Guide d’administration des téléphones de conférence IP Cisco 7832 pour Cisco Unified Communications Manager

Première publication : 30 août 2017

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

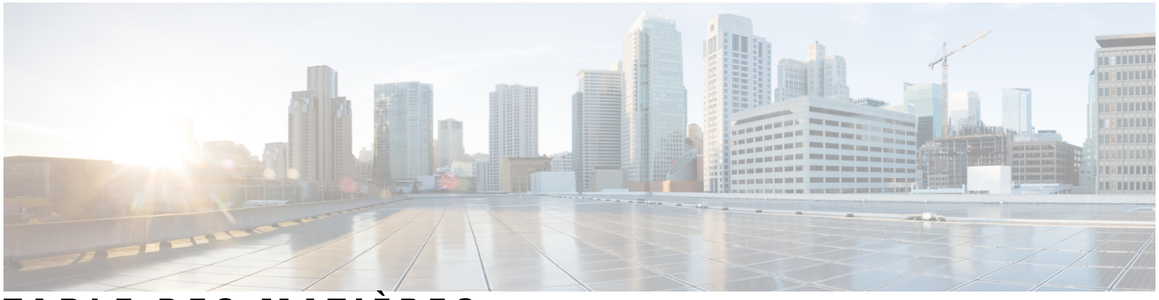


TABLE DES MATIÈRES

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).

Fonctionnalité	Nouveautés et mises à jour
Prise en charge du protocole SIP OAuth sur SRST	Renforcement de la sécurité pour votre réseau téléphonique, à la page 62

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 62

Fonctionnalité	Nouveautés et mises à jour
Migration du téléphone sans utiliser de version de transition	Migration de votre téléphone vers un téléphone multiplateforme directement, à la page 78

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

Tableau 1 : Nouveautés et mises à jour

Fonctionnalité	Nouvelles sections ou sections modifiées
Améliorations SIP OAuth	Renforcement de la sécurité pour votre réseau téléphonique, à la page 62
Améliorations de l'interface utilisateur	Surviveable Remote Site Telephony (SRST), à la page 53
Améliorations de Oauth pour MRA	Mobile and Remote Access Through Expressway, à la page 105

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 40
Ajouter des informations supplémentaires au champ d'accès au Web	Configuration spécifique au produit, à la page 82

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

Aucune révision n'a été apportée au guide d'administration, relative à la version 12.7(1) du micrologiciel.

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

Aucune révision n'a été apportée au guide d'administration, relative à la version 12.6(1) du micrologiciel.

Nouveautés et modifications des informations 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.

Le tableau suivant répertorie les modifications apportées au *Guide d'administration des téléphones de conférence IP Cisco 7832 pour Cisco Unified Communications Manager* pour prendre en charge la version du micrologiciel 12.5(1) SR3.

Tableau 2 : Révisions apportées au Guide d'administration du téléphone IP Cisco 7832, relatives à la version 12.5(1) SR3 du micrologiciel.

Révision	Les sections nouvelles ou mises 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 29
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 159

Nouveautés et modifications des informations de la version 12.5(1) SR2 du micrologiciel

Aucune révision n'a été apportée au guide d'administration, relative à la version 12.5(1) SR2 du micrologiciel.

La version 12.5(1) SR2 du micrologiciel remplace les versions 12.5(1) et 12.5(1) SR1. La version du micrologiciel 12.5 (1) et la version du micrologiciel 12.5 (1) SR1 ont été reportées au profit du micrologiciel version 12.5 (1) SR2.

Nouveautés et modifications des informations de la version 12.5(1) SR1 du micrologiciel

Le tableau suivant répertorie les modifications apportées au *Guide d'administration des téléphones de conférence IP Cisco 7832 pour Cisco Unified Communications Manager* pour prendre en charge la version du micrologiciel 12.5(1) SR1.

Tableau 3 : Révisions apportées au Guide d'administration du téléphone de conférence IP Cisco 7832, relatives à la version 12.5(1) SR1 du microprogramme.

Révision	Les sections nouvelles ou mises à jour
Prise en charge de la courbe elliptique	Fonctionnalités de sécurité prises en charge, à la page 63
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 107
Prise en charge de l'intégration du code d'activation	Intégration par code d'activation pour les téléphones sur site, à la page 28

Nouveautés et modifications des informations de la version 12.5(1) du micrologiciel

Le tableau suivant répertorie les modifications apportées au *Guide d'administration des téléphones de conférence IP Cisco 7832 pour Cisco Unified Communications Manager* pour prendre en charge la version du micrologiciel 12.5(1).

Tableau 4 : Révisions apportées au Guide d'administration du téléphone de conférence IP Cisco 7832, relatives à la version 12.5(1) du microprogramme.

Révision	Les sections nouvelles ou mises à jour
Prise en charge de la radiomessagerie de chuchotement sur Cisco Unified Communications Manager Express	Interaction avec Cisco Unified Communications Manager Express, à la page 22
Prise en charge de la désactivation des codes de chiffrement TLS	Configuration spécifique au produit, à la page 82
Prise en charge de la composition Enbloc pour l'amélioration de la minuterie de délai entre chiffres T.302.	Configuration spécifique au produit, à la page 82

Nouveautés et modifications des informations de la version 12.1(1) du micrologiciel

Le tableau suivant répertorie les modifications apportées au *Guide d'administration des téléphones de conférence IP Cisco 7832 pour Cisco Unified Communications Manager* pour prendre en charge la version du micrologiciel 12.1(1).

Révision	Les sections nouvelles ou mises à jour
Prise en charge de Mobile and Remote Access Through Expressway	• Mobile and Remote Access Through Expressway, à la page 105 • Scénarios de déploiement, à la page 107 • Configurer des informations d'authentification permanentes pour la connexion à Expressway, à la page 108
Prise en charge de l'activation ou la désactivation de TLS 1.2 pour l'accès au serveur web.	Configuration spécifique au produit, à la page 82
Prise en charge du codec audio G722.2 AMR-WB	• Le Téléphone Cisco IP Conference Phone 7832, à la page 9 • Champs relatifs aux statistiques d'appel, à la page 126

SECTION I

À propos des téléphones de conférence IP Cisco

CHAPITRE 2

Matériel du téléphone de conférence IP Cisco

Le Téléphone Cisco IP Conference Phone 7832

Le Téléphone Cisco IP Conference Phone 7832 améliore les communications inter-personnelles, combinant des performances audio supérieures haute-définition (HD) et une couverture à 360 degrés de toutes les tailles de salles de conférence et de bureaux. Il fournit aux mélomanes une expérience sonore avec un haut-parleur en duplex intégral à large bande (G.722) bidirectionnel doté de la fonctionnalité mains libres. Le Téléphone Cisco IP Conference Phone 7832 est une solution simple qui répond aux défis de la plupart des salles.

Le téléphone dispose de microphones sensibles avec une couverture à 360 degrés. Cette couverture permet aux utilisateurs de parler d'une voix normale et d'être entendus clairement jusqu'à une distance de 2,1 m. Le téléphone propose également une technologie résistant aux interférences des téléphones portables et autres périphériques sans fil, garantie de restitution de communications claires exemptes de perturbations.

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.

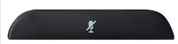
Pour pouvoir fonctionner dans un réseau de téléphonie IP, le téléphone IP Cisco doit être connecté à un périphérique réseau, comme un commutateur Cisco Catalyst. Vous devez également enregistrer le téléphone IP Cisco auprès d'un système Cisco Unified Communications Manager avant de pouvoir passer et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

Boutons et matériel du téléphone IP Cisco 7832

L'illustration suivante montre le téléphone de conférence IP Cisco 7832.

Illustration 1 : Boutons et fonctionnalités des téléphones de conférence IP Cisco 7832

Le tableau ci-dessous décrit les boutons du téléphone de conférence IP Cisco 7832.

1	Barre de **Mise en sourdine**	 Activer ou désactiver le microphone. Lorsque le microphone est coupé, la barre de DEL est allumée en rouge.
2	Barre de DEL	Indique l'état des appels : • Vert fixe : appel actif • Vert clignotant : appel entrant • Vert avec des impulsions : appel en attente • Rouge fixe : appel mis en sourdine
3	Boutons de touches	Permettent d'accéder à des fonctions et à des services.
4	Barre de navigation et bouton **Sélection**	 Parcourez les menus, mettez des éléments en surbrillance et sélectionnez l'élément en surbrillance. Lorsque le téléphone est inactif, appuyez sur la touche **Haut** pour accéder à la liste des appels récents, puis appuyez sur **Bas** pour accéder à la liste des Favoris.

5	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). Lorsque vous réglez le volume, la barre de DEL s'allume en blanc pour afficher la modification du volume.

Touches programmables des téléphones de conférence

Vous pouvez interagir avec les fonctionnalités de votre téléphone à l'aide des touches programmables. 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.

Les touches programmables La touche programmable ●● indique que davantage de fonctions programmables sont disponibles.

Documentation associée

Consultez les sections suivantes pour obtenir des informations associées.

Documentation des téléphones IP Cisco 7832 de conférence

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.

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/index.php/regulations/export-administration-regulations-ear.

Différences de terminologie

Dans ce document, le terme *Téléphone IP Cisco* inclut le téléphone de conférence IP Cisco 7832.

Le tableau suivant présente les différences de terminologie qui existent entre le *Guide de l'utilisateur des téléphone de conférence IP Cisco 7832*, le *Guide d'administration des téléphone de conférence IP Cisco 7832 pour Cisco Unified Communications Manager*, et la documentation de Cisco Unified Communications Manager.

Tableau 5 : Différences de terminologie

Guide de l'utilisateur	Guide d'administration
Indicateurs de message	Indicateur de message en attente (MWI)
Système de messagerie vocale	Système de messagerie vocale

CHAPITRE 3

Caractéristiques techniques

Spécifications physiques et environnementales

Le tableau suivant présente les spécifications environnementales et matérielles nécessaires au bon fonctionnement des téléphones de conférence.

Tableau 6 : Caractéristiques environnementales et physiques

Spécification	**Valeur ou plage de valeurs**
Température de fonctionnement	De 0 à 40 °C (de 32 à 104 °F)
Humidité relative en fonctionnement	De 10 à 90 % (sans condensation)
Température de stockage	De –10 °C à 60° C (de 14° à 114° F)
Hauteur	226 mm
Largeur	226 mm
Profondeur	54,4 mm
Poids	0,907 kg (2,0 lb)

Spécification	Valeur ou plage de valeurs
Alimentation	• IEEE PoE Class 2. Le téléphone est compatible avec les deux serv Discovery Protocol et Link Layer Discovery Protocol - Power ov • Si les commutateurs LAN connectés ne prennent pas en charge P l'alimentation électrique et fournir une alimentation PoE
Câbles	Catégorie 3/5/5e/6 pour câbles 10 Mbits/s avec 4 paires Catégorie 5/5e/6 pour câbles 100 Mbits/s avec 4 paires **Remarque** Les câbles comprennent 4 paires de fils pour un total de 8
Exigences relatives aux distances	La spécification Ethernet suppose que la longueur maximale des câble 100 mètres (330 pieds).

Pour plus d'informations, reportez-vous à la *Fiche technique du téléphone de conférence IP Cisco 7832* : http://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-7800-series/datasheet-listing.html

Spécifications relatives aux câbles

- Jack RJ-45 pour la connexion 10/100BaseT au réseau.

Conditions requises pour l'alimentation du téléphone

Le téléphone de conférence IP Cisco peut utiliser les sources d'alimentation suivantes :

- PoE (Power over Ethernet)
- Le câble d'injecteur PoE de téléphone de conférence IP Cisco 7832 et l'amplificateur de puissance Cisco 3
- Injecteur de courant pour téléphone IP Cisco

Remarque Le câble d'injecteur PoE n'est pas actuellement disponible.

Tableau 7 : Instructions relatives à l'alimentation du téléphone de conférence IP Cisco

Type d'alimentation	Directives
Alimentation PoE : fournie par un commutateur par le biais du câble Ethernet raccordé au téléphone.	Pour assurer le fonctionnement ininterrompu du téléphone, prévoyez une alimentation d pour le commutateur. 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.

Type d'alimentation	Directives
Alimentation externe : assurée par le câble d'injecteur PoE de téléphone de conférence IP Cisco 7832 et l'amplificateur de puissance Cisco 3	Le câble d'injecteur et l'amplificateur de puissance alimentent le câble Ethernet. Lorsque vous installez un téléphone alimenté par un adaptateur d'injection, connecte à l'alimentation électrique avant de connecter le câble Ethernet au téléphone. Lor supprimez un téléphone qui utilise l'adaptateur d'injection, déconnectez le câble E téléphone avant de couper l'alimentation de l'adaptateur.
Alimentation externe : assurée par l'injecteur de courant pour téléphone IP Cisco	L'injecteur de courant alimente le câble Ethernet. Lorsque vous installez un téléphone alimenté par un injecteur d'alimentation, connec à l'alimentation électrique avant de connecter le câble Ethernet au téléphone. Lor supprimez un téléphone qui utilise un injecteur, déconnectez le câble Ethernet du avant de couper l'alimentation de l'injecteur.

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 pendant la durée prévue jusqu'à ce que l'utilisateur appuie sur un 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.

Rubriques connexes

Planification du mode Économies d'énergie pour un téléphone IP Cisco, à la page 95
Planifier EnergyWise sur le téléphone IP Cisco, à la page 96

Protocoles réseau pris en charge

Les téléphones de conférence IP Cisco prennent en charge plusieurs protocoles réseau Cisco et normes du secteur, qui sont nécessaires pour les communications vocales. Le tableau suivant présente une vue d'ensemble des protocoles réseau pris en charge par les téléphones.

Tableau 8 : Protocoles réseau pris en charge sur le téléphone de conférence IP Cisco

Protocole réseau	Objectifs	Notes sur l'utilisation
Protocole BootP (Bootstrap Protocol)	Le protocole BootP permet à un périphérique réseau tel qu'un téléphone, de détecter certaines informations de démarrage, notamment son adresse IP.	-
Cisco Discovery Protocol (CDP)	CDP est un protocole de détection de périphériques qui est intégré à tous les équipements fabriqués par Cisco. Les périphériques peuvent utiliser CDP pour publier leur existence auprès d'autres périphériques et pour recevoir des informations concernant les autres périphériques du réseau.	Les téléphones utilisent CDP pour échanger avec le commutateur Cisco Catalyst, des informations telles l'ID du VLAN auxiliaire, les détails de la gestion de l'énergie selon le port, et les informations de configuration de la qualité de service (QoS).
Protocole DHCP (Dynamic Host Configuration Protocol)	Le protocole DHCP alloue dynamiquement une adresse IP qu'il affecte aux périphériques réseau. Grâce au protocole DHCP, vous pouvez connecter un téléphone IP au réseau et le rendre opérationnel sans avoir besoin d'affecter manuellement une adresse IP, ou de configurer d'autres paramètres réseau.	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 prendre connaissance des autres configurations DHCP prises en charge, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager. **Remarque** Si vous ne pouvez pas utiliser l'option 150, utilisez l'option DHCP 66.
Protocole HTTP (HyperText Transfer Protocol)	HTTP est le protocole standard de transfert d'informations et de déplacement de documents sur Internet et sur le web.	Les téléphones utilisent HTTP pour les services XML, la mise à disposition, les mises à niveau et la résolution de problèmes.
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.	Les applications web prenant en charge HTTP et HTTPS comportent deux URL configurées. Les téléphones qui prennent en charge le protocole HTTPS sélectionnent l'URL HTTPS. Une icône représentant un verrou est affichée à l'écran du téléphone si la connexion au service est établie via HTTPS.

Protocole réseau	Objectifs	Notes sur l'utilisation
IEEE 802.1X	La norme IEEE 802.1X définit un protocole d'authentification et de contrôle d'accès des clients et des serveurs, qui empêche les clients non autorisés de se connecter à un réseau local via des ports de commutation publiquement accessibles. 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 applique la norme IEEE 802.1X par l'intermédiaire de la prise en charge des méthodes d'authentification suivantes : EAP-FAST et EAP-TLS. Lorsque l'authentification 802.1X est activée sur le téléphone, vous devez désactiver le VLAN voix.
Protocole IP	Le protocole IP est un protocole de messagerie qui adresse et envoie des paquets sur le réseau.	Pour communiquer avec le protocole IP, les périphériques réseau doivent être affectés d'une adresse IP, d'un sous-réseau et d'une passerelle. Les valeurs d'adresse IP, de sous-réseau et de passerelle sont automatiquement affectées lorsque vous utilisez le téléphone avec le protocole de configuration d'hôte dynamique (DHCP). Si vous n'utilisez pas DHCP, vous devez affecter manuellement ces propriétés à chaque téléphone, localement. Les téléphones 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.

Protocole réseau	Objectifs	Notes sur l'utilisation
LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Devices)	LLDP-MED est une extension de la norme LLDP développée pour les produits audio.	LLDP-MED est pris en charge sur le port de commutation des téléphones, pour communiquer des informations telles que : • La configuration du VLAN • La détection de périphériques • La gestion de l'alimentation • La gestion de l'inventaire 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
Protocole RTP (Real-Time Transport Protocol)	RTP est un protocole standard de transport de données en temps réel, notamment l'audio et la vidéo interactives, sur des réseaux de données.	Les téléphones utilisent le protocole RTP pour envoyer et recevoir le trafic voix en temps réel provenant d'autres téléphones et passerelles.
Protocole RTCP (Real-Time Control Protocol)	RTCP fonctionne en conjonction avec RTP pour fournir des données QoS (notamment la gigue, la latence et le retard aller-retour) sur les flux RTP.	Le protocole RTCP est activé par défaut.
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.	Tout comme d'autres protocoles VoIP, SIP est conçu pour adresser les fonctions de signalisation et de gestion des sessions sur un réseau de téléphonie en paquets. La signalisation permet la transmission des informations d'appel dans les limites du 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 et à la fois en IPv6 et IPv4.
Protocole SRTP (Secure Real-Time Transfer)	Le protocole SRTP est une extension du profil audio/vidéo du protocole en temps réel (RTP) ; il assure l'intégrité des paquets RTP et du protocole de contrôle en temps réel (RTCP), fournissant l'authentification, l'intégrité et le chiffrement des paquets multimédia entre deux terminaux.	Les téléphones utilisent SRTP pour le chiffrement multimédia.
Protocole TCP (Transmission Control Protocol)	Le protocole TCP est un protocole de transport orienté connexion.	Les téléphones utilisent TCP pour se connecter à Cisco Unified Communications Manager et pour accéder aux services XML.

Protocole réseau	Objectifs	Notes sur l'utilisation
Transport Layer Security (Protocole TLS, Sécurité des couches de transport)	TLS est un protocole standard de sécurisation et d'authentification des communications.	Lorsque la sécurité est mise en œuvre, les téléphones utilisent le protocole TLS pour s'enregistrer de manière sécurisée auprès de Cisco Unified Communications Manager. Pour obtenir plus d'informations, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.
Protocole TFTP (Trivial File Transfer Protocol)	Le protocole TFTP permet de transférer des fichiers sur le réseau. Sur le téléphone, TFTP permet d'obtenir un fichier de configuration spécifique au type du téléphone.	Le protocole TFTP nécessite la présence d'un serveur TFTP sur le réseau ; ce serveur sera automatiquement identifié à partir du serveur DHCP. Si vous voulez qu'un téléphone utilise un autre serveur TFTP que celui qui est spécifié par le serveur DHCP, vous devez affecter manuellement l'adresse IP du serveur TFTP dans le menu Paramétrage réseau du 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.	Les téléphones émettent et reçoivent des flux RTP qui utilisent UDP.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page 12

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 12

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.

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).

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

Comportement du téléphone pendant les périodes de congestion du réseau

Tout élément susceptible de dégrader la performance du réseau risque d'affecter la qualité audio du téléphone, 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.

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.

SECTION II

Installation du téléphone

CHAPITRE 4

Installation des téléphones de conférence 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 12

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**.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page 12

Installation du téléphone de conférence

Après s'être connecté au réseau, le téléphone entame le processus de démarrage et s'enregistre auprès de Cisco Unified Communications Manager. Vous devez configurer les paramètres réseau sur le téléphone si vous désactivez 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.

Une fois que le téléphone se connecte, il détermine si une nouvelle version du micrologiciel doit être installée sur le téléphone.

Avant de commencer

Vérifiez que la dernière version du micrologiciel est installée sur votre Cisco Unified Communications Manager. Vérifiez ici la mise à jour des packages du périphérique :

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

Procédure

Étape 1 Choisissez la source d'alimentation du téléphone :

- PoE (Power over Ethernet)
- Un injecteur de courant pour téléphone Téléphone IP Cisco Unified

Pour plus d'informations, reportez-vous à Modes d’alimentation de votre téléphone de conférence , à la page 32.

Étape 2 Raccorder le téléphone au commutateur.

- Si vous utilisez PoE, branchez le câble Ethernet au port LAN et branchez l'autre extrémité au téléphone.
- Si vous utilisez l'injecteur de courant du Téléphone IP Cisco Unified, branchez l'injecteur au port LAN à l'aide d'un câble Ethernet. Reliez le cordon d'alimentation à l'injecteur et branchez le cordon d'alimentation dans une prise électrique. Utilisez un autre câble Ethernet pour connecter l'injecteur au téléphone de conférence.

Chaque téléphone est livré avec un câble Ethernet.

Étape 3 Suivez le processus de démarrage du téléphone. Cette étape permet de vérifier la bonne configuration du téléphone.

Étape 4 Si vous n'utilisez pas l'enregistrement automatique, configurez manuellement les paramètres de sécurité sur le téléphone.

Reportez-vous à Configurez les paramètres de sécurité., à la page 70.

Étape 5 Permettre au téléphone une mise à niveau vers l'image du micrologiciel actuel qui est stockée sur votre Cisco Unified Communications Manager.

Étape 6 Passez des appels à l'aide du téléphone pour vérifier le bon fonctionnement du téléphone et de ses fonctionnalités.

Étape 7 Indiquez aux utilisateurs finals comment utiliser leurs téléphones et comment en configurer les options. Cette étape garantit que les utilisateurs disposent des informations adéquates pour utiliser efficacement leurs téléphones Cisco.

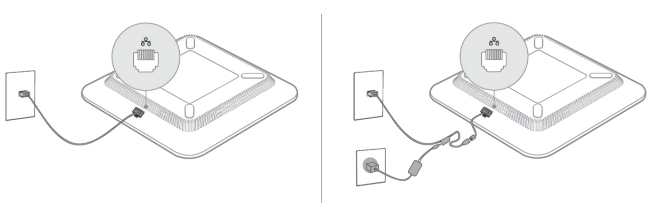
Modes d’alimentation de votre téléphone de conférence

Votre téléphone de conférence doit être alimenté à partir d'une de ces sources :

- Power over Ethernet (PoE), que fournit votre réseau.
- Un injecteur de courant pour téléphone IP Cisco.
- Un câble d'alimentation PoE et un amplificateur de puissance Cube 3.

L'illustration suivante montre le PoE et les options d'alimentation utilisant un câble d'alimentation PoE.

Illustration 2 : Options d'alimentation de téléphone de conférence



Configuration du téléphone à partir des menus de paramétrage

Le téléphone comprend de nombreux paramètres réseau configurables que vous devrez peut-être modifier pour que vos utilisateurs puissent se servir du téléphone. Vous pouvez accéder à ces paramètres et modifier certains d'entre eux, par le biais des menus du téléphone.

Le téléphone présente les menus de paramétrage suivants :

- Paramétrage réseau : fournit des options permettant d'afficher et de configurer divers paramètres réseau.
    - Paramétrage IPv4 : ce sous-menu fournit des options réseau supplémentaires.
    - Paramétrage IPv6 : ce sous-menu fournit des options réseau supplémentaires.
- Paramétrage de sécurité : fournit des options permettant d'afficher et de configurer divers paramètres de sécurité.

Remarque Vous pouvez contrôler si un téléphone a accès au menu Paramètres et aux options de ce menu. Utilisez le champ **Accès aux paramètres** de la Cisco Unified Communications Manager AdministrationFenêtre de configuration du téléphone pour contrôler l'accès. Le champ **Accès aux paramètres** accepte les valeurs suivantes :

- Activé : permet l'accès au menu Paramètres.
- Désactivé : empêche l'accès à la plupart des entrées du menu Paramètres. L'utilisateur peut toujours accéder à **Paramètres** > **État**.
- Restreint : permet l'accès aux éléments du menu Préférences utilisateur et État 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 admin., vérifiez le champ **Accès aux paramètres**.

Vous configurez les paramètres qui sont en affichage uniquement sur le téléphone dans Cisco Unified Communications Manager Administration.

Procédure

Étape 1 Appuyez sur **Applications** .

Étape 2 Appuyez sur **Paramètres**.

Étape 3 Sélectionnez **Paramètres admin**.

Étape 4 Saisissez un mot de passe si nécessaire, puis cliquez sur **Connexion**.

Étape 5 Sélectionnez **Paramétrage réseau** ou **Paramétrage de sécurité**.

Étape 6 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 7 Pour afficher un sous-menu, répétez l’étape 5.

Étape 8 Pour quitter un menu, appuyez sur **Préc**.

Rubriques connexes

Redémarrage ou réinitialisation du téléphone de conférence, à la page 143
Configuration des paramètres réseau, à la page 35
Configurez les paramètres de sécurité., à la page 70

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 menu sur le téléphone

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

- Utilisez les flèches du pavé de navigation pour mettre en surbrillance le champ que vous souhaitez modifier. Appuyez sur la touche **Sélectionner** du 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 de fonction si vous faites une erreur. Cette touche de fonction efface le caractère situé à gauche du curseur.
- Appuyez sur **Récup.** puis sur **Appliq.** pour annuler toutes les modifications que vous avez effectuées.
- Pour saisir un point (par exemple, dans une adresse IP), appuyez sur la touche ***** du clavier.
- 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

Redémarrage ou réinitialisation du téléphone de conférence, à la page 143
Appliquer un mot de passe à un téléphone, à la page 34

Configuration des paramètres réseau

Procédure

Étape 1 Appuyez sur **Paramètres**.

Étape 2 Sélectionnez **Paramètres admin** > **Paramétrage réseau**.

Étape 3 Définissez les champs comme indiqué dans Champs de configuration réseau, à la page 35.
Une fois que vous aurez défini les champs, vous devrez réinitialiser le téléphone.

Champs de configuration réseau

Le menu Configuration réseau contient les champs et sous-menus pour IPv4 et IPv6.

Pour modifier certains champs, vous devez arrêter DHCP.

Tableau 9 : Menu de configuration réseau

Entrée	Type	Par défaut	Description
Paramétrage IPv4	Menu		Reportez-vous au tableau « Sous-menu de la configuration IPv4 ». Cette option ne s'affiche que lorsque le mode IPv4 a été sélectionné ou en mode double pile.
Paramétrage IPv6	Menu		Reportez-vous au tableau « Sous-menu de la configuration IPv6 ».
Nom d'hôte	Chaîne		Nom d'hôte du téléphone. Si vous utilisez DHCP, ce nom est automatiquement attribué.

Entrée	Type	Par défaut	Description
Nom du domaine	Chaîne		Le nom du domaine DNS (Domain Name System) dans lequel le téléphone se situe. Pour modifier ce champ, désactivez DHCP.
ID VLAN opérationnel			Le réseau local virtuel (VLAN) qui est configuré sur un commutateur Catalyst Cisco dont le téléphone est membre.
ID VLAN admin.			Le VLAN auxiliaire dont le téléphone est membre.
Config. port de commut.	Négociation auto 10 Half 10 Full 100 Half 100 Full	Négociation auto	Débit et duplex du port de commutation, où : • 10 Half = 10-BaseT/half duplex • 10 Full = 10-BaseT/full duplex • 100 Half = 100-BaseT/half duplex • 100 Full = 100-BaseT/full duplex
LLDP-MED - Port logiciel	Désactivé Activé	Activé	Indique si LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery) est activé sur le port de commutation.

Tableau 10 : Sous-menu de configuration IPv4

Entrée	Type	Par défaut	Description
DHCP	Désactivé Activé	Activé	Active ou désactive l'utilisation du protocole DHCP.
Adresse IP			Adresse de protocole Internet version 4 (IPv4) du téléphone. Pour modifier ce champ, désactivez DHCP.
Masque de sous-réseau			Masque de sous-réseau utilisé par le téléphone. Pour modifier ce champ, désactivez DHCP.

Entrée	Type	Par défaut	Description
Routeur par défaut 1			Routeur par défaut utilisé par le téléphone. Pour modifier ce champ, désactivez DHCP.
Serveur DNS 1			Serveur du système de noms de domaine principal (DNS) (Serveur DNS 1) utilisé par le téléphone. Pour modifier ce champ, désactivez DHCP.
TFTP secondaire	Non Oui	Non	Indique si le téléphone utilise un autre serveur TFTP.
Serveur TFTP 1			Le serveur TFTP (Trivial File Transfer Protocol) principal utilisé par le téléphone. 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. Reportez-vous aux notes TFTP après la tableau final.

Entrée	Type	Par défaut	Description
Serveur TFTP 2			Serveur TFTP secondaire utilisé par le téléphone. 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 le fichier 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. Reportez-vous à la section des notes TFTP après la tableau final.
Libération adresse DHCP	Non Oui	Non	

Tableau 11 : Sous-menu de configuration IPv6

Entrée	Type	Par défaut	Description
DHCPv6 activé	Désactivé Activé	Activé	Active ou désactive l'utilisation du protocole DHCP IPv6.
Adresse IPv6			L'adresse IPv6 du téléphone. Pour modifier ce champ, désactivez DHCP.
Longueur du préfixe IPv6			Longueur de l'adresse IPv6. Pour modifier ce champ, désactivez DHCP.
Routeur IPv6 par défaut 1			Routeur IPv6 par défaut. Pour modifier ce champ, désactivez DHCP.
Serveur IPv6 DNS 1			Serveur DNS IPv6 principal Pour modifier ce champ, désactivez DHCP.
Autre TFTP IPv6	Non Oui	Non	Indique si le téléphone utilise un autre serveur TFTP IPv6.

Entrée	Type	Par défaut	Description
Serveur TFTP IPv6 1			Serveur TFTP IPv6 principal utilisé par le téléphone. Reportez-vous à la section des notes TFTP après ce tableau.
Serveur TFTP IPv6 2			Serveur TFTP IPv6 secondaire utilisé par le téléphone. Reportez-vous à la section des notes TFTP après ce tableau.
Adresse IPv6 libérée	Non Oui	Non	

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 va obtenir et utiliser 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 IPv6, reportez-vous à :

- « Configuration de périphérique commun » dans le *Guide des fonctionnalités et services de Cisco Unified Communications Manager*, au chapitre « Prise en charge IPv6 pour les périphériques Cisco Unified Communications ».
- *Guide de déploiement IPv6 des systèmes de collaboration Cisco version 12.0*, situé à l'adresse : https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html

Notes TFTP

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

Pour plus d'informations sur les fichiers CTL et ITL, consultez le *Guide de sécurité pour Cisco Unified Communications Manager*.

Vérification du bon démarrage du téléphone

Une fois que le téléphone est mis sous tension, il est soumis à un processus de diagnostic de démarrage.

Procédure

Allumez téléphone.

Lorsque l'écran principal s'affiche, il a démarré correctement.

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.

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

Installation du téléphone Cisco Unified Communications Manager

Configuration d'un téléphone de conférence IP Cisco

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

Pour obtenir des informations sur ces étapes, reportez-vous à la documentation de votre version 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
- L’adresse MAC : voir Détermination de l’adresse MAC du téléphone, à la page 48
- 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
- Numéro de répertoire (DN) à affecter au téléphone
- Utilisateur Cisco Unified Communications Manager à associer au téléphone.
- Informations sur l'utilisation du téléphone influant sur le modèle de touches programmables, les fonctionnalités, les services téléphone IP ou les applications du téléphone

Pour plus d'informations, consultez la documentation relative à votre version particulière de Cisco Unified Communications Manager et consultez les liens connexes.

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

Pour obtenir plus d'informations, reportez-vous à l’accord de licence relatif à votre version de Cisco Unified Communications Manager.

Étape 3 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 et le modèle de touches programmables.

Étape 4 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 5 Définissez un espace de restriction d'appels. Dans Cisco Unified Communications Manager Administration, cliquez sur **Call Routing (Routage d'appels)** > **Class of Control (Classe de contrôle)** > **Calling Search Space (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 6 Configurez un profil de sécurité pour le protocole et le type du périphérique. Sélectionnez **Système** > **Sécurité** > **Profil de sécurité du téléphone**.

Étape 7 Configurez le téléphone. Sélectionnez **Périphérique** > **Téléphone**.

a) Recherchez le téléphone à modifier, ou ajoutez un nouveau téléphone.
b) Configurez le téléphone en renseignant les champs obligatoires dans le volet Info. Périphérique de la fenêtre de configuration du téléphone.
    - Adresse MAC (requise) : vérifiez que la valeur comprend 12 caractères hexadécimaux.
    - Description : saisissez un texte descriptif qui pourra vous aider à rechercher des informations sur cet utilisateur.
    - Pool de périphériques (requis) :
    - Profil de téléphone commun
    - Espace de restriction d'appels
    - Emplacement

- Propriétaire (utilisateur ou anonyme), et si l'utilisateur est sélectionné, l'ID utilisateur du propriétaire

Le périphérique est ajouté dans la base de données Cisco Unified Communications Manager, ainsi que ses paramètres par défaut.

Pour obtenir des informations sur les champs de configuration spécifique au produit, reportez-vous au bouton « ? » Aide du bouton de la fenêtre Configuration du téléphone et le lien associé.

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.

c) Dans la fenêtre Protocol Specific Information (Informations spécifiques au protocole), choisissez un profil de sécurité de périphérique et définissez le mode de sécurité.

Remarque Choisissez un profil de sécurité conforme à la stratégie de sécurité générale de l'entreprise. Si le téléphone ne prend pas en charge la sécurité, choisissez un profil non sécurisé.

d) Dans la zone Extension Information (Informations sur le poste), cochez la case Enable Extension Mobility (Activer la mobilité des postes) si le téléphone prend en charge Cisco Extension Mobility.
e) Cliquez sur **Enregistrer**.

Étape 8 Sélectionnez **Périphérique** > **Paramètres du périphérique** > **Profil SIP** pour configurer des paramètres SIP.

Étape 9 Sélectionnez **Périphérique** > **Téléphone** pour configurer les numéros de répertoire (lignes) du téléphone, en renseignant les champs requis dans la fenêtre Directory Number Configuration (Configuration des numéros de répertoire).

a) Recherchez le téléphone.
b) Dans le volet gauche de la fenêtre de configuration du téléphone, cliquez sur Ligne 1.

   Les téléphones de conférence ne comportent qu'une seule ligne.

c) Dans le champ N° d'annuaire, saisissez un numéro valide pouvant être composé.

Remarque Ce champ doit contenir le même numéro que celui affiché dans le champ Numéro de téléphone de la fenêtre End User Configuration (Configuration de l'utilisateur final).

d) Dans la liste déroulante Route Partition (Partition de routage), choisissez la partition dont le numéro de répertoire est membre. Si vous ne souhaitez pas restreindre l'accès au numéro de répertoire, choisissez <None> (Aucune) pour la partition.
e) Dans la zone de liste déroulante Espace de restriction d'appels, choisissez l'espace de restriction d'appels approprié. La valeur que vous sélectionnez s'appliquera à tous les périphériques qui utilisent ce numéro de répertoire.
f) Dans la zone Call Forward and Call Pickup Settings (Paramètres de renvoi et d'interception d'appels), sélectionnez les éléments (par exemple, Forward All (Renvoyer tout), Forward Busy Internal (Renvoi en interne si occupé)) et les destinations correspondantes auxquelles les appels seront renvoyés.

Exemple :

Pour que les appels entrants externes et internes qui reçoivent un signal d'occupation soient renvoyés à la messagerie vocale de la ligne, cochez la case Messagerie vocale située en regard des éléments Forward Busy Internal (Renvoi en interne si occupé) et Forward Busy External (Renvoi en externe si occupé), dans la colonne gauche de la zone Call Pickup and Call Forward Settings (Paramètres de renvoi et d'interception d'appels).

g) Pour la Ligne 1 dans le volet Périphérique, configurez les champs suivants :

- Display (champ Internal Caller ID) (Afficher - champ ID de l’appelant interne) : vous pouvez saisir le prénom et le nom de l’utilisateur de ce périphérique, afin que ce nom soit affiché pour tous les appels internes. Laissez ce champ vide si vous voulez que le système affiche le numéro de poste du téléphone.
- External Phone Number Mask (Masque du numéro de téléphone externe) : indique le numéro de téléphone (ou le masque) qui est utilisé pour envoyer les informations concernant l’ID de l’appelant lorsqu'un appel est passé sur cette ligne. Vous pouvez saisir un maximum de 24 caractères numériques et la lettre « X ». Les X représentent le numéro de répertoire et doivent apparaître à la fin du masque.

Exemple :

Si vous spécifiez le masque 408902XXXX, le numéro d’ID d’appelant 4089026640 sera affiché pour un appel externe passé sur le numéro de poste 6640.

Ce paramètre ne s'applique qu’au périphérique actuel, sauf si vous cochez la case située à droite (Update Shared Device Settings, Mettre à jour les paramètres de périphérique partagés) et si vous cliquez sur **Propagate Selected** (Propager la sélection). La case à cocher située à droite n’est affichée que si d’autres périphériques partagent ce numéro de répertoire.

h) Sélectionnez **Enregistrer**.

Pour obtenir plus d'informations sur les numéros de répertoire, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager et aux liens connexes.

Étape 10 (facultatif) Associez l’utilisateur à un téléphone. Cliquez sur **Associate End Users** (Associer des utilisateurs finals), dans la partie inférieure de la fenêtre de configuration du téléphone, pour associer un utilisateur à la ligne configurée.

a) Utilisez **Find** (Rechercher) avec les champ de recherche pour localiser l’utilisateur.
b) Cochez la case située près du nom de l'utilisateur, puis cliquez sur **Add Selected** (Ajouter la sélection).

Le nom et l’ID utilisateur de l’utilisateur apparaissent dans le volet Users Associated With Line (Utilisateurs associés à la ligne) de la fenêtre Directory Number Configuration (Configuration des numéros de répertoire).

c) Sélectionnez **Enregistrer**.

L’utilisateur est dorénavant associé à la Ligne 1 du téléphone.

Étape 11 (facultatif) Associez l’utilisateur à ce périphérique :

a) Choisissez **Gestion des utilisateurs** > **Utilisateur final**.
b) Utilisez les zones de recherche et la commande **Find** (Rechercher) pour localiser l’utilisateur que vous avez ajouté.
c) Cliquez sur l’ID utilisateur.
d) Dans la zone Directory Number Associations (Associations de numéros de répertoire), définissez le numéro de poste principal dans la zone de liste déroulante.
e) (facultatif) Dans la zone Mobility Information (Informations sur la mobilité), cochez la case Enable Mobility (Activer la mobilité).
f) Dans la zone Permissions Information (Informations sur les autorisations), utilisez les bouton **Add to Access Control Group** (Ajouter au groupe de contrôle d'accès) pour ajouter cet utilisateur à n’importe quel groupe d’utilisateurs.

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

g) Pour afficher les détails concernant un groupe, sélectionnez le groupe et cliquez sur **Détails**.
h) Dans la zone Mobilité de poste, cochez la case Enable Extension Mobility Cross Cluster (Activer Extension Mobility Cross Cluster) si l'utilisateur peut utiliser le service Extension Mobility Cross Cluster.
i) Dans la zone Informations sur le périphérique, cliquez sur **Device Associations** (Associations de périphériques).
j) Utilisez les champs de recherche et la commande **Find** (Rechercher) pour localiser le périphérique à associer à l'utilisateur.
k) Sélectionnez le périphérique, puis cliquez sur **Save Selected/Changes** (Enregistrer la sélection/les modifications).
l) Cliquez sur **Aller** près du lien apparenté « Back to User » (Retour à l'utilisateur) dans l'angle supérieur droit de l'écran.
m) Sélectionnez **Enregistrer**.

Étape 12 Personnalisez les modèles de touches programmables. Sélectionnez **Périphérique** > **Paramètres du périphérique** > **Softkey Template** (Modèle de touche programmable).

Utilisez la page pour ajouter, supprimer ou modifier l'ordre des fonctionnalités de touche programmable affichées sur le téléphone de l'utilisateur, selon les besoins.

Le téléphone de conférence possède des exigences de touches programmables spécifiques. Consultez les liens connexes pour plus d'informations.

Étape 13 Configurez les services du téléphone IP Cisco et affectez les services. Sélectionnez **Périphérique** > **Paramètres du périphérique** > **Services téléphoniques**.

Fournit des services de téléphonie IP au téléphone.

Remarque Les utilisateurs peuvent ajouter des services sur leur téléphone ou modifier ces services dans le portail d'aide en libre-service de Cisco Unified Communications.

Étape 14 (facultatif) Ajoutez des informations utilisateur dans le répertoire global de Cisco Unified Communications Manager. Sélectionnez **User Management (Gestion des utilisateurs)** > **Utilisateur final**, puis cliquez sur **Ajouter nouveau** et configurez les champs requis. Les champs obligatoires sont indiqués par un astérisque (*).

Remarque Si votre société utilise un annuaire LDAP (Lightweight Directory Access Protocol) pour stocker des informations sur les utilisateurs, vous pouvez installer et configurer Cisco Unified Communications afin qu'il utilise l'annuaire LDAP actuel ; reportez-vous à Configuration du répertoire d'entreprise, à la page 111. Une fois que le champ Enable Synchronization from the LDAP Server (Activer la synchronisation sur le serveur LDAP) est activé, vous ne pouvez plus ajouter d'autres utilisateurs à partir de Cisco Unified Communications Manager Administration.

a) Définissez les champs ID utilisateur et Nom.
b) Affectez un mot de passe (pour le portail d'aide en libre-service).
c) Affectez un code PIN (pour Cisco Extension Mobility et le répertoire personnel).
d) Associez l'utilisateur à un téléphone.

Donne aux utilisateurs le contrôle sur leur téléphone, en leur permettant de renvoyer des appels ou d'ajouter des numéros abrégés ou des services.

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

Étape 15 (facultatif) Associez un utilisateur à un groupe d’utilisateurs. Sélectionnez **User Management (Gestion des utilisateurs)** > **User Settings (Paramètres utilisateur)** > **Access Control Group (Accès au groupe de contrôle)**.

Affecte aux utilisateurs une liste commune de rôles et d'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.

Pour que les utilisateurs finals puissent accéder au portail d’aide en libre-service de Cisco Unified Communications, vous devez les ajouter au groupe d’utilisateurs standard de Cisco Communications Manager.

Rubriques connexes

Caractéristiques et configuration des téléphones de conférence IP Cisco, à la page 77
Configuration spécifique au produit, à la page 82
Documentation des Cisco Unified Communications Manager, à la page 12
Configuration d’un nouveau modèle de touches programmables, à la page 78

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, sélectionnez **Paramètres** > **Informations sur le téléphone**, puis 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 48.

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

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page 12

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 12

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 12

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 51.

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 12

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).

Surviveable Remote Site Telephony (SRST)

Le mode Surviveable Remote Site Telephony (SRST) garantit que les fonctions du téléphone restent accessibles en cas d'interruption des communications avec l'instance Cisco Unified Communications Manager qui a le contrôle. 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 obtenir des informations sur la solution SRST, reportez-vous à http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/tsd-products-support-series-home.html

Le tableau suivant présente les fonctionnalités disponibles pendant le basculement.

Tableau 12 : 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	

Fonctionnalité	Prise en charge	Remarques
Mettre en attente	Oui	
Reprise	Oui	
Conférence	Oui	Uniquement à 3 voies et mixage local seulement.
Liste des conférences	Non	
Transfert	Oui	Consultation seulement.
Transfert sur appels actifs (Transfert direct)	Non	
Réponse automatique	Oui	
Appel en attente	Oui	
Afficher l'ID de l'appelant	Oui	
Présentation de la session Unified	Oui	La conférence est la seule fonctionnalité prise en charge, en raison des limitations liées aux autres fonctionnalités.
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	
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.

Fonctionnalité	Prise en charge	Remarques
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.
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.
Intrcpt	Non	La touche ne s'affiche pas.
Interception d'appels de groupe	Non	La touche ne s'affiche pas.
Autre interception	Non	La touche ne s'affiche pas.
ID des appels malveillants	Non	La touche ne s'affiche pas.
QRT	Non	La touche ne s'affiche pas.
Groupe de recherche	Non	La touche ne s'affiche pas.
Mobilité	Non	La touche ne s'affiche pas.
Confidentialité	Non	La touche ne s'affiche pas.
Rappel automatique	Non	La touche Rappel ne s'affiche pas.
URL de service	Oui	La touche de ligne programmable avec une URL de service assignée ne s'affiche pas.

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 12

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 des téléphones

CHAPITRE 7

Sécurité du Téléphone de conférence IP Cisco

Présentation de la sécurité du téléphone IP Cisco

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.

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

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

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

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.

Le téléphone de conférence IP Cisco série 7832 est conforme à la norme Federal Information Processing Standard (FIPS). Pour fonctionner correctement, le mode FIPS nécessite une taille de clé RSA de 2048 bits ou plus. Si le certificat de serveur RSA 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.

Vous ne pouvez pas utiliser des clés privées (certificat valable localement, LSC, ou MIC) en mode FIPS.

Si le téléphone a un certificat valable localement (LSC) existant qui est inférieur à 2048 bits, vous devez mettre à jour la taille de clé du certificat LSC à une valeur égale ou supérieure à 2048 bits avant d'activer FIPS.

Rubriques connexes

Configuration d’un certificat localement important, à la page 71
Documentation des Cisco Unified Communications Manager, à la page 12

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).
- *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.

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.

Le tableau suivant présente une vue d'ensemble des fonctionnalités de sécurité prises en charge sur les téléphones de conférence IP Cisco 7832. Pour obtenir plus d'informations sur ces fonctionnalités, sur Cisco Unified Communications Manager et sur la sécurité des téléphones IP Cisco, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Tableau 13 : Vue d'ensemble des fonctionnalités de sécurité

Fonctionnalité	Description
Authentification de l'image	Des fichiers binaires signés (dotés de l'extension .sbn) empêch un téléphone. La modification de l'image entraînerait l'échec c
Installation de certificats sur le site du client	Un certificat unique doit être affecté à chaque téléphone pour l installé en usine (MIC), mais pour plus de sécurité, vous pouve certificat doit être installé à l'aide de la fonction proxy d'autorité (LSC) à partir du menu Paramétrage de sécurité du téléphone.
Authentification du périphérique	A lieu entre le serveur Cisco Unified Communications Manag Détermine si une connexion sécurisée peut être établie entre le crée un chemin de signalement sécurisé entre ces entités grâce les téléphones qui ne peuvent pas être authentifiés par le serve
Authentification des fichiers	Valide les fichiers signés numériquement qui ont été téléchargé n'ont pas été modifiés après leur création. Les fichiers qui ne p téléphone. Le téléphone rejette ces fichiers, sans traitement sup
Authentification de la signalisation	Utilise le protocole TLS pour vérifier que les paquets de signa
Certificat installé en usine	Chaque téléphone contient un certificat unique installé en usin MIC est la preuve unique et permanente de l'identité du téléph téléphone.
Référence SRST sécurisée	Un fois que vous avez configuré une référence SRST pour la s Communications Manager Administration, le serveur TFTP aj au téléphone. Un téléphone sécurisé utilise alors une connexio

Fonctionnalité	Description
Chiffrement multimédia	Utilise SRTP pour assurer que les flux multimédia entre les reçoit et lit les données. Implique la création d'une paire de périphériques, et la sécurisation de la remise des clés penda
CAPF (fonction proxy de l'autorité de certification)	Met en œuvre des parties de la procédure de génération de avec le téléphone pour générer des clés et pour installer des du téléphone, des certificats provenant d'autorités de certifi
Profils de sécurité	Détermine si le téléphone n'est pas sécurisé, s'il est authent
Fichiers de configuration chiffrés	Permettent d'assurer la confidentialité des fichiers de confi
Désactivation facultative de la fonctionnalité de serveur Web d'un téléphone	Vous pouvez empêcher l'accès à la page Web d'un télépho
Renforcement de la sécurité du téléphone	Options de sécurité supplémentaires, paramétrables depuis • Désactivation de l'accès aux pages Web d'un téléphon **Remarque** Vous pouvez afficher les paramètres actuels de téléphone.
Authentification 802.1x	Le téléphone peut utiliser l'authentification 802.1X pour d

Chiffrement AES 256	S'ils sont connectés à Cisco Unified Communications Man AES 256 pour TLS et SIP lors du chiffrement du signaleme des connexions TLS 1.2 à l'aide de codes AES-256 confor fédérales de traitement d'informations (FIPS). Les nouveau
	• Pour les connexions TLS :
	  • TLS_ECDHE_RSA_WITH_AES_256_GCM_S
	  • TLS_ECDHE_RSA_WITH_AES_128_GCM_S
	• Pour sRTP :
	  • AEAD_AES_256_GCM
	  • AEAD_AES_128_GCM
	Pour plus d'informations, reportez-vous à la documentation

Certificats ECDSA (Elliptic Curve Digital Signature Algorithm)	Dans le cadre de la certification de critères communs (CC) version 11.0. Cela affecte tous les produits de système d'expl 11.5 et versions ultérieures.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page 12

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 sont pris en charge entre deux téléphones. Les conférences sécurisées, la mobilité des numéros de poste de Cisco et les lignes partagées peuvent être configurées par un pont de conférence sécurisé.

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 14 : 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 respec le niveau de sécurité, appel`
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.

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.

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 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.
- 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.
- Configurer le VLAN voix : la norme 802.1x ne prenant pas en considération les 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 multi-domaine, vous pouvez continuer d'utiliser le VLAN voix.
- Désactivé : si le commutateur ne prend pas en charge l'authentification multi-domaine, désactivez le VLAN voix et envisagez d'attribuer le port au VLAN natif.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page 12

Affichage des fonctionnalités de sécurité actuelles sur le téléphone

Pour obtenir plus d'informations sur les fonctionnalités, sur Cisco Unified Communications Manager et sur la sécurité des téléphones IP Cisco, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Procédure

Étape 1 Sélectionnez **Paramètres**.

Étape 2 Sélectionnez **Paramètres admin.** > **Paramétrage de sécurité**.

La plupart des fonctionnalités de sécurité ne sont disponibles que si une liste de confiance des certificats (CTL) est installée sur le téléphone.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page 12

Affichage des profils de sécurité

Tous les téléphones IP Cisco prenant en charge Cisco Unified Communications Manager utilisent un profil de sécurité, qui définit si le téléphone est authentifié, chiffré ou non sécurisé. Pour obtenir des informations sur la configuration d'un profil de sécurité et de son application sur le téléphone, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Système** > **Sécurité** > **Profil de sécurité du téléphone**.

Étape 2 Examinez le paramètre Mode de sécurité.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page 12

Configurez les paramètres de sécurité.

Procédure

Étape 1 Appuyez sur **Paramètres**.

Étape 2 Sélectionnez **Paramètres admin.** > **Paramétrage de sécurité**.

Étape 3 Définissez les champs.
Une fois que vous aurez défini les champs, vous devrez réinitialiser le téléphone.

Champs de configuration de la sécurité

Le menu Paramétrage de sécurité contient les champs et les sous-menus pour les listes de confiance et d'authentification 802.1x.

Tableau 15 : Menu Paramétrage de sécurité

Entrée	Type	Par défaut	Description
Mode de sécurité			Lecture seule
LSC			Reportez-vous à Configuration d'un certificat localement important, à la page 71.
Liste de confiance	Menu		Reportez-vous au tableau « Sous-menu de la liste de confiance ».
Authentification 802.1x	Menu		Reportez-vous au tableau « Sous-menu d'authentification 802.1x ».

Tableau 16 : Sous-menu Liste de confiance

Entrée	Type	Par défaut	Description
Fichier CTL	Menu		Affiche une liste des fichiers CTL.
Fichier ITL	Menu		Affiche une liste des fichiers ITL.
Configuration (signée)	Menu		Reportez-vous au tableau « Sous-menu de la liste de confiance ».

Tableau 17 : Sous-menu de configuration

Entrée	Type	Par défaut	Description
Routeur SRST			Affiche l'adresse IP du SRST.

Tableau 18 : Sous-menu Authentification 802.1x

Entrée	Type	Par défaut	Description
Authentification du périphérique	Désactivé Activé	Désactivé	
État transaction	Sous-menu		Reportez-vous au tableau « Sous-menu de l'état des transactions ».

Tableau 19 : Sous-menu de l'état des transactions

Entrée	Type	Par défaut	Description
État transaction	Déconnecté Connecté		
Protocoles			Liste des protocoles.

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 À partir du téléphone, choisissez **Paramètres** .

Étape 4 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 5 Sélectionnez **LSC** et appuyez sur **Sélect.** ou sur **MàJ**.

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

Étape 6 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.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page 12

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.

CHAPITRE 8

Personnalisation du téléphone de conférence IP Cisco

Sonneries de téléphone personnalisées

Le téléphone IP Cisco est livré avec deux sonneries par défaut incluses dans le matériel : Compression d'impulsions1 et Compression d'impulsions2. 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 (MIC). Les fichiers MIC, ainsi qu’un fichier 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 la mauvaise casse pour écrire le nom du fichier, le téléphone n’appliquera pas vos changements.

Pour plus d'informations, consultez le chapitre « Personnaliser les sonneries et les fonds d'écran du téléphone », du Guide de Configuration des fonctionnalités de Cisco Unified Communications Manager.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page 12

Configuration d'une sonnerie personnalisée

Procédure

Étape 1 Créez un fichier MIC pour chaque sonnerie personnalisée (une sonnerie par fichier).

Vérifiez que les fichiers MIC respectent les directives relatives au format stipulées à la section Formats de fichiers de sonneries personnalisées.

Étape 2 Téléchargez les nouveaux fichiers MIC que vous avez créés sur le serveur TFTP Cisco de chaque instance de Cisco Unified Communications Manager dans votre cluster.

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

Étape 3 Utilisez un éditeur de texte pour modifier le fichier Ringlist-wb.

Reportez-vous à la section « Formats de fichiers de sonneries personnalisées » pour savoir comment formater ce fichier et pour voir un exemple de fichier Ringlist-wb.

Étape 4 Enregistrez vos modifications et fermez le fichier Ringlist-wb.

Étape 5 Pour mettre en cache le nouveau fichier Ringlist.-wb :

- Arrêtez et redémarrez le service TFTP à l'aide de Cisco Unified Serviceability
- Désactivez et réactivez le paramètre de service TFTP « Activer la mise en cache des fichiers de constantes et des fichiers Bin au démarrage », situé dans la zone Paramètres de Service avancés.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page 12

Formats de fichiers de sonneries personnalisées

Le fichier Ringlist-wb.xml définit un objet XML qui contient une liste de sonneries de téléphone. Ce fichier peut contenir jusqu'à 50 types de sonneries. Chaque type de sonnerie contient un pointeur vers le fichier MIC utilisé pour ce type de sonnerie, ainsi que le texte qui apparaît dans le menu Type de sonnerie du téléphone IP Cisco pour cette sonnerie. Ce fichier est hébergé sur le serveur Cisco TFTP de chaque instance de Cisco Unified Communications Manager.

L'objet XML CiscoIPPhoneRinglist utilise l'ensemble de balises simples suivant pour décrire les informations :

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

Les caractéristiques suivantes s'appliquent aux noms de définition. Vous devez inclure les champs DisplayName et FileName pour chaque type de sonnerie de téléphone, car ils sont nécessaires.

- Le champ DisplayName correspond au nom de la sonnerie personnalisée du fichier PCM associé, affiché dans le menu Type de sonnerie du téléphone IP Cisco.
- Le champ FileName correspond au nom du fichier MIC de la sonnerie personnalisée à associer au nom d'affichage.

Remarque Les champs DisplayName et FileName ne doivent pas comprendre plus de 25 caractères.

L'exemple suivant illustre un fichier Ringlist-wb.xml définissant deux types de sonnerie de téléphone :

```
<CiscoIPPhoneRingList>
 <Ring>
```

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

Les fichiers MIC correspondant aux sonneries doivent respecter les exigences suivantes pour pouvoir être lus correctement sur les téléphones IP Cisco :

- MIC brut (sans en-tête)
- 8 000 échantillons par seconde ;
- 8 bits par échantillon ;
- compression Mu-law ;
- taille maximale de la sonnerie : 16 080 échantillons ;
- taille minimale de la sonnerie : 240 échantillons ;
- nombre d'échantillons dans la sonnerie = multiple de 240.
- La sonnerie doit débuter et se terminer au point zéro.

Pour créer des fichiers MIC pour des sonneries de téléphone personnalisées, utilisez n'importe quel package d'édition audio prenant en charge ces exigences relatives au format de fichier.

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

Caractéristiques et configuration des téléphones de conférence IP Cisco

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

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

Configuration d'un nouveau modèle de touches programmables

Vous devez ajouter des touches programmables à un modèle de touches programmables pour permettre aux utilisateurs d'accéder à certaines fonctionnalités. Par exemple, si vous souhaitez que les utilisateurs puissent utiliser Ne pas déranger, vous devez activer la touche programmable. Pour obtenir plus d'informations, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Vous souhaitez créer plusieurs modèles. Par exemple, vous pouvez souhaiter avoir un modèle pour téléphone de salle de conférence et un autre modèle pour un téléphone de bureau de cadre.

Cette procédure présente les étapes pour créer un nouveau modèle de touche programmable et l'affecter à un téléphone en particulier. De même que d'autres fonctionnalités du téléphone, vous pouvez également utiliser le modèle pour les téléphones de conférence ou 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** > **Softkey Template** (Modèle de touche programmable).

Étape 3 Cliquez sur **Rechercher**.

Étape 4 Sélectionnez l'une des options suivantes :

- Cisco Unified Communications Manager 11.5 et versions précédentes :**Utilisateur standard**
- Cisco Unified Communications Manager 12.0 et versions ultérieures :**Utilisateur de conférence personnelle** ou **utilisateur de conférence publique**.

Étape 5 Cliquez sur **Copier**.

Étape 6 Modifiez le nom du modèle.

Par exemple, le modèle de salle de conférence 7832.

Étape 7 Cliquez sur **Enregistrer**.

Étape 8 Accédez à la page **Configurer la disposition de la touche programmable** dans le menu supérieur droit.

Étape 9 Pour chaque état d'appel, configurez les fonctions à afficher.

Étape 10 Cliquez sur **Enregistrer**.

Étape 11 Revenez à **l'écran de Liste/Recherche** dans le menu supérieur droit.

Vous verrez votre nouveau modèle dans la liste des modèles.

Étape 12 Sélectionnez **Périphérique** > **Téléphone**.

Étape 13 Recherchez le téléphone auquel appliquer le nouveau modèle et sélectionnez-le.

Étape 14 Dans le champ **modèle de touche programmable**, sélectionnez le nouveau modèle de touche programmable.

Étape 15 Cliquez sur **Enregistrer** et **Appliquer la configuration**.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page 12

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. Le téléphone IP gère chaque service comme une application distincte.

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 Présentation du portail d'aide en libre-service, à la page 57 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 12

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.

Rubriques connexes

Configurer des informations d'authentification permanentes pour la connexion à Expressway, à la page 108

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.

Rubriques connexes

Configuration spécifique au produit, à la page 82

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.

Rubriques connexes

Configuration spécifique au produit, à la page 82

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.

Rubriques connexes

Configuration spécifique au produit, à la page 82

Configuration spécifique au produit

Le tableau suivant décrit les champs dans le volet de Configuration spécifique au produit. Certains champs de ce tableau n'apparaissent que sur la page **Périphérique** > **Téléphone**.

Tableau 20 : Champs de configuration spécifique au produit

Nom du champ	Type de champ ou choix	Par défaut	Description
Accès aux paramètres	Désactivé Activé Restreint	Activé	Active, désactive ou restreint l'accès aux paramètres de configuration régionaux au sein du menu Paramètres. Avec l'accès restreint, les menus Préférences et État sont accessibles. Avec l'accès désactivé, le menu État peut être consulté.
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.
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.

Nom du champ	Type de champ ou choix	Par défaut	Description
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 de rétroéclairage inactif	Jours de la semaine		Définit les jours où le rétro-éclairage ne s'allume pas automatiquement à l'heure spécifiée dans le champ Heure d'activation du rétro-éclairage. Sélectionnez un ou plusieurs jours dans la liste déroulante. Pour choisir plusieurs jours, maintenez la touche **Crtl enfoncée et cliquez** sur les jours souhaités. Reportez-vous à Planification du mode Économies d'énergie pour un téléphone IP Cisco, à la page 95.
Heure d'activité du rétroéclairage	hh:mn	07:30	Définit l'heure à laquelle le rétro-éclairage est automatiquement activé tous les jours (sauf les jours indiqués dans le champ Jours d'inactivité du rétro-éclairage). Entrez l'heure dans ce champ au format 24 heures ; 00:00 correspondant à minuit. Par exemple, pour allumer automatiquement le rétroéclairage à 7 heures du matin, saisissez 07:00. Par exemple, pour activer le rétro-éclairage à 14 h 00 (14h00), saisissez 14h00. Si ce champ est vide, le rétro-éclairage s'allume automatiquement à 0:00. Reportez-vous à Planification du mode Économies d'énergie pour un téléphone IP Cisco, à la page 95.

Nom du champ	Type de champ ou choix	Par défaut	Description
Durée d'activité du rétroéclairage	hh:mn	10:30	Définit la durée pendant laquelle le rétro-éclairage reste allumé après s'être activé à l'heure spécifiée par le champ Heure d'activation du rétro-éclairage. Par exemple, pour que le rétro-éclairage 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 du rétro-éclairage est égale à 0:00 et la durée de rétroéclairage est vide (ou égale à 24:00), le rétroéclairage ne s'éteint pas. Reportez-vous à Planification du mode Économies d'énergie pour un téléphone IP Cisco, à la page 95.
Délai avant inactivité du rétroéclairage	hh:mn	1:00	Définit la durée pendant laquelle le téléphone est inactif avant l'extinction du rétro-éclairage. S'applique uniquement lorsque le rétro-éclairage 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). Par exemple, pour éteindre le rétro-éclairage lorsque le téléphone est inactif pendant 1 heure et 30 minutes après qu'un utilisateur a allumé le rétro-éclairage, saisissez 01:30. Reportez-vous à Planification du mode Économies d'énergie pour un téléphone IP Cisco, à la page 95.
Rétroécl. activé lors d'un appel entrant	Désactivé Activé	Activé	Allume le rétro-éclairage lorsqu'il y a un appel entrant.

Nom du champ	Type de champ ou choix	Par défaut	Description
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. Reportez-vous à Planifier EnergyWise sur le téléphone IP Cisco, à la page 96.

Nom du champ	Type de champ ou choix	Par défaut	Description
Heure d'activation du téléphone	hh:mn	00:00	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. Reportez-vous à Planifier EnergyWise sur le téléphone IP Cisco, à la page 96.
Heure de désactivation du téléphone	hh:mn	24:00	Définit 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. 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. Reportez-vous à Planifier EnergyWise sur le téléphone IP Cisco, à la page 96.

Nom du champ	Type de champ ou choix	Par défaut	Description
Phone Off Idle Timeout (Délai d'inactivité avant désactivation)	mm	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. Reportez-vous à Planifier EnergyWise sur le téléphone IP Cisco, à la page 96.
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. Reportez-vous à Planifier EnergyWise sur le téléphone IP Cisco, à la page 96.
Domaine EnergyWise	Jusqu'à 127 caractères.		Identifie le domaine EnergyWise dans lequel le téléphone se situe. Reportez-vous à Planifier EnergyWise sur le téléphone IP Cisco, à la page 96.
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. Reportez-vous à Planifier EnergyWise sur le téléphone IP Cisco, à la page 96.

Nom du champ	Type de champ ou choix	Par défaut	Description
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. Reportez-vous à Planifier EnergyWise sur le téléphone IP Cisco, à la page 96.

Nom du champ	Type de champ ou choix	Par défaut	Description
Stratégie de jointure et de transfert direct	Même ligne activé Désactiver la même ligne	Même ligne activé	Contrôle la possibilité d'un utilisateur de joindre et transférer des appels. • Activer la même ligne : les utilisateurs peuvent transférer ou joindre directement un appel sur la ligne en cours vers un autre appel sur la même ligne. • Désactiver la même ligne : 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.
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.
Temporisation de la touche "autres"	Nombre entier de 0, ou de 5 à 30 secondes	5	Contrôle la durée pendant laquelle une ligne de touches programmables secondaires est affichée avant que le téléphone n'affiche le jeu initial de touches programmables. 0 désactive la minuterie.
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>`** Reportez-vous à Contrôle des informations de débogage à l'aide de Cisco Unified Communications Manager, à la page 163.
Journal à distance	Désactivé Activé	Désactivé	Contrôle la possibilité d'envoyer des journaux au serveur syslog. Reportez-vous à Contrôle des informations de débogage à l'aide de Cisco Unified Communications Manager, à la page 163.

Nom du champ	Type de champ ou choix	Par défaut	Description
Consigner le profil	Par défaut Préréglage Téléphonie SIP UI Réseau Support Mise à niveau Accessoire Sécurité EnergyWise MobileRemoteAccess	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 • Energywise : enregistre des informations relatives aux économies d'énergie • MobileRemoteAccess : enregistre des informations relatives à Mobile and Remote Access Through Expressway. Reportez-vous à Contrôle des informations de débogage à l’aide de Cisco Unified Communications Manager, à la page 163.
Serveur de journaux IPv6	Chaîne de 256 caractères maximum		Identifie le serveur Syslog IPv6 pour la sortie de débogage du téléphone. Reportez-vous à Contrôle des informations de débogage à l’aide de Cisco Unified Communications Manager, à la page 163.
Protocole CDP (Cisco Discovery Protocol) - port commuté	Désactivé Activé	Activé	Contrôle du protocole de découverte Cisco sur le téléphone.

Nom du champ	Type de champ ou choix	Par défaut	Description
Protocole LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Discover) : port commuté	Désactivé Activé	Activé	Active LLDP-MED sur le port de commutation.
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.
Energy Efficient Ethernet (EEE) : Switch Port (Optimisation énergétique d'Ethernet : Port de commutation)	Désactivé Activé	Désactivé	Contrôle EEE sur le port de commutation.
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 Désactivé Activé	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.
Configuration à distance du port de commutation	Désactivé Négociation auto 10 Half 10 Full 100 Half 100 Full	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.
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).

Nom du champ	Type de champ ou choix	Par défaut	Description
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 journal d'appel à partir d'une ligne partagée 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.
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.

Nom du champ	Type de champ ou choix	Par défaut	Description
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.
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. Les valeurs valides spécifient Normal (la détection d'un échec de connexion Unified CM se produit à la vitesse standard du système) ou Différé (la détection d'un basculement de connexion Unified CM se produit environ quatre fois moins vite qu'avec Normal). Pour que les échecs de connexion à Unified CM soient identifiés plus rapidement, choisissez Normale. Si vous préférez que le basculement soit légèrement différé, afin que le système puisse tenter de rétablir automatiquement la connexion, choisissez Différé. La différence de temps exacte entre la détection Normale et la détection Différée des échecs de connexion dépend de nombreuses variables qui changent constamment.
ID de spécification spéciale	Chaîne		Contrôle des fonctions personnalisées à partir des charges spéciales Engineering (ES).
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.

Nom du champ	Type de champ ou choix	Par défaut	Description
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 souhaitez 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 obtenir plus d'informations, reportez-vous à Configurer des informations d'authentification permanentes pour la connexion à Expressway, à la page 108.
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 obtenir plus d'informations, reportez-vous à Configurer des informations d'authentification permanentes pour la connexion à Expressway, à la page 108.
Désactiver les codes de chiffrement TLS	Reportez-vous à Désactiver les chiffrements Transport Layer Security, à la page 94.	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.

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).

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.

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 21 : 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.

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 22 : 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, (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, le bandeau lumineux sur le téléphone de conférence passe au rouge.

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.
- 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 12

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 12

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 d'un enregistrement invoqué par le périphérique

La fonctionnalité d'enregistrement invoqué par le périphérique peut être configurée dans Cisco Unified Communications Manager Administration. Pour obtenir plus d'informations, reportez-vous à la documentation de votre version de Cisco Unified Communications Manager.

Procédure

Étape 1 Définissez le paramètre Pont intégré du téléphone IP sur **Actif**.

Étape 2 Sur la page de configuration des lignes, définissez l'option Enregistrement par **Enregistrement d'appel sélectif activé** et sélectionnez le profil d'enregistrement approprié.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page 12

Configuration de UCR 2008

Les paramètres permettant la prise en charge de UCR 2008 sont hébergés dans Cisco Unified Communications Manager Administration. Le tableau suivant décrit les paramètres et indique le chemin à suivre pour modifier les paramètres.

Tableau 23 : Emplacement du paramètre UCR 2008

Paramètre	Chemin d'administration
Mode FIPS	**Périphérique** > **Paramètres du périphérique** > **Profil du téléphone commun**
	Système > **Configuration des téléphones d'entreprise**
	Périphérique > **Téléphones**
SSH Access	**Périphérique** > **Téléphone**
	Périphérique > **Paramètres du périphérique** > **Profil du téléphone commun**
Accès au Web	**Périphérique** > **Téléphone**
	Système > **Configuration des téléphones d'entreprise**
	Périphérique > **Paramètres du périphérique** > **Profil du téléphone commun**
Système > **Configuration des téléphones d'entreprise**	
Mode d'adressage IP	**Périphérique** > **Paramètres du périphérique** > **Configuration de périphérique commun**
Préférence de mode d'adressage IP pour la signalisation	**Périphérique** > **Paramètres du périphérique** > **Configuration de périphérique commun**

Configuration de UCR 2008 dans la configuration de périphérique commun

Suivez cette procédure pour définir les paramètres UCR 2008 suivants :

- Mode d'adressage IP
- Préférence de mode d'adressage IP pour la signalisation

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Paramètres du périphérique** > **Configuration de périphérique commun**.

Étape 2 Définissez le paramètre Mode d'adressage IP.

Étape 3 Définissez le paramètre Mode préférence IP pour signalisation.

Étape 4 Sélectionnez **Enregistrer**.

Configuration de UCR 2008 dans le profil de téléphone commun

Suivez cette procédure pour définir les paramètres UCR 2008 suivants :

- Mode FIPS
- SSH Access
- Accès au Web

Procédure

Étape 1 Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Paramètres du périphérique** > **Profil de téléphone commun**.

Étape 2 Définissez le paramètre Mode FIPS par **Activé**.

Étape 3 Définissez le paramètre Accès SSH par **Désactivé**.

Étape 4 Définissez le paramètre Accès au Web par **Désactivé**.

Étape 5 Définissez le paramètre SRTCP 80 bits sur **Activé**.

Étape 6 Sélectionnez **Enregistrer**.

Configuration de UCR 2008 dans la configuration de téléphones d'entreprise

Suivez cette procédure pour définir les paramètres UCR 2008 suivants :

- Mode FIPS
- Accès au Web

Procédure

Étape 1	Dans Cisco Unified Communications Manager Administration, sélectionnez **Système** > **Configuration des téléphones d'entreprise**.
Étape 2	Définissez le paramètre Mode FIPS par **Activé**.
Étape 3	Définissez le paramètre Accès au Web par **Désactivé**.
Étape 4	Sélectionnez **Enregistrer**.

Configuration de UCR 2008 sur le téléphone

Suivez cette procédure pour définir les paramètres UCR 2008 suivants :

- Mode FIPS
- SSH Access
- Accès au Web

Procédure

Étape 1	Dans Cisco Unified Communications Manager Administration, sélectionnez **Périphérique** > **Téléphone**.
Étape 2	Définissez le paramètre Accès SSH par **Désactivé**.
Étape 3	Définissez le paramètre Mode FIPS par **Activé**.
Étape 4	Définissez le paramètre Accès au Web sur **Désactivé**.
Étape 5	Sélectionnez **Enregistrer**.

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-7800-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).

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

Le tableau suivant présente les divers scénarios de déploiement de Mobile and Remote Access Through Expressway.

Scénario	Actions
Un utilisateur sur site se connecte au réseau de la société, après avoir déployé Mobile and Remote Access Through Expressway.	Le réseau de l'entreprise est détecté et le téléphone s'enregistre auprès de Cisco Unified Communications Manager, comme il le ferait normalement.
Un utilisateur distant se connecte au réseau de la société à l'aide de Mobile and Remote Access Through Expressway.	Le téléphone détecte qu'il est en mode hors site, la fenêtre de connexion à Mobile and Remote Access Through Expressway s'affiche, et l'utilisateur se connecte au réseau d'entreprise. Les utilisateurs doivent disposer d'un nom de service, d'un nom d'utilisateur et d'un mot de passe valides pour pouvoir se connecter au réseau. Les utilisateurs doivent également réinitialiser le mode de service pour effacer le paramètre TFTP secondaire avant de pouvoir accéder au réseau de l'entreprise. Cette opération efface le paramètre serveur TFTP secondaire afin que le téléphone puisse détecter le réseau hors site. Si le téléphone est déployé est neuf, les utilisateurs peuvent ignorer l'étape de réinitialisation des paramètres réseau. Si les options DHCP 150 ou 66 sont activées sur le routeur de leur réseau, les utilisateurs risquent de ne pas pouvoir se connecter au réseau d'entreprise. Les utilisateurs doivent désactiver ces paramètres DHCP ou configurer directement leur adresse IP statique.

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)

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 80
Configuration spécifique au produit, à la page 82

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**.

CHAPITRE 10

Configuration des répertoires d’entreprise et personnel

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.

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 12

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

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.

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.

SECTION IV

Résolution des problèmes du téléphone

CHAPITRE 11

Surveillance des systèmes téléphoniques

Présentation de la surveillance des systèmes téléphoniques

Vous pouvez visualiser diverses informations concernant le téléphone dans les menus d'état du téléphone et sur les pages Web du téléphone. Ces informations sont notamment les suivantes :

- Les informations sur le périphérique
- Les informations sur la configuration du réseau
- Les statistiques réseau
- Les journaux des périphériques
- Les statistiques de streaming

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.

Rubriques connexes

Dépannage, à la page 147

État du téléphone IP Cisco

Les sections suivantes décrivent comment afficher les informations sur le modèle, les messages d'état et les statistiques réseau sur les téléphones IP Cisco.

- 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.

Afficher la fenêtre Informations sur le téléphone

Procédure

Étape 1 Appuyez sur la touche **Paramètres** > **Informations sur le téléphone**.

Étape 2 Pour quitter le menu, appuyez sur **Quitter**.

Affichage du menu État

Procédure

Étape 1 Appuyez sur la touche **Paramètres** > **État**.

Étape 2 Pour quitter le menu, appuyez sur **Préc**.

Affichage de la fenêtre Messages d'état

Procédure

Étape 1 Appuyez sur la touche **Paramètres** > **État** > **Messages d'état**.

Étape 2 Pour quitter le menu, appuyez sur **Préc**.

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 24 : Messages d'état du téléphone IP Cisco

Message	Description	Explication possible et action
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 est dispo IP est disponible pour le téléphone.

Message	Description	Explication possible et action
Erreur taille TFTP	Le fichier de configuration est trop volumineux pour le système de fichiers du téléphone.	Éteignez le téléphone puis rallumez
Erreur checksum ROM	Le fichier de téléchargement logiciel est endommagé.	Obtenez une nouvelle copie du mic placez-la dans le répertoire TFTPPa fichiers dans ce répertoire que lorsq TFTP est fermé ; sinon, les fichiers n
Adresse IP en double	Un autre périphérique utilise l'adresse IP qui est affectée au téléphone.	Si le téléphone est doté d'une adres vous n'avez pas affecté une adresse Si vous utilisez DHCP, vérifiez la c DHCP.
Suppression des fichiers CTL et ITL	Suppression du fichier CTL ou ITL.	Aucune. Ce message est uniquement

MàJ langue : erreur	Un ou plusieurs fichiers de localisation sont introuvables dans le répertoire TFTP Path ou sont incorrects. La langue n'a pas été changée.	Depuis Cisco Unified Operating Sys que les fichiers suivants sont bien sit dans la Gestion des fichiers TFTP :
		• Situé dans un sous-répertoire p langue du réseau :
		  • tones.xml
		• Dans le sous-répertoire qui po 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'un télé téléphone est ajouté à la base de do Communications Manager. Si le tél base de données Cisco Unified Com serveur TFTP génère la réponse **`Fi introuvable`**. • Le téléphone n'est pas enregist Communications Manager. Vous devez ajouter le téléphon Unified Communications Man l'enregistrement automatique d • Si vous utilisez DHCP, vérifiez vers le serveur TFTP adéquat. • Si vous utilisez des adresses IP configuration du serveur TFTP

Message	Description	Explication possible et action
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 peut toujou de Cisco Unified Communications Ma
Adresse IP libérée	Le téléphone est configuré pour libérer l'adresse IP.	Le téléphone reste inactif jusqu'à sa mis la réinitialisation de l'adresse DHCP.
Expiration DHCP IPv4	Le serveur DHCP IPv4 n'a pas répondu.	Le réseau est occupé : les erreurs devrai résolues dès la diminution de la charge Pas de connectivité réseau entre le serv téléphone : vérifiez les connexions rés Le serveur DHCP IPv4 est en panne : v du serveur DHCP IPv4. Les erreurs persistent : envisagez d'aff statique.
Expiration DHCP IPv6	Le serveur DHCP IPv6 n'a pas répondu.	Le réseau est occupé : les erreurs devrai résolues dès la diminution de la charge Pas de connectivité réseau entre le serv téléphone : vérifiez les connexions rés Le serveur DHCP IPv6 est en panne : v du serveur DHCP IPv6. Les erreurs persistent : envisagez d'aff statique.
Expiration DNS IPv4	Le serveur DNS IPv4 n'a pas répondu.	Le réseau est occupé : les erreurs devrai résolues dès la diminution de la charge Pas de connectivité réseau entre le serv téléphone : vérifiez les connexions rés Le serveur DNS IPv4 est en panne : vé serveur DNS IPv4.
Expiration DNS IPv6	Le serveur DNS IPv6 n'a pas répondu.	Le réseau est occupé : les erreurs devrai résolues dès la diminution de la charge Pas de connectivité réseau entre le serv téléphone : vérifiez les connexions rés Le serveur DNS IPv6 est en panne : vé serveur DNS IPv6.
DNS - Hôte IPv4 inconnu	Le DNS IPv4 n'a pas pu résoudre le nom du serveur TFTP ou de Cisco Unified Communications Manager.	Vérifiez que les noms d'hôte du serveu Unified Communications Manager sont dans le DNS IPv4. Envisagez d'utiliser des adresses IPv4

Message	Description	Explication possible et action
DNS - Hôte IPv6 inconnu	Le DNS IPv6 n’a pas pu résoudre le nom du serveur TFTP ou de Cisco Unified Communications Manager.	Vérifiez que les noms d’hôte du ser Unified Communications Manager s dans le DNS IPv6. Envisagez d’utiliser des adresses IP
Image : rejet HC	L'application téléchargée n’est pas compatible avec le matériel du téléphone.	Ceci se produit lorsque vous tentez une version du logiciel qui ne prenc changements de matériel effectués s Vérifiez l'ID de chargement attribu Cisco Unified Communications Ma **Périphérique** > **Téléphone**). Saisis 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 adress routeur par défaut est configuré. Si vous utilisez DHCP, le serveur DH par défaut. Vérifiez la configuration
Pas de serveur DNS IPv4	Un nom a été défini, mais aucune adresse du serveur DNS IPv4 n’est spécifiée dans la configuration de DHCP ou de l’adresse IP statique.	Si le téléphone est doté d'une adress serveur DNS IPv4 est configuré. Si vous utilisez DHCP, le serveur DH DNS IPv4. Vérifiez la configuration
Pas de serveur DNS IPv6	Un nom a été défini, mais aucune adresse du serveur DNS IPv6 n’est spécifiée dans la configuration de DHCP ou de l’adresse IP statique.	Si le téléphone est doté d'une adress serveur DNS IPv6 est configuré. Si vous utilisez DHCP, le serveur DH DNS IPv6. Vérifiez la configuration
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 conf Communications Manager ; ce dern la sécurité par défaut. La liste de confiance n’est pas conf Pour plus d'informations sur les Lis documentation propre à votre versio Cisco Unified Communications Ma
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.	Des changements ont vraisemblable configuration de Cisco Unified Con l’utilisateur a appuyé sur le bouton A pour valider les modifications.

Message	Description	Explication possible et action
Erreur accès TFTP	Le serveur TFTP pointe vers un répertoire qui n'existe pas.	Si vous utilisez DHCP, vérifiez que le se le serveur TFTP adéquat. Si vous utilisez des adresses IP statiques du serveur TFTP.
Erreur TFTP	Le téléphone ne reconnaît pas un code d'erreur fourni par le serveur TFTP.	Contactez le centre d'assistance technic
Délai TFTP expiré	Le serveur TFTP n'a pas répondu.	Le réseau est occupé : les erreurs devraie résolues dès la diminution de la charge Pas de connectivité réseau entre le serve vérifiez les connexions réseau. Le serveur TFTP est en panne : vérifiez serveur TFTP .
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 expire génér n'est pas configuré sur le commutateur
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 installés s mise à jour des nouveaux fichiers CTL Voici les raisons possibles de cet échec • Une panne réseau s'est produite. • Le serveur TFTP a subi une panne • Le nouveau jeton de sécurité utilis CTL et le certificat TFTP utilisé p ont été introduits, mais ils ne sont fichiers CTL et ITL actuels du télé • Une panne s'est produite sur le tél Solutions possibles: • Vérifiez la connectivité réseau. • Vérifiez que le serveur TFTP est a normalement. • Si le serveur Transactional Vsam en charge par Cisco Unified Comm vérifiez si le serveur TVS est actif normalement. • Vérifiez la validité du jeton de sécu Si vous avez essayé toutes les solutions supprimez manuellement les fichiers C réinitialisez le téléphone. Pour plus d'informations sur les Listes documentation propre à votre version p Cisco Unified Communications Manag

Message	Description	Explication possible et action
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 uniquement Pour plus d'informations sur les Lis documentation propre à votre versi Cisco Unified Communications Ma
Erreur de version	Le nom du téléphone fichier image du téléphone est incorrect.	Assurez-vous de l’exactitude du fic
XmlDefault.cnf.xml ou .cnf.xml, selon le nom de périphérique du téléphone	Nom du fichier de configuration.	Aucune. Ce message indique le non du téléphone.

Rubriques connexes

Documentation des Cisco Unified Communications Manager, à la page 12

Affichage de la fenêtre Statistiques réseau

Procédure

Étape 1 Appuyez sur **Paramètres** > **État** > **Statistiques réseau**.

Étape 2 Pour quitter le menu, appuyez sur **Préc**.

Champs relatifs aux statistiques réseau

Le tableau suivant décrit les éléments de l’écran Statistiques réseau.

Tableau 25 : Champs relatifs aux statistiques réseau

Élément	Description
Tx Frames (Trames émises)	Le nombre de paquets envoyés par le téléphone
Tx broadcast	Le nombre de paquets de diffusion envoyés par le téléphone
Transmission individuelle	Le nombre total de paquets à diffusion individuelle émis par le téléphone
Rx Frames (Trames reçues)	Le nombre de paquets reçus par le téléphone
Rx broadcast	Le nombre de paquets de diffusion reçus par le téléphone
Rx unicast	Le nombre total de paquets à diffusion individuelle reçus par le téléphone
CDP ID périphérique du voisin	L’identifiant d’un périphérique branché dans ce port et détecté par le protocole CDP.
CDP Adresse IP du voisin	L’identifiant d’un périphérique branché dans ce port et détecté par le protocole CDP, qui utilise IP.

Élément	Description
CDP Port du voisin	L'identifiant d'un périphérique branché dans ce port et détecté par le protocole CDP.
Cause du redémarrage : l'une des valeurs suivantes : • Réinitialisation matérielle (réinitialisation par mise sous tension) • Réinitialisation logicielle (le contrôleur de la mémoire est également réinitialisé) • Réinitialisation logicielle (le contrôleur de mémoire n'est pas réinitialisé) • Watchdog Reset (Réinitialisation par le chien de garde) • Initialisé • Inconnue	La raison de la dernière réinitialisation du téléphone
Port 1	L'état des liaisons et la connexion du port réseau (par exemple, **`100 Mo auto duplex intégral`** signifie que le port PC est à l'état de liaison montante et a négocié automatiquement une connexion de 100 Mbits/s en duplex intégral)

Élément	Description
IPv4	Les informations concernant l'état de DHCP. Ces informations comprennent les états suivants : • CDP BOUND (Liaison CDP) • CDP INIT (Initialisation CDP) • DHCP BOUND (Liaison DHCP) • DHCP DISABLED (DHCP désactivé) • DHCP INIT (Initialisation DHCP) • DHCP INVALID (DHCP incorrect) • DHCP REBINDING (Nouvelle liaison DHCP) • DHCP REBOOT (Redémarrage DHCP) • DHCP RENEWING (Renouvellement DHCP) • DHCP REQUESTING (Requête DHCP) • DHCP RESYNC (Resynchronisation DHCP) • DHCP UNRECOGNIZED (DHCP non reconnu) • DHCP WAITING COLDBOOT TIMEOUT (DHCP - Temporisation démarrage à froid) • DISABLED DUPLICATE IP (Adresse IP en double désactivée) • SET DHCP COLDBOOT (Définir redémarrage à froid DHCP) • SET DHCP DISABLED (Définir désactivation DHCP) • SET DHCP FAST (Définition DHCP rapide)

Élément	Description
IPv6	

Élément	Description
	Les informations concernant l'état de DHCP. Ces informations comprennent les états suivants : • CDP INIT (Initialisation CDP) • DHCP6 BOUND (Liaison DHCP6) • DHCP6 DISABLED (DHCP6 désactivé) • DHCP6 RENEW (Renouvellement DHCP6) • DHCP6 REBIND (Nouvelle liaison DHCP6) • DHCP6 INIT (Initialisation DHCP6) • DHCP6 SOLICIT (Sollicitation de DHCP6) • DHCP6 REQUEST (Requête DHCP6) • DHCP6 RELEASING (Libération de DHCP6) • DHCP6 RELEASED (DHCP6 libéré) • DHCP6 DISABLING (Désactivation de DHCP6) • DHCP6 DECLINING (Refus DHCP6) • DHCP6 DECLINED (DHCP6 refusé) • DHCP6 INFOREQ (Requête infos DHCP6) • DHCP6 INFOREQ DONE (Requête infos DHCP6 terminée) • DHCP6 INVALID (DHCP6 incorrect) • DISABLED DUPLICATE IPV6 (Adresse IPv6 en double désactivée) • DHCP6 DECLINED DUPLICATE IP (DHCP6 a refusé une adresse IP en double) • ROUTER ADVERTISE (Publication routeur) • DHCP6 WAITING COLDBOOT TIMEOUT (DHCP6 - Temporisation du démarrage à froid) • DHCP6 TIMEOUT USING RESTORED VAL (DHCP6 - Temporisation avec valeurs restaurées) • DHCP6 TIMEOUT CANNOT RESTORE (DHCP6 échec restauration temporisation) • IPV6 STACK TURNED OFF (Pile IPv6 désactivée) • ROUTER ADVERTISE (Publication routeur) • ROUTER ADVERTISE (Publication routeur) • UNRECOGNIZED MANAGED BY (Géré par inconnu)

Élément	Description
	• ILLEGAL IPV6 STATE (État IPv6 illicite)

Affichage de la fenêtre Statistiques d'appel

Procédure

Étape 1 Appuyez sur **Paramètres** > **État** > **Statistiques d'appel**.

Étape 2 Pour quitter le menu, appuyez sur **Préc**.

Champs relatifs aux statistiques d'appel

Le tableau suivant décrit les éléments de l’écran Statistiques d'appel.

Tableau 26 : Les éléments de statistiques d'appel

Élément	Description
Codec appelé	Type de flux vocal reçu (flux RTP audio à partir de codec) : • G.729 • G.722 • G.722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS • iSAC
Codec appelant	Type de flux vocal transmis (flux RTP audio à partir de codec) : • G.729 • G.722 • G.722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS • iSAC

Élément	Description
Appelé - Taille	Taille, en millisecondes, des paquets de voix inclus dans le flux de voix reçu (transmission de flux par RTP).
Appelant - Taille	Taille, en millisecondes, des paquets de voix inclus dans le flux de voix émis.
Paquets 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 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 max	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	
Ratio cumulé de masquage	Nombre total de trames de masquage divisé par le nombre total de trames de conversation reçues depuis le début du flux de voix.
Ratio de temps de masquage	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.
Ratio de masquage max.	Taux de masquage par intervalle 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 du flux de voix (inclut les secondes masquées de haut niveau).
Durée en sec. 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.

Élément	Description
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.

Page web du téléphone IP Cisco

Chaque téléphone IP Cisco possède une page Web sur laquelle figurent diverses informations sur le téléphone, notamment :

- Information périphérique : affiche les paramètres du périphérique et les informations connexes sur le téléphone.
- Paramétrage réseau : affiche les informations sur la configuration réseau et sur les autres paramètres du téléphone.
- Statistiques réseau : affiche des liens hypertexte vers des informations sur le trafic réseau.
- Journaux des périphériques : affiche des liens hypertexte vers des informations relatives à la résolution de problèmes.
- Statistiques de streaming : affiche des liens hypertexte vers diverses statistiques de transmission de flux.

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

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 **Paramètres** > **Paramètres administrateur** > **Configuration réseau** > **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://<IP_address>

Page Web d'informations sur le périphérique

La zone Info. périphérique de la page Web du téléphone présente les paramètres du périphérique et des informations relatives au téléphone. Le tableau suivant décrit ces éléments.

Pour afficher la zone Info. périphérique, accédez à la page Web du téléphone, puis cliquez sur le lien hypertexte **Info. périphérique**.

Tableau 27 : Champs de la page Web d'informations sur le périphérique

Champ	Description
Mode de service	Le mode de service pour le téléphone.
Domaine du service	Le domaine du service.
État du service	État actuel du service.
Adresse MAC	Adresse MAC (Media Access Control) du téléphone.
Host Name	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.
ID image app	Indique la version de l'image de l'application.
ID image démarrage	Indique la version de limage du programme de démarrage.
Version	L'identifiant du micrologiciel qui est en cours d'exécution sur le téléphone.
Version du matériel	Le numéro de révision mineure du matériel du téléphone.
Numéro de série	Le numéro de série unique du téléphone.
Numéro du modèle	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 matériel • Nom de modèle de téléphone • Identificateur du produit • ID de la version (VID) : indique le numéro de version du matériel principal. • Numéro de série

Champ	Description
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 système installée.
Mémoire libre du Java heap	Quantité de mémoire libre du Java heap.
Mémoire libre du Java pool	Quantité de mémoire libre pour le pool Java.
Mode FIPS activé	Indique si le mode FIPS est activé.

Page Web de configuration réseau

La zone Configuration réseau de la page Web d’un téléphone présente des informations sur le paramétrage réseau et 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.

Pour afficher la zone Configuration réseau, accédez à la page Web du téléphone, puis cliquez sur le lien hypertexte **Configuration réseau**.

Tableau 28 : Éléments de la zone Configuration réseau

Élément	Description
Adresse MAC	Adresse MAC (Media Access Control) du téléphone.
Host Name	Le nom d’hôte que le serveur DHCP a affecté au téléphone.
Nom de 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 télé obtient l’adresse IP.
Serveur BOOTP	Indique si le téléphone obtient la configuration d’un serveur de protocole Bootstrap (BootP).
DHCP	Indique si le téléphone utilise DHCP.
Adresse IP	Adresse de protocole Internet (IP) du téléphone.
Masque de sous-réseau	Masque de sous-réseau utilisé par le téléphone.
Routeur par défaut 1	Routeur par défaut utilisé par le téléphone.

Élément	Description
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.
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.
Unified CM 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 peu 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 téléphon actuellement des services de traitement d'appels • En attente : le serveur Cisco Unified Communications Manager vers lequel le télépho si le serveur actuel devient indisponible • Vide : aucune connexion en cours à ce serveur Cisco Unified Communications Man Un élément peut également afficher la désignation SRST (Survivable Remote Site Teleph identifie un routeur SRST capable de fournir des fonctionnalités Cisco Unified Communicati limitées. Ce routeur prend le contrôle du traitement des appels si tous les autres serveurs C Communications Manager deviennent inaccessibles. Cisco Unified Communications Ma apparaît toujours à la fin de la liste des serveurs, même s'il est actif. Vous pouvez configu du routeur SRST dans la section Pool de périphériques de la fenêtre de configuration de C 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 obtient les services de téléphone IP Cisco.
URL d'inactivité	URL affichée sur le téléphone lorsque ce dernier est inactif pendant la durée spécifiée da Durée inactiv. URL, et lorsqu'aucun menu n'est ouvert.
Durée inactiv. URL	Durée, en secondes, pendant laquelle le téléphone est inactif et pendant laquelle aucun m ouvert, avant l'activation du service XML spécifié par l'URL d'inactivité.

Élément	Description
URL 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
Config. port de commut.	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
Langue utilisateur	Langue associée à l'utilisateur du téléphone. Présente un ensemble d'informations détaillées d à la prise en charge des utilisateurs, notamment la langue, la police, le format de date/d'heure informations textuelles relatives au clavier alphanumérique.
Langue réseau	Langue réseau associée à l'utilisateur du téléphone. Présente un ensemble d'informations déta destinées à la prise en charge du téléphone dans un emplacement donné, notamment les défini 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.
Écoute collective	Indique si la fonction d'écoute coll. est activée sur le téléphone. L'écoute collective vous perr parler dans le combiné et écouter en même temps via le haut-parleur.
GARP activé	Indique si le téléphone apprend les adresses MAC à partir de réponses Gratuitous ARP.
Sélection de ligne auto active	Indique si le téléphone met en évidence les appels entrants sur toutes les lignes.
DSCP pour le contrôle d'appel	Classification IP du DSCP pour la signalisation du contrôle des appels.
DSCP pour la configuration	Classification IP du DSCP pour n'importe quel transfert de configuration du téléphone.
DSCP pour les services	Classification IP du DSCP pour les services basés sur le téléphone.
Mode de sécurité	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.

Élément	Description
Accès SSH actif	Indique si le téléphone accepte ou bloque les connexions SSH.
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, l 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 co Lorsque CDP est désactivé dans Cisco Unified Communications Manager, un avertissem pour indiquer que CDP ne doit être désactivé sur le port de commutateur que si le téléphone à un commutateur tiers. Les valeurs actuelles des ports PC et de commutateur sont affichées dans le menu Paramè
LLDP-MED - Port logiciel	Indique si LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery) est a port de commutation.
Hiérarchisation énergie LLDP	Publie la hiérarchisation d'énergie du téléphone auprès du commutateur, afin que le comm fournisse des niveaux d'alimentation adéquats aux téléphones. Les paramètres sont les su • Inconnu : Il s'agit de la valeur par défaut. • Faible • Élevé • Critique
ID de ressource LLDP	Définit l'identifiant de ressource qui est affecté au téléphone pour la gestion de l'inventai
Fichier CTL	Identifie le fichier CTL.
Fichier ITL	Le fichier ITL contient la liste de confiance initiale.
Signature ITL	Renforce la sécurité grâce à l'algorithme (SHA-1) des fichiers CTL et ITL.
Serveur CAPF	Le nom du serveur CAPF utilisé par le téléphone.
TVS	Le composant principal de la sécurité par défaut. Grâce aux services de vérification de la confiance TVS (Trust Verification Services), les téléphones IP Cisco Unified peuvent aut serveurs d'applications, notamment les services de mobilité des numéros de poste, le répe MIDlet, pendant l'établissement de la connexion HTTPS.
Serveur TFTP	Le nom du serveur TFTP utilisé par le téléphone.
Synchronisation automatique des ports	Synchronise les ports au plus bas débit, ce qui élimine la perte de paquets.
Configuration à distance du port de commutation	Permet à l'administrateur de configurer à distance le débit et la fonction du port du tablea Desktop Collaboration Experience, dans Cisco Unified Communications Manager Admin
Mode d'adressage IP	Affiche le mode d'adressage IP qui est disponible sur le téléphone.

Élément	Description
Commande du mode de préférence IP	Indique la version de l'adresse IP utilisée par le téléphone pendant la signalisation avec Cisco Communications Manager lorsque IPv4 et IPv6 sont tous deux disponibles sur le téléphone.
Mode de Préférences IP pour média	Indique que pour le multimédia, le périphérique utilise une adresse IPv4 pour se connecter à Unified Communications Manager.
Configuration IPv6 automatique	Indique si la configuration automatique est activée ou désactivée sur le téléphone.
IPv6 DAD	Vérifie l'unicité des nouvelles adresses IPv6 à diffusion unique avant leur affectation à des in
Accepter les messages de redirection IPv6	Indique si le téléphone accepte les messages de redirection du routeur utilisé pour le numéro 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 de d'écho envoyé à une adresse IPv6.
Serveur de chargement IPv6	Utilisé pour optimiser la durée d'installation des mises à niveau de microprogramme sur le té et pour alléger la charge du WAN en stockant des images localement, éliminant ainsi la néces traverser la liaison WAN à chaque mise à niveau du téléphone.
Serveur de journaux IPv6	Indique l'adresse IP et le port de l'ordinateur de journalisation distant auquel le téléphone en messages de journalisation.
Serveur CAPF IPv6	Nom commun (provenant du certificat Cisco Unified Communications Manager) du CAPF u le téléphone.
DHCPv6	Le protocole DHCP (protocole de configuration dynamique d'hôte) affecte automatiquement IPv6 aux périphérique lorsque vous les connectez au réseau. DHCP est activé par défaut sur l téléphones IP Cisco Unified.
Adresse IPv6	Affiche l'adresse IPv6 actuelle du téléphone ou permet à l'utilisateur de saisir une nouvelle a IPv6.
Longueur du préfixe IPv6	Affiche la longueur de préfixe actuelle du sous-réseau ou permet à l'utilisateur de saisir une n longueur de préfixe.
Routeur IPv6 par défaut 1	Affiche le routeur par défaut utilisé par le téléphone ou permet à l'utilisateur de saisir un nou routeur IPv6 par défaut.
Serveur IPv6 DNS 1	Affiche le serveur DNSv6 principal utilisé par le téléphone ou permet à l'utilisateur de saisir un serveur.
Serveur IPv6 DNS 2	Affiche le serveur DNSv6 secondaire utilisé par le téléphone ou permet à l'utilisateur de sais nouveau serveur DNSv6 secondaire.
Autre TFTP IPv6	Permet à l'utilisateur de définir l'utilisation d'un autre serveur IPv6 TFTP (secondaire).
Serveur TFTP IPv6 1	Affiche le serveur TFTP IPv6 principal utilisé par le téléphone ou permet à l'utilisateur de dé nouveau serveur TFTP principal.

Élément	Description
Serveur TFTP IPv6 2	Affiche le serveur TFTP IPv6 secondaire utilisé si le service TFTP IPv6 principal n'est pa ou permet à l'utilisateur de définir un nouveau serveur TFTP secondaire.
Adresse IPv6 libérée	Permet à l'utilisateur de libérer des informations relatives à IPv6.
Niveau d'énergie EnergyWise	Une mesure de l'énergie consommée par les périphériques d'un réseau EnergyWise.
Domaine EnergyWise	Une groupement administratif de périphériques dont le but est de surveiller et de contrôle consommation d'énergie.

Page Web Informations Ethernet

Le tableau suivant décrit le contenu de la page Web Informations Ethernet.

Tableau 29 : 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.
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 de réseau

Le tableau suivant décrit les informations contenues dans les pages Web de zone réseau.

Remarque Lorsque vous cliquez sur le lien **Réseau** sous Statistiques réseau, la page est intitulée « Informations sur le port ».

Tableau 30 : Éléments de la zone réseau

Élément	Description
TotalPkt Rx	Le nombre total de paquets reçus par le téléphone.
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 tokenDrop	Le nombre total de paquets abandonnés pour cause de ressources insuffisantes (par exemple, débordement FIFO).
Tx totalGoodPkt	Le nombre total de bons paquets (multidiffusion, de diffusion et à diffusion individuelle) reçus par le téléphone.
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.
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.
CDP Adresse IP du voisin	L'adresse IP du périphérique voisin détecté par CDP.
CDP Adresse IPv6 du voisin	L'adresse IPv6 du périphérique voisin détecté par CDP.
CDP Port du voisin	Le port du périphérique voisin auquel le téléphone est connecté, que CDP a détecté.
LLDP ID du périphérique voisin	L'identifiant d'un périphérique branché dans ce port et détecté par LLDP.
LLDP Adresse IP du voisin	L'adresse IP du périphérique voisin détecté par LLDP.
LLDP Adresse IPv6 du voisin	L'adresse IPv6 du périphérique voisin détecté par CDP.

Élément	Description
LLDP Port du voisin	Le port du périphérique voisin dans lequel le téléphone est branché, détectée par LLDP.
Informations port	Informations sur le débit et sur le mode duplex.

Pages Web des Journaux de la console, Vidages mémoire, Messages d'état et Affichage du débogage

Sous l'en-tête de journaux des périphériques, des liens hypertextes des journaux de la console, des vidages mémoire, des messages d'état et de l'affichage de débogage fournissent des informations permettant de surveiller et de dépanner le téléphone.

- Journaux de la console : présente des liens hypertexte pointant 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 : présente des liens hypertexte vers des fichiers de vidage individuels. Les fichiers de vidage mémoire contiennent les données relatives aux pannes du téléphone.
- Messages d'état : affiche les 10 plus récents messages d'état générés par le téléphone depuis sa dernière mise sous tension. Ces informations sont également disponibles sur l'écran Messages d'état du téléphone.
- Affichage debug : affiche les messages de débogage que l'assistance technique de Cisco pourra utiliser pour vous aider à résoudre un problème, le cas échéant.

Page Web des statistiques de streaming

Un téléphone IP Cisco peut transmettre simultanément des informations en continu, en amont et en aval, à un maximum de cinq 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.

Pour afficher une zone Statistiques de streaming, accédez à la page Web du téléphone, puis cliquez sur le lien hypertexte correspondant au **Flux**.

Le tableau suivant présente les éléments des zones Statistiques de diffusion en flux continu.

Tableau 31 : Champs de statistiques de streaming

Élément	Description
Adr. distante	L'adresse IP et le port UDP de la destination du flux.
Adr. locale	L'adresse IP et le port UPD du téléphone.
Hr début	L'horodatage interne indiquant l'heure à laquelle Cisco Unified Communications M demandé que le téléphone commence à émettre des paquets.
État du flux	Indique si la transmission en continu est active ou non.

Élément	Description
Host Name	Unique ; nom fixe qui est automatiquement attribué au téléphone en fonction de son ad MAC.
Paquets 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 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 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 Appelé	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 Appelé	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 Appelé	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.
Ratio cumulé de masquage	Le nombre total de trames de masquage divisé par le nombre total de trames de convers reçues depuis le début du flux de voix.

Élément	Description
Ratio de temps de masquage	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 c conversation active.
Ratio de masquage max.	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).
Durée en sec. masquées de haut niveau	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 max	La valeur maximale de la gigue instantanée, en millisecondes.
Appelant - Taille	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.
Heure de réception du rapport de l'appelant (voir remarque)	La plus récente heure à laquelle un rapport d'appelant RTCP a été reçu.
Appelé - Taille	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.

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

Maintenance

Redémarrage ou réinitialisation du téléphone de conférence

Vous effectuez une réinitialisation de base d'un téléphone pour le restaurer si celui-ci rencontre une erreur. Vous pouvez également restaurer les paramètres de sécurité et de configuration aux valeurs de paramètres usine par défaut.

Redémarrage du téléphone de conférence

Lorsque vous redémarrez le téléphone, les modifications de configuration utilisateur et réseau qui ne sont pas écrites dans la mémoire flash du téléphone sont perdues.

Procédure

Appuyez sur la touche **Paramètres** > **Paramètres Admin** > **Réinitialiser les paramètres** > **Réinitialisation du périphérique**.

Réinitialisation des paramètres du téléphone de conférence à partir du Menu du téléphone

Procédure

Étape 1 Appuyez sur **Paramètres**.

Étape 2 Sélectionnez **Paramètres admin.** > **Réinitialiser les paramètres**.

Étape 3 Sélectionnez le type de réinitialisation.

- **Tous** : restaure les paramètres d'usine.

- **Réinitialiser le périphérique** : réinitialise le périphérique. Ne modifie pas les paramètres existants.
- **Réseau** : restaure la configuration du réseau par défaut.
- **Mode de service** : désactive le mode de service en cours, désactive la connexion VPN, puis redémarre le téléphone.
- **Sécurité** : restaure la configuration de sécurité par défaut. Cette option supprime le fichier CTL.

Étape 4 Appuyez sur la touche **Réinitialiser** ou **Annuler**.

Réinitialisation du téléphone à l'aide des paramètres d'usine depuis le clavier du téléphone

Lorsque vous réinitialisez le téléphone à l'aide du clavier, le téléphone rétablit les paramètres d'usine.

Procédure

Étape 1 Débranchez le téléphone :

- Si vous utilisez PoE, débranchez le câble LAN.
- Si vous utilisez l'amplificateur de puissance, débranchez-le.

Étape 2 Attendez pendant 5 secondes.

Étape 3 Appuyez et maintenez la pression sur **#**, et rebranchez le téléphone.

Étape 4 Lorsque le téléphone démarre, la bande LED s'allume. Lorsque la bande lumineuse s'allume, appuyez sur les touches **123456789*0#** dans l'ordre.

Lorsque vous avez appuyé sur ces boutons, la réinitialisation d’usine du téléphone commence.

Si vous appuyez sur les boutons dans le mauvais ordre, le téléphone s'allume normalement.

Avertissement N’éteignez pas le téléphone avant la fin de la réinitialisation d'usine ou avant l'affichage de l’écran principal.

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 32 : 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 13

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 33 : Résolution des problèmes du téléphone IP Cisco

Résumé	Explication
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	Les paramètres de mot de passe administrateur sont verrouillés par défaut, empêcher les utilisateurs d'effectuer des modifications pouvant affecter la co réseau. Vous devez déverrouiller les paramètres de mot de passe administra pouvoir les configurer. Pour de plus amples informations, reportez-vous à Appliquer un mot de pa téléphone, à la page 34. **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. Pour obtenir plus d'informations, reporte Affichage de la fenêtre Statistiques d'appel, à la page 126.
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 Pour obtenir plus d'informations, reportez-vous à Affichage de la fenêtre St d'appel, à la page 126.
Situation de bouclage	Une situation de bouclage peut se produire dans les conditions suivantes : • L'option Config. port de commut. du téléphone doit être définie par 1 (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 bon démarrage du téléphone, à la page 40

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 bon démarrage du téléphone, à la page 40

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 159.

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. Reportez-vous à la section « Affichage de la fenêtre Messages d’état » pour obtenir des instructions sur l’accès aux messages d'état et la liste des erreurs potentielles, leur explication et leur résolution.

Rubriques connexes

Affichage de la fenêtre Messages d’état, à la page 116

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 159

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.

Rubriques connexes

Vérification des paramètres DHCP, à la page 161

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.

Rubriques connexes

Vérification des paramètres DNS, à la page 162

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 162.

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.

Rubriques connexes

Créez un nouveau fichier de configuration de téléphone, à la page 161

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 48 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 48.

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 152 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.

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.

Rubriques connexes

Vérification des paramètres DHCP, à la page 161

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

Vous pouvez vérifier si un téléphone IP Cisco a reçu une commande de réinitialisation de la part de Cisco Unified Communications Manager en appuyant sur **Réglages** sur le téléphone et en choisissant **Paramètres admin** > **État** > **Statistiques du 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 160.

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 de son

Les sections suivantes présentent les solutions permettant de résoudre les problèmes de son.

Pas de chemin audio

Problème

Une ou plusieurs personnes n'entendent aucun son lors d'un appel.

Solution

Si, lors d'un appel, au moins une personne ne reçoit aucune donnée audio, cela signifie que la connectivité IP entre les téléphones n'est pas établie. Vérifiez la configuration des routeurs et des commutateurs afin de vous assurer que la connectivité IP est correctement configurée.

Son haché

Problème

Un utilisateur se plaint d'un son haché lors d'un appel.

Cause

Il y a peut-être une discordance dans la configuration de la gigue.

Solution

Vérifiez les statistiques AvgJtr et MaxJtr. Un grande différence entre ces statistiques peut indiquer un problème de gigue sur le réseau ou d'importants débits périodiques de l'activité réseau.

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.

Vérifier les paramètres TFTP

Procédure

Étape 1 Sur le téléphone, appuyez sur **Applications** .

Étape 2 Sur le téléphone, appuyez sur **Paramètres**.

Étape 3 Sélectionnez **Configuration réseau** > **Configuration IPv4**.

Étape 4 Vérifiez le champ Serveur TFTP 1.

Si vous avez attribué une adresse IP statique au téléphone, vous devez saisir manuellement une valeur pour l'option Serveur TFTP 1.

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 5 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 6 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

Détermination de l'adresse MAC du téléphone, à la page 48
Redémarrage ou réinitialisation du téléphone de conférence, à la page 143

Vérification des paramètres DHCP

Procédure

Étape 1 Sur le téléphone, appuyez sur **Applications** .

Étape 2 Sur le téléphone, appuyez sur **Paramètres**.

Étape 3 Sélectionnez **Configuration réseau** > **Configuration IPv4**.

Étape 4 Vérifiez le champ 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 :

https://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html

Étape 5 Vérifiez les champs adresse IP, masque de sous-réseau et routeur par défaut.

Si vous affectez une adresse IP statique au téléphone, vous devez manuellement saisir ces paramètres pour ces options.

Étape 6 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 :

https://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

Méthodes disponibles pour ajouter des téléphones, à la page 48
Documentation des Cisco Unified Communications Manager, à la page 12

Vérification des paramètres DNS

Procédure

Étape 1 Sur le téléphone, appuyez sur **Applications** .

Étape 2 Sur le téléphone, appuyez sur **Paramètres**.

Étape 3 Sélectionnez **Configuration réseau** > **Configuration IPv4**

Étape 4 Vérifiez que le champ Serveur DNS 1 est correctement configuré.

Étape 5 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), Energywise, MobileRemoteAccess
- 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 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 12

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 (Chine)
- 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`**.