rouge fixe).
2	Caméra Téléphone IP Cisco 8845, 8865 et 8865NR uniquement	Utilisez la caméra pour les appels vidéo.

3	Boutons de fonctions programmables et boutons de ligne	Accédez à vos lignes téléphoniques, fonctions et sessions d'appel. Lors de l'ajout des fonctionnalités aux touches de ligne téléphonique, vous êtes limité par le nombre de touches de ligne disponibles. Vous ne pouvez pas ajouter plus de fonctionnalités que le nombre de touches de ligne sur votre téléphone. Pour obtenir plus d'informations, reportez-vous à la section Touches programmables, lignes et boutons de fonctions du chapitre « Matériel du téléphone IP Cisco ».
4	Boutons de touches	Accédez aux fonctions et services. Pour obtenir plus d'informations, reportez-vous à la section Touches programmables, lignes et boutons de fonctions du chapitre « Matériel du téléphone IP Cisco ».
5	**Retour**, cluster de navigation et **Libérer**	**Retour** Pour revenir à l'écran ou au menu précédent. Cluster de navigation anneau de navigation et bouton **Select.** : pour naviguer entre les menus, mettre des éléments en surbrillance et sélectionner l'élément en surbrillance. **Libérer** Pour mettre fin à un appel ou à une session connectés.
6	**Attente/Reprise**, **Conférence** et **Transfert**	**Attente/Reprise** Pour mettre un appel actif en attente et reprendre l'appel en attente. **Conférence** Pour créer une conférence téléphonique. **Transfert** Pour transférer un appel.
7	**Haut-parleur**, **Muet** et **Casque**	**Haut-parleur** Pour activer ou désactiver le mode haut-parleur. Lorsque le mode haut-parleur est activé, le bouton est allumé. **Muet** Pour activer ou désactiver le microphone. Lorsque le son du microphone est coupé, le bouton est allumé. **Casque** Pour activer ou désactiver le casque. Lorsque le casque est en marche, le bouton est éclairé. Pour quitter le mode casque, vous décrochez le combiné ou sélectionnez **Haut-parleur** .

8	**Contacts**, **Applications** et **Messages**	**Contacts** Pour accéder aux répertoires personnel et d'entreprise. **Applications** Pour accéder aux appels récents, aux préférences utilisateur, aux paramètres du téléphone et aux informations sur le modèle de téléphone. **Messages** Pour appeler automatiquement votre système de messagerie vocale.
9	Bouton **Volume**	Réglez le volume du combiné, du casque et du haut-parleur (en mode décroché), ainsi que le volume de la sonnerie (en mode raccroché).

Touches programmables et boutons de ligne et de fonction

Plusieurs méthodes permettent d'interagir avec les fonctionnalités de votre téléphone :

- Les touches programmables, situées sous l'écran, permettent d'accéder aux fonctions affichées à l'écran au-dessus de ces dernières. Elles changent en fonction de votre activité du moment. La touche programmable **Plus...** indique que des fonctions supplémentaires sont disponibles.
- Les boutons de ligne et de fonction, situés des deux côtés de l'écran, permettent d'accéder aux fonctionnalités du téléphone et aux lignes téléphoniques.
  - Boutons de fonction : utilisés pour des fonctions telles que **Numérotation rapide** ou **Interception d'appels**, et pour afficher votre statut sur une autre ligne.
  - Boutons de ligne : pour prendre un appel ou reprendre un appel en attente. Lorsqu'ils ne sont pas utilisés pour un appel actif, ils permettent d'initier des fonctions téléphoniques, telles que l'affichage des appels en absence.

Les boutons de fonction et de ligne s'allument et leur couleur indique l'état de l'appel :

État et couleur du voyant	**Mode ligne normale : boutons de ligne**	**Mode ligne normale : boutons de fonction** **Mode ligne renforcée**
Voyant vert, fixe	Appel actif ou appel intercom bidirectionnel, appel en attente, confidentialité en cours d'utilisation	Appel actif ou appel intercom bidirectionnel, confidentialité en cours d'utilisation
Voyant vert, clignotant	Non applicable	appel en attente
Voyant orange, fixe	Appel entrant, reprise d'un appel, Intercom unidirectionnel, connecté à un groupe de recherche	Appel intercom unidirectionnel, connecté à un groupe de recherche
Voyant orange, clignotant	Non applicable	Appel entrant, appel récupéré

État et couleur du voyant	Mode ligne normale : boutons de ligne	Mode ligne normale : boutons de fonction Mode ligne renforcée
Voyant rouge, fixe	Ligne distante en cours d'utilisation, ligne distante en attente, fonctionnalité Ne pas déranger active	Ligne distante en cours d'utilisation, fonctionnalité Ne pas déranger active
Voyant rouge, clignotant	Non applicable	ligne distante en attente

Votre administrateur peut associer certaines fonctions à des touches programmables ou à des boutons de fonction. Vous pouvez aussi accéder à certaines fonctions au moyen des touches programmables ou des touches du clavier associées.

Protéger la caméra de votre téléphone vidéo

La caméra de votre téléphone vidéo est fragile et pourrait être endommagée pendant le transport du téléphone.

Avant de commencer

Vous devez disposer de l'un des éléments suivants :

- La boîte et le matériel d'emballage d'origine du téléphone
- Du matériel d'emballage, comme de la mousse ou du plastique à bulles

Procédure

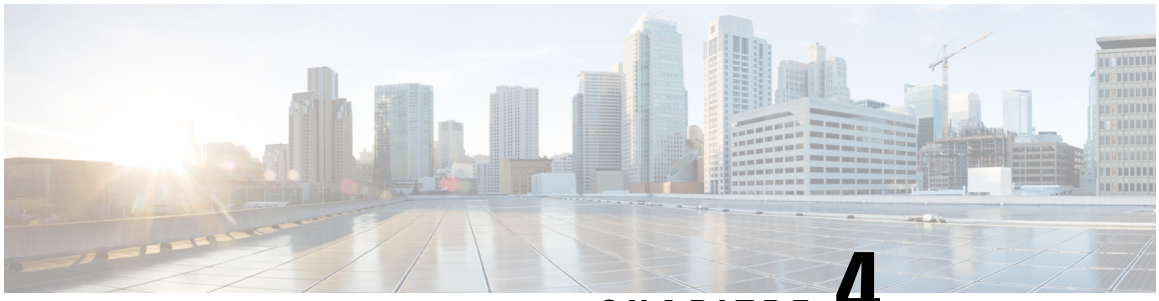
Étape 1 Si vous disposez de la boîte d'origine :

a) Mettez la mousse sur la caméra de façon que l'objectif soit bien protégé.
b) Placez le téléphone dans sa boîte d'origine.

Étape 2 Si vous ne disposez pas de la boîte, entourez soigneusement le téléphone avec de la mousse ou du plastique à bulles pour protéger la caméra. Assurez-vous que la mousse protège et entoure la caméra de manière à ce qu'il ne soit pas possible d'appuyer sur la caméra de n'importe quelle direction, sinon la caméra risque d'être endommagée au cours du transport.

SECTION II

Installation du téléphone IP Cisco



CHAPITRE 4

Installation du téléphone IP Cisco

Vérification de la configuration du réseau

Lorsqu'ils déploient un nouveau système de téléphonie IP, les administrateurs système et les administrateurs réseau doivent effectuer diverses tâches de configuration initiale, afin de préparer le réseau pour le service de téléphonie IP. Pour plus d'informations et une liste de contrôle pour la configuration et l'installation d'un réseau de téléphonie IP Cisco, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.

Pour que le téléphone fonctionne correctement sur le réseau, le réseau doit respecter certaines conditions. Une condition requise est la bande passante appropriée. Les téléphones nécessitent davantage de bande passante que les 32 kbit/s recommandés lorsqu'ils s'enregistrent auprès de Cisco Unified Communications Manager. Lorsque vous configurez votre bande passante de qualité de service, tenez compte de cette exigence de bande passante plus élevée. Pour plus d'informations, reportez-vous aux *Conceptions de réseau de référence de Solution Cisco Collaboration System 12.x (SRND)* ou version ultérieure (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.html).

Remarque Le téléphone affiche la date et l'heure de Cisco Unified Communications Manager. Il peut y avoir une différence d'un maximum de 10 secondes entre l'heure affichée sur le téléphone et l'heure de Cisco Unified Communications Manager.

Procédure

Étape 1 Configurez un réseau VoIP conforme aux exigences suivantes :

- La VoIP doit être configurée sur les routeurs et passerelles.
- Cisco Unified Communications Manager est installé sur le réseau et configuré pour le traitement des appels.

Étape 2 Configurez le réseau pour la prise en charge d'un des éléments suivants :

- Prise en charge du protocole DHCP
- Affectation manuelle d'une adresse IP, d'une passerelle et d'un masque de sous-réseau

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Intégration par code d'activation pour les téléphones sur site

Vous pouvez utiliser l'intégration par code d'activation pour configurer rapidement les nouveaux téléphones sans enregistrement automatique. Cette approche, vous permet de contrôler le processus d'intégration du téléphone à l'aide de l'une des actions suivantes :

- Outil d'administration en masse de Cisco Unified Communications Manager (BAT, Bulk Administration Tool)
- Interface de Cisco Unified Communications Manager Administration
- Service Web administratif XML (AXL)

Activez cette fonction à partir de la section **Informations sur le périphérique** de la page Configuration du téléphone. Sélectionnez **Code d'activation nécessaire pour l'intégration** si vous souhaitez que cette fonction s'applique à un téléphone unique sur site.

Les utilisateurs doivent saisir un code d'activation avant que leurs téléphones ne puissent être enregistrés. L'intégration par code d'activation peut être appliquée à des téléphones individuels, à un groupe de téléphones, ou sur l'ensemble du réseau.

Ceci est un moyen simple pour les utilisateurs d'intégrer leur téléphone, car ils n'ont besoin que de saisir un code d'activation à 16 chiffres. Les codes sont saisis manuellement ou à l'aide d'un code QR si le téléphone dispose d'une caméra vidéo. Nous vous recommandons d'utiliser une méthode sécurisée pour transmettre aux utilisateurs ces informations. Mais si un utilisateur est affecté à un téléphone, cette information est disponible sur le portail d'aide en libre-service (Self Care). Les enregistrements du journal d'audit lorsqu'un utilisateur accède au code à partir du portail.

Les codes d'activation ne peuvent être utilisés qu'une seule fois, et ils expirent au bout d'une semaine par défaut. Si un code expire, vous devrez en fournir un nouveau à l'utilisateur.

Vous constaterez que cette approche est un moyen simple de sécuriser votre réseau car un téléphone ne peut pas s'enregistrer tant que le certificat d'installation de fabrication (MIC, Manufacturing Installed Certificate) et le code d'activation ne sont pas vérifiés. Cette méthode est également un moyen pratique de traiter en masse

l'intégration des téléphones car elle n'utilise pas l'outil de prise en charge de téléphone enregistré automatiquement (TAPS) ou l'enregistrement automatique des téléphones intégrés. Le taux d'intégration est un téléphone par seconde ou sur le point 3600 téléphones par heure. Les téléphones peuvent être ajoutés à l'aide de Cisco Unified Communications Manager Administration, du Service Web administratif XML (AXL) ou avec l'outil d'administration en masse.

Les téléphones existants sont réinitialisés une fois qu'ils sont configurés pour l'intégration par code d'activation. Ils ne s'enregistrent pas jusqu'à ce que le code d'activation soit saisi et le MIC du téléphone soit vérifié. Informez les utilisateurs actuels que vous passez à l'intégration par code d'activation avant de la mettre en œuvre.

Pour plus d'informations, reportez-vous au *Guide d'Administration de Cisco Unified Communications Manager et service IM et Presence, version 12.0(1)* ou ultérieure.

Intégration par code d'activation et Mobile and Remote Access

Vous pouvez utiliser le code d'activation intégré à Mobile and Remote Access lorsque vous déployez des téléphones IP Cisco pour les utilisateurs distants. Cette fonctionnalité est un moyen sécurisé de déployer des téléphones hors site lorsque l'enregistrement automatique n'est pas nécessaire. Toutefois, vous pouvez configurer un téléphone pour l'enregistrement automatique en local, et des codes d'activation lorsque vous êtes hors site. Cette fonctionnalité est similaire à l'intégration par code d'activation pour les téléphones sur site, mais rend également le code d'activation disponible pour les téléphones hors site.

L'intégration par code d'activation pour Mobile and Remote Access (Accès mobile et distant) nécessite Cisco Unified Communications Manager 12.5 (1) SU1 ou version ultérieure et Cisco Expressway X 12.5 ou version ultérieure. Le gestionnaire de licences intelligent doit également être activé.

Vous pouvez activer cette fonctionnalité à partir de Cisco Unified Communications Manager Administration, mais tenez compte des points suivants :

- Activez cette fonction à partir de la section **Informations sur le périphérique** de la page Configuration du téléphone.
- Sélectionnez **Code d'activation nécessaire pour l'intégration** si vous souhaitez que cette fonction s'applique à un téléphone unique sur site.
- Sélectionnez **Autoriser le code d'activation** via MRA et **Exiger un code d'activation pour l'intégration** si vous souhaitez utiliser l'intégration par l'activation pour un seul téléphone hors-site. Si le téléphone est sur site, il passe en mode Mobile and Remote Access et utilise Expressway. Si le téléphone ne parvient pas à joindre Expressway, il n'est pas enregistré tant qu'il n'est pas hors site.

Pour obtenir plus d'informations, consultez les documents suivants :

- *Guide d'Administration de Cisco Unified Communications Manager et service IM et Presence, version 12.0(1).*
- *Mobile and Remote Access Through Cisco Expressway* pour Cisco Expressway X12.5 ou version ultérieure

Activation de l'enregistrement automatique des téléphones

Le téléphone IP Cisco requiert Cisco Unified Communications Manager pour gérer le traitement des appels. Consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager

ou l'aide contextuelle dans Cisco Unified Communications Manager Administration pour vérifier que Cisco Unified Communications Manager est correctement configuré afin de pouvoir gérer le téléphone ainsi qu'acheminer et traiter les appels comme il faut.

Avant d'installer le téléphone IP Cisco, vous devez choisir une méthode pour ajouter les téléphones à la base de données de Cisco Unified Communications Manager.

Si vous activez l'enregistrement automatique avant d'installer les téléphones, vous pourrez :

- Ajouter des téléphones sans collecter préalablement les adresses MAC des téléphones.
- Ajouter automatiquement un téléphone IP Cisco dans la base de données Cisco Unified Communications Manager lorsque vous connecterez physiquement le téléphone à votre réseau de téléphonie IP. Pendant l'enregistrement automatique, Cisco Unified Communications Manager attribue le prochain numéro de répertoire séquentiel disponible au téléphone.
- Ajouter rapidement des téléphones à la base de données de Cisco Unified Communications Manager et modifier n'importe quel paramètre, comme les numéros de répertoire, depuis Cisco Unified Communications Manager.
- Déplacer les téléphones enregistrés automatiquement vers de nouveaux emplacements et les affecter à différents pools de périphériques, sans aucune incidence sur leurs numéros de répertoire.

L'enregistrement automatique est désactivé par défaut. Dans certains cas, il est possible que vous ne souhaitiez pas utiliser l'enregistrement automatique ; par exemple, si vous voulez attribuer un numéro de répertoire particulier au téléphone ou si vous voulez utiliser une connexion sécurisée avec Cisco Unified Communications Manager. Pour plus d'informations sur l'activation de l'enregistrement automatique, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager. Lorsque vous configurez le cluster pour le mode mixte au moyen du client CTL de Cisco, l'enregistrement automatique est automatiquement désactivé, cependant vous pouvez l'activer. Lorsque vous configurez le cluster pour le mode non sécurisé au moyen du client CTL de Cisco, l'enregistrement automatique n'est pas automatiquement activé.

Vous pouvez ajouter des téléphones à l'aide de l'enregistrement automatique et de TAPS, l'outil de prise en charge des téléphones enregistrés automatiquement, sans collecter préalablement les adresses MAC des téléphones.

TAPS se sert de BAT (Bulk Administration Tool) pour mettre à jour un lot de téléphones ayant été ajoutés à la base de données de Cisco Unified Communications Manager avec des adresses MAC factices. Utilisez TAPS pour mettre à jour les adresses MAC et pour télécharger des configurations prédéfinies pour les téléphones.

Cisco vous recommande d'utiliser l'enregistrement automatique et TAPS pour ajouter moins de 100 téléphones à votre réseau. Pour ajouter plus de 100 téléphones à votre réseau, utilisez l'outil d'administration globale (BAT).

Pour mettre en application TAPS, l'utilisateur final ou vous-même devez composer un numéro de répertoire TAPS et suivre les invites vocales. Une fois que le processus est terminé, le téléphone contient le numéro de répertoire et d'autres paramètres, puis il est mis à jour dans Cisco Unified Communications Manager avec la bonne adresse MAC.

Vérifiez que l'enregistrement automatique est activé et correctement configuré dans Cisco Unified Communications Manager Administration avant de connecter un téléphone IP Cisco au réseau. Pour plus d'informations sur l'activation et la configuration de l'enregistrement automatique, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.

L'enregistrement automatique doit être activé dans Cisco Unified Communications Manager Administration pour que TAPS fonctionne.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, cliquez sur **Système** > **Cisco Unified CM**.

Étape 2 Cliquez sur **Trouver** et sélectionnez le serveur requis.

Étape 3 Dans **Informations d'auto enregistrement**, configurez ces champs.

- **Modèle de périphérique universel**
- **Modèle de ligne universel**
- **Premier numéro de répertoire**
- **Dernier numéro de répertoire**

Étape 4 Décochez la case **Enregistrement automatique désactivé sur Cisco Unified Communications Manager**.

Étape 5 Cliquez sur **Enregistrer**.

Étape 6 Cliquez sur **Appliquer la configuration**.

Installation d'un téléphone IP Cisco

Après s'être connecté au réseau, le téléphone entame le processus de démarrage et s'enregistre auprès de Cisco Unified Communications Manager. Pour terminer l'installation du téléphone, configurez les paramètres réseau du téléphone, selon que vous souhaitiez activer ou désactiver le service DHCP.

Si vous utilisez l'enregistrement automatique, vous devez mettre à jour les informations de configuration spécifiques au téléphone, notamment l'association du téléphone à un utilisateur, ou la modification du tableau de boutons ou du numéro de répertoire.

Remarque Avant d'utiliser des périphériques externes, veuillez lire la section Périphériques externes, à la page 26.

Pour plus d'informations sur l'installation d'accessoires, consultez le *Guide des accessoires des téléphones IP Cisco série 7800 et 8800 pour téléphone Cisco Unified Communications Manager*.

Si vous disposez d'un câble LAN à votre bureau, vous pouvez connecter votre téléphone au réseau local avec le port switch, puis connecter votre ordinateur au port PC. Pour obtenir plus d'informations, reportez-vous à Partager une connexion réseau avec votre téléphone et votre ordinateur, à la page 51.

Vous pouvez également connecter en série deux téléphones entre eux. Connectez le port PC du premier téléphone au port de commutation du deuxième téléphone.

Avertissement Ne pas connecter les ports de commutation et PC au LAN.

Procédure

Étape 1 Choisissez la source d'alimentation du téléphone :

- PoE (Power over Ethernet)
- Alimentation externe

Pour obtenir plus d'informations, reportez-vous à Conditions requises pour l'alimentation du téléphone, à la page 16.

Étape 2 Branchez le combiné sur le port du combiné et enfoncez le câble dans le canal du téléphone.

Le combiné compatible large bande est spécialement conçu pour être utilisé avec un téléphone IP Cisco. Le combiné inclut une bande lumineuse qui présente les appels entrants et les messages vocaux en attente.

Avertissement Si le câble n'est pas enfoncé dans le canal du téléphone, la carte de circuit imprimé peut être endommagée. Le canal du câble réduit la charge sur le connecteur et la carte de circuit imprimé.

Étape 3 Branchez un casque ou un casque sans fil. Vous pourrez toujours ajouter le casque ultérieurement.

Enfoncez le câble dans le chemin de câble.

Avertissement Si le câble n'est pas enfoncé dans le canal du téléphone, la carte de circuit imprimé à l'intérieur du téléphone peut être endommagée. Le canal du câble réduit la charge sur le connecteur et la carte de circuit imprimé.

Étape 4 Branchez un câble Ethernet droit entre le commutateur et le port réseau 10/100/1000 du téléphone IP Cisco. Chaque téléphone IP Cisco est livré avec un câble Ethernet.

Utilisez un câblage de catégorie 3, 5, 5e ou 6 pour les connexions de 10 Mbits/s, un câblage de catégorie 5, 5e ou 6 pour les connexions de 100 Mbits/s, et un câblage de catégorie 5e ou 6 pour les connexions de 1 000 Mbits/s. Pour plus d'informations, reportez-vous aux directives de la section Brochage des ports réseau et PC, à la page 14.

Étape 5 À l'aide d'un câble Ethernet droit, raccordez un autre périphérique réseau, tel qu'un ordinateur de bureau, au port PC du téléphone IP Cisco. Vous pourrez toujours connecter un périphérique réseau ultérieurement.

Utilisez un câblage de catégorie 3, 5, 5e ou 6 pour les connexions de 10 Mbits/s, un câblage de catégorie 5, 5e ou 6 pour les connexions de 100 Mbits/s, et un câblage de catégorie 5e ou 6 pour les connexions de 1 000 Mbits/s. Pour plus d'informations, reportez-vous aux directives de la section Brochage des ports réseau et PC, à la page 14.

Étape 6 Si le téléphone est posé sur un bureau, réglez le support. Dans le cas des téléphones muraux, vous devrez peut-être régler le support de combiné pour vous assurer que le combiné ne puisse pas glisser hors du téléphone.

Étape 7 Suivez le processus de démarrage du téléphone. Cette étape ajoute au téléphone les numéros de répertoire principaux et secondaires ainsi que les fonctionnalités associées et vérifie que le téléphone est correctement configuré.

Étape 8 Si vous configurez les paramètres réseau du téléphone, vous pouvez définir une adresse IP pour le téléphone, à l'aide de DHCP ou en saisissant manuellement l'adresse IP.

Reportez-vous à la section Configurer des paramètres réseau, à la page 61 et à la section Configuration réseau, à la page 245.

Étape 9 Mettez à niveau le téléphone en installant la plus récente image du micrologiciel.

Les mises à niveau de micrologiciel sur l'interface WLAN risquent de durer plus longtemps que les mises à niveau sur l'interface câblée, selon la qualité et la bande passante de la connexion sans fil. Certaines mises à niveau peuvent durer plus d'une heure.

Étape 10 Passez des appels sur le téléphone IP Cisco pour vérifier le bon fonctionnement du téléphone et de ses fonctionnalités.

Reportez-vous au *Guide de l'utilisateur des téléphones IP Cisco série 8800*.

Étape 11 Indiquez aux utilisateurs finals comment utiliser leurs téléphones et comment en configurer les options. Cette étape permet de garantir que les utilisateurs disposent des informations adéquates pour bien utiliser leur téléphone IP Cisco.

Partager une connexion réseau avec votre téléphone et votre ordinateur

Votre téléphone et votre ordinateur doivent être connectés à votre réseau pour fonctionner. Si vous ne disposez que d'un seul port Ethernet, vos périphériques peuvent partager la connexion réseau.

Avant de commencer

Votre administrateur doit activer le port PC dans Cisco Unified Communications Manager avant que vous ne puissiez l'utiliser.

Procédure

Étape 1 Branchez le port commutateur du téléphone au réseau local à l'aide d'un câble Ethernet.

Étape 2 Branchez votre ordinateur sur le port PC du téléphone à l'aide d'un câble Ethernet.

Configuration du téléphone depuis les menus de configuration

Le téléphone IP Cisco présente les menus de configuration suivants :

- Paramétrage réseau : donne accès aux options d'affichage et de configuration des paramètres réseau comme IPv4-uniquement, IPv6-uniquement, WLAN et Ethernet.
- Paramétrage Ethernet : les éléments de ce sous-menu donnent accès aux options de configuration du téléphone IP Cisco sur un réseau Ethernet.
- Configuration du client Wi-Fi : les éléments de ce sous-menu donnent accès aux options de configuration du téléphone IP Cisco avec un réseau WLAN (wireless local area network). La Wifi est prise en charge sur les téléphones IP Cisco 8861 et 8865 uniquement.

Remarque Le port PC du téléphone est désactivé lorsque le Wi-Fi est activé sur votre téléphone.

- Paramétrage IPv4 et Paramétrage IPv6 : ces sous-menus du menu Configuration Ethernet et du menu Configuration du client Wi-Fi donnent accès à des options réseau supplémentaires.
- Paramétrage de sécurité : donne accès aux options de consultation et de configuration des paramètres de sécurité comme le mode de sécurité, la liste sécurisée ou l'authentification 802.1x.

Avant de pouvoir modifier les paramètres des options du menu Paramétrage réseau, vous devez déverrouiller la modification des options.

Remarque Vous pouvez contrôler si un téléphone a accès au menu Paramètres ou aux options de ce menu en utilisant le champ Accès aux paramètres de la fenêtre Configuration du téléphone Cisco Unified Communications Manager Administration. Le champ Accès aux paramètres accepte les valeurs suivantes :

- Activé : permet l'accès au menu Paramètres.
- Désactivé : empêche l'accès au menu Paramètres.
- Restreint : permet l'accès au menu Préférences utilisateur et l'enregistrement des changements du volume. Empêche l'accès aux autres options du menu Paramètres.

Si vous ne pouvez pas accéder à une option du menu Paramètres administrateur, cochez la case Accès aux paramètres.

Procédure

Étape 1 Appuyez sur **Applications**.

Étape 2 Sélectionnez **Paramètres admin**.

Étape 3 Sélectionnez **Paramétrage réseau** ou **Paramétrage de sécurité**.

Étape 4 Saisissez votre identifiant utilisateur et votre mot de passe si nécessaire, puis cliquez sur **Connexion**.

Étape 5 Effectuez l'une des actions suivantes pour afficher le menu souhaité :

- Utilisez les flèches de navigation pour sélectionner le menu souhaité, puis appuyez sur **Sélect**.
- Utilisez le clavier du téléphone pour saisir le numéro qui correspond au menu.

Étape 6 Pour afficher un sous-menu, répétez l'étape 5.

Étape 7 Pour quitter un menu, appuyez sur **Quitter** ou sur la flèche Précédent.

Appliquer un mot de passe à un téléphone

Vous pouvez appliquer un mot de passe au téléphone. Si vous le faites, aucune modification ne peut être réalisée des options d'administration du téléphone sans saisie du mot de passe sur l'écran Paramètres Admin.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, naviguez jusqu'à la fenêtre Common Phone Profile Configuration (Configuration du profil de téléphone commun), en sélectionnant (**Périphérique** > **Paramètres du périphérique** > **Profil de téléphone commun**).

Étape 2 Saisissez un mot de passe dans la zone Local Phone Unlock Password (Mot de passe de déverrouillage du téléphone local).

Étape 3 Appliquez le mot de passe au profil de téléphone commun utilisé par le téléphone.

Saisie de texte et sélection de menus sur le téléphone

Pour modifier la valeur d'une option, procédez comme suit :

- Utilisez les flèches du pavé de navigation pour surligner le champ à modifier, puis appuyez sur **Sélect.** sur le pavé de navigation pour activer le champ. Une fois le champ activé, vous pouvez saisir des valeurs.
- Utilisez les touches du clavier pour saisir des chiffres et des lettres.
- Pour saisir des lettres à l'aide du clavier, utilisez la touche numérique correspondante. Appuyez sur celle-ci une ou plusieurs fois pour ajouter une lettre donnée. Par exemple, appuyez une fois sur la touche **2** pour « a, », deux fois plus rapidement pour « b, », et trois fois plus rapidement pour « c. ». Lorsque vous vous arrêtez, le curseur avance automatiquement pour vous permettre de saisir la lettre suivante.
- Appuyez sur la touche programmable flèche si vous avez fait une erreur. Cette touche de fonction efface le caractère situé à gauche du curseur.
- Appuyez sur **Annuler** avant d'appuyer sur **Enregistrer** pour abandonner les modifications que vous avez effectuées.
- Pour saisir une adresse IP, entrez les valeurs dans les quatre segments déjà séparés. Lorsque vous avez saisi les chiffres les plus à gauche avant le premier point, utilisez la touche flèche de droite pour passer au segment suivant. Le point suivant les chiffres les plus à gauche est inséré automatiquement.
- Pour saisir les deux points d'une adresse IPv6, appuyez sur la touche ***** du clavier.

Remarque Plusieurs méthodes sont disponibles sur le téléphone IP Cisco pour réinitialiser ou restaurer les paramètres, si nécessaire.

Rubriques connexes

Réinitialisation de base, à la page 281
Appliquer un mot de passe à un téléphone, à la page 52

Activer le réseau local sans fil sur le téléphone

Avant de configurer un LAN sans fil, vérifiez que votre téléphone prend en charge l'utilisation sans fil. Les Téléphones IP Cisco 8861 et 8865 prennent en charge un déploiement de LAN sans fil. Le téléphone IP Cisco 8865NR ne prend pas en charge l'utilisation d'un LAN sans fil.

Vérifiez que la couverture Wi-Fi de l'endroit où le réseau LAN sans fil est déployé convient à la transmission de paquets de voix.

Si vous avez activé la connectivité Wi-Fi pour la voix et que vous utilisez le mod de sécurité EAP-FAST ou PEAP, authentifiez le réseau Wi-Fi auprès de l'application de connexion WLAN. Les modes de sécurité WEP, PSK et Ouvert s'authentifient sur le réseau Wi-Fi.

Une méthode d'itinérance rapide sécurisée est recommandée pour les utilisateurs de la Wifi.

Remarque Le port PC du téléphone est désactivé lorsque le Wi-Fi est activé sur votre téléphone.

Pour la totalité des informations de configuration, reportez-vous au *Guide de déploiement d'un réseau WLAN pour téléphone IP Cisco Série 8800* disponible à l'URL suivante :

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

Le *Guide de déploiement d'un réseau WLAN pour téléphone IP Cisco Série 8800* contient les informations de configuration suivantes :

- Configuration du réseau sans fil
- Configuration du réseau sans fil dans Cisco Unified Communications Manager Administration
- Configuration du réseau sans fil sur le téléphone IP Cisco

Avant de commencer

Vérifiez que le Wi-Fi est activé sur le téléphone et que le câble Ethernet est déconnecté.

Procédure

Étape 1 Pour activer l'application, appuyez sur **Applications**.

Étape 2 Accédez à **Paramètres administrateur** > **Configuration réseau** > **Configuration du client Wi-Fi** > **Nom du réseau**.
Une liste des points d'accès sans fil auxquels vous pouvez vous connecter s'affiche.

Étape 3 Activez le Réseau sans fil.

Configurer le réseau LAN sans fil depuis Cisco Unified Communications Manager

Dans Cisco Unified Communications Manager Administration, vous devez activer un paramètre nommé « Wi-Fi » pour le téléphone IP Cisco sans fil.

Remarque Dans la fenêtre Configuration du téléphone de Cisco Unified Communications Manager Administration (**Périphérique** > **Téléphone**), utilisez l'adresse MAC de la ligne filaire lorsque vous configurez l'adresse MAC. L'enregistrement auprès de Cisco Unified Communications Manager n'utilise pas d'adresse MAC sans fil.

Effectuez la procédure suivante dans Cisco Unified Communications Manager Administration.

Procédure

Étape 1 Pour activer le réseau LAN sans fil sur un téléphone particulier, procédez comme suit :

a) Sélectionnez **Périphérique** > **Téléphone**.
b) Localisez le téléphone souhaité.
c) Sélectionnez le paramètre **Activé** pour le paramètre Wi-Fi dans la section Présentation de la configuration spécifique au produit.
d) Activez la case à cocher **Remplacer les paramètres communs.**.

Étape 2 Pour activer le réseau LAN sans fil sur un groupe de téléphones,

a) Sélectionnez **Périphérique** > **Paramètres du périphérique** > **Profil de téléphone commun**.
b) Sélectionnez le paramètre **Activé** pour le paramètre Wi-Fi.

Remarque Pour garantir le fonctionnement de la configuration de cette étape, décochez la case **Remplacer les paramètres communs** mentionnée à l'étape 1d.

c) Activez la case à cocher **Remplacer les paramètres communs.**.
d) Associez les téléphones à ce profil de téléphone commun en utilisant **Périphérique** > **Téléphone** .

Étape 3 Pour activer le réseau LAN sans fil sur tous les téléphones compatibles WLAN de votre réseau,

a) Sélectionnez **Système** > **Configuration des téléphones d'entreprise**.
b) Sélectionnez le paramètre **Activé** pour le paramètre Wi-Fi.

Remarque Pour garantir le fonctionnement de la configuration de cette étape, décochez la case **Remplacer les paramètres communs** mentionnée à l'étape 1d et à l'étape 2c.

c) Activez la case à cocher **Remplacer les paramètres communs.**.

Configuration d'un réseau LAN sans fil depuis le téléphone

Pour pouvoir connecter le téléphone IP Cisco à un réseau local sans fil, vous devez configurer le profil réseau du téléphone avec les paramètres WLAN appropriés. Vous pouvez utiliser le menu **Configuration du réseau** du téléphone pour accéder au sous-menu **Configuration du client Wi-Fi** et saisir ainsi les paramètres WLAN.

Remarque Le port PC du téléphone est désactivé lorsque le Wi-Fi est activé sur votre téléphone.

Remarque L'option **Configuration du client Wi-Fi** n'apparaît pas dans le menu **Configuration du réseau** lorsque le Wi-Fi est désactivé dans Cisco Unified Communications Manager.

Pour plus d'informations, consultez le *Guide de déploiement WLAN du téléphone IP Cisco* série 8800 à l'adresse : http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html.

Le champ **Modifiable par l'utilisateur** du profil LAN sans fil contrôle la possibilité pour l'utilisateur de configurer les modes de sécurité sur le téléphone. Lorsqu'un utilisateur ne peut pas modifier certains champs, les champs apparaissent grisés.

Avant de commencer

Configurer le LAN sans fil depuis Cisco Unified Communications Manager.

Procédure

Étape 1 Appuyez sur **Applications**.

Étape 2 Sélectionnez **Paramètres administrateur** > **Configuration réseau** > **Configuration du client Wi-Fi**.

Étape 3 Configurez le mode Sans fil comme décrit dans le tableau suivant.

Tableau 19 : Options du menu Configuration du client Wi-Fi

Option	Description	Pour modifier
Nom réseau	Spécifie le SSID (Service Set Identifier), un identifiant unique utilisé lors de la connexion aux points d'accès sans fil. Affiche une liste des points d'accès sans fil disponibles.	Reportez-vous à Configurer des paran réseau, à la page 61.

Option	Description	Pour modifier
Configuration IPv4 uniquement	Dans le sous-menu de configuration Paramétrage IPv4, vous pouvez effectuer les actions suivantes : • Activer ou désactiver l'utilisation par le téléphone de l'adresse IP attribuée par le serveur DHCP. • Saisir manuellement l'adresse IP, le masque de sous-réseau, les routeurs par défaut, le serveur DNS et les serveurs TFTP secondaires. Pour plus d'informations sur les champs d'adresse IPv4, reportez-vous à la section Champs IPv4, à la page 63.	Faites défiler la liste jusqu'à Param appuyez sur **Sélectionner**.
Paramétrage IPv6 uniquement	Dans le sous-menu Configuration IPv6, vous pouvez effectuer les actions suivantes : • Activer ou désactiver l'utilisation par le téléphone de l'adresse IPv6 attribuée par le serveur DHCPv6 ou obtenue via SLAAC depuis un routeur prenant en charge IPv6. • Saisir manuellement l'adresse IPv6, la longueur du préfixe, les routeurs par défaut, le serveur DNS et les serveurs TFTP secondaires. Pour plus d'informations sur les champs d'adresse IPv6, reportez-vous à la section Champs IPv6, à la page 65.	Faites défiler la liste jusqu'à Confi et appuyez sur **Sélectionner**.
Adresse MAC	L'adresse MAC (Media Access Control) unique du téléphone.	Affichage uniquement. Ne peut pa configuré.
Nom de domaine	Le nom du domaine DNS (Domain Name System) dans lequel le téléphone se situe.	Reportez-vous à Configurer des pa réseau, à la page 61.

Étape 4 Appuyez sur **Enregistrer** pour valider les modifications ou appuyez sur **Revenir** pour abandonner la connexion.

Définir le nombre de tentatives d'authentification de réseau local sans fil (WLAN)

Une demande d'authentification est une confirmation d'informations de connexion de l'utilisateur. Ceci se produit lorsqu'un téléphone qui a déjà joint un réseau Wi-Fi essaie de se reconnecter au serveur Wi-Fi. C'est le cas par exemple lorsqu'une session Wi-Fi expire ou qu'une connexion Wi-Fi est interrompue et puis établie à nouveau.

Vous pouvez configurer le nombre de fois qu'un téléphone Wi-Fi envoie une demande d'authentification sur le serveur Wi-Fi. Le nombre de tentatives par défaut est de 2, mais vous pouvez définir ce paramètre entre 1 et 3. Si un téléphone échoue l'authentification, l'utilisateur est invité à se reconnecter.

Vous pouvez appliquer le paramètre Tentatives d'authentification de WLAN à des téléphones individuels, à un ensemble de téléphones portables ou à tous les téléphones Wi-Fi de votre réseau.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone** et localisez le téléphone.

Étape 2 Naviguez jusqu'à la zone Configuration spécifique au produit et définissez le champ **Tentatives d'authentification au WLAN**.

Étape 3 Sélectionnez **Enregistrer**.

Étape 4 Sélectionnez **Appliquer la configuration**.

Étape 5 Redémarrez le téléphone.

Activer le Mode invite du réseau local sans fil

Activez le Mode d'invite de profil 1 de réseau local sans fil si vous souhaitez qu'un utilisateur se connecte au réseau Wi-Fi lorsque son téléphone se met en marche ou est réinitialisé.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone**.

Étape 2 Localisez le téléphone à configurer.

Étape 3 Accédez à la zone Configuration spécifique au produit et définissez le champ **Mode d'invite de profil 1 de réseau local sans fil** sur **Activer**.

Étape 4 Sélectionnez **Enregistrer**.

Étape 5 Sélectionnez **Appliquer la configuration**.

Étape 6 Redémarrez le téléphone.

Définir un profil Wifi à l'aide de Cisco Unified Communications Manager

Vous pouvez configurer un profil de réseau Wifi, puis affecter le profil aux téléphones qui prennent en charge la Wifi. Le profil contient les paramètres requis pour les téléphones pour se connecter à Cisco Unified Communications Manager en Wifi. Lorsque vous créez et que vous utilisez un profil de réseau Wifi, vos utilisateurs et vous n'avez pas besoin de configuration du réseau sans fil pour les téléphones individuels.

Les profils Wifi sont pris en charge par Cisco Unified Communications Manager version 10.5(2) ou ultérieure. Les protocoles EAP-FAST, PEAP-GTC et PEAP-MSCHAPv2 sont pris en charge par Cisco Unified Communications Manager version 10.0 et versions ultérieures. EAP-TLS est pris en charge par Cisco Unified Communications Manager 11.0 ou version ultérieure.

Un profil de réseau Wifi vous permet de prévenir ou de limiter les modifications apportées à la configuration du réseau Wifi sur le téléphone par l'utilisateur.

Nous vous recommandons d'utiliser un profil de sécurité avec le cryptage TFTP activé pour protéger les clés et les mots de passe lorsque vous utilisez un profil de réseau Wifi.

Lorsque vous configurez des téléphones pour qu'ils utilisent l'authentification EAP-FAST, PEAP-MSCHAPv2, ou PEAP-GTC, vos utilisateurs individuels ont besoin d'identifiants utilisateurs et de mots de passe individuels pour se connecter au téléphone.

Les téléphones ne prennent en charge qu'un seul certificat de serveur qui peut être installé soit avec SCEP, soit avec la méthode d'installation manuelle, mais pas par les deux méthodes. Les téléphones ne prennent pas en charge la méthode TFTP d'installation du certificat.

Remarque Les téléphones qui permettent de se connecter à Cisco Unified Communications Manager au moyen de Mobile and Remote Access through Expressway ne peuvent pas utiliser le profil réseau Wifi. Vous ne disposez pas du SSID, du mode d'authentification et des informations de connexion du téléphone de l'utilisateur, vous ne pouvez pas configurer de profil LAN sans fil pour leur téléphone.

Procédure

Étape 1 Dans Cisco Unified Communications Administration, sélectionnez **Périphérique** > **Paramètres du périphérique** > **Profil LAN sans fil**.

Étape 2 Cliquez sur **Ajouter nouveau**.

Étape 3 Dans la section **informations de profil de réseau local sans fil**, définissez les paramètres :

- **Nom** : entrez un nom unique pour le profil réseau Wifi. Ce nom s'affiche sur le téléphone.
- **Description** : entrez une description pour le profil réseau Wifi pour vous aider à différencier ce profil d'autres profils Wifi.
- **Modifiable par l'utilisateur** : sélectionnez une option :
  - **Autorisé** : indique que l'utilisateur peut modifier les paramètres Wifi à partir de son téléphone. Cette option n'est pas sélectionnée par défaut.
  - **Non autorisé** : indique que l'utilisateur ne peut pas modifier les paramètres Wifi à partir de son téléphone.
  - **Restreint** : indique que l'utilisateur peut modifier le nom d'utilisateur Wifi et le mot de passe sur son téléphone. Mais les utilisateurs ne sont pas autorisés à modifier les autres paramètres Wifi sur le téléphone.

Étape 4 Dans la section **Paramètres sans fil**, définissez les paramètres :

- **Identifiant SSID (nom de réseau)** : saisissez le nom de réseau disponible dans l'environnement de l'utilisateur auquel le téléphone peut être connecté. Ce nom s'affiche sous la liste des réseaux disponibles sur le téléphone et le téléphone peut se connecter à ce réseau sans fil.
- **Bande de fréquence** : les options disponibles sont Auto, 2,4 GHz et 5 GHz. Ce champ détermine la bande de fréquence qu'utilise la connexion sans fil. Si vous sélectionnez Auto, le téléphone tente d'utiliser d'abord la bande des 5 GHz et n'utilise la bande des 2,4 GHz que lorsque celle des 5 GHz n'est pas disponible.

Étape 5 Dans la section **Paramètres d'authentification**, définissez la **Méthode d'authentification** à l'une de ces méthodes d'authentification : EAP-FAST, EAP-TLS, PEAP-MSCHAPv2, PEAP-GTC, PSK, WEP et Aucune.

Après avoir défini ce champ, vous pouvez voir affichés de nouveaux champs que vous devez configurer.

- **Certificat utilisateur** : requis pour l'authentification EAP-TLS. Sélectionnez **installé en usine** ou **installé par l'utilisateur**. Le téléphone a besoin qu'un certificat soit installé, automatiquement à partir du SCEP ou manuellement à partir de la page d'administration du téléphone.
- **Phrase secrète PSK** : nécessaire pour l'authentification PSK. Saisissez 8 à 63 caractères ASCII ou une phrase secrète de 64 caractères hexadécimaux.
- **Clé WEP** : nécessaire pour l'authentification WEP. Saisissez une clé WEP hexadécimale ou au format ASCII 40/102 ou 64/128.
  - ASCII 40/104 comporte 5 caractères.
  - ASCII 64/128 comporte 13 caractères.
  - HEX 40/104 comporte 10 caractères.
  - HEX 64/128 comporte 26 caractères.
- **Fournir des informations de connexion partagée** : nécessaire pour l'authentification EAP-FAST, PEAP-MSCHAPv2 et PEAP-GTC.
  - Si l'utilisateur gère le nom d'utilisateur et le mot de passe, laissez les champs **nom d'utilisateur** et **mot de passe** vides.
  - Si tous les utilisateurs partagent le même nom d'utilisateur et même mot de passe, vous pouvez saisir ces informations dans les champs **nom d'utilisateur** et **mot de passe**.
  - Entrez une description dans le champ **Description du mot de passe**.

  Remarque Si vous devez attribuer un nom d'utilisateur et un mot de passe uniques à chaque utilisateur, vous devez créer un profil pour chaque utilisateur.

Remarque Le champ **profil d'accès au réseau** n'est pas pris en charge par les téléphones IP Cisco 8861 et 8865.

Étape 6 Cliquez sur **Enregistrer**.

Que faire ensuite

Appliquer le groupe de profil WLAN à un pool de périphériques (**Système** > **Pool de périphériques**) ou directement sur votre téléphone (**Périphérique** > **Téléphone**).

Définir un groupe Wifi à l'aide de Cisco Unified Communications Manager

Vous pouvez créer un groupe de profils LAN sans fil et ajouter un profil de LAN sans fil à ce groupe. Le groupe de profils peut ensuite affecté au téléphone lorsque vous configurez le téléphone.

Procédure

Étape 1 Dans Cisco Unified Communications Administration, sélectionnez **Périphérique** > **Paramètres du périphérique** > **Groupe de profils LAN sans fil**.

Vous pouvez également définir un groupe de profils LAN sans fil à partir de **Système** > **Pool de périphériques**.

Étape 2 Cliquez sur **Ajouter nouveau**.

Étape 3 Dans la section **Informations sur le groupe de profils LAN sans fil**, saisissez un nom de groupe et une description.

Étape 4 Dans la section **Profils pour ce groupe de profils LAN sans fil**, sélectionnez un profil disponible à partir de la liste **Profils disponibles** et déplacez le profil sélectionné vers la liste **Profils sélectionnés**.

Lorsque plus d'un profil de LAN sans fil est sélectionné, le téléphone utilise uniquement le premier profil de LAN sans fil.

Étape 5 Cliquez sur **Enregistrer**.

Configurer des paramètres réseau

Procédure

Étape 1 Appuyez sur **Applications** .

Étape 2 Pour accéder au menu Paramètres réseau, sélectionnez **Paramètres administrateur** > **Configuration Ethernet**.

Étape 3 Définissez les champs comme indiqué dans Champs de configuration Ethernet, à la page 61.

Étape 4 Une fois que vous avez défini les champs, sélectionnez **Appliquer** et **Enregistrer**.

Étape 5 Redémarre le téléphone.

Champs de configuration Ethernet

Le menu Configuration réseau contient les champs et sous-menus pour IPv4 et IPv6. Pour modifier certains champs, tout d'abord désactivez DHCP.

Lors de l'établissement d'une connexion VPN, les valeurs des champs de données Ethernet sont remplacées.

Tableau 20 : Options du menu Configuration Ethernet

Entrée	Type	Description
Paramétrage IPv4	Menu	Voir la section Champs IPv4. Cette option s'affiche seulement lorsque le téléphone est configuré en mode IPv4 et IPv6.
Paramétrage IPv6	Menu	Voir la section « Champs IPv6 ».

Entrée	Type	Description
Adresse MAC	Chaîne	L'adresse MAC (Media Access Control) unique du téléphone. Affichage uniquement. Ne peut pas être configuré.
Nom de domaine	Chaîne	Le nom du domaine DNS (Domain Name System) dans lequel le télépho Pour modifier ce champ, désactivez DHCP.
ID VLAN opérationnel		Le VLAN (Virtual Local Area Network) auxiliaire configuré sur un comm dont le téléphone fait partie. Ce paramètre reste vide si le VLAN auxiliaire ou le VLAN d'administrati Si le téléphone n'a pas reçu de VLAN auxiliaire, cette option indique le V Le téléphone n'hérite pas le VLAN opérationnel du VLAN Admin si le p Protocol ou Link Level Discovery Protocol Media Endpoint Discovery es Pour attribuer manuellement l'ID du VLAN, utilisez l'option ID VLAN a
ID VLAN admin.		VLAN auxiliaire dont le téléphone est membre. Utilisé seulement si le téléphone ne reçoit aucun VLAN auxiliaire de la pa cette valeur est ignorée.
VLAN PC		Permet au téléphone d'interagir avec les commutateurs tiers qui ne prenne voix. L'option ID VLAN admin doit être paramétrée pour pouvoir modifi
Paramétrage du port logiciel	Négociation auto 1000 Full 100 Half 10 Half 10 Full	Débit et duplex du port réseau. Les valeurs valides sont : • Négociation automatique (valeur par défaut) • 1000 Full :1000-BaseT/duplex intégral • 100 Half : 100-BaseT/semi duplex • 100 Full : 100-BaseT/duplex intégral • 10 Half : 10-BaseT/semi duplex • 10 Full : 10-BaseT/duplex intégral Si le téléphone est relié à un commutateur, configurez le port sur le comm que le téléphone, ou configurez les deux sur Négociation auto. Déverrouillez les options de configuration réseau si vous souhaitez modi modifiez le paramètre de cette option, vous devez effectuer les mêmes m Configuration port PC.

Entrée	Type	Description
Paramétrage port PC	Négociation auto 1000 Full 100 Half 10 Half 10 Full	Débit et duplex du port PC. Valeurs valides : • Négociation automatique (valeur par défaut) • 1000 Full : 1000-BaseT/duplex intégral • 100 Half : 100-BaseT/semi duplex • 100 Full : 100-BaseT/duplex intégral • 10 Half : 10-BaseT/semi duplex • 10 Full : 10-BaseT/duplex intégral Si le téléphone est relié à un commutateur, configurez le port sur le co que le téléphone, ou configurez les deux sur Négociation auto. Déverrouillez les options de configuration réseau si vous souhaitez m modifiez le paramètre de cette option, vous devez effectuer les même Configuration port commutation. Pour configurer simultanément le paramètre sur plusieurs téléphones, à à distance dans la fenêtre Configuration des téléphones d'entreprise (**S téléphones d'entreprise**). Si les ports sont configurés pour la Configuration des ports à distance Communications Manager, les données ne peuvent pas être modifiées

Champs IPv4

Tableau 21 : Options du menu Configuration IPv4

Entrée	Description
DHCP activé	Indique si DHCP est activé ou désactivé sur le téléphone. Si DHCP est activé, le serveur DHCP attribue une adresse IP au téléphone. Si DHCP est désactivé, l'administrateur doit attribuer manuellement une adresse IP au téléphone. Pour plus d'informations, reportez-vous à Configuration du téléphone pour l'utilisation de DHCP, à la page 67 et à Configuration du téléphone pour la non-utilisation de DHCP, à la page 67.
Adresse IP	Adresse de protocole Internet (IP) du téléphone. Si vous attribuez une adresse IP via cette option, vous devez également attribuer un masque de sous-réseau et un routeur par défaut. Reportez-vous aux options Masque de sous-réseau et Routeur par défaut de ce tableau.
Masque de sous-réseau	Le masque de sous-réseau utilisé par le téléphone.
Routeur par défaut	Le routeur par défaut utilisé par le téléphone.
Serveur DNS 1 Serveur DNS 2 Serveur DNS 3	Le serveur de noms de domaine (DNS) (Serveur DNS 1) et les serveurs DNS secondaires facultatifs (Serveurs DNS 2 et 3) utilisés par le téléphone.

Entrée	Description
TFTP secondaire	Indique si le téléphone utilise un serveur TFTP secondaire.
Serveur TFTP 1	Le serveur TFTP (Trivial File Transfer Protocol) principal utilisé par le téléphone. Si vous n'utilisez pas DHCP dans votre réseau et que vous souhaitez modifier ce serveur, vous devez utiliser l'option Serveur TFTP 1. Si vous paramétrez l'option TFTP secondaire sur Activé, vous devez saisir une valeur différente de zéro pour l'option Serveur TFTP 1. Si le serveur TFTP principal et le serveur TFTP secondaire ne figurent pas dans le fichier CTL ou ITL du téléphone, vous devez déverrouiller le fichier pour pouvoir enregistrer les modifications apportées à l'option Serveur TFTP 1. Dans ce cas, le téléphone supprime le fichier lorsque vous enregistrez les modifications apportées à l'option Serveur TFTP 1. Un nouveau fichier CTL ou ITL est ensuite téléchargé depuis la nouvelle adresse du Serveur TFTP 1. Lorsque le téléphone recherche le serveur TFTP, il donne priorité aux serveurs TFTP attribués manuellement, quel que soit le protocole utilisé. Si votre configuration comporte à la fois des serveurs TFTP IPv4 et IPv6, le téléphone hiérarchise la recherche de serveur TFTP en donnant priorité aux serveurs TFTP IPv6 et aux serveurs TFTP IPv4 attribués manuellement. Le téléphone recherche un serveur TFTP dans l'ordre suivant : **1.** Les serveurs TFTP IPv4 attribués manuellement **2.** Tout serveur IPv6 attribué manuellement **3.** Les serveurs TFTP attribués par DHCP **4.** Les serveurs TFTP attribués par DHCPv6 **Remarque** Pour plus d'informations sur les fichiers CTL et ITL, consultez le *Guide de sécurité pour Cisco Unified Communications Manager*.

Entrée	Description
Serveur TFTP 2	Le serveur TFTP secondaire facultatif utilisé par le téléphone si le serveur TFTP principal n'est pas disponible. Si le serveur TFTP principal et le serveur TFTP secondaire ne figurent pas dans le fichier CTL ou ITL du téléphone, vous devez déverrouiller le fichier pour pouvoir enregistrer les modifications apportées à l'option Serveur TFTP 2. Dans ce cas, le téléphone supprime l'un des deux fichiers lorsque vous enregistrez les modifications apportées à l'option Serveur TFTP 2. Un nouveau fichier CTL ou ITL est ensuite téléchargé depuis la nouvelle adresse du Serveur TFTP 2. Si vous avez oublié de déverrouiller le fichier CTL ou ITL, vous pouvez modifier l'adresse du Serveur TFTP 2 dans l'un des deux fichiers, puis les effacer en appuyant sur Effacer dans le menu Configuration de la sécurité. Un nouveau fichier CTL ou ITL est ensuite téléchargé depuis la nouvelle adresse du Serveur TFTP 2. Lorsque le téléphone recherche le serveur TFTP, il donne priorité aux serveurs TFTP attribués manuellement, quel que soit le protocole utilisé. Si votre configuration comporte à la fois des serveurs TFTP IPv4 et IPv6, le téléphone hiérarchise la recherche de serveur TFTP en donnant priorité aux serveurs TFTP IPv6 et aux serveurs TFTP IPv4 attribués manuellement. Le téléphone recherche un serveur TFTP dans l'ordre suivant : **1.** Les serveurs TFTP IPv4 attribués manuellement **2.** Tout serveur IPv6 attribué manuellement **3.** Les serveurs TFTP attribués par DHCP **4.** Les serveurs TFTP attribués par DHCPv6 **Remarque** Pour plus d'informations sur le fichier CTL ou ITL, consultez le Guide de sécurité pour téléphone Cisco Unified Communications Manager.
Serveur BOOTP	Indique si le téléphone a reçu l'adresse IP depuis un serveur BOOTP plutôt que depuis un serveur DHCP.
Libération adresse DHCP	Libère l'adresse IP attribuée par DHCP. Ce champ est modifiable si DHCP est activé. Si vous souhaitez retirer le téléphone du réseau VLAN et libérer l'adresse IP pour la ré-attribuer, configurez cette option sur Oui et appuyez sur Appliquer.

Champs IPv6

Avant de paramétrer les options de configuration IPv6 sur votre périphérique, vous devez activer et configurer IPv6 dans Cisco Unified Communication Administration. Les champs de configuration de périphérique suivants s'appliquent lors de la configuration IPv6 :

- Mode d'adressage IP
- Préférence du mode d'adressage IP pour le signalement

Si IPv6 est activé dans le cluster Unified, le paramètre par défaut pour le mode d'adressage IP est IPv4 et IPv6. Dans ce mode d'adressage, le téléphone obtient et utilise une adresse IPv4 et une adresse IPv6. Il peut

utiliser les adresses IPv4 et IPv6 selon les exigences des supports. Le téléphone utilise soit l'adresse IPv4 soit l'adresse IPv6 pour le signalement du contrôle des appels.

Pour plus d'informations sur le déploiement d'IPv6, reportez-vous au Guide de déploiement IPv6 de Cisco Collaboration systèmes version 12.0.

La configuration IPv6 s'effectue à partir des menus suivants :

- Lorsque le Wifi est désactivé : **Configuration Ethernet** > **Configuration IPv6**
- Lorsque le Wifi est activé : **Configuration du client Wi-Fi** > **Configuration IPv6**

Utilisez le clavier du téléphone pour saisir ou modifier une adresse IPv6. Pour saisir deux-points (:), appuyez sur l'astérisque (*) de votre clavier. Pour saisir les chiffres hexadécimaux a, b et c, appuyez sur la touche 2 de votre clavier, faites dérouler le menu pour sélectionner le chiffre souhaité, puis appuyez sur **Entrée**. Pour saisir les chiffres hexadécimaux d, e et f, appuyez sur la touche 3 de votre clavier, faites dérouler le menu pour sélectionner le chiffre souhaité, puis appuyez sur **Entrée**.

Le tableau suivant décrit les informations IPv6 uniquement consultables dans le menu IPv6.

Tableau 22 : Options du menu Configuration IPv6

Entrée	Valeur par défaut	Description
DHCPv6 activé	Oui	Indique la méthode utilisée par le télép Lorsque DCHPv6 est activé, le télépho par le routeur compatible IPv6. Si DHC DHCPv6) ou sans état (via SLAAC).
Adresse IPv6	::	Affiche l'adresse IPv6 uniquement actu Une adresse IPv6 valide présente une l sont pris en charge : • Huit groupes de quatre chiffres he • Format compressé pour réduire ur deux-points double. Si l'adresse IP est attribuée grâce à cett routeur par défaut.
Longueur du préfixe IPv6	0	Affiche la longueur de préfixe actuelle préfixe. La longueur du préfixe de sous-réseau
Routeur IPv6 par défaut	::	Affiche le routeur par défaut utilisé par l par défaut.
Serveur IPv6 DNS 1	::	Affiche le serveur DNSv6 principal uti
Serveur IPv6 DNS 2	::	Affiche le serveur DNSv6 secondaire ut secondaire.
Autre TFTP IPv6	Non	Permet à l'utilisateur de définir l'utilisa

Entrée	Valeur par défaut	Description
Serveur TFTP IPv6 1	::	Affiche le serveur TFTP IPv6 princ TFTP principal.
Serveur TFTP IPv6 2	::	(Optionnel) Affiche le serveur TFT permet à l'utilisateur de saisir un no
Adresse IPv6 libérée	Non	Permet à l'utilisateur de libérer les i

Configuration du téléphone pour l'utilisation de DHCP

Pour activer DHCP et autoriser le serveur DHCP à attribuer automatiquement une adresse IP au téléphone IP Cisco et diriger le téléphone vers un serveur TFTP, procédez comme suit :

Procédure

Étape 1 Appuyez sur **Applications** .

Étape 2 Choisissez **Paramètres Admin** > **Configuration réseau** > **Configuration Ethernet** > **Paramétrage IPv4**.

Étape 3 Pour activer DHCP, définissez DHCP activé sur **Oui**. Le protocole DHCP est activé par défaut.

Étape 4 Pour utiliser un serveur TFTP secondaire, définissez le serveur TFTP secondaire sur **Oui**, puis saisissez l'adresse IP pour le serveur TFTP.

Remarque Rapprochez-vous de l'administrateur réseau pour déterminer si vous devez attribuer un serveur TFTP secondaire plutôt qu'utiliser le serveur TFTP que DHCP attribue.

Étape 5 Appuyez sur **Appliquer**.

Configuration du téléphone pour la non-utilisation de DHCP

Lorsque vous n'utilisez pas DHCP, vous devez configurer localement sur le téléphone l'adresse IP, le masque de sous-réseau, le serveur TFTP et le routeur par défaut.

Procédure

Étape 1 Appuyez sur **Applications** .

Étape 2 Choisissez **Paramètres Admin** > **Configuration réseau** > **Configuration Ethernet** > **Paramétrage IPv4**.

Étape 3 Pour désactiver DHCP et définir manuellement une adresse IP :

a) Définissez DHCP activé sur **Non**.
b) Saisissez l'adresse IP statique du téléphone.
c) Saisissez le masque de sous-réseau.
d) Saisissez les adresses IP du routeur par défaut.
e) Définissez le serveur TFTP secondaire sur **Oui**, puis saisissez l'adresse IP pour le serveur TFTP 1.

Étape 4 Appuyez sur **Appliquer**.

Serveur de chargement

Le Serveur de chargement est utilisé pour optimiser la durée d'installation des mises à niveau des micrologiciels téléphoniques et décharger le WAN en stockant des images localement, ce qui annule la nécessité de traverser le lien WAN pour chaque mise à niveau.

Vous pouvez définir le Serveur de chargement sur un autre nom ou une autre Adresse IP du serveur TFTP (autre que Serveur TFTP 1 ou Serveur TFTP 2) à partir duquel le micrologiciel du téléphone peut être récupéré pour les mises à niveau. Lorsque l'option Serveur de chargement est définie, le téléphone contacte le serveur désigné pour la mise à niveau des micrologiciels.

Remarque Une option Serveur de chargement vous permet de spécifier un serveur TFTP secondaire pour les mises à niveau de téléphone uniquement. Le téléphone continue d'utiliser Serveur TFTP 1 ou Serveur TFTP 2 pour obtenir les fichiers de configuration. L'option Serveur de chargement ne permet pas la gestion du processus et des fichiers, comme le transfert de fichiers, leur compression ou leur suppression.

Le Serveur de chargement est configuré depuis la fenêtre Configuration des téléphones d'entreprise. Dans Cisco Unified Communications Manager Administration, choisissez **Périphérique** > **Téléphone** >**Configuration des téléphones d'entreprise**.

Vérification du démarrage du téléphone

Une fois que le téléphone IP Cisco est branché, il commence son processus de diagnostic de démarrage en passant par les étapes suivantes.

1. Les boutons Fonction et Session clignotent l'un après l'autre en orange et vert pendant les différentes phases de démarrage à mesure que le téléphone vérifie le matériel.
2. L'écran principal affiche `Enregistrement auprès de Cisco Unified Communications Manager`.

Si le téléphone passe correctement ces stades, il a démarré correctement et le bouton **Sélectionner** reste allumé jusqu'à ce qu'il soit sélectionné.

Configurer les services téléphoniques pour les utilisateurs

Pour pouvez permettre aux utilisateurs d’accéder aux services de téléphonie IP Cisco sur le téléphone IP. Vous pouvez également affecter un bouton à différents services téléphoniques. Ces services incluent des applications XML et des MIDlets Java signés par Cisco qui permettent l'affichage de contenu interactif avec texte et images sur le téléphone. Le téléphone IP gère chaque service comme une application distincte. Ces services incluent par exemple les horaires des cinémas locaux, les cours de la bourse et les bulletins météo.

Pour qu’un utilisateur puisse accéder à un service :

- Vous devez utiliser Cisco Unified Communications Manager Administration pour configurer les services qui ne sont pas présents par défaut.
- L'utilisateur doit s'abonner aux services à l'aide de Portail d'aide en libre-service pour Cisco Unified Communications. Cette application Web fournit une interface utilisateur graphique pour la configuration limitée des applications de téléphonie IP par l'utilisateur final. Les utilisateurs ne peuvent cependant pas s'abonner aux services que vous configurez pour l'abonnement d'entreprise.

Pour obtenir plus d'informations, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Avant de configurer des services, obtenez les URL des sites à configurer et vérifiez que les utilisateurs peuvent accéder à ces sites sur le réseau de téléphonie IP de votre entreprise. Cette action ne s'applique pas pour les services par défaut fournis par Cisco.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Paramètres du périphérique** > **Services téléphoniques**

Étape 2 Vérifiez que les utilisateurs peuvent accéder au Portail d'aide en libre-service pour Cisco Unified Communications, où ils pourront sélectionner les services configurés et s'y abonner.

Reportez-vous à Gestion du portail d'aide en libre-service, à la page 85 pour obtenir un récapitulatif des informations que vous devez mettre à la disposition des utilisateurs finals.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Modifier le modèle de téléphone d'un utilisateur

Votre utilisateur ou vous-même pouvez modifier le modèle de téléphone d'un utilisateur. La modification peut être requise pour plusieurs raisons, par exemple :

- Vous avez mis à jour votre Cisco Unified Communications Manager (Unified CM) vers une version logicielle qui ne prend pas en charge le modèle de téléphone.
- L'utilisateur souhaite obtenir un autre modèle de téléphone que son modèle actuel.
- Le téléphone nécessite une réparation ou un remplacement.

Unified CM identifie l'ancien téléphone et utilise l'adresse MAC de l'ancien téléphone pour identifier la configuration de ce dernier. Unified CM copie la configuration de l'ancien téléphone dans la configuration du nouveau téléphone. La configuration du nouveau téléphone est de ce fait identique à celle de l'ancien téléphone.

Si vous remplacez un ancien téléphone disposant du micrologiciel SCCP par un modèle de Téléphone IP Cisco série 8800, le nouveau téléphone est configuré pour le mode ligne de session.

Si un modèle d'extension de touches est configuré pour l'ancien téléphone, Unified CM copie les informations du module d'extension en même temps sur le nouveau téléphone. Lorsque l'utilisateur connecte un module d'extension de touches compatible avec le nouveau téléphone, le nouveau module d'extension reçoit les informations de module d'extension migrées.

Si l'ancien téléphone a un modèle d'extension de touches configuré et que le nouveau téléphone ne prend pas en charge de module d'extension, Unified CM ne copie pas les informations du module d'extension.

Limitation : si l'ancien téléphone a plus de lignes ou de boutons de ligne que le nouveau téléphone, le nouveau téléphone ne dispose pas des lignes supplémentaires ou de boutons de ligne configurés.

Le téléphone redémarre une fois la configuration terminée.

Avant de commencer

Configurez votre Cisco Unified Communications Manager conformément aux instructions du *Guide de Configuration des fonctionnalités de Cisco Unified Communications Manager*.

Vous devez disposer d'un téléphone neuf, inutilisé qui est préinstallé avec le micrologiciel version 12.8 (1) ou ultérieure.

Procédure

Étape 1 Mettez l'ancien téléphone hors tension.

Étape 2 Allumez le nouveau téléphone.

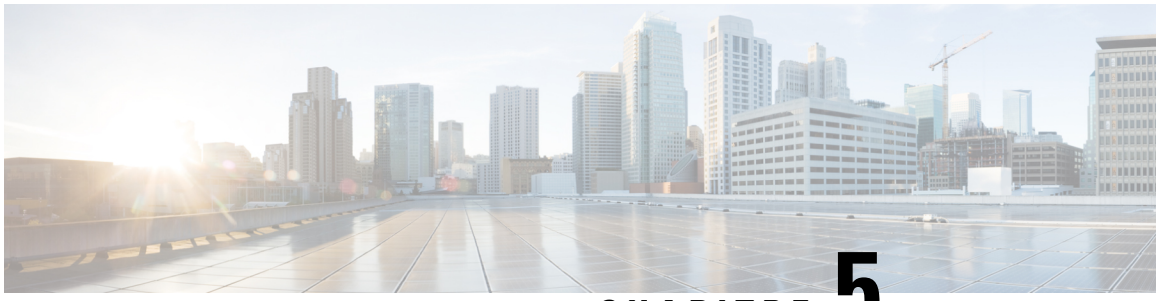
Étape 3 Sur le nouveau téléphone, sélectionnez **Remplacer un téléphone existant**.

Étape 4 Saisissez le numéro de poste principal de l'ancien téléphone.

Étape 5 Si l'ancien téléphone a un code PIN affecté, saisissez-le.

Étape 6 Appuyez sur **Envoyer**.

Étape 7 S'il y a plus d'un périphérique pour l'utilisateur, sélectionnez le périphérique à remplacer, puis appuyez sur **Continuer** .



CHAPITRE 5

Configuration d'un téléphone Cisco Unified Communications Manager

Configuration du téléphone IP Cisco

Si l'enregistrement automatique n'est pas activé et que le téléphone n'est pas enregistré dans la base de données de Cisco Unified Communications Manager, vous devez configurer le téléphone IP Cisco manuellement dans Cisco Unified Communications Manager. Certaines étapes de cette procédure sont facultatives, selon la configuration de votre système et les besoins des utilisateurs.

Pour plus d'informations sur Cisco Unified Communications Manager Administration, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.

Effectuez les étapes de la procédure de configuration suivante dans Cisco Unified Communications Manager Administration.

Procédure

Étape 1 Recueillez les informations suivantes sur le téléphone :

- Le modèle du téléphone
- Adresse MAC
- L'emplacement physique du téléphone
- Le nom ou l'ID utilisateur de l'utilisateur du téléphone

- Le pool de périphériques
- La partition, l'espace de restriction d'appels et les informations sur le site
- Nombre de lignes et numéros de répertoire (DN) associés à attribuer au téléphone
- Utilisateur Cisco Unified Communications Manager à associer au téléphone.
- Informations sur l'utilisation du téléphone influant sur le modèle de bouton de téléphone, les fonctionnalités du téléphone, les services téléphone IP ou les applications du téléphone

Ces informations fournissent une liste de pré-requis à la configuration des téléphones et identifient la configuration préliminaire à effectuer avant de configurer les téléphones individuellement, comme les modèles de bouton de téléphone.

Étape 2 Vérifiez que vous disposez de suffisamment de licences par unité pour votre téléphone.

Étape 3 Personnalisez le modèle de bouton de téléphone (si nécessaire) en modifiant le nombre de boutons de ligne, de numérotation rapide ou d'URL de service. Sélectionnez **Périphérique** > **Paramètres du périphérique** > **Modèle de bouton de téléphone** pour créer et mettre à jour les modèles.

Vous pouvez ajouter un bouton Confidentialité, Tous les appels ou Mobilité suivant les besoins de l'utilisateur.

Pour obtenir plus d'informations, reportez-vous à Modèles de boutons de téléphone, à la page 202.

Étape 4 Définissez les pools de périphériques. Sélectionnez **Système** > **Pool de périphériques**.

Les pools de périphériques définissent des caractéristiques communes à des périphériques, notamment la région, le groupe date/heure, le modèle de touches programmables et les informations MLPP.

Étape 5 Définissez le profil de téléphone commun. Sélectionnez **Périphérique** > **Paramètres du périphérique** > **Profil de téléphone commun**.

Les profils de téléphone communs fournissent des données nécessaires au serveur Cisco TFTP, et des paramètres de téléphone communs, notamment la fonctionnalité Ne pas déranger et les options de contrôle des fonctionnalités.

Étape 6 Définissez un espace de restriction d'appels. Dans Cisco Unified Communications Manager Administration, cliquez sur **Routage d'appels** > **Classe de contrôle** > **Espace de restriction d'appels**.

Les espaces de restriction d'appels sont un groupe de partitions dans lesquelles une recherche est effectuée pour déterminé comment acheminer un appel composé. L'espace de restriction d'appels du périphérique et l'espace de restriction d'appels du numéro de répertoire sont utilisés ensemble. L'espace de restriction d'appels du numéro de répertoire est prioritaire sur celui du périphérique.

Étape 7 Configurez un profil de sécurité pour le protocole et le type du périphérique. Sélectionnez **Système** > **Sécurité** > **Profil de sécurité du téléphone**.

Étape 8 Ajoutez et configurez le téléphone en remplissant les champs nécessaires dans la fenêtre Configuration du téléphone. Un astérisque (*) à côté du nom d'un champ indique que ce champ est nécessaire (par exemple, adresse MAC et Pool de périphériques).

Cette étape ajoute le périphérique avec les paramètres par défaut à la base de données de Cisco Unified Communications Manager.

Pour plus d'informations sur les champs de configuration propres à un produit, reportez-vous au « ? » Aide de la fenêtre de configuration du téléphone.

Remarque Pour savoir comment ajouter simultanément le téléphone et l'utilisateur dans la base de données Cisco Unified Communications Manager, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Étape 9 Ajoutez et configurez les numéros de répertoire (lignes) sur le téléphone en remplissant les champs requis dans la fenêtre Configuration du numéro de répertoire. Un astérisque (*) à côté du nom d'un champ indique que ce champ est nécessaire (par exemple, numéro de répertoire et le groupe de présence).

Cette étape ajoute au téléphone des numéros de répertoire principaux et secondaires ainsi que des fonctions associées à ces numéros.

Remarque Si vous ne configurez pas le numéro de répertoire principal, le message `Non déployé` s'affichera sur le téléphone.

Étape 10 Configurez les boutons de numérotation abrégée et affectez des numéros abrégés.

Les utilisateurs peuvent modifier les paramètres de numérotation rapide sur leurs téléphones en utilisant le Portail d'aide en libre-service pour téléphone Cisco Unified Communications.

Étape 11 Configurez les services pour téléphone IP Cisco Unified et affectez des services (optionnel) pour assurer les services téléphone IP.

Les utilisateurs peuvent ajouter ou modifier les services sur les téléphones en utilisant le Portail d'aide en libre-service pour téléphone Cisco Unified Communications.

Remarque Les utilisateurs peuvent s'abonner au service téléphone IP seulement si la case Abonnement entreprise n'est pas cochée lors de la première configuration du service téléphone IP dans Cisco Unified Communications Manager Administration.

Remarque Certains services par défaut, assurés par Cisco, sont classés comme abonnements d'entreprise. L'utilisateur ne peut donc pas les ajouter via le Portail d'aide en libre-service. Ces services se trouvent sur le téléphone par défaut et peuvent être supprimés du téléphone uniquement si vous les désactivez depuis Cisco Unified Communications Manager Administration.

Étape 12 Attribuez des services aux boutons programmables (optionnel) pour permettre l'accès à un service téléphone IP ou à une URL.

Étape 13 Ajoutez les informations de l'utilisateur en remplissant les champs requis. Un astérisque (*) en regard du nom du champ signale un champ obligatoire ; par exemple, l'ID de l'utilisateur et le nom de famille. Cette étape permet d'ajouter des informations sur l'utilisateur au répertoire global de Cisco Unified Communications Manager.

Remarque Attribuez un mot de passe (pour le Portail d'aide en libre-service) et un code PIN (pour téléphone Cisco Extension Mobility et le Répertoire personnel).

Remarque Si votre entreprise utilise un répertoire LDAP (Lightweight Directory Access Protocol) pour stocker les informations concernant les utilisateurs, vous pouvez installer et configurer Cisco Unified Communications de manière à ce qu'il utilise votre répertoire LDAP existant.

Remarque Pour savoir comment ajouter simultanément le téléphone et l'utilisateur dans la base de données Cisco Unified Communications Manager, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Étape 14 Associez un utilisateur à un groupe d'utilisateurs. Cette étape attribue aux utilisateurs une liste commune des rôles et des autorisations qui s'appliquent à tous les utilisateurs d'un groupe d'utilisateurs. Les administrateurs peuvent gérer les groupes d'utilisateurs, les rôles et les autorisations pour contrôler le niveau d'accès (et par conséquent, le niveau de sécurité) des utilisateurs système. Par exemple, vous devez ajouter des utilisateurs au groupe standard des utilisateurs finaux Cisco CCM pour que ces utilisateurs puissent accéder au Portail d'aide en libre-service pour téléphone Cisco Unified Communications Manager.

Étape 15 Associez un utilisateur à un téléphone (optionnel). Cette étape donne aux utilisateurs un certain niveau de contrôle de leur téléphone, comme le renvoi d'appels, l'ajout de numéros de numérotation abrégée ainsi que l'ajout de services.

Aucun utilisateur n'est associé à certains téléphones, notamment dans le cas des téléphones installés dans des salles de conférence.

Étape 16 Si vous n'êtes pas déjà dans la fenêtre Configuration de l'utilisateur final, choisissez **Gestion des utilisateurs** > **Utilisateur final** pour effectuer les dernières tâches de la configuration. Utilisez les champs de recherche ainsi que **Rechercher** pour trouver l'utilisateur (par exemple, John Doe), puis cliquez sur son ID utilisateur pour accéder à la fenêtre de Configuration de l'utilisateur final associée.

Étape 17 Sur l'écran, dans la zone Associations de numéros de répertoire, choisissez la ligne principale depuis la liste déroulante.

Étape 18 Dans la zone Mobility Information (Informations sur la mobilité), cochez la case Enable Mobility (Activer la mobilité).

Étape 19 Dans la zone Informations sur les autorisations, utilisez les boutons Groupe d'utilisateurs pour ajouter cet utilisateur à n'importe quel groupe.

Par exemple, vous pouvez ajouter l'utilisateur à un groupe qui est défini en tant que Groupe d'utilisateurs finals standard de CCM.

Étape 20 Pour afficher tous les groupes d'utilisateurs configurés, choisissez **Gestion des utilisateurs** > **Groupe d'utilisateurs**.

Étape 21 Dans la zone Mobilité de poste, cochez la case Activer le cluster croisé d'extension de mobilité si l'utilisateur a accès au service Cluster croisé d'extension de mobilité.

Étape 22 Sélectionnez **Enregistrer**.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Détermination de l'adresse MAC du téléphone

Pour ajouter des téléphones à Cisco Unified Communications Manager, vous devez déterminer l'adresse MAC d'un téléphone.

Procédure

Effectuez l'une des opérations ci-dessous :

- Sur le téléphone, appuyez sur **Applications**, choisissez **Informations sur le téléphone** et examinez le champ Adresse MAC.

- Regardez l'étiquette MAC située à l'arrière du téléphone.
- Affichez la page Web du téléphone et cliquez sur **Informations sur le périphérique**.

Méthodes disponibles pour ajouter des téléphones

Après avoir installé le téléphone IP Cisco, vous pouvez choisir l'une des options suivantes pour ajouter des téléphones dans la base de données Cisco Unified Communications Manager.

- Ajout de téléphones un à un avec Cisco Unified Communications Manager Administration
- Ajout de plusieurs téléphones avec l'outil d'administration en grand nombre (BAT)
- Enregistrement automatique
- Outil d'administration globale et outil de prise en charge des téléphones enregistrés automatiquement (TAPS)

Avant d'ajouter des téléphones individuellement ou avec l'outil d'administration en grand nombre, vous devez connaître l'adresse MAC du téléphone. Pour obtenir plus d'informations, reportez-vous à Détermination de l'adresse MAC du téléphone, à la page 74.

Pour plus d'informations sur l'outil d'administration BAT, consultez la documentation propre à votre version particulière de Cisco Unified Communications Manager.

Ajout de téléphones individuellement

Collectez l'adresse MAC et les informations sur le téléphone relatives au téléphone que vous allez ajouter à Cisco Unified Communications Manager.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone**.

Étape 2 Cliquez sur **Ajouter nouveau**.

Étape 3 Sélectionnez le type du téléphone.

Étape 4 Cliquez sur **Suivant**.

Étape 5 Renseignez les informations sur le téléphone, notamment l'adresse MAC.

Pour obtenir des instructions exhaustives et des informations conceptuelles sur Cisco Unified Communications Manager, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Étape 6 Sélectionnez **Enregistrer**.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Ajout de téléphones à l'aide du modèle de téléphone de l'outil d'administration globale (BAT)

L'outil d'administration globale (BAT) de Cisco Unified Communications permet d'exécuter des opérations par lots, notamment l'enregistrement de plusieurs téléphones.

Pour ajouter des téléphones à l'aide de BAT uniquement (pas en conjonction avec TAPS), vous devez obtenir l'adresse MAC correcte de chaque téléphone.

Pour plus d'informations à propos de l'utilisation du BAT, consultez la documentation propre à votre version particulière de Cisco Unified Communications Manager.

Procédure

Étape 1 Dans Cisco Unified Communications Administration, sélectionnez **Administration globale** > **Téléphones** > **Modèle de téléphone**.

Étape 2 Cliquez sur **Ajouter nouveau**.

Étape 3 Sélectionnez un type de téléphone et cliquez sur **Suivant**.

Étape 4 Saisissez les détails des paramètres propres aux téléphones, comme le pool de périphériques, le modèle de bouton de téléphone, le profil de sécurité des périphériques, etc.

Étape 5 Cliquez sur **Enregistrer**.

Étape 6 Sélectionnez **Périphérique** > **Téléphone** > **Ajouter nouveau** pour ajouter un téléphone à l'aide du modèle de téléphone de l'outil d'administration globale.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Ajout d'utilisateurs à Cisco Unified Communications Manager

Vous pouvez afficher et gérer des informations sur les utilisateurs enregistrés auprès de Cisco Unified Communications Manager. Dans Cisco Unified Communications Manager, chaque utilisateur peut aussi effectuer les tâches suivantes :

- Accéder au répertoire d'entreprise et à d'autres répertoire personnalisés à partir d'un téléphone IP Cisco.
- Créer un répertoire personnel.
- Configurer la numérotation abrégée et appeler des numéros de renvoi.
- S'abonner à des services qui sont accessibles sur un téléphone IP Cisco.

Procédure

Étape 1 Pour ajouter des utilisateurs individuellement, reportez-vous à Ajouter un utilisateur directement à Cisco Unified Communications Manager, à la page 77.

Étape 2 Pour ajouter des utilisateurs par lots, utilisez l'outil d'administration globale. Cette méthode permet également de définir un mot de passe par défaut identique pour tous les utilisateurs.

Pour obtenir plus d'informations, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Ajout d'un utilisateur à partir d'un annuaire LDAP externe

Si vous avez ajouté un utilisateur dans un annuaire LDAP (un répertoire autre que Cisco Unified Communications Server), vous pouvez immédiatement synchroniser l'annuaire LDAP avec l'instance de Cisco Unified Communications Manager dans laquelle vous ajoutez l'utilisateur et son téléphone.

Remarque Si vous ne synchronisez pas immédiatement l'annuaire LDAP avec Cisco Unified Communications Manager, le calendrier de synchronisation de l'annuaire LDAP, dans la fenêtre Annuaire LDAP, détermine l'heure à laquelle la prochaine synchronisation automatique est programmée. La synchronisation doit avoir lieu avant que vous n'associiez un nouvel utilisateur à un périphérique.

Procédure

Étape 1 Connectez-vous à Cisco Unified Communications Manager Administration.

Étape 2 Sélectionnez **Système** > **LDAP** > **Annuaire LDAP**.

Étape 3 Utilisez **Rechercher** pour localiser votre annuaire LDAP.

Étape 4 Cliquez sur le nom de l'annuaire LDAP.

Étape 5 Cliquez sur **Effectuer la synchronisation complète**.

Ajouter un utilisateur directement à Cisco Unified Communications Manager

Si vous n'utilisez pas un répertoire LDAP (Lightweight Directory Access Protocol), vous pouvez ajouter un utilisateur directement avec Cisco Unified Communications Manager Administration en procédant comme suit :

Remarque Si LDAP est synchronisé, vous ne pouvez pas ajouter un utilisateur avec Cisco Unified Communications Manager Administration.

Procédure

Étape 1 Depuis Cisco Unified Communications Manager Administration, sélectionnez **Gestion des utilisateurs** > **Utilisateur final**.

Étape 2 Cliquez sur **Ajouter nouveau**.

Étape 3 Dans le volet Informations utilisateur, saisissez les éléments suivants :

- ID utilisateur : saisissez le nom d'identification de l'utilisateur final. Cisco Unified Communications Manager ne permet pas de modifier l'ID utilisateur après sa création. Vous pouvez utiliser les caractères spéciaux =, +, <, >, #,;, \,, « » et les espaces. **Exemple** : jeandurant
- Mot de passe et Confirmation du mot de passe : saisissez au moins cinq caractères alphanumériques ou spéciaux pour le mot de passe de l'utilisateur final. Vous pouvez utiliser les caractères spéciaux =, +, <, >, #,;, \,, « » et les espaces.
- Nom de famille : Saisissez le nom de famille de l'utilisateur final. Vous pouvez utiliser les caractères spéciaux suivants : =, +, <, >, #, ;, \, , « », et les espaces vides. **Exemple** : durant
- Numéro de téléphone : saisissez le numéro de répertoire principal de l'utilisateur final. Les utilisateurs finals peuvent avoir plusieurs lignes sur leur téléphone. **Exemple** : 26640 (le numéro de téléphone d'entreprise interne de Jean Durant)

Étape 4 Cliquez sur **Enregistrer**.

Ajouter un utilisateur à un groupe d'utilisateurs finaux

Pour ajouter un utilisateur au groupe d'utilisateurs finaux standard Cisco Unified Communications Manager, procédez comme suit :

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Gestion des utilisateurs** > **Paramètres utilisateur** > **Groupe d'utilisateurs**.

La fenêtre Find and List Users (Recherche et affichage d'utilisateurs) apparaît.

Étape 2 Saisissez les critères de recherche appropriés et cliquez sur **Find** (Rechercher).

Étape 3 Sélectionnez le lien **Utilisateurs finaux standard de CCM**. La fenêtre Configuration du groupe d'utilisateurs des utilisateurs finaux standard de CCM s'ouvre.

Étape 4 Sélectionnez **Ajouter des utilisateurs finals au groupe**. La fenêtre Recherche et affichage d'utilisateurs s'ouvre.

Étape 5 Utilisez les cases de la liste déroulante Rech util pour rechercher les utilisateurs à ajouter, puis cliquez sur **Find** (Rechercher).

La liste des utilisateurs correspondants à vos critères de recherche s'affiche.

Étape 6 Dans la liste d'enregistrements qui apparaît, cliquez sur la case à cocher située en regard des utilisateurs à ajouter à ce groupe d'utilisateurs. Si la liste est longue, utilisez les liens situés au bas de la fenêtre pour afficher plus de résultats.

Remarque La liste des résultats de la recherche n'inclut pas les utilisateurs qui appartiennent déjà au groupe d'utilisateurs.

Étape 7 Sélectionnez **Ajouter sélection**.

Associer des téléphones aux utilisateurs

Vous pouvez associer des téléphones à des utilisateurs dans la fenêtre Utilisateur final de Cisco Unified Communications Manager.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Gestion des utilisateurs** > **Utilisateur final**.

La fenêtre Recherche et affichage d'utilisateurs s'ouvre.

Étape 2 Saisissez les critères de recherche appropriés et cliquez sur **Find** (Rechercher).

Étape 3 Dans la liste des enregistrements qui s'affiche, sélectionnez le lien correspondant à l'utilisateur.

Étape 4 Sélectionnez **Device Association** (Association de périphérique).

La page Association de périphérique d'utilisateur s'affiche.

Étape 5 Saisissez les critères de recherche appropriés et cliquez sur **Find** (Rechercher).

Étape 6 Pour sélectionner le périphérique à associer à l'utilisateur, cochez la case située à droite du périphérique.

Étape 7 Sélectionnez **Save Selected/Changes** (Enregistrer la sélection/les modifications) pour associer le périphérique à l'utilisateur.

Étape 8 Dans la liste déroulante Liens connexes située dans l'angle supérieur droit de la fenêtre, sélectionnez **Back to User** (Retour à l'utilisateur), puis cliquez sur **Aller**.

La fenêtre de configuration de l'utilisateur final apparaît et les périphériques associés que vous avez sélectionnés sont affichés dans le volet des périphériques contrôlés.

Étape 9 Sélectionnez **Save Selected/Changes** (Enregistrer la sélection/les modifications).

Survivable Remote Site Telephony (SRST)

SRST (Survivable Remote Site Telephony) permet de garantir que les fonctions de base du téléphone restent accessibles lorsque la connectivité WAN est perdue. Dans ce cas, le téléphone peut garder actif un appel en cours, et l'utilisateur peut accéder à un sous-ensemble des fonctionnalités disponibles. Lors d'un basculement, un message d'alerte s'affiche sur le téléphone.

Pour plus d'informations sur les micrologiciels pris en charge et sur SRST, consultez la page *Informations de compatibilité Cisco Unified Survivable Remote Site Telephony* sur Cisco.com. (http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-device-support-tables-list.html).

Le tableau suivant présente les fonctionnalités disponibles pendant le basculement.

Tableau 23 : Prise en charge de la fonctionnalité SRST

Fonctionnalité	Prise en charge	Remarques
Nouvel appel	Oui	
Mettre fin à l'appel	Oui	
Renumérotation	Oui	
Réponse	Oui	
Mettre en attente	Oui	
Reprise	Oui	
Conférence	Oui	
Conférence sur appels actifs (Joindre)	Non	La touche Appels act. ne s'affiche pas.
Liste des conférences	Non	
Transfert	Oui	
Transfert sur appels actifs (Transfert direct)	Non	
Réponse automatique	Oui	
Appel en attente	Oui	
Afficher l'ID de l'appelant	Oui	
Indicateur sonore de message en attente	Oui	
Touche de ligne programmable Tous les appels	Oui	
Touche de ligne programmable Répondre	Oui	
Présentation de la session Unified	Oui	La conférence est la seule fonctionnalité prise en charge, en raison des limitations liées aux autres fonctionnalités.

Fonctionnalité	Prise en charge	Remarques
Messagerie vocale	Oui	Votre messagerie vocale ne sera pas synchronisée avec celle des autres utilisateurs du cluster Cisco Unified Communications Manager.
Renvoi de tous les appels	Oui	L'état du renvoi n'est disponible que sur le téléphone qui définit le renvoi, car il n'y a pas d'affichage de lignes partagées en mode SRST. Les paramètres de Renvoi de tous les appels ne sont pas conservés lors du basculement vers SRST depuis Cisco Unified Communications Manager ou lors du retour vers Communications Manager depuis SRST. Toutes les options de renvoi de tous les appels initiales encore actives dans Communications Manager doivent être indiquées lorsque le périphérique se reconnecte à Communications Manager après le basculement.
Numérotation simplifiée	Oui	
Touche de ligne programmable Service IRL	Oui	
Vers la messagerie vocale (Rvoi Im)	Non	La touche Renvoi immédiat ne s'affiche pas.
Filtres de ligne	Partiel	Les lignes sont prises en charge mais ne peuvent pas être partagées.
Surveillance du parcage	Non	La touche Parquer ne s'affiche pas.
Insertion	Non	La touche Inser. ne s'affiche pas.
Indication des messages en attente améliorée	Non	Les badges de décompte des messages n'apparaissent pas sur l'écran du téléphone. Seule l'icône Message en attente s'affiche.
Parcage d'appels dirigé	Non	La touche ne s'affiche pas.
FLO	Partiel	La touche de fonction FLO est similaire aux touches de numérotation simplifiée.
Récupération d'un appel en attente	Non	Les appels restent en attente indéfiniment.
Attente à distance	Non	Les appels apparaissent comme des appels mis en attente localement.
MultConf	Non	La touche MultConf ne s'affiche pas.

Fonctionnalité	Prise en charge	Remarques
Intrcpt	Non	La touche ne provoque aucune action.
Interception d'appels de groupe	Non	La touche ne provoque aucune action.
Autre interception	Non	La touche ne provoque aucune action.
ID des appels malveillants	Non	La touche ne provoque aucune action.
QRT	Non	La touche ne provoque aucune action.
Groupe de recherche	Non	La touche ne provoque aucune action.
Intercom	Non	La touche ne provoque aucune action.
Mobilité	Non	La touche ne provoque aucune action.
Confidentialité	Non	La touche ne provoque aucune action.
Rappel automatique	Non	La touche Rappel ne s'affiche pas.
Vidéo	Oui	La visioconférence n'est pas prise en charge.
Vidéo	Oui	La visioconférence n'est pas prise en charge.
Ligne partagée	Non	
Numérotation simplifiée FLO	Oui	

Solution E-SRST (Enhanced Survivable Remote Site Telephony)

La solution E-SRST (Enhanced Survivable Remote Site Telephony) s'assure que les fonctionnalités téléphoniques supplémentaires disponibles restent accessibles lorsque la connectivité WAN est perdue. Outre les fonctionnalités prises en charge par la solution SRST (Survivable Remote Site Telephony), la solution E-SRST prend en charge les fonctionnalités suivantes :

- Ligne partagée
- Supervision de ligne occupée (FLO)
- Appels vidéo

Pour plus d'informations sur les micrologiciels pris en charge et sur SRST, consultez la page *Informations de compatibilité Cisco Unified Survivable Remote Site Telephony* sur Cisco.com. (http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-device-support-tables-list.html).

Règles de numérotation de l'application

Les règles de numérotation d'application sont utilisées pour convertir les numéros des contacts mobiles partagés en numéros pouvant être composés sur le réseau. Les règles de numérotation d'application ne s'appliquent pas

lorsque l'utilisateur compose un numéro manuellement, ou si le numéro est modifié avant que l'utilisateur passe l'appel.

Les règles de numérotation d'application sont définies dans Cisco Unified Communications Manager.

Pour plus d'informations sur les règles de numérotation, reportez-vous au *Guide de Configuration système de Cisco Unified Communications Manager*, chapitre « Configurer des règles de numérotation ».

Configuration des règles de numérotation de l'application

Procédure

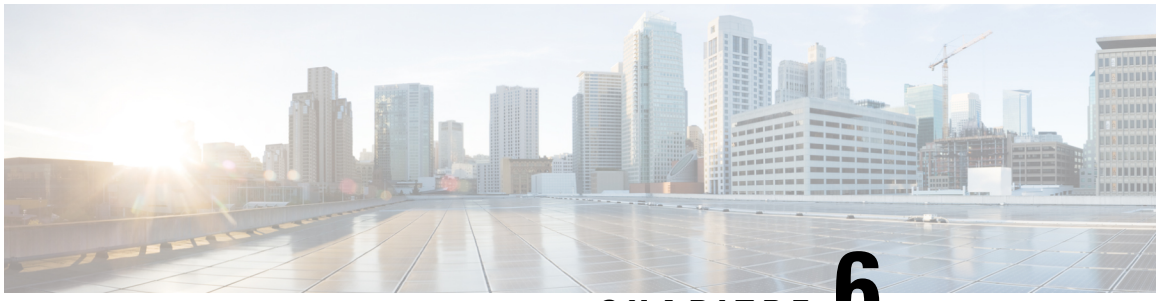
Étape 1 Dans AdministrationCisco Unified Communications Manager, allez à **Call Routing (Routage d'appels)** > **Règles de numérotation** > **Règle de numérotation d'application**.

Étape 2 Sélectionnez **Ajouter nouveau** pour créer une nouvelle règle de numérotation d'application, ou sélectionnez une règle de numérotation d'application et modifiez-la.

Étape 3 Renseignez les champs suivants :

- **Nom** : ce champ comporte le nom unique de la règle de numérotation, qui peut contenir jusqu'à 20 caractères alphanumériques et n'importe quelle combinaison d'espaces, de points (.), de tirets (-) et de tirets bas (_).
- **Description** : ce champ comporte une brève description que vous saisissez pour la règle de numérotation.
- **Numéro commençant par** : ce champ comporte les premiers chiffres des numéros de répertoire auxquels vous souhaitez appliquer cette règle de numérotation de l'application.
- **Nombre de chiffres** : ce champ requis comporte les premiers chiffres des numéros de répertoire auxquels vous souhaitez appliquer cette règle de numérotation de l'application.
- **Nombre total de chiffres à supprimer** : ce champ requis comporte le nombre de chiffres qui seront supprimés par Cisco Unified Communications Manager dans les numéros de répertoire auxquels cette règle de numérotation est appliquée.
- **Préfixe avec modèle** : ce champ requis comporte le modèle à ajouter aux numéros de répertoire auxquels cette règle de numérotation est appliquée.
- **Priorité de la règle de numérotation de l'application** : ce champ s'affiche lorsque vous saisissez les informations du champ Préfixe avec modèle. Ce champ sert à définir l'ordre de priorité des règles de numérotation d'application.

Étape 4 Redémarrez Cisco Unified Communications Manager.



CHAPITRE 6

Gestion du portail d'aide en libre-service

Présentation du portail d'aide en libre-service

Les utilisateurs peuvent accéder au portail d'aide en libre-service de Cisco Unified Communications pour personnaliser et contrôler les fonctionnalités et les paramètres du téléphone.

En tant qu’administrateur, vous contrôlez l'accès au portail d'aide en libre-service. Vous devez également fournir les informations nécessaires à vos utilisateurs pour qu'ils puissent y accéder.

Avant qu'un utilisateur puisse accéder au portail de libre-service de Cisco Unified Communications, vous devez utiliser Cisco Unified Communications ManagerCisco Unified Communications Manager Administration pour ajouter l'utilisateur à un groupe standard d'utilisateurs finaux.

Vous devez communiquer aux utilisateurs finaux les informations suivantes sur le portail d'aide en libre-service :

- L'URL d'accès à l'application. L’URL est :

  `https://<server_name:portnumber>/ucmuser/`, où nom_serveur est l'hôte sur lequel le serveur Web est installé et numéro de port, le numéro de port de cet hôte.

- Un ID utilisateur et un mot de passe par défaut pour accéder à l’application.
- Une présentation des tâches que les utilisateurs peuvent effectuer à l’aide du portail.

Ces paramètres correspondent aux valeurs que vous avez saisies lorsque vous avez ajouté l'utilisateur à Cisco Unified Communications Manager

Pour obtenir plus d'informations, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Configuration de l'accès des utilisateurs au portail d'aide en libre-service

Pour qu'un utilisateur puisse accéder au portail d'aide en libre-service, vous devez lui accorder une autorisation d'accès.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Gestion des utilisateurs** > **Utilisateur final**.

Étape 2 Recherchez l'utilisateur.

Étape 3 Cliquez sur le lien ID utilisateur.

Étape 4 Vérifiez qu'un mot de passe et un code PIN sont configurés pour l'utilisateur.

Étape 5 Dans la section informations d'autorisation, vérifiez que la liste des groupes inclut **Utilisateurs finaux standard de CCM**.

Étape 6 Sélectionnez **Enregistrer**.

Personnalisation de l'affichage du portail d'aide en libre-service

La plupart des options sont affichées dans le portail d'aide en libre-service. Toutefois, vous devez définir les options suivantes à l'aide des paramètre de configuration d'entreprise de Cisco Unified Communications Manager Administration:

- Afficher les paramètres de sonnerie
- Afficher les paramètres de libellé de ligne

Remarque Les paramètres s'appliquent à toutes les pages du portail d'aide en libre-service de votre site.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Système** > **Paramètres d'entreprise**.

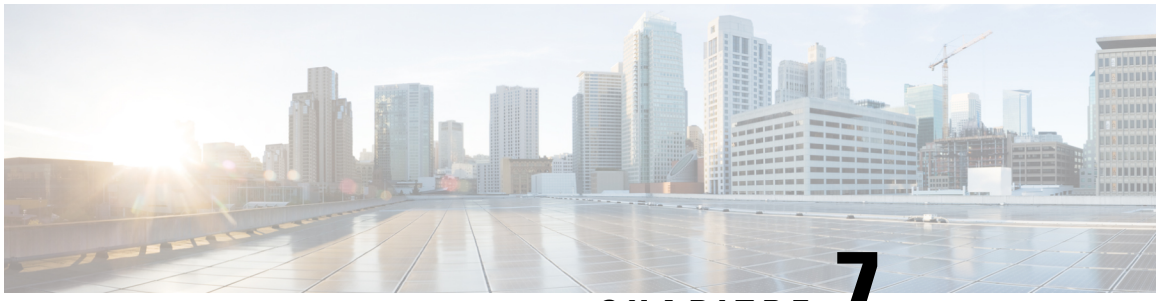
Étape 2 Dans la zone Portail d'aide en libre-service, définissez le champ **d'aide en libre-service Portal Default Server** (Serveur par défaut du portail d'aide en libre-service).

Étape 3 Activez ou désactivez les paramètres auxquels les utilisateurs peuvent accéder dans le portail.

Étape 4 Sélectionnez **Enregistrer**.

SECTION III

Administration du téléphone IP Cisco



CHAPITRE 7

Sécurité du téléphone IP Cisco

Renforcement de la sécurité pour votre réseau téléphonique

Vous pouvez activer Cisco Unified Communications Manager 11.5(1) et 12.0(1) pour fonctionner dans un environnement de sécurité renforcée. Grâce à ces améliorations, votre réseau téléphonique fonctionne dans le cadre d'un ensemble de commandes de gestion des risques et de sécurité strictes, pour vous protéger, ainsi que vos utilisateurs.

Cisco Unified Communications Manager 12.5 (1) ne prend pas en charge un environnement de sécurité renforcée. Désactivez FIPS avant la mise à niveau vers Cisco Unified Communications Manager 12.5 (1) ou votre TFTP et d'autres services ne fonctionneront pas correctement.

L'environnement de sécurité renforcée inclut les fonctionnalités suivantes :

- Authentification de recherche de contacts.
- TCP en tant que protocole par défaut pour l'enregistrement d'audit à distance.
- Mode FIPS.
- Une politique d'authentification améliorée.
- Prise en charge de la gamme SHA-2 de hachage pour la signature numérique.
- Prise en charge d'une taille de clé RSA de 512 et 4096 bits.

Avec Cisco Unified Communications Manager version 14.0 et le micrologiciel du téléphone IP Cisco version 14.0 et ultérieure, les téléphones prennent en charge l'authentification SIP OAuth.

OAuth est pris en charge par le protocole TFTP (Trivial File Transfer Protocol) proxy avec la version Cisco Unified Communications Manager 14.0 (1) SU1 ou ultérieure, et la version du micrologiciel du téléphone IP Cisco est 14.1 (1). Les proxy TFTP et OAuth pour proxy TFTP ne sont pas pris en charge sur Mobile Remote Access (MRA).

Pour plus d'informations sur la sécurité, voir ce qui suit :

- *Guide de configuration système de Cisco Unified Communications Manager, version 14.0(1)* ou ultérieure (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html).

- *Présentation de la sécurité des téléphones IP Cisco série 7800 et 8800* (https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html)
- *Guide de la sécurité de Cisco Unified Communications Manager*https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Remarque Le téléphone IP Cisco ne peut stocker qu'un nombre limité de fichiers de liste de confiance d'identité (ITL). Les fichiers ITL ne peuvent pas dépasser la limite de 64K sur le téléphone, alors limitez le nombre de fichiers que Cisco Unified Communications Manager envoie au téléphone.

Fonctionnalités de sécurité prises en charge

Les fonctionnalités de sécurité offrent une protection contre diverses menaces, notamment les menaces relatives à l'identité du téléphone et aux données. Ces fonctionnalités établissent et maintiennent des flux de communication authentifiés entre le téléphone et le serveur Cisco Unified Communications Manager. De plus, elles veillent à ce que le téléphone utilise uniquement des fichiers à signature numérique.

Les versions 8.5(1) et ultérieures de Cisco Unified Communications Manager incluent Security par défaut, qui permet aux fonctionnalités de sécurité pour les téléphones IP Cisco d'être utilisées sans le client CTL :

- Signature des fichiers de configuration du téléphone
- Chiffrement des fichiers de configuration du téléphone
- HTTPS avec Tomcat et d'autres services Web

Remarque Il est toutefois nécessaire d'exécuter le client CTL et d'utiliser les eTokens matériels pour bénéficier du signalement sécurisé et des fonctionnalités multimédia.

Implémenter la sécurité dans le système Cisco Unified Communications Manager permet de prévenir les usurpations d'identité pour le téléphone et le serveur Cisco Unified Communications Manager, la falsification des données ainsi que la falsification du signalement des appels et des flux multimédia.

Pour se protéger contre ces menaces, le réseau de téléphonie IP Cisco Unified établit et maintient des flux de communication sécurisés (chiffrés) entre un téléphone et le serveur, signe numériquement les fichiers avant leur transfert vers un téléphone et crypte les flux multimédia ainsi que le signalement des appels entre les téléphones IP Cisco Unified.

Lorsque vous effectuez les tâches nécessaires associées au CAPF (fonction proxy de l'autorité de certification), un LSC (certificat valable localement) est installé sur les téléphones. Vous pouvez utiliser Cisco Unified Communications Manager Administration pour configurer un LSC, comme indiqué dans le guide de sécurité de Cisco Unified Communications Manager. Vous pouvez également lancer l'installation d'un LSC depuis le menu Paramétrage de sécurité du téléphone. Vous pouvez aussi effectuer dans ce menu la mise à jour ou la suppression du certificat LSC.

Un certificat valable localement ne peut être utilisé comme certificat utilisateur pour EAP-TLS avec l'authentification de réseau local sans fil.

Les téléphones utilisent le profil de sécurité du téléphone, qui détermine si le périphérique est sécurisé ou non. Pour plus d'informations sur l'application du profil de sécurité au téléphone, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.

Si vous configurez des paramètres de sécurité dans Cisco Unified Communications Manager Administration, sachez que le fichier de configuration du téléphone contient des informations sensibles. Pour garantir la confidentialité d'un fichier de configuration, vous devez configurer son chiffrement. Pour plus d'informations, reportez-vous à la documentation relative à votre version particulière de Cisco Unified Communications Manager.

Le téléphone IP Cisco série 8800 est conforme à Federal Information Processing Standard (FIPS). Pour fonctionner correctement, le mode FIPS exige une taille de clé de 2048 bits ou supérieure. Si le certificat n'est pas à la taille 2048 bits ou plus, le téléphone ne s'enregistre pas auprès de Cisco Unified Communications Manager et le message `Le téléphone n'a pas pu être enregistré. La taille de la clé de certificat n'est pas conforme à FIPS` s'affiche sur le téléphone.

Si le téléphone comporte un LSC (certificat valable localement), vous devez mettre à jour la taille de clé du LSC à 2048 bits ou plus avant d'activer FIPS.

Le tableau suivant fournit une vue d'ensemble des fonctionnalités de sécurité prises en charge par le téléphone. Pour obtenir plus d'informations, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Pour afficher les paramètres de sécurité en cours sur un téléphone, y compris le mode de sécurité, la liste de confiance et l'authentification 802. 1 X, appuyez sur la touche **Applications** et choisissez **Paramètres Admin** > **Paramétrage de sécurité**.

Tableau 24 : Vue d'ensemble des fonctionnalités de sécurité

Fonctionnalité	Description
Authentification de l’image	Des fichiers binaires signés (avec l'extension .sbn) permettent de prévenir la falsification du fichier image du micrologiciel avant que celui-ci ne soit chargé sur un téléphone. La modification de l’image entraînerait l’échec du processus d'authentification du téléphone et le rejet de la nouvelle image.
Chiffrement des fichiers image	Des fichiers binaires chiffrés (avec l'extension .sebn) permettent de prévenir la falsification du fichier image du micrologiciel avant que celui-ci ne soit chargé sur un téléphone. La modification de l’image entraînerait l’échec du processus d'authentification du téléphone et le rejet de la nouvelle image.
Installation d'un certificat sur site client	Un certificat unique doit être affecté à chaque téléphone IP Cisco pour l’authentification de périphérique. Les téléphones comportent un certificat installé par le fabricant (MIC), mais pour plus de sécurité, vous pouvez spécifier l'installation d'un certificat dans Cisco Unified Communications Manager Administration en utilisant la fonctionnalité proxy d'autorité de certificat (CAPF). Vous pouvez aussi installer un certificat valable localement (LSC) à partir du menu Paramétrage de sécurité du téléphone.

Fonctionnalité	Description
Authentification du périphérique	A lieu entre le serveur Cisco Unified Communications Manager et le téléphone lorsque chaque entité accepte le certificat de l'autre entité. Détermine si une connexion sécurisée peut être établie entre le téléphone et un Cisco Unified Communications Manager. Si nécessaire, elle crée un chemin de signalement sécurisé entre ces entités grâce au protocole TLS. Cisco Unified Communications Manager n'enregistre que les téléphones qu'il peut authentifier.
Authentification des fichiers	Valide les fichiers signés numériquement qui ont été téléchargés sur le téléphone. Le téléphone valide la signature pour garantir qu'aucune falsification n'a eu lieu après la création du fichier. Les fichiers qui ne peuvent pas être authentifiés ne sont pas inscrits dans la mémoire flash du téléphone. Le téléphone rejette ces fichiers, sans traitement supplémentaire.
Chiffrement des fichiers	Le chiffrement garantit la confidentialité des informations sensibles lorsque le fichier est en transit vers le téléphone. De plus, le téléphone valide la signature pour confirmer qu'aucune falsification n'a eu lieu après la création du fichier. Les fichiers qui ne peuvent pas être authentifiés ne sont pas inscrits dans la mémoire flash du téléphone. Le téléphone rejette ces fichiers, sans traitement supplémentaire.
Authentification du signalement	Utilise le protocole TLS pour vérifier qu'aucune falsification des paquets de signalement n'a eu lieu pendant la transmission.
Certificat installé en usine	Chaque téléphone IP Cisco contient un certificat unique installé en usine (MIC), qui est utilisé pour l'authentification du périphérique. Le MIC agit comme une preuve unique et permanente d'identité pour le téléphone et permet à Cisco Unified Communications Manager d'authentifier le téléphone.
Chiffrement multimédia	Utilise SRTP pour garantir la sécurité des flux multimédia entre les périphériques pris en charge et pour garantir que seul l'appareil souhaité peut recevoir et lire les données. Implique la création d'une paire de clés multimédia principales pour les périphériques, la remise de ces clés sur les périphériques, et la sécurisation de la remise des clés pendant leur transport.
CAPF (fonction proxy de l'autorité de certification)	Met en œuvre des parties de la procédure de génération de certificat qui nécessitent un traitement trop intensif pour le téléphone, et interagit avec le téléphone pour générer des clés et pour installer des certificats. La fonctionnalité CAPF peut être configurée pour demander à la place du téléphone, des certificats provenant d'autorités de certification spécifiées par le client, ou pour générer des certificats localement.
Profil de sécurité	Détermine si un téléphone n'est pas sécurisé, s'il est authentifié, chiffré ou protégé. Les autres entrées de ce tableau décrivent des fonctionnalités de sécurité.
Fichiers de configuration chiffrés	Permettent d'assurer la confidentialité des fichiers de configuration du téléphone.
Désactivation optionnelle d'un serveur web pour un téléphone	Pour des raisons de sécurité, vous pouvez empêcher l'accès aux pages web pour un téléphone (qui révèlent un certain nombre de statistiques opérationnelles pour le téléphone) ainsi qu'au portail d'aide en libre-service.

Fonctionnalité	Description
Renforcement de la sécurité du téléphone	Options de sécurité supplémentaires, paramétrables depuis Cisco Unified Communications Manager Administration : • Désactivation du port PC • Désactivation des requêtes ARP gratuites (GARP) • Désactivation de l'accès au VLAN vocal du PC • Désactivation de l'accès au menu Paramètres ou fourniture d'un accès restreint permettant d'accéder seulement au menu Préférences et à la sauvegarde des changements de volume. • Désactivation de l'accès aux pages web pour un téléphone • Désactivation du port d'accessoires Bluetooth • Restriction des codes de chiffrement TLS
Authentification 802.1x	Le téléphone IP Cisco peut utiliser l'authentification 802.1X pour demander et obtenir l'accès au réseau. Pour plus d'informations, reportez-vous à la section Authentification 802.1x, à la page 115.
Basculement SIP sécurisé pour SRST	Lorsque vous configurez une référence de sécurité Survivable Remote Site Telephony (SRST) et que vous réinitialisez les périphériques associés dans Cisco Unified Communications Manager Administration, le serveur TFTP ajoute le certificat SRST au fichier cnf.xml du téléphone et envoie ce fichier au téléphone. Un téléphone sécurisé utilise alors une connexion TLS pour interagir avec le routeur compatible SRST.
Chiffrement du signalement	Garantit le chiffrement de tous les messages de signalement SIP transmis entre l'appareil et le serveur Cisco Unified Communications Manager.
Alerte Liste de confiance mise à jour	Lorsque la liste de confiance est mise à jour sur le téléphone, Cisco Unified Communications Manager reçoit une alerte indiquant la réussite ou l'échec de la mise à jour. Pour plus d'informations, reportez-vous au tableau suivant.

Chiffrement AES 256	S'ils sont connectés à Cisco Unified Communications Manager version 10.5(2) ou ultérieure, les téléphones peuvent utiliser le chiffrement AES 256 pour TLS et SIP lors du chiffrement du signalement et des flux multimédia. Les téléphones peuvent ainsi établir et prendre en charge des connexions TLS 1.2 à l'aide de codes AES-256 conformes aux normes SHA-2 (algorithme de hachage sécurisé) et respectant les normes fédérales de traitement d'informations (FIPS). Les codes de chiffrement sont les suivants :
	• Pour les connexions TLS :
	  • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	  • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	• Pour sRTP :
	  • AEAD_AES_256_GCM
	  • AEAD_AES_128_GCM
	Pour plus d'informations, reportez-vous à la documentation de Cisco Unified Communications Manager.

Fonctionnalité	Description
Certificats ECDSA (Elliptic Curve Digital Signature Algorithm)	Dans le cadre de la certification de critères communs (CC), Cisco Unified Communications Manager a ajouté des certificats ECDSA dans la version 11.0. Cela affecte tous les produits de système d'exploitation vocal (VOS) à partir de la version CUCM 11.5 et versions ultérieures.

Le tableau suivant contient les différents messages d'alerte de mise à jour de la liste de confiance ainsi que leur signification. Pour plus d'informations, reportez-vous à la documentation de Cisco Unified Communications Manager

Tableau 25 : Messages d'alerte Liste de confiance mise à jour

Code et message	Description
1 - TL_SUCCESS	Nouveau CTL et/ou ITL reçu
2 - CTL_INITIAL_SUCCESS	Nouveau CTL reçu, pas de TL existant
3 - ITL_INITIAL_SUCCESS	Nouveau ITL reçu, pas de TL existant
4 - TL_INITIAL_SUCCESS	Nouveaux CTL et ITL reçus, pas de TL existant
5 - TL_FAILED_OLD_CTL	Échec de la MàJ du nouveau CTL, mais TL précédent présent
6 - TL_FAILED_NO_TL	Échec de la MàJ du nouveau TL, pas de TL précédent présent
7 - TL_FAILED	Échec générique
8 - TL_FAILED_OLD_ITL	Échec de la MàJ du nouveau ITL, mais TL précédent présent
9 - TL_FAILED_OLD_TL	Échec de la MàJ de la nouveau TL, mais TL précédent présent

Le menu Paramétrage de sécurité fournit des informations sur les différents paramètres de sécurité. Il permet également d'accéder au menu Liste de confiance et indique si les fichiers CTL ou ITL sont installés sur le téléphone.

Le tableau suivant décrit les options disponibles dans le menu Paramétrage de sécurité.

Tableau 26 : Menu Paramétrage de sécurité

Option	Description	Pour modifier
Mode de sécurité	Affiche le mode de sécurité qui est défini pour le téléphone.	Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone**. Les paramètres sont affichés dans la partie Informations propres au protocole de la fenêtre Configuration du téléphone.
LSC	Indique si un certificat valable localement utilisé pour des fonctionnalités de sécurité est installé sur le téléphone (Oui) ou n'est pas installé sur le téléphone (Non).	Pour plus d'informations sur la gestion du LSC pour votre téléphone, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.

Option	Description	Pour modifier
Liste de confiance	La Liste sécurisée dispose de sous-menus pour le CTL, l'ITL et les fichiers de configuration signés. Le sous-menu Fichier CTL affiche le contenu du fichier CTL. Le sous-menu Fichier ITL affiche le contenu du fichier ITL. Le menu Liste sécurisée affiche également les informations suivantes : • Signature CTL : l'empreinte SHA1 du fichier CTL • CM unifié / Serveur TFTP : le nom du Cisco Unified Communications Manager et du serveur TFTP utilisés par le téléphone. Affiche une icône de certificat si un certificat est installé pour ce serveur. • Serveur CAPF : le nom du serveur CAPF utilisé par le téléphone. Affiche une icône de certificat si un certificat est installé pour ce serveur. • Routeur SRST : l'adresse IP du routeur SRST de confiance que le téléphone peut utiliser. Affiche une icône de certificat si un certificat est installé pour ce serveur.	Pour obtenir plus d'informations, reportez-vous à Configuration d'un certificat localement important, à la page 95.
Authentification 802.1x	Permet d'activer l'authentification 802.1x sur ce téléphone.	Reportez-vous à Authentification 802.1x, à la page 115.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Configuration d'un certificat localement important

Cette tâche s'applique à la configuration d'un certificat valable localement avec la méthode de chaîne d'authentification.

Avant de commencer

Vérifiez que les configurations de sécurité pour Cisco Unified Communications Manager et pour CAPF (Certificate Authority Proxy Function, fonction proxy d'autorité de certificat) ont été effectuées :

- Le fichier CTL ou ITL doit être doté d'un certificat CAPF.
- Les certificats CAPF doivent être installés dans Cisco Unified Communications Operating System Administration.
- CAPF doit être configuré et en cours d'exécution.

Pour plus d'informations sur ces paramètres, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.

Procédure

Étape 1 Obtenez le code d'authentification CAPF qui a été défini lors de la configuration de CAPF.

Étape 2 À partir du téléphone, appuyez sur **Applications** .

Étape 3 Sélectionnez **Paramètres admin.** > **Paramétrage de sécurité**.

Remarque Vous pouvez contrôler l'accès au menu Paramètres grâce au champ Accès aux paramètres de la fenêtre Configuration du téléphone de Cisco Unified Communications Manager Administration.

Étape 4 Sélectionnez **LSC** et appuyez sur **Sélect.** ou sur **MàJ**.

Le téléphone vous invite à saisir une chaîne d'authentification.

Étape 5 Saisissez le code d'authentification et appuyez sur **Soum**.

Le téléphone commence à installer, mettre à jour ou supprimer le certificat valable localement, selon le mode de configuration du CAPF. Au cours de cette procédure, une série de messages apparaît dans le champ d'option LSC du menu Paramétrage de sécurité, et vous pouvez ainsi surveiller la progression de l'opération. Lorsque la procédure est terminée, le texte Installé ou Non installé s'affiche à l'écran du téléphone.

Le processus d'installation, de mise à jour ou de suppression du certificat valable localement peut prendre un certain temps.

Lorsque l'installation sur le téléphone réussit, le message `Installé` s'affiche. Si le téléphone affiche `Non installé`, la chaîne d'autorisation est peut-être incorrecte, ou il est peut-être impossible d'effectuer une mise à niveau sur le téléphone. Si l'opération de CAPF supprime le certificat valable localement, le téléphone affiche `Non installé` pour indiquer la réussite de l'opération. Le serveur CAPF enregistre les messages d'erreur. Reportez-vous à la documentation relative au serveur CAPF pour savoir où trouver les journaux et pour connaître la signification des messages d'erreur.

Activer le mode FIPS

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone** et localisez le téléphone.

Étape 2 Déplacez-vous jusqu'à la zone Configuration spécifique au produit.

Étape 3 Définissez le champ **Mode FIPS** à Activé.

Étape 4 Sélectionnez **Appliquer la configuration**.

Étape 5 Sélectionnez **Enregistrer**.

Étape 6 Redémarrez le téléphone.

Sécurité des appels téléphoniques

Lorsque la sécurité est appliquée à un téléphone, une icône s'affiche à l'écran du téléphone. Une tonalité de sécurité est également émise au début des appels lorsque le téléphone connecté est sécurisé et protégé.

Lors d'un appel sécurisé, tous les flux de signalisation d'appel et multimédia sont chiffrés. Les appels sécurisé offrent un niveau élevé de sécurité, ce qui assure leur intégrité et leur confidentialité. Lorsqu'un appel en cours est chiffré, l'icône de progression de l'appel située à droite du minuteur de durée de l'appel sur l'écran du téléphone est remplacée par l'icône suivante :  .

Remarque Si l'appel est acheminé au moyen de tronçons autres que des tronçons IP, par exemple, par PSTN, l'appel risque de ne pas être sécurisé même s'il est chiffré sur le réseau IP et que l'icône représentant un verrou y est associée.

Lors d'un appel sécurisé, une tonalité de sécurité est émise au début de l'appel pour indiquer que l'autre téléphone connecté reçoit et émet aussi de l'audio sécurisé. Si l'appel se connecte à un téléphone non sécurisé, la tonalité de sécurité n'est pas émise.

Remarque Les appels sécurisés ne sont pris en charge que pour les connexions entre deux téléphones. Certaines fonctionnalités, comme la conférence téléphonique et la ligne partagée, ne sont pas disponibles lorsque l'appel sécurisé est configuré.

Lorsqu'un téléphone est configuré comme sécurisé (chiffré et authentifié) dans Cisco Unified Communications Manager, vous pouvez lui accorder le statut « protégé ». Ensuite, si vous le souhaitez, le téléphone protégé peut être configuré pour émettre une tonalité indicative au début de l'appel :

- Protected Device (Périphérique protégé) : pour remplacer l'état d'un téléphone sécurisé par l'état protégé, cochez la case Protected Device (Périphérique protégé) dans la fenêtre Phone Configuration (Configuration du téléphone) de Cisco Unified Communications Manager Administration (**Périphérique** > **Téléphone**).
- Play Secure Indication Tone (Émettre la tonalité de sécurisation) : pour que le téléphone protégé émette une tonalité indiquant que le téléphone est sécurisé ou non, définissez cette option par True. Par défaut, l'option Play Secure Indication Tone (Émettre la tonalité de sécurisation) est définie par False. Vous pouvez régler cette option dans Cisco Unified Communications Manager Administration (**Système** > **Paramètres de service**). Sélectionnez le serveur, puis le service Unified Communications Manager. Dans la fenêtre Service Parameter Configuration (Configuration des paramètres de service), sélectionnez l'option dans la zone Fonction - Tonalité de sécurité. La valeur par défaut est False.

Identification d'une conférence téléphonique sécurisée

Vous pouvez lancer une conférence téléphonique sécurisée et surveiller le niveau de sécurité des participants. Le processus d'établissement d'une conférence téléphonique sécurisée est le suivant :

1. Un utilisateur lance la conférence sur un téléphone sécurisé.
2. Cisco Unified Communications Manager attribue un pont de conférence sécurisé à l'appel.
3. À mesure que les participants sont ajoutés à la conférence, Cisco Unified Communications Manager vérifie le mode de sécurité de chaque téléphone et maintient le niveau de sécurité de la conférence.

4. Le téléphone affiche le niveau de sécurité de la conférence téléphonique. Lors des conférences sécurisées, l'icône de sécurisation est affichée à droite du texte **Conférence** sur l'écran du téléphone.

Remarque Les appels sécurisés sont pris en charge entre deux téléphones. Pour les téléphones sécurisés, certaines fonctionnalités, comme la conférence téléphonique, la ligne partagée et Extension Mobility (Mobilité de poste), ne sont pas disponibles lorsque l'appel sécurisé est configuré.

Le tableau suivant présente des informations sur les modifications du niveau de sécurité en fonction du niveau de sécurité du téléphone de l'initiateur, le niveau de sécurité des participants, et la disponibilité des ponts de conférence sécurisés.

Tableau 27 : Restrictions relatives à la sécurisation des conférences téléphoniques

Niveau de sécurité du téléphone de l'initiateur	Fonctionnalité utilisée	Niveau de sécurité des participants	Résultat de l'action
Non sécurisé	Conférence	Sécurisé	Pont de conférence non sécurisé Conférence non sécurisée
Sécurisé	Conférence	Au moins un membre n'est pas sécurisé.	Pont de conférence sécurisé Conférence non sécurisée
Sécurisé	Conférence	Sécurisé	Pont de conférence sécurisé Conférence de niveau sécurisé chiffré
Non sécurisé	MultConf	Le niveau de sécurité minimum est chiffré.	L'initiateur reçoit le message `Ne respecte le niveau de sécurité, appel re`
Sécurisé	MultConf	Le niveau de sécurité minimum est non sécurisé.	Pont de conférence sécurisé La conférence accepte tous les appels.

Identification d'un appel téléphonique sécurisé

Un appel sécurisé est établi lorsque votre téléphone et le téléphone distant sont configurés avec la sécurisation des appels. L'autre téléphone peut résider sur le même réseau IP Cisco, ou sur un autre réseau hors du réseau IP. Il n'est possible de passer des appels sécurisés qu'entre deux téléphones. Il est nécessaire de configurer un pont de conférence sécurisé pour que les conférences téléphoniques prennent en charge les appels sécurisés.

Le processus d'établissement d'un appel sécurisé est le suivant :

1. Un utilisateur passe l'appel sur un téléphone sécurisé (mode de sécurité sécurisé).
2. L'icône de sécurisation apparaît à l'écran du téléphone. Cette icône indique que le téléphone est configuré pour les appels sécurisés, mais cela ne signifie pas que l'autre téléphone connecté est sécurisé.

3. L'utilisateur entend une tonalité de sécurité si l'appel est connecté à un autre téléphone sécurisé, indiquant que les deux extrémités de la conversation sont chiffrées et sécurisées. Si l'appel est connecté à un téléphone non sécurisé, l'utilisateur n'entend pas la tonalité de sécurité.

Remarque Les appels sécurisés sont pris en charge entre deux téléphones. Pour les téléphones sécurisés, certaines fonctionnalités, comme la conférence téléphonique, la ligne partagée et Extension Mobility (Mobilité de poste), ne sont pas disponibles lorsque l'appel sécurisé est configuré.

Seuls les téléphones protégés émettent ces tonalités de sécurisation ou de non-sécurisation. Les téléphones non protégés n'émettent jamais les tonalités. Si l'état global de l'appel change au cours d'un appel, la tonalité indicative change et le téléphone protégé émet la tonalité adéquate.

L'émission d'une tonalité sur les téléphones protégés est soumise aux conditions suivantes :

- Lorsque l'option Play Secure Indication Tone (Émettre la tonalité de sécurisation) est activée :
  - Lorsqu'une connexion sécurisée de bout en bout est établie et que l'état de l'appel est sécurisé, le téléphone émet la tonalité de sécurisation (trois bips longs avec des pauses).
  - Lorsqu'une connexion média non sécurisée de bout en bout est établie et que l'appel est non sécurisé, le téléphone émet la tonalité d'indication de non sécurité (six bips courts avec de brèves pauses).

Lorsque l'option Play Secure Indication Tone (Émettre la tonalité de sécurisation) est désactivée, aucune tonalité n'est émise.

Fourniture de chiffrement pour l'insertion

Cisco Unified Communications Manager vérifie le statut de sécurité du téléphone lorsque des conférences sont établies et modifie les indications de sécurité pour la conférence ou bloque la réalisation de l'appel pour maintenir l'intégrité et la sécurité du système.

Un utilisateur ne peut pas s'insérer dans un appel chiffré si le téléphone utilisé pour l'insertion n'est pas configuré pour le chiffrement. Lorsque l'insertion échoue dans ce cas, une tonalité de réorganisation (Tonalité occupé rapide) sort du téléphone sur lequel a été lancée l'insertion.

Si le téléphone de l'initiateur est configuré pour le chiffrement, l'initiateur de l'insertion peut s'insérer dans un appel non sécurisé à partir du téléphone chiffré. Après l'insertion, Cisco Unified Communications Manager classe l'appel comme étant non sécurisé.

Si le téléphone de l'initiateur est configuré pour le chiffrement, l'initiateur de l'insertion peut s'insérer dans un appel chiffré et le téléphone indique que l'appel est chiffré.

Sécurité WLAN

Tout périphérique WLAN étant à portée peut recevoir n'importe quel trafic WLAN : en conséquence, la sécurisation des communications voix est un élément essentiel des réseaux WLAN. Pour garantir qu'aucun intrus ne manipule ou n'intercepte le trafic voix, l'architecture de sécurité SAFE de Cisco prend en charge les téléphones IP Cisco ainsi que les points d'accès Cisco Aironet. Pour plus d'informations sur la sécurité dans les réseaux, consultez http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html.

La solution de téléphonie IP Cisco sans fil assure la sécurité des réseaux sans fil, empêchant les connexions non autorisées et les communications dangereuses à l'aide des méthodes d'authentification suivantes prises en charge par les téléphones IP Cisco sans fil :

- Authentification ouverte : tout périphérique sans fil peut demander une authentification dans un système ouvert. Le point d'accès qui reçoit la requête peut accorder l'authentification à n'importe quel demandeur ou seulement aux demandeurs présents sur une liste d'utilisateurs. Les communications entre le périphérique sans fil et le point d'accès peuvent être non chiffrées ou les périphériques peuvent utiliser des clés WEP (Wired Equivalent Privacy) pour plus de sécurité. Les périphériques utilisant WEP tentent uniquement de s'authentifier auprès des points d'accès utilisant WEP.
- Authentification EAP-FAS (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling) : cette architecture de sécurité client-serveur chiffre les transactions EAP circulant par un tunnel TLS (Transport Level Security) entre un point d'accès et un serveur RADIUS, comme le serveur Cisco ACS (Access Control Server).

  Le tunnel TLS utilise des identifiants PAC (Protected Access Credentials) lors de l'authentification du client (téléphone) avec le serveur RADIUS. Le serveur envoie un identifiant AID (Authority ID) au client (téléphone), qui sélectionne ensuite le PAC approprié. Le client (téléphone) renvoie un champ PAC-Opaque au serveur RADIUS. Le serveur déchiffre le PAC grâce à la clé principale. Les deux terminaux détiennent alors la clé PAC et un tunnel TLS est créé. EAP-FAST prend en charge le provisionnement automatique de PAC, mais vous devez activer cette option sur le serveur RADIUS.

Remarque Par défaut, dans Cisco ACS, le PAC expire au bout d'une semaine. Si le téléphone détient un PAC qui a expiré, l'authentification avec le serveur RADIUS prend plus de temps, car le téléphone doit obtenir un nouveau PAC. Pour éviter les délais de provisionnement de PAC, configurez la durée de vie du PAC à 90 jours ou plus sur le serveur ACS ou RADIUS.

- L'authentification Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) : EAP-TLS requiert un certificat client pour l'authentification et l'accès au réseau. Dans le cas d'EAP-TLS filaire, le certificat client peut être le MIC du téléphone ou un certificat valable localement. Le certificat valable localement (LSC) est le certificat d'authentification client recommandé dans le cas de l'EAP-TLS filaire.
- Protocole PEAP (Protected Extensible Authentication Protocol) : modèle propriétaire Cisco d'authentification mutuelle via mot de passe entre le client (téléphone) et un serveur RADIUS. Un téléphone IP Cisco peut utiliser PEAP pour s'authentifier auprès d'un réseau sans fil. Les méthodes d'authentification PEAP-MSCHAPv2 et PEAP-GTC sont prises en charge.

Les modèles d'authentification suivants utilisent le serveur RADIUS pour gérer les clés d'authentification :

- WPA/WPA2 : utilise les informations du serveur RADIUS pour générer des clés d'authentification uniques. Ces clés étant générées par le serveur RADIUS centralisé, WPA/WPA2 assure une sécurité renforcée par rapport aux clés WPA pré-partagées stockées par le point d'accès et le téléphone.
- Itinérance sécurisée rapide : utilise le serveur RADIUS et les informations d'un serveur de domaine sans fil (WDS) pour gérer et authentifier les clés. Le serveur WDS crée un cache d'informations d'identification pour les périphériques clients ayant activé CCKM, permettant ainsi une ré-authentification rapide et sécurisée. Le téléphone IP Cisco série 8800 prend en charge 802.11r (FT). 11r (FT) et CCKM sont tous deux pris en charge pour autoriser l'itinérance sécurisée rapide. Mais, Cisco recommande d'utiliser le 802.11r (FT) plutôt que la méthode aérienne.

Avec WPA/WPA2 et CCKM, les clés de chiffrement ne sont pas saisies sur le téléphone, mais sont extrapolées automatiquement entre le point d'accès et le téléphone. Toutefois, les nom d'utilisateur et mot de passe EAP utilisés pour l'authentification doivent être saisis sur chaque téléphone.

Pour garantir la sécurité du trafic voix, le téléphone IP Cisco prend en charge les protocoles WEP et TKIP ainsi que la norme AES (Advanced Encryption Standards) pour le chiffrement. Lorsque ces mécanismes sont utilisés pour le chiffrement, les paquets de signalement SIP et les paquets de RTP (Real-Time Transport Protocol) vocal sont chiffrés entre le point d'accès et le téléphone IP Cisco.

WEP

Lorsque le réseau sans fil utilise WEP, l'authentification a lieu au point d'accès et s'effectue de manière ouverte ou via clés partagées. La clé WEP configurée sur le téléphone doit correspondre à la clé WEP configurée sur le point d'accès pour des connexions réussies. Le téléphone IP Cisco prend en charge les clés WEP qui utilisent un chiffrement 40 bits ou 128 bits et qui restent statiques sur le téléphone et le point d'accès.

L'authentification EAP et CCKM peut utiliser des clés WEP pour le chiffrement. Le serveur RADIUS gère la clé WEP et transmet une clé WEP unique au point d'accès après l'authentification pour chiffrer tous les paquets voix. En conséquence, ces clés WEP peuvent changer à chaque authentification.

TKIP

WPA et CCKM utilisent un chiffrement TKIP qui bénéficie de nombreux avantages par rapport à WEP. TKIP assure un chiffrement des clés par paquet et des vecteurs d'initialisation (IV) plus longs qui renforcent le chiffrement. De plus, un message de vérification d'intégrité (MIC) garantit la non-altération des paquets chiffrés. TKIP permet de supprimer le caractère prévisible de WEP, qui faciliterait le déchiffrage de la clé WEP par des intrus.

AES

Une méthode de codage utilisée pour l'authentification WPA2. Ce standard national de chiffrement utilise un algorithme symétrique qui emploie une clé identique pour le chiffrement et le décodage. AES utilise un chiffrement CBC (Cipher Blocking Chain) de 128 bits et prend ainsi en charge les tailles de clé de 128, 192 et 256 bits au minimum. Le téléphone IP Cisco prend en charge une taille de clé de 256 bits.

Remarque Le téléphone IP Cisco ne prend pas en charge le protocole CKIP (Cisco Key Integrity Protocol) avec CMIC.

Les modèles d'authentification et de chiffrement sont configurés dans le LAN sans fil. Les VLAN sont configurés dans le réseau et sur les points d'accès. Ils spécifient différentes combinaisons d'authentification et de chiffrement. Un SSID s'associe avec un VLAN et avec un modèle spécifique d'authentification et de chiffrement. Pour que les périphériques clients sans fil réussissent à s'authentifier, vous devez configurer les mêmes SSID avec leurs modèles d'authentification et de chiffrement sur les points d'accès et le téléphone IP Cisco.

Certains modèles d'authentification nécessitent des types de chiffrement spécifiques. Avec l'authentification ouverte, vous pouvez utiliser une clé WEP statique pour le chiffrement, ce qui renforcera la sécurité. Toutefois, si vous utilisez une authentification par clé partagée, vous devez choisir une clé WEP statique pour le chiffrement et configurer une clé WEP sur le téléphone.

Remarque

- Lorsque vous utilisez des clés pré-partagées WPA ou WPA2, ces clés doivent être configurées de manière statique sur le téléphone. Ces clés doivent correspondre à celles présentes sur le point d'accès.
- Le téléphone IP Cisco ne prend pas en charge la négociation automatique EAP. Pour utiliser le mode EAP-FAST, vous devez le préciser.

Le tableau suivant liste les modèles d'authentification et de chiffrement configurés sur les points d'accès Cisco Aironet et pris en charge par le téléphone IP Cisco. Ce tableau précise les options de configuration réseau pour le téléphone correspondant à la configuration du point d'accès.

Tableau 28 : Modèles d'authentification et de chiffrement

Configuration du téléphone IP Cisco	**Configuration des points d'accès**			
Mode sécurité	Sécurité	Gestion des clés	Chiffrement	Itinérance rapide
Aucune	Aucune	Aucune	Aucune	S/O
WEP	WEP statique	Statique	WEP	S/O
Clé pré-partagée	Clé pré-partagée	WPA	TKIP	Aucune
		WPA2	AES	FT
EAP-FAST	EAP-FAST	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
EAP-TLS	EAP-TLS	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
PEAP-MSCHAPV2	PEAP-MSCHAPV2	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
PEAP-GTC	PEAP-GTC	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM

Pour plus d'informations sur la configuration des modèles d'authentification et de chiffrement sur les points d'accès, consultez le *Guide de configuration Cisco Aironet* spécifique au modèle et à la version que vous utilisez via l'URL suivante :

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

Configurer le mode d'authentification

Pour sélectionner le mode d'authentification correspondant à ce profil, suivez ces étapes :

Procédure

Étape 1 Choisissez le profil réseau à configurer.

Étape 2 Choisissez le mode d'authentification.

Remarque En fonction de ce que vous avez sélectionné, vous devez configurer des options supplémentaires dans Sécurité sans fil ou Chiffrement sans fil. Pour plus d'informations, reportez-vous à la section Sécurité WLAN, à la page 99.

Étape 3 Cliquez sur **Enregistrer** pour apporter la modification.

Informations d'identification de sécurité sans fil

Lorsque votre réseau utilise EAP-FAST et PEAP pour l'authentification de l'utilisateur, vous devez configurer le nom d'utilisateur et le mot de passe si nécessaire sur le service d'authentification de l'utilisateur à distance (RADIUS) et le téléphone.

Remarque Si vous utilisez des domaines à l'intérieur du réseau, vous devez saisir le nom d'utilisateur avec le nom de domaine au format : *domaine\nomutilisateur*.

Les actions suivantes pourraient entraîner la suppression du mot de passe Wifi existant :

- Entrez un id utilisateur ou un mot de passe non valide
- L'installation d'une autorité de certification racine expirée ou non valide lorsque le type EAP est défini sur PEAP-MSCHAPV2 ou PEAP-GTC
- Désactivation du type EAP sur le serveur RADIUS utilisé par le téléphone avant la modification d'un téléphone pour le nouveau type de protocole EAP

Pour modifier le type de protocole EAP, procédez comme suit dans l'ordre indiqué :

- Activez les nouveaux types EAP sur le RADIUS.
- Modifiez le type EAP sur un téléphone en utilisant le nouveau type de protocole EAP.

Conservez le type EAP actuel configuré sur le téléphone jusqu'à ce que le nouveau type de protocole EAP soit activé sur le serveur RADIUS. Une fois que le nouveau type EAP est activé sur le serveur RADIUS, vous pouvez modifier le type EAP sur le téléphone. Une fois que tous les téléphones ont été modifiés avec le nouveau type de protocole EAP, vous pouvez désactiver le type EAP précédent si vous le souhaitez.

Configurer un nom d'utilisateur et un mot de passe

Pour saisir ou modifier le nom d'utilisateur ou le mot de passe pour le profil réseau, vous devez utiliser la même chaîne nom d'utilisateur et mot de passe que celle configurée dans le serveur RADIUS. Les mots de passe ou les noms d'utilisateur peuvent comprendre un maximum de 64 caractères.

Pour configurer le nom d'utilisateur et le mot de passe dans la zone Informations d'identification Sécurité sans fil, procédez comme suit :

Procédure

Étape 1 Choisissez le profil réseau.
Étape 2 Dans le champ Nom d'utilisateur, saisissez le nom d'utilisateur réseau pour ce profil.
Étape 3 Dans le champ Mot de passe, saisissez le mot de passe réseau pour ce profil.
Étape 4 Cliquez sur **Enregistrer** pour apporter la modification.

Paramétrage de la clé pré-partagée

Consultez les sections suivantes pour vous aider lorsque vous définissez des clés pré-partagées.

Formats de clés prépartagées

Le téléphone IP Cisco prend en charge les formats ASCII et hexadécimaux. Vous devez utiliser l'un de ces formats lorsque vous configurez une clé pré-partagée WPA :

Hexadécimal

Pour les clés hexadécimales, vous saisissez 64 chiffres hexadécimaux (0 à 9 et A à F) ; par exemple, AB123456789CD01234567890EFAB123456789CD01234567890EF3456789C

ASCII

Pour les clés ASCII, vous saisissez une chaîne de caractères qui utilisent les chiffres de 0 à 9 et les lettres de A à Z (majuscules et minuscules), symboles compris, et qui présentent une longueur de 8 à 63 caractères ; par exemple, GREG12356789ZXYW

Configuration d'un PSK

Pour configurer un PSK dans la zone Informations d'identification Sans fil, procédez comme suit :

Procédure

Étape 1 Choisissez le profil réseau qui active la clé pré-partagée WPA ou la clé pré-partagée WPA2.
Étape 2 Dans la zone Type de clé, saisissez la clé appropriée.
Étape 3 Saisissez une chaîne ASCII ou des chiffres hexadécimaux dans le champ Phrase-passe/Clé pré-partagée.
Étape 4 Cliquez sur **Enregistrer** pour apporter la modification.

Chiffrement sans fil

Si votre réseau sans fil utilise un chiffrement WEP et que vous définissez le Mode d'authentification sur Ouvert + WEP, vous devez saisir une clé WEP hexadécimale ou ASCII.

Les clés WEP du téléphone doivent correspondre aux clés WEP attribuées au point d'accès. Le téléphone IP Cisco et les points d'accès Cisco Aironet prennent tous les deux en charge les clés de cryptage 40 bits et 128 bits.

Formats de clé WEP

Vous devez utiliser l'un de ces formats lorsque vous configurez une clé WEP :

Hexadécimal

Four les clés hexadécimales, vous utilisez l'une des tailles de clé suivantes :

40 bits

Vous saisissez une chaîne de clé de cryptage à 10 chiffres qui utilise les chiffres hexadécimaux (0 à 9 et A à F) ; par exemple, ABCD123456.

128 bits

Vous saisissez une chaîne de clé de cryptage à 26 chiffres qui utilise les chiffres hexadécimaux (0 à 9 et A à F) ; par exemple, AB123456789CD01234567890EF.

ASCII

Pour les clés ASCII, vous saisissez une chaîne de caractères qui utilisent les chiffres de 0 à 9 et les lettres de A à Z (majuscules et minuscules) et tous les symboles, avec l'une des tailles de clés suivantes :

40 bits

Vous saisissez une chaîne de 5 caractères ; par exemple, GREG5.

128 bits

Vous saisissez une chaîne de 13 caractères ; par exemple, GREGSSECRET13.

Configuration des clés WEP

Pour configurer des clés WEP, procédez comme suit.

Procédure

Étape 1 Choisissez le profil réseau qui utilise Ouv. + WEP ou Part. + WEP.

Étape 2 Dans la zone Type de clé, saisissez la clé appropriée.

Étape 3 Dans la zone Taille de clé, choisissez l'une de ces longueurs de chaînes de caractères :

- **40**
- **128**

Étape 4 Dans le champ Clé de chiffrement, entrez la chaîne de clé appropriée à partir du Type de clé et de la Taille de clé sélectionnés. Reportez-vous à Formats de clé WEP, à la page 105.

Étape 5 Cliquez sur **Enregistrer** pour apporter la modification.

Exportation d'un certificat d'autorité de certification à partir d'ACS avec les Services de certificats Microsoft

Exportez le certificat de l'autorité de certification racine à partir du serveur ACS. Pour plus d'informations, reportez-vous à la documentation de l'autorité de certification ou RADIUS.

Certificat installé en usine

Cisco a inclus un Certificat installé par l'usine (MIC) dans le téléphone à l'usine.

Pendant l'authentification EAP-TLS, le serveur ACS doit vérifier la confiance du téléphone et le téléphone doit vérifier la confiance du serveur ACS.

Pour vérifier le MIC, le certificat racine de l'usine et le certificat de l'autorité de certification (CA) de l'usine doivent être exportés à partir d'un téléphone IP Cisco et installés sur le serveur Cisco ACS. Ces deux certificats font partie de la chaîne de certificats de confiance utilisée pour vérifier le MIC par le serveur Cisco ACS.

Pour vérifier le serveur Cisco ACS, un certificat secondaire sécurisé (le cas échéant) et un certificat racine (créé à partir d'une autorité de certification) du serveur Cisco ACS doivent être exportés et installés sur le téléphone. Ces certificats font partie de la chaîne de certificats de confiance utilisée pour vérifier la sécurité du certificat à partir du serveur ACS.

Certificat installé par l'utilisateur

Pour utiliser un certificat installé par un utilisateur, une demande de signature de certificat (CSR, Certificate Signing Request) est générée et envoyée à l'Autorité de certification pour approbation. Un certificat utilisateur peut également être généré par l'autorité de certification sans CSR.

Pendant l'authentification EAP-TLS, le serveur ACS vérifie la confiance du téléphone et le téléphone vérifie la confiance du serveur ACS.

Pour vérifier l'authenticité du certificat installé par l'utilisateur, vous devez installer un certificat secondaire de confiance (le cas échéant) et un certificat racine de l'Autorité de certification ayant approuvé le Certificat utilisateur sur le serveur Cisco ACS. Ces certificats font partie de la chaîne de certificats de confiance utilisée pour vérifier la sécurité du certificat installé par l'utilisateur.

Pour vérifier le serveur Cisco ACS, exportez un certificat secondaire sécurisé (le cas échéant) et un certificat racine (créé à partir d'une autorité de certification) sur le serveur Cisco ACS et les certificats exportés sont installés sur le téléphone. Ces certificats font partie de la chaîne de certificats de confiance utilisée pour vérifier la sécurité du certificat à partir du serveur ACS.

Installation de certificats d'authentification EAP-TLS

Pour installer les certificats d'authentification pour EAP-TLS, procédez comme suit :

Procédure

Étape 1 Depuis la page Web du téléphone, réglez la date et l'heure Cisco Unified Communications Manager sur le téléphone.

Étape 2 Si vous utilisez le certificat installé le fabricant (MIC) :

a) Depuis la page Web du téléphone, exportez le certificat racine CA et le certificat fabricant CA.
b) Depuis Internet Explorer, installez les certificats sur le serveur Cisco ACS et modifiez la liste sécurisée.
c) Importation de l'autorité de certification racine vers le téléphone.

Pour obtenir plus d'informations, reportez-vous aux ressources suivantes :

- Exportation et installation de certificats sur ACS, à la page 107
- Exportation d'un certificat d'autorité de certification à partir d'ISE avec les Services de certificats Microsoft, à la page 108

Étape 3 En utilisant l'outil de configuration ACS, configurez le compte utilisateur.

Pour obtenir plus d'informations, reportez-vous aux ressources suivantes :

- Configuration d'un compte utilisateur ACS et installation d'un certificat, à la page 109
- *Guide de l'utilisateur pour téléphone Cisco Secure ACS pour Windows*(http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html)

Définition de la date et de l'heure

EAP-TLS utilise une authentification par certificat qui requiert le bon réglage de l'horloge interne du téléphone IP Cisco. La date et l'heure du téléphone peuvent changer lorsque ce dernier s'enregistre auprès de Cisco Unified Communications Manager.

Remarque Si un nouveau certificat d'authentification de serveur est demandé et que l'heure locale est antérieure à l'heure GMT, il se peut que la validation du certificat d'authentification échoue. Cisco vous recommande de régler les date et heure locales après l'heure GMT.

Pour régler les date et heure locales qui conviennent sur le téléphone, procédez comme suit :

Procédure

Étape 1 Sélectionnez **Date et heure** dans le volet de navigation de gauche.

Étape 2 Si le paramètre du champ Date et heure actuelles du téléphone est différent du champ Date et heure locales, cliquez sur **Configurer le téléphone avec la date et l'heure locales**.

Étape 3 Cliquez sur **Redémarrage du téléphone**, puis cliquez sur **OK**.

Exportation et installation de certificats sur ACS

Pour utiliser le MIC, exportez le certificat racine de l'usine et le certificat de l'autorité de certification (CA) de l'usine, puis installez-les sur le serveur Cisco ACS.

Pour exporter le certificat racine d'usine et le certificat CA d'usine vers le serveur ACS, procédez comme suit :

Procédure

Étape 1 À partir de la page Web du téléphone, choisissez **Certificats**.

Étape 2 Cliquez sur **Exporter** à côté du certificat racine d'usine.

Étape 3 Enregistrez le certificat et copiez-le sur le serveur ACS.

Étape 4 Répétez les étapes 1 et 2 pour le certificat d'Autorité de certification d'usine.

Étape 5 À partir de la page Configuration système du serveur ACS, entrez le chemin de fichier pour chaque certificat, puis installez les certificats.

Remarque Pour plus d'informations sur l'utilisation de l'outil de configuration ACS, consultez l'aide en ligne ACS ou le *Guide de l'utilisateur de Cisco Secure ACS pour Windows*(http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html).

Étape 6 Utilisez la page Modifier la liste de confiance des certificats (CTL) pour ajouter les certificats qui devront être sécurisés par ACS.

Méthodes d'exportation de certificats ACS

Selon le type de certificat que vous exportez depuis ACS, utilisez l'une des méthodes suivantes :

- Pour exporter le certificat d'autorité de certification du serveur ACS ayant signé le certificat installé par l'utilisateur ou le certificat ACS, reportez-vous à Exportation d'un certificat d'autorité de certification à partir d'ISE avec les Services de certificats Microsoft, à la page 108.
- Pour exporter le certificat d'autorité de certification à partir du serveur ACS qui utilise un certificat auto-signé, reportez-vous à Exportation de certificat d'autorité de certification à partir d'ACS avec Internet Explorer, à la page 108.

Exportation d'un certificat d'autorité de certification à partir d'ISE avec les Services de certificats Microsoft

Utilisez cette méthode pour exporter le certificat d'autorité de certification du serveur ISE ayant signé le certificat installé par l'utilisateur ou le certificat ISE.

Pour exporter le certificat d'autorité de certification à l'aide de la page Web Services de certificats Microsoft, procédez comme suit.

Procédure

Étape 1 Sur la page Web Services de certificats Microsoft, sélectionnez **Télécharger un certificat d'Autorité de certification, une chaîne de certificats ou une liste de révocation de certificats**.

Étape 2 À la page suivante, surlignez le certificat d'autorité de certification actuel dans la zone de texte, choisissez DER sous Méthode de codage, puis cliquez sur **Télécharger un certificat de l'Autorité de certification**.

Étape 3 Enregistrez le certificat d'autorité de certification.

Exportation de certificat d'autorité de certification à partir d'ACS avec Internet Explorer

Utilisez cette méthode pour exporter le certificat d'autorité de certification à partir du serveur ACS qui utilise un certificat auto-signé.

Pour exporter des certificats à partir du serveur ACS avec Internet Explorer, procédez comme suit.

Procédure

Étape 1 Dans Internet Explorer, sélectionnez **Outils** > **Options Internet**, puis cliquez sur l'onglet Contenu.

Étape 2 Sous Certificats, cliquez sur **Certificats**, puis sur l'onglet Autorités de certification racines de confiance.

Étape 3 Surlignez le certificat racine, puis cliquez sur **Exporter**. L'Assistant Exportation de certificat s'ouvre.

Étape 4 Cliquez sur **Suivant**.

Étape 5 Dans la fenêtre suivante, sélectionnez **X.509 binaire encodé DER (*.cer)**, puis cliquez sur **Suivant**.

Étape 6 Spécifiez un nom pour le certificat, puis cliquez sur **Suivant**.

Étape 7 Enregistrez le certificat d'autorité de certification à installer sur le téléphone.

Requête et importation d'un certificat installé par l'utilisateur

Pour demander et installer le certificat sur le téléphone, suivez ces étapes.

Procédure

Étape 1 Depuis la page Web du téléphone, sélectionnez le profil réseau utilisant EAP-TLS, puis sélectionnez Installé par l'utilisateur dans le champ Certificat EAP-TLS.

Étape 2 Cliquez sur **Certificats**.

Sur la page Installation d'un certificat utilisateur, le champ Nom commun doit correspondre au nom d'utilisateur dans le serveur ACS.

Remarque Vous pouvez modifier le champ Nom commun si nécessaire. Vérifiez qu'il correspond au nom d'utilisateur dans le serveur ACS. Reportez-vous à Configuration d'un compte utilisateur ACS et installation d'un certificat, à la page 109.

Étape 3 Saisissez les informations à afficher sur le certificat, puis cliquez sur **Soumettre** pour générer la requête CSR (Certificate Signing Request).

Installation du certificat racine du serveur d'authentification

Pour installer le certificat racine du serveur d'authentification sur le téléphone, procédez comme suit.

Procédure

Étape 1 Exportez le certificat racine du serveur d'authentification à partir du ACS. Reportez-vous à Méthodes d'exportation de certificats ACS, à la page 108.

Étape 2 Rendez-vous sur la page Web du téléphone, puis choisissez **Certificats**.

Étape 3 Cliquez sur **Importer** à côté du certificat racine du serveur d'authentification.

Étape 4 Redémarrez le téléphone.

Configuration d'un compte utilisateur ACS et installation d'un certificat

Pour configurer le nom du compte utilisateur et installer le certificat racine MIC pour le téléphone sur le serveur ACS, procédez comme suit :

Remarque Pour plus d'informations sur l'utilisation de l'outil de configuration ACS, consultez l'aide en ligne ACS ou le *Guide de l'utilisateur de Cisco Secure ACS pour Windows*.

Procédure

Étape 1 À partir de la page Configuration des utilisateurs de l'outil de configuration ACS, créez un nom de compte utilisateur de téléphone s'il n'est pas déjà configuré.

En général, le nom d'utilisateur inclut l'adresse MAC du téléphone à la fin. Aucun mot de passe n'est nécessaire pour EAP-TLS.

Remarque Assurez-vous que le nom d'utilisateur correspond au champ Nom commun sur la page Installation du Certificat utilisateur. Reportez-vous à Requête et importation d'un certificat installé par l'utilisateur, à la page 109.

Étape 2 Sur la page Configuration système, à la section EAP-TLS, activez ces champs :

- **Autoriser EAP-TLS**
- **Comparaison CN des certificats**

Étape 3 Sur la page Configuration de l'Autorité de certification ACS, ajoutez le Certificat racine d'usine et le Certificat de l'Autorité de certification d'usine au serveur ACS.

Étape 4 Activez le Certificat racine d'usine et le Certificat de l'Autorité de certification d'usine dans la liste de confiance des certificats ACS.

Paramétrage PEAP

Le protocole EAP (Extensible Authentication Protocol) utilise des certificats clés publics côté serveur pour authentifier les clients en créant un tunnel SSL/TLS chiffré entre le client et le serveur d'authentification.

Le téléphone IP Cisco 8865 ne prend en charge qu'un certificat de serveur qui peut être installé avec SCEP ou par une méthode manuelle, mais pas par les deux méthodes. Le téléphone ne prend pas en charge la méthode TFTP d'installation du certificat.

Remarque La validation du serveur d'authentification peut être activée en important le certificat du serveur d'authentification.

Avant de commencer

Avant de configurer l'authentification PEAP pour le téléphone, assurez-vous que ces conditions préalables requises par Cisco Secure ACS sont remplies :

- Le certificat racine ACS doit être installé.

- Un certificat peut également être installé pour activer la validation du serveur pour PEAP. Mais si un certificat du serveur est installé, la validation du serveur est activée.
- Le paramètre Autoriser EAP-MSCHAPv2 doit être activé.
- Le compte utilisateur et le mot de passe doivent être configurés.
- Pour l'authentification du mot de passe, vous pouvez utiliser la base de données ACS locale ou une base de données externe (comme Windows ou LDAP).

Activation de l'authentification PEAP

Procédure

Étape 1 À partir de la page Web Configuration des téléphones, choisissez le mode d'authentification PEAP.

Étape 2 Saisissez un nom d'utilisateur et un mot de passe.

Sécurité des réseaux locaux sans fil

Les téléphones Cisco qui prennent en charge la Wifi ont des exigences supérieures en matière de sécurité et nécessitent une configuration supplémentaire. Ces étapes supplémentaires comprennent l'installation de certificats et de la configuration de la sécurité sur les téléphones et sur Cisco Unified Communications Manager.

Pour plus d'informations, reportez-vous au *Guide de sécurité de Cisco Unified Communications Manager*.

Page d'administration du téléphone IP Cisco

Les téléphones Cisco qui prennent en charge le Wifi contiennent des pages Web spéciales qui sont différentes des pages des autres téléphones. Vous pouvez utiliser ces pages Web spéciales pour configurer la sécurité du téléphone lorsque le protocole d'enregistrement simple des certificats (SCEP) n'est pas disponible. Utilisez ces pages pour installer manuellement des certificats de sécurité sur un téléphone, pour télécharger un certificat de sécurité, ou pour configurer manuellement l'heure et la date du téléphone.

Ces pages Web affichent également les informations que vous voyez sur les pages Web d'autres téléphones, notamment les informations sur le périphérique, la configuration réseau, les journaux et les statistiques.

Rubriques connexes

Page web du téléphone IP Cisco, à la page 241

Configuration de la Page d'Administration du téléphone

La page web d'administration est activée lorsque le téléphone est livré à partir de l'usine et le mot de passe est défini sur Cisco. Mais si un téléphone est enregistré auprès de Cisco Unified Communications Manager, la page web d'administration doit être activée et un nouveau mot de passe doit être configuré.

Activer cette page web et définir les informations de connexion avant d'utiliser la page web pour la première fois, une fois terminé l'enregistrement du téléphone.

Une fois activée, la page web d'administration est accessible sur le port HTTPS 8443 (`https://x.x.x.x:8443`, x.x.x.x étant une adresse IP de téléphone).

Avant de commencer

Choisissez un mot de passe avant d'activer la page web d'administration. Le mot de passe peut être n'importe quelle combinaison de lettres ou de chiffres, mais doit être comprise entre 8 et 127 caractères.

Votre nom d'utilisateur est défini de manière permanente sur Admin.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone**.

Étape 2 Localiser votre téléphone.

Étape 3 Dans la section **Configuration spécifique au produit**, définissez le paramètre **Web Admin** sur **Activé**.

Étape 4 Saisissez un mot de passe dans le champ **Mot de passe administrateur**.

Étape 5 Sélectionnez **Enregistrer** puis cliquez sur **OK**.

Étape 6 Sélectionnez **Appliquer la configuration** et cliquez sur **OK**.

Étape 7 Redémarrez le téléphone.

Accéder à la page web d'administration du téléphone

Lorsque vous souhaitez accéder aux pages web d'administration, vous devez spécifier le port d'administration.

Procédure

Étape 1 Obtenir l'adresse IP du téléphone :

- Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone**, et localisez le téléphone. Les téléphones qui s'enregistrent auprès de Cisco Unified Communications Manager affichent l'adresse IP dans la fenêtre **Trouver et lister les téléphones** ainsi qu'en haut de la fenêtre **Configuration du téléphone**.
- Sur le téléphone, appuyez sur la touche **Applications**  , choisissez **Informations sur le téléphone**, puis faites défiler jusqu'au champ d'adresse IPv4.

Étape 2 Ouvrez un navigateur Web et saisissez l'URL suivante, dans laquelle *adresse_IP* est l'adresse IP du téléphone IP Cisco :

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

Étape 3 Saisissez le mot de passe dans le champ Mot de passe.

Étape 4 Cliquez sur **Soumettre**.

Installer un certificat utilisateur à partir de la page web d'administration du téléphone

Vous pouvez installer manuellement un certificat utilisateur sur un téléphone si le Protocole d'inscription des certificats simples (SCEP) n'est pas disponible.

Le certificat installé en usine préinstallé (MIC, Manufacturing Installed Certificate) est utilisable en tant que certificat utilisateur pour EAP-TLS.

Après l'installation du certificat utilisateur, vous devez l'ajouter à la liste de confiance du serveur RADIUS.

Avant de commencer

Avant d'installer un certificat utilisateur pour un téléphone, vous devez avoir :

- Un certificat utilisateur enregistré sur votre PC. Le certificat doit être au format PKCS #12.
- Le mot de passe extrait du certificat.

Procédure

Étape 1 À partir de la page web d'administration du téléphone, choisissez **Certificats**.

Étape 2 Localisez le champ installation utilisateur et cliquez sur **Installer**.

Étape 3 Trouvez le certificat sur votre PC.

Étape 4 Dans le champ **Extraire le mot de passe**, saisissez le mot de passe extrait du certificat.

Étape 5 Cliquez sur **Télécharger**.

Étape 6 Redémarrez le téléphone une fois que le téléchargement est terminé.

Installer un certificat du serveur d'authentification à partir de la page web d'administration du téléphone

Vous pouvez installer manuellement un certificat de serveur d'authentification sur un téléphone si le Protocole d'inscription des certificats simples (SCEP) n'est pas disponible.

Le certificat d'autorité de certification racine qui a émis le certificat du serveur RADIUS doit être installé pour EAP-TLS.

Avant de commencer

Avant d'installer un certificat sur un téléphone, vous devez disposer d'un certificat du serveur d'authentification enregistré sur votre PC. Le certificat doit être codé en PEM (Base-64) ou DER.

Procédure

Étape 1 À partir de la page web d'administration du téléphone, choisissez **Certificats**.

Étape 2 Localisez le champ **serveur d'authentification (Page Web d'administration) de l'autorité de certification** et cliquez sur **Installer**.

Étape 3 Trouvez le certificat sur votre PC.

Étape 4 Cliquez sur **Télécharger**.

Étape 5 Redémarrez le téléphone une fois que le téléchargement est terminé.

Si vous installez plus d'un certificat, installez tous les certificats avant de redémarrer le téléphone.

Supprimer manuellement un certificat de sécurité à partir de la page web d'administration du téléphone

Vous pouvez supprimer manuellement un certificat de sécurité à partir d'un téléphone si le Protocole d'inscription des certificats simples (SCEP) n'est pas disponible.

Procédure

Étape 1 À partir de la page web d'administration du téléphone, choisissez **Certificats**.

Étape 2 Localisez le certificat sur la page **Certificats**.

Étape 3 Cliquez sur **Supprimer**.

Étape 4 Redémarrez le téléphone une fois terminé le processus de suppression.

Définir manuellement la date et l'heure du téléphone

Avec l'authentification par certificat, le téléphone doit afficher la date et l'heure. Un serveur d'authentification vérifie la date et l'heure du téléphone par rapport à la date d'expiration du certificat. Si les dates et heures du téléphone et du serveur ne correspondent pas, le téléphone cesse de fonctionner.

Utilisez cette procédure pour saisir manuellement la date et l'heure sur le téléphone si le téléphone ne reçoit pas les informations correctes de votre réseau.

Procédure

Étape 1 À partir de la page web d'administration du téléphone, allez à **Date et heure**.

Étape 2 Effectuez l'une des actions suivantes :

- Cliquez sur **Configurer le téléphone avec la Date et heure locales** pour synchroniser le téléphone avec un serveur local.
- Dans le champ **Spécifier la Date et heure**, sélectionnez le mois, jour, l'année, l'heure, les minutes et secondes, en utilisant les menus et cliquez sur **Configurer le téléphone à une date et heure spécifiques**.

Configuration de SCEP

Le protocole simple d'enregistrement de certificats (SCEP) représente la norme pour la mise à disposition et le renouvellement automatiques de certificats. Il permet d'éviter l'installation manuelle des certificats sur vos téléphones.

Configurer les paramètres de configuration spécifique au produit SCEP

Vous devez configurer les paramètres SCEP suivants sur votre page web du téléphone

- Adresse IP RA
- Empreinte SHA-1 ou SHA-256 du certificat CA de certification racine du serveur SCEP

L'autorité d'inscription (Registration Authority, RA) Cisco IOS fait office de proxy pour le serveur SCEP. Le client SCEP sur le téléphone utilise les paramètres qui sont téléchargés à partir de Cisco Unified

Communications Manager. Après avoir configuré les paramètres, le téléphone envoie une demande `SCEP getcs` à la RA et le certificat racine CA est validé à l'aide de l'empreinte défini.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone**.

Étape 2 Localisez le téléphone.

Étape 3 Faites défiler la page jusqu'à la zone **Configuration spécifique au produit**.

Étape 4 Cochez la case **Serveur SCEP de réseau local sans fil** pour activer le paramètre SCEP.

Étape 5 Cochez la case **Empreinte d'autorité de certification racine de réseau local sans fil (SHA256 ou SHA1)** pour activer le paramètre SCEP QED.

Prise en charge du serveur protocole d'inscription du certificat simple

Si vous utilisez un serveur de protocole d'inscription du certificat simple (SCEP), le serveur peut gérer automatiquement vos certificats d'utilisateur et le serveur. Sur le serveur SCEP, configurez le SCEP Agent d'inscription à :

- Se comporter comme un point de confiance d'infrastructure de clé publique
- Agir en tant qu'infrastructure de clé publique RA
- Réaliser l'authentification du périphérique à l'aide d'un serveur RADIUS

Pour plus d'informations, consultez votre documentation de serveur SCEP.

Authentification 802.1x

Les téléphones IP Cisco prennent en charge l’authentification 802.1X.

Les téléphones IP Cisco et les commutateurs Catalyst Cisco utilisent généralement le protocole de découverte Cisco (CDP) pour s’identifier entre eux et pour déterminer des paramètres tels que l’allocation d’un réseau VLAN et les exigences relatives à l'alimentation en ligne. CDP n’identifie pas localement les postes de travail raccordés. Les téléphones IP Cisco fournissent un mécanisme de connexion directe à EAPOL. Grâce à ce mécanisme, un poste de travail raccordé au téléphone IP Cisco peut faire passer des messages EAPOL à l’authentifiant 802.1X et au commutateur LAN. Le mécanisme de connexion directe assure que le téléphone IP n’agisse pas en tant que commutateur LAN pour authentifier un terminal de données avant d'accéder au réseau.

Les téléphones IP Cisco fournissent également un mécanisme de déconnexion d’EAPOL par proxy. Si l’ordinateur raccordé localement est déconnecté du téléphone IP, le commutateur LAN ne détecte pas l’interruption de la liaison physique, car la liaison entre le commutateur LAN et le téléphone IP est maintenue. Pour éviter de compromettre l’intégrité du réseau, le téléphone IP envoie au commutateur un message EAPOL-Logoff au nom de l’ordinateur en aval, pour que le commutateur LAN efface la valeur d’authentification correspondant à l'ordinateur en aval.

La prise en charge de l’authentification 802.1X requiert plusieurs composants :

- Téléphone IP Cisco : le téléphone envoie la requête d'accès au réseau. Les téléphones IP Cisco contiennent un demandeur 802.1X. Ce demandeur permet aux autoriser de contrôler la connectivité des téléphones

IP aux ports de commutation LAN. La version actuelle du demandeur 802.1X du téléphone utilise les options EAP-FAST et EAP-TLS pour l'authentification réseau.

- Cisco Secure Access Control Server (ACS) (ou un autre serveur d'authentification tiers) : le serveur d'authentification et le téléphone doivent tous deux être configurés avec un secret partagé qui authentifie le téléphone.
- Commutateur Catalyst Cisco (ou commutateur de fabricant tiers) : le commutateur doit prendre en charge 802.1X, pour pouvoir agir en tant qu'authentifiant et transmettre des messages entre le téléphone et le serveur d'authentification. Une fois l'échange terminé, le commutateur accorde ou refuse au téléphone l'autorisation d'accéder au réseau.

Vous devez effectuer les actions suivantes pour configurer 802.1X.

- Configurez les autres composants avant d'activer l'authentification 802.1X sur le téléphone.
- Configure PC Port (Configurer le port PC) : La norme 802.1X ne tenant pas compte des VLAN, il est recommandé qu'un seul périphérique soit authentifié pour un port de commutation donné. Toutefois, certains commutateurs (notamment les commutateurs Catalyst Cisco) prennent en charge l'authentification sur plusieurs domaines. La configuration du commutateur détermine si vous pouvez brancher un ordinateur dans le port PC du téléphone.
  - Activé : si vous utilisez un commutateur qui prend en charge l'authentification sur plusieurs domaines, vous pouvez activer le port PC et y brancher un ordinateur. Dans ce cas, les téléphones IP Cisco prennent en charge la déconnexion d'EAPOL par proxy pour surveiller les échanges d'authentification entre le commutateur et l'ordinateur relié. Pour obtenir plus d'informations sur la prise en charge de la norme IEEE 802.1X sur les commutateurs Catalyst Cisco, reportez-vous aux guides de configuration des commutateurs Catalyst Cisco, disponibles à l'adresse :

    Http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
  - Désactivé : si le commutateur ne prend pas en charge plusieurs périphériques compatibles 802.1X sur le même port, vous devez désactiver le port PC lorsque l'authentification 802.1X est activée. Si vous ne désactivez pas ce port et tentez par la suite d'y raccorder un ordinateur, le commutateur refusera l'accès réseau au téléphone et à l'ordinateur.
- Configure Voice VLAN (Configurer le VLAN voix) : la norme 802.1X ne tenant pas compte des VLAN, vous devez configurer ce paramètre en fonction de la prise en charge du commutateur.
  - Activé : si vous utilisez un commutateur qui prend en charge l'authentification sur plusieurs domaines, vous pouvez continuer à utiliser le VLAN voix.
  - Désactivé : si le commutateur ne prend pas en charge l'authentification sur plusieurs domaines, désactivez le VLAN voix et envisagez d'affecter le port à un VLAN natif.

Accéder à l'authentification 802.1X

Vous pouvez accéder aux paramètres d'Authentification 802.1X en procédant comme suit :

Procédure

Étape 1 Appuyez sur **Applications** .

Étape 2 Choisissez **Param. Admin** > **Paramétrage de sécurité** > **Authentification 802.1x**

Étape 3 Configurez les options comme décrit dans la section Options d'authentification 802.1X, à la page 117.

Étape 4 Pour quitter ce menu, appuyez sur **Quitter**.

Options d'authentification 802.1X

Le tableau suivant décrit les options d'authentification 802.1X :

Tableau 29 : Paramètres d'authentification 802.1X

Option	Description	Pour modifier
Auth. périphérique	Détermine si l'authentification 802.1X est activée : • Activé : le téléphone utilise l'Authentification 802.1x pour demander l'accès réseau. • Désactivé : paramètre par défaut. Le téléphone utilise CDP pour obtenir un accès réseau et VLAN.	Reportez-vous à Définition de l'o périphérique, à la page 117.
État transaction	État : affiche l'état de l'Authentification 802.1x : • Déconnecté : indique que l'Authentification 802.1x n'est pas configurée sur le téléphone. • Authentifié : indique que le téléphone est authentifié. • En attente : indique que le processus d'authentification est en cours. Protocole : affiche la méthode EAP utilisée pour l'Authentification 802.1x (il peut s'agir du protocole EAP-FAST ou EAP-TLS).	Affichage uniquement. Ne peut p configuré.

Définition de l'option Auth. périphérique

Procédure

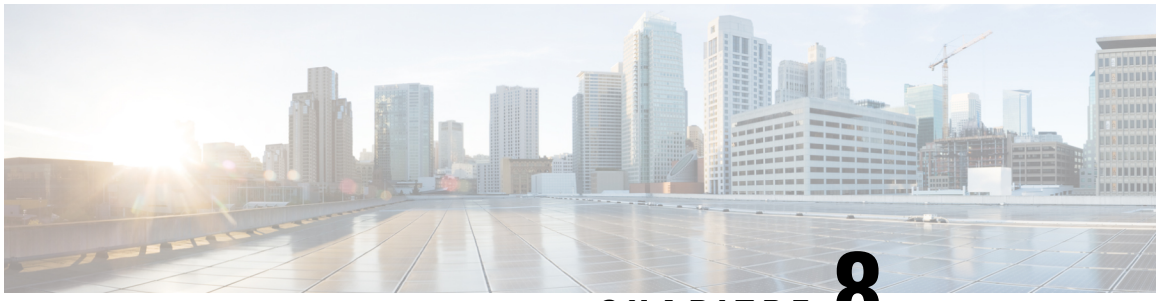
Étape 1 Appuyez sur **Applications** .

Étape 2 Choisissez **Paramètres admin** > **Paramétrage de sécurité** > **Authentification 802.1X**

Étape 3 Définissez l'option Auth. périphérique :

- **Oui**
- **Non**

Étape 4 Appuyez sur **Appliquer**.



CHAPITRE 8

Personnalisation du téléphone IP Cisco

Sonneries personnalisées

Le téléphone est fourni avec trois sonneries implémentées dans le matériel : Soleil, Compression d'impulsions, Compression d'impulsions 1.

Cisco Unified Communications Manager fournit aussi un ensemble par défaut de sonneries téléphoniques supplémentaires implémentées dans le logiciel sous forme de fichiers de modulation par impulsions et codage (PCM). Les fichiers MIC, ainsi qu'un fichier XML (appelé Ringlist-wb.xml) décrivant les options de liste de sonneries qui sont disponibles sur votre site, figurent dans le répertoire TFTP de chaque serveur Cisco Unified Communications Manager.

Attention Tous les noms de fichier respectent la casse. Si vous utilisez Ringlist-wb.xml comme nom de fichier, le téléphone n'appliquera pas vos changements.

Pour plus d'informations, consultez le chapitre « Sonneries et fonds d'écran personnalisés du téléphone », du Guide de Configuration des fonctionnalités de Cisco Unified Communications Manager pour téléphone Cisco Unified Communications Manager version 12.0 (1) ou version ultérieure.

Images d'arrière-plan personnalisées

Vous pouvez personnaliser un téléphone IP Cisco avec une image de fond ou un fond d'écran. Les fonds d'écran personnalisés sont un moyen courant d'afficher des logos d'entreprise ou des images, et de nombreuses entreprises les utilisent pour mettre en valeur leurs téléphones.

Depuis la version 12.7(1) du micrologiciel, vous pouvez personnaliser les fonds d'écran à la fois sur les téléphones et les modules d'extension de touches. Mais vous avez besoin d'une image pour le téléphone et d'une image pour le module d'extension.

Le téléphone analyse la couleur de votre fond d'écran et modifie la couleur de la police et des icônes de manière à ce qu'elles puissent être lues. Si votre fond d'écran est sombre, le téléphone modifie les polices et les icônes en blancs. Si votre fond d'écran est clair, le téléphone affiche les polices et les icônes en noir.

Il est préférable de choisir une image simple, par exemple une couleur unie ou un motif pour votre arrière-plan. Évitez les images à contraste élevé.

Vous pouvez ajouter un fond d'écran personnalisé de l'une des deux manières suivantes :

- Utilisez le fichier de liste
- À l'aide d'un profil de téléphone commun

Si vous souhaitez que l'utilisateur puisse sélectionner votre image à partir des différents fonds d'écran disponibles sur le téléphone, modifiez le fichier de liste. Mais si vous souhaitez envoyer l'image au téléphone, créez ou modifiez un profil de téléphone commun existant.

Quelle que soit l'approche, notez les éléments suivants :

- Vos images doivent être au format PNG et les dimensions de la taille totale de l'image doivent être inférieures ou égales aux dimensions suivantes :
  - Miniatures d'image 139 pixels (longueur) X 109 pixels (hauteur).
  - Téléphone IP Cisco série 8800 : 800 pixels par 480 pixels
  - Module d'extension de touches pour téléphone IP Cisco 8851 et 8861 avec deux écrans LCD : 320 par 480 pixels
  - Module d'extension de touches pour téléphone IP Cisco avec deux écrans LCD : 320 par 480 pixels
  - Module d'extension de touches pour téléphone IP Cisco 8800 avec un seul écran LCD : 272 x 480 pixels
- Téléchargez les images, les miniatures et le fichier de liste sur le serveur TFTP. Le répertoire est :
  - Téléphone IP Cisco série 8800 : Desktops/800x480x24
  - Module d'extension de touches pour téléphone IP Cisco 8851 et 8861 avec deux écrans LCD : Postes de travail/320 par 480 pixels
  - Module d'extension de touches pour téléphone IP Cisco 8865 avec deux écrans LCD : Desktops/320x480x24
  - Module d'extension de touches pour téléphone IP Cisco 8800 avec un seul écran LCD : Desktops/272x480x24

  Redémarrez le serveur TFTP une fois que le téléchargement est effectué.
- Si vous ne souhaitez pas que les utilisateurs sélectionnent leur propre fond d'écran, désactivez **Activer l'accès au paramètre Image d'arrière-plan du téléphone à l'utilisateur final**. Enregistrez et appliquez le profil du téléphone. Redémarrez les téléphones afin que vos modifications soient prises en compte.

Remarque Vous pouvez appliquer des images d'arrière-plan du téléphone en masse avec le **profil de téléphone commun**. Mais la configuration en masse nécessite que vous désactiviez la **Activer l'accès de l'utilisateur final au paramètre image d'arrière-plan du téléphone**. Pour plus d'informations sur la configuration en masse des images d'arrière-plan, reportez-vous au chapitre « Configurer le profil de téléphone commun » des Meilleures pratiques relatives aux papiers peints personnalisés pour les téléphones IP Cisco série 8800 .)

Pour plus d'informations sur la personnalisation du fond d'écran, consultez la documentation suivante :

- Meilleures pratiques relatives aux papiers peints personnalisés pour les téléphones IP Cisco série 880).
- « Sonneries et fonds d'écran personnalisés du téléphone », du Guide de Configuration des fonctionnalités de Cisco Unified Communications Manager pour téléphone Cisco Unified Communications Manager version 12.0 (1) ou version ultérieure.
- Reportez-vous au chapitre « Paramètres » du *Guide de l'utilisateur des téléphones IP Cisco série 8800*.

Configuration du codec large bande

Le codec G.722 est activé par défaut pour le téléphone IP Cisco. Si Cisco Unified Communications Manager est configuré pour utiliser G.722 et si le terminal éloigné prend en charge G.722, alors l'appel est connecté en utilisant le codec G.722 au lieu du G.711.

Cette situation a lieu que l'utilisateur ait activé ou non un casque ou combiné large bande. Cependant, si le casque ou le combiné est activé, il est possible que l'utilisateur perçoive une plus grande sensibilité audio pendant l'appel. Si la sensibilité accrue est la conséquence d'une optimisation de la clarté sonore, elle signifie aussi que davantage de bruit ambiant peut être entendu sur le terminal distant, notamment lorsque du papier est froissé ou qu'une conversation est en cours en arrière-plan. Même sans casque ou combiné large bande, certains utilisateurs peuvent trouver gênante la sensibilité accrue du G.722. D'autres utilisateurs peuvent apprécier la sensibilité accrue du G.722.

Le paramètre de service Publier les codecs G.722 et iSAC influe sur la prise en charge de la téléphonie large bande pour tous les périphériques enregistrés auprès du serveur Cisco Unified Communications Manager ou pour un téléphone spécifique, selon la fenêtre Cisco Unified Communications Manager Administration dans laquelle le paramètre est configuré.

Procédure

Étape 1 Pour configurer la prise en charge de la téléphonie large bande sur tous les périphériques :

a) Depuis Cisco Unified Communications Manager Administration, sélectionnez **Système** > **Paramètres d'entreprise**

b) Configuration du champ Publier les codecs G.722 et iSAC

La valeur par défaut de ce paramètre d'entreprise est **Vrai**, ce qui signifie que tous les modèles de téléphone IP Cisco enregistrés sur Cisco Unified Communications Manager publient le codec G.722 sur Cisco Unified Communications Manager. Si chaque terminal impliqué dans la tentative d'appel prend en

charge G.722 dans l'ensemble de fonctionnalités, Cisco Unified Communications Manager choisit ce codec pour l'appel chaque fois que cela est possible.

Étape 2 Pour configurer la prise en charge de la téléphonie large bande sur un périphérique précis :

a) Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone**.

b) Configurez le paramètre Publier les codecs G.722 et iSAC dans le menu Configuration spécifique au produit.

Par défaut, ce paramètre spécifique à un produit utilise la valeur indiquée par le paramètre d'entreprise. Si vous souhaitez modifier ce paramètre de manière individuelle pour les téléphones, sélectionnez **Activé** ou **Désactivé**.

Configuration de l'affichage d'un message d'inactivité

Vous pouvez configurer l'affichage d'un message d'inactivité (texte seulement ; la taille du fichier texte ne doit pas excéder 1 Mo) qui apparaît à l'écran du téléphone. L'affichage du message d'inactivité est un service XML que le téléphone requiert lorsqu'il est inactif (pas utilisé) pendant une période de temps donnée et qu'aucun menu de fonctions n'est ouvert.

Pour obtenir des instructions détaillées sur la création et l'affichage d'un message d'inactivité, consultez *Creating Idle URL Graphics on Cisco IP Phone* (Création de graphiques d'URL d'inactivité sur le téléphone IP Cisco) à l'adresse suivante :

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

De plus, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager pour les informations suivantes :

- Spécification de l'URL du service XML d'affichage de message d'inactivité :
  - Pour un téléphone unique : champ Inactif dans la fenêtre Configuration du téléphone de Cisco Unified Communications Manager Administration.
  - Pour plusieurs téléphones simultanément : champ URL d'inactivité de la fenêtre Configuration des paramètres d'entreprise, ou champ Inactif de l'outil d'administration globale (BAT).
- Spécification de la durée pendant laquelle le téléphone est inutilisé avant l'invocation du service XML d'affichage d'inactivité :
  - Pour un téléphone unique : champ Idle Timer (Minuteur d'inactivité) dans la fenêtre Configuration du téléphone de Cisco Unified Communications Manager Administration.
  - Pour plusieurs téléphones simultanément : champ Durée inactivité URL de la fenêtre Configuration des paramètres d'entreprise, ou champ Durée d'inactivité de l'outil d'administration globale (BAT).

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone**.

Étape 2 Dans le champ Inactif, saisissez l'URL du service XML d'affichage du message d'inactivité.

Étape 3 Dans le champ Durée d'inactivité, saisissez le délai devant s'écouler avant que le service XML d'affichage du message d'inactivité s'affiche sur le téléphone inactif.

Étape 4 Sélectionnez **Enregistrer**.

Personnaliser la tonalité

Vous pouvez configurer vos téléphones afin que les utilisateurs puissent entendre des tonalités différentes pour les appels internes et externes. En fonction de vos besoins, vous pouvez choisir entre trois options de tonalité :

- Valeur par défaut : une tonalité différente pour les appels internes et externes.
- Interne : la tonalité interne est utilisée pour tous les appels.
- Externe : la tonalité externe est utilisée pour tous les appels.

Toujours utiliser la tonalité est un champ obligatoire de Cisco Unified Communications Manager.

Procédure

Étape 1 Dans Cisco Unified Communications Manager, sélectionnez **Système** > **Paramètres de service**.

Étape 2 Sélectionnez le serveur de votre choix.

Étape 3 Sélectionnez **Cisco CallManager** en tant que service.

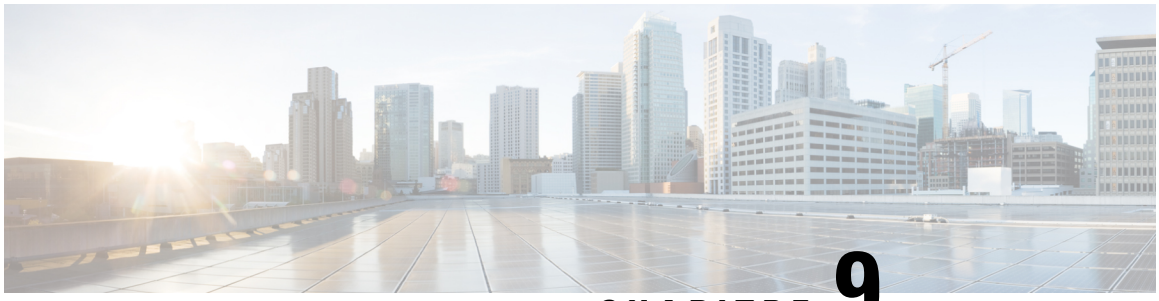
Étape 4 Faites défiler la page jusqu'au volet relatif aux paramètres.

Étape 5 Définir **Toujours utiliser la tonalité** sur l'une des actions suivantes :

- Externe
- Interne
- Par défaut

Étape 6 Sélectionnez **Enregistrer**.

Étape 7 Redémarrez vos téléphones.



CHAPITRE 9

Fonctionnalités et configuration du téléphone

Présentation des fonctionnalités et configuration du téléphone

Après avoir installé des téléphones IP Cisco sur le réseau, après avoir configuré leurs paramètres réseau et après les avoir ajoutés à Cisco Unified Communications Manager, vous devez utiliser l'application Cisco Unified Communications Manager Administration pour configurer les fonctions de téléphonie, éventuellement modifier les modèles de téléphone, configurer les services et attribuer des utilisateurs.

Vous pouvez modifier des paramètres supplémentaires pour le téléphone IP Cisco à partir de Cisco Unified Communications Manager Administration. Utilisez cette application Web pour configurer les critères d'enregistrement de téléphone et les espaces de restriction d'appels, pour configurer les répertoires d'entreprise et les services, ainsi que pour modifier les modèles de bouton de téléphone, entre autres tâches.

Lors de l'ajout des fonctionnalités aux touches de ligne téléphonique, vous êtes limité par le nombre de touches de ligne disponibles. Vous ne pouvez pas ajouter plus de fonctionnalités que le nombre de touches de ligne sur votre téléphone.

Assistance pour les utilisateurs de téléphones IP Cisco

Si vous êtes administrateur système, vous êtes probablement la principale source d'informations des utilisateurs de téléphone IP Cisco de votre réseau ou de votre société. Il est important de fournir aux utilisateurs finaux des informations précises et à jour.

Pour utiliser efficacement certaines fonctionnalités des téléphones IP Cisco (notamment la numérotation rapide, les services et les options du système de messagerie vocale), les utilisateurs doivent recevoir des informations de votre part ou de l'équipe en charge du réseau, ou être en mesure de vous contacter pour obtenir de l'aide. Prenez soin de communiquer aux utilisateurs le nom des personnes à contacter pour obtenir de l'aide, et les instructions nécessaires pour les contacter.

Nous vous recommandons de créer sur votre site d'assistance interne, une page Web sur laquelle les utilisateurs finaux pourront consulter les informations importantes sur leurs téléphones IP Cisco.

Pensez à inclure les informations suivantes sur ce site :

- Les guides de l'utilisateur de tous les modèles de téléphone IP Cisco que vous prenez en charge
- Des informations sur l'accès au portail d'aide en libre-service Cisco Unified Communications
- La liste des fonctionnalités prises en charge
- Le guide de l'utilisateur ou le guide de référence rapide de votre système de messagerie vocale

Fonctionnalités du téléphone

Après avoir ajouté des téléphones IP Cisco dans Cisco Unified Communications Manager, vous pouvez ajouter des fonctionnalités aux téléphones. Le tableau suivant présente la liste des fonctionnalités de téléphonie prises en charge ; nombreuses d'entre elles peuvent être configurées à l'aide de Cisco Unified Communications Manager Administration.

Pour obtenir des informations sur l'utilisation de la plupart de ces fonctionnalités sur le téléphone, reportez-vous au *Guide de l'utilisateur des téléphones IP Cisco série 8800*. Reportez-vous à la section Boutons de fonctions et touches programmables, à la page 145 pour obtenir la liste des fonctionnalités pouvant être configurées en tant que boutons programmables, touches programmables dédiées et boutons de fonction.

Remarque Cisco Unified Communications Manager Administration met également à votre disposition plusieurs paramètres de service que vous pouvez utiliser pour configurer différentes fonctions de téléphonie. Pour obtenir des informations sur l'accès des paramètres de service et leur configuration, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Pour plus d'informations sur les fonctions d'un service, sélectionnez le nom du paramètre ou le bouton d'aide **point d'interrogation (?)** dans la fenêtre Configuration spécifique au produit.

Pour plus d'informations, reportez-vous à la documentation relative à votre version particulière de Cisco Unified Communications Manager.

Fonctionnalité	Description et informations supplémentaires
Numérotation abrégée	Permet aux utilisateurs de composer rapidement un numéro de téléphone en entrant un code d'index affecté (1 à 199) sur le clavier du téléphone. **Remarque** Vous pouvez utiliser la numérotation abrégée lorsque le combiné est raccroché ou lorsqu'il est décroché. Les utilisateurs peuvent affecter des codes d'index à partir du portail d'aide en libre-service.
Alerte d'appel entrant actionnable	Fournit diverses options permettant de contrôler les alertes d'appel entrant. Vous pouvez désactiver ou activer l'alerte d'appel. Vous pouvez aussi activer ou désactiver l'affichage de l'ID de l'appelant. Reportez-vous à Alerte d'appel entrant actionnable, Configuration spécifique au produit, à la page 149.
Prise en charge du chiffrement AES 256 pour les téléphones	Renforce la sécurité grâce à la prise en charge de TLS 1.2 et de nouveaux codages. Pour obtenir plus d'informations, reportez-vous à Fonctionnalités de sécurité prises en charge, à la page 90.
Message d'accueil de l'agent	Permet à un agent de créer et de mettre à jour un message d'accueil préenregistré émis au début d'un appel de client, avant le début de la conversation entre l'agent et l'appelant. L'agent peut préenregistrer un seul message d'accueil ou plusieurs si nécessaire. Reportez-vous à la section Activer le message d'accueil de l'agent, à la page 178.
Interception de tous les appels	Permet aux utilisateurs d'intercepter un appel sur n'importe quelle ligne de leur groupe d'interception d'appel, quel que soit son mode d'acheminement vers le téléphone. Pour plus d'informations sur l'interception d'appels, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Règles de numérotation de l'application	Convertissent les numéros de contacts mobiles partagés en numéros composables via le réseau. Reportez-vous à la section Règles de numérotation de l'application, à la page 82.
Parcage d'appels dirigé assisté	Permet aux utilisateurs de parquer un appel en appuyant sur un seul bouton, grâce à la fonctionnalité de parcage direct. Les administrateurs doivent configurer un bouton de fonction de supervision de ligne occupée (FLO)Parcage d'appel dirigé assisté. Lorsque les utilisateurs appuient sur un bouton de supervision de ligne occupée (FLO)Parcage d'appel dirigé assisté d'un appel actif, l'appel actif est parqué à l'emplacement de parcage direct associé au boutonParcage d'appel dirigé assisté. Pour plus d'informations sur le parcage d'appels, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Indicateur d'attente de message audible (IAMA)	Une tonalité saccadée dans le combiné, le casque ou le haut-parleur indique à l'utilisateur qu'il a un ou plusieurs messages vocaux sur une ligne. **Remarque** La tonalité saccadée est propre à la ligne. Vous ne l'entendez que si vous utilisez la ligne associée aux messages en attente.

Fonctionnalité	Description et informations supplémentaires
Réponse automatique	Prend automatiquement les appels entrants après une sonnerie ou deux. La réponse automatique fonctionne avec le haut-parleur ou le casque. Pour obtenir des informations sur les numéros de répertoire, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.
Synchronisation des ports automatiques	Synchronise les ports à la vitesse minimale entre les ports d'un téléphone pour supprimer la perte de paquets. Reportez-vous à Synchronisation automatique des ports, Configuration spécifique au produit, à la page 149.
Interception auto	Permet à l'utilisateur d'utiliser la fonction d'interception par simple effleurement pour les fonctionnalités d'interception d'appels. Pour plus d'informations sur l'interception d'appels, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Insertion	Permet à l'utilisateur de s'insérer dans un appel en établissant une conférence téléphonique à trois participants, à l'aide du pont de conférence intégré du téléphone cible. Voir « InsConf » dans le tableau suivant.
Blocage du transfert externe à externe	Empêche les utilisateurs de transférer un appel externe à un autre numéro externe. Pour plus d'informations sur le transfert d'appels externes, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Connexions multiples Bluetooth	Permet à l'utilisateur d'associer plusieurs périphériques au téléphone. L'utilisateur peut alors connecter en même temps un appareil mobile par Bluetooth ainsi qu'un casque Bluetooth. Le téléphone IP Cisco 8851NR ne prend pas en charge Bluetooth.
Fonction de supervision de ligne occupée (FLO)	Permet à l'utilisateur de surveiller l'état des appels d'un numéro de répertoire associé à un bouton de numérotation abrégée du téléphone. Pour obtenir des informations sur la présence, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.
Interception - Supervision de ligne occupée (FLO)	Permet d'améliorer la numérotation abrégée FLO. Permet de configurer un numéro de répertoire sur lequel l'utilisateur peut surveiller les appels entrants. Lorsque le numéro de répertoire reçoit un appel entrant, le système avertit l'utilisateur qui surveille les appels, afin que celui-ci puisse intercepter l'appel. Pour plus d'informations sur l'interception d'appels, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Rappel automatique	Déclenche une alerte sonore et visuelle sur le téléphone des utilisateurs lorsqu'un correspondant occupé ou indisponible devient disponible. Pour plus d'informations sur le rappel, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.

Fonctionnalité	Description et informations supplémentaires
Restrictions relatives à l'affichage des appels	Détermine quelles informations seront affichées pour les lignes d'appel ou connectées, selon les parties qui interviennent lors de l'appel. Pour plus d'informations sur l'organisation du routage et les restrictions sur l'affichage des appels, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Renvoi d'appel	Permet aux utilisateurs de rediriger les appels entrants vers un autre numéro. Les options de renvoi d'appels incluent Renvoyer tout, Renvoi si occupé, Renvoi si sans réponse et Renvoi si pas de couverture. Pour plus d'informations sur les numéros de répertoire, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager ainsi que Personnalisation de l'affichage du portail d'aide en libre-service, à la page 86.
Interruption des boucles de renvoi de tous les appels	Détecte et empêche les boucles Renvoyer tout. Lorsqu'une boucle Renvoyer tout est détectée, la configuration du renvoi de tous les appels est ignorée et l'appel sonne.
Prévention des boucles de renvoi de tous les appels	Détecte et empêche les boucles Renvoyer tout. Lorsqu'une boucle Renvoyer tout est détectée, la configuration du renvoi de tous les appels est ignorée et l'appel sonne.
Affichage configurable du renvoi d'appels	Empêche l'utilisateur de configurer une destination pour le Renvoi de tous les appels directement sur le téléphone, ce qui créerait une boucle ou une chaîne de Renvoi de tous les appels ayant plus de sauts que permis par le paramètre de service Nombre maximal de sauts de renvoi. Pour obtenir des informations sur les numéros de répertoire, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.
Remplacement de la destination du renvoi d'appel	Permet de remplacer le paramètre Renvoi tous appels lorsque la cible de cette option redirige un appel vers l'initiateur de renvoi de tous les appels. Cette fonctionnalité permet à la cible du renvoi de tous les appels de joindre l'initiateur du renvoi de tous les appels en cas d'appel important. Le remplacement est effectué que le numéro de téléphone de la cible du renvoi de tous les appels soit interne ou externe. Pour plus d'informations sur le numéro de répertoire, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Notification de renvoi d'appel	Permet de configurer les informations que l'utilisateur voit lorsqu'il reçoit un appel renvoyé. Reportez-vous à la section Configuration de la notification de renvoi d'appel, à la page 180.
Historique des appels pour ligne partagée	Permet de visualiser l'activité des lignes partagées dans l'historique des appels du téléphone. Cette fonctionnalité permet de : • Journaliser les appels en absence d'une ligne partagée • Journaliser tous les appels pris et passés sur une ligne partagée

Fonctionnalité	Description et informations supplémentaires
Parcage d'appel	Permet aux utilisateurs de parquer (stocker temporairement) un appel, puis de le récupérer sur un autre téléphone du système Cisco Unified Communications Manager. Vous pouvez configurer le champ **Dédier une ligne pour le parcage d'appels** dans le volet **Présentation de la configuration spécifique du produit** pour parquer l'appel sur la ligne d'origine ou une ligne différente. Lorsque le champ est activé, l'appel parqué demeure sur la ligne de l'utilisateur et ce dernier peut utiliser la touche programmable **Reprendre** pour reprendre l'appel. L'utilisateur voit le numéro de poste de l'appel parqué sur l'écran du téléphone. Lorsque le champ est désactivé, l'appel parqué est transféré à la ligne du parc d'appels. La ligne de l'utilisateur revient à l'état inactif et ce dernier peut voir le numéro de poste du parc d'appels dans une fenêtre contextuelle. L'utilisateur compose le numéro de poste pour prendre l'appel. Pour plus d'informations sur le parcage d'appels, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Interception d'appel	Permet aux utilisateurs de rediriger vers leur téléphone, un appel qui sonne sur un autre téléphone de leur groupe d'interception d'appel. Vous pouvez configurer une alerte sonore et visuelle pour la ligne principale du téléphone. Cette alerte avertit les utilisateurs qu'un appel sonne dans leur groupe d'interception d'appel. Pour plus d'informations sur l'interception d'appels, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Enregistrement d'appel	Permet à un superviseur d'enregistrer un appel actif. L'utilisateur peut entendre une tonalité d'alerte sonore lors d'un appel qui est enregistré. Lorsqu'un appel est sécurisé, une icône en forme de verrou indique l'état de sécurité de l'appel sur les téléphones IP Cisco. Les parties connectées peuvent également entendre une tonalité d'alerte sonore indiquant que l'appel est sécurisé et qu'il est en cours d'enregistrement. **Remarque** Lors de la surveillance ou de l'enregistrement d'un appel actif, l'utilisateur peut recevoir ou passer des appels Intercom ; toutefois, s'il passe un appel Intercom, l'appel actif est mis en attente, ce qui entraîne l'interruption de l'enregistrement et la suspension de la surveillance. Pour reprendre la surveillance, la partie dont l'appel est surveillé doit reprendre l'appel. Pour plus d'informations sur la surveillance et l'enregistrement, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Appel en attente	Indique (et permet aux utilisateurs de prendre) un appel entrant qui sonne pendant que l'utilisateur est en ligne. Les informations sur l'appel entrant sont affichées sur l'écran du téléphone. Pour plus d'informations sur le numéro de répertoire, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.

Fonctionnalité	Description et informations supplémentaires
Sonnerie d'appel en attente	Permet aux utilisateurs de la mise en attente de configurer une sonnerie au lieu du bip standard. Les options sont Sonnerie et Sonner une fois. Pour obtenir des informations sur les numéros de répertoire, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.
Afficher l'ID de l'appelant	L'identification de l'appelant, telle que son numéro de téléphone, son nom ou un texte descriptif, est affichée sur l'écran du téléphone. Pour plus d'informations sur l'organisation du routage, les restrictions sur l'affichage des appels et les numéros de répertoire, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Blocage de l'ID de l'appelant	Permet à l'utilisateur de bloquer l'affichage de son numéro de téléphone ou de son adresse e-mail sur les téléphones sur lesquels l'identification de l'appelant est activée. Pour plus d'informations sur l'organisation du routage et les numéros de répertoire, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Normalisation de l'appelant	La normalisation de l'appelant présente à l'utilisateur les appels téléphoniques avec un numéro de téléphone composable. Les éventuels codes d'échappement sont ajoutés aux numéros, afin que l'utilisateur puisse aisément rappeler l'appelant. Le numéro composable est enregistré dans l'historique des appels et peut être enregistré dans le Carnet d'adresses personnel.
CAST pour SIP	Établit la communication entre Cisco Unified Video Advantage (CUVA) et les téléphones IP Cisco, pour prendre en charge la vidéo sur l'ordinateur même si le téléphone IP n'est pas équipé de la vidéo.
Insertion	Permet à un utilisateur de s'insérer dans un appel non privé sur une ligne téléphonique partagée. cBarge ajoute un utilisateur à un appel et le convertit en téléconférence, ce qui permet à cet utilisateur et aux autres tiers d'accéder aux fonctionnalités de téléconférence. La téléconférence est créée grâce à la fonctionnalité pont de conférence du Cisco Unified Communications Manager. Vous devez activer la touche programmable et la fonctionnalité de pont de conférence pour que cInser fonctionne correctement. Dans les Firmware version 10.2(2) et ultérieures, la fonctionnalité cBarge est accessible via la touche programmable Insertion. Pour plus d'informations, reportez-vous au chapitre « Insertion », Guide de Configuration des fonctionnalités de Cisco Unified Communications Manager.
Charger un périphérique mobile	Permet à un utilisateur de charger un appareil mobile en le connectant au port USB du téléphone IP Cisco. Reportez-vous au *Guide de l'utilisateur des téléphones IP Cisco série 8800* .

Fonctionnalité	Description et informations supplémentaires
Cisco Extension Mobility	Permet aux utilisateurs l'accès à la configuration de leur téléphone IP Cisco telles que la vitesse, des services et des apparences de ligne se compose à partir d'un téléphone IP Cisco partagé. Cisco Extension Mobility peut être utile pour les personnes qui travaillent à différents endroits dans l'entreprise, ou qui partagent un espace de travail avec des collègues.
Cisco Extension Mobility Cross Cluster (EMCC)	Permet aux utilisateurs configurés dans un cluster de se connecter à un téléphone IP Cisco membre d'un autre cluster. Les utilisateurs d'un cluster domestique se connectent à un téléphone IP Cisco membre d'un cluster visiteur. **Remarque** Configurez Cisco Extension Mobility sur les téléphones IP Cisco avant de configurer EMCC.
Cisco IP Manager Assistant (IPMA)	Propose des fonctions de routage et d'autres fonctions de gestion d'appels pour aider les managers et les assistants à traiter les appels téléphoniques plus efficacement. Reportez-vous à la section Configurer Cisco IP Manager Assistant, à la page 195.
Module d'extension de touches pour téléphone Cisco IP Phone 8800 Module d'extension de touches pour téléphone Cisco IP Phone 8851/8861 Module d'extension de touches pour téléphone Cisco IP Phone 8865	Fournit des touches supplémentaires en ajoutant un module d'extension au téléphone. Pour des informations supplémentaires sur l'installation d'accessoires, consultez le *Guide des accessoires des téléphones IP Cisco série 7800 et 8800 pour téléphone Cisco Unified Communications Manager*.
Téléphone IP Cisco 8811 Assistance	Prend en charge le Téléphone IP Cisco 8811.
Assistance du téléphone IP Cisco 8851NR	Fournit une assistance pour le téléphone IP Cisco 8851NR
Négociation de la version de Cisco Unified Communications Manager Express (Unified CME)	Cisco Unified Communication Manager Express utilise une balise spéciale dans les informations envoyées au téléphone pour qu'il s'identifie. Grâce à cette balise, le téléphone peut fournir à l'utilisateur des services pris en charge par le commutateur. Reportez-vous à : • *Guide de l'administrateur système Cisco Unified Communications Manager Express* • Interaction avec Cisco Unified Communications Manager Express, à la page 23
Cisco Unified Video Advantage (CUVA)	Permet aux utilisateurs de passer des appels vidéo en utilisant un téléphone IP Cisco, un PC et une caméra. **Remarque** Configurez les paramètres de fonctionnalités vidéo dans la section Product Specific Configuration Layout (Disposition de la configuration spécifique au produit) de la page Phone Configuration (Configuration du téléphone). Reportez-vous à la documentation de Cisco Unified Video Advantage.
Cisco WebDialer	Permet aux utilisateurs de passer des appels à partir d'applications Internet ou de bureau.

Fonctionnalité	Description et informations supplémentaires
Sonnerie classique	Prend en charge les sonneries incorporées dans le micrologiciel du téléphone ou téléchargées depuis le Cisco Unified Communications Manager. Cette fonction a pour effet de rendre communes les sonneries disponibles avec les autres téléphones IP Cisco Reportez-vous à la section Sonneries personnalisées, à la page 119.
Conférence	Permet aux utilisateurs de parler simultanément avec plusieurs interlocuteurs, en appelant individuellement chaque participant. Les fonctionnalités de conférence incluent Conférence et MultConf. Permet à un participant non initiateur d'une conférence standard (ad hoc) d'ajouter ou de supprimer des participants. Cela permet aussi à n'importe quel participant de la conférence de fusionner deux conférences standard sur la même ligne. Ces fonctionnalités peuvent être activées à l'aide du paramètre de service Advance Adhoc Conference (Conférence ad hoc avancée), qui est désactivé par défaut dans Cisco Unified Communications Manager Administration. **Remarque** Si ces fonctionnalités sont activées, veillez à en informer vos utilisateurs.
Energy Efficient Ethernet (EEE) configurable pour PC et port de commutation	Permet de contrôler les fonctions EEE d'un port d'ordinateur personnel et d'un port de commutation, en activant ou en désactivant EEE. La fonctionnalité contrôle les deux types de ports individuellement. La valeur par défaut est Activé. Reportez-vous à la section Configuration de Energy Efficient Ethernet (EEC) pour les ports SW et PC, à la page 181.
Taille de police configurable	Permet aux utilisateurs d'augmenter ou de réduire le nombre maximum de caractères affichés par le téléphone IP sur l'historique des appels et l'écran d'appel en modifiant la taille de la police. Une police plus petite augmente le nombre maximum de caractères affichés et une police plus grande réduit le nombre maximum de caractères affichés.
Applications CTI	Un point de routage d'intégration de téléphonie informatique (CTI) peut définir un périphérique virtuel afin qu'il reçoive simultanément plusieurs appels pour la redirection contrôlée par des applications.
Refuser tout	Permet à un utilisateur de transférer directement un appel entrant, connecté ou en attente vers un système de messagerie vocale. Lorsqu'un appel est refusé, la ligne devient disponible pour passer ou recevoir de nouveaux appels. Pour plus d'informations sur la redirection immédiate, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Enregistrement invoqué par le périphérique	Permet aux utilisateurs finals d'enregistrer leurs appels téléphoniques en appuyant sur une touche programmable. En outre, les administrateurs peuvent continuer à enregistrer les appels téléphoniques par le biais de l'interface utilisateur CTI. Pour plus d'informations sur la surveillance et l'enregistrement, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.

Fonctionnalité	Description et informations supplémentaires
Parcage d'appels dirigé	Permet à l'utilisateur de transférer un appel actif à un numéro de parcage d'appel dirigé disponible, que l'utilisateur compose normalement ou à l'aide d'un numéro abrégé. Un bouton FLO Appel parqué indique si un numéro de parcage d'appel dirigé est occupé et fournit au numéro de parcage d'appel dirigé, l'accès à la numérotation rapide. **Remarque** Si vous mettez en œuvre le parcage d'appel dirigé, évitez de configurer la touche programmable Parquer. Ainsi, les utilisateurs ne confondront pas les deux fonctionnalités de parcage d'appels. Pour obtenir des informations sur le parcage d'appels, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.
Affichage des icônes de niveau de batterie et de puissance du signal	Affiche la batterie et la puissance du signal du téléphone mobile sur le téléphone IP lorsque le téléphone mobile est connecté au téléphone IP via Bluetooth. Le téléphone IP Cisco 8851NR ne prend pas en charge Bluetooth.
Sonneries personnalisées	Les utilisateurs peuvent paramétrer la manière dont leur téléphone signale les appels entrants et les nouveaux messages vocaux. Pour plus d'informations sur l'interception d'appels, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Ne pas déranger (NPD)	Lorsque la fonction NPD est activée, aucune sonnerie ne retentit lorsqu'un appel est reçu, ou aucune notification visuelle ou sonore n'a lieu. Lorsqu'elle est activée, l'en-tête du téléphone devient rouge et Ne pas déranger s'affiche sur le téléphone. Si la fonction de préséance et préemption à plusieurs niveaux (MLPP) est configurée et l'utilisateur reçoit un appel prioritaire, le téléphone sonne avec une sonnerie spéciale. Reportez-vous à la section Configuration de la fonctionnalité Ne pas déranger, à la page 177.
Activer/Désactiver JAL / TAL	Permet à l'administrateur de contrôler les fonctionnalités JAL (Join Across Lines) et TAL (Direct Transfer Across Lines). Reportez-vous à Stratégie de jointure et de transfert direct, Configuration spécifique au produit, à la page 149.
EnergyWise	Permet de désactiver (éteindre) et de sortir de veille (allumer) un téléphone IP à des heures prédéterminées, afin d'économiser de l'énergie. Reportez-vous à la section Planifier EnergyWise sur le téléphone IP Cisco, à la page 174.
Mode ligne renforcée	Activez ce mode pour utiliser les boutons des deux côtés de l'écran du téléphone comme touches de ligne. Reportez-vous à Configuration des touches de ligne supplémentaires, à la page 207
Enhanced Secure Extension Mobility Cross Cluster (EMCC)	Améliore la fonctionnalité de cluster croisé de mobilité des postes sécurisée (EMCC) en conservant les configurations réseau et de sécurité sur le téléphone de connexion. De ce fait, les stratégies de sécurité sont mises à jour, la bande passante du réseau est conservée et les pannes réseau sont évitées dans le cluster visiteur (VC).

Fonctionnalité	Description et informations supplémentaires
Service de numérotation abrégée	Permet aux utilisateurs de saisir un code de numérotation abrégée pour passer un appel. Des codes de numérotation abrégée peuvent être affectés à des numéros de téléphone ou à des entrées du Carnet d'adresses personnel. Reportez-vous à « Services » dans le tableau suivant. Reportez-vous à la section Modification du modèle de boutons de téléphone pour le carnet d'adresses personnel ou la numérotation rapide, à la page 205.
Interception d'appels de groupe	Permet aux utilisateurs de prendre un appel qui sonne sur un téléphone dont le numéro de répertoire appartient à un autre groupe. Pour obtenir des informations sur l'interception d'appels, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.
Contrôle de l'effet local du casque	Permet à l'administrateur de définir le niveau d'effet local d'un casque filaire.
Récupération d'un appel en attente	Limite la durée maximale de mise en attente d'un appel et redirige celui-ci vers le poste l'ayant mis en attente en avertissant l'utilisateur. Les appels récupérés sont distingués des appels entrants par une seule sonnerie (ou un bip, selon le paramètre de notification d'appel entrant défini pour la ligne). Cette notification est répétée si l'appel n'est pas repris. Pour les appels qui déclenchent la récupération d'appel, une icône animée apparaît également dans la bulle de l'appel. Vous pouvez configurer la priorité d'appel de manière à donner la préférence aux appels entrants ou aux appels récupérés.
État d'attente	Permet aux téléphones dotés d'une ligne partagée de faire la distinction entre les lignes locale et distante qui ont mis l'appel en attente.
Attente/Reprise	Permet de faire passer un appel connecté d'un état actif à un état d'attente. • Aucune configuration n'est nécessaire, sauf si vous voulez utiliser la musique d'attente. Reportez-vous à la section « Musique d'attente » de ce tableau pour obtenir plus d'informations. • Reportez-vous à la section « Récupération d'appel » de ce tableau.
Téléchargement HTTP	Optimise le processus de téléchargement de fichier en configurant l'utilisation de HTTP par défaut sur le téléphone. Si le téléchargement HTTP échoue, le téléphone utilise à nouveau le téléchargement TFTP.

Fonctionnalité	Description et informations supplémentaires
Groupe de recherche	Fournit le partage d'image pour les appels de numéros de répertoire principaux. Un groupe de recherche contient une série de numéros de répertoire pouvant prendre les appels entrants. Lorsque le premier numéro de répertoire du groupe de recherche est occupé, le système recherche, dans un ordre prédéfini, le prochain numéro de répertoire disponible dans le groupe et dirige les appels vers ce téléphone. Vous pouvez disposer de **l'ID de l' appelant** (si l'ID de l'appelant est configuré), le **numéro d'annuaire** et le **numéro de pilote du groupe de recherche** s' affichent sur l'alerte d'appel entrant pour l'appel du groupe de recherche. Le numéro du groupe de recherche s'affiche après l'étiquette "Groupe de recherche". Pour plus d'informations sur les Groupes de recherche et l'organisation du routage, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Durée de notification d'appel entrant	Permet de définir la durée pendant laquelle une notification d'appel entrant est affichée sur l'écran du téléphone. Reportez-vous à Durée de notification d'appel entrant, Configuration spécifique au produit, à la page 149.
Proximité intelligente	Permet aux utilisateurs d'associer un appareil mobile au téléphone à l'aide du Bluetooth et d'utiliser le téléphone pour passer et recevoir des appels. Reportez-vous à la section Activation d'Intelligent Proximity, à la page 211. Les téléphones IP Cisco 8811, 8841 et 8851NR ne prennent pas en charge Bluetooth ou la Proximité intelligente.
Intercom	Permet aux utilisateurs de passer et de recevoir des appels intercom à l'aide des boutons de téléphone programmables. Vous pouvez configurer les boutons de ligne Intercom pour : • Composer directement un numéro de poste intercom donné. • Passer un appel intercom, puis inviter l'utilisateur à saisir un numéro intercom valide. **Remarque** Si l'utilisateur se connecte quotidiennement au même téléphone à l'aide de son profil Cisco Extension Mobility, affectez le modèle de boutons du téléphone contenant les informations Intercom à ce profil, et définissez le téléphone en tant que périphérique Intercom par défaut de la ligne Intercom.
Prise en charge IPv6 uniquement	Permet l'utilisation de l'adressage IP étendu sur les téléphones IP Cisco. La configuration IPv4 et IPv6 est recommandée et entièrement prise en charge. Certaines fonctionnalités ne sont pas prises en charge dans un paramétrage autonome. Seules les adresses IPv6 sont affectées. Reportez-vous à la section Configurer des paramètres réseau, à la page 61.
Tampon d'instabilité	La fonctionnalité Tampon d'instabilité permet de gérer une gigue de 10 millisecondes (ms) à 1000 ms pour les flux audio. Elle s'exécute en mode adaptatif et ajuste dynamiquement la quantité de gigue.

Fonctionnalité	Description et informations supplémentaires
Jointure	Permet aux utilisateurs de combiner deux appels qui sont sur la même ligne pour créer une conférence téléphonique et rester connectés sur l'appel.
État de la ligne pour les listes d'appels	Permet d'afficher l'état de disponibilité État de la ligne pour les numéros de ligne surveillés dans la liste Historique des appels. Les états de ligne sont : • Hors connexion • Disponible • En cours d'utilisation • Ne pas déranger Reportez-vous à Activation de la fonction Ligne occupée pour des listes d'appels, à la page 180.
État de ligne dans le Répertoire d'entreprise	Permet d'afficher l'état d'un contact du Répertoire d'entreprise. • Hors connexion • Disponible • En cours d'utilisation • Ne pas déranger Reportez-vous à Activation de la fonction Ligne occupée pour des listes d'appels, à la page 180.
Libellé de ligne	Définit pour une ligne téléphonique, un texte de libellé au lieu du numéro de répertoire. Reportez-vous à la section Définition du libellé d'une ligne, à la page 190.
Déconnexion de groupes de recherche	Permet aux utilisateurs de se déconnecter d'un groupe de recherche et d'empêcher temporairement les appels de sonner sur leur téléphone lorsqu'ils ne peuvent pas prendre d'appels. La déconnexion de groupes de recherche n'empêche pas les appels qui ne sont pas des appels de groupe de recherche de sonner sur leur téléphone. Pour plus d'informations sur l'organisation du routage, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Identification d'appel malveillant (IDAM)	Permet aux utilisateurs d'avertir l'administrateur système lorsqu'ils reçoivent des appels suspects.
Conférence MultConf (Meet-Me)	Permet aux utilisateurs de tenir une conférence MultConf, pour laquelle les autres participants appellent un numéro prédéterminé à une heure convenue.

Fonctionnalité	Description et informations supplémentaires
Message en attente	Définit des numéros de répertoire pour l'activation et la désactivation des indicateurs de message en attente. Un système de messagerie vocale directement connecté utilise le numéro de répertoire spécifié pour définir ou effacer une indication de message en attente sur un téléphone IP Cisco donné. Pour plus d'informations sur la messagerie vocale et les messages en attente, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Indicateur de message en attente	Un témoin lumineux sur le combiné qui indique qu'un utilisateur a un ou plusieurs nouveaux messages vocaux. Pour plus d'informations sur la messagerie vocale et les messages en attente, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Volume de sonnerie minimum	Définit un volume minimum pour la sonnerie d'un téléphone IP.
Enregistrement des appels en absence	Permet aux utilisateurs de spécifier si les appels en absence doivent être consignés dans le répertoire des appels en absence d'une apparence de ligne donnée. Pour plus d'informations sur le numéro de répertoire, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Connectivité mobile	Permet aux utilisateurs de gérer les appels professionnels à l'aide d'un seul numéro de téléphone, et d'intercepter les appels en cours sur le téléphone de bureau ou sur un périphérique distant tel qu'un téléphone portable. Les utilisateurs peuvent restreindre le groupe d'appelants selon leur numéro de téléphone et selon l'heure. Pour plus d'informations sur Cisco Unified Mobility, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Mobile and Remote Access Through Expressway	Permet aux télétravailleurs de se connecter aisément et en toute sécurité au réseau d'entreprise, sans utiliser de tunnel client de réseau privé virtuel (VPN). Reportez-vous à Mobile and Remote Access Through Expressway, à la page 183
Accès vocal mobile	Étend les fonctionnalités de connectivité mobile, en permettant aux utilisateurs d'accéder à un système de réponse vocale interactif (IVR) pour passer des appels sur un périphérique distant tel qu'un téléphone portable. Pour plus d'informations sur Cisco Unified Mobility, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.

Fonctionnalité	Description et informations supplémentaires
Surveillance et enregistrement	Permet à un superviseur d'écouter discrètement un appel actif. Le superviseur ne peut pas être entendu par l'autre interlocuteur. L'utilisateur peut entendre une tonalité d'alerte sonore lors d'un appel qui est surveillé. Lorsqu'un appel est sécurisé, une icône en forme de verrou indique l'état de sécurité de l'appel sur les téléphones IP Cisco. Les parties connectées peuvent également entendre une tonalité d'alerte sonore indiquant que l'appel est sécurisé et qu'il est en cours de surveillance. **Remarque** Lors de la surveillance ou de l'enregistrement d'un appel actif, l'utilisateur peut recevoir ou passer des appels intercom ; toutefois, s'il passe un appel intercom, l'appel actif est mis en attente, ce qui entraîne l'interruption de l'enregistrement et la suspension de la surveillance. Pour reprendre la surveillance, la partie dont l'appel est surveillé doit reprendre l'appel.
Préséance et préemption à plusieurs niveaux	Permet aux utilisateurs de passer et de recevoir des appels urgents ou critiques dans des environnements spécialisés, notamment dans des bureaux de l'administration publique ou militaire. Reportez-vous à Préséance et préemption à plusieurs niveaux, à la page 200.
Plusieurs appels par apparence de ligne	Chaque ligne peut prendre en charge plusieurs appels. Par défaut, le téléphone prend en charge deux appels actifs par ligne et au maximum six appels actifs par ligne. Un seul appel peut être connecté ; tous les autres sont automatiquement mis en attente. Le système permet de configurer un nombre maximum d'appels ou un déclencheur d'occupation de ligne d'une valeur maximale de 6/6. Toute configuration supérieure à 6/6 n'est pas prise en charge officiellement. Pour plus d'informations sur le numéro de répertoire, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Musique d'attente (MoH)	Émet de la musique pendant que les appelants sont mis en attente.
Silence	Coupe le son du microphone du combiné ou du casque.
Aucun nom d'alerte	Permet aux utilisateurs finaux d'identifier plus aisément les appels transférés, grâce à l'affichage du numéro de téléphone de l'appelant initial. L'appel est affiché en tant qu'appel d'alerte suivi du numéro de téléphone de l'appelant.
Composition avec combiné raccroché	Permet à l'utilisateur de composer un numéro sans décrocher le combiné. L'utilisateur peut ensuite décrocher le combiné ou appuyer sur Compos.
Autre interception de groupe	Permet à l'utilisateur de prendre un appel qui sonne sur un téléphone d'un autre groupe, qui est associé au groupe de l'utilisateur. Pour obtenir des informations sur l'interception d'appels, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.
Messages affichés sur le téléphone pour les utilisateurs de la mobilité des postes	Cette fonctionnalité améliore l'interface du téléphone pour les utilisateurs de la mobilité des postes, grâce à des messages conviviaux.

Fonctionnalité	Description et informations supplémentaires
Notification de liste de confiance du téléphone dans Cisco Unified Communications Manager	Permet au téléphone d'envoyer une alerte au Cisco Unified Communications Manager lorsque la liste de confiance (TL) est mise à jour. Reportez-vous à la section Fonctionnalités de sécurité prises en charge, à la page 90.
Prise en charge de PLK pour les statistiques de file d'attente	Cette fonctionnalité permet aux utilisateurs de demander les statistiques de file d'attente des appels pour les pilotes de recherche, qui s'affichent ensuite sur l'écran du téléphone.
Composition de numéro avec plus	Permet à l'utilisateur de composer des numéros E.164 précédés du signe plus (+). Pour composer le signe +, l'utilisateur doit appuyer et maintenir la pression sur la touche étoile (*) pendant au moins 1 seconde. Ceci s'applique à la composition du premier chiffre des appels combiné raccroché (notamment en mode Modifier) et combiné décroché.
Gestion de l'énergie sur LLDP	Permet au téléphone de gérer l'énergie à l'aide du protocole LLDP (Link Level Endpoint Discovery Protocol) et du protocole CDP (Cisco Discovery Protocol). Reportez-vous à Négociation d'alimentation, Configuration spécifique au produit, à la page 149.
Numérotation prédictive	Simplifie l'établissement d'un appel. La liste Récents est modifiée pour n'afficher que les numéros de téléphone qui sont similaires au numéro composé. La numérotation prédictive est activée lorsque le mode ligne renforcée est activé. L'interface utilisateur de nouvel appel simplifiée doit être désactivée pour que la numérotation prédictive fonctionne.
Confidentialité	Empêche les utilisateurs qui partagent une ligne de s'ajouter à un appel et d'afficher sur l'écran de leur téléphone, des informations relatives à l'appel de l'autre utilisateur. Pour plus d'informations sur l'insertion et la confidentialité, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Appel automatique d'une ligne privée (PLAR)	L'administrateur du Cisco Unified Communications Manager peut configurer un numéro de téléphone que le téléphone IP Cisco composera dès que le combiné sera décroché. Ceci peut être utile pour les téléphones qui sont dédiés aux appels en cas d'urgence ou aux appels de « service d'assistance téléphonique ». L'administrateur peut configurer un délai allant jusqu'à 15 secondes. Cela permet à l'utilisateur de passer un appel avant que le téléphone ne devienne le numéro par défaut de la hotline. Le temporisateur est configurable par le biais du paramètre **Temporisateur de décroché au premier chiffre** dans la section **Périphérique** > **Paramètres du périphérique** > **Profil SIP**. Pour obtenir plus d'informations, consultez le *Guide de Configuration des fonctionnalités de Cisco Unified Communications Manager*.
Outil de rapport de problème	Soumet des historiques d'appels ou effectue un rapport de problèmes auprès d'un administrateur. Reportez-vous à Outil de rapport de problème, à la page 188.

Fonctionnalité	Description et informations supplémentaires
Touches de fonctionnalité programmables	Vous pouvez attribuer des fonctions, comme Nouvel appel, Rappel automatique et Renvoi de tous les appels, à des boutons de ligne. Pour plus d'informations sur les modèles de boutons de téléphone, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Outil de génération de rapports de qualité (QRT)	Permet aux utilisateurs de soumettre des informations concernant des appels téléphoniques problématiques en appuyant sur un bouton. L'outil QRT peut être configuré pour l'un de deux modes utilisateur, selon la quantité d'interaction utilisateur souhaitée avec l'outil QRT.
Récents	Permet aux utilisateurs de voir les 150 appels individuels ou de groupe les plus récents. Vous pouvez consulter les numéros composés récemment, les appels en absence et supprimer un enregistrement d'appel.
Bis	Permet aux utilisateurs d'appeler le dernier numéro de téléphone composé en appuyant sur un bouton ou sur la touche programmable Bis.
Configuration à distance des ports	Vous permet de configurer à distance la vitesse et la fonction duplex des ports Ethernet du téléphone en utilisant le Cisco Unified Communications Manager Administration. Ceci optimise la performance lors de déploiements volumineux avec des paramètres de port spécifiques. **Remarque** Si les ports sont configurés pour une Configuration des ports à distance dans Cisco Unified Communications Manager, les données ne peuvent pas être changées sur le téléphone. Reportez-vous à Configuration à distance des ports, Configuration spécifique au produit, à la page 149.
Réacheminement des appels directs d'une destination distante vers le numéro professionnel	Réachemine un appel direct du téléphone portable de l'utilisateur vers son numéro professionnel (téléphone de bureau). Pour les appels entrants sur la destination distante (téléphone portable), seule la destination distante sonne ; le téléphone de bureau ne sonne pas. Lorsque l'utilisateur répond à un appel entrant sur son téléphone portable, son téléphone de bureau affiche le message Utilisé à distance. Pendant ces appels, les utilisateurs peuvent utiliser les diverses fonctionnalités de leur téléphone portable. Pour plus d'informations sur Cisco Unified Mobility, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Supprimer le minuteur du message « Appel terminé »	Améliore le temps de réponse de fin d'appel en supprimant le message `Appel terminé` affiché sur l'écran du téléphone.
Paramètre Sonnerie	Identifie le type de sonnerie utilisé pour une ligne lorsqu'un autre appel est en cours sur le téléphone. Pour plus d'informations sur les numéros de répertoire, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager ainsi que Sonneries personnalisées, à la page 119.

Fonctionnalité	Description et informations supplémentaires
RTCP Hold For SIP (Attente RTCP pour SIP)	Empêche la passerelle de mettre fin aux appels en attente. La passerelle vérifie l'état du port RTCP pour déterminer si un appel est actif ou non. Si le port du téléphone est gardé ouvert, la passerelle ne mettra pas fin aux appels en attente.
Conférence sécurisée	Permet aux téléphones sécurisés d'établir des conférences téléphoniques à l'aide d'un pont de conférence sécurisé. À mesure que de nouveaux participants sont ajoutés en utilisant les touches dynamiques Conf., Jointure ou Insertion ou encore la création de conférences MeetMe, l'icône d'appel sécurisé s'affiche tant que tous les participants utilisent des téléphones sécurisés. Le niveau de sécurité de chaque participant à la conférence est indiqué dans la liste des conférences. Les initiateurs peuvent supprimer les participants non sécurisés de la liste des conférences. Les participants qui ne sont pas des initiateurs peuvent ajouter ou supprimer les participants à la conférence si le paramètre Advanced Adhoc Conference Enabled est activé. Pour plus d'informations concernant les ponts de conférence et la sécurité, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager ainsi que Fonctionnalités de sécurité prises en charge, à la page 90.
EMCC sécurisé	Améliore la fonctionnalité EMCC, en renforçant la sécurité des utilisateurs qui se connectent à leur téléphone depuis un bureau distant.
Services	Permet d'utiliser le menu de configuration des services du téléphone IP Cisco, dans Cisco Unified Communications Manager Administration, pour définir et mettre à jour la liste des services téléphoniques auxquels les utilisateurs peuvent s'abonner. Pour plus d'informations sur les services, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Bouton d'accès à l'URL des services	Permet aux utilisateurs d'accéder aux services à partir d'un bouton programmable au lieu d'utiliser le menu Services du téléphone. Pour plus d'informations sur les services, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Affichage de l'ID et du numéro de l'appelant	Le nom et le numéro de l'appelant peuvent être affiché sur le téléphone lors d'un appel entrant. La taille de l'écran LCD du téléphone IP limite la longueur d'affichage de l'ID et du numéro de l'appelant. La fonctionnalité d'affichage de l'ID et du téléphone de l'appelant s'applique uniquement à l'alerte d'appel et ne modifie pas le comportement des fonctionnalités de renvoi d'appel et de groupe de recherche. Reportez-vous à la section « ID de l'appelant » de ce tableau.

Fonctionnalité	Description et informations supplémentaires
Simplification de la connexion Extension Mobility avec les casques Cisco	Permet aux utilisateurs de se connecter à Extension Mobility avec leurs casques Cisco. Lorsque le téléphone est en mode MRA, l'utilisateur peut utiliser le casque pour se connecter au téléphone Cette fonctionnalité nécessite Cisco Unified Communications Manager (UCM) version 11.5 (1) SU8, 11.5 (1) SU.9, 12.5 (1) SU3 ou version ultérieure. Pour plus d'informations, reportez-vous au *Guide de configuration des fonctionnalités de Cisco Unified Communications Manager*, version 11.5(1)SU8 ou ultérieure, ou version 12.5(1)SU3 ou ultérieure
Prise en charge simplifiée des tablettes	Permet à un utilisateur de tablette Android ou iOS d'associer sa tablette au téléphone à l'aide du Bluetooth, puis d'utiliser le téléphone pour la partie audio d'un appel sur la tablette. Reportez-vous à la section Activation d'Intelligent Proximity, à la page 211. Le téléphone IP Cisco 8851NR ne prend pas en charge Bluetooth.
Numérotation rapide	Compose un numéro donné qui a été préalablement enregistré.
Accès SSH	Vous permet d'activer ou de désactiver le paramètre d'accès SSH à l'aide de Cisco Unified Communications Manager Administration. Lorsque le serveur SSH est activé, le téléphone accepte les connexions SSH. Lorsque le serveur SSH est désactivé sur le téléphone, ce dernier ne peut pas accéder à SSH. Reportez-vous à accès SSH, Configuration spécifique au produit, à la page 149.
Routage selon l'heure	Limite l'accès aux fonctionnalités de téléphonie spécifiées, selon la période de temps. Pour plus d'informations concernant la période horaire et le routage horaire, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Mise à jour du fuseau horaire	Met à jour les changements de fuseau horaire sur le téléphone IP Cisco. Pour plus d'informations sur la date et l'heure, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.
Transfert	Permet aux utilisateurs de rediriger les appels connectés de leur téléphone vers un autre numéro.
Transfert : transfert direct	Transfert : la première demande de transfert va toujours initier un nouvel appel en utilisant le même numéro de répertoire, après avoir mis l'appel actif en attente. L'utilisateur peut transférer directement les appels en utilisant la fonctionnalité Transférer un appel actif. Certaines applications JTAPI/TAPI ne sont pas prises en charge par l'implémentation de la fonctionnalité Jointure et transfert direct sur le téléphone IP Cisco. Il est donc possible que vous deviez configurer les Règles de jointure et de transfert direct pour désactiver cette fonctionnalité sur la même ligne ou même sur plusieurs lignes. Pour plus d'informations sur le numéro de répertoire, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.

Fonctionnalité	Description et informations supplémentaires
TVS	Les services de vérification de la liste de confiance (TVS) permettent aux téléphones d'authentifier des configurations signées et d'authentifier d'autres serveurs ou homologues sans augmenter la taille de la liste de confiance des certificats (CTL), et sans qu'il soit nécessaire de télécharger un fichier CTL mis à jour sur le téléphone. TVS est activé par défaut. Les informations TVS sont affichées dans le menu de configuration de la sécurité du téléphone.
UCR 2013	Les téléphones IP Cisco répondent aux exigences UCR 2013 (Unified Capabilities Requirements) en mettant à disposition les fonctionnalités suivantes : • Prise en charge de la norme de traitement des informations fédérales (FIPS) 140-2 • Prise en charge du balisage SRTCP 80 bits En qualité d'administrateur de téléphones IP, vous devez configurer des paramètres spécifiques dans Cisco Unified Communications Manager Administration.
Notification de ligne principale non configurée	Avertit l'utilisateur lorsque la ligne principale n'est pas configurée. L'utilisateur voit le message `Non déployé` sur l'écran du téléphone.
Mises à jour de l'interface utilisateur pour la liste, l'alerte et la messagerie vocale visuelle.	Augmente la taille de la fenêtre de l'application pour limiter le nombre de chaînes tronquées.
Mode vidéo	Permet à un utilisateur de sélectionner le mode d'affichage vidéo pour une vidéoconférence, en fonction des modes configurés dans le système. Pour plus d'informations sur la vidéo, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager. Disponible uniquement pour les téléphones IP Cisco 8845, 8865 et 8865NR.
Prise en charge de la vidéo	Active ou désactive la prise en charge de la vidéo sur le téléphone. Le paramètre Capacités vidéo doit être activé pour les appels vidéo dans la fenêtre Configuration du téléphone de Cisco Unified Communications Manager. Il est activé par défaut. Disponible uniquement pour les téléphones IP Cisco 8845, 8865 et 8865NR.
Vidéo via PC	Permet aux utilisateurs de passer des appels vidéo en utilisant leur téléphone IP Cisco Unified, leur PC et une caméra externe. Cette fonctionnalité permet aux utilisateurs de passer des appels vidéo avec Cisco Jabber ou les produits Cisco Unified Video Advantage.
Messagerie vocale visuelle	Remplace l'invite audio de la messagerie vocale par une interface graphique. Reportez-vous au *Guide d'installation et de configuration de la messagerie vocale visuelle* situé dans http://www.cisco.com/en/US/partner/products/ps9829/prod_installation_guides_list.html#anchor3.

Fonctionnalité	Description et informations supplémentaires
Système de messagerie vocale	Permet aux appelants de laisser des messages lorsque personne ne répond au téléphone. Pour plus d'informations sur la messagerie vocale, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager ainsi que Configuration de la messagerie vocale, à la page 197.
VPN	Grâce à SSL, permet la connexion à un réseau privé virtuel (VPN) sur le téléphone IP Cisco Unified lorsque celui-ci est situé en dehors d'un réseau de confiance, ou lorsque les communications entre le téléphone et le Unified Communications Manager doivent passer par des réseaux non approuvés.
Accès au Web désactivé par défaut	Renforce la sécurité en désactivant l'accès à tous les services Web, notamment HTTP. Les utilisateurs ne peuvent accéder aux services Web que si vous activez l'accès à Internet.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Boutons de fonctions et touches programmables

Le tableau suivant présente des informations sur les fonctionnalités disponibles par le biais des touches programmables et des boutons de fonctions dédiés, et les fonctionnalités que vous devrez peut-être configurer en tant que boutons de fonctions programmables. La mention « Prise en charge » dans le tableau indique que la fonctionnalité est prise en charge pour le type de bouton ou de touche programmable correspondant. Des deux types de boutons et de touches programmables, seuls les boutons de fonctions programmables doivent être configurés dans l'administration du téléphone IP Cisco.

Pour obtenir des informations sur la configuration des boutons de fonctions programmables, reportez-vous à Modèles de boutons de téléphone, à la page 202.

Tableau 30 : Fonctions, boutons et touches programmables correspondants

Nom de la fonction	Bouton de fonction dédié	Bouton de fonction programmable	Touche programmable
Appels d'alerte	Non pris en charge	Pris en charge	Non pris en charge
Ts app.	Non pris en charge	Pris en charge	Non pris en charge
Réponse	Non pris en charge	Pris en charge	Pris en charge
Insertion dans une conférence (cBarge)	Non pris en charge	Non pris en charge	Pris en charge
Rappel automatique	Non pris en charge	Pris en charge	Pris en charge
Renvoi de tous les appels	Non pris en charge	Non pris en charge	Pris en charge
Parcage d'appels	Non pris en charge	Pris en charge	Pris en charge

Nom de la fonction	Bouton de fonction dédié	Bouton de fonction programmable	Touche programmable
Parcage d'appels, état de la ligne	Non pris en charge	Pris en charge	Non pris en charge
Interception d'appels (Interception)	Non pris en charge	Pris en charge	Pris en charge
Interception d'appels, état de la ligne	Non pris en charge	Pris en charge	Non pris en charge
Conférence	Pris en charge	Non pris en charge	Pris en charge
Détourner	Non pris en charge	Non pris en charge	Pris en charge
Ne pas déranger	Non pris en charge	Pris en charge	Pris en charge
Interception d'appels de groupe	Non pris en charge	Pris en charge	Pris en charge
Attente	Pris en charge	Non pris en charge	Pris en charge
Groupes de recherche	Non pris en charge	Pris en charge	Non pris en charge
Intercom	Non pris en charge	Pris en charge	Non pris en charge
Identification d'appel malveillant (IDAM)	Non pris en charge	Pris en charge	Pris en charge
MultConf	Non pris en charge	Pris en charge	Pris en charge
Fusionner	Non pris en charge	Non pris en charge	Pris en charge
Mobile Connect (Mobilité)	Non pris en charge	Pris en charge	Pris en charge
Silence	Pris en charge	Non pris en charge	Non pris en charge
Autre interception	Non pris en charge	Pris en charge	Pris en charge
Prise en charge de PLK pour les états de la file d'attente	Non pris en charge	Non pris en charge	Pris en charge
Confidentialité	Non pris en charge	Pris en charge	Non pris en charge
État de la file d'attente	Non pris en charge	Pris en charge	Non pris en charge
Outil de génération de rapports de qualité (QRT)	Non pris en charge	Pris en charge	Pris en charge
Enreg.	Non pris en charge	Non pris en charge	Pris en charge
Renumérotation	Non pris en charge	Pris en charge	Pris en charge

Nom de la fonction	Bouton de fonction dédié	Bouton de fonction programmable	Touche programmable
Numérotation simplifiée	Non pris en charge	Pris en charge	Non pris en charge
Numérotation rapide, état de la ligne	Non pris en charge	Pris en charge	Non pris en charge
Prise en charge du bouton Attente sur un casque USB	Non pris en charge	Non pris en charge	Pris en charge
Transfert	Pris en charge	Non pris en charge	Pris en charge

Configuration des fonctionnalités téléphoniques

Vous pouvez configurer des téléphones pour avoir de nombreuses fonctionnalités, en fonction des besoins de vos utilisateurs. Vous pouvez appliquer des fonctions à tous les téléphones, un groupe de téléphones, ou à des téléphones individuels.

Lorsque vous définissez des fonctionnalités, la fenêtre Cisco Unified Communications Manager Administration affiche des informations qui ne s'appliquent pas à tous les téléphones et les informations qui s'appliquent au modèle de téléphone. Les informations spécifiques au modèle de téléphone sont dans la zone Configuration spécifique au produit de la fenêtre.

Pour plus d'informations sur les champs qui s'appliquent à tous les modèles de téléphones, reportez-vous à la documentation de Cisco Unified Communications Manager.

Lorsque vous définissez un champ, la fenêtre dans laquelle vous définissez le champ est importante car il existe une priorité entre les fenêtres. L'ordre de priorité est :

1. Téléphones individuels (priorité la plus élevée)
2. Groupe de téléphones
3. Tous les téléphones (ordre le plus bas)

Par exemple, si vous ne souhaitez pas qu'un ensemble spécifique d'utilisateurs accède aux pages Web de téléphone, mais que le reste de vos utilisateurs puisse accéder aux pages, vous :

1. Activez l'accès aux pages web du téléphone pour tous les utilisateurs.
2. Désactivez l'accès aux pages web du téléphone pour chaque utilisateur, ou configurez un groupe d'utilisateurs et désactivez l'accès aux pages web du téléphone pour le groupe d'utilisateurs.
3. Si un utilisateur spécifique dans le groupe d'utilisateurs a besoin d'accéder aux pages web du téléphone, vous pouvez activer l'accès pour cet utilisateur spécifique.

Définir des fonctionnalités téléphoniques pour tous les téléphones

Procédure

Étape 1 Connectez-vous à Cisco Unified Communications Manager Administration en tant qu'administrateur.
Étape 2 Sélectionnez **Système** > **Configuration des téléphones d'entreprise**.
Étape 3 Définissez les champs que vous souhaitez modifier.
Étape 4 Cochez la case **Remplacer les paramètres d'entreprise** des champs modifiés.
Étape 5 Cliquez sur **Enregistrer**.
Étape 6 Cliquez sur **Appliquer la configuration**.
Étape 7 Redémarrez les téléphones.

Remarque Cela aura des répercussions sur tous les téléphones de votre entreprise.

Définir des fonctionnalités du téléphone pour un groupe de téléphones

Procédure

Étape 1 Connectez-vous à Cisco Unified Communications Manager Administration en tant qu'administrateur.
Étape 2 Sélectionnez **Périphérique** > **Paramètres du périphérique** > **Profil de téléphone commun**.
Étape 3 Localiser le profil.
Étape 4 Accédez au panneau de Configuration spécifique à un produit et configurez les champs.
Étape 5 Cochez la case **Remplacer les paramètres d'entreprise** des champs modifiés.
Étape 6 Cliquez sur **Enregistrer**.
Étape 7 Cliquez sur **Appliquer la configuration**.
Étape 8 Redémarrez les téléphones.

Définir des fonctionnalités du téléphone pour un seul téléphone

Procédure

Étape 1 Connectez-vous à Cisco Unified Communications Manager Administration en tant qu'administrateur.
Étape 2 Sélectionnez **Périphérique** > **Téléphone**.
Étape 3 Localisez le téléphone associé à l'utilisateur.
Étape 4 Accédez au panneau de Configuration spécifique à un produit et configurez les champs.
Étape 5 Cochez la case **Remplacer les paramètres communs** des champs modifiés.

Étape 6 Cliquez sur **Enregistrer**.

Étape 7 Cliquez sur **Appliquer la configuration**.

Étape 8 Redémarrez le téléphone.

Configuration spécifique au produit

Le tableau suivant décrit les champs dans le volet de Configuration spécifique au produit.

Tableau 31 : Champs de configuration spécifique au produit

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Désactivation du haut-parleur	Case à cocher	Non coché	Désactive la fonction haut-parleur du téléphone.
Désactiver le haut-parleur et le casque	Case à cocher	Non coché	Désactive la fonction haut-parleur et casque du téléphone.
Désactiver le combiné	Case à cocher	Non coché	Désactive la fonction combiné du téléphone.
Port PC	Activé Désactivé	Activé	Contrôle la possibilité d'utiliser le port PC pour connecter un ordinateur au réseau local.
Accès aux paramètres	Désactivé Activé Restreint	Activé	Active, désactive ou restreint l'accès aux paramètres de configuration régionaux dans l'application Paramètres. • Désactivé : le menu Paramètres n'affiche pas d'options. • Activé : toutes les entrées dans le menu Paramètres sont accessibles. • Restreint : seul le menu Paramètres du téléphone est accessible.
Accès au VLAN vocal du PC	Activé Désactivé	Activé	Indique si le téléphone autorise un périphérique affecté au port de l'ordinateur à accéder au VLAN vocal. • Désactivé : l'ordinateur ne peut pas envoyer et recevoir des données sur le VLAN vocal ou à partir du téléphone. • Activé : l'ordinateur peut envoyer et recevoir des données à partir du VLAN vocal ou à partir du téléphone. Définissez ce champ sur activé si une application s'exécute sur le PC qui va contrôler le trafic du téléphone. Ces applications pourraient inclure les applications de surveillance et enregistrement, et l'utilisation du logiciel de surveillance du réseau pour des raisons d'analyse.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Capacités vidéo	Activé Désactivé	8845, 8865 et 8865NR : activé 8811, 8851, 8851NR, 8861 : désactivé	Permet aux utilisateurs de passer des appels vidéo en utilisant un téléphone IP Cisco, un PC et une caméra.
Accès au Web	Désactivé Activé	Désactivé	Active ou désactive l'accès aux pages web du téléphone via un navigateur web. **Avertissement** Si vous activez ce champ, vous risquez de rendre visibles des informations confidentielles sur le téléphone.
Désactiver TLS 1.0 et TLS 1.1 pour l'accès Web	Désactivé Activé	Désactivé	Contrôle l'utilisation de TLS 1.2 pour la connexion au serveur web. • Désactivé : un téléphone configuré pour TLS 1.0, TLS 1.1 ou TLS 1.2 peut fonctionner comme un serveur HTTPs. • Activé : seul un téléphone configuré pour TLS 1.2 peut fonctionner comme un serveur HTTPs.
Composition de numéro Enbloc	Désactivé Activé	Désactivé	Contrôle la méthode de numérotation. • Désactivé : Cisco Unified Communications Manager attend que le temporisateur inter-chiffres expire lorsque se chevauchent le plan de numérotation ou le modèle de routage. • Activé : toute la chaîne de numéro composé est envoyée à Cisco Unified Communications Manager une fois l'appel terminé. Pour éviter le délai d'expiration du minuteur T.302, nous vous recommandons d'activer la numérotation Enbloc chaque fois qu'il existe un chevauchement de modèle de plan de numérotation ou de routage. Les Codes d'autorisation forcée (FAC) ou les Codes d'affaire client (CMC) ne prennent pas en charge la numérotation Enbloc. Si vous utilisez les FAC ou les CMC pour gérer la comptabilité et l'accès aux appels, vous ne pouvez pas utiliser cette fonctionnalité.
Jours d'inactivité de l'écran	Jours de la semaine		Définit les jours où l'écran ne s'allume pas automatiquement à l'heure spécifiée dans le champ Heure d'activation de l'écran. Sélectionnez un ou plusieurs jours dans la liste déroulante. Pour choisir plusieurs jours, maintenez la touche **Crtl enfoncée et cliquez** sur les jours souhaités.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Heure d'activation de l'écran	hh:mn		Définit l'heure à laquelle l'écran est automatiquement activé tous les jours (sauf les jours indiqués dans le champ Jours d'inactivité de l'écran). Entrez l'heure dans ce champ au format 24 heures ; 00:00 correspondant à minuit. Par exemple, pour allumer automatiquement l'écran à 7 heures du matin, saisissez 07:00. Par exemple, pour activer l'écran à 14h00, (14h00), saisissez 14h00. Si ce champ est vide, l'écran s'allume automatiquement à 0:00.
Durée d'activité de l'écran	hh:mn		Définit la durée pendant laquelle l'écran reste allumé après s'être activé à l'heure spécifiée par le champ Heure d'activation de l'écran. Par exemple, pour que l'écran reste allumé pendant 4 heures et 30 minutes après son activation automatique, entrez 04:30. Lorsque ce champ est vide, le téléphone s'éteint à la fin de la journée (0:00). Si l'heure d'activation de l'écran est 0:00 et si le champ Durée d'activité de l'écran est vide (ou a la valeur 24:00), l'écran ne s'éteint pas.
Temporisation d'inactivité de l'écran	hh:mn	01:00	Définit la durée pendant laquelle le téléphone est inactif avant l'extinction de l'écran. S'applique uniquement lorsque l'écran a été désactivé comme planifié, et qu'il a été activé par l'utilisateur (qui a appuyé sur une touche du téléphone ou qui a soulevé le combiné). Entrez une valeur dans ce champ au format heures:minutes. Par exemple, pour éteindre l'écran lorsque le téléphone est inactif pendant 1 heure et 30 minutes après qu'un utilisateur a allumé l'écran, saisissez 01:30. Pour obtenir plus d'informations, reportez-vous à Configuration de l'affichage d'un message d'inactivité, à la page 122.
Activation de l'affichage lors des appels entrants	Désactivé Activé	Activé	Allume l'écran inactif lorsqu'il y a un appel entrant.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Activer Power Save Plus	Jours de la semaine		Définit le calendrier des jours durant lesquels le téléphone s'éteint. Sélectionnez un ou plusieurs jours dans la liste déroulante. Pour choisir plusieurs jours, maintenez la touche **Crtl enfoncée et cliquez** sur les jours souhaités. Lorsque la case Activer Power Save Plus est activée, vous recevez un message vous avertissant des risques en cas d'urgence (e911). **Avertissement** Lorsque le mode Power Save Plus (le « Mode ») est en vigueur, les terminaux configurés pour ce mode ne peuvent pas passer des appels d'urgence ni recevoir des appels entrants. En sélectionnant ce mode, vous acceptez les termes suivants : (i) Vous prenez l'entière responsabilité de fournir des méthodes alternatives pour contacter les services d'urgence et recevoir des appels lorsque le mode est en vigueur ; (ii) Cisco ne peut être tenu pour responsable de l'activation du mode et vous êtes le seul responsable de l'activation du mode ; (iii) Vous informez pleinement les utilisateurs des effets de ce mode sur les appels, les appels en cours et tout autre appel. Pour désactiver le mode Power Save Plus, déscochez la case Allow EnergyWise Overrides (Permettre le remplacement par EnergyWise). Si la case Allow EnergyWise Overrides (Permettre le remplacement par EnergyWise) est activée sans qu'aucun jour ne soit sélectionné dans le champ Activer Power Save Plus, le mode Power Save Plus n'est pas désactivé.
Heure d'activation du téléphone	hh:mn		Détermine l'heure à laquelle le téléphone est automatiquement allumé les jours qui sont sélectionnés dans le champ activer Power Save Plus. Entrez l'heure dans ce champ au format 24 heures ; 00:00 correspondant à minuit. Par exemple, pour allumer automatiquement le téléphone à 7h00, saisissez 07:00. Pour allumer automatiquement le téléphone à 14h00, (14h00), saisissez 14h00. La valeur par défaut est un champ vide, ce qui signifie 00:00. L'heure d'activation du téléphone doit être ultérieure d'au moins 20 minutes à l'heure de désactivation du téléphone. Par exemple, si l'heure d'arrêt du téléphone est 07:00, l'heure de mise en route du téléphone ne doit pas être antérieure à 07:20.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Heure de désactivation du téléphone	hh:mn		Identifie l'heure à laquelle le téléphone s'éteint lors des jours sélectionnés dans le champ Activer Power Save Plus. Si les valeurs des champs Heure d'activation du téléphone et Heure de désactivation du téléphone sont identiques, le téléphone ne s'éteint pas. Entrez l'heure dans ce champ au format 24 heures ; 00:00 correspondant à minuit. Par exemple, pour éteindre automatiquement le téléphone à 7h00, saisissez 7h00. Pour éteindre automatiquement le téléphone à 14h00, (14h00), saisissez 14h00. La valeur par défaut est un champ vide, ce qui signifie 00:00. L'heure d'activation du téléphone doit être ultérieure d'au moins 20 minutes à l'heure de désactivation du téléphone. Par exemple, si l'heure d'arrêt du téléphone est 07:00, l'heure de mise en route du téléphone ne doit pas être antérieure à 07:20.
Phone Off Idle Timeout (Délai d'inactivité avant désactivation)	de 20 à 1440 minutes.	60	Indique la durée pendant laquelle le téléphone doit rester inactif avant de pouvoir s'éteindre. Ce délai a lieu dans les conditions suivantes : • Lorsque le téléphone était en mode Power Save Plus, comme planifié et a été sorti du mode Power Save Plus car l'utilisateur a appuyé sur la touche Sélect. • Lorsque le téléphone est remis sous tension par le commutateur connecté. • Lorsque l'heure de désactivation du téléphone a été atteinte mais que le téléphone est toujours en cours d'utilisation.
Enable Audible Alert (Activer l'alerte sonore)	Case à cocher	Non coché	Lorsque cette option est activée, le téléphone émet une alerte sonore qui commence 10 minutes avant l'heure de désactivation du téléphone. Cette case à cocher n'est pertinente que lorsqu'un ou plusieurs jours sont sélectionnés dans la zone de liste Activer Power Save Plus.
Domaine EnergyWise	Jusqu'à 127 caractères.		Identifie le domaine EnergyWise dans lequel le téléphone se situe.
EnergyWise Secret (Secret EnergyWise)	Jusqu'à 127 caractères.		Identifie le mot de passe de sécurité secret qui est utilisé pour communiquer avec les terminaux du domaine EnergyWise.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Allow EnergyWise Overrides (Permettre le remplacement par EnergyWise)	Case à cocher	Non coché	Détermine si vous autorisez ou non les règles du contrôleur de domaine EnergyWise à envoyer des mises à jour d'alimentation aux téléphones. Les conditions suivantes s'appliquent : • Un ou plusieurs jours doivent avoir été sélectionnés dans le champ Activer One Power Save Plus. • Les paramètres de Cisco Unified Communications Manager Administration prennent effet à la date spécifiée même si EnergyWise envoie une redéfinition. Supposons par exemple que l'heure de désactivation du téléphone est définie par 22:00 (22h00), que la valeur du champ Heure d'activation du téléphone est 06:00 (6h00), et qu'un ou plusieurs jours sont sélectionnés dans le champ Activer Power Save Plus. • Si EnergyWise demande la désactivation du téléphone à 20:00 (20h00), cette directive reste effective (en supposant qu'aucune intervention de l'utilisateur du téléphone n'ait lieu) jusqu'à l'heure d'activation du téléphone, soit 6h00. • À 06:00, le téléphone s'allume et continue de recevoir les modifications de niveau de puissance depuis les paramètres de Cisco Unified Communications Manager Administration. • Pour changer de nouveau le niveau de puissance du téléphone, EnergyWise doit émettre une nouvelle commande de variation du niveau de puissance. Pour désactiver le mode Power Save Plus, déscochez la case Allow EnergyWise Overrides (Permettre le remplacement par EnergyWise). Si la case Allow EnergyWise Overrides (Permettre le remplacement par EnergyWise) est activée sans qu'aucun jour ne soit sélectionné dans le champ Activer Power Save Plus, le mode Power Save Plus n'est pas désactivé.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Stratégie de jointure et de transfert direct	Même ligne, plusieurs lignes activé Même ligne activé uniquement Même ligne, plusieurs lignes désactivé	Même ligne, plusieurs lignes activé	Contrôle la possibilité d'un utilisateur de joindre et transférer des appels. • Même ligne, plusieurs lignes activé : les utilisateurs peuvent transférer ou joindre directement un appel sur la ligne en cours vers un autre appel sur une autre ligne. • Même ligne activé uniquement : les utilisateurs peuvent uniquement transférer ou joindre directement des appels lorsque les deux appels sont sur une même ligne. • Même ligne, plusieurs lignes désactivé : les utilisateurs ne peuvent pas joindre ou transférer des appels sur la même ligne. Les fonctionnalités de jointure et de transfert sont désactivées et l'utilisateur ne peut pas utiliser la fonction joindre ou de transfert direct.
Renvoi au port PC	Désactivé Activé	Désactivé	Indique si le téléphone renvoie au port d'accès, les paquets émis et reçus sur le port réseau.
Tonalité d'enregistrement	Désactivé Activé	Désactivé	Contrôle la lecture de la tonalité lorsqu'un utilisateur enregistre un appel.
Vol. tonalité d'enreg. local	Nombre entier de 0 à 100	100	Contrôle le volume de la sonnerie de l'enregistrement de l'utilisateur local.
Vol. tonalité d'enreg. à distance	Nombre entier de 0 à 100	50	Contrôle le volume de la sonnerie de l'enregistrement de l'utilisateur distant.
Durée de la tonalité d'enreg.	Entier de 1 à 3000 millisecondes		Contrôle la durée de la tonalité de l'enregistrement.
Serveur de fichier journal	Chaîne de 256 caractères maximum		Identifie le serveur Syslog IPv4 pour la sortie de débogage du téléphone. Le format de l'adresse est : **`adresse:<port>@@base=<0-7>;pfs=<0-1>`**
Protocole CDP (Cisco Discovery Protocol) - port commuté	Désactivé Activé	Activé	Contrôle Cisco Discovery Protocol sur le port de commutation du téléphone.
Protocole CDP (Cisco Discovery Protocol) - port d'ordinateur	Désactivé Activé	Activé	Contrôle Cisco Discovery Protocol sur le port PC du téléphone.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Protocole LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Discover) : port commuté	Désactivé Activé	Activé	Active LLDP-MED sur le port de commutation.
Protocole LLDP (Link Layer Discovery Protocol) : port d'ordinateur	Désactivé Activé	Activé	Active LLDP-MED sur le port PC.
ID de ressource LLDP	Chaîne de 32 caractères maximum		Définit l'identifiant de ressource qui est affecté au téléphone pour la gestion de l'inventaire.
Hiérarchisation énergie LLDP	Inconnue Faible Élevé Critique	Inconnue	Affecte une priorité énergétique du téléphone au commutateur, permettant ainsi au commutateur de fournir une alimentation appropriée aux téléphones.
Authentification 802.1x	Contrôlé par l'utilisateur Activé Désactivé	Contrôlé par l'utilisateur	Spécifie l'état de la fonctionnalité d'authentification 802. 1 x. • Contrôlé par l'utilisateur : l'utilisateur peut configurer le 802. 1 x sur le téléphone. • Désactivé : l'authentification 802.1x n'est pas utilisée. • Activé : l'authentification 802.1 x est utilisée, et vous configurez l'authentification pour les téléphones.
Synchronisation automatique des ports	Désactivé Activé	Désactivé	Synchronise les ports à la vitesse minimale entre les ports d'un téléphone pour supprimer la perte de paquets.
Configuration à distance du port de commutation	Désactivé Activé	Désactivé	Vous permet de configurer la vitesse et la fonction duplex du port de commutation du téléphone à distance. Ceci optimise la performance lors de déploiements volumineux avec des paramètres de port spécifiques. Si les ports de commutation sont configurés pour une Configuration des ports à distance dans Cisco Unified Communications Manager, les données ne peuvent pas être changées sur le téléphone.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Configuration à distance du port d'ordinateur	Désactivé Activé	Désactivé	Vous permet de configurer la vitesse et la fonction duplex du port PC du téléphone à distance. Ceci optimise la performance lors de déploiements volumineux avec des paramètres de port spécifiques. Si les ports sont configurés pour une Configuration des ports à distance dans Cisco Unified Communications Manager, les données ne peuvent pas être changées sur le téléphone.
SSH Access	Désactivé Activé	Désactivé	Contrôle l'accès au démon SSH par le port 22. Laisser le port 22 ouvert rend le téléphone vulnérable aux attaques par déni de service (DoS).
Minuteur de la notification d'appel entrant	0, 3, 4, 5, 6, 7, 8, 9, 10, 15, 30, 60	5	Indique la durée, en secondes, pendant laquelle la notification est affichée. La durée inclut les temps d'apparition et de disparition de la fenêtre. 0 signifie que la notification d'appel entrant est désactivée.
Paramètres régionaux de sonnerie	Par défaut Japon	Par défaut	Contrôle le modèle de sonnerie.
Minuteur de reprise TLS	Nombre entier de 0 à 3600 secondes	3600	Contrôle la possibilité de reprendre une session TLS sans répéter le processus d'authentification TLS complet. Si le champ est défini sur 0, la reprise de la session TLS est désactivée.
Mode FIPS	Désactivé Activé	Désactivé	Active ou désactive le mode FIPS (Federal Information Processing Standards) sur le téléphone.
Enregistrer le journal des appels de la ligne partagée	Désactivé Activé	Désactivé	Indique si l'enregistrement d'un appel de ligne partagée dans le journal des appels doit être effectué.
Volume minimum de la sonnerie	0 : mode silencieux 1–15	0 : mode silencieux	Contrôle le volume minimum de la sonnerie du téléphone. Vous pouvez configurer un téléphone afin que la sonnerie ne puisse pas être désactivée.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Partage de micrologiciel par les homologues	Désactivé Activé	Activé	Permet au téléphone de trouver les autres téléphones du même modèle sur le sous-réseau et de partager les fichiers de mise à jour du micrologiciel. Si le téléphone a une nouvelle version de micrologiciel, il peut la partager avec les autres téléphones. Si une des autres téléphones a une nouvelle version de micrologiciel, le téléphone peut télécharger le micrologiciel à partir de l'autre téléphone, au lieu de la faire à partir du serveur TFTP. Le partage de micrologiciel par les homologues : • Limite la congestion des transferts TFTP vers des serveurs TFTP centralisés distants. • Élimine la nécessité de contrôler manuellement les mises à niveau de micrologiciel. • Elle réduit les temps d'arrêt du téléphone pendant les mises à niveau lorsqu'un grand nombre de téléphones sont simultanément réinitialisés. • Permet de mises à niveau dans des succursales ou des scénarios de déploiement de bureaux distants qui s'exécutent sur des liaisons WAN à bande passante limitée.
Serveur de chargement	Chaîne de 256 caractères maximum		Identifie le serveur IPv4 secondaire utilisé par le téléphone pour obtenir des micrologiciels et mises à niveau. Le format de l'adresse est : **adresse:<port>@@base=<0-7>;pfs=<0-1>**
Serveur de chargement IPv6	Chaîne de 256 caractères maximum		Identifie le serveur IPv6 secondaire utilisé par le téléphone pour obtenir des micrologiciels et mises à niveau. Le format de l'adresse est : **[addresse]:<port>@@base=<0-7>;pfs=<0-1>**
Cmde UI casque large bande	Désactivé Activé	Activé	Permet à l'utilisateur d'utiliser le codec large bande pour un casque analogique.
Casque large bande	Désactivé Activé	Activé	Active ou désactive l'utilisation d'un casque large bande sur le téléphone. Utilisé conjointement avec un casque large bande contrôlé par l'utilisateur. Pour obtenir plus d'informations, reportez-vous à Configuration du codec large bande, à la page 121.
Wi-Fi	Désactivé Activé	Activé	Permet aux téléphones IP Cisco 8861 et 8865 de se connecter au réseau Wi-Fi. Les téléphones qui ne prennent pas en charge cette fonction n'affichent pas le champ.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Port USB arrière	Désactivé Activé	8861, 8865 et 8865NR : activé	Contrôle la possibilité d'utiliser le port USB au dos des téléphones IP Cisco 8861 et 8865. Les téléphones qui ne prennent pas en charge cette fonction n'affichent pas le champ.
Port USB latéral	Désactivé Activé	Activé	Contrôle la possibilité d'utiliser le port USB latéral des téléphones IP Cisco 8851, 8851NR, 8861, 8865 et 8865NR. Les téléphones qui ne prennent pas en charge cette fonction n'affichent pas le champ.
Accès à la console	Désactivé Activé	Désactivé	Indique si la console série est activée ou désactivée.
Bluetooth	Désactivé Activé	Activé	Active ou désactive l'option Bluetooth sur le téléphone. S'il est désactivé, l'utilisateur ne peut pas activer Bluetooth sur le téléphone. Pris en charge sur les téléphones IP Cisco 8845, 8851, 8861 et 8865. Les téléphones qui ne prennent pas en charge cette fonction n'affichent pas le champ.
Autorise l'importation des contacts Bluetooth	Désactivé Activé	Activé	Permet à l'utilisateur d'importer des contacts à partir de son appareil mobile connecté à l'aide de Bluetooth. Lorsque la fonctionnalité est désactivée, l'utilisateur ne peut pas importer des contacts à partir de son appareil mobile connecté sur son téléphone. Pris en charge sur les téléphones IP Cisco 8845, 8851, 8861 et 8865. Les téléphones qui ne prennent pas en charge cette fonction n'affichent pas le champ.
Autoriser le Mode mains libres Mobile Bluetooth	Désactivé Activé	Activé	Permet aux utilisateurs de profiter des propriétés acoustiques du téléphone avec leur périphérique mobile ou leur tablette. L'utilisateur apparie le périphérique mobile ou la tablette au téléphone via Bluetooth. Lorsque la fonctionnalité est désactivée, l'utilisateur ne peut pas associer l'appareil mobile ou une tablette à son téléphone. Avec un périphérique mobile jumelé, l'utilisateur peut passer et recevoir des appels mobiles sur le téléphone. Avec une tablette, l'utilisateur peut rediriger l'audio de la tablette vers le téléphone. Les utilisateurs peuvent jumeler au téléphone plusieurs périphériques mobiles, tablettes et un casque Bluetooth. Cependant, un seul périphérique et un seul casque peuvent être connectés en même temps. Les téléphones qui ne prennent pas en charge cette fonction n'affichent pas le champ.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Profils Bluetooth	Mains libres Périphériques d'interface utilisateur	Mains libres	Indique les profils Bluetooth sur le téléphone qui sont activés ou désactivés. Les téléphones qui ne prennent pas en charge cette fonction n'affichent pas le champ.
Gratuitous ARP	Désactivé Activé	Désactivé	Active ou désactive la possibilité pour le téléphone d'acquérir les adresses MAC à partir de réponses Gratuitous ARP. Cette fonctionnalité est nécessaire pour surveiller ou enregistrer les flux vocaux.
Affichage de tous les appels sur la ligne principale	Désactivé Activé	Désactivé	Indique si tous les appels présentés à ce téléphone seront affichés sur la ligne principale ou non. L'objectif de ce champ est de faciliter pour l'utilisateur final la visualisation de tous les appels sur toutes les lignes en un coup de œil, plutôt que de devoir choisir une ligne pour afficher les appels sur cette ligne. En d'autres termes, lorsque plusieurs lignes sont configurés sur le téléphone, il est généralement plus logique d'être en mesure de voir tous les appels sur toutes les lignes sous la forme d'un affichage combiné. Lorsque cette fonctionnalité est activée, tous les appels seront affichés sur la ligne principale, mais vous pouvez toujours choisir une ligne spécifique pour filtrer l'affichage pour afficher uniquement les appels sur cette ligne spécifique.
Serveur HTTPS	HTTP et HTTPS activés HTTPS uniquement	HTTP et HTTPS activés	Contrôle le type de communication vers le téléphone. Si vous sélectionnez HTTPS uniquement, les communications téléphoniques sont plus sûres.
Serveur de journaux IPv6	Chaîne de 256 caractères maximum		Identifie le serveur de journaux IPv6. Le format de l'adresse est : **`[addresse]:<port>@@base=<0-7>;pfs=<0-1>`**
Journal à distance	Désactivé Activé	Désactivé	Contrôle la possibilité d'envoyer des journaux au serveur syslog.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Consigner le profil	Par défaut Préréglage Téléphonie SIP UI Réseau Support Mise à niveau Accessoire Sécurité Wi-Fi VPN EnergyWise MobileRemoteAc	Préréglage	Spécifie le profil d'enregistrement prédéfini. • Par défaut : niveau de consignation de débogage par défaut • Préréglage : ne va pas remplacer le paramètre d'enregistrement de débogage local du téléphone • Téléphonie : enregistre des informations sur les fonctionnalités de téléphonie ou d'appel • SIP : enregistre des informations sur la signalisation SIP • L'interface utilisateur : enregistre des informations sur l'interface utilisateur du téléphone • Réseau : enregistre des informations relatives au réseau • Support : enregistre les informations relatives au support • Mise à niveau : enregistre des informations relatives à la mise à niveau • Accessoires : enregistre des informations relatives aux accessoires • Sécurité : enregistre des informations relatives à la sécurité • Wi-Fi : enregistre des informations relatives à la Wi-Fi • VPN : enregistre des informations relatives au réseau privé virtuel • Energywise : enregistre des informations relatives aux économies d'énergie • MobileRemoteAC : enregistre des informations relatives à Mobile and Remote Access through Expressway
Publier les codecs G.722 et iSAC	Utiliser le paramètre par défaut du système Désactivé Activé	Utiliser le paramètre par défaut du système	Indique si le téléphone publie les codecs G.722 et iSAC à destination de Cisco Unified Communications Manager. • Utiliser les paramètres système par défaut : se réfère au paramètre spécifié dans le paramètre d'entreprise Publier le codec G.722. • Désactivé : ne publie pas le codec G.722 à destination de Cisco Unified Communications Manager. • Activé : publie le codec G.722 à destination de Cisco Unified Communications Manager. Pour plus d'informations, reportez-vous à la remarque qui suit le tableau.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Détecter les échecs de connexion à Cisco Unified CM	Normal Retardé	Normal	Ce champ détermine la sensibilité avec laquelle le téléphone détecte des échecs de connexion à Cisco Unified Communications Manager (Unified CM), ce qui représente la première étape avant le basculement du périphérique vers un périphérique Unified CM/SRST de secours. • Normale : la détection des échecs de connexion à Unified CM est effectuée à la vitesse standard du système. Choisissez cette valeur pour une reconnaissance plus rapide d'un échec de connexion Unified CM. • Retardé : la détection d'un basculement de connexion Unified CM se produit environ quatre fois moins vite que la normale. Choisissez cette valeur si vous préférez que le basculement soit légèrement différé, afin que le système puisse tenter de rétablir automatiquement la connexion. La différence de temps exacte entre la détection Normale et la détection Différée des échecs de connexion dépend de nombreuses variables qui changent constamment. Ce champ ne s'applique qu'à la connexion Ethernet filaire.
Négociation d'alimentation	Désactivé Activé	Activé	Permet au téléphone de gérer l'énergie à l'aide du protocole LLDP (Link Level Endpoint Discovery Protocol) et du protocole CDP (Cisco Discovery Protocol). La gestion de l'énergie ne doit pas être désactivée lorsque le téléphone est connecté à un commutateur qui prend en charge la gestion de l'énergie. S'il est désactivé, le commutateur risque de couper l'alimentation électrique du téléphone.
Fournir la tonalité depuis le bouton Libérer	Désactivé Activé	Désactivé	Contrôle si l'utilisateur entend une tonalité lorsque vous appuyez sur la touche libérer. • Désactivé : l'utilisateur n'entend pas de tonalité. • Activé : l'utilisateur entend la tonalité.
Image d'arrière-plan	Chaîne de 64 caractères maximum		Spécifie le fichier de papier peint par défaut. Lorsqu'un papier peint par défaut est défini, l'utilisateur ne peut pas modifier le papier-peint du téléphone.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Interface utilisateur Nouvel appel simplifiée	Désactivé Activé	Désactivé	Contrôle l'interface utilisateur pour la composition. Lorsque il est activé, l'utilisateur ne peut pas sélectionner un numéro à partir de la liste des appels récents. Lorsqu'il est activé, ce champ fournit une fenêtre simplifiée afin que l'utilisateur passe un appel. L'utilisateur ne voit pas la boîte de dialogue de l'historique des appels qui s'affiche lorsque le téléphone est utilisé. L'affichage de la fenêtre contextuelle est considéré comme utile, aussi l'Interface utilisateur nouvel appel simplifiée est désactivée par défaut.
Revenir à tous les appels	Désactivé Activé	Désactivé	Indique si le téléphone reviendra à Tous les appels après la fin de chaque appel ou non, si l'appel comporte un filtre autre que Ligne principale, Tous les appels ou Appels d'alerte.
Afficher l'historique des appels pour la ligne sélectionnée uniquement	Désactivé Activé	Désactivé	Contrôle l'affichage de la liste des appels récents. • Désactivé : la liste des appels récents affiche l'historique des appels de toutes les lignes. • Activé : la liste des appels récents affiche l'historique des appels pour la ligne sélectionnée.
Alerte d'appel entrant actionnable	Désactivé Afficher pour tous les appels entrants Afficher pour tous les appels invisibles	Afficher pour tous les appels entrants	Contrôle le type d'alerte d'appel entrant qui s'affiche sur l'écran du téléphone. L'objectif de ce champ est de réduire le nombre de pressions sur le bouton de l'utilisateur final nécessaires pour répondre à un appel. • Désactivé : l'alerte d'appel entrant actionnable est désactivée et l'utilisateur voit l'alerte contextuelle d'appel entrant habituelle. • Afficher pour tous les appels entrants : l'alerte actionnable d'appel entrant s'affiche pour tous les appels, peu importe leur visibilité. • Afficher pour les appels entrants invisibles : l'alerte actionnable d'appel entrant s'affiche pour les appels qui n'apparaissent pas sur le téléphone. Ce paramètre se comporte d'une manière similaire à la notification contextuelle d'alerte d'appel entrant.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
bit DF	0 1	0	Contrôle le mode d'envoi des paquets réseau. Les paquets peuvent être envoyés par tranches (fragments) de tailles diverses. Lorsque le Bit DF est défini sur 1 dans l'en-tête du paquet, les données utiles du réseau ne se fragmentent pas lorsqu'elles traversent des périphériques réseau, comme des commutateurs et des routeurs. La suppression de la fragmentation évite une analyse incorrecte du côté du récepteur, mais entraîne un léger ralentissement. Le paramètre Bit DF ne s'applique pas au trafic ICMP, VPN, VXC VPN ou DHCP.
Filtre de ligne par défaut	Liste des noms de périphériques téléphoniques séparés par des virgules		Indique la liste des téléphones figurant dans le filtre par défaut. Lorsque le filtre de ligne par défaut est configuré, les utilisateurs voient un filtre nommé `planification quotidienne` dans **Notifications d'appel** dans le menu **Paramètres** > **Préférences** du téléphone. Le filtre Planning quotidien s'ajoute au filtre Tous les appels prédéfini. Si le filtre de ligne par défaut n'est pas configuré, le téléphone vérifie toutes les lignes provisionnées. S'il est configuré, le téléphone vérifie les lignes paramétrées sur Cisco Unified Communications Manager si l'utilisateur sélectionne le filtre par défaut comme filtre actif ou s'il n'y a pas de filtre personnalisé. Les filtres de ligne personnalisés permettent de filtrer les lignes de priorité élevée pour réduire l'activité d'alerte. Vous pouvez définir la priorité de notification d'appel d'alerte sur un sous-ensemble de lignes couvert par un filtre d'alerte. Le filtre personnalisé génère des alertes contextuelles traditionnelles ou des alertes actionnables pour les appels entrants sur les lignes sélectionnées. Pour chaque filtre, seul le sous-ensemble de lignes couvert génère une alerte. Cette fonctionnalité offre un moyen pour les utilisateurs ayant plusieurs lignes de réduire l'activité d'alerte par le filtrage et l'affichage des alertes qu'à partir de lignes de haute priorité. Les utilisateurs finaux peuvent la configurer eux-mêmes. Vous pouvez également programmer le filtre de ligne par défaut et envoyer le filtre au niveau du téléphone.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
La plus faible priorité d'état de la ligne en alerte	Désactivé Activé	Désactivé	Indique l'état d'alerte lorsque vous utilisez des lignes partagées. • Désactivé : lorsqu'un appel entrant est en alerte sur la ligne partagée, l'icône d'état de la LED ou de la ligne indique l'état d'alerte au lieu d'Utilisé à distance. • Activé : lorsqu'un appel entrant est en alerte sur la ligne partagée, l'utilisateur voit l'icône Utilisé à distance.
Affichage à une seule colonne du KEM (Module d'extension de touches)	Désactivé Activé	Désactivé	Contrôle l'affichage du module d'extension de touches. • Désactivé : le module d'extension utilise le mode deux colonnes. • Activé : le module d'extension utilise le mode une colonne. Les téléphones qui ne prennent pas en charge cette fonction n'affichent pas le champ.
Energy Efficient Ethernet (EEE) : port PC	Désactivé Activé	Désactivé	Contrôle EEE sur le port PC.
Energy Efficient Ethernet (EEE) : port de commutation	Désactivé Activé	Désactivé	Contrôle EEE sur le port de commutation.
Démarrer le port vidéo			Définit le début de la plage de ports pour les appels vidéo. Les téléphones qui ne prennent pas en charge cette fonction n'affichent pas le champ.
Arrêter le port vidéo			Définit la fin de la plage de ports pour les appels vidéo. Les téléphones qui ne prennent pas en charge cette fonction n'affichent pas le champ.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Informations d'identification utilisateur permanentes pour la connexion à Expressway	Désactivé Activé	Désactivé	Contrôle si le téléphone stocke les informations de connexion des utilisateurs. Désactivé, l'utilisateur voit toujours l'invite pour se connecter au serveur Expressway for Mobile and Remote Access (MRA). Si vous voulez faciliter la connexion des utilisateurs, vous activez ce champ afin que les informations d'identification de connexion à Expressway soient permanentes. L'utilisateur doit alors seulement saisir ses informations d'identification de connexion la première fois. À n'importe quel moment par la suite (lorsque le téléphone est sous tension hors site), les informations de connexion sont pré remplies sur l'écran de connexion. Pour plus d'informations, reportez-vous à la section Mobile and Remote Access Through Expressway, à la page 183.
URL de téléchargement pour l'assistance clients	Chaîne de 256 caractères maximum		Fournit l'URL de l'outil de rapport de problème (PRT). Si vous déployez des périphériques dotés de Mobile and Remote Access through Expressway, vous devez aussi ajouter l'adresse du serveur PRT dans la liste des serveurs HTTP autorisés du serveur Expressway. Pour plus d'informations, reportez-vous à la section Mobile and Remote Access Through Expressway, à la page 183.
Admin Web	Désactivé Activé	Désactivé	Active ou désactive l'accès administrateur aux pages web du téléphone via un navigateur web. Pour plus d'informations, reportez-vous à la section Configuration de la Page d'Administration du téléphone, à la page 111. Les téléphones qui ne prennent pas en charge cette fonction n'affichent pas le champ.
Mot de passe Admin	Chaîne de 8 à 127 caractères		Définit le mot de passe administrateur lorsque vous accédez aux pages web du téléphone en tant qu'administrateur. Les téléphones qui ne prennent pas en charge cette fonction n'affichent pas le champ.
Serveur WLAN SCEP	Chaîne de 256 caractères maximum		Spécifie le serveur SCEP utilisé par le téléphone pour obtenir les certificats d'authentification WLAN. Saisissez le nom d'hôte ou l'adresse IP (format d'adressage IP standard) du serveur. Les téléphones qui ne prennent pas en charge cette fonction n'affichent pas le champ.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Empreinte d'autorité de certification racine WLAN (SHA256 ou SHA1)	Chaîne de 95 caractères maximum		Spécifie l'empreinte SHA256 ou SHA1 de l'autorité de certification racine à utiliser pour la validation au cours du processus SCEP lors de l'émission de certificats pour l'authentification WLAN. Nous vous recommandons d'utiliser l'empreinte SHA256, qui peut être obtenue par OpenSSL (par exemple openssl x509 dans rootca.cer -sha256 -fingerprint) ou à l'aide d'un navigateur Web pour examiner les détails du certificat. Entrez la valeur des 64 caractères hexadécimaux pour l'empreinte SHA256 ou la valeur des 40 caractères hexadécimaux pour l'empreinte SHA1 avec un séparateur commun (deux-points, tiret, point, espace) ou sans séparateur. Si vous utilisez un séparateur, alors le séparateur doit être placé à intervalle régulier après tous les 2, 4, 8, 16 ou 32 caractères hexadécimaux pour une empreinte SHA256 ou tous les 2, 4 ou 8 caractères hexadécimaux pour une empreinte SHA1. Les téléphones qui ne prennent pas en charge cette fonction n'affichent pas le champ.
Tentatives d'authentification WLAN			Les téléphones qui ne prennent pas en charge cette fonction n'affichent pas le champ.
Mode invite de profil 1 WLAN	Désactivé Activé	Désactivé	Les téléphones qui ne prennent pas en charge cette fonction n'affichent pas le champ.
Mode ligne	Mode ligne Session Mode ligne renforcée	Mode ligne Session	Contrôle la ligne affichée sur le téléphone. • Mode ligne Session : les boutons d'un côté de l'écran sont des touches de ligne. • Mode ligne renforcée : les boutons des deux côtés de l'écran du téléphone sont des touches de ligne. La numérotation prédictive et les alertes d'appel entrants actionnables sont activées par défaut en mode ligne renforcée.
Sonnerie Configurable Admin	Désactivé Lever de soleil Compression d'impulsions 1 Compression d'impulsions 2	Désactivé	Contrôle la sonnerie, ainsi que la possibilité pour les utilisateurs de définir la sonnerie. • Lorsque ce paramètre est défini à la valeur **désactivé**, les utilisateurs peuvent configurer la sonnerie par défaut de leur téléphone. • Pour toutes les autres valeurs, les utilisateurs ne peuvent pas modifier la sonnerie. L'élément de menu **Sonnerie** du menu **Paramètres** est grisé.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Utilisation du Service clientèle	Chaîne de 64 caractères maximum	Vide	Utiliser uniquement pour le centre d'assistance technique de Cisco.
Désactiver les codes de chiffrement TLS	Reportez-vous à Désactiver les chiffrements Transport Layer Security, à la page 171.	Aucun	Désactive le code de chiffrement TLS sélectionné. Désactivez plus d'une suite de chiffrement en sélectionnant et maintenant la touche **Ctrl** sur votre clavier. Si vous sélectionnez tous les codes de chiffrement du téléphone, le service TLS du téléphone est affecté.
Alerte Parler moins fort	Activé Désactivé	Activé	Contrôle la fonctionnalité Parler moins fort • Désactivé : • Le téléphone n'affiche pas l'option **Parler moins fort** dans le menu **Paramètres** . • Les utilisateurs ne verront pas le message à l'écran lorsqu'ils parleront fort. • Activé : • Les utilisateurs contrôlent la fonctionnalité à partir de l'option **Parler moins fort** du menu **Paramètres** . Par défaut, ce champ est défini sur **Activer**.
Marquer un appel comme étant indésirable	Activé Désactivé	Activé	Contrôle la fonctionnalité Marquer l'appel comme indésirable. • Désactivé : • Le téléphone n'affiche pas la touche de fonction **Marquer comme indésirable** . • L'élément **Liste de courriers indésirables** du menu **Paramètres** ne s'affiche pas. • S'il y a une liste de courriers indésirables, la liste est effacée et ne peut pas être récupérée. • Activé : • Le téléphone affiche la touche de fonction **Marquer comme indésirable** . • L'élément **Liste de courriers indésirables** du menu **Paramètres** s'affiche.
Dédier une ligne pour Call Park	Désactivé Activé	Activé	Contrôle si un appel parqué occupe ou non une ligne. Pour plus d'informations, reportez-vous à la documentation de Cisco Unified Communications Manager.

Nom du champ	Type de champ ou choix	Par défaut	Description et instructions d'utilisation
Affichage des libellés de ligne dans ELM	Désactivé Activé	Activé	Contrôle l'affichage de l'étiquette de ligne pendant un appel lorsque le mode ligne étendue est configuré. • Activé • Si le nom de l'appelant est configuré, il affiche le nom dans la première ligne de la session d'appel et l'étiquette de ligne locale sur la deuxième ligne. • Si le nom de l'appelant n'est pas configuré, il affiche le numéro distant sur la première ligne et l'étiquette de ligne locale sur la deuxième ligne. • Désactivé • Si le nom de l'appelant est configuré, il affiche le nom sur la première ligne de la session d'appel et le numéro sur la seconde ligne. • Si le nom de l'appelant n'est pas configuré, il affiche **uniquement** le numéro distant. Ce champ est obligatoire.

Remarque La négociation de codecs s'effectue en deux étapes :

1. Le téléphone publie le codec pris en charge à destination de Cisco Unified Communications Manager. Tous les points d'accès ne prennent pas en charge le même ensemble de codecs.
2. Lorsque Cisco Unified Communications Manager obtient la liste des codecs pris en charge à partir de tous les téléphones impliqués dans la tentative d'appel, il choisit un codec pris en charge par tous les téléphones, en fonction de plusieurs facteurs y compris le paramètre de paire de régions.

Meilleures pratiques en matière de Configuration de fonction

Vous pouvez configurer les fonctionnalités du téléphone en fonction des besoins de vos utilisateurs. Mais nous avons des recommandations pour certaines situations et déploiements qui peuvent vous aider.

Environnements à volume élevé d'appels

Dans un environnement à volume d'appels élevé, il est recommandé de configurer certaines fonctions de manière spécifique.

Champ	Zone d'administration	Paramètre recommandé
Toujours utiliser la ligne principale	Informations sur le périphérique	Désactivé ou Activé Pour obtenir plus d'informations, reportez-vous à Champ : toujours utiliser la ligne principale, à la page 171.
Alerte d'appel entrant actionnable	Configuration spécifique au produit	Afficher pour tous les appels entrants
Affichage de tous les appels sur la ligne principale	Configuration spécifique au produit	Activé
Revenir à tous les appels	Configuration spécifique au produit	Activé

Environnements multilignes

Dans un environnement multlignes, il est recommandé de configurer certaines fonctions de manière spécifique.

Champ	Zone d'administration	Paramètre recommandé
Toujours utiliser la ligne principale	Informations sur le périphérique	Désactivé Pour obtenir plus d'informations, reportez-vous à Champ : toujours utiliser la ligne principale, à la page 171.
Alerte d'appel entrant actionnable	Configuration spécifique au produit	Afficher pour tous les appels entrants
Affichage de tous les appels sur la ligne principale	Configuration spécifique au produit	Activé
Revenir à tous les appels	Configuration spécifique au produit	Activé

Environnement de mode ligne Session

Le Mode ligne renforcée est l'outil par défaut pour la gestion de la plupart des environnements d'appel. Toutefois, si ce mode ne correspond pas au mieux à vos besoins, vous pouvez utiliser le mode ligne Session.

Champ	Zone d'administration	Paramétrage recommandé pour le mode ligne Session
Affichage de tous les appels sur la ligne principale	Configuration spécifique au produit	Désactivé
Revenir à tous les appels	Configuration spécifique au produit	Désactivé
Alerte d'appel entrant actionnable	Configuration spécifique au produit	Activé par défaut (version du micrologiciel 11.5 (1) ou version ultérieure).

Rubriques connexes

Configuration des touches de ligne supplémentaires, à la page 207
Fonctions disponibles en mode ligne renforcée, à la page 207

Champ : toujours utiliser la ligne principale

Ce champ indique si la ligne principale sur un téléphone IP est utilisée lorsqu'un utilisateur décroche. Si ce paramètre est défini sur Vrai, lorsqu'un téléphone décroche, la ligne principale est sélectionnée et devient la ligne active. Même si un appel sonne sur la seconde ligne de l'utilisateur, lorsque le téléphone est décroché, il rend uniquement la première ligne active. Il ne répond pas à l'appel entrant sur la seconde ligne. Dans ce cas, l'utilisateur doit sélectionner la seconde ligne pour répondre à l'appel. La valeur par défaut est Faux.

L'objectif du champ Toujours utiliser la ligne principale est très similaire à la combinaison Afficher tous les appels sur la ligne principale et Récupérer tous les appels lorsque de ces deux fonctions sont activées. Toutefois, la principale différence est que lorsque Toujours utiliser la ligne principale est activée, les appels entrants sont sans réponse sur la seconde ligne. Seule la tonalité est émise sur la ligne principale. Il existe certains environnements de volume élevé d'appels où il s'agit de l'expérience utilisateur de votre choix. En général, il est préférable de laisser ce champ désactivé à l'exception des environnements de volume élevé d'appels qui nécessitent cette fonction.

Désactiver les chiffrements Transport Layer Security

Vous pouvez désactiver les codes de sécurité TLS (Transport Layer Security) à l'aide du paramètre **Désactiver les codes de chiffrement TLS**. Cela vous permet d'adapter votre sécurité aux vulnérabilités connues et d'aligner votre réseau avec les stratégies de votre entreprise en matière de codes de chiffrement.

Aucun n'est le paramètre par défaut.

Désactivez plus d'une suite de chiffrement en sélectionnant et maintenant la touche **Ctrl** sur votre clavier. Si vous sélectionnez tous les codes de chiffrement du téléphone, le service TLS du téléphone est affecté. Les options disponibles sont les suivantes :

- Aucune
- 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

Pour plus d'informations sur la sécurité du téléphone, consultez *le Livre blanc de présentation de la sécurité du téléphone IP Cisco série 7800 et 8800* (https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html).

Activer l'historique des appels d'une ligne partagée

Permet de visualiser votre activité de lignes partagées dans l'historique des appels du téléphone. Cette fonction :

- Journalise les appels en absence d'une ligne partagée.
- Journalise tous les appels pris et passés sur une ligne partagée.

Avant de commencer

Désactivez la confidentialité avant d'activer l'historique des appels pour la ligne partagée. Sinon, l'historique des appels n'affiche pas les appels que les autres utilisateurs prennent.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone**.

Étape 2 Localisez le téléphone à configurer.

Étape 3 Naviguez jusqu'au journal des appels depuis la liste déroulante des lignes partagées dans la zone de configuration spécifique au produit.

Étape 4 Sélectionnez **Activé** dans la liste déroulante.

Étape 5 Sélectionnez **Enregistrer**.

Planification du mode Économies d'énergie pour un téléphone IP Cisco

Pour économiser de l'énergie et pour assurer la longévité de l'affichage du téléphone, vous pouvez configurer l'écran pour qu'il soit désactivé lorsqu'il n'est pas utilisé.

Vous pouvez configurer des paramètres dans Cisco Unified Communications Manager Administration pour éteindre l'écran à une heure donnée certains jours et pendant toute la journée les autres jours de la semaine. Par exemple, vous pouvez désactiver l'écran après les heures d'ouverture les jours de semaine, et toute la journée le samedi et le dimanche.

Vous pouvez effectuer l'une des actions suivantes pour activer l'écran lorsqu'il est désactivé :

- Appuyer sur n'importe quel bouton du téléphone.

  Le téléphone exécute l'action indiquée par ce bouton et active l'écran.

- Décrocher le combiné.

Lorsque vous activez l'écran, il reste allumé jusqu'à ce que le téléphone soit resté inactif pendant une durée donnée, puis est automatiquement désactivé.

Pour obtenir plus d'informations, reportez-vous à Configuration spécifique au produit, à la page 149

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone**.

Étape 2 Localisez le téléphone à configurer.

Étape 3 Accédez à la zone Configuration spécifique à un produit et configurez les champs suivants :

- Jours d'inactivité de l'écran

- Heure d'activation de l'écran
- Durée d'activité de l'écran
- Temporisation d'inactivité de l'écran

Tableau 32 : Champs de configuration du mode Économies d'énergie

Champ	Description
Jours d'inactivité de l'écran	Les jours pendant lesquels l'écran n'est pas automatiquement activé à l'heure indiquée dans le champ Heure d'activation de l'écran. Sélectionnez un ou plusieurs jours dans la liste déroulante. Pour sélectionner plusieurs jours, appuyez sur Ctrl et cliquez simultanément sur chaque jour souhaité.
Heure d'activation de l'écran	L'heure à laquelle l'écran est automatiquement activé tous les jours (sauf les jours indiqués dans le champ Jours d'inactivité de l'écran). Entrez l'heure dans ce champ au format 24 heures ; 00:00 correspondant à minuit. Par exemple, pour allumer automatiquement l'écran à 7 heures du matin (07:00), saisissez **07:00**. Par exemple, pour activer l'écran à 14h00, (14h00), saisissez **14h00**. Si ce champ est vide, l'écran est automatiquement activé à 0:00.
Durée d'activité de l'écran	Durée pendant laquelle l'écran reste allumé après s'être activé à l'heure spécifiée par le champ Heure d'activation de l'écran. Entrez une valeur dans ce champ au format *heures:minutes*. Par exemple, pour que l'écran reste allumé pendant 4 heures et 30 minutes après son activation automatique, entrez **04:30**. Lorsque ce champ est vide, le téléphone est désactivé à la fin de la journée (0:00). **Remarque** Si l'heure d'activation de l'écran est 0:00 et si le champ Durée d'activité de l'écran est vide (ou a la valeur 24:00), l'écran reste toujours allumé.
Temporisation d'inactivité de l'écran	La durée pendant laquelle le téléphone est inactif avant la désactivation de l'écran. S'applique uniquement lorsque l'écran a été désactivé comme planifié, et qu'il a été activé par l'utilisateur (qui a appuyé sur une touche du téléphone ou qui a soulevé le combiné). Entrez une valeur dans ce champ au format *heures:minutes*. Par exemple, pour éteindre l'écran lorsque le téléphone est inactif pendant 1 heure et 30 minutes après qu'un utilisateur a allumé l'écran, saisissez **01:30**. La valeur par défaut est 01:00.

Étape 4 Sélectionnez **Enregistrer**.

Étape 5 Sélectionnez **Appliquer la configuration**.

Étape 6 Redémarrez le téléphone.

Planifier EnergyWise sur le téléphone IP Cisco

Pour réduire la consommation électrique, configurez le téléphone pour qu'il se mette en veille (éteint) et sorte de veille (allumé) si votre système est équipé d'un contrôleur EnergyWise.

Configurez les paramètres dans Cisco Unified Communications Manager Administration pour activer EnergyWise et configurer les heures auxquelles le téléphone se met en veille et se rallume. Ces paramètres sont étroitement liés aux paramètres de configuration de l'écran du téléphone.

Lorsque le mode EnergyWise est activé et qu'une durée de mise en veille est définie, le téléphone envoie une requête au commutateur afin de le sortir de l'état de veille à l'heure définie. Le commutateur retourne une acceptation ou un refus de la requête. Si le commutateur rejette la requête ou ne répond pas, le téléphone n'est pas mis en veille. Si le commutateur accepte la requête, le téléphone inactif entre en veille, réduisant ainsi la consommation électrique à un niveau prédéfini. Un téléphone qui n'est pas inactif définit une durée d'inactivité et entre en veille dès l'expiration de la durée d'inactivité.

Pour sortir le téléphone de l'état de veille, appuyez sur Sélect. À l'heure de sortie de veille planifiée, le système restaure l'alimentation électrique du téléphone, ce qui entraîne sa sortie de veille.

Pour obtenir plus d'informations, reportez-vous à Configuration spécifique au produit, à la page 149

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone**.

Étape 2 Localisez le téléphone à configurer.

Étape 3 Naviguez jusqu'à la zone Product Specific Configuration (Configuration spécifique au produit) et définissez les champs suivants.

- Activer Power Save Plus
- Heure d'activation du téléphone
- Heure de désactivation du téléphone
- Phone Off Idle Timeout (Délai d'inactivité avant désactivation)
- Enable Audible Alert (Activer l'alerte sonore)
- Domaine EnergyWise
- EnergyWise Secret (Secret EnergyWise)
- Allow EnergyWise Overrides (Permettre le remplacement par EnergyWise)

Tableau 33 : Champs de configuration du mode EnergyWise

Champ	Description
Activer Power Save Plus	Sélectionne le calendrier des jours où le téléphone est éteint. Vous pouvez sélectionner plusieurs jours en appuyant sur la touche Ctrl et en la maintenant enfoncée tout en cliquant sur les jours dans le calendrier. Par défaut, aucun jour n'est sélectionné. Lorsque l'option activer Power Save Plus est activée, vous recevez un message qui vous avertit de préoccupations relatives aux appels en cas d'urgence. **Avertissement** Lorsque le mode Power Save Plus (le « Mode ») est actif, les terminaux qui sont configurés pour le mode sont désactivés pour les appels en cas d'urgence et pour la réception d'appels entrants. En sélectionnant ce mode, vous acceptez les termes suivants : (i) Vous prenez l'entière responsabilité de fournir des méthodes alternatives pour contacter les services d'urgence et recevoir des appels lorsque le mode est en vigueur ; (ii) Cisco ne peut être tenu pour responsable de l'activation du mode et vous êtes le seul responsable de l'activation du mode ; (iii) Vous informez pleinement les utilisateurs des effets de ce mode sur les appels, les appels en cours et tout autre appel. **Remarque** Pour désactiver le mode Power Save Plus, déscochez la case Allow EnergyWise Overrides (Permettre le remplacement par EnergyWise). Si la case Allow EnergyWise Overrides (Permettre le remplacement par EnergyWise) est activée sans qu'aucun jour ne soit sélectionné dans le champ Activer Power Save Plus, le mode Power Save Plus n'est pas désactivé.
Heure d'activation du téléphone	Détermine l'heure à laquelle le téléphone est automatiquement allumé les jours qui sont sélectionnés dans le champ activer Power Save Plus. Entrez l'heure dans ce champ au format 24 heures ; 00:00 correspondant à minuit. Par exemple, pour allumer automatiquement le téléphone à 7h00, saisissez 07:00. Pour allumer automatiquement le téléphone à 14h00, saisissez 14h00. La valeur par défaut est un champ vide, ce qui signifie 00:00. **Remarque** L'heure d'activation du téléphone doit être ultérieure d'au moins 20 minutes à l'heure de désactivation du téléphone. Par exemple, si l'heure d'arrêt du téléphone est 07:00, l'heure de mise en route du téléphone ne doit pas être antérieure à 07:20.
Heure de désactivation du téléphone	L'heure à laquelle le téléphone s'éteint les jours qui sont sélectionnés dans le champ Activer Power Save Plus. Si les valeurs des champs Heure d'activation du téléphone et Heure de désactivation du téléphone sont identiques, le téléphone ne s'éteint pas. Entrez l'heure dans ce champ au format 24 heures ; 00:00 correspondant à minuit. Par exemple, pour éteindre automatiquement le téléphone à 7h00, saisissez 7h00. Pour éteindre automatiquement le téléphone à 14h00, (14h00), saisissez 14h00. La valeur par défaut est un champ vide, ce qui signifie 00:00. **Remarque** L'heure d'activation du téléphone doit être ultérieure d'au moins 20 minutes à l'heure de désactivation du téléphone. Par exemple, si l'heure d'arrêt du téléphone est 07:00, l'heure de mise en route du téléphone ne doit pas être antérieure à 07:20.

Champ	Description
Phone Off Idle Timeout (Délai d'inactivité avant désactivation)	La durée pendant laquelle le téléphone doit être inactif avant sa désactivation. Ce délai a lieu dans les conditions suivantes : • Lorsque le téléphone était en mode Power Save Plus, comme planifié et a été sorti du mode Power Save Plus car l'utilisateur a appuyé sur la touche **Sélect**. • Lorsque le téléphone est remis sous tension par le commutateur connecté. • Lorsque l'heure de désactivation du téléphone a été atteinte mais que le téléphone est toujours en cours d'utilisation. Les valeurs valides pour ce champ sont comprises en 20 et 1 440 minutes. La valeur par défaut est de 60 minutes.
Enable Audible Alert (Activer l'alerte sonore)	Lorsque cette option est activée, le téléphone émet une alerte sonore qui commence 10 minutes avant l'heure de désactivation du téléphone. L'alerte sonore utilise la sonnerie du téléphone, qui retentit brièvement à des instants précis pendant les 10 minutes d'alerte. La sonnerie d'alerte est émise au volume défini par l'utilisateur. Le calendrier de l'alerte sonore est le suivant : • 10 minutes avant l'arrêt, l'alerte retentit quatre fois. • 7 minutes avant l'arrêt, l'alerte retentit quatre fois. • 4 minutes avant l'arrêt, l'alerte retentit quatre fois. • 30 secondes avant l'arrêt, l'alerte retentit 15 fois ou sonne jusqu'à ce que le téléphone s'éteigne. Cette case à cocher n'est pertinente que lorsqu'un ou plusieurs jours sont sélectionnés dans la zone de liste Activer Power Save Plus.
Domaine EnergyWise	Le domaine EnergyWise qui héberge le téléphone. Ce champ peut contenir un maximum de 127 caractères.
EnergyWise Secret (Secret EnergyWise)	Le mot de passe de sécurité secret utilisé pour communiquer avec les terminaux du domaine EnergyWise. Ce champ peut contenir un maximum de 127 caractères.

Champ	Description
Allow EnergyWise Overrides (Permettre le remplacement par EnergyWise)	Cette case à cocher détermine si vous autorisez la stratégie du contrôleur de domaine EnergyWise à envoyer aux téléphones des mises à jour du niveau de puissance. Les conditions suivantes s'appliquent : • Un ou plusieurs jours doivent avoir été sélectionnés dans le champ Activer One Power Save Plus. • Les paramètres de Cisco Unified Communications Manager Administration prennent effet à la date spécifiée même si EnergyWise envoie une redéfinition. Supposons par exemple que l'heure de désactivation du téléphone est définie par 22:00 (22h00), que la valeur du champ Heure d'activation du téléphone est 06:00 (6h00), et qu'un ou plusieurs jours sont sélectionnés dans le champ Activer Power Save Plus. • Si EnergyWise demande la désactivation du téléphone à 20:00 (20h00), cette directive reste effective (en supposant qu'aucune intervention de l'utilisateur du téléphone n'ait lieu) jusqu'à l'heure d'activation du téléphone, soit 6h00. • À 6h00, le téléphone s'allume et recommence à recevoir les variations de niveau de puissance des paramètres de Unified Communications Manager Administration. • Pour changer de nouveau le niveau de puissance du téléphone, EnergyWise doit émettre une nouvelle commande de variation du niveau de puissance. **Remarque** Pour désactiver le mode Power Save Plus, déscochez la case Allow EnergyWise Overrides (Permettre le remplacement par EnergyWise). Si la case Allow EnergyWise Overrides (Permettre le remplacement par EnergyWise) est activée sans qu'aucun jour ne soit sélectionné dans le champ Activer Power Save Plus, le mode Power Save Plus n'est pas désactivé.

Étape 4 Sélectionnez **Enregistrer**.

Étape 5 Sélectionnez **Appliquer la configuration**.

Étape 6 Redémarrez le téléphone.

Configuration de la fonctionnalité Ne pas déranger

Lorsque la fonction Ne pas déranger (NPD) est activée, aucune sonnerie ne retentit lorsqu'un appel est reçu, ou aucune notification visuelle ou sonore n'a lieu.

Lorsque Ne pas déranger (NPD) est activé, la section d'en-tête de l'écran du téléphone change de couleur et `Ne pas déranger` s'affiche sur le téléphone.

Vous pouvez configurer le téléphone à l'aide d'un modèle de bouton de téléphone, en sélectionnant la fonctionnalité NPD.

Pour obtenir plus d'informations, consultez les informations sur la fonctionnalité Ne pas déranger dans la documentation de votre version de Cisco Unified Communications Manager.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone**.

Étape 2 Localisez le téléphone à configurer.

Étape 3 Définissez les paramètres suivants :

- Ne pas déranger : cette case à cocher permet d'activer NPD sur le téléphone.
- Option NPD : sonnerie désactivée, Rejet d'appel ou Utiliser le profil de téléphone commun.

  Ne spécifiez pas Refus d'appel si vous souhaitez que les appels de priorité (MLPP) fassent sonner ce téléphone lorsque la fonction NPD est activée.
- DND Incoming Call Alert (Alerte NPD pour les appels entrants) : choisissez, le cas échéant, le type d'alerte à émettre sur un téléphone pour les appels entrants lorsque la fonctionnalité NPD est active.

  Remarque Ce paramètre se trouve à la fois dans la fenêtre Profil de téléphone commun et la fenêtre de configuration du téléphone. La valeur figurant dans la fenêtre Configuration du téléphone est prioritaire.

Étape 4 Sélectionnez **Enregistrer**.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Activer le message d'accueil de l'agent

La fonction de message d'accueil permet à un agent de créer et de mettre à jour un message d'accueil préenregistré lancé au début d'un appel, par exemple un appel client, avant le début de la conversation entre l'agent et l'appelant. L'agent peut préenregistrer un ou plusieurs messages d'accueil, si nécessaire, et les créer ou les mettre à jour.

Lorsqu'un client appelle, l'agent et l'appelant entendent tous les deux le message d'accueil préenregistré. L'agent peut rester silencieux jusqu'à la fin du message d'accueil ou l'agent peut répondre à l'appel au-dessus du message.

Tous les codecs pris en charge pour le téléphone sont pris en charge pour les appels de message d'accueil de l'agent.

Pour plus d'informations sur l'insertion et la confidentialité, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.

Procédure

Étape 1 Depuis Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone**.

Étape 2 Localisez le téléphone IP à configurer.

Étape 3 Faites défiler le volet Informations sur le périphérique et définissez **Pont intégré** par Activé ou Par défaut.

Étape 4 Sélectionnez **Enregistrer**.

Étape 5 Vérifiez le paramétrage du pont :

a) Sélectionnez **Système** > **Paramètres de service**.
b) Sélectionnez le serveur et le service appropriés.
c) Allez au volet relatif aux paramètres de tout le cluster (périphérique - téléphone) et définissez **Builtin Bridge Enable** (Activer le pont intégré) par Oui.
d) Sélectionnez **Enregistrer**.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Configuration de la surveillance et de l'enregistrement

Grâce à la fonctionnalité de surveillance et d'enregistrement, un superviseur peut surveiller silencieusement des appels actifs. Aucun des participants à l'appel ne peut entendre le superviseur. Les utilisateurs peuvent entendre une alerte sonore pendant les appels qui sont surveillés.

Lorsqu'un appel est sécurisé, une icône en forme de verrou s'affiche. Les appelants peuvent aussi entendre une alerte sonore qui indique que l'appel est surveillé. Les parties connectées peuvent également entendre une alerte sonore indiquant que l'appel est sécurisé et surveillé.

Lors de la surveillance ou de l'enregistrement d'un appel actif, l'utilisateur peut recevoir ou passer des appels Intercom ; toutefois, s'il passe un appel Intercom, l'appel actif est mis en attente. Cette action entraîne l'interruption de l'enregistrement et la suspension de la surveillance. Pour reprendre la surveillance, la personne qui fait l'objet de la surveillance doit reprendre l'appel.

Pour plus d'informations sur la surveillance et l'enregistrement, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.

La procédure suivante permet d'ajouter un utilisateur aux groupes d'utilisateurs de la surveillance standard.

Avant de commencer

Cisco Unified Communications Manager doit être configuré pour prendre en charge la surveillance et l'enregistrement.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **User management (Gestion des utilisateurs)** > **Application User (Utilisateur de l'application)**.

Étape 2 Cochez les groupes d'utilisateurs Standard CTI Allow Call Monitoring (CTI standard - Permettre la surveillance des appels) et Standard CTI Allow Call Recording (CTI standard - Permettre l'enregistrement des appels).

Étape 3 Cliquez sur **Ajouter sélection**.

Étape 4 Cliquez sur **Add to User Group** (Ajouter au groupe d'utilisateurs).

Étape 5 Ajoutez les téléphones des utilisateurs à la liste des périphériques contrôlés des utilisateurs d'application.

Étape 6 Sélectionnez **Enregistrer**.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Configuration de la notification de renvoi d'appel

Vous pouvez contrôler les paramètres de renvoi d'appel.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone**.

Étape 2 Localisez le téléphone à configurer.

Étape 3 Configurez les champs de notification de renvoi d'appel.

Champ	Description
Nom de l'appelant	Lorsque cette case est cochée, le nom de l'appelant est affiché dans la fenêtre de notification. Cette case est cochée par défaut.
Numéro de l'appelant	Lorsque cette case est cochée, le numéro de l'appelant est affiché dans la fenêtre de notification. Par défaut, cette case à cocher n'est pas sélectionnée.
Redirected Number (Redirigé par)	Lorsque cette case est cochée, les informations sur le dernier appelant à avoir renvoyé l'appel sont affichées dans la fenêtre de notification. Exemple : si l'appelant A appelle B, mais que B a renvoyé tous ses appels à C, et que C a renvoyé tous ses appels à D, la zone de notification de l'écran du téléphone de D contient les informations sur le téléphone de l'appelant C. Par défaut, cette case à cocher n'est pas sélectionnée.
Numéro composé	Lorsque cette case est cochée, les informations sur le destinataire initial de l'appel sont affichées dans la fenêtre de notification. Exemple : si l'appelant A appelle B, mais que B a renvoyé tous ses appels à C, et que C a renvoyé tous ses appels à D, la zone de notification de l'écran du téléphone de D contient les informations sur le téléphone de l'appelant B. Cette case est cochée par défaut.

Étape 4 Sélectionnez **Enregistrer**.

Activation de la fonction Ligne occupée pour des listes d'appels

Le champ Ligne occup. pour list. d'app. contrôle également la fonctionnalité d'état de la ligne du répertoire d'entreprise.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, cliquez sur **Système** > **Paramètres d'entreprise**.

Étape 2 Pour le champ Ligne occup. pour list. d'app., activez ou désactivez la fonctionnalité.

Par défaut, la fonction est désactivée.

Les paramètres que vous définissez dans la zone Product Specific Configuration (Configuration spécifique au produit) peuvent aussi être affichés dans la fenêtre Configuration du périphérique de plusieurs appareils et dans la fenêtre Configuration des téléphones d'entreprise. Si vous définissez les mêmes paramètres dans ces fenêtres, le paramètre prioritaire est déterminé dans l'ordre suivant :

1. Paramètres de la fenêtre Configuration du périphérique
2. Paramètres de la fenêtre Profil de téléphone commun
3. Paramètres de la fenêtre Configuration des téléphones d'entreprise

Étape 3 Sélectionnez **Enregistrer**.

Configuration de Energy Efficient Ethernet (EEC) pour les ports SW et PC

La norme IEEE 802.3az Energy Efficient Ethernet (EEE) est une extension de la norme IEEE 802.3 assurant la réduction de la consommation énergétique sans réduire les fonctions vitales des interfaces réseau. La configuration de EEE permet à l'administrateur de contrôler les fonctions EEE sur le port PC et le port de commutateur.

Remarque Les administrateurs doivent vérifier que la case Forcer est cochée sur toutes les pages UCM applicable pour que EEE puisse fonctionner.

L'administrateur contrôle les fonctions EEE grâce aux deux paramètres suivants :

- **Energy Efficient Ethernet** : port PC : assure une connexion fluide avec les ordinateurs. L'administrateur peut sélectionner les options Activé ou Désactivé pour contrôler cette fonction.
- **Energy Efficient Ethernet** : port de commutateur : assure une connexion fluide

Pour obtenir plus d'informations, reportez-vous àConfiguration spécifique au produit, à la page 149

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez l'une des fenêtres suivantes :

- **Périphérique** > **Téléphone**
- **Périphérique** > **Paramètres du périphérique** > **Profil du téléphone commun**
- **Système** > **Configuration des téléphones d'entreprise**

Si vous configurez le paramètre dans plusieurs fenêtres, l'ordre de priorité est le suivant :

1. **Périphérique** > **Téléphone**
2. **Périphérique** > **Paramètres du périphérique** > **Profil du téléphone commun**

3. **Système** > **Configuration des téléphones d'entreprise**

Étape 2 Si nécessaire, localisez le téléphone.

Étape 3 Définissez les champs **Energy Efficient Ethernet : port PC** et **Energy Efficient Ethernet : port switch**.

- Energy Efficient Ethernet : port PC
- Energy Efficient Ethernet: Switch Port (Optimisation énergétique d'Ethernet : Port de commutation)

Étape 4 Sélectionnez **Enregistrer**.

Étape 5 Sélectionnez **Appliquer la configuration**.

Étape 6 Redémarrez le téléphone.

Configurer la plage de ports RTP/sRTP

Vous pouvez configurer les valeurs des ports du protocole de transport en temps réel (RTP) et du protocole de transport sécurisé en temps réel (sRTP) dans le profil SIP. Les valeurs des ports RTP et sRTP sont comprises entre 2048 et 65535, la valeur par défaut étant comprise entre 16384 et 32764. Certaines valeurs de port dans la plage des ports RTP et sRTP sont destinées à d'autres services téléphoniques. Vous ne pouvez pas configurer ces ports pour RTP ou sRTP.

Pour plus d'informations sur les profils SIP, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.

Procédure

Étape 1 Sélectionnez **Périphérique** > **Paramètres du périphérique** > **Profil SIP**

Étape 2 Choisissez les critères de recherche à utiliser et cliquez sur **Find** (Rechercher).

Étape 3 Sélectionnez le profil à modifier.

Étape 4 Définissez le Port de média de début et le Port de média de fin par des valeurs incluant le début et la fin de la plage de ports.

La liste suivante présente les ports UDP utilisés pour d'autres services téléphoniques et qui ne sont donc pas disponibles pour les protocoles RTP et sRTP :

Port 4051

Utilisé pour la fonctionnalité Partage d'image

Port 5060

Utilisé pour le transport SIP sur UDP

Plage de ports 49152 à 53247

Utilisée pour les ports éphémères locaux

Plage de ports 53248 à 65535

Utilisée pour la fonctionnalité VPN à tunnel unique de VxC

Étape 5 Cliquez sur **Enregistrer**.

Étape 6 Cliquez sur **Appliquer la configuration**.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Mobile and Remote Access Through Expressway

Mobile and Remote Access Through Expressway(MRA) permet aux utilisateurs distants de se connecter aisément et en toute sécurité au réseau d'entreprise, sans utiliser de tunnel client de réseau privé virtuel (VPN). Expressway utilise le protocole TLS (Transport Layer Security) pour sécuriser le trafic réseau. Pour qu'un téléphone puisse authentifier un certificat Expressway et établir une session TLS, il faut que le certificat Expressway soit signé par une autorité de certification publique approuvée par le micrologiciel du téléphone. Il n'est pas possible d'installer ou d'approuver d'autres certificats d'autorité de certification sur les téléphones pour authentifier un certificat Expressway.

La liste des certificats d'autorité de certification incorporés au micrologiciel du téléphone est disponible à l'adresse http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html.

Mobile and Remote Access Through Expressway (MRA) fonctionne avec Cisco Expressway. Vous devez donc vous familiariser avec la documentation de Cisco Expressway, notamment le *Guide d'administration de Cisco Expressway* et le *Guide de déploiement de la configuration de base de Cisco Expressway*. La documentation de Cisco Expressway est disponible à l'adresse http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html.

Seul le protocole IPv4 est pris en charge pour les utilisateurs de Mobile and Remote Access Through Expressway.

Pour obtenir des informations supplémentaires sur l'utilisation de Mobile and Remote Access Through Expressway, reportez-vous aux documents suivants :

- *Cisco Preferred Architecture for Enterprise Collaboration, Design Overview (Architecture préférée par Cisco pour Enterprise Collaboration, présentation conceptuelle)*
- *Cisco Preferred Architecture for Enterprise Collaboration, CVD (Architecture préférée par Cisco pour Enterprise Collaboration, CVD)*
- *Guide de déploiement de Unified Communications Mobile and Remote Access via Cisco VCS*
- *Cisco TelePresence Video Communication Server (VCS), Configuration Guides (Guides de configuration de Cisco TelePresence Video Communication Server (VCS))*
- *Guide de déploiement de Mobile and Remote Access Through Cisco Expressway*

Au cours du processus d'enregistrement du téléphone, le téléphone synchronise la date et l'heure affichées avec celles du serveur NTP (Network Time Protocol). Avec MRA, la balise de l'option DHCP 42 est utilisée pour localiser les adresses IP des serveurs NTP désignés pour la synchronisation de la date et de l'heure. Si la balise de l'option DHCP 42 est introuvable dans les informations de configuration, le téléphone recherche la balise 0.tandberg.pool.ntp.org pour identifier les serveurs NTP.

Après l'enregistrement, le téléphone utilise les informations du message SIP pour synchroniser la date et l'heure affichées sauf si un serveur NTP est configuré dans la configuration du téléphone de Cisco Unified Communications Manager.

Remarque Si l'option TFTP Encrypted Config (Configuration chiffrée par TFTP) est activée pour le profil de sécurité d'un de vos téléphones, vous ne pouvez pas utiliser le téléphone avec Mobile and Remote Access. La solution MRA ne prend pas en charge l'interaction des périphériques avec la fonction proxy d'autorité de certificat (CAPF).

Mobile and Remote Access Through Expressway prend en charge le mode Ligne améliorée.

Le mode SIP OAuth est pris en charge pour MRA. Ce mode vous permet d'utiliser des jetons d'accès OAuth pour l'authentification dans des environnements sécurisés.

Remarque Pour SIP OAuth en mode Mobile and Remote Access (Accès mobile et à distance, MRA), n'utilisez que l'intégration par code d'activation avec Mobile and Remote Access lorsque vous déployez le téléphone. L'activation avec un nom d'utilisateur et un mot de passe n'est pas prise en charge.

SIP OAuth mode nécessite Expressway x14.0 (1) et versions ultérieures, ou Cisco Unified Communications Manager 14.0 (1) et versions ultérieures

Pour obtenir des informations supplémentaires sur le mode AAuth SIP, consultez le *Guide de Configuration des fonctionnalités de Cisco Unified Communications Manager*, version 14.0(1) ou ultérieure.

Scénarios de déploiement

Les sections suivantes présentent les divers scénarios de déploiement de Mobile and Remote Access Through Expressway.

Un utilisateur sur site se connecte au réseau de l'entreprise

Après avoir déployé Mobile and Remote Access Through Expressway, connectez-vous au réseau de l'entreprise lorsque vous êtes sur site. Le téléphone détecte le réseau et s'enregistre auprès de Cisco Unified Communications Manager.

Un utilisateur hors site se connecte au réseau de l'entreprise

Lorsque vous n'êtes pas au bureau, le téléphone détecte qu'il est en mode hors site. La fenêtre de connexion de Mobile and Remote Access Through Expressway s'affiche et vous vous connectez au réseau de l'entreprise.

Notez les éléments suivants:

- Vous devez avoir un domaine de service, un nom d'utilisateur ainsi qu'un mot de passe valides pour pouvoir vous connecter au réseau.
- Réinitialisez le mode de service pour effacer le paramètre TFTP secondaire avant de pouvoir accéder au réseau de l'entreprise. Cela efface le paramètre Serveur TFTP secondaire pour que le téléphone puisse détecter le réseau hors site et qu'il ne tente pas d'établir une connexion VPN. Ignorez cette étape si un téléphone est déployé pour la première fois.
- Si les options DHCP 150 ou 66 sont activées sur le routeur de votre réseau, vous risquez de ne pas pouvoir vous connecter au réseau d'entreprise. Réinitialisez le mode de service pour entrer en mode MRA.

Un utilisateur hors site se connecte au réseau de la société à l'aide d'un VPN

Lorsque vous êtes hors site, connectez-vous au réseau de l'entreprise à l'aide d'un VPN, après avoir déployé Mobile and Remote Access Through Expressway.

Effectuer une réinitialisation de base pour réinitialiser les configurations de votre téléphone si celui-ci rencontre une erreur.

Vous devez configurer le paramètre TFTP alternatif (**Paramètres Admin** > **Paramètres réseau** > **IPv4**, champ**Serveur TFTP alternatif 1**).

Rubriques connexes

Réinitialisation de base, à la page 281

Chemins de média et établissement de la connectivité Interactive

Vous pouvez déployer l'établissement de la connectivité Interactive (ECI) pour améliorer la fiabilité des appels mobiles et l'accès à distance (MRA, Mobile and Remote Access) qui passent par un pare-feu ou une traduction d'adresses réseau (NAT). ICE est un déploiement facultatif qui utilise des services Serial Tunneling and Traversal Using Relays around NAT (TURN) pour sélectionner le meilleur chemin de médias pour un appel.

Le serveur secondaire TURN et le basculement du serveur TURN ne sont pas pris en charge.

Pour plus d'informations sur MRA et ICE, reportez-vous au *Guide de configuration système de Cisco Unified Communications Manager, version 12.0(1)* ou ultérieure. Vous pouvez également trouver des informations supplémentaires dans les documents de demande de commentaires de l'Internet Engineering Task Force (IETF) :

- *Traversée à l'aide de relais autour du NAT (TURN) : extensions de relais aux utilitaires de conversion de session pour NAT (STUN)* (RFC 5766)
- *Établissement de la connectivité interactive (ECI) : Un protocole de réseau pour la traversée de traduction d'adresse (NAT) pour les protocoles d'offre/de réponse* (RFC 5245)

Fonctionnalités téléphoniques disponibles pour Mobile and Remote Access Through Expressway

Mobile and Remote Access Through Expressway fournit un accès sécurisé sans VPN aux services de collaboration des utilisateurs d'appareils Cisco mobiles et distants. Toutefois, pour préserver la sécurité du réseau, l'accès à certaines fonctionnalités téléphoniques est restreint.

Les fonctionnalités téléphoniques disponibles dans Mobile and Remote Access Through Expressway figurent dans la liste ci-après.

Tableau 34 : Prise en charge des fonctionnalités et Mobile and Remote Access Through Expressway

Fonctionnalité du téléphone	Version du micrologiciel du téléphone
Numérotation abrégée	10.3(1) et ultérieure
Répondre au premier	11.5(1) SR1 et ultérieure
Parcage d'appels dirigé assisté	10.3(1) et ultérieure
Réponse automatique	11.5(1) SR1 et ultérieure
Insertion et InsConf	11.5(1) SR1 et ultérieure

Fonctionnalité du téléphone	Version du micrologiciel du téléphone
Fonction de supervision de ligne occupée (FLO)	10.3(1) et ultérieure
Interception - Supervision de ligne occupée (FLO)	10.3(1) et ultérieure
Numérotation simplifiée - Supervision de ligne occupée (FLO)	10.3(1) et ultérieure
Rappel automatique	10.3(1) et ultérieure
Renvoi d'appel	10.3(1) et ultérieure
Notification de renvoi d'appel	10.3(1) et ultérieure
Parcage d'appels	10.3(1) et ultérieure
Interception d'appel	10.3(1) et ultérieure
Cisco Unified Serviceability	11.5(1) SR1 et ultérieure
Licence d'accès client (LAC)	11.5(1) SR1 et ultérieure
Conférence	10.3(1) et ultérieure
Liste de la conférence / Supprimer un participant	11.5(1) SR1 et ultérieure
Répertoire d'entreprise	11.5(1) SR1 et ultérieure
Applications CTI (contrôlée par CTI)	11.5(1) SR1 et ultérieure
Transfert direct	10.3(1) et ultérieure
Parcage d'appels dirigé	10.3(1) et ultérieure
Sonnerie distinctive	11.5(1) SR1 et ultérieure
Détourner	10.3(1) et ultérieure
Mode de ligne renforcée	12.1(1) et ultérieure
Détourner	10.3(1) et ultérieure
Codes d'accès forcé et Codes d'affaire client	11.5(1) SR1 et ultérieure
Interception d'appels de groupe	10.3(1) et ultérieure
Attente/Reprise	10.3(1) et ultérieure
Récupération d'un appel en attente	10.3(1) et ultérieure
Renvoi immédiat	10.3(1) et ultérieure
Joindre	10.3(1) et ultérieure
Identification d'appel malveillant (IDAM)	11.5(1) SR1 et ultérieure

Fonctionnalité du téléphone	Version du micrologiciel du téléphone
Conférence MultConf (Meet-Me)	10.3(1) et ultérieure
Indicateur de message en attente	10.3(1) et ultérieure
Connectivité mobile	10.3(1) et ultérieure
Accès vocal mobile	10.3(1) et ultérieure
Préséance et préemption à plusieurs niveaux (MLPP, Multilevel Precedence and Preemption)	11.5(1) SR1 et ultérieure
Téléphone IP	11.5(1) SR1 et ultérieure
Musique d'attente (MoH)	10.3(1) et ultérieure
Silence	10.3(1) et ultérieure
Profils réseau (automatiques)	11.5(1) SR1 et ultérieure
Composition avec le combiné décroché	10.3(1) et ultérieure
Composition d'un numéro sans décrocher le combiné	10.3(1) et ultérieure
Composition de numéro avec plus	10.3(1) et ultérieure
Confidentialité	11.5(1) SR1 et ultérieure
Appel automatique d’une ligne privée (PLAR)	11.5(1) SR1 et ultérieure
Renumérotation	10.3(1) et ultérieure
Numérotation rapide (ne prend pas en charge une pause)	10.3(1) et ultérieure
Bouton d'accès à l’URL des services	11.5(1) SR1 et ultérieure
Transfert	10.3(1) et ultérieure
Composition d'URI (Uniform Resource Identifier)	10.3(1) et ultérieure

Configurer des informations d'authentification permanentes pour la connexion à Expressway

Lorsqu’un utilisateur se connecte au réseau à l'aide de Mobile and Remote Access Through Expressway, l'utilisateur est invité à saisir un nom d’utilisateur, un mot de passe et un nom domaine de service. Si vous activez le paramètre Infos d'auth. permanentes pour la connexion à Expressway, les informations d'authentification de l’utilisateur sont stockées afin qu’il n’ait plus besoin de les saisir. Par défaut, ce paramètre est désactivé.

Vous pouvez configurer les informations d'identification pour conserver un seul téléphone, un groupe de téléphones ou tous les téléphones.

Rubriques connexes

Configuration des fonctionnalités téléphoniques, à la page 147

Configuration spécifique au produit, à la page 149

Génération d'un code QR pour la connexion MRA

Les utilisateurs ayant un téléphone avec une caméra peuvent scanner un code QR pour se connecter à MRA plutôt que de saisir manuellement le domaine de service et leur nom d'utilisateur.

Procédure

Étape 1 Utilisez un générateur de codes QR pour générer un code QR avec le domaine du service ou le domaine du service et le nom d'utilisateur séparés d'une virgule. Par exemple, mra.exemple.com ou mra.exemple.com,nomutilisateur.

Étape 2 Imprimez le code QR et communiquez-le à l'utilisateur.

Outil de rapport de problème

Les utilisateurs peuvent vous envoyer des rapports de problème à l'aide le l'outil de rapport de problème.

Remarque Les journaux de l'outil de rapport de problème sont requis par le centre d'assistance technique de Cisco lors de la résolution de problèmes. Les journaux sont supprimés si vous redémarrez le téléphone. Collectez les journaux avant de redémarrer les téléphones.

Pour émettre un rapport de problème, les utilisateurs doivent accéder à l'outil de rapport de problème et indiquer la date et l'heure auxquelles le problème a eu lieu, et fournir une description du problème.

Si le téléchargement du PRT échoue, vous pouvez accéder au fichier PRT du téléphone à partir de l'URL **`http:// <phone-ip-address> /FS/ <prt-file-name>`**. Cette URL est affichée sur le téléphone dans les cas suivants :

- Si le téléphone est configuré avec les valeurs d'usine. L'URL est active pendant une heure. Au bout d'une heure, l'utilisateur devra essayer à nouveau d'envoyer les journaux du téléphone.
- Si le téléphone a téléchargé un fichier de configuration et si le système de contrôle d'appels autorise le téléphone à accéder à Internet.

Vous devez ajouter une adresse de serveur dans le champ **URL de téléchargement de l'assistance utilisateur** de Cisco Unified Communications Manager.

Si vous déployez des périphériques avec Mobile and Remote Access through Expressway, vous devez aussi ajouter l'adresse du serveur PRT dans la liste des serveurs HTTP autorisés du serveur Expressway.

Configuration d'une URL de téléchargement de l'assistance utilisateurs

Vous devez utiliser un serveur doté d'un script de téléchargement en amont pour pouvoir recevoir des fichiers PRT. Le PRT utilise un mécanisme HTTP POST, les paramètres suivants étant inclus dans le téléchargement (utilisant le chiffrement MIME multipartie) :

- devicename (exemple : « SEP001122334455 »)

- serialno (exemple : « FCH12345ABC »)
- username (le nom d'utilisateur configuré dans Cisco Unified Communications Manager, le propriétaire du périphérique)
- prt_file (exemple : « probrep-20141021-162840.tar.gz »)

Vous trouverez ci-dessous un exemple de script. Le script est uniquement fourni à titre de référence. Cisco ne fournit pas d'assistance pour les scripts de téléchargement en amont installés sur les serveurs des clients.

```
<?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.");
}

?>
```

Remarque Les téléphones ne prennent en charge que les URL HTTP.

Procédure

Étape 1 Configurez un serveur pouvant exécuter votre script de téléchargement PRT.

Étape 2 Rédigez un script pouvant traiter les paramètres susmentionnés, ou modifiez l'exemple de script fourni selon vos besoins.

Étape 3 Téléchargez le script sur votre serveur.

Étape 4 Dans Cisco Unified Communications Manager, allez à la zone Product Specific Configuration Layout (Disposition de la configuration spécifique au produit) de la fenêtre de configuration du périphérique individuel, de la fenêtre Profil de téléphone commun ou de la fenêtre Configuration des téléphones d'entreprise.

Étape 5 Cochez la case **URL de téléchargement de l'assistance utilisateurs** et saisissez l'URL de votre serveur de téléchargement.

Exemple :

http://exemple.com/prtscript.php

Étape 6 Enregistrez vos modifications.

Définition du libellé d'une ligne

Vous pouvez configurer un téléphone afin qu'il affiche un texte de libellé au lieu du numéro de répertoire. Utilisez ce libellé pour définir la ligne d'après son nom ou sa fonction. Par exemple, si un utilisateur partage des lignes du téléphone, vous pouvez définir la ligne par le nom de la personne qui partage la ligne.

Lors de l'ajout d'un libellé à un module d'extension de touches, seuls les 25 premiers caractères sont affichés sur une ligne.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone**.

Étape 2 Localisez le téléphone à configurer.

Étape 3 Localisez l'instance de la ligne et définissez le champ Libellé de ligne.

Étape 4 (facultatif) Si le libellé doit être appliqué à d'autres périphérique qui partagent la ligne, cochez la case Mettre à jour les paramètres du périphérique partagé et cliquez sur **Propager la sélection**.

Étape 5 Sélectionnez **Enregistrer**.

Configuration des informations de banque double

Pour configurer des informations de banque double, procédez comme suit :

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, choisissez **Périphérique** > **Valeurs par défaut de périphérique**.

Étape 2 Vérifiez les informations de charge dans le champ Informations sur la charge inactive.

Étape 3 Choisissez **Administration en grand nombre** > **Importation/Exportation** > **Exportation** > **Valeurs par défaut de périphérique**, puis planifiez une tâche d'exportation.

Étape 4 Téléchargez le fichier .tar exporté, puis décompressez-le.

Étape 5 Vérifiez le format du fichier dans le fichier CSV exporté et vérifiez que le fichier CSV présente une colonne Informations sur la charge inactive avec la valeur qui convient.

Remarque La valeur du fichier CSV doit correspondre à la valeur par défaut du périphérique dans la fenêtre Cisco Unified Communications Manager Administration.

Surveillance du parcage

La surveillance du parcage est prise en charge uniquement lorsqu'un téléphone IP Cisco parque un appel. La surveillance du parcage surveille alors l'état d'un appel parqué. La bulle d'appel de surveillance du parcage ne s'efface pas tant que l'appel parqué n'est pas récupéré ou abandonné par l'appel parqué. Cet appel parqué peut être récupéré en utilisant la même bulle d'appel sur le téléphone qui a parqué l'appel.

Configuration des minuteurs de la surveillance du parcage

Cisco Unified Communications Manager Administration dispose de trois paramètres de minuteur de service pour la surveillance du parcage influant sur tout le cluster : Minuteur de récupération pour la surveillance du parcage, Minuteur périodique de récupération pour la surveillance du parcage et Minuteur de renvoi sans récupération pour la surveillance du parcage. Chaque paramètre de service contient une valeur par défaut et ne nécessite pas de configuration particulière. Ces paramètres pour minuteur sont destinés à la surveillance du parcage uniquement ; le Minuteur d'affichage pour le parcage d'appels et le Minuteur de récupération pour le parcage d'appels ne sont pas utilisés pour la surveillance du parcage. Reportez-vous au tableau suivant pour des explications de ces paramètres.

Configurez les minuteurs sur la page Paramètres de service de Cisco Unified Communications Manager.

Procédure

Étape 1 Dans Cisco Unified Communications Manager, sélectionnez **Système** > **Paramètres de service**.

Étape 2 Vous pouvez mettre à jour les champs Minuteur de récupération pour la surveillance du parcage, Minuteur périodique de récupération pour la surveillance du parcage et Minuteur de renvoi sans récupération pour la surveillance du parcage dans le volet Paramètres pour tout le cluster (communs à toutes les fonctionnalités).

Tableau 35 : Paramètres de service pour la surveillance du parcage

Champ	Description
Park Monitoring Reversion Timer (Minuteur de récupération pour la surveillance du parcage)	La valeur par défaut est 60 secondes. Ce paramètre détermine le nombre de secondes d'atten Cisco Unified Communications Manager notifie l'utilisateur de récupérer un appel qu'il a pa minuteur démarre lorsque l'utilisateur appuie sur la touche Parquer du téléphone et un rappe lorsque le minuteur prend fin. Vous pouvez redéfinir la valeur spécifiée par ce paramètre de service individuellement pour dans la section Surveillance du parcage de la fenêtre Configuration du numéro de répertoire Cisco Unified Communications Manager, sélectionnez **Routage des appels** > **Numéro de r** Saisir une valeur de 0 permet d'utiliser immédiatement l'intervalle périodique de récupération le paramètre de service du Minuteur périodique de récupération pour la surveillance du parc (Reportez-vous à l'explication qui suit). Par exemple, si ce paramètre est défini sur zéro et qu périodique de récupération pour la surveillance du parcage est défini sur 15, l'utilisateur est im notifié de l'appel parqué et le sera toutes les 15 secondes jusqu'à ce que le Minuteur de renv récupération pour la surveillance du parcage (voir l'explication qui suit) prenne fin.

Champ	Description
Minuteur périodique de récupération pour la surveillance du parcage	La valeur par défaut est 30 secondes. Ce paramètre détermine l'intervalle (en secondes) d'attente Cisco Unified Communications Manager notifie encore l'utilisateur qu'un appel est parqué. Pour l'appel parqué, l'utilisateur peut simplement décrocher le combiné lorsqu'il est notifié. Cisco Un Communications Manager continue de notifier l'utilisateur à propos de l'appel tant que celui-ci re et jusqu'à ce que le Minuteur de renvoi sans récupération pour la surveillance du parcage (voir l'e qui suit) prenne fin. Saisir une valeur de 0 permet de désactiver les notifications périodiques à p l'appel parqué.
Minuteur de renvoi sans récupération pour la surveillance du parcage	La valeur par défaut est 300 secondes. Ce paramètre détermine la durée (en secondes) pendant la notifications de parcage sont actives avant que l'appel parqué ne soit renvoyé à la destination de sans récupération pour la surveillance du parcage spécifiée dans la fenêtre Configuration du nu répertoire du téléphone ayant effectué le parcage. (Si aucune destination de renvoi n'est précisé Cisco Unified Communications Manager Administration, l'appel retourne sur la ligne qui l'a par paramètre se déclenche lorsque la durée spécifiée dans le paramètre de service du Minuteur de réc pour la surveillance du parcage prend fin. Lorsque le Minuteur de renvoi sans récupération pou surveillance du parcage prend fin, l'appel est retiré sur parcage et renvoyé vers la destination sp retourne sur la ligne qui l'a parqué.

Configuration des paramètres de la surveillance du parcage pour les numéros de répertoire

La fenêtre Directory Number Configuration (Configuration du numéro de répertoire) contient une zone Park Monitoring (Surveillance du parcage) dans laquelle vous pouvez configurer les trois paramètres.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Call Routing (Routage d'appels)** > **Directory Number (Numéro de répertoire)**.

Étape 2 Définissez les champs de la surveillance du parcage comme décrit dans le tableau suivant.

Tableau 36 : Paramètres de la surveillance du parcage

Champ	Description
Park Monitoring Forward No Retrieve Destination External (Renvoi sans récupération vers destination externe pour la surveillance du parcage)	Lorsque l'appelant parqué est une partie externe, l'appel est renvoyé vers la destination spécifiée dans le paramètre Park Monitoring Forward No Retrieve Destination External (Renvoi sans récupération vers destination externe pour la surveillance du parcage) de la personne ayant effectué le parcage. Si la valeur du champ Forward No Retrieve Destination External (Renvoi sans récupération vers destination externe) est vide, l'appelant parqué est renvoyé sur la ligne de la personne ayant effectué le parcage.

Champ	Description
Park Monitoring Forward No Retrieve Destination Internal (Renvoi sans récupération vers destination interne pour la surveillance du parcage)	Lorsque l'appelant parqué est une partie interne, l'appel est renvoyé vers la destination spécifiée dans le paramètre Park Monitoring Forward No Retrieve Destination (Renvoi sans récupération vers destination interne pour la surveillance du parcage) de la personne ayant effectué le parcage. Si la valeur du champ Forward No Retrieve Destination Internal est vide, l'appelant parqué est renvoyé sur la ligne de la personne ayant effectué le parcage.
Park Monitoring Reversion Timer (Minuteur de récupération pour la surveillance du parcage)	Ce paramètre détermine le nombre de secondes d'attente avant que Cisco Unified Communications Manager notifie l'utilisateur de récupérer un appel qu'il a parqué. Le minuteur démarre lorsque l'utilisateur appuie sur la touche Parquer du téléphone et un rappel est présenté lorsque le minuteur prend fin. Par défaut : 60 secondes Si vous saisissez une valeur différente de zéro, cette valeur redéfinit la valeur de ce paramètre configurée dans la fenêtre Paramètres de service. Cependant, si vous saisissez ici une valeur égale à zéro, alors la valeur de la fenêtre Paramètres de service est utilisée.

Configuration de la surveillance du parcage pour les listes de recherche

Lorsqu'un appel qui a été dirigé via la liste de recherche est parqué, la valeur du paramètre Hunt Pilot Park Monitoring Forward No Retrieve Destination est utilisée (sauf si elle est vide) lorsque Park Monitoring Forward No Retrieve Timer expire.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, choisissez **Routage d'appels** > **Diriger/Rechercher** > **Pilote de recherche**.

Étape 2 Définissez le paramètre Hunt Pilot Park Monitoring Forward No Retrieve Destination.

Si la valeur du paramètre Hunt Pilot Park Monitoring Forward No Retrieve Destination est vide, l'appel est renvoyé à la destination configurée dans la fenêtre Configuration du numéro de répertoire lorsque Park Monitoring Forward No Retrieve Timer expire.

Configuration de la plage des ports audio et vidéo

Le trafic audio et vidéo pour être envoyé vers différentes plages de ports RTP pour améliorer la qualité de service (QoS).

Les champs suivants contrôlent la plage des ports dans Cisco Unified Communications Manager Administration :

- Ports audio
    - Port média de début (par défaut : 16384)

- Port média de fin (par défaut : 32766)

- Ports vidéo
  - Lancer la vidéo (il s'agit de définir le port vidéo de démarrage).
    - Minimum : 2048
    - maximum : 65535
  - Arrêter la vidéo (il s'agit de définir le port vidéo d'arrêt)
    - Minimum : 2048
    - maximum : 65535

Les règles suivantes s'appliquent lors de la configuration des champs de ports vidéo :

Une fois que le Port RTP vidéo de début et le Port RTP vidéo de fin ont été configurés, le téléphone utilise les ports contenus dans la plage de ports vidéo pour le trafic vidéo. Le trafic audio utilise les ports média.

Si les plages de ports audio et vidéo se chevauchent, les ports concernés transmettent à la fois le trafic audio et le trafic vidéo. Si la plage des ports vidéo n'est pas configurée correctement, le téléphone utilise les ports audio pour le trafic audio et le trafic vidéo.

Pour obtenir plus d'informations, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Paramètres du périphérique** > **Profil SIP**

Étape 2 Configurez les champs Port média de début et Port média de fin pour la plage de ports audio.

Étape 3 Sélectionnez **Enregistrer**.

Étape 4 Sélectionnez l'une des fenêtres suivantes :

- **Système** > **Configuration des téléphones d'entreprise**
- **Périphérique** > **Paramètres du périphérique** > **Profil du téléphone commun**
- **Périphérique** > **Téléphone** > **Configuration du téléphone**

Étape 5 Configurez les champs Port RTP vidéo de début et Port RTP vidéo de fin pour la plage des ports nécessaires.

Les règles suivantes s'appliquent lors de la configuration des champs de ports vidéo :

- La valeur du champ Port RTP vidéo de fin doit être supérieure à la valeur du champ Port RTP vidéo de début.
- La différence entre le champ Port RTP vidéo de début et le champ Port RTP vidéo de fin doit être d'au moins 16.

Étape 6 Sélectionnez **Enregistrer**.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Configurer Cisco IP Manager Assistant

Cisco IP Manager Assistant (IPMA) propose des fonctions de routage pour aider les managers et les assistants à traiter les appels téléphoniques plus efficacement.

Les services IPMA doivent être configurés dans Cisco Unified Communications Manager avant que vous puissiez y accéder. Pour obtenir des informations détaillées sur la configuration de IPMA, consultez le *Guide de Configuration des fonctionnalités de Cisco Unified Communications Manager*.

IPMA comprend trois composants principaux :

Manager

Un manager a des appels interceptés par le service de routage d'appel.

Assistant

Un assistant gère les appels pour le compte d'un manager.

Assistant Console

La console de l'assistant est une application de bureau qui peut être utilisée par les assistants pour effectuer des tâches et gérer la plupart des fonctions.

IPMA prend en charge deux modes de fonctionnement : prise en charge de ligne proxy et prise en charge de ligne partagée. Les deux modes prennent en charge plusieurs appels par ligne pour le manager. Le service IPMA prend en charge les lignes proxy et partagées dans un cluster.

En mode ligne partagée, le manager et l'assistant ont un numéro de répertoire identique, et les appels sont traités sur la ligne partagée. Le téléphone du manager et celui de l'assistant sonnent lorsqu'un appel est reçu sur la ligne partagée. Le mode ligne partagée ne prend pas en charge la sélection de l'assistant par défaut, la supervision de l'assistant, le filtrage d'appels ou le renvoi de tous les appels.

Si vous configurez Cisco IPMA en mode ligne partagée, le manager et l'assistant partagent un numéro de répertoire ; par exemple, 1701. L'assistant traite les appels d'un manager sur le numéro de répertoire partagé. Lorsqu'un manager reçoit un appel sur le numéro de répertoire 1701, le téléphone du manager ainsi que celui de l'assistant sonnent.

Certaines fonctionnalités IPMA ne sont pas disponibles en mode ligne partagée, comme sélection de l'assistant par défaut, supervision de l'assistant, filtrage d'appels et renvoi de tous les appels. L'assistant ne peut pas consulter ces fonctions ni y accéder dans l'application Assistant Console. Le téléphone de l'assistant ne possède pas la touche fonction correspondant au Renvoi de tous les appels. Le téléphone du manager ne possède pas de touche programmable pour la Surveillance de l'assistant, L'interception d'appel ou le Renvoi de tous les appels.

Pour accéder à la prise en charge de ligne partagée sur les périphériques utilisateurs, vous devez d'abord utiliser Cisco Unified Communications Manager Administration pour configurer et lancer le service Cisco IP Manager Assistant

En mode ligne proxy, l'assistant traite les appels pour le compte d'un manager, grâce à un numéro proxy. Le mode ligne proxy prend en charge toutes les fonctionnalités IPMA.

Lorsque vous configurez Cisco IPMA en mode ligne proxy, le manager et l'assistant ne partagent pas de numéro de ligne de poste. L'assistant traite les appels pour un manager avec un numéro proxy. Le numéro proxy n'est pas le numéro de répertoire du Manager. C'est un autre numéro choisi par le système et utilisé par un assistant pour gérer les appels du manager. En mode ligne proxy, un manager et un assistant ont accès à toutes les fonctionnalités disponibles dans IPMA, y compris la sélection de l'assistant par défaut, la supervision de l'assistant, le filtrage d'appels et le renvoi de tous les appels.

Pour accéder à la prise en charge de ligne proxy sur les périphériques utilisateurs, vous devez d'abord utiliser Cisco Unified Communications Manager Administration pour configurer et lancer le service Cisco IP Manager Assistant.

Vous accédez aux fonctionnalités IPMA en utilisant les touches programmables et via les Services téléphoniques. Le modèle de touches programmables est configuré dans Cisco Unified Communications Manager. IPMA prend en charge les modèles de touches programmables suivants :

Manager standard

Assiste le manager en mode proxy.

Manager en mode ligne partagée standard

Assiste le manager en mode ligne partagée.

Assistant standard

Assiste l'assistant en mode proxy et ligne partagée.

Le tableau suivant décrit les touches programmables disponibles dans le modèle de touches programmables :

Tableau 37 : Touches programmables IPMA

Touche programmable	État de l'appel	Description
Renvoi	Entrant, Connecté, En attente	Renvoie l'appel sélectionné à une cible pré-configurée.
Intercept	Tous états	Renvoie un appel depuis le téléphone de l'assistant vers le téléphone du manager et déclenche la réponse automatique.
Observation	Tous états	Permet de consulter l'état d'un appel en cours de traitement par un assistant.
TransVM	Entrant, Connecté, En attente	Renvoie l'appel sélectionné vers la messagerie vocale du manager.
Renvoi de tous les appels	Tous états	Renvoie tous les appels acheminés vers le manager vers une cible préconfigurée.

Remarque Intercept, Observation et Renvoyer tout doivent être configurés uniquement pour un téléphone de manager sur en mode ligne proxy.

La procédure suivante présente les étapes nécessaires :

Procédure

Étape 1	Configurez les téléphones et les utilisateurs.
Étape 2	Associez les téléphones aux utilisateurs.
Étape 3	Activez le service Cisco IP Manager Assistant dans la fenêtre Activation du service.
Étape 4	Configurez les paramètres d'administration système.
Étape 5	Si nécessaire, configurez les paramètres de service IPMA pour tout le cluster.
Étape 6	(facultatif) Configurez le profil utilisateur CAPF
Étape 7	(facultatif) Configurez les paramètres de service IPMA pour la sécurité.
Étape 8	Arrêtez et redémarrez le service IPMA.
Étape 9	Configurez les paramètres téléphone, manager et assistant, y compris les modèles de touches programmables.
Étape 10	Configurez l'application Cisco Unified Communications Manager Assistant.
Étape 11	Configurez les règles de numérotation.
Étape 12	Installez l'application Assistant Console.
Étape 13	Configurez les applications Console pour le manager et l'assistant.

Configuration de la messagerie vocale

La messagerie vocale visuelle est configurée pour tous les téléphones IP Cisco, pour un utilisateur individuel ou pour un groupe d'utilisateurs, depuis Cisco Unified Communications Manager Administration.

Remarque Pour plus d'informations sur la configuration, consultez la documentation messagerie vocale visuelle Cisco sur http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html.

Le client de messagerie vocale visuelle n'est pas pris en charge comme un midlet sur un des Téléphones IP Cisco 8800.

Procédure

Étape 1	Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Paramètres du périphérique** > **Services téléphoniques**.
Étape 2	Sélectionnez **Ajouter** pour créer un nouveau service pour la Messagerie vocale visuelle.
Étape 3	Dans la fenêtre Configuration du service téléphonique IP, saisissez les informations suivantes dans leurs champs respectifs : • Nom du service : saisissez **`VisualVoiceMail`**. • Nom ASCII du service : saisissez **`VisualVoiceMail`**. • URL du service : saisissez **`VisualVoiceMail`**. • Catégorie du service : sélectionnez **Service XML** dans le menu déroulant. • Type de service : sélectionnez **Messages** dans le menu déroulant.
Étape 4	Cochez **Activer** et cliquez sur **Enregistrer**.

Remarque Vérifiez que vous n'avez pas coché **Abonnement entreprise**.

Étape 5 Dans la fenêtre Informations sur les paramètre de service, cliquez sur **Nouveau paramètre** et saisissez les informations suivantes dans leurs champs respectifs :

- Nom du paramètre. Saisissez voicemail_server.
- Nom affiché du paramètre. Saisissez voicemail_server.
- Valeur par défaut. Saisissez le nom d'hôte du serveur Unity principal.
- Description du paramètre

Étape 6 Cochez **Parameter is Required (Paramètre requis)** et cliquez sur **Enregistrer**.

Remarque Vérifiez que vous n'avez pas coché **Parameter is a Password (mask contents) (Paramètre est un mot de passe (masquer le contenu))**.

Étape 7 Fermez la fenêtre et sélectionnez **Enregistrer** à nouveau dans la fenêtre Configuration du service téléphonique.

Configuration de la Messagerie vocale visuelle pour un utilisateur spécifique

Pour configurer la Message vocale visuelle pour un utilisateur donné, procédez comme suit.

Remarque Pour obtenir des informations sur la configuration, consultez la documentation relative à la Messagerie vocale visuelle Cisco à la page http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html.

Procédure

Étape 1 Dans l'administration de Cisco Unified Communications Manager, choisissez **Périphérique** > **Téléphone**.

Étape 2 Sélectionnez le périphérique associé à l'utilisateur que vous recherchez.

Étape 3 Dans le menu déroulant Liens associés, choisissez **S'abonner/Se désabonner des services**, puis cliquez sur **Aller**.

Étape 4 Sélectionnez le service VisualVoiceMail que vous avez créé, puis choisissez **Suivant** > **S'abonner**.

Configuration de la Messagerie vocale visuelle pour un groupe d'utilisateurs

Pour ajouter un lot de téléphones IP Cisco à Cisco Unified Communications Manager avec un abonnement à Messagerie vocale visuelle, créez un modèle de téléphone dans l'outil BAT pour chaque type de téléphone et dans chaque modèle de téléphone. Vous pouvez ensuite vous abonner au service Messagerie vocale visuelle et utiliser le modèle pour ajouter les téléphones.

Si vous avez des téléphones IP Cisco déjà enregistrés et que vous souhaitez abonner ces téléphones au service Messagerie vocale visuelle, créez un modèle de téléphone dans BAT, effectuez l'abonnement au service Messagerie vocale visuelle sur le modèle, puis utilisez l'outil BAT pour mettre à jour les téléphones.

Pour plus d'informations, reportez-vous à http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html.

Services garantis SIP

Assured Services SIP(AS-SIP) (Services garantis SIP) est un ensemble de fonctions et de protocoles qui offrent un flux d'appels hautement sécurisé pour les téléphones IP Cisco et les téléphones tiers. Les fonctionnalités suivantes sont collectivement dénommées AS-SIP :

- Préséance et préemption à plusieurs niveaux (MLPP, Multilevel Precedence and Preemption)
- Marquage DSCP (Differentiated Services Code Point)
- Sécurité de la couche transport (TLS, Transport Layer Security) et protocole de transport sécurisé en temps réel (SRTP, Secure Real-time Transport Protocol)
- Protocole IP version 6 (IPv6)

AS-SIP est souvent utilisé avec la fonction préséance et préemption à plusieurs niveaux (MLPP) pour classer les appels en cas d'urgence. Avec MLPP, vous affectez un niveau de priorité à vos appels sortants, à partir du niveau 1 (faible) au niveau 5 (élevé). Lorsque vous recevez un appel, une icône de niveau de priorité s'affiche sur le téléphone qui indique la priorité d'appel.

Pour configurer AS-SIP, effectuez les tâches suivantes sur Cisco Unified Communications Manager :

- Configurer un utilisateur Digest : configurez l'utilisateur final pour utiliser l'authentification digest pour les requêtes SIP entrantes.
- Configurer le Port sécurisé SIP du téléphone : Cisco Unified Communications Manager utilise ce port pour écouter les téléphones SIP pour les enregistrements de lignes SIP sur TLS.
- Redémarrer les Services : après avoir configuré le port sécurisé, redémarrer les services du fournisseur Cisco Unified Communications Manager et Cisco CTL. Configurer le profil SIP pour AS-SIP : configurer un profil SIP avec des paramètres SIP pour vos terminaux AS-SIP et vos lignes principales SIP. Les paramètres spécifiques au téléphone ne sont pas téléchargés dans le cas d'un téléphone AS-SIP de fabricant tiers. Ils sont uniquement utilisés par Cisco Unified Manager. Les téléphones de fabricants tiers doivent configurer localement les mêmes paramètres.
- Configurer le profil de sécurité pour AS-SIP : vous pouvez utiliser le profil de sécurité du téléphone pour attribuer des paramètres de sécurité tels que TLS, SRTP et l'authentification digest.
- Configurer le point de terminaison AS-SIP : configurer un point de terminaison de téléphone IP Cisco ou un point de terminaison tiers avec prise en charge AS-SIP.
- Associer le périphérique avec l'utilisation de la terminaison : associer le point de terminaison à un utilisateur.
- Configurer un profil de sécurité de ligne principale SIP pour AS-SIP : vous pouvez utiliser le profil de sécurité de ligne principale sip pour affecter des fonctionnalités de sécurité telles que l'authentification TLS ou digest à une ligne principale SIP.
- Configurez la ligne principale SIP pour AS-SIP : configurez une ligne principale SIP avec prise en charge AS-SIP.
- Configurer les fonctionnalités AS-SIP : configurer des fonctionnalités AS-SIP supplémentaires telles que MLPP, TLS, V.150 et IPv6.

Pour obtenir des informations détaillées sur la configuration de AS-SIP, consultez le chapitre "Configurer les points de terminaison AS-SIP" du *Guide de Configuration des fonctionnalités de Cisco Unified Communications Manager*.

Migration de votre téléphone vers un téléphone multiplateforme directement

Vous pouvez maintenant migrer facilement votre téléphone vers un téléphone multiplateforme en une seule étape sans utiliser une version de transition du micrologiciel. Il vous suffit d'obtenir et d'autoriser la licence de migration à partir du serveur.

Pour plus d'informations, reportez-vous à 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

Préséance et préemption à plusieurs niveaux

La fonction Préséance et Préemption à Plusieurs Niveaux (MLPP) vous permet de donner la priorité à certains appels au cours des situations d'urgence ou d'autres crises. Vous attribuez à vos appels sortants une priorité comprise entre 1 et 5. Les appels entrants affichent une icône qui indique la priorité de l'appel. Les utilisateurs authentifiés peuvent préempter les appels vers des stations ciblées ou via des lignes principales TDM auxquelles vous êtes entièrement abonné.

Cette fonctionnalité garantit au personnel de haut niveau la communication avec les organisations et le personnel critiques.

MLPP est souvent utilisé avec les services garantis Assured Services SIP(AS-SIP). Pour obtenir des informations détaillées sur la configuration MLPP, reportez-vous au chapitre "Configurer la préséance et préemption à plusieurs niveaux" du *Guide de Configuration système de Cisco Unified Communications Manager*.

Configurer un modèle de touches programmables

À l'aide de Cisco Unified Communications Manager Administration, vous pouvez associer un maximum de 18 touches programmables aux applications prises en charge par le téléphone. Cisco Unified Communications Manager prend en charge les modèles de touches programmables Utilisateur standard et Fonctionnalité standard.

Une application prenant en charge les touches programmables présente un ou plusieurs modèles de touches programmables standard associés. Pour modifier un modèle de touches programmables standard, vous devez le copier, le renommer, puis mettre à jour le nouveau modèle. Vous pouvez aussi modifier les modèles de touches programmables non standard.

Le paramètre Contrôle des touches programmables montre si les touches programmables d'un téléphone sont contrôlées par la fonction Modèle de touches programmables. Le paramètre Contrôle des touches programmables est un champ obligatoire.

Pour plus d'informations sur la configuration de cette fonction, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager.

Les téléphones IP Cisco ne prennent pas en charge toutes les touches programmables configurables dans Configuration du modèle de touches programmables de Cisco Unified Communications Manager. Cisco Unified Communications Manager vous permet d'activer ou de désactiver certaines touches programmables dans les paramètres de configuration de la politique de contrôle. Le tableau suivant liste les fonctions et les touches programmables pouvant être configurées dans un modèle de touches programmables et détermine si elles sont prises en charge par les téléphones IP Cisco.

Remarque Cisco Unified Communications Manager permet de configurer n'importe quelle touche programmable d'un modèle de touches programmables, mais les touches programmables qui ne sont pas prises en charge ne sont pas affichées sur le téléphone.

Tableau 38 : Touches programmables configurables

Fonctionnalité	Touches programmables configurables dans Configuration du modèle de touches programmables	Prise en charge comme touche programmable
Réponse	Répondre (Répond.)	Pris en charge
Rappel automatique	Rappeler (rappel)	Pris en charge
Renvoi de tous les appels	Renvoyer tout (RenvTt)	Pris en charge
Parcage d'appels	Parque un appel (Parquer)	Pris en charge
Interception d'appel	Interception (Intrcpt)	Pris en charge
Insertion	Insertion	Pris en charge
Insertion dans une conférence (cBarge)	Insertion Conférence	Pris en charge
Conférence	Conférence (Confrn)	Pris en charge
Liste des conférences	Liste de conférence (ConfList)	Pris en charge
Détourner	Renvoi immédiat (Rvoi Im)	Pris en charge
Ne pas déranger	Activation ou désactivation de la fonction Ne pas déranger (NPD)	Pris en charge
Mettre fin à l'appel	Fin appel (Fin app.)	Pris en charge
Interception d'appels de groupe	Interception groupe (GPickUP)	Pris en charge
Attente	Mise en attente (Attente)	Pris en charge
Groupe de recherche	Groupmt (Groupmt)	Pris en charge
Joindre	Joindre (Joindre)	Non pris en charge
Identification d'appel malveillant	Activation ou désactivation de l'identification d'appel malveillant (IDAM)	Pris en charge
MultConf	MultConf (MultConf)	Pris en charge
Connectivité mobile	Mobilité (Mobilité)	Pris en charge

Fonctionnalité	Touches programmables configurables dans Configuration du modèle de touches programmables	Prise en charge comme touche programmable
NvAppel	Nouvel appel (NvAppel)	Pris en charge
Autre interception	Autre interception (AGrpIntr)	Pris en charge
Prise en charge de PLK pour les statistiques de file d'attente	État de la file d'attente	Non pris en charge
Outil de génération de rapports qualité	Outil de génération de rapports de qualité (QRT)	Pris en charge
Renumérotation	Bis (Bis)	Pris en charge
Supprimer le dernier participant à une conférence	Supprimer le dernier participant à une conférence (Supprimer)	Non pris en charge
Reprend.	Reprendre (Reprend.)	Pris en charge
Sélection	Sélectionner (Select)	Non pris en charge
Numérotation simplifiée	Composition d'un numéro abrégé (NumAbr)	Pris en charge
Transfert	Transfert (Trfr)	Pris en charge
Commande du mode vidéo	Commande du mode vidéo (ModeVid.)	Non pris en charge

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez l'une des fenêtres suivantes :

- Pour configurer les modèles de touches programmables, sélectionnez **Périphérique** > **Paramètres du périphérique** > **Modèle de touches programmables**.
- Pour attribuer un modèle de touches programmables à un téléphone, sélectionnez **Périphérique** > **Téléphone** et configurez le champ Modèle de touches programmables.

Étape 2 Enregistrez les modifications.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Modèles de boutons de téléphone

Les modèles de boutons de téléphone permettent d'affecter des fonctionnalités de numérotation rapide et de traitement des appels à des boutons programmables. Les fonctionnalités de traitement des appels pouvant être affectées à des boutons incluent Répondre, Mobilité et Tous les appels.

Il est préférable de modifier les modèles avant d'enregistrer les téléphones sur le réseau. Ainsi, vous pourrez accéder aux options de modèle de boutons de téléphone personnalisé dans Cisco Unified Communications Manager pendant l'enregistrement.

Modification du modèle de boutons de téléphone

Pour plus d'informations sur les services téléphone IP et la configuration des boutons de ligne, reportez-vous à la documentation relative à votre version particulière de Cisco Unified Communications Manager.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Paramètres du périphérique** > **Modèle de boutons du téléphone**.

Étape 2 Cliquez sur **Rechercher**.

Étape 3 Sélectionnez le modèle du téléphone.

Étape 4 Sélectionnez **Copier**, saisissez le nom du nouveau modèle, puis sélectionnez **Enregistrer**.

La fenêtre Configuration du modèle de boutons du téléphone s'ouvre.

Étape 5 Sélectionnez le bouton à affecter, puis sélectionnez **URL de service** dans la liste déroulante Fonctionnalités correspondant à la ligne.

Étape 6 Sélectionnez **Enregistrer** pour créer un nouveau modèle de boutons de téléphone qui utilise l'URL du service.

Étape 7 Sélectionnez **Périphérique** > **Téléphone** et ouvrez la fenêtre Phone Configuration (Configuration du téléphone) correspondant au téléphone.

Étape 8 Sélectionnez le nouveau modèle de boutons de téléphone dans la liste Modèle de boutons de téléphone.

Étape 9 Sélectionnez **Enregistrer** pour valider les modifications, puis sélectionnez **Appliquer la configuration** pour appliquer les modifications.

L'utilisateur du téléphone peut dorénavant accéder au portail d'aide en libre-service et associer le service à un bouton du téléphone.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Attribuer un modèle de boutons de téléphone pour tous les appels

Affectez un bouton Tous les appels dans le modèle du téléphone pour les utilisateurs ayant plusieurs lignes partagées.

Lorsque vous configurez un bouton Tous les appels sur le téléphone, les utilisateurs utilisent le bouton Tous les appels pour :

- Voir une liste consolidée des appels en cours à partir de toutes les lignes sur le téléphone.
- Voir (sous Historique des appels) une liste consolidée de tous les appels en absence à partir de toutes les lignes sur le téléphone.

- Passer un appel sur la ligne principale de l'utilisateur lorsque l'utilisateur décroche. Le bouton Tous les appels passe automatiquement par défaut sur la ligne principale de l'utilisateur pour tous les appels sortants.

Procédure

Étape 1 Modifiez le modèle de bouton de téléphone pour inclure le bouton Tous les appels.

Étape 2 Appliquez le modèle au téléphone.

Configuration d'un Carnet d'adresses personnel ou de la numérotation abrégée en tant que service du téléphone IP

Vous pouvez modifier un modèle de boutons de téléphone pour associer une URL de service à un bouton programmable. Ainsi, les utilisateurs pourront accéder au carnet d'adresses personnel et aux numéros abrégés en appuyant sur un seul bouton. Avant de modifier le modèle de boutons du téléphone, vous devez configurer le Carnet d'adresses personnel ou les numéros abrégés en tant que service du téléphone IP. Pour obtenir plus d'informations, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Pour configurer le Carnet d'adresses personnel ou la numérotation abrégée en tant que service du téléphone IP (si ce ne sont pas déjà des services), procédez comme suit :

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Paramètres du périphérique** > **Services téléphoniques**.

La fenêtre Find and List IP Phone Services (Recherche et affichage des services de téléphonie IP) apparaît.

Étape 2 Cliquez sur **Ajouter nouveau**.

La fenêtre IP Phone Services Configuration (Configuration des services de téléphonie IP) apparaît.

Étape 3 Saisissez les paramètres suivants :

- Nom du service : Saisissez **Carnet d'adresses personnel**.
- Description du service : Saisissez une description facultative du service.
- URL de service

  Pour le Carnet d'adresses personnel, entrez l'URL suivante :

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

  Pour la numérotation rapide, entrez l'URL suivante :

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

  Pour le Carnet d'adresses personnel, entrez l'URL suivante :

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

Pour la numérotation rapide, entrez l'URL suivante :

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

- Catégorie de service : sélectionnez **Service XML**.
- Type de service : sélectionnez **Répertoires**.
- Activer : sélectionnez la case à cocher.

http://<IP_address> or *https://<IP_address>* (selon le protocole pris en charge par le téléphone IP Cisco).

Étape 4 Sélectionnez **Enregistrer**.

Remarque Si vous modifiez l'URL du service, supprimez un paramètre de service du téléphone IP, ou remplacez le nom d'un paramètre de service téléphonique par un service téléphonique auquel les utilisateurs sont abonnés, vous devez cliquer sur **Update Subscriptions** (Mettre à jour les abonnements) pour mettre à jour tous les utilisateurs actuellement abonnés ; sinon, les utilisateurs doivent s'abonner à nouveau au service pour obtenir l'URL correcte.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Modification du modèle de boutons de téléphone pour le carnet d'adresses personnel ou la numérotation rapide

Vous pouvez modifier un modèle de boutons de téléphone pour associer une URL de service à un bouton programmable. Ainsi, les utilisateurs pourront accéder au carnet d'adresses personnel et aux numéros abrégés en appuyant sur un seul bouton. Avant de modifier le modèle de boutons du téléphone, vous devez configurer le Carnet d'adresses personnel ou les numéros abrégés en tant que service du téléphone IP.

Pour plus d'informations sur les services téléphone IP et la configuration des boutons de ligne, reportez-vous à la documentation relative à votre version particulière de Cisco Unified Communications Manager.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Paramètres du périphérique** > **Modèle de boutons du téléphone**.

Étape 2 Cliquez sur **Rechercher**.

Étape 3 Sélectionnez le modèle du téléphone.

Étape 4 Sélectionnez **Copier**, saisissez le nom du nouveau modèle, puis sélectionnez **Enregistrer**.

La fenêtre Configuration du modèle de boutons du téléphone s'ouvre.

Étape 5 Sélectionnez le bouton à affecter, puis sélectionnez **URL de service** dans la liste déroulante Fonctionnalités correspondant à la ligne.

Étape 6 Sélectionnez **Enregistrer** pour créer un nouveau modèle de boutons de téléphone qui utilise l'URL du service.

Étape 7 Sélectionnez **Périphérique** > **Téléphone** et ouvrez la fenêtre Phone Configuration (Configuration du téléphone) correspondant au téléphone.

Étape 8 Sélectionnez le nouveau modèle de boutons de téléphone dans la liste Modèle de boutons de téléphone.

Étape 9 Sélectionnez **Enregistrer** pour valider les modifications, puis sélectionnez **Appliquer la configuration** pour appliquer les modifications.

L'utilisateur du téléphone peut dorénavant accéder au portail d'aide en libre-service et associer le service à un bouton du téléphone.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Configuration du réseau privé virtuel

La fonctionnalité VPN Cisco vous aide à préserver la sécurité du réseau tout en apportant à vos utilisateurs une méthode sécurisée et fiable de se connecter au réseau d'entreprise. Utilisez cette fonctionnalité quand :

- Un téléphone se situe à l'extérieur d'un réseau sécurisé
- Le trafic réseau entre le téléphone et Cisco Unified Communications Manager passe par un réseau non sécurisé

Avec un VPN, il existe trois approches communes de l'authentification client :

- Certificats numériques
- Mots de passe
- Nom d'utilisateur et mot de passe

Chaque méthode présente ses avantages. Toutefois, si les règles de sécurité de votre entreprise le permettent, nous vous conseillons une approche par certificats, car ceux-ci permettent une connexion fluide sans aucune intervention de l'utilisateur. Les certificats LSC et MIC sont pris en charge.

Pour configurer les fonctionnalités VPN, effectuez d'abord la mise à disposition du périphérique sur site, puis déployez le périphérique hors site.

Pour plus d'informations sur l'authentification par certification et sur l'utilisation d'un réseau VPN, reportez-vous à la notice technique *Exemple d'un téléphone VPN AnyConnect avec authentification par certification sur une configuration ASA*. L'URL de ce document est http://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/115785-anyconnect-vpn-00.html.

Avec une approche par mot de passe ou par nom d'utilisateur et mot de passe, un utilisateur se voit demander ses identifiants de connexion. Définissez les identifiants de connexion utilisateur conformément aux règles de sécurité de votre entreprise. Vous pouvez également configurer le paramètre Activer la persistance du mot de passe de manière à ce que le mot de passe utilisateur soit enregistré sur le téléphone. Le mot de passe utilisateur est enregistré jusqu'à ce qu'un échec de tentative de connexion survienne, qu'un utilisateur efface le mot de passe ou que le téléphone se réinitialise ou ne soit plus alimenté.

Le paramètre Activer la détection automatique des réseaux est également un outil utile. Lorsque vous cochez cette case, le client VPN fonctionne uniquement lorsqu'il détecte qu'il se trouve en dehors du réseau d'entreprise. Par défaut, ce paramètre est désactivé.

Votre téléphone Cisco prend en charge la version Cisco SVC IPPhone Client v1.0 en tant que type de client.

Pour plus d'informations sur la maintenance, la configuration et l'utilisation d'un réseau privé virtuel avec un VPN, reportez-vous au *Guide de sécurité pour téléphone Cisco Unified Communications Manager*, chapitre « Configuration d'un réseau privé virtuel ». L'URL de ce document est http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

La fonctionnalité VPN Cisco utilise SSL (Secure Sockets Layer) pour préserver la sécurité du réseau.

Remarque Saisissez le paramètre de serveur TFTP secondaire lorsque vous configurez un téléphone hors site pour VPN SSL pour ASA en utilisant un client intégré.

Configuration des touches de ligne supplémentaires

Activez le mode ligne renforcée pour utiliser les boutons des deux côtés de l'écran du téléphone comme touches de ligne. La numérotation prédictive et les alertes d'appel entrants actionnables sont activées par défaut en mode ligne renforcée.

Avant de commencer

Vous devez créer un nouveau modèle de bouton du téléphone personnalisé.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone**.

Étape 2 Localisez le téléphone à configurer.

Étape 3 Naviguez jusqu'au menu Configuration spécifique à un produit, puis définissez le champ **Mode ligne** sur **Mode ligne renforcée**.

Étape 4 Naviguez jusqu'à la zone informations sur le périphérique et définissez le champ **Modèle de bouton du téléphone** à une valeur de modèle personnalisé.

Étape 5 Sélectionnez **Appliquer la configuration**.

Étape 6 Sélectionnez **Enregistrer**.

Étape 7 Redémarrez le téléphone.

Rubriques connexes

Environnement de mode ligne Session, à la page 170

Fonctions disponibles en mode ligne renforcée

Le mode ligne renforcée (ELM) peut être utilisé avec Mobile and Remote Access Through Expressway.

ELM peut également être utilisé avec une ligne de substitution, une configuration de routage d'appel dans laquelle les appels sont transférés vers une autre ligne partagée si la ligne partagée initiale est occupée. Lorsque ELM est utilisé avec une ligne de substitution, les appels récents vers des lignes partagées sont consolidés sous un seul numéro de répertoire. Pour plus d'informations sur les lignes de substitution, consultez le *Guide*

de Configuration des fonctionnalités de Cisco Unified Communications Manager pour téléphone Cisco Unified Communications Manager version 12.0 (1) ou version ultérieure.

ELM prend en charge la plupart des fonctionnalités, mais pas toutes. L'activation d'une fonction n'implique pas qu'elle soit prise en charge. Lisez le tableau suivant pour confirmer qu'une fonctionnalité est prise en charge.

Tableau 39 : Fonction prise en charge et Mode ligne renforcée

Fonctionnalité	Pris en charge	Version du micrologiciel
Réponse	Oui	11.5(1) et ultérieure
Réponse automatique aux appels	Oui	11.5(1) et ultérieure
Insertion/InsConf (cBarge)	Oui	11.5(1) et ultérieure
Parcage d'appels dirigé avec BLF	Oui	12.0(1) et ultérieure
Intégration de smartphone Bluetooth	Non	-
Casques Bluetooth USB	Oui	11.5(1) et ultérieure
Rappel automatique	Oui	11.5(1) et ultérieure
Chaperon des appels	Non	-
Renvoi de tous les appels	Oui	11.5(1) et ultérieure
Parcage d'appels	Oui	12.0(1) et ultérieure
Parcage d'appels, état de la ligne	Oui	12.0(1) et ultérieure
Interception d'appel	Oui	11.5(1) et ultérieure
Interception d'appels, état de la ligne	Oui	11.5(1) et ultérieure
Renvoi de tous les appels sur plusieurs lignes	Oui	11.5(1) et ultérieure
Cisco Extension Mobility Cross Cluster	Oui	La version 12.0(1) et ultérieures prend en charge cette fonctionnalité.
Cisco IP Manager Assistant (IPMA)	Non	-
Cisco Unified Communications Manager Express	Non	-
Conférence	Oui	11.5(1) et ultérieure
Applications CTI (couplage de la téléphonie et de l'informatique)	Oui	11.5(1) et ultérieure

Fonctionnalité	Pris en charge	Version du micrologiciel
Refuser	Oui	11.5(1) et ultérieure
Enregistrement invoqué par le périphérique	Oui	11.5(1) SR1 et ultérieure
Ne pas déranger	Oui	11.5(1) et ultérieure
SRST améliorée	Non	-
Extension Mobility	Oui	11.5(1) et ultérieure
Interception d'appels de groupe	Oui	La version 12.0(1) et ultérieures prend en charge cette fonctionnalité.
Attente	Oui	11.5(1) et ultérieure
Groupes de recherche	Oui.	12.0(1) et ultérieure
Alerte d'appel entrant avec minuteur configurable	Non	-
Intercom	Oui	11.5(1) et ultérieure
Module d'extension de touches	Les modules d'extension de touches du téléphone IP Cisco 8851/8861 et 8865 prennent en charge ce Mode	12.0(1) et ultérieure
Identification d'appel malveillant (IDAM)	Oui	11.5(1) et ultérieure
MultConf	Oui	11.5(1) et ultérieure
Connectivité mobile	Oui	11.5(1) et ultérieure
Préséance et préemption à plusieurs niveaux	Non	-
Silence	Oui	11.5(1) et ultérieure
Autre interception	Oui	12.0(1) et ultérieure
Prise en charge PLK (Programmable Line Key) pour l'État de la file d'attente	Oui	11.5(1) et ultérieure
Confidentialité	Oui	11.5(1) et ultérieure
État de la file d'attente	Oui	11.5(1) et ultérieure
Outil de génération de rapports de qualité (QRT)	Oui	11.5(1) et ultérieure

Fonctionnalité	Pris en charge	Version du micrologiciel
Prise en charge des paramètres régionaux Droite à gauche	Non	-
Renumérotation	Oui	11.5(1) et ultérieure
Écoute discrète et enregistrement	Oui	11.5(1) SR1 et ultérieure
Numérotation simplifiée	Oui	11.5(1) et ultérieure
Survivable Remote Site Telephony (SRST)	Oui	11.5(1) et ultérieure
Transfert	Oui	11.5(1) et ultérieure
Composition d'URI (Uniform Resource Identifier)	Oui	11.5(1) et ultérieure
Appels vidéo	Oui	11.5(1) et ultérieure
Visual Voicemail	Oui	11.5(1) et ultérieure
Messagerie vocale	Oui	11.5(1) et ultérieure

Rubriques connexes

Environnement de mode ligne Session, à la page 170

Configurer le minuteur de reprise TLS

La reprise de session TLS active la reprise d'une session TLS sans répéter le processus d'authentification TLS dans son intégralité. Elle peut réduire significativement la durée que prend l'échange des données pour la connexion TLS.

Bien que les téléphones prennent en charge les sessions TLS, toutes les sessions TLS ne prennent pas en charge la reprise TLS. La liste suivante décrit les différentes sessions et la prise en charge de la reprise TLS :

- Session TLS pour signalement SIP : prend en charge la reprise
- Client HTTPS : prend en charge la reprise
- CAPF : prend en charge la reprise
- TVS : prend en charge la reprise
- EAP-TLS : ne prend pas en charge la reprise
- EAP-FAST : ne prend pas en charge la reprise
- Client VPN : ne prend pas en charge la reprise

Pour obtenir plus d'informations, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone**.

Étape 2 Configurez le paramètre du minuteur de reprise TLS.

La plage de la minuterie est comprise entre 0 et 3600 secondes. La valeur par défaut est 3600. Si le champ a la valeur 0, la reprise de session TLS est désactivée.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Activation d'Intelligent Proximity

Remarque Cette procédure ne s'applique qu'aux téléphones prenant en charge Bluetooth. Les téléphones IP Cisco 8811, 8841, 8851NR et 8865NR ne prennent pas en charge Bluetooth.

Intelligent Proximity permet aux utilisateurs de profiter des propriétés acoustiques du téléphone avec leur périphérique mobile ou leur tablette. L'utilisateur apparie le périphérique mobile ou la tablette au téléphone via Bluetooth.

Avec un périphérique mobile jumelé, l'utilisateur peut passer et recevoir des appels mobiles sur le téléphone. Avec une tablette, l'utilisateur peut rediriger l'audio de la tablette vers le téléphone.

Les utilisateurs peuvent jumeler au téléphone plusieurs périphériques mobiles, tablettes et un casque Bluetooth. Cependant, un seul périphérique et un seul casque peuvent être connectés en même temps.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Téléphone** > **Périphérique**.

Étape 2 Localisez le téléphone que vous souhaitez modifier.

Étape 3 Localisez le champ Bluetooth et définissez ce champ sur **Activé**.

Étape 4 Localisez le champ Autoriser le mode mains libres mobile Bluetooth et réglez ce champ sur **Activé**.

Étape 5 Enregistrez vos modifications et appliquez-les au téléphone.

Configuration de la résolution de transmission vidéo

Les téléphones IP Cisco 8845, 8865 et 8865NR prennent en charge les formats vidéo suivants :

- 720p (1280x720)
- WVGA (800x480)
- 360p (640x360)

- 240p (432x240)
- VGA (640x480)
- CIF (352x288)
- SIF (352x240)
- QCIF (176x144)

Les téléphones IP Cisco avec capacité vidéo négocient la meilleure résolution en fonction de la bande passante et de la configuration du téléphone ou de ses limitations en résolution. Exemple : sur un appel direct de 88x5 à 88x5, les téléphones ne transmettent pas de la 720p réelle, ils transmettent une résolution 800x480. Cette limitation est entièrement due à la résolution 5 pouces WVGA de l'écran des 88x5, qui affiche 800x480 pixels.

Type de vidéo	Résolution vidéo	Images par seconde (fps)	Amplitude du débit binaire vidéo
720p	1280 x 720	30	1360-2500 kbps
720p	1280 x 720	15	790-1359 kbps
WVGA	800 x 480	30	660-789 kbps
WVGA	800 x 480	15	350-399 kbps
360p	640 x 360	30	400-659 kbps
360p	640 x 360	15	210-349 kbps
240p	432 x 240	30	180-209 kbps
240p	432 x 240	15	64-179 kbps
VGA	640 x 480	30	520-1500 kbps
VGA	640 x 480	15	280-519 kbps
CIF	352 x 288	30	200-279 kbps
CIF	352 x 288	15	120-199 kbps
SIF	352 x 240	30	200-279 kbps
SIF	352 x 240	15	120-199 kbps
QCIF	176 x 144	30	94-119 kbps
QCIF	176 x 144	15	64-93 kbps

Gestion des casques sur les versions antérieures de Cisco Unified Communications Manager

Si vous disposez d'une version de Cisco Unified Communications Manager antérieure à la 12.5(1)SU1, vous pouvez configurer à distance vos paramètres de casque Cisco pour une utilisation avec des téléphones sur site.

La configuration du casque à distance sur Cisco Unified Communication Manager version 10.5(2), 11.0(1), 11.5(1), 12.0(1) et 12.5(1) nécessite que vous téléchargiez un fichier sur le site Web de téléchargement du logiciel Cisco, que vous modifiiez le fichier, puis que vous le téléchargiez sur le serveur TFTP de Cisco Unified Communications Manager. Il s'agit d'un fichier de notification d'objet JavaScript (JSON). La configuration de casque mise à jour est appliquée aux casques d'entreprise sur une période de 10 à 30 minutes pour éviter qu'une file d'attente de trafic ne se crée sur le serveur TFTP.

Remarque Vous pouvez gérer et configurer des casques par l'intermédiaire de Cisco Unified Communications Manager Administration version 11.5 (1) SU7.

Notez les éléments suivants lorsque vous travaillez sur le fichier JSON :

- Les paramètres ne sont pas appliqués s'il manque une ou des parenthèses dans le code. Utilisez un outil en ligne tel que JSON Formatter et vérifiez le format.
- Définir le paramètre " **HeureMiseàjour** " à l'heure d'origine ou la configuration n'est pas appliquée. Vous pouvez aussi augmenter la valeur de " **HeureMiseàjour** " de +1 pour la rendre supérieure à celle de la version précédente.
- Ne modifiez pas le nom de paramètre ou le paramètre ne sera pas appliqué.

Pour plus d'informations sur le service TFTP, reportez-vous au chapitre "Gérer le micrologiciel du périphérique" du *Guide d'Administration de Cisco Unified Communications Manager et service IM et Presence*.

Mettez à jour vos téléphones à la plus récente version du micrologiciel avant d'appliquer le fichier `defaultheadsetconfig.json`. Le tableau ci-dessous décrit les paramètres par défaut que vous pouvez ajuster avec le fichier JSON.

Télécharger le fichier de configuration du casque par défaut

Avant de configurer les paramètres du casque à distance, vous devez télécharger le fichier d'exemple JSON le plus récent (JavaScript Object Notation).

Procédure

Étape 1 Accédez à l'URL suivante :https://software.cisco.com/download/home/286320550.

Étape 2 Choisissez **Casques Cisco série 500**.

Étape 3 Sélectionnez votre série de casque

Étape 4 Choisissez un dossier de version et sélectionnez le fichier zip.

Étape 5 Cliquez sur le bouton **Télécharger** ou **Ajouter au panier**, puis suivez les invites.

Étape 6 Décompressez le fichier directement sur votre PC.

Que faire ensuite

Modifier le fichier de configuration du casque par défaut, à la page 214

Modifier le fichier de configuration du casque par défaut

Notez les éléments suivants lorsque vous utilisez le fichier JavaScript Object Notation (JSON) :

- Les paramètres ne sont pas appliqués s'il manque une ou des parenthèses dans le code. Utilisez un outil en ligne tel que JSON Formatter et vérifiez le format.
- Définir le paramètre "**updatedTime**" à l'heure d'origine ou la configuration n'est pas appliquée.
- Vérifiez que **NomMicrologiciel** est égal à `LATEST` ou les configurations ne seront pas appliquées.
- Ne modifiez pas un nom de paramètre ou le paramètre ne sera pas appliqué.

Procédure

Étape 1 Ouvrez le fichier `defaultheadsetconfig.json` à l'aide d'un éditeur de texte.

Étape 2 Modifiez les valeurs du paramètre **HeureMiseàjour** et du casque que vous souhaitez modifier.

Vous trouverez ci-dessous un exemple de script. Le script est uniquement fourni à titre de référence. Vous pouvez l'utiliser comme guide lors de la configuration des paramètres de votre casque. Utilisez le fichier JSON qui était inclus dans la version du micrologiciel.

```
{
  "headsetConfig": {
    "templateConfiguration": {
      "configTemplateVersion": "1",
      "updatedTime": 1537299896,
      "reportId": 3,
      "modelSpecificSettings": [
        {
          "modelSeries": "530",
          "models": [
            "520",
            "521",
            "522",
            "530",
            "531",
            "532"
          ],
          "modelFirmware": [
            {
              "firmwareName": "LATEST",
              "latest": true,
              "firmwareParams": [
                {
                  "name": "Speaker Volume",
                  "access": "Both",
                  "usageId": 32,
```

```
            "value": 7
          },
          {
            "name": "Microphone Gain",
            "access": "Both",
            "usageId": 33,
            "value": 2
          },
          {
            "name": "Sidetone",
            "access": "Both",
            "usageId": 34,
            "value": 1
          },
          {
            "name": "Equalizer",
            "access": "Both",
            "usageId": 35,
            "value": 3
          }
        ]
      }
    ]
  },
  {
    "modelSeries": "560",
    "models": [
      "560",
      "561",
      "562"
    ],
    "modelFirmware": [
      {
        "firmwareName": "LATEST",
        "latest": true,
        "firmwareParams": [
          {
            "name": "Speaker Volume",
            "access": "Both",
            "usageId": 32,
            "value": 7
          },
          {
            "name": "Microphone Gain",
            "access": "Both",
            "usageId": 33,
            "value": 2
          },
          {
            "name": "Sidetone",
            "access": "Both",
            "usageId": 34,
            "value": 1
          },
          {
            "name": "Equalizer",
            "access": "Both",
            "usageId": 35,
            "value": 3
          },
          {
            "name": "Audio Bandwidth",
            "access": "Admin",
            "usageId": 36,
```

```
                    "value": 0
                  },
                  {
                    "name": "Bluetooth",
                    "access": "Admin",
                    "usageId": 39,
                    "value": 0
                  },
                  {
                    "name": "DECT Radio Range",
                    "access": "Admin",
                    "usageId": 37,
                    "value": 0
                  }
                  {
                     "name": "Conference",
                    "access": "Admin",
                    "usageId": 41,
                    "value": 0
                ]
              }
            ]
          }
        ]
      }
    }
}
```

Étape 3 Enregistrez le fichier `defaultheadsetconfig.json`.

Que faire ensuite

Installer le fichier de configuration par défaut.

Installer le fichier de configuration par défaut sur Cisco Unified Communications Manager

Une fois que vous avez modifié le fichier `defaultheadsetconfig.json`, installez-le sur Cisco Unified Communications Manager à l'aide de l'outil de gestion des fichiers TFTP.

Procédure

Étape 1 Dans Cisco Unified OS administration, sélectionnez **Mises à niveau logicielles** > **Gestion des fichiers TFTP**.

Étape 2 Sélectionnez **Télécharger un fichier**.

Étape 3 Sélectionnez **Choisir un fichier** et naviguez jusqu'au fichier `defaultheadsetconfig.json`.

Étape 4 Sélectionnez **Télécharger un fichier**.

Étape 5 Cliquez sur **Fermer**.

Redémarrer le serveur Cisco TFTP.

Après avoir chargé le fichier `defaultheadsetconfig.json` dans le répertoire TFTP, redémarrez le serveur TFTP Cisco et réinitialisez les téléphones. Au bout d'environ 10 à 15 minutes, le processus de téléchargement commence et les nouvelles configurations sont appliquées aux casques. Cela prend 10 à 30 minutes de plus pour appliquer les paramètres.

Procédure

Étape 1 Connectez-vous à Cisco Unified Serviceability et sélectionnez **Outils** > **Centre de contrôle - -Services des fonctionnalités**.

Étape 2 Dans la liste déroulante **Serveur**, choisissez le serveur sur lequel le service TFTP Cisco est en cours d'exécution.

Étape 3 Cliquez sur le bouton radio correspondant au **service TFTP** de Cisco.

Étape 4 Cliquez sur **Redémarrer**.

Redémarrer le serveur Cisco TFTP.

CHAPITRE 10

Répertoire personnel et professionnel

Configuration du répertoire d'entreprise

Le Répertoire d'entreprise permet à l'utilisateur de rechercher les numéros de téléphone de ses collègues. Pour pouvoir utiliser cette fonctionnalité, vous devez configurer des répertoires d'entreprise.

Cisco Unified Communications Manager utilise un répertoire LDAP (Lightweight Directory Access Protocol) pour stocker les informations d'authentification et d'autorisation concernant les utilisateurs des applications Cisco Unified Communications Manager qui interfacent avec Cisco Unified Communications Manager. L'authentification établit les droits d'un utilisateur concernant l'accès au système. L'autorisation définit les ressources de téléphonie qu'un utilisateur est autorisé à utiliser, comme par exemple un numéro de poste donné.

Les téléphones IP Cisco utilisent l'allocation dynamique pour SecureApp sur le client et les serveurs. Cela permet de garantir que votre téléphone peut lire les certificats supérieurs à 4 Ko et réduit la fréquence des messages d'erreur `Hôte introuvable` lorsqu'un utilisateur accède à son répertoire.

Pour obtenir plus d'informations, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Une fois la configuration de l'annuaire LDAP terminée, les utilisateurs peuvent utiliser le service Répertoire d'entreprise de leur téléphone pour rechercher des utilisateurs dans le répertoire d'entreprise.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Configuration du répertoire personnel

Le répertoire personnel permet aux utilisateurs de stocker un ensemble de numéros personnels.

Le répertoire personnel est constitué des fonctionnalités suivantes :

- Le Carnet d'adresses personnel (PAB, Personal Address Book)
- La numérotation abrégée

- L'outil de synchronisation du carnet d'adresses (TABSynch)

Les utilisateurs peuvent se servir de ces méthodes pour accéder aux fonctionnalités du répertoire personnel :

- À partir d'un navigateur Web : les utilisateurs peuvent accéder aux fonctionnalités Carnet d'adresses personnel et Numérotation abrégée depuis le portail d'aide en libre-service de Cisco Unified Communications.
- Sur le téléphone IP Cisco : choisissez **Contacts** pour effectuer une recherche dans le répertoire d'entreprise ou le répertoire personnel de l'utilisateur.
- À partir d'une application Microsoft Windows : les utilisateurs peuvent utiliser l'outil de synchronisation TABSynch pour synchroniser leur carnet d'adresses personnel avec le carnet d'adresses Microsoft Windows (WAB). Les utilisateurs qui souhaitent utiliser le carnet d'adresses Microsoft Outlook (OAB), doivent d'abord importer les données de ce carnet d'adresses dans le carnet d'adresses Windows (WAB). La fonction TabSync peut alors être utilisée pour synchroniser le carnet d'adresses Windows avec le répertoire personnel. Pour obtenir des instructions sur TABSync, reportez-vous à Téléchargement du synchroniseur de carnet d'adresses du téléphone IP Cisco, à la page 221 et à Configuration du synchroniseur, à la page 222.

Les téléphones IP Cisco utilisent l'allocation dynamique pour SecureApp sur le client et les serveurs. Cela permet de garantir que votre téléphone peut lire les certificats supérieurs à 4 Ko et réduit la fréquence des messages d'erreur `Hôte introuvable` lorsqu'un utilisateur accède à son répertoire.

Pour vous assurer que les utilisateurs du synchroniseur de carnet d'adresses du téléphone IP Cisco accèdent uniquement à leur données d'utilisateur final, activez le service Web Cisco UXL dans Cisco Unified Serviceability.

Pour configurer le répertoire personnel à partir d'un navigateur Web, les utilisateurs doivent accéder au portail d'aide en libre-service. Vous devez communiquer aux utilisateurs une URL et les informations d'authentification.

Configuration des entrées du répertoire personnel d'un utilisateur

Les utilisateurs peuvent configurer des entrées de répertoire personnel sur le téléphone IP Cisco. Pour configurer un répertoire personnel, les utilisateurs doivent avoir accès aux fonctionnalités suivantes :

- Portail d'aide en libre-service : vérifiez que les utilisateurs savent comment accéder au portail d'aide en libre-service. Pour obtenir plus d'informations, reportez-vous à Configuration de l'accès des utilisateurs au portail d'aide en libre-service, à la page 86.
- Synchroniseur de carnet d'adresses du téléphone IP Cisco : prenez soin de distribuer le programme d'installation aux utilisateurs. Reportez-vous à Téléchargement du synchroniseur de carnet d'adresses du téléphone IP Cisco, à la page 221.

Remarque Le synchroniseur du carnet d'adresses du téléphone IP Cisco n'est pris en charge que par les versions de Windows non prises en charge (par exemple, Windows XP et versions antérieures). L'outil n'est pas pris en charge sur les versions plus récentes de Windows. À l'avenir, il sera supprimé de la liste des modules additionnels de Cisco Unified Communications Manager.

Téléchargement du synchroniseur de carnet d'adresses du téléphone IP Cisco

Pour télécharger une copie du synchroniseur afin de l'envoyer aux utilisateurs, procédez comme suit :

Procédure

Étape 1 Pour obtenir le programme d'installation, sélectionnez **Application** > **Modules complémentaires** dans Cisco Unified Communications Manager Administration.

Étape 2 Sélectionnez **Télécharger**, situé à côté du nom du composant logiciel enfichable du synchroniseur de carnet d'adresses du téléphone IP Cisco.

Étape 3 Lorsque la boîte de dialogue de téléchargement du fichier apparaît, sélectionnez **Enregistrer**.

Étape 4 Envoyez le fichier TabSyncInstall.exe et les instructions de la section Déploiement du synchroniseur de carnet d'adresses du téléphone IP Cisco, à la page 221 à tous les utilisateurs qui doivent installer cette application.

Déploiement du synchroniseur de carnet d'adresses du téléphone IP Cisco

Le synchroniseur de carnet d'adresses du téléphone IP Cisco synchronise les données stockées dans le carnet d'adresses Microsoft Windows avec le répertoire Cisco Unified Communications Manager et le carnet d'adresses personnel du portail d'aide en libre-service.

Conseil Pour synchroniser le carnet d'adresses Windows avec le carnet d'adresses personnel, vous devez avoir saisi tous les utilisateurs du carnet d'adresses Windows dans le carnet d'adresses Windows avant d'effectuer les procédures suivantes.

Installation du synchroniseur

Procédez comme suit pour installer le synchroniseur de carnet d'adresses du téléphone IP Cisco :

Procédure

Étape 1 Demandez à l'administrateur système de vous fournir le fichier d'installation du synchroniseur de carnet d'adresses du téléphone IP Cisco.

Étape 2 Cliquez deux fois sur le fichier TabSyncInstall.exe que votre administrateur vous a procuré.

Étape 3 Sélectionnez **Exécuter**.

Étape 4 Cliquez sur **Suivant**.

Étape 5 Lisez les informations de l'accord de licence, puis sélectionnez **J'accepte**. Cliquez sur **Suivant**.

Étape 6 Sélectionnez le répertoire dans lequel vous souhaitez installer l'application et sélectionnez **Suivant**.

Étape 7 Sélectionnez **Installer**.

Étape 8 Sélectionnez **Terminer**.

Étape 9 Pour compléter le processus, suivez les étapes décrites à la section Configuration du synchroniseur, à la page 222.

Configuration du synchroniseur

Procédez comme suit pour configurer le synchroniseur de carnet d'adresses du téléphone IP Cisco :

Procédure

Étape 1 Ouvrez le synchroniseur de carnet d'adresses du téléphone IP Cisco.

Si vous avez accepté le répertoire d'installation par défaut, vous pouvez ouvrir l'application en sélectionnant **Démarrer** > **Tous les programmes** > **Cisco Systems** > **TabSync**.

Étape 2 Pour configurer les informations utilisateur, sélectionnez **Utilisateur**.

Étape 3 Entrez le nom et le mot de passe de l'utilisateur du téléphone IP Cisco et sélectionnez **OK**.

Étape 4 Pour configurer les informations du serveur Cisco Unified Communications Manager, sélectionnez **Serveur**.

Étape 5 Saisissez l'adresse IP ou le nom d'hôte et le numéro de port du serveur Cisco Unified Communications Manager puis sélectionnez **OK**.

Si vous ne disposez pas ces informations, contactez l'administrateur système.

Étape 6 Pour lancer le processus de synchronisation de répertoire, sélectionnez **Synchroniser**.

La fenêtre Synchronization Status (État de la synchronisation) présente l'état de la synchronisation du carnet d'adresses. Si vous avez sélectionné l'intervention utilisateur pour la règle relative aux entrées doubles, la fenêtre Sélection d'entrées doubles apparaît, le cas échéant.

Étape 7 Sélectionnez l'entrée à inclure dans votre carnet d'adresses personnel et sélectionnez **OK**.

Étape 8 Lorsque la synchronisation est terminée, sélectionnez **Quitter** pour fermer le Synchroniseur de carnet d'adresses de Cisco Unified CallManager.

Étape 9 Pour vérifier que la synchronisation a réussi, connectez-vous au portail d'aide en libre-service et sélectionnez **Carnet d'adresses personnel**. Les utilisateurs figurant dans votre carnet d'adresses Windows doivent apparaître.

SECTION IV

Résolution des problèmes du téléphone IP Cisco

CHAPITRE 11

Surveillance des systèmes téléphoniques

État du téléphone IP Cisco

Cette section décrit comment afficher les informations de modèle, les messages d'état et les statistiques réseau sur le téléphone IP Cisco 8800.

- Caractéristiques : affiche des informations sur le matériel et les logiciels du téléphone.
- Menu d'état : permet d'accéder aux écrans d'affichage des messages d'état, des statistiques réseau et des statistiques relatives à l'appel en cours.

Vous pouvez utiliser les informations affichées sur ces écrans pour surveiller le fonctionnement d'un téléphone et pour fournir une assistance lors d'un dépannage.

La plupart de ces informations, ainsi que d'autres informations apparentées, peuvent être obtenues à distance par le biais de la page Web du téléphone.

Pour plus d'informations sur le dépannage, reportez-vous à la section Dépannage, à la page 261.

Affichage de la fenêtre Informations sur le téléphone

Pour afficher l'écran Caractéristiques, procédez comme suit.

Procédure

Étape 1 Appuyez sur **Applications** .

Étape 2 Sélectionnez **Informations sur le téléphone**.

Si l'utilisateur est connecté à un serveur sécurisé ou authentifié, l'icône correspondante (verrou ou certificat) est affichée dans la fenêtre Informations sur le téléphone, à droite de l'option du serveur. Si l'utilisateur n'est pas connecté à un serveur sécurisé ou authentifié, aucune icône n'est affichée.

Étape 3 Pour quitter l'écran Caractéristiques, appuyez sur **Quitter**.

Champs d'informations sur le téléphone

Le tableau suivant décrit les paramètre d'informations sur le téléphone.

Tableau 40 : Paramètres d'informations sur le téléphone

Option	Description
Référence	Le numéro de modèle du téléphone.
Adresse IPv4	Adresse IP du téléphone.
Nom d'hôte	Nom d'hôte du téléphone.
Charge active	Version du micrologiciel actuellement installée sur le téléphone. L'utilisateur peut appuyer sur **Détails** pour plus d'informations.
Charge inactive	La charge inactive n'apparaît que lorsqu'un téléchargement est en cours. Une icône de téléchargement et l'état « Mise à niveau en cours » ou « Échec de la mise à niveau » s'affichent également. Si un utilisateur appuie sur **Détails** pendant une mise à niveau, le nom du fichier téléchargé ainsi que ses composants s'affichent. Le téléchargement d'une nouvelle image du micrologiciel peut être paramétré en avance depuis la fenêtre de maintenance. Ainsi, plutôt que d'attendre que tous les téléphones téléchargent le micrologiciel, le système passe plus rapidement de la réinitialisation d'un chargement existant à l'état Inactif à l'installation du nouveau chargement. Lorsque le téléchargement est terminé, l'icône change pour indiquer l'état achevé. Une coche s'affiche si le téléchargement est réussi ou un « X » s'affiche si le téléchargement a échoué. Si possible, le reste des téléchargements de chargements continue.
Dernière mise à niveau	Date de la mise à niveau du micrologiciel la plus récente.
Serveur actif	Nom de domaine du serveur auprès duquel le téléphone est enregistré.
Serveur en veille	Nom de domaine du serveur de veille.

Afficher le menu État

Le menu État inclut les options suivantes, qui fournissent des informations sur le téléphone et son fonctionnement :

- Messages d'état : affiche l'écran Messages d'état, qui affiche un journal des messages système importants.
- Statistiques Ethernet : affiche l'écran Statistiques Ethernet, qui affiche les statistiques de trafic Ethernet.

- Statistiques sans fil : affiche l'écran Statistiques Sans fil, le cas échéant.
- Statistiques d'appel : affiche les compteurs et les statistiques pour l'appel en cours.
- Point d'accès actuel : affiche l'écran Point d'accès actuel, le cas échéant.

Pour afficher le menu État, procédez comme suit :

Procédure

Étape 1 Pour afficher le menu État, appuyez sur **Applications** .
Étape 2 Sélectionnez **Paramètres Admin** > **État**.
Étape 3 Pour quitter le menu État, appuyez sur **Quitter**.

Afficher la fenêtre Messages d'état

La fenêtre Messages d'état affiche les 30 derniers messages d'état générés par le téléphone. Vous pouvez accéder à cet écran à tout moment, même si le téléphone n'a pas fini de démarrer.

Procédure

Étape 1 Appuyez sur **Applications** .
Étape 2 Sélectionnez **Paramètres admin.** > **Statut** > **Messages d'état**.
Étape 3 Pour supprimer les messages d'état actuels, appuyez sur **Effacer**.
Étape 4 Pour quitter l'écran Messages d'état, appuyez sur **Quitter**.

Champs relatifs aux messages d'état

Le tableau suivant présente les messages d'état qui figurent sur l'écran Messages d'état du téléphone.

Tableau 41 : Messages d'état sur le téléphone IP Cisco Unified

Message	Description	Explication et action possibles
Erreur taille du TFTP CFG	Le fichier de configuration est trop volumineux pour le système de fichiers du téléphone.	Éteignez le téléphone puis rallu
Erreur checksum	Le fichier de téléchargement logiciel est endommagé.	Obtenez une nouvelle copie du et placez-la dans le répertoire T copier des fichiers dans ce répe du serveur TFTP est fermé ; sinc endommagés.
Impossible d'obtenir une adresse IP de DHCP	Le téléphone n'a pas encore obtenu d'adresse IP à partir d'un serveur DHCP. Cela peut se produire lorsque vous effectuez une réinitialisation d'usine ou initiale.	Vérifiez que le serveur DHCP adresse IP est disponible pour

Message	Description	Explication et action possibles
CTL et ITL installés	Les fichiers CTL et ITL sont installés sur le téléphone.	Aucune. Ce message est uniqueme d'information. Ni le fichier CTL n installé auparavant.
CTL installée	Un fichier Liste de confiance des certificats (CTL, Certificate Trust List) est installé sur le téléphone.	Aucune. Ce message est uniqueme d'information. Le fichier CTL n'a précédemment.
Échec MàJ CTL	Le téléphone n'a pas pu mettre à jour le fichier CTL (liste de confiance des certificats).	Cela est dû à un problème avec le fi TFTP.
Expiration DHCP	Le serveur DHCP ne répond pas.	Le réseau est occupé : les erreurs c automatiquement résolues dès la d réseau. Aucune connectivité réseau entre l téléphone : vérifiez les connexions Le serveur DHCP est hors service : du serveur DHCP. Les erreurs persistent : envisagez l' IP statique.
Expiration DNS	Le serveur DNS n'a pas répondu.	Le réseau est occupé : les erreurs c automatiquement résolues dès la d réseau. Aucune connectivité réseau entre l téléphone : vérifiez les connexions Le serveur DNS est hors service : du serveur DNS.
DNS - Hôte inconnu	Le service DNS n'a pas pu résoudre le nom du serveur TFTP ou du Cisco Unified Communications Manager.	Vérifiez que les noms d'hôte du se Cisco Unified Communications Ma configurés dans le DNS. Envisagez d'utiliser des adresses I d'hôte.
Adresse IP en double	Un autre périphérique utilise l'adresse IP qui est affectée au téléphone.	Si le téléphone est doté d'une adre que vous n'avez pas affecté une ad Si vous utilisez DHCP, vérifiez la DHCP.
Suppression des fichiers CTL et ITL	Suppression du fichier CTL ou ITL.	Aucune. Ce message est uniqueme d'information.

Message	Description	Explication et action possibles
Erreur de mise à jour des paramètres régionaux	Un ou plusieurs fichiers de localisation n'ont pas pu être trouvés dans le répertoire TFTPPath ou n'étaient pas valides. La langue n'a pas été changée.	Depuis Cisco Unified Operatin vérifiez que les fichiers suivan sous-répertoires dans la Gestio • Situé dans un sous-réperto la langue du réseau : • tones.xml • Dans le sous-répertoire qu utilisateur : • glyphs.xml • dictionary.xml • kate.xml
Fichier introuvable <Cfg File>	Le fichier basé sur le nom et de configuration par défaut est introuvable sur le serveur TFTP.	Le fichier de configuration d'u le téléphone est ajouté à la base Communications Manager. Si l la base de données Cisco Unifie le serveur TFTP génère la répo **`introuvable`**. • Le téléphone n'est pas enr Communications Manage Vous devez ajouter le télép Unified Communications pas l'enregistrement auton obtenir plus d'information disponibles pour ajouter d • Si vous utilisez DHCP, vé pointe vers le serveur TF • Si vous utilisez des adress configuration du serveur
Fichier introuvable <CTLFile.tlv>	Ce message s'affiche sur le téléphone lorsque le cluster Cisco Unified Communications Manager n'est pas en mode sécurisé.	Aucun impact ; le téléphone pe auprès de Cisco Unified Comm
Adresse IP libérée	Le téléphone est configuré pour libérer l'adresse IP.	Le téléphone reste inactif jusq jusqu'à la réinitialisation de l'a
ITL installé	Le fichier ITL est installé sur le téléphone.	Aucune. Ce message est uniqu d'information. Le fichier ITL n'

Message	Description	Explication et action possibles
Image : rejet HC	L'application téléchargée n'est pas compatible avec le matériel du téléphone.	Ceci se produit lorsque vous tentez téléphone, une version du logiciel q les changements de matériel effect Vérifiez l'ID de chargement attribu Cisco Unified Communications M **Périphérique** > **Téléphone**). Saisi affichée sur le téléphone.
Aucun routeur par défaut	Aucun routeur par défaut n'est indiqué dans la configuration de l'adresse statique ou de DHCP.	Si le téléphone est doté d'une adres que le routeur par défaut est confi Si vous utilisez DHCP, le serveur routeur par défaut. Vérifiez la con DHCP.
Adr. IP serveur DNS manquante	Un nom a été spécifié, mais la configuration d'IP statique ou DHCP n'a pas spécifié d'adresse de serveur DNS.	Si le téléphone a une adresse IP sta serveur DNS est bien configuré. Si vous utilisez DHCP, le serveur serveur DNS. Vérifiez la configura
Aucune liste de confiance installée	Le fichier CTL ou le fichier ITL n'est pas installé sur le téléphone.	La liste de confiance n'est pas confi Communications Manager ; ce der charge la sécurité par défaut.
Un téléphone n'a pas pu être enregistré. La taille de clé du certificat n'est pas compatible FIPS.	FIPS nécessite que le certificat du serveur RSA comporte 2048 bits ou plus.	Mettre à jour le certificat.
Redémarrage requis par Cisco Unified Communications Manager	Le téléphone redémarre sur demande de Cisco Unified Communications Manager.	Il est possible que la configuration changée dans Cisco Unified Comm que ces modifications aient été val Appliquer.
Erreur d'accès TFTP	Le serveur TFTP pointe vers un répertoire qui n'existe pas.	Si vous utilisez DHCP, vérifiez que vers le serveur TFTP adéquat. Si vous utilisez des adresses IP sta configuration du serveur TFTP.
Erreur TFTP	Le téléphone ne reconnaît pas un code d'erreur fourni par le serveur TFTP.	Contactez le centre d'assistance tec
Expiration TFTP	Le serveur TFTP n'a pas répondu.	Le réseau est occupé : les erreurs d résoudre d'elles-mêmes lorsque la diminuera. Pas de connectivité réseau entre le téléphone : vérifiez les connexions Le serveur TFTP est en panne : vér serveur TFTP .

Message	Description	Explication et action possibles
Délai expiré	Le demandeur a tenté d'exécuter une transaction 802.1X mai le délai a expiré car l'authentifiant était absent.	Le délai d'authentification expi 802.1X n'est pas configuré sur
Échec de la MàJ de la liste de confiance	La mise à jour des fichiers CTL et ITL a échoué.	Des fichiers CTL et ITL sont in la mise à jour des nouveaux fic Voici les raisons possibles de c • Une panne réseau s'est pr • Le serveur TFTP a subi u • Le nouveau jeton de sécur fichier CTL et le certificat fichier ITL ont été introdu disponibles dans les fichie téléphone. • Une panne s'est produite Solutions possibles: • Vérifiez la connectivité ré • Vérifiez que le serveur TF fonctionne normalement. • Si le serveur Transactiona pris en charge par Cisco U Communications Manage est actif et fonctionne nor • Vérifiez la validité du jeto TFTP. Si vous avez essayé toutes les so supprimez manuellement les fi réinitialisez le téléphone.
Liste de confiance mise à jour	Le fichier CTL, le fichier ITL ou les deux fichiers ont été mis à jour.	Aucune. Ce message est uniqu d'information.
Erreur de version	Le nom du téléphone fichier image du téléphone est incorrect.	Assurez-vous de l'exactitude du
XmlDefault.cnf.xml ou .cnf.xml, selon le nom de périphérique du téléphone	Nom du fichier de configuration.	Aucune. Ce message indique le configuration du téléphone.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Afficher l'écran Informations réseau

Utilisez les informations affichées sur l'écran d'informations sur le réseau pour résoudre les problèmes de connexion sur un téléphone.

Si un utilisateur rencontre des problèmes de connexion à un réseau téléphonique, un message s'affiche sur le téléphone.

Procédure

Étape 1 Pour afficher le menu État, appuyez sur **Applications** .

Étape 2 Sélectionnez **Paramètres admin.** > **Statut** > **Messages d'état**.

Étape 3 Sélectionnez **Informations réseau**.

Étape 4 Pour quitter les informations du réseau, appuyez sur la touche **Quitter**.

Afficher l'écran Statistiques réseau

L'écran Statistiques réseau affiche des informations sur les performances du réseau et du téléphone.

Pour afficher l'écran Statistiques réseau, procédez comme suit :

Procédure

Étape 1 Appuyez sur **Applications** .

Étape 2 Sélectionnez **Paramètres Admin**>**Statut**>**Statistiques réseau**.

Étape 3 Pour réinitialiser à 0 les statistiques de trames reçues (Rx Frames), de trames émises (Tx Frames) et de trames multidiffusion émises (Tx multicast), appuyez sur **Effacer**.

Étape 4 Pour quitter l'écran Statistiques Ethernet, appuyez sur **Quitter**.

Informations sur les statistiques Ethernet

Les tableaux suivants décrivent les informations disponibles à l'écran Statistiques Ethernet.

Tableau 42 : Informations sur les statistiques Ethernet

Élément	Description
Rx Frames (Trames reçues)	Nombre de paquets reçus par le téléphone.
Tx Frames (Trames émises)	Nombre de paquets envoyés par le téléphone.
Rx Broadcasts (Trames de diffusion reçues)	Nombre de paquets de diffusion reçus par le téléphone.

Élément	Description
Cause de redémarrage	Cause de la dernière réinitialisation du téléphone. Indique une des valeurs suivantes : • Initialisé • TCP-timeout • CM-closed-TCP • TCP-Bad-ACK • CM-reset-TCP • CM-aborted-TCP • CM-NAKed • KeepaliveTO • Failback • Phone-Keypad • Phone-Re-IP • Reset-Reset • Reset-Restart • Phone-Reg-Rej • Image : rejet HC • CM-ICMP-Unreach • Phone-Abort
Temps écoulé	Durée écoulée depuis le dernier redémarrage du téléphone.
Port 1	État de la liaison et connexion avec le port réseau. Par exemple, **`Auto 100 Mb Full-Duplex`** signifie que le port réseau est en liaison active et a négocié automatiquement une connexion duplex intégral de 100 Mbits/s.
Port 2	État de la liaison et connexion avec le port PC.
État DHCP (IPv4 / IPv6)	• En mode IPv4-uniquement, affiche seulement l'état DHCPv4, comme DHCP BOUND. • En mode IPv6, affiche seulement l'état DHCPv6, comme ROUTER ADVERTISE. • Des informations sur l'état DHCPv6 sont affichées.

Les tableaux suivants décrivent les messages apparaissant pour les états DHCPv4 et DHCPv6.

Tableau 43 : Messages des statistiques Ethernet DHCPv4

État DHCPv4	Description
CDP INIT (Initialisation CDP)	CDP n'est pas lié ou WLAN est hors service
DHCP BOUND (Liaison DHCP)	DHCPv4 est lié
DHCP DISABLED (DHCP désactivé)	DHCPv4 est désactivé

État DHCPv4	Description
DHCP INIT (Initialisation DHCP)	DHCPv4 est initialisé
DHCP INVALID (DHCP incorrect)	DHCPv4 est non valide, il s'agit de son état initial
DHCP RENEWING (Renouvellement DHCP)	DHCPv4 est en cours de renouvellement
DHCP REBINDING (Nouvelle liaison DHCP)	DHCPv4 est en cours de ré-assignation
DHCP REBOOT (Redémarrage DHCP)	DHCPv4 a initié son redémarrage
DHCP REQUESTING (Requête DHCP)	DHCPv4 effectue une demande
DHCP RESYNC (Resynchronisation DHCP)	DHCPv4 est en cours de resynchronisation
DHCP WAITING COLDBOOT TIMEOUT (DHCP - Temporisation démarrage à froid)	DHCPv4 est en cours de démarrage
DHCP UNRECOGNIZED (DHCP non reconnu)	État DHCPv4 non reconnu
DISABLED DUPLICATE IP (Adresse IP en double désactivée)	Adresse IPv4 en double
DHCP TIMEOUT	Délai DHCPv4 expiré
IPV4 STACK TURNED OFF	Le téléphone est en mode IPv6 uniquement, le mode IPv4 Pile est désactivé
ILLEGAL IPV4 STATE	État IPv4 illégal, ne devrait pas se produire

Tableau 44 : Messages des statistiques Ethernet DHCPv6

État DHCPv6	Description
CDP INIT (Initialisation CDP)	CDP est en cours d'initialisation
DHCP6 BOUND (Liaison DHCP6)	DHCPv6 est lié
DHCP6 DISABLED (DHCP6 désactivé)	DHCPv6 est désactivé
DHCP6 RENEW (Renouvellement DHCP6)	DHCPv6 est en cours de renouvellement
DHCP6 REBIND (Nouvelle liaison DHCP6)	DHCPv6 est en cours de ré-assignation
DHCP6 INIT (Initialisation DHCP6)	DHCPv6 est en cours d'initialisation
DHCP6 SOLICIT (Sollicitation de DHCP6)	DHCPv6 est en cours de sollicitation
DHCP6 REQUEST (Requête DHCP6)	DHCPv6 effectue une demande
DHCP6 RELEASING (Libération de DHCP6)	DHCPv6 est en cours de libération
DHCP6 RELEASED (DHCP6 libéré)	DHCPv6 a libéré
DHCP6 DISABLING (Désactivation de DHCP6)	DHCPv6 est en cours de désactivation

État DHCPv6	Description
DHCP6 DECLINING (Refus DHCP6)	DHCPPv6 est en cours de refus
DHCP6 DECLINED (DHCP6 refusé)	DHCPv6 a été refusé
DHCP6 INFOREQ (Requête infos DHCP6)	DHCPv6 est en attente d'informations
DHCP6 INFOREQ DONE (Requête infos DHCP6 terminée)	DHCPv6 a reçu les informations
DHCP6 INVALID (DHCP6 incorrect)	DHCPv6 est non valide, il s'agit de son état initial
DISABLED DUPLICATE IPV6 (Adresse IPv6 en double désactivée)	DHCPv6 est désactivé, mais adresse IPv6 en double détectée
DHCP6 DECLINED DUPLICATE IP (DHCP6 a refusé une adresse IP en double)	DHCPv6 a été refusé, adresse IPv6 en double détectée.
ROUTER ADVERTISE., (DUPLICATE IP)	Adresse IPv6 auto-configurée en double
DHCP6 WAITING COLDBOOT TIMEOUT (DHCP6 - Temporisation du démarrage à froid)	DHCPv6 est en cours de démarrage
DHCP6 TIMEOUT USING RESTORED VAL (DHCP6 - Temporisation avec valeurs restaurées)	Délai DHCPv6 expiré, utilisation de la valeur sauvegardée dans la mémoire flash
DHCP6 TIMEOUT CANNOT RESTORE (DHCP6 échec restauration temporisation)	Délai DHCPv6 expiré, aucune valeur sauvegardée dans la mémoire flash
IPV6 STACK TURNED OFF (Pile IPv6 désactivée)	Le téléphone est en mode IPv4 uniquement avec IPv6 Stack désactivé
ROUTER ADVERTISE., (GOOD IP)	
ROUTER ADVERTISE., (BAD IP)	
UNRECOGNIZED MANAGED BY (Géré par inconnu)	Adresse IPv6 ne provenant pas du routeur ni du serveur DHCPv6
ILLEGAL IPV6 STATE (État IPv6 illicite)	État IPv6 illégal, ne devrait pas se produire

Afficher l'écran Statistiques sans fil

Cette procédure s'applique uniquement aux téléphones IP sans fil Cisco 8861.

Pour afficher l'écran Statistiques sans fil, procédez comme suit :

Procédure

Étape 1 Appuyez sur **Applications** .

Étape 2 Sélectionnez **Param. Admin**>**État** > **Statistiques sans fil**.

Étape 3 Pour réinitialiser les Statistiques sans fil sur 0, appuyez sur **Effacer**.

Étape 4 Pour quitter l'écran Statistiques sans fil, appuyez sur **Quitter**.

Statistiques WLAN

Le tableau suivant décrit les statistiques WLAN sur le téléphone.

Tableau 45 : Statistiques WLAN du téléphone IP Cisco Unified

Élément	Description
tx bytes	Nombre d'octets transmis par le téléphone.
rx bytes	Nombre d'octets reçus par le téléphone.
tx packets	Nombre de paquets transmis par le téléphone.
rx packets	Nombre de paquets reçus par le téléphone.
tx packets dropped	Nombre de paquets abandonnés pendant la transmission.
rx packets dropped	Nombre de paquets abandonnés pendant la réception.
tx packets errors	Nombre de paquets erronés transmis par le téléphone.
rx packets errors	Nombre de paquets erronés reçus par le téléphone.
Tx frames	Nombre de MSDU transmises avec succès.
tx multicast frames	Nombre de MSDU de multidiffusion transmises avec succès.
tx retry	Nombre de MSDU transmises avec succès après une ou plusieurs retransmissions.
tx multi retry	Nombre de MSDU de multidiffusion transmises avec succès après une ou plusieurs retransmissions.
tx failure	Nombre de MSDU non transmises à cause du nombre de tentatives de transit dépassant la limite de tentatives.
rts succeess	Ce compteur augmente lorsqu'un CTS est reçu en réponse à un RTS.
rts failure	Ce compteur augmente lorsqu'un CTS n'est pas reçu en réponse à un RTS.
ack failure	Ce compteur augmente lorsqu'un ACK n'est pas reçu quand attendu.
rx duplicate frames	Nombre de trames reçues que le champ Contrôle de séquence a indiquées comme étant des doublons.
rx fraagmented packets	Nombre de MPDU de type Données ou Gestion reçues avec succès.
Roaming count	Nombre d'itinérances effectuées avec succès.

Afficher la fenêtre Statistiques d'appel

Vous pouvez accéder à l'écran Statistiques d'appel du téléphone pour afficher les compteurs, les statistiques et les mesures de qualité d'écoute de l'appel le plus récent.

Remarque Vous pouvez aussi afficher à distance les statistiques d'appel, en accédant à la page Web Statistiques de streaming dans un navigateur Web. Cette page Web contient des statistiques RTCP supplémentaires qui ne sont pas disponibles sur le téléphone.

Un appel peut utiliser plusieurs flux de voix, mais les données ne sont capturées que pour le flux de voix le plus récent. Les flux de voix sont des flux de paquets entre deux terminaux. Si un terminal est mis en attente, le flux de voix s'arrête, même si l'appel est toujours connecté. Lorsque l'appel reprend, un nouveau flux de paquets de voix commence, et les nouvelles données d'appel remplacent les anciennes.

Procédure

Étape 1 Appuyez sur **Applications**.

Étape 2 Sélectionnez **Param Admin** > **État** > **Statistiques d'appel**.

Étape 3 Pour quitter l'écran Statistiques d'appel, appuyez sur **Quitter**.

Champs relatifs aux statistiques d'appel

Le tableau suivant décrit les éléments de l'écran Statistiques d'appel.

Tableau 46 : Éléments de statistiques d'appel pour le téléphone Cisco Unified

Élément	Description
Codec appelé	Type de flux vocal reçu (flux RTP audio à partir de codec) : • G.729 • G.722 • G722.2 AMR-WB • G.711 mu-law • G.711 A-law • iLBC • Opus • iSAC

Élément	Description
Codec de l'appelant	Type de flux vocal transmis (flux RTP audio à partir de codec) : • G.729 • G.722 • G722.2 AMR-WB • G.711 mu-law • G.711 A-law • iLBC. • Opus • iSAC
Taille appelé	Taille, en millisecondes, des paquets de voix inclus dans le flux de voix reçu (transmission de flux par RTP).
Taille de l'appelant	Taille, en millisecondes, des paquets de voix inclus dans le flux de voix émis.
Paquets de l'appelé	Nombre de paquets de voix RTP reçus depuis l'ouverture du flux de voix. **Remarque** Ce nombre n'est pas nécessairement identique au nombre de paquets de voix RTP reçus depuis le début de l'appel, car l'appel peut avoir été mis en attente.
Paquets de l'appelant	Nombre de paquets de voix RTP transmis depuis l'ouverture du flux de voix. **Remarque** Ce nombre n'est pas nécessairement identique au nombre de paquets de voix RTP transmis depuis le début de l'appel, car l'appel peut avoir été mis en attente.
Gigue moyenne	Estimation de la gigue moyenne, en millisecondes, des paquets RTP (retard dynamique subi par un paquet lorsqu'il traverse le réseau), qui a été observée depuis l'ouverture du flux de voix de réception.
Gigue maximale	Gigue maximale, en millisecondes, observée depuis l'ouverture du flux de voix de réception.
Refusé par l'appelé	Nombre de paquets RTP inclus dans le flux de voix de réception et abandonnés (paquets incorrects, trop de retard, etc.). **Remarque** Le téléphone supprime les paquets d'une charge utile de bruit de confort de type 19, qui sont générés par les passerelles Cisco, car ils augmentent ce nombre.
Paquets perdus appelé	Paquets RTP manquants (perdus en chemin).
Mesures de la qualité d'écoute	

Élément	Description
Taux de masquage cumulé	Nombre total de trames de masquage divisé par le nombre total de trames de conversation reçues depuis le début du flux de voix.
Taux de masquage par intervalle	Nombre de trames de masquage divisé par le nombre de trames de voix incluses dans le précédent intervalle de 3 secondes de conversation active. Si la détection d'activité vocale (VAD) est utilisée, un intervalle plus long peut être nécessaire pour accumuler 3 secondes de conversation active.
Taux de masquage maximal	Taux de masquage par intervalle le plus élevé depuis le début du flux de voix.
Durée en secondes masquées	Durée, en secondes, des événements de masquage (trames perdues) depuis le début du flux de voix (inclut les secondes masquées de haut niveau).
Durée en secondes masquées de haut niveau	Durée, en secondes, pendant laquelle plus de 5 % des événements de masquage (trames perdues) se sont produits depuis le début du flux de voix.
Latence	Estimation de la latence du réseau, exprimée en millisecondes. Cette valeur représente une moyenne mobile du retard aller-retour, mesurée à la réception des blocs de rapport du récepteur RTCP.

Afficher la fenêtre du point d'accès actuel

L'écran Point d'accès actuel affiche des statistiques sur le point d'accès utilisé par le téléphone IP Cisco 8861 pour les communications sans fil.

Procédure

Étape 1 Appuyez sur **Applications** .

Étape 2 Sélectionnez **Paramètres admin** > **Statut** > **Point d'accès actuel**.

Étape 3 Pour quitter l'écran Point d'accès actuel, appuyez sur **Quitter**.

Champs Points d'accès actuels

Le tableau suivant décrit les champs de l'écran Point d'accès actuel.

Tableau 47 : Éléments de Point d'accès actuel

Élément	Description
Nom AP (Nom du point d'accès)	Nom du point d'accès, s'il est conforme à la norme CCX. Sinon, l'adresse MAC s'affiche ici.
Adresse MAC	Adresse MAC du point d'accès.
Fréquence	La dernière fréquence à laquelle ce point d'accès a été observé.
Canal actuel	Le dernier canal dans lequel le point d'accès à été observé.

Élément	Description
Dernier RSSI	Le dernier RSSI dans lequel le point d'accès a été observé.
Intervalle de balise	Nombre d'unités de temps entre les balises. Une unité de temps correspond à 1,024 ms.
Capacité	Ce champ contient plusieurs sous-champs indiquant les capacités optionnelles demandées ou publiées.
Taux de base	Les débits de données requis par le point d'accès et le point d'accès sur lequel la station doit être capable de fonctionner.
Taux facultatifs	Les débits de données pris en charge par le point d'accès et les points d'accès optionnels sur lesquels la station peut fonctionner.
Débits VHT (rx) pris en charge	Ensemble de RX MCS pris en charge par VHT reçus du point d'accès.
Débits VHT (tx) pris en charge	Ensemble de TX MCS pris en charge par VHT reçus du point d'accès.
HT MCS pris en charge	Ensemble de MCS pris en charge par HT reçus depuis le point d'accès.
Période de DTIM	Chaque nième balise marque une période DTIM. Après chaque balise DTIM, le point d'accès envoie tous les paquets de diffusion ou de multidiffusion en file d'attente pour un périphérique en économie d'énergie.
Code du pays	Code du pays à deux chiffres. Il est possible que les informations relatives au pays ne soient pas affichées si l'élément d'information (IE, information element) du pays n'est pas présent dans la balise.
Canaux	Une liste des canaux pris en charge (depuis l'IE du pays).
Exigence d'alimentation	La puissance d'alimentation à laquelle la puissance de transmission maximale doit être réduite par rapport à la limite du domaine de réglementation.
Restriction d'alimentation	Puissance de transmission maximale permise sur ce canal en dBm.
Utilisation du canal	Le pourcentage de temps, normalisé à 255, pendant lequel le point d'accès a détecté que le support était occupé, comme indiqué par le mécanisme CS (carrier sense) physique ou virtuel.
Nombre de stations	Le nombre total de stations actuellement associées à ce point d'accès.
Capacité d'admission	Un entier non signé qui précise la durée restante de temps de support est accessible par contrôle d'admission explicite, en unités de 32 microsecondes par seconde. Si sa valeur est 0, le point d'accès ne prend pas en charge cet élément d'information et la capacité est inconnue.
WMM pris en charge	Prise en charge des extensions Wifi Multimedia.

Élément	Description
UAPSD pris en charge	Le point d'accès prend en charge UAPSD (Unscheduled Automatic Power Enregistrer Delivery). Il est possible que cette fonctionnalité ne soit disponible que si WMM est pris en charge. Cette fonctionnalité est essentielle pour le temps de parole et pour atteindre une densité d'appel maximale sur le téléphone IP sans fil.
Proxy ARP	Les points d'accès répondant à la norme CCX prennent en charge la réponse aux requêtes ARP IP au nom de la station associée. Cette fonction est essentielle au temps de veille sur le téléphone IP sans fil.
Version CCX	Si le point d'accès est conforme à la norme CCX, ce champ affiche la version CCX.
Acheminement au mieux	Contient les informations relatives à la file d'attente Acheminement au mieux.
Arrière-plan	Contient les informations relatives à la file d'attente Arrière-plan.
Vidéo	Contient les informations relatives à la file d'attente Vidéo.
Voix	Contient les informations relatives à la file d'attente Voix.

Page web du téléphone IP Cisco

Chaque téléphone IP Cisco possède une page Web sur laquelle figurent diverses informations sur le téléphone, notamment :

- Informations périphérique : affiche les paramètres du périphérique et les informations qui y sont associées pour le téléphone.
- Paramétrage réseau : affiche les informations de configuration du réseau ainsi que des informations sur d'autres paramètres du téléphone.
- Statistiques réseau : affiche des liens hypertexte donnant des informations sur le trafic réseau.
- Journaux des périphériques : affiche des liens hypertexte donnant des informations que vous pouvez utiliser pour le dépannage.
- Statistiques de diffusion en flux continu : affiche des liens hypertexte affichant diverses statistiques de streaming.
- Système : affiche un lien hypertexte pour redémarrer le téléphone.

Cette section décrit les informations qui figurent sur la page web du téléphone. Vous pouvez utiliser ces informations pour surveiller à distance l'utilisation d'un téléphone et pour fournir une assistance lors d'un dépannage.

Ces informations sont également disponibles directement sur le téléphone.

Accéder à la page Web du téléphone

Pour accéder à la page Web d'un téléphone, procédez comme suit :

Remarque Si vous ne parvenez pas à accéder à la page Web, il se peut qu'elle soit désactivée par défaut.

Procédure

Étape 1 Obtenez l'adresse IP du téléphone IP Cisco à l'aide d'une des méthodes suivantes :

a) Recherchez le téléphone dans Cisco Unified Communications Manager Administration, en sélectionnant **Périphérique** > **Téléphone**. Les téléphones qui s'enregistrent auprès de Cisco Unified Communications Manager affichent l'adresse IP dans la fenêtre **Trouver et lister les téléphones** ainsi qu'en haut de la fenêtre **Configuration du téléphone**.

b) Sur le téléphone IP Cisco, appuyez sur **Applications**, choisissez **Paramètres Admin** > **Configuration du réseau** > **Configuration Ethernet** > **Configuration IPv4**, puis faites défiler la page jusqu'au champ Adresse IP.

Étape 2 Ouvrez un navigateur Web et saisissez l'URL suivante, dans laquelle *adresse_IP* est l'adresse IP du téléphone IP Cisco :

`http://`*adresse_IP*

Informations sur le périphérique

La zone Informations périphérique de la page Web d'un téléphone affiche les Paramètres du périphérique et les informations associées pour le téléphone. Le tableau suivant décrit ces éléments.

Remarque Certains éléments du tableau suivant ne s'appliquent pas à tous les modèles de téléphone.

Pour afficher la zone **Informations périphérique**, accédez à la page Web du téléphone comme décrit en Accéder à la page Web du téléphone, à la page 241, puis cliquez sur le lien hypertexte **Informations périphérique**.

Tableau 48 : Éléments de la zone Info. périphérique

Élément	Description
Mode de service	Le mode de service pour le téléphone.
Nom du service	Le domaine du service.
État du service	État actuel du service.
Adresse MAC	Adresse MAC (Media Access Control) du téléphone.
Nom d'hôte	Unique ; nom fixe qui est automatiquement attribué au téléphone en fonction de son adresse MAC.
NR téléphone	Le numéro de répertoire qui est affecté au téléphone.

Élément	Description
ID de chargement app	la version du micrologiciel applicatif qui est en cours d'exécution sur le téléphone.
ID image démarrage	Version du micrologiciel de démarrage.
Version	L'identifiant du micrologiciel qui est en cours d'exécution sur le téléphone.
Module d'extension de touches 1	Identifiant du premier module d'extension de touches, le cas échéant. S'applique aux Téléphones IP Cisco 8851, 8851NR, 8861, 8865, et 8865NR.
Module d'extension de touches 2	Identifiant du second module d'extension de touches, le cas échéant. S'applique aux Téléphones IP Cisco 8851, 8851NR, 8861, 8865, et 8865NR.
Module d'extension de touches 3	Identifiant du troisième module d'extension de touches, le cas échéant. S'applique aux Téléphones IP Cisco 8851, 8851NR, 8861, 8865, et 8865NR.
Version du matériel	Le numéro de révision mineure du matériel du téléphone.
Numéro de série	Le numéro de série unique du téléphone.
Référence	Le numéro de modèle du téléphone.
Message en attente	Indique si un message vocal est en attente sur la ligne principale de ce téléphone.
UDI	Affiche les informations Cisco UDI (Unique Device Identifier) suivantes du téléphone : • Type de périphérique : indique le type de matériel. Par exemple, les écrans de tous les modèles de téléphone. • Description du périphérique : affiche le nom du téléphone associé au type de modèle indiqué. • Identificateur de produit : spécifie le modèle de téléphone. • ID de la version (VID) : indique le numéro de version du matériel principal. • Numéro de série : affiche le numéro de série unique du téléphone.
UDI du module d'extension des touches	Identifiant unique de périphérique (UDI, Unique Device Identifier) Cisco du module d'extension de touches. S'applique aux Téléphones IP Cisco 8851, 8851NR, 8861, 8865, et 8865NR.

Élément	Description
Nom du casque	Affiche le nom du casque Cisco associé dans la colonne de gauche. La colonne de droite contient les informations suivantes : • Port : affiche la manière dont le casque se connecte au téléphone. • USB • AUX • Version : affiche la version du micrologiciel du casque. • Portée Radio : affiche le niveau de résistance configuré pour la radio DECT. Applicable au Casque Cisco série 560 seulement. • Bande passante : affiche si le casque utilise une bande large ou une bande étroite. Applicable au Casque Cisco série 560 seulement. • Bluetooth : affiche si Bluetooth est activé ou désactivé. Applicable au Casque Cisco série 560 seulement. • Conférence : s'affiche si la fonction de conférence est activée ou désactivée. Applicable au Casque Cisco série 560 seulement. • Source du micrologiciel : affiche la méthode de mise à niveau du micrologiciel autorisée : • Restreindre à UCM uniquement • Autoriser à partir d'UCM ou de Cisco Cloud Applicable au Casque Cisco série 560 seulement.
Heure	L'heure du groupe Date/Heure dont le téléphone est membre. Ces informations proviennent de Cisco Unified Communications Manager.
Fuseau horaire	Le fuseau horaire du groupe Date/Heure dont le téléphone est membre. Ces informations proviennent de Cisco Unified Communications Manager.
Date	La date du groupe Date/Heure dont le téléphone est membre. Ces informations proviennent de Cisco Unified Communications Manager.
Mémoire libre du système	Quantité de mémoire inutilisée sur le téléphone
Mémoire libre du Java heap	Quantité de mémoire libre interne du Java heap
Mémoire libre du Java pool	Quantité de mémoire libre interne du pool Java
Mode FIPS activé	Indique si le mode FIPS (Federal Information Processing Standards) est activé.

Configuration réseau

La zone Paramétrage réseau de la page Web d'un téléphone affiche les informations de configuration réseau ainsi que des informations sur d'autres paramètres du téléphone. Le tableau suivant décrit ces éléments.

Vous pouvez afficher et définir beaucoup de ces éléments dans le menu Paramétrage réseau du téléphone IP Cisco.

Remarque Certains éléments du tableau suivant ne s'appliquent pas à tous les modèles de téléphone.

Pour afficher la zone **Paramétrage réseau**, accédez à la page Web du téléphone comme expliqué en Accéder à la page Web du téléphone, à la page 241 , puis cliquez sur le lien hypertexte **Paramétrage réseau**.

Tableau 49 : Éléments de la zone Configuration réseau

Élément	Description
Adresse MAC	Adresse MAC (Media Access Control) du téléphone.
Nom d'hôte	Le nom d'hôte que le serveur DHCP a affecté au téléphone.
Nom du domaine	Le nom du domaine DNS (Domain Name System) dans lequel le téléphone se situe.
Serveur DHCP	L'adresse IP du serveur DHCP (Dynamic Host Configuration Protocol) à partir duquel le obtient l'adresse IP.
Serveur BOOTP	Indique si le téléphone obtient la configuration d'un serveur de protocole Bootstrap (Boo
DHCP	Indique si le téléphone utilise DHCP.
Adresse IP	Adresse de protocole Internet (IPv4) du téléphone.
Masque de sous-réseau	Masque de sous-réseau utilisé par le téléphone.
Routeur par défaut	Routeur par défaut utilisé par le téléphone.
Serveur DNS 1 à 3	Le serveur de noms de domaine (DNS) (Serveur DNS 1) et les serveurs DNS secondaires (Serveurs DNS 2 et 3) utilisés par le téléphone.
TFTP secondaire	Indique si le téléphone utilise un autre serveur TFTP.
Serveur TFTP 1	Le serveur TFTP (Trivial File Transfer Protocol) principal utilisé par le téléphone.
Serveur TFTP 2	Le serveur TFTP (Trivial File Transfer Protocol) secondaire utilisé par le téléphone.
Libération adresse DHCP	Indique le paramètre de l'option Libération d'adresse DHCP dans le menu Configuration téléphone.
ID VLAN opérationnel	Le réseau local virtuel (VLAN) qui est configuré sur un commutateur Catalyst Cisco dont est membre.
ID VLAN admin.	Le VLAN auxiliaire dont le téléphone est membre.

Élément	Description
Serveur CUCM 1 à 5	Noms d'hôte ou adresses IP, classés par ordre de priorité, des serveurs Cisco Unified Communications Manager auprès desquels le téléphone peut s'enregistrer. Un élément peut ég afficher l'adresse IP d'un routeur SRST pouvant fournir des fonctionnalités Cisco Unified Communications Manager limitées, si un tel routeur est disponible. Pour un serveur disponible, un élément affiche l'adresse IP du serveur Cisco Unified Communications Manager ainsi que l'un des états suivants : • Actif : le serveur Cisco Unified Communications Manager depuis lequel le téléphone re actuellement des services de traitement d'appels • En attente : le serveur Cisco Unified Communications Manager vers lequel le téléphone commuté en cas d'indisponibilité du serveur actuel • Vide : aucune connexion en cours à ce serveur Cisco Unified Communications Manager Un élément peut également afficher la désignation SRST (Survivable Remote Site Telephony identifie un routeur SRST capable de fournir des fonctionnalités Cisco Unified Communications limitées. Ce routeur prend le contrôle du traitement des appels si tous les autres serveurs Cisco Communications Manager deviennent inaccessibles. Cisco Unified Communications Manage apparaît toujours à la fin de la liste des serveurs, même s'il est actif. Vous pouvez configurer du routeur SRST dans la section Pool de périphériques de la fenêtre de configuration de Cisco Communications Manager.
URL d'information	URL du texte d'aide qui s'affiche sur le téléphone.
URL des répertoires	URL du serveur à partir duquel le téléphone accède aux informations de répertoire.
URL des messages	URL du serveur à partir duquel le téléphone obtient les services de message.
URL des services	URL du serveur à partir duquel le téléphone accède aux services Téléphone IP Cisco Unified
URL d'inactivité	URL affichée sur le téléphone lorsque ce dernier est inactif pendant la durée spécifiée dans le Durée inactiv. URL, et lorsqu'aucun menu n'est ouvert.
Durée d'inactivité de l'URL	Durée, en secondes, pendant laquelle le téléphone est inactif et pendant laquelle aucun menu ouvert, avant l'activation du service XML spécifié par l'URL d'inactivité.
URL du serveur proxy	URL du serveur proxy, qui envoie des requêtes HTTP à des adresses d'hôte non locaux de la client HTTP du téléphone, et qui fournit les réponses de l'hôte non local au client HTTP du té
URL d'authentification	URL que le téléphone utilise pour valider les requêtes envoyées au serveur Web du téléphone
Paramétrage du port logiciel	Débit et duplex du port de commutation, où : • A = Négociation automatique • 10H = 10-BaseT/semi duplex • 10F = 10-BaseT/duplex intégral • 100H = 100-BaseT/semi duplex • 100F = 100-BaseT/duplex intégral • 1000F = 1000-BaseT/duplex intégral • Aucun lien = Pas de connexion au port de commutation

Élément	Description
Paramétrage port PC	Débit et duplex du port PC, où : • A = Négociation automatique • 10H = 10-BaseT/semi duplex • 10F = 10-BaseT/duplex intégral • 100H = 100-BaseT/semi duplex • 100F = 100-BaseT/duplex intégral • 1000F = 1000-BaseT/duplex intégral • Aucun lien = Pas de connexion au port d'ordinateur
Port PC désactivé	Indique si le port de l'ordinateur sur le téléphone est activé ou non.
Langue utilisateur	Langue associée à l'utilisateur du téléphone. Présente un ensemble d'informations détaillé à la prise en charge des utilisateurs, notamment la langue, la police, le format de date/d'he informations textuelles relatives au clavier alphanumérique.
Langue réseau	Langue réseau associée à l'utilisateur du téléphone. Présente un ensemble d'informations destinées à la prise en charge du téléphone dans un emplacement donné, notamment les dé tonalités et des cadences utilisées par le téléphone.
Version langue utilisateur	Version de la langue utilisateur qui est chargée sur le téléphone.
Version langue réseau	Version de la langue réseau qui est chargée sur le téléphone.
Haut-parleur activé	Indique si le haut-parleur est activé sur le téléphone.
GARP actif	Indique si le téléphone apprend les adresses MAC à partir de réponses Gratuitous ARP.
Renvoi au port PC	Indique si le téléphone renvoie au port d'accès, les paquets émis et reçus sur le port réseau
Fonction vidéo activée	Indique si le téléphone peut participer aux appels vidéo lorsqu'il se connecte à une caméra ac équipée.
VLAN voix actif	Indique si le téléphone autorise un périphérique affecté au port d'ordinateur à accéder au V
VLAN PC activé	VLAN qui identifie et supprime les balises 802.1P/Q des paquets envoyés à l'ordinateur.
Sélection de ligne automatique active	Indique si le téléphone sélectionne automatiquement une ligne lorsque le téléphone est dé
Contrôle de protocole DSCP	Classification IP du DSCP pour la signalisation du contrôle des appels.
DSCP de configuration	Classification IP du DSCP pour n'importe quel transfert de configuration du téléphone.
DSCP de services	Classification IP du DSCP pour les services basés sur le téléphone.
Mode de sécurité (non sécurisé)	Mode de sécurité qui est défini pour le téléphone.
Accès Web activé	Indique si l'accès à Internet est activé (Oui) ou désactivé (Non) pour le téléphone.
Accès SSH actif	Indique si le port SSH a été activé ou désactivé.

Élément	Description
CDP : port de commutation	Indique si CDP est pris en charge sur le port de commutation (activé par défaut). Activez CDP sur le port de commutation pour l'affectation de VLAN pour le téléphone, la g l'énergie, la gestion de la qualité de service (QoS) et la sécurité 802.1x. Activez CDP sur le port de commutation lorsque le téléphone se connecte à un port de comm Lorsque CDP est désactivé dans Cisco Unified Communications Manager, un avertissement pour indiquer que CDP ne doit être désactivé sur le port de commutateur que si le téléphone se à un commutateur tiers. Les valeurs actuelles des ports PC et de commutateur sont affichées dans le menu Paramètres
CDP : port PC	Indique si CDP est pris en charge sur le port d'ordinateur (activé par défaut). Lorsque CDP est désactivé dans Cisco Unified Communications Manager, un avertissement pour indiquer que désactiver CDP sur le port PC empêche le fonctionnement de CVTA. Les valeurs actuelles de CDP pour les ports PC et de commutation figurent dans le menu Par
LLDP-MED : Port switch	Indique si LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery) est activ port de commutation.
LLDP-MED : Port PC	Indique si LLDP-MED est activé sur le port PC.
Hiérarchisation énergie LLDP	Priorité énergétique du téléphone au commutateur, permettant ainsi au commutateur de fourn alimentation appropriée aux téléphones. Les paramètres sont les suivants : • Inconnu : Il s'agit de la valeur par défaut. • Faible • Élevé • Critique
ID de ressource LLDP	Identifiant de ressource qui est affecté au téléphone pour la gestion de l'inventaire.
Fichier CTL	Code de hachage MD5 du fichier CTL.
Fichier ITL	Le fichier ITL contient la liste de confiance initiale.
Signature ITL	Code de hachage MD5 du fichier ITL
Serveur CAPF	Serveur CPF en cours d'utilisation
TVS	Le composant principal de la sécurité par défaut. Grâce aux services de vérification de la list confiance TVS (Trust Verification Services), les téléphones IP Cisco Unified peuvent authen serveurs d'applications, notamment les services de mobilité des numéros de poste, le réperto MIDlet, pendant l'établissement de la connexion HTTPS.
Serveur TFTP	Le nom du serveur TFTP utilisé par le téléphone.
Serveur TFTP	Le nom du serveur TFTP utilisé par le téléphone.
Synchronisation automatique des ports	Indique si le téléphone synchronise automatiquement la vitesse du port pour supprimer la pe paquets.

Élément	Description
Configuration à distance du port de commutation	Indique si le port switch est contrôlé à distance.
Configuration à distance du port PC	Indique si le port PC est contrôlé à distance.
Mode d'adressage IP	Identifie le mode d'adressage : • IPv4 uniquement • IPv4 et IPv6 • IPv6 uniquement
Commande du mode de préférence IP	Indique la version de l'adresse IP utilisée par le téléphone pendant la signalisation avec C Communications Manager lorsque IPv4 et IPv6 sont tous deux disponibles sur le téléphor
Mode de Préférences IP pour média	
Configuration IPv6 automatique	Indique que pour le multimédia, le périphérique utilise une adresse IPv4 pour se connecte Unified Communications Manager.
Protection contre les adresses en double IPv6	
Accepter les messages de redirection IPv6	Indique si le téléphone accepte les messages de redirection du routeur utilisé pour le num destination.
Demande d'écho de multidiffusion de réponse IPv6	Indique que le téléphone envoie un message de réponse à l'écho en réponse à un message d'écho envoyé à une adresse IPv6-uniquement.
Serveur de chargement IPv6	Utilisé pour optimiser la durée d'installation des mises à niveau de microprogramme sur et pour alléger la charge du WAN en stockant des images localement, éliminant ainsi la n traverser la liaison WAN à chaque mise à niveau du téléphone.
Serveur de journaux IPv6	
Serveur CAPF IPv6	Indique l'adresse IP et le port de l'ordinateur de journalisation distant auquel le téléphone messages de journalisation.
DHCPv6	Indique la méthode utilisée par le téléphone pour obtenir l'adresse IPv6 uniquement. Lorsque DCHPv6 est activé, le téléphone obtient l'adresse IPv6 via le serveur DHCPv6 ou par RA envoyé par le routeur compatible IPv6. Si DHCPv6 est désactivé, le téléphone n'a adresse IPv6 avec état (via le serveur DHCPv6) ou sans état (via SLAAC). **Remarque** Contrairement à DHCPv4, même si DHCPv6 est désactivé, le téléphone peut générer une adresse SLAAC si la configuration automatique est activée.

Élément	Description
Adresse IPv6	Affiche l'adresse IPv6-uniquement actuelle du téléphone. Deux formats d'adresse sont pris en charge : • Huit groupes de quatre chiffres hexadécimaux séparés par des deux-points X:X:X:X:X: • Format compressé pour réduire une chaîne de groupes de zéros consécutifs en un group représenté par un deux-points double.
Long. préfix IPv6	Affiche la longueur du préfixe IPv6-uniquement actuelle du sous-réseau.
Routeur IPv6 par défaut	Affiche le routeur IPv6 par défaut utilisé par le téléphone.
Serveur DNS IPv6 1 à 2	Affiche le serveur DNSv6 principal et secondaire utilisé par le téléphone
Autre TFTP IPv6	Indique si un serveur TFTP IPv6 alternatif est utilisé.
Serveur TFTP IPv6 1 à 2	Affiche le serveur TFTP IPv6 principal et secondaire utilisé par le téléphone.
Adresse IPv6 libérée	S'affiche si l'utilisateur a publié les informations relatives à IPv6.
Niveau d'énergie EnergyWise	Le niveau de puissance qui est utilisé lorsque le téléphone est en mode veille.
Domaine EnergyWise	Le domaine EnergyWise qui héberge le téléphone.
DF_BIT	Indique la définition de bits DF des paquets.

Statistiques réseau

Les liens hypertexte de Statistiques réseau sur une page Web de téléphone indiquent des informations sur le trafic réseau sur votre téléphone :

- Informations Ethernet : affiche des informations sur le trafic Ethernet.
- Accès : affiche des informations sur le trafic réseau échangé avec le port PC du téléphone.
- Réseau : affiche des informations sur le trafic réseau échangé avec le port réseau du téléphone.

Pour afficher une zone Statistiques réseau, accédez à la page Web du téléphone, puis cliquez sur le lien hypertexte **Informations Ethernet**, **Accès** ou **Réseau**.

Page Web Informations Ethernet

Le tableau suivant décrit le contenu de la page Web Informations Ethernet.

Tableau 50 : Éléments d'informations Ethernet

Élément	Description
Tx Frames (Trames émises)	Le nombre total de trames émises par le téléphone.
Tx broadcast	Le nombre total de trames de diffusion émises par le téléphone.

Élément	Description
Tx multicast	Le nombre total de trames multidiffusion émises par le téléphone.
Transmission individuelle	Le nombre total de paquets à transmission individuelle émis par le téléphone.
Rx Frames (Trames reçues)	Le nombre total de trames reçues par le téléphone
Rx broadcast	Le nombre total de trames de diffusion reçues par le téléphone.
Rx multicast	Le nombre total de trames multidiffusion reçues par le téléphone.
Rx unicast	Le nombre total de trames à diffusion individuelle reçues par le téléphone.
Rx PacketNoDes	Le nombre total de paquets abandonnés à cause du descripteur non DMA (Accès direct à la mémoire).

Pages Web d'accès et de réseau

Le tableau suivant décrit les informations contenues dans les pages Web d'accès et de réseau.

Tableau 51 : Champs d'accès et de réseau

Élément	Description
TotalPkt Rx	Le nombre total de paquets reçus par le téléphone.
Rx crcErr	Le nombre total de paquets reçus avec des échecs CRC.
Rx alignErr	Le nombre total de paquets reçus, d'une longueur de 64 à 1 522 octets, et contenant une séquence de trame incorrecte (FCS).
Rx multicast	Le nombre total de paquets multidiffusion reçus par le téléphone.
Rx broadcast	Le nombre total de paquets de diffusion reçus par le téléphone.
Rx unicast	Le nombre total de paquets à diffusion individuelle reçus par le téléphone.
Rx shortErr	Le nombre total de paquets d'erreurs FCS ou de paquets d'erreur d'alignement reçus, d'une taille inférieure à 64 octets.
Rx shortGood	Le nombre total de bons paquets reçus, d'une taille inférieure à 64 octets.
Rx longGood	Le nombre total de bons paquets reçus, d'une taille supérieure à 1 522 octets.
Rx longErr	Le nombre total de paquets d'erreurs FCS ou de paquets d'erreur d'alignement reçus, d'une taille supérieure à 1 522 octets.
Rx size64	Le nombre total de paquets reçus, y-compris les paquets incorrects, d'une taille comprise entre 0 et 64 octets.

Élément	Description
Rx size65to127	Le nombre total de paquets reçus, y-compris les paquets incorrects, d'une taille comprise entre 65 et 127 octets.
Rx size128to255	Le nombre total de paquets reçus, y-compris les paquets incorrects, d'une taille comprise entre 128 et 255 octets.
Rx size256to511	Le nombre total de paquets reçus, y-compris les paquets incorrects, d'une taille comprise entre 256 et 511 octets.
Rx size512to1023	Le nombre total de paquets reçus, y-compris les paquets incorrects, d'une taille comprise entre 512 et 1023 octets.
Rx size1024to1518	Le nombre total de paquets reçus, y-compris les paquets incorrects, d'une taille comprise entre 1024 et 1518 octets.
Rx tokenDrop	Le nombre total de paquets abandonnés pour cause de ressources insuffisantes (par exemple, débordement FIFO).
Tx excessDefer	Le nombre total de paquets dont la transmission a été différée pour cause de support occupé.
Tx lateCollision	Le nombre de fois qu'une collision a eu lieu, supérieur à 512 bits fois après le début de la transmission de paquets.
Tx totalGoodPkt	Le nombre total de bons paquets (multidiffusion, de diffusion et à diffusion individuelle) reçus par le téléphone.
Tx Collisions	Le nombre total de collisions ayant eu lieu lors de la transmission d'un paquet.
Tx excessLength	Le nombre total de paquets qui n'ont pas été transmis car 16 tentatives de transmission on été effectuées.
Tx broadcast	Le nombre total de paquets de diffusion transmis par le téléphone.
Tx multicast	Le nombre total de paquets multidiffusion transmis par le téléphone.
LLDP FramesOutTotal	Le nombre total de trames LLDP envoyées par le téléphone.
LLDP AgeoutsTotal	Le nombre total de trames LLDP qui ont dépassé le délai d'attente maximal dans le cache.
LLDP FramesDiscardedTotal	Le nombre total de trames LLDP qui ont été abandonnées parce qu'un des TLV obligatoires était absent, défectueux, ou contenait une longueur de chaîne hors plage.
LLDP FramesInErrorsTotal	Le nombre total de trames LLDP reçues avec une ou plusieurs erreurs détectables.
LLDP FramesInTotal	Le nombre total de trames LLDP reçues par le téléphone.
LLDP TLVDiscardedTotal	Le nombre total de TLV LLDP abandonnés.

Élément	Description
LLDP TLVUnrecognizedTotal	Le nombre total de TLV LLDP non reconnus sur le téléphone.
CDP ID périphérique du voisin	L'identifiant d'un périphérique branché dans ce port et détecté par CDP.
Adresse IPv6 voisine CDP	Adresse IP du périphérique voisin détecté par le protocole CDP.
CDP Port du voisin	Port du périphérique voisin dans lequel le téléphone est branché, détectée par le protocole CDP.
LLDP ID du périphérique voisin	Identifiant d'un périphérique connecté à ce port et détecté par LLDP.
Adresse IPv6 voisine LLDP	Adresse IP du périphérique voisin détecté par le protocole LLDP.
LLDP Port du voisin	Port du périphérique voisin dans lequel le téléphone est branché, détectée par le protocole LLDP.
Informations port	Informations sur le débit et sur le mode duplex.

Journaux des périphériques

Les liens hypertexte du journal de périphérique suivants sur une page Web de téléphone fournissent des informations permettant de surveiller et de dépanner le téléphone.

- Journaux de la console : inclut des liens hypertexte vers des fichiers journaux individuels. Les fichiers journaux de la console incluent les messages d'erreur et de débogage reçus sur le téléphone.
- Vidages mémoire : inclut des liens hypertexte vers des fichiers d'image mémoire individuels. Les fichiers de vidage mémoire contiennent les données relatives aux pannes du téléphone.
- Messages d'état : affiche les 10 derniers messages d'état générés par le téléphone depuis qu'il s'est allumé depuis la dernière fois. Ces informations sont également affichées sur l'écran Messages d'état du téléphone.
- Affichage du débogage : affiche des messages du débogage qui pourraient être utiles à TAC Cisco si vous avez besoin d'assistance pour le dépannage.

Statistiques de diffusion en flux continu

Un téléphone IP Cisco Unified peut diffuser un flux d'informations simultanément depuis ou vers un maximum de trois périphériques. Un téléphone transmet des informations en continu lors d'un appel, ou lorsqu'il utilise un service qui envoie ou reçoit de l'audio ou des données.

Les zones Statistiques de diffusion en flux continu de la page Web du téléphone présentent des informations sur les flux.

Le tableau suivant présente les éléments des zones Statistiques de diffusion en flux continu.

Tableau 52 : Éléments des zones Statistiques de diffusion en flux continu

Élément	Description
Adresse distante	L'adresse IP et le port UDP de la destination du flux.
Adresse locale	L'adresse IP et le port UPD du téléphone.

Élément	Description
Heure de début	L'horodatage interne indiquant l'heure à laquelle Cisco Unified Communications Mana demandé que le téléphone commence à émettre des paquets.
État du flux	Indique si la transmission en continu est active ou non.
Nom d'hôte	Unique ; nom fixe qui est automatiquement attribué au téléphone en fonction de son ad MAC.
Paquets de l'appelant	Le nombre total de paquets de données RTP émis par le téléphone depuis le début de c connexion. La valeur est 0 si la connexion est définie par le mode réception seulement.
Octets de l'appelant	Le nombre total d'octets de charge utile émis par le téléphone dans des paquets de don RTP depuis le début de cette connexion. La valeur est 0 si la connexion est définie par l réception seulement.
Codec de l'appelant	Le type de codage audio défini pour le flux émis.
Rapports de l'appelant envoyés (voir remarque)	Le nombre de fois où un rapport d'appelant RTCP a été envoyé.
Heure d'envoi du rapport de l'appelant (voir remarque)	L'horodatage Interne indiquant l'heure d'envoi du dernier rapport d'appelant RTCP.
Paquets perdus Rcvr	Le nombre total de paquets de données RTP perdus par le téléphone depuis le début de réception de données sur cette connexion. Correspond au nombre de paquets attendus m nombre de paquets réellement reçus, le nombre de paquets reçus incluant tous les paqu différés ou en double. La valeur est 0 si la connexion est définie par le mode envoi seul
Gigue moyenne	Une estimation de la déviation moyenne du temps d'interarrivée des paquets de donnée en millisecondes. La valeur est 0 si la connexion est définie par le mode envoi seuleme
Codec appelé	Le type de codage audio défini pour le flux reçu.
Rapports de l'appelé envoyés (voir remarque)	Le nombre de fois où un rapport d'appelé RTCP a été envoyé.
Heure d'envoi du rapport de l'appelé (voir remarque)	L'horodatage Interne indiquant l'heure d'envoi d'un rapport d'appelé RTCP.
Paquets Rcvr	Le nombre total de paquets de données RTP reçus par le téléphone depuis le début de la ré de données sur cette connexion. Inclut les paquets reçus de différentes sources s'il s'agi appel multidiffusion. La valeur est 0 si la connexion est définie par le mode envoi seule
Octets Rcvr	Le nombre total d'octets de charge utile reçus par le téléphone dans des paquets de don RTP depuis le début de la réception sur cette connexion. Inclut les paquets reçus de diff sources s'il s'agit d'un appel multidiffusion. La valeur est 0 si la connexion est définie mode envoi seulement.

Élément	Description
Facteur k de qualité d'écoute MOS	Cette note est une estimation objective de la note d'opinion moyenne (MOS) pour la d'écoute (LQK), qui varie entre 5 (excellente) et 1 (mauvaise). Cette note est détern fonction des événements de dissimulation audibles dus à la perte de trames dans l'int 8 dernières secondes du flux de voix. Pour obtenir plus d'informations, reportez-vou Surveillance de la qualité vocale, à la page 284. **Remarque** La note de qualité d'écoute MOS LQK peut varier en fonction du type utilisé par le Téléphone IP Cisco Unified.
Facteur k moyen de qualité d'écoute MOS	La note de qualité d'écoute MOS LQK moyenne observée sur toute la durée du flux
Facteur k minimal de qualité d'écoute MOS	La note de qualité d'écoute MOS LQK la plus basse observée depuis le début du flu
Facteur k maximal de qualité d'écoute MOS	Valeur de référence ou note de qualité d'écoute MOS LQK la plus élevée observée début du flux de voix. Ces codecs assurent les notes de qualité d'écoute MOS LQK maximales suivantes d conditions normales, sans perte de trames : • Le G.711 obtient une note de 4,5. • Le G.729 A /AB obtient une note de 3,7.
Version note de qual. d'écoute	La version de l'algorithme propriétaire Cisco utilisé pour le calcul des notes MOS L
Taux de masquage cumulé	Le nombre total de trames de masquage divisé par le nombre total de trames de con reçues depuis le début du flux de voix.
Taux de masquage par intervalle	Le nombre de trames de masquage divisé par le nombre de trames de voix incluses précédent intervalle de 3 secondes de conversation active. Si la détection d'activité voc est utilisée, un intervalle plus long peut être nécessaire pour accumuler 3 secondes conversation active.
Taux de masquage maximal	Le temps de masquage le plus élevé depuis le début du flux de voix.
Durée en sec. masquées	Durée, en secondes, des événements de masquage (trames perdues) depuis le début voix (inclut les secondes masquées de haut niveau).
Nombre de secondes de masquage important	La durée, en secondes, pendant laquelle plus de 5 pour cent des événements de masqua perdues) se sont produits depuis le début du flux de voix.
Latence (voir remarque)	Estimation de la latence du réseau, exprimée en millisecondes. Cette valeur représe moyenne mobile du retard aller-retour, mesurée à la réception des blocs de rapport du RTCP.
Gigue maximale	La valeur maximale de la gigue instantanée, en millisecondes.
Taille de l'appelant	La taille des paquets RTP, en millisecondes, pour le flux émis.
Rapports de l'appelant reçus (voir remarque)	Le nombre de fois où un rapport d'appelant RTCP a été reçu.

Élément	Description
Heure de réception du rapport de l'appelant (voir remarque)	La plus récente heure à laquelle un rapport d'appelant RTCP a été reçu.
Taille appelé	La taille des paquets RTP, en millisecondes, pour le flux reçu.
Refusé par l'appelé	Les paquets RTP qui ont été reçus du réseau, puis supprimés des tampons de gigue.
Rapports de l'appelé reçus (voir remarque)	Le nombre de fois où un rapport d'appelé RTCP a été reçu.
Heure de réception du rapport de l'appelé (voir remarque)	Heure de réception du dernier rapport de l'appelé en date.
Rcvr codé	Indique si le destinataire utilise le chiffrement.
Appelant codé	Indique si l'expéditeur utilise le chiffrement.
Trames de l'expéditeur	Nombre de trames émises.
Trames partielles de l'expéditeur	Nombre de trames partielles émises.
Trames I de l'expéditeur	Nombre de trames I émises. Les trames I sont utilisées pour la transmission vidéo.
Trames I de l'appelant	Nombre de trames d'actualisation de décodeur instantané (IDR) émises. Les trames IDI utilisées pour la transmission vidéo.
Débit de trames de l'expéditeur	Vitesse à laquelle l'expéditeur envoie les trames.
Bande passante de l'appelant	Bande passante dont dispose l'appelant.
Résolution de l'appelant	Résolution vidéo de l'expéditeur.
Trames Rcvr	Nombre de trames reçues.
Trames partielles de l'appelé	Nombre de trames partielles reçues.
Trames I de l'appelé	Nombre de trames I reçues.
Trames I de l'appelé	Nombre de trames IDR reçues.
Demande Trames I Rcvr	Nombre de trames IDR demandées reçues.
Débit de trames Rcvr	Vitesse à laquelle l'appelé reçoit les trames.
Trames perdues par l'appelé	Nombre de trames non reçues.
Erreurs de trame de l'appelé	Nombre de trames non reçues.
Largeur de bande Rcvr	La bande passante de l'appelé.

Élément	Description
Résolution Rcvr	Résolution vidéo de l'appelé.
Domain	Domaine où réside le téléphone.
Entrée de l'appelant	Nombre de fois où l'appelant est entré.
Entrée de l'appelé	Nombre de fois où l'appelé est entré.
Byes	Nombre de trames « Bye (Au revoir) »
Heure de début de l'appelant	Heure de début de l'appelant.
Heure de début de l'appelé	Heure de début de l'appelé.
État de la ligne	Indique si le téléphone est en cours de diffusion d'un flux
Outil de l'appelant	Type de codage audio défini pour le flux
Rapports de l'appelant	Rapports de l'appelant RTCP
Heure du rapport de l'appelant	Dernière heure à laquelle un rapport d'appelant RTCP a été envoyé.
Gigue de l'appelé	Gigue maximale du flux
Outil de l'appelé	Type de codage audio défini pour le flux
Rapports de l'appelé	Nombre de fois auxquelles on a accédé à ce rapport statistiques de flux à partir de la
Heure du rapport de l'appelé	Horodatage interne indiquant quand ce rapport statistiques de flux a été créé
Est vidéo	Indique si l'appel était un appel vidéo ou audio seulement.
ID de l'appel	Identification de l'appel téléphonique
ID du groupe	Identification du groupe auquel appartient le téléphone.

Remarque Lorsque le protocole de contrôle RTP est désactivé, aucune donnée n'est générée pour ce champ : il affiche donc 0.

Demander des informations à partir du téléphone dans XML

Pour des raisons de dépannage, vous pouvez envoyer la requête d'informations depuis le téléphone. L'information vous sera transmise au format XML. Les informations suivantes sont disponibles :

- CallInfo contient les informations de session d'appel pour une ligne particulière.
- LineInfo contient les informations de configuration de ligne pour le téléphone.
- ModeInfo contient les informations sur le mode du téléphone.

Avant de commencer

L'accès Web doit être activé pour récupérer les informations.

Le téléphone doit être associé à un utilisateur.

Procédure

Étape 1 Pour obtenir des informations sur les appels, saisissez l'URL suivante dans un navigateur : **http://<phone ip address>/CGI/Java/CallInfo<x>**

où

- <*phone ip address*> est l'adresse IP du téléphone
- <*x*> est le numéro de la ligne sur laquelle obtenir des informations.

Cette commande renvoie un document XML.

Étape 2 Pour obtenir des informations sur la ligne, saisissez l'URL suivante dans un navigateur : **http://<phone ip address>/CGI/Java/LineInfo**

où

- <*phone ip address*> est l'adresse IP du téléphone

Cette commande renvoie un document XML.

Étape 3 Pour obtenir des informations sur le modèle, saisissez l'URL suivante dans un navigateur : **http://<phone ip address>/CGI/Java/ModeInfo**

où

- <*phone ip address*> est l'adresse IP du téléphone

Cette commande renvoie un document XML.

Exemple de résultat CallInfo

Le code XML suivant est un exemple de résultat de la commande 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>
```

Exemple de résultat LineInfo

Le code XML suivant est un exemple de résultat de la commande 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>
```

Exemple de résultat ModeInfo

Le code XML suivant est un exemple de résultat de la commande 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>
```

CHAPITRE 12

Dépannage

Informations générales concernant la résolution de problèmes

Le tableau suivant présente des informations générales sur la résolution des éventuels problèmes rencontrés sur le téléphone IP Cisco.

Tableau 53 : Dépannage du téléphone IP Cisco

Résumé	Explication
Raccordement d'un téléphone IP Cisco à un autre téléphone IP Cisco	Cisco ne prend pas en charge le raccordement de deux téléphones IP au port PC. Chaque téléphone IP doit être directement branché dans un po commutation. Si les téléphones sont raccordés sur une ligne au moyen ils ne fonctionneront pas.
En cas d'avalanche de messages de diffusion prolongée, les téléphones IP sont réinitialisés, ou incapables de passer ou de recevoir des appels	En cas d'avalanche de messages de diffusion de couche 2 prolongée (dur minutes) sur le VLAN voix, les téléphones IP pourront être réinitialisés appel actif, ou être incapables de passer ou de recevoir des appels. Les risquent de ne pas être réactivés avant la fin de l'avalanche de messages

Résumé	Explication
Déplacement d'une connexion réseau du téléphone à un poste de travail	Si vous allumez votre téléphone au moyen de la connexion réseau, soyez p vous décidez de débrancher la connexion réseau du téléphone et de raccorde à un ordinateur de bureau. **Avertissement** La carte réseau de l'ordinateur ne peut pas recevoir de courant a de la connexion réseau ; elle risquerait d'être détruite si du co passait par la connexion. Pour protéger la carte réseau, attende minimum 10 secondes après avoir débranché le câble du télép avant de le raccorder à l'ordinateur. Ce délai est suffisant pour commutateur détecte l'absence du téléphone sur la ligne, et po cesse d'alimenter le câble.
Changement de la configuration du téléphone	Par défaut, les options de configuration réseau sont verrouillées pour empê utilisateurs d'effectuer des modifications pouvant influer sur leur connectivi Vous devez déverrouiller les options de configuration réseau pour pouvoir configurer. Pour obtenir plus d'informations, reportez-vous à Appliquer un passe à un téléphone, à la page 52. **Remarque** Si le mot de passe administrateur n'est pas défini dans le profi téléphone commun, l'utilisateur peut modifier les paramètres
Discordance de codecs entre le téléphone et un autre périphérique	Les statistiques RxType (Type pour la réception) et TxType (Type pour l'é indiquent le codec utilisé lors d'une conversation entre le téléphone IP Cisc autre périphérique. Les valeurs de ces statistiques doivent concorder. Sinon que l'autre périphérique peut traiter la conversation des codecs, ou qu'un tra est installé pour traiter le service.
Discordance d'échantillons sonores entre le téléphone et un autre périphérique	Les statistiques RxType (Type pour la réception) et TxType (Type pour l'é indiquent la taille des paquets de voix utilisés lors d'une conversation entre le IP Cisco et un autre périphérique. Les valeurs de ces statistiques doivent c
Situation de bouclage	Une situation de bouclage peut se produire dans les conditions suivantes : • L'option de configuration du port de commutation dans le menu Conf réseau du téléphone est réglée sur 10 Half (10-BaseT/semi duplex). • Le téléphone doit être alimenté par un bloc d'alimentation externe. • Le téléphone doit être éteint (bloc d'alimentation débranché). Dans ce cas, le port de commutation du téléphone peut être désactivé et le suivant est affiché dans le journal de la console du commutateur : HALF_DUX_COLLISION_EXCEED_THRESHOLD Pour résoudre ce problème, réactivez le port à partir du commutateur.

Problèmes liés au démarrage

Une fois que vous avez installé un téléphone sur votre réseau et que vous l'avez ajouté dans Cisco Unified Communications Manager, le téléphone devrait démarrer comme décrit à la rubrique connexe ci-après.

Si le téléphone ne démarre pas correctement, reportez-vous aux sections suivantes pour savoir comment résoudre le problème.

Rubriques connexes

Vérification du démarrage du téléphone, à la page 68

Le téléphone IP Cisco ne suit pas le processus de démarrage normal

Problème

Lorsque vous connectez un téléphone IP Cisco au port réseau, le téléphone ne suit pas le processus de démarrage normal décrit à la rubrique connexe et l'écran du téléphone n'affiche pas d'informations.

Cause

Le fait que le téléphone ne suive pas le processus de démarrage peut être dû à des câbles défectueux, à de mauvais branchements, à des pannes réseau, à des pannes électriques ou à un dysfonctionnement du téléphone.

Solution

Pour savoir si le téléphone est fonctionnel, utilisez les suggestions suivantes pour éliminer d'autres problèmes potentiels.

- Vérifiez que le port réseau est fonctionnel :
  - Remplacez les câbles Ethernet par des câbles dont le bon fonctionnement est connu.
  - Débranchez un téléphone IP Cisco qui fonctionne d'un autre port et branchez-le dans ce port réseau pour vérifier que le port est actif.
  - Branchez le téléphone IP Cisco qui ne démarre pas dans un autre port réseau qui fonctionne.
  - Branchez le téléphone IP Cisco qui ne démarre pas directement dans le port du commutation, éliminant ainsi le branchement au panneau de câblage du bureau.
- Vérifiez que le téléphone est alimenté :
  - Si vous utilisez un bloc d'alimentation externe, vérifiez que la prise électrique fonctionne.
  - Si vous utilisez l'alimentation en ligne, utilisez plutôt un bloc d'alimentation externe.
  - Si vous utilisez un bloc d'alimentation externe, remplacez le téléphone par un appareil qui fonctionne.
- Si le téléphone ne démarre toujours pas normalement, mettez le téléphone sous tension à partir de l' l'image du logiciel de sauvegarde.
- Si le téléphone ne démarre toujours pas normalement, réinitialisez le téléphone aux valeurs d'usine.
- Si l'écran du téléphone IP Cisco n'affiche aucun caractère pendant au moins cinq minutes après que vous ayez appliqué ces solutions, contactez un agent de l'assistance technique Cisco pour obtenir de l'aide.

Rubriques connexes

Vérification du démarrage du téléphone, à la page 68

Le téléphone IP Cisco ne s'enregistre pas auprès de Cisco Unified Communications Manager

Si le téléphone exécute la première étape du processus de démarrage (les boutons LED clignotent) mais continue à afficher en boucle les messages qui apparaissent à l'écran du téléphone, le téléphone ne démarre pas normalement. Le téléphone ne peut pas démarrer comme il faut tant qu'il ne se connecte pas au réseau Ethernet et qu'il s'inscrive auprès d'un serveur Cisco Unified Communications Manager.

En outre, des problèmes relatifs à la sécurité risquent d'empêcher le téléphone de démarrer normalement. Pour plus d'informations, reportez-vous à la section Procédures de dépannage, à la page 273.

Affichage de messages d'erreur par le téléphone

Problème

Des messages d'état indiquent des erreurs lors du démarrage.

Solution

Lorsque le téléphone passe par le processus de démarrage, vous pouvez accéder à des messages d'état qui vous donnent des informations sur l'origine d'un problème.

Rubriques connexes

Afficher la fenêtre Messages d'état, à la page 227

Le téléphone ne parvient pas à se connecter au serveur TFTP ou à Cisco Unified Communications Manager

Problème

Si une panne survient sur le réseau entre le téléphone et le serveur TFTP ou Cisco Unified Communications Manager, le téléphone ne peut pas démarrer correctement.

Solution

Vérifiez que le réseau est actif.

Le téléphone ne parvient pas à se connecter au serveur TFTP

Problème

Les paramètres du serveur TFTP sont peut-être incorrects.

Solution

Vérifiez l'exactitude des paramètres TFTP.

Rubriques connexes

Vérifier les paramètres TFTP, à la page 274

Le téléphone ne parvient pas à se connecter au serveur

Problème

Les champs relatifs à l'adressage IP et au routage ne sont peut-être pas correctement configurés.

Solution

Vérifiez les paramètres d'adressage IP et de routage du téléphone. Si vous utilisez DHCP, ces valeurs doivent être disponibles sur le serveur DHCP. Si vous avez affecté une adresse IP statique au téléphone, vous devez saisir ces valeurs manuellement.

Le téléphone ne parvient pas à se connecter à l'aide de DNS

Problème

Les paramètres DNS sont peut-être incorrects.

Solution

Si vous utilisez DNS pour accéder au serveur TFTP ou à Cisco Unified Communications Manager, vous devez spécifier un serveur DNS.

Les services Cisco Unified Communications Manager et TFTP ne s'exécutent pas

Problème

Si les services Cisco Unified Communications Manager ou TFTP ne s'exécutent pas, les téléphones risquent de ne pas démarrer correctement. Dans ce cas, il est probable qu'une panne affecte tout le système, et que les autres téléphones et périphériques ne puissent pas démarrer normalement.

Solution

Si le service Cisco Unified Communications Manager ne s'exécute pas, tous les périphériques du réseau qui dépendent de lui pour passer des appels téléphoniques sont affectés. Si le service TFTP ne s'exécute pas, de nombreux périphériques ne peuvent pas démarrer normalement. Pour obtenir plus d'informations, reportez-vous à Démarrage d'un service, à la page 277.

Endommagement du fichier de configuration

Problème

Si un téléphone donné présente des problèmes que vous ne parvenez pas à résoudre à l'aide des suggestions données dans ce chapitre, le fichier de configuration est peut-être endommagé.

Solution

Créez un nouveau fichier de configuration de téléphone.

Enregistrement d'un téléphone Cisco Unified Communications Manager

Problème

Le téléphone n'est pas enregistré auprès de Cisco Unified Communications Manager

Solution

Un téléphone IP Cisco ne peut s'enregistrer auprès d'un serveur Cisco Unified Communications Manager que si le téléphone est ajouté sur le serveur, ou si l'enregistrement automatique est activé. Lisez les informations et les procédures de la section Méthodes disponibles pour ajouter des téléphones, à la page 75 pour vérifier que le téléphone a été ajouté à la base de données Cisco Unified Communications Manager.

Pour vérifier que le téléphone figure dans la base de données Cisco Unified Communications Manager, sélectionnez **Périphérique** > **Téléphone** dans Cisco Unified Communications Manager Administration. Cliquez sur **Find** (Rechercher) pour rechercher le téléphone d'après son adresse MAC. Pour obtenir des informations sur la détermination d'une adresse MAC, reportez-vous à Détermination de l'adresse MAC du téléphone, à la page 74.

Si le téléphone figure déjà dans la base de données Cisco Unified Communications Manager, le fichier de configuration est peut-être endommagé. Reportez-vous à Endommagement du fichier de configuration, à la page 265 pour obtenir de l'aide.

Le téléphone IP Cisco ne parvient pas à obtenir une adresse IP

Problème

Si un téléphone ne parvient pas à obtenir une adresse IP lors de son démarrage, il se peut que le téléphone ne soit pas sur le même réseau ou sur le même VLAN que le serveur DHCP, ou que le port de commutation auquel le téléphone se connecte soit désactivé.

Solution

Vérifiez que le réseau ou le VLAN auquel le téléphone se connecte a accès au serveur DHCP, et que le port de commutation est activé.

Téléphone non en cours d'enregistrement

Problème

L'écran du téléphone affiche l'invite « Saisir le code d'activation ou le domaine de service. »

Solution

Le téléphone n'a pas d'adresse TFTP. Vérifiez que l'option 150 est fournie par le serveur DHCP ou qu'un TFTP alternatif est configuré manuellement.

Problèmes liés à la réinitialisation du téléphone

Si des utilisateurs signalent que leurs téléphones se réinitialisent pendant les appels ou pendant que leurs téléphones sont inactifs, vous devez rechercher la cause du problème. Si la connexion réseau et la connexion à Cisco Unified Communications Manager sont stables, le téléphone ne devrait pas être réinitialisé.

En général, un téléphone est réinitialisé en cas de problèmes de connexion au réseau ou à Cisco Unified Communications Manager.

Le téléphone est réinitialisé suite à des pannes réseau intermittentes

Problème

Des pannes intermittentes peuvent se produire sur votre réseau.

Solution

Des pannes réseau intermittentes affectent le trafic voix et de données de manière différente. Il se peut que des pannes intermittentes surviennent sur votre réseau sans que celui-ci ne les détecte. Si tel le cas, le trafic de données peut renvoyer des paquets perdus et vérifier que les paquets sont reçus et émis. Toutefois, le trafic voix ne peut pas procéder à une nouvelle capture des paquets perdus. Plutôt que de rétablir une connexion réseau interrompue, le téléphone se réinitialise et tente de se reconnecter au réseau. Contactez l'administrateur système pour obtenir des informations sur les problèmes connus sur le réseau vocal.

Le téléphone est réinitialisé suite à des erreurs de paramétrage DHCP

Problème

Les paramètres DHCP sont peut-être incorrects.

Solution

Vérifiez que vous avez correctement configuré le téléphone pour utiliser DHCP. Vérifiez que le serveur DHCP est correctement configuré. Vérifiez la durée du bail DHCP. Il est recommandé de définir la durée du bail à 8 jours.

Le téléphone est réinitialisé à cause d'une adresse IP statique incorrecte

Problème

L'adresse IP statique affectée au téléphone est peut-être incorrecte.

Solution

Si une adresse IP statique est affectée au téléphone, vérifiez que vous avez saisi les paramètres adéquats.

Le téléphone est réinitialisé pendant une période d'utilisation intensive du réseau

Problème

Si le téléphone semble être réinitialisé pendant une période d'utilisation importante du réseau, il est possible qu'aucun VLAN vocal n'ait été configuré sur votre système.

Solution

Isolez les téléphones sur un VLAN auxiliaire distinct pour améliorer la qualité du trafic voix.

Le téléphone se réinitialise - Réinitialisation intentionnelle

Problème

Si vous n'êtes pas le seul administrateur ayant accès à Cisco Unified Communications Manager, vérifiez que les téléphones n'ont pas été réinitialisés intentionnellement par une autre personne.

Solution

Pour savoir si le téléphone IP Cisco a reçu une commande de réinitialisation de la part de Cisco Unified Communications Manager, appuyez sur **Applications** sur le téléphone et sélectionnez **Paramètres admin.** > **État** > **Statistiques réseau**.

- Si le champ Cause du redémarrage affiche `Réinit.-Réinit.`, le téléphone a reçu une commande Réinit./Réinit. de Cisco Unified Communications Manager Administration.
- Si le champ Cause du redémarrage affiche `Réinit.-Redém.`, le téléphone a reçu une commande Réinit./Redém. de Cisco Unified Communications Manager Administration.

Le téléphone est réinitialisé suite à des problèmes liés à DNS ou à la connexion

Problème

La réinitialisation du téléphone se poursuit et vous suspectez des problèmes avec DNS ou avec la connexion.

Solution

Si le téléphone continue sa réinitialisation, éliminez les erreurs de DNS ou les autres erreurs de connectivité en procédant comme indiqué à la section Détermination des problèmes DNS ou de connectivité, à la page 275.

Le téléphone ne s'allume pas

Problème

Le téléphone ne semble pas s'allumer.

Solution

Dans la plupart des cas, un téléphone redémarre lorsqu'il est allumé via un bloc d'alimentation externe, mais que cette connexion est interrompue et que le téléphone passe à PoE. De même, un téléphone peut redémarrer s'il est allumé à l'aide de PoE, puis se connecte à un bloc d'alimentation externe.

Le téléphone ne parvient pas à se connecter au réseau local

Problème

La connexion physique au réseau local peut être interrompue.

Solution

Vérifiez que la connexion Ethernet à laquelle le téléphone IP Cisco se connecte est active. Par exemple, vérifiez si le port ou le commutateur auquel le téléphone se connecte est éteint et si le commutateur ne redémarre pas. Vérifiez aussi qu'aucun câble n'est endommagé.

Problèmes liés à la sécurité du téléphone IP Cisco

Les sections qui suivent présentent des solutions aux problèmes liés aux fonctionnalités de sécurité du téléphone IP Cisco. Pour obtenir des informations sur la résolution de l'un ce des problèmes, et pour tout renseignement supplémentaire sur la résolution des problèmes de sécurité, reportez-vous au *Guide de la sécurité de Cisco Unified Communications Manager*.

Problèmes liés au fichier CTL

Les sections qui suivent présentent des solutions aux problèmes susceptibles d'être rencontrés avec le fichier CTL.

Erreur d'authentification, le téléphone ne peut pas authentifier le fichier CTL

Problème

Une erreur d'authentification de périphérique s'est produite.

Cause

Le fichier CTL ne possède pas de certificat Cisco Unified Communications Manager, ou possède un certificat incorrect.

Solution

Installez un certificat correct.

Le téléphone ne parvient pas à authentifier le fichier CTL

Problème

Le téléphone ne parvient pas à authentifier le fichier CTL.

Cause

Le jeton de sécurité qui a signé le fichier CTL mis à jour n'existe pas dans le fichier CTL du téléphone.

Solution

Changez le jeton de sécurité du fichier CTL et installez le nouveau fichier sur le téléphone.

Le fichier CTL s'authentifie mais les autres fichiers de configuration ne s'authentifient pas

Problème

Le téléphone ne peut authentifier aucun autre fichier de configuration que le fichier CTL.

Cause

Un enregistrement TFTP est endommagé, ou le fichier de configuration n'est pas signé par le certificat correspondant dans la liste de confiance du téléphone.

Solution

Vérifiez l'enregistrement TFTP et le certificat dans la liste de confiance.

Le fichier ITL s'authentifie mais les autres fichiers de configuration ne s'authentifient pas

Problème

Le téléphone ne peut authentifier aucun autre fichier de configuration que le fichier ITL.

Cause

Le fichier de configuration n'est peut-être pas signé par le certificat correspondant dans la liste de confiance du téléphone.

Solution

Signez de nouveau le fichier de configuration à l'aide du certificat adéquat.

L'autorisation TFTP échoue

Problème

Le téléphone signale un échec d'autorisation TFTP.

Cause

L'adresse TFTP du téléphone n'existe pas dans le fichier CTL.

Si vous avez créé un nouveau fichier CTL doté d'un nouvel enregistrement TFTP, le fichier CTL actuel du téléphone risque de ne pas contenir d'enregistrement pour le nouveau serveur TFTP.

Solution

Vérifiez la configuration de l'adresse TFTP dans le fichier CTL.

Le téléphone ne s'enregistre pas

Problème

Le téléphone ne s'enregistre pas auprès de Cisco Unified Communications Manager.

Cause

Le fichier CTL ne contient pas les informations adéquates pour le serveur Cisco Unified Communications Manager.

Solution

Modifiez les informations relatives au serveur Cisco Unified Communications Manager dans le fichier CTL.

Le système n'exige pas de fichiers de configuration signés

Problème

Le téléphone ne requiert pas de fichiers de configuration signés.

Cause

Le fichier CTL ne contient pas d'entrées TFTP dotées de certificats.

Solution

Configurez des entrées TFTP dotées de certificats dans le fichier CTL.

Problèmes relatifs aux appels vidéo

Aucune vidéo entre deux téléphones vidéo IP de Cisco

Problème

La vidéo n'est pas diffusée en continu entre deux téléphones vidéo IP Cisco.

Solution

Vérifiez qu'aucun Point de terminaison de média (MTP) n'est utilisé dans le flux d'appels.

Bégaiements vidéo ou trames perdues

Problème

Lorsque je suis sur un appel vidéo, la vidéo remplit son tampon ou perd des trames.

Solution

La qualité de l'image dépend de la bande passante de l'appel. L'augmentation du débit binaire accroît la qualité de votre vidéo, mais nécessite des ressources réseau supplémentaires. Toujours utiliser le débit binaire le plus adapté à votre type de vidéo. Un appel vidéo en 720p et 15 images par seconde nécessite un débit de 790 kbit/s ou plus. Un appel vidéo en 720p et 30 images par seconde nécessite un débit de 1360 kbit/s ou plus.

Pour plus d'informations sur la bande passante, reportez-vous à la section Configuration de la résolution de la transmission vidéo du chapitre « Configuration et fonctions téléphoniques ».

Solution

Assurez-vous que le débit binaire maximal de la session pour le paramètre d'appels vidéo est configuré pour correspondre au moins à la plage de débit binaire vidéo minimal. Sur Cisco Unified Communications Manager, accédez à **Système** > **informations régionales** > **Région**.

Je ne peux pas transférer un appel vidéo

Problème

Je ne peux pas transférer un appel vidéo à partir de mon téléphone de bureau vers mon appareil mobile.

Solution

Cisco Unified Mobility ne s'étend pas aux appels vidéo. Un appel vidéo est reçu sur le téléphone de bureau ne peut pas être pris sur votre téléphone portable.

Pas d'appel vidéo pendant une téléconférence

Problème

Un appel vidéo est transformé en appel audio lorsque j’ajoute deux ou davantage personnes à l'appel.

Vous devez utiliser un pont de conférence vidéo dans le cas des conférences vidéo Meet-Me et à la demande.

Problèmes généraux liés aux appels téléphoniques

Les sections qui suivent présentent des solutions aux problèmes généraux liés aux appels téléphoniques.

Impossible de passer un appel téléphonique

Problème

Un utilisateur se plaint de ne pas pouvoir passer un appel.

Cause

Le téléphone n'a pas d'adresse IP DHCP, il ne peut pas s'enregistrer auprès de Cisco Unified Communications Manager. Les téléphones équipés d'un écran LCD affichent le message `Configuration IP` ou `Enregistrement`. Les téléphones sans écran LCD émettent la tonalité toutes lignes occupées (au lieu de la tonalité de numérotation) dans le combiné lorsque l'utilisateur tente de passer un appel.

Solution

1. Effectuez les actions suivantes :
    1. Le câble Ethernet est branché.
    2. Le service Cisco CallManager est en cours d'exécution sur le serveur Cisco Unified Communications Manager.
    3. Les deux téléphones sont enregistrés auprès du même Cisco Unified Communications Manager.
2. Les journaux de débogage et de capture du serveur audio sont activés sur les deux téléphones. Si nécessaire, activez le débogage Java.

Le téléphone ne reconnaît pas les chiffres DTMF ou les chiffres sont différés

Problème

L'utilisateur signale que des chiffres ne sont pas affichés ou sont affichés avec du retard lorsqu'il utilise le clavier.

Cause

Si l'utilisateur appuie trop rapidement sur les touches, il se peut qu'il saute des chiffres ou que des chiffres soient différés.

Solution

L'utilisateur ne doit pas appuyer rapidement sur les touches.

Procédures de dépannage

Ces procédures peuvent être utilisées pour identifier les problèmes et les résoudre.

Créer un rapport sur les problèmes téléphoniques à partir de Cisco Unified Communications Manager

Vous pouvez générer un rapport sur les problèmes téléphoniques à partir de Cisco Unified Communications Manager. Cette action donne les mêmes informations que celles générées par la touche programmable Outil de rapport de problème (PRT) sur le téléphone.

Le rapport de problème contient des informations sur le téléphone et sur les casques.

Procédure

Étape 1 Dans Cisco Unified CM Administration, sélectionnez **Périphérique** > **Téléphone**.

Étape 2 Cliquez sur **Rechercher** et sélectionnez un ou plusieurs téléphones IP Cisco.

Étape 3 Cliquez sur **Générer le rapport PRT pour la sélection** pour collecter les journaux PRT pour les casques utilisés sur les téléphones IP Cisco sélectionnés.

Créer un journal de console à partir de votre téléphone

Vous générez un journal de console lorsque votre téléphone ne parvient pas à se connecter au réseau et que vous ne pouvez pas accéder à l'outil de rapport de problème (PRT).

Avant de commencer

Branchez un câble de console sur le port auxiliaire situé à l'arrière de votre téléphone.

Procédure

Étape 1 Sur votre téléphone, appuyez sur **Applications**.

Étape 2 Accédez à **Paramètres admin** > **Ports aux**.

Étape 3 Sélectionnez **collecter le journal de la console** pour collecter les journaux des périphériques.

Vérifier les paramètres TFTP

Procédure

Étape 1 Sur le téléphone IP Cisco, appuyez sur **Applications**, choisissez **Param. Admin** > **Paramétrage réseau** > **Configuration Ethernet** > **Configuration IPv4** > **Serveur TFTP 1**.

Étape 2 Si vous avez attribué une adresse IP statique au téléphone, vous devez saisir manuellement une valeur pour l'option Serveur TFTP 1.

Étape 3 Si vous utilisez DHCP, le téléphone obtient l'adresse du serveur TFTP du serveur DHCP. Vérifiez que l'adresse IP est configurée dans l'Option 150.

Étape 4 Vous pouvez aussi activer le téléphone afin qu'il utilise un autre serveur TFTP. Un tel paramétrage est particulièrement utile si le téléphone a été récemment déplacé.

Étape 5 Si le DHCP local ne fournit pas l'adresse TFTP correcte, activez le téléphone afin qu'il utilise un autre serveur TFTP.

Ceci est souvent nécessaire dans les scénarios faisant intervenir un VPN.

Détermination des problèmes DNS ou de connectivité

Procédure

Étape 1 Utilisez le menu Réinitialiser les paramètres pour réinitialiser les paramètres du téléphone à leurs valeurs par défaut.

Étape 2 Modifiez les paramètres DHCP et IP :

a) Désactivez DHCP.

b) Affectez des valeurs IP statiques au téléphone. Utilisez le routeur par défaut qui est utilisé par les autres téléphones fonctionnels.

c) Affectez un serveur TFTP. Utilisez le serveur TFTP qui est utilisé par les autres téléphones fonctionnels.

Étape 3 Sur le serveur Cisco Unified Communications Manager, vérifiez que les fichiers de l'hôte local sont dotés du nom de serveur Cisco Unified Communications Manager correct mappé sur l'adresse IP correcte.

Étape 4 Dans Cisco Unified Communications Manager, sélectionnez **Système** > **Serveur** et vérifiez que l'adresse IP, et non le nom DNS, fait référence au serveur.

Étape 5 Dans Cisco Unified Communications Manager, sélectionnez **Périphérique** > **Phone**. Cliquez sur **Find** (Rechercher) pour rechercher ce téléphone. Vérifiez que vous avez affecté l'adresse MAC adéquate pour ce téléphone IP Cisco.

Étape 6 Éteignez le téléphone puis rallumez-le.

Rubriques connexes

Réinitialisation de base, à la page 281
Détermination de l'adresse MAC du téléphone, à la page 74

Vérification des paramètres DHCP

Procédure

Étape 1 Sur le téléphone, appuyez sur **Applications** .

Étape 2 Sélectionnez **Wifi** > **Paramétrage réseau** > **Paramétrage IPv4**, puis recherchez les options suivantes :

- Serveur DHCP : si vous avez attribué une adresse IP statique au téléphone, il n'est pas nécessaire de saisir une valeur pour l'option Serveur DHCP. Toutefois, si vous utilisez un serveur DHCP, vous devez

indiquer une valeur pour cette option. Si vous ne trouvez aucune valeur, consultez la configuration du routage IP et du VLAN. Reportez-vous au document *Troubleshooting Switch Port and Interface Problems* (Résolution des problèmes de port de commutation et d'interface), disponible à l'adresse suivante :

http://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html

- Adresse IP, Masque de sous-réseau, Routeur par défaut : si vous avez attribué une adresse IP statique au téléphone, vous devez saisir manuellement les paramètres relatifs à ces options.

Étape 3 Si vous utilisez DHCP, vérifiez les adresses IP distribuées par votre serveur DHCP.

Reportez-vous au document *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks* (Présentation et dépannage de DHCP dans des réseaux d'entreprise ou des commutateurs Catalyst), disponible à l'adresse suivante :

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml

Créez un nouveau fichier de configuration de téléphone

Lorsque vous effacez un téléphone de la base de données de Cisco Unified Communications Manager, le fichier de configuration est supprimé du serveur TFTP Cisco Unified Communications Manager. Le ou les numéro(s) de répertoire du téléphone restent dans la base de données de Cisco Unified Communications Manager. Ils sont appelés numéros de répertoire non affectés et peuvent être utilisés pour d'autres périphériques. Si les numéros de répertoire non attribués ne sont pas utilisés par d'autres périphériques, supprimez ces numéros de répertoire de la base de données de Cisco Unified Communications Manager. Vous pouvez utiliser le rapport de plan de routage pour afficher et supprimer les numéros de référence non affectés. Pour obtenir plus d'informations, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Si vous modifiez les boutons d'un modèle de boutons de téléphone, ou si vous affectez un autre modèle de boutons à un téléphone, les numéros de répertoire risquent de ne plus être accessibles à partir du téléphone. Les numéros de répertoire sont toujours attribués au téléphone dans la base de données de Cisco Unified Communications Manager, mais le téléphone ne dispose d'aucun bouton pour répondre aux appels. Ces numéros de répertoire doivent être supprimés du téléphone et effacés si nécessaire.

Procédure

Étape 1 Dans Cisco Unified Communications Manager, Sélectionnez **Périphérique** > **Phone** et cliquez sur **Find** (Rechercher) pour localiser le téléphone qui pose problème.

Étape 2 Sélectionnez **Supprimer** pour effacer le téléphone de la base de données de Cisco Unified Communications Manager.

Remarque Lorsque vous effacez un téléphone de la base de données de Cisco Unified Communications Manager, le fichier de configuration est supprimé du serveur TFTP Cisco Unified Communications Manager. Le ou les numéro(s) de répertoire du téléphone restent dans la base de données de Cisco Unified Communications Manager. Ils sont appelés numéros de répertoire non affectés et peuvent être utilisés pour d'autres périphériques. Si les numéros de répertoire non attribués ne sont pas utilisés par d'autres périphériques, supprimez ces numéros de répertoire de la base de données de Cisco Unified Communications Manager. Vous pouvez utiliser le rapport de plan de routage pour afficher et supprimer les numéros de référence non affectés.

Étape 3 Ajoutez à nouveau le téléphone à la base de données de Cisco Unified Communications Manager.

Étape 4 Éteignez le téléphone puis rallumez-le.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv
Méthodes disponibles pour ajouter des téléphones, à la page 75

Identification des problèmes d'authentification 802.1X

Procédure

Étape 1 Vérifiez que vous avez configuré correctement les composants requis.

Étape 2 Confirmez que le secret partagé est configuré sur le téléphone.

- S'il est configuré, vérifiez que le serveur d'authentification présente le même secret partagé.
- Si le secret partagé n'est pas configuré sur le téléphone, saisissez-le et assurez-vous qu'il correspond au secret partagé sur le serveur d'authentification.

Vérification des paramètres DNS

Pour vérifier les paramètres DNS, procédez comme suit :

Procédure

Étape 1 Appuyez sur **Applications** .

Étape 2 Sélectionnez **Paramètres administrateur** > **Paramétrage réseau** > **Paramétrage IPv4** > **Serveur DNS 1**.

Étape 3 Vous devez aussi vérifier qu'une entrée CNAME a été apportée au serveur DNS pour le serveur TFTP et pour le système Cisco Unified Communications Manager.

Vous devez aussi vous assurer que DNS est configuré pour la recherche inversée.

Démarrage d'un service

Les services doivent être activés pour pouvoir être démarrés ou arrêtés.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Cisco Unified Serviceability** dans la liste déroulante Navigation et cliquez sur **Aller**.

Étape 2 Sélectionnez **Outils** > **Centre de contrôle - Services de fonction**.

Étape 3 Sélectionnez le serveur Cisco Unified Communications Manager principal dans la liste déroulante Serveur.

La fenêtre contient les noms des services du serveur que vous avez choisi, l'état des services et un volet de contrôle des services dans lequel vous pouvez démarrer ou arrêter un service.

Étape 4 Si un service s'est arrêté, cliquez sur la case d'option correspondante, puis sur **Démarrer**.

Le symbole État service carré est remplacé par une flèche.

Contrôle des informations de débogage à l'aide de Cisco Unified Communications Manager

Si vous rencontrez sur votre téléphone, des problèmes que vous ne parvenez pas à résoudre, le centre d'assistance technique de Cisco peut vous venir en aide. Vous devrez activer le débogage pour le téléphone, reproduire le problème, désactiver le débogage, puis envoyer les journaux au centre d'assistance technique en vue d'une analyse.

Comme le débogage capture des informations détaillées, le trafic des communications peut ralentir le téléphone, ce qui le rendra moins réactif. Après avoir capturé les journaux, vous devrez désactiver le débogage pour assurer le bon fonctionnement du téléphone.

Les informations de débogage peuvent inclure un code à un chiffre qui reflète la gravité du problème. Les problèmes sont évalués selon les critères suivants :

- 0 - Urgent
- 1 - Alerte
- 2 - Critique
- 3 – Erreur
- 4 - Avertissement
- 5 – Notification
- 6 - Informations
- 7 - Débogage

Contactez le centre d'assistance technique de Cisco pour plus d'informations et pour obtenir de l'aide.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez l'une des fenêtres suivantes :

- **Périphérique** > **Paramètres du périphérique** > **Profil du téléphone commun**
- **Système** > **Configuration des téléphones d'entreprise**
- **Périphérique** > **Téléphone**

Étape 2 Définissez les paramètres suivants :

- Log Profile (Consigner le profil) - valeurs : Preset (Prédéfini) (valeur par défaut), Default (Par défaut), Telephony (Téléphonie), SIP, UI, Network (Réseau), Media (Multimédia), Upgrade (Mise à niveau), Accessory (Accessoire), Security (Sécurité), Wi-Fi, VPN, Energywise, MobileRemoteAccess

  Remarque Pour assurer la prise en charge des paramètres à plusieurs niveaux et dans plusieurs sections, cochez la case Log Profile.

- Remote Log (Journal à distance) - valeurs : Désactiver (valeur par défaut), Activer
- IPv6 Log Server or Log Server (Serveur de journaux IPv6 ou Serveur de journaux) : Adresse IP (adresse IPv4 ou IPv6)

Remarque Lorsqu'il est impossible de joindre le serveur de journaux, le téléphone cesse d'envoyer des messages de débogage.

- Le format de l'adresse IPv4 du serveur de journalisation est le suivant : **adresse:<port>@@base=<0-7>;pfs=<0-1>**
- Le format de l'adresse IPv6 du serveur de journalisation est le suivant : **adresse:<port>@@base=<0-7>;pfs=<0-1>**
- Où :
  - L'adresse IPv4 est délimitée par des points (.)
  - L'adresse IPv6 est délimitée par le symbole deux points (:)

Autres informations relatives à la résolution de problèmes

Pour tout renseignement supplémentaire sur la résolution d'éventuels problèmes rencontrés sur votre téléphone, visitez le site web Cisco suivant et naviguez jusqu'au modèle de téléphone pertinent :

https://www.cisco.com/cisco/web/psa/troubleshoot.html

CHAPITRE 13

Maintenance

Réinitialisation de base

Effectuer une réinitialisation de base d'un téléphone IP Cisco permet de résoudre la situation si le téléphone rencontre une erreur en proposant une réinitialisation ou une restauration de divers paramètres de configuration et de sécurité.

Le tableau suivant décrit les différentes manières d'effectuer une réinitialisation simple. Vous pouvez réinitialiser un téléphone en effectuant n'importe laquelle de ces opérations après le démarrage du téléphone. Choisissez l'opération la plus appropriée pour votre situation.

Tableau 54 : Méthodes de réinitialisation simple

Opération	Action	Expli
Redémarrer le téléphone	Appuyez sur **Applications**. Allez dans **Paramètres Admin** > **Réinitialiser les paramètres** > **Réinitialisation du périphérique**.	Réini ou ré précé
Réinitialiser les paramètres	Pour réinitialiser les paramètres, appuyez sur **Applications** et choisissez **Paramètres administrateur** > **Réinitialiser les paramètres** > **Réseau**.	Réini valeu
	Pour réinitialiser le fichier CTL, appuyez sur **Applications** puis choisissez **Paramètres administrateur** > **Réinitialiser les paramètres** > **Sécurité**.	Réini

Réinitialisation du téléphone sur les paramètres d'usine depuis le clavier du téléphone

Vous pouvez réinitialiser le téléphone aux paramètres d'usine. La réinitialisation efface tous les paramètres du téléphone.

Procédure

Étape 1 Coupez le courant du téléphone en suivant l'une des méthodes suivantes :

- Débranchez l'adaptateur secteur.
- Débranchez le câble LAN.

Étape 2 Attendez pendant 5 secondes.

Étape 3 Appuyez et maintenez enfoncée la touche **#** , puis rebranchez le téléphone. Ne libérez la touche **#** que lorsque les boutons **Casque** et **Haut- parleur** sont allumés.

Remarque Dans certaines versions matérielles, le bouton **Coupure micro** s'allume également en même temps que les boutons **Casque** et **Haut-parleur** lorsque vous rebranchez le téléphone. Dans ce cas, attendez qu'ils se déconnectent et libérez la touche **#** uniquement lorsque les boutons du **casque** et du **haut-parleur** sont allumés à nouveau.

Étape 4 Saisissez la séquence de touches suivante :

```
123456789*0#
```

Le voyant du bouton **Casque** se désactive une fois que vous appuyez sur la touche **1**. Après la saisie de la séquence de touches, le bouton **Silence** s'allume.

Avertissement N’éteignez pas le téléphone avant la fin de la réinitialisation d'usine ou avant l'affichage de l’écran principal.

Le téléphone est réinitialisé.

Réinitialisation de tous les paramètres de menu du téléphone

Effectuez cette tâche si vous souhaitez rétablir les valeurs par défaut des paramètres de configuration de votre utilisateur et de votre réseau.

Procédure

Étape 1 Appuyez sur **Applications**  .

Étape 2 Choisissiez **Paramètres administrateur** > **Réinitialiser les paramètres** > **Tous les paramètres**.

Si nécessaire, déverrouillez les options du téléphone.

Redémarrez votre téléphone à partir de l'image de sauvegarde

Votre téléphone IP Cisco possède une deuxième image de sauvegarde qui vous permet de restaurer le téléphone lorsque l'image par défaut a été altérée.

Pour réinitialiser votre téléphone à partir de l'image de sauvegarde, procédez comme suit.

Procédure

Étape 1 Débranchez le câble d'alimentation.

Étape 2 Appuyez sur la touche étoile (*) et maintenez-la enfoncée.

Étape 3 Reconnectez l'alimentation. Continuez d'appuyer sur la touche étoile jusqu'à ce que le voyant Silence s'éteigne.

Étape 4 Relâchez la touche étoile.
Le téléphone redémarre à partir de l'image de sauvegarde.

Effectuer la réinitialisation de la configuration réseau

Réinitialise les paramètres de configuration réseau sur leurs valeurs par défaut et réinitialise le téléphone. Cette méthode mène le DHCP à reconfigurer l'adresse IP du téléphone.

Procédure

Étape 1 Dans le menu Paramètres administrateur, si nécessaire, déverrouillez les options du téléphone.

Étape 2 Choisissez **Réinitialiser les paramètres** > **Configuration réseau**.

Effectuer la réinitialisation de la configuration réseau de l'utilisateur

Réinitialise à la valeur des paramètres enregistrés précédemment les modifications apportées à la configuration réseau et à la configuration des utilisateurs mais que le téléphone n'a pas écrit dans sa mémoire flash.

Procédure

Étape 1 Dans le menu Paramètres administrateur, si nécessaire, déverrouillez les options du téléphone.

Étape 2 Choisissez **Réinitialiser les paramètres** > **Réinitialiser le périphérique**.

Suppression du fichier CTL

Cette opération efface uniquement le fichier CTL du téléphone.

Procédure

Étape 1 Dans le menu Paramètres administrateur, si nécessaire, déverrouillez les options du téléphone.

Étape 2 Choisissez **Réinitialiser les paramètres** > **Paramètres de sécurité**.

Outil de rapport sur la qualité

L'outil de rapport sur la qualité (QRT, Quality Report Tool) est un outil de création de rapport de problèmes généraux et de qualité d'écoute pour les téléphones IP Cisco. La fonctionnalité QRT est installée pendant l'installation de Cisco Unified Communications Manager.

Vous pouvez configurer les téléphones IP Cisco des utilisateurs avec QRT. Ainsi, les utilisateurs pourront signaler les éventuels problèmes rencontrés lors de leurs appels, en appuyant sur RappQualité. Cette touche programmable ou ce bouton n'est disponible que lorsque le téléphone IP Cisco est dans l'état Connecté, Conférence connectée, Transfert connecté, ou Raccroché.

Lorsqu'un utilisateur appuie sur RappQualité, la liste des catégories de problèmes s'affiche. L'utilisateur sélectionne la catégorie de problèmes appropriée, et cette action est consignée dans un fichier XML. Les informations consignées dépendent de la sélection de l'utilisateur et du fait que le périphérique de destination soit un téléphone IP Cisco ou non.

Pour plus d'informations à propos de l'utilisation du QRT, consultez la documentation propre à votre version particulière de Cisco Unified Communications Manager.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Surveillance de la qualité vocale

Pour mesurer la qualité d'écoute des appels qui sont émis et reçus sur le réseau, les téléphones IP Cisco utilisent les mesures statistiques basées sur des événements de masquage. Le DSP émet des trames de masquage pour masquer la perte de trames dans le flux de paquets de voix.

- Mesure Ratio de masquage : indique le ratio de masquage de trames par rapport au nombre total de trames de voix. Un ratio de masquage est calculé toutes les 3 secondes.
- Mesure Secondes masquées : indique la durée, en secondes, pendant laquelle le DSP émet des trames de masquage pour masquer la perte de trames. Une « seconde masquée » de haut niveau est une seconde pendant laquelle le DSP émet plus de cinq pour cent de trames de masquage.

Remarque Le ratio de masquage et les secondes masquées sont des mesures basées sur la perte de trames. Un ratio de masquage de zéro indique que le réseau IP transmet des trames et des paquets en temps et en heure, sans perte.

Vous pouvez accéder aux mesures de la qualité d'écoute sur l'écran Statistiques d'appel du téléphone IP Cisco, ou à distance à l'aide des statistiques de streaming.

Conseils pour la résolution de problèmes de qualité d'écoute

Lorsque vous remarquez d'importantes variations persistantes des mesures, consultez le tableau suivant pour obtenir des informations générales sur la résolution de problèmes.

Tableau 55 : Variation des mesures de la qualité vocale

Variation de mesure	Condition
Le ratio de masquage et les secondes masquées augmentent considérablement	Troubles du réseau dus à une perte de paquets ou à une gigue élevée.
Le ratio de masquage est proche de zéro ou nul, mais la qualité d'écoute est mauvaise.	• Bruit ou distorsions dans le canal audio, par exemple un écho ou des niveaux sonores. • Appels en tandem faisant l'objet de plusieurs opérations d'encodage ou de décodage, par exemple appels d'un réseau cellulaire ou d'un réseau de carte prépayée. • Problèmes acoustiques provenant d'un haut-parleur, d'un téléphone portable mains libres ou d'un casque sans fil. Observez les compteurs de paquets transmis (TxCnt) et de paquets reçus (RxCnt) pour vérifier que les paquets de voix circulent de manière fluide.
Les notes MOS LQK diminuent considérablement	Endommagement du réseau suite à une perte de paquets ou à des niveaux de gigue élevés : • Les diminutions de MOS LQK peuvent indiquer un endommagement généralisé et uniforme. • Les diminutions de MOS LQK isolées peuvent indiquer un endommagement par salves. Effectuez une vérification croisée du ratio de masquage et des secondes masquées pour rechercher la preuve d'une perte de paquets et d'une gigue éventuelles.
Les notes MOS LQK augmentent considérablement	• Vérifiez si le téléphone utilise un autre codec que celui attendu (RxType et TxType). • Vérifiez si la version de MOS LQK a changé suite à une mise à niveau de micrologiciel.

Remarque Les mesures de la qualité vocale prennent uniquement en compte la perte de trames, et non le bruit ou la distorsion.

Nettoyage des téléphones IP Cisco

Pour nettoyer votre téléphone IP Cisco, utilisez uniquement un chiffon doux et sec pour essuyer doucement le téléphone et son écran. N'appliquez pas de produits, qu'ils soient liquides ou en poudre, directement sur votre téléphone. Comme pour tous les équipements électroniques qui ne sont pas résistants aux intempéries, les produits liquides ou en poudre peuvent endommager les composants et provoquer des pannes.

Lorsque le téléphone est en mode veille, l'écran est éteint et le bouton Select n'est pas allumé. Lorsque le téléphone est dans cet état, vous pouvez nettoyer l'écran, à condition d'être certain que le téléphone restera en mode veille jusqu'à ce que vous ayez terminé le nettoyage.

CHAPITRE 14

Assistance utilisateur internationale

Programme d'installation des paramètres régionaux des terminaux Unified Communications Manager

Par défaut, les téléphones IP Cisco sont configurés pour la langue anglaise (États-Unis). Pour utiliser les téléphones IP Cisco avec d'autres paramètres régionaux, vous devez installer la version spécifique locale du programme d'installation des paramètres régionaux des terminaux Unified Communications Manager sur chaque serveur Cisco Unified Communications Manager dans le cluster. Le programme d'installation des paramètres régionaux installe sur votre système le plus récent texte traduit pour l'interface utilisateur du téléphone et les tonalités spécifiques au pays correspondant, afin de les mettre à la disposition des téléphones IP Cisco.

Pour accéder au programme d'installation des paramètres locaux requis pour une version, accédez à la page Téléchargement de logiciel, accédez au modèle de votre téléphone, puis sélectionnez le lien vers le programme d'installation des paramètres locaux des terminaux d'Unified Communications Manager.

Pour obtenir plus d'informations, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Remarque Le plus récent programme d'installation de paramètres régionaux ne sera peut-être pas disponible immédiatement ; visitez régulièrement le site Web pour connaître la disponibilité des mises à jour.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page xv

Assistance pour la journalisation des appels internationaux

Si votre système téléphonique est configuré pour la journalisation des appels internationaux (normalisation des appelants), les entrées de journal des appels, de renumérotation ou de répertoire d'appels peuvent inclure le symbole plus (+) pour représenter votre indicatif téléphonique international. Selon la configuration de votre système téléphonique, le symbole + peut être remplacé par l'indicatif international correct, ou vous devrez peut-être remplacer manuellement ce symbole + par votre indicatif international. En outre, bien que le journal des appels ou l'entrée de répertoire puisse afficher l'intégralité du numéro international d'un appel reçu, l'écran du téléphone risque d'afficher le version locale abrégée du numéro, sans indicatif international ou régional.

Limitation de langue

Il n'existe aucune prise en charge de saisie de texte alphanumérique au clavier (KATE, Keyboard Alphanumeric Text Entry) localisée pour les paramètres régionaux asiatiques suivants :

- Chinois (Hong Kong)
- Chinois (Taiwan)
- Japonais (Japon)
- Coréen (République de Corée)

La valeur par défaut en anglais (États-Unis) KATE est proposée à l'utilisateur à la place.

Par exemple, l'écran du téléphone affiche le texte en coréen, mais la touche **2** du clavier affichera **a b c 2 A B C**.

La saisie du chinois fonctionne de la même manière que sur les PC et les téléphones portables en chinois. Le programme d'installation des paramètres régionaux chinois est nécessaire pour que la fonction de saisie en chinois fonctionne.