GUIDE D'ADMINISTRATION

Cisco Small Business

Cisco Configuration Assistant - Version 3.0(1)
Smart Business Communications System
Guide d'administration

Numéro de version du document 78-19942-01

Sommaire

Sommair

1

Présentation de base de Configuration Assistant

Bienvenue dans Cisco Configuration Assistant

- Cliquez **ici** pour obtenir des informations sur l'utilisation de l'aide.
- Voir **Configuration de base, page 79** pour des instructions sur la création de sites clients et l'utilisation des assistants de configuration de périphériques intégrés.
- Voir **Ressources pour la planification et la mise en œuvre de votre solution SBCS, page 123** pour des informations sur la communauté SBCS et les ressources pour les partenaires.

Si vous débutez sous Cisco Configuration Assistant (CCA), les informations dans ces rubriques vous aideront à faire vos premiers pas :

- **Qu'est-ce que Cisco Configuration Assistant ?**
- **Configuration minimale requise**
- **Téléchargement et installation de CCA**
- **Vérification des mises à jour de l'application CCA**
- **Contrôle de compatibilité de version CCA**
- **Interface utilisateur**
- **Application et enregistrement de la configuration**
- **Affichage et gestion des erreurs**
- **Messages d'avertissement pour la voix**
- **Définition des préférences**
- **Notification des messages système**
- **Utilisation de l'aide en ligne**

- **Impression des fenêtres, des rapports et des graphiques de CCA**

Qu'est-ce que Cisco Configuration Assistant ?

Configuration Assistant est une application permettant de gérer les plateformes et les périphériques Cisco Small Business Pro. Les périphériques peuvent être gérés de manière indépendante ou en groupes appelés *sites clients*, à partir de n'importe où sur votre intranet. Son interface graphique vous permet d'effectuer les opérations suivantes :

- Configurer un Cisco Smart Business Communications System (SBCS)
- Configurer les connexions de ports
- Configurer les fonctions de téléphonie de votre site client
- Gérer les licences de téléphonie sur les périphériques VoIP
- Paramétrer la traduction d'adresses réseau, les réseaux privés virtuels et les pare-feu
- Configurer les fonctions LAN sans fil de votre site client, dont la sécurité et l'accès des invités sans fil
- Gérer et contrôler la sécurité du réseau
- Afficher l'intégralité du site client dans la topologie
- Afficher les volets frontaux des périphériques gérés
- Surveiller l'état, la bande passante et les liaisons d'un périphérique
- Afficher des rapports d'inventaire et des statistiques
- Mettre à jour le logiciel des périphériques
- Redémarrer et rétablir la configuration par défaut sur les périphériques
- Sauvegarder et restaurer une configuration de site

Pour réaliser ces opérations, vous pouvez sélectionner la fonction adéquate depuis la barre de fonctions de CCA, comme l'indique le chapitre **rubrique "Barre de fonctions" à la page 26**.

Configuration minimale requise

Le PC sur lequel vous installez CCA doit respecter la configuration minimale requise suivante.

Configuration minimale requise	
Systèmes d'exploitation pris en charge (Windows)	Microsoft Windows Vista Ultimate (32 ou 64 bits) Microsoft Windows XP Professionnel, Service Pack 2 ou supérieur Microsoft Windows 7 (64 bits et 32 bits) Vous devez avoir une autorisation en écriture pour votre répertoire d'origine et pour le répertoire d'installation de afin que CCA puisse créer les fichiers journaux et les fichiers de préférence nécessaires. Pour les PC sous Windows Vista et Windows 7, vous devez disposer d'un compte d'administrateur pour mettre à jour, installer et utiliser CCA. Lorsque vous utilisez CCA sur des PC sous Windows 7, annulez la fonction de mise en veille automatique. Pour modifier ces réglages, procédez comme suit : ▪ Allez dans **Panneau de configuration** > **Options d'alimentation.** Le réglage par défaut est Usage normal. ▪ Cliquez sur **Economie d'énergie**. ▪ Augmentez la valeur "Mettre l'ordinateur en veille" de 15 minutes (par défaut) à **Jamais**.
Compatibilité sous Mac OS (nécessite un logiciel de virtualisation)	**Mac OS** : 10.5 ou supérieur **Système d'exploitation virtuel** : Parallels Desktop 3.0 VMware Fusion 1.0 et les versions supérieures **Système d'exploitation hôte** : Microsoft Windows XP (Service Pack 2 ou supérieur), Windows Vista Ultimate. CCA prend également en charge le contrôle à distance à l'aide de clients VNC.

Configuration minimale requise	
Matériel	PC avec un port LAN FastEthernet ou supérieur
Processeur	1,8 GHz Intel Core 2 Duo ou supérieur
Espace disque	400 Mo (recommandés)
Mémoire	1 Go minimum ; 2 Go recommandés
Affichage	Résolution d'écran 1280 x 1024 ou supérieure
Navigateur	Microsoft Internet Explorer 8.0 ou supérieur, avec Javascript actif. Le plug-in Adobe Flash Player 10 ou une version supérieure pour Microsoft Internet Explorer doit aussi être installée (ainsi que toute autre version du plug-in pour les différents navigateurs Web). Javascript doit être activé sur le navigateur Microsoft Internet Explorer.

Téléchargement et installation de CCA

Pour installer CCA sur votre PC, suivez les étapes suivantes :

ETAPE1 Accédez à l'adresse : www.cisco.com/go/configassist.

Vous devez être inscrit sur le site Cisco.com mais vous n'avez besoin d'aucune autre autorisation.

ETAPE 2 Dans le volet Support technique, cliquez sur le lien **Télécharger le logiciel**.

ETAPE 3 Si vous n'êtes pas connecté, vous serez redirigé vers la page de connexion de Cisco.com. Introduisez votre nom d'utilisateur et votre mot de passe pour vous connecter.

ETAPE 4 Localisez le fichier d'installation de CCA (par exemple : `Cisco-config-assistant-win-k9-3_0-en.exe`).

ETAPE 5 Téléchargez le fichier d'installation de CCA et exécutez-le. Vous pouvez exécuter le fichier d'installation directement à partir du Web si votre navigateur vous le permet.

CCA est gratuit. Il peut être téléchargé, installé et utilisé sans aucun frais.

Suivez les instructions à l'écran lorsque vous démarrez le programme d'installation. A la dernière page, cliquez sur Configurer ces paramètres sous l'onglet Avancé. Cliquez sur **Terminer** pour achever l'installation.

Si vous utilisez une ancienne version de CCA, utilisez la fonction Mise à jour de l'application pour télécharger la dernière version. Voir la rubrique **rubrique "Vérification des mises à jour de l'application CCA" à la page 19**.

Une fois CCA installé, cliquez sur **Démarrer** > **Tous les programmes** > **Cisco Configuration Assistant** > **Cisco Configuration Assistant** ou utilisez le raccourci pour démarrer CCA.

Puisque CCA n'est pas connecté à un site client ou à un périphérique, seuls quelques éléments de menu et la fenêtre Connexion s'affichent au premier démarrage de CCA. Lorsque CCA n'est pas connecté à un périphérique ou à un site client, la barre de menus et la barre de fonctions ne prennent en charge que les tâches permettant de personnaliser CCA. La barre de fonctions, qui contient d'ordinaire les fonctions du périphérique, est vide.

Pour vous connecter à un périphérique ou créer un site client, consultez les rubriques **Créer et gérer les sites clients, page 80** et **Connexion à un site client ou à un périphérique autonome, page 91**.

Vérification des mises à jour de l'application CCA

Maintenez CCA à jour en recherchant et en installant les mises à jour sur Cisco.com.

Pour utiliser la fonction de mise à jour automatique, vous devez disposer d'un compte sur Cisco.com.

CCA vous invite à rechercher une mise à jour si

- Il détecte un nouveau type de périphérique ou un périphérique avec un logiciel mis à jour parmi les périphériques qu'il gère.
- Vous avez défini une recherche périodique au moyen de la fenêtre Préférences et l'intervalle de temps a expiré.

- La version de CCA que vous utilisez est plus ancienne que la version utilisée pour configurer le périphérique ou le site client auquel vous voulez vous connecter.

Vous pouvez également effectuer une recherche à la demande en sélectionnant l'option **Système** > **Mise à jour de l'application** dans la barre de menus.

Si CCA trouve une mise à jour, vous pouvez lire la description de son contenu et décider si vous souhaitez l'installer.

Contrôle de compatibilité de version CCA

Au démarrage de CCA et lorsque vous vous connectez à un site client ou à un périphérique, la fenêtre de conflit de version de CCA s'affiche si la version que vous utilisez est antérieure à celle qui a été utilisée pour configurer le système.

Le message suivant s'affiche : "La version de CCA que vous utilisez est antérieure à la version utilisée pour configurer le périphérique. Cela risque de provoquer des erreurs. Cisco conseille vivement la mise à jour vers la version X.x de CCA ou une version ultérieure. Voulez-vous effectuer la mise à jour ?"

Si vous choisissez l'option **Oui**, vous serez invité à introduire votre nom d'utilisateur et votre mot de passe Cisco.com pour accéder aux mises à jour.

Interface utilisateur

L'interface utilisateur de CCA facilite la gestion des fonctions réseau et la demande de services de CCA. Les parties principales de l'interface utilisateur sont les suivantes :

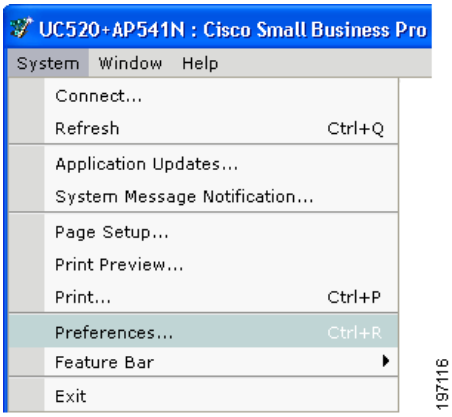
- **Barre de menus.**Ligne de menus en haut de la fenêtre CCA. Elle contient les services d'application, une liste des fenêtres ouvertes et l'aide en ligne. Pour en savoir plus sur la barre de menus, voir **Barre de menus, page 22**.
- **Barre d'outils.**Barre d'outils. Ligne d'icônes juste sous la barre de menus. Ces icônes représentent les services d'application utilisés le plus fréquemment, ainsi que les fonctions réseau le plus fréquemment configurées. Pour en savoir plus sur chaque icône, voir **Barre d'outils, page 24**.

- **Espace de travail.**Zone principale de la fenêtre de CCA. Tous les éléments compris entre la barre d'outils et la barre d'état. Contient deux parties : la barre de fonctions et le bureau de CCA.
- **Barre de fonctions.** Panneau extensible à gauche de l'espace de travail de CCA dans lequel vous sélectionnez les fonctions à configurer et les tâches à exécuter. Si vous ne connaissez pas le nom d'une fonction, vous pouvez le rechercher. Pour en savoir plus sur la barre de fonctions, voir **Barre de fonctions, page 26**.
- **Desktop.** Côté droit de l'espace de travail de CCA où se trouvent le Panneau de contrôle, les fenêtres de configuration et les assistants. C'est ici que s'affichent les rapports et que vous entrez les informations de configuration des fonctions réseau. Pour en savoir plus sur le bureau, voir **Bureau de CCA, page 28**.
- **Barre d'état.** Barre au bas de la fenêtre de CCA. Au démarrage de CCA, la barre d'état s'affiche et progresse vers la droite au fur et à mesure que les périphériques du réseau sont acquis. La barre d'état indique également quand les données de voix sont chargées. Au terme de ce processus, CCA est prêt à l'emploi.

  Ce processus d'acquisition se répète en fonction de la fréquence d'interrogation du réseau. En cas de perte de la liaison avec le site client ou le périphérique autonome, la barre d'état affiche *Pas de liaison*.
- **Fenêtre Topologie.** Plan de votre réseau et bien d'autres éléments, selon les options sélectionnées dans l'affichage. Pour en savoir plus, voir **Fenêtre Topologie, page 33**.
- **Vue volet frontal.** Hiérarchie des périphériques de votre réseau, image de l'armoire de répartition des périphériques et état de chaque périphérique et de ses ports. Pour en savoir plus, voir **Vue volet frontal, page 44**.

Barre de menus

La barre de menu contient des fonctions utiles pour l'utilisation de CCA. Les fonctions se répartissent dans les menus suivants : Système, Fenêtre et Aide



Menu	Fonction	Utilisation
Système	Connexion	Connexion à un site client ou à un périphérique autonome.
	Actualiser	Actualise la Vue volet frontal et la fenêtre Topologie en sondant les membres du site.
	Mise à jour de l'application	Permet de vérifier la présence de mises à jour pour l'application.
	Notification des messages système	Réception des messages système par e-mail.
	Mise en page, Aperçu avant impression, Imprimer	Utilisation des fonctions d'impression traditionnelles pour imprimer les affichages, les fenêtres et les graphiques.
	Préférences	Définition des préférences utilisateur pour CCA.
	Barre de fonctions	Définition du mode d'affichage de la barre de fonctions (Standard ou Masquage automatique).

Menu	Fonction	Utilisation
Fenêtre	Sélection d'une fenêtre dans la liste des fenêtres actives	Accès à une fenêtre dans la liste des fenêtres actives
Aide	Sommaire	Consultation de la rubrique d'aide de CCA.
	Nouveautés	Présentation d'une liste des nouvelles fonctions et des améliorations apportées à CCA d'une version à l'autre.
	Aide pour la fenêtre active	Présentation de la rubrique d'aide pour la fenêtre ou la vue active. Vous pouvez également accéder à l'aide relative à la fenêtre active en appuyant sur la touche **F1**.
	Feed-back	Envoi de votre feed-back sur CCA à Cisco.
	Informations de démarrage	Présentation d'un récapitulatif des nouvelles fonctions et des fonctions modifiées depuis la version précédente.
	Support technique	Coordonnées du Small Business Support Center et instructions pour la création du journal de dépannage.
	À propos de	Informations sur la licence utilisateur et numéro de version de CCA que vous utilisez.

Barre d'outils

La barre d'outils contient des icônes pour les tâches les plus souvent utilisées. Ce tableau décrit les actions entreprises par CCA lorsque vous cliquez sur les icônes. Placez la souris sur les icônes de la barre d'outils pour afficher une courte description de chaque élément.

Icône	Action
Connexion	Ouvre la fenêtre Connexion dans laquelle vous identifiez un site client ou un périphérique autonome que CCA doit gérer.
Actualiser	Actualise la Vue volet frontal et la fenêtre Topologie en sondant les membres du site client. CCA met à jour le statut des périphériques et des ports, et affiche tous les nouveaux membres.
Imprimer	Envoie le graphique, le rapport ou des sélections de l'aide en ligne vers une imprimante.
Préférences	Ouvre la fenêtre Préférences dans laquelle vous pouvez déterminer les préférences de l'utilisateur pour l'interface.
Enregistrer la configuration	Appliquez les modifications apportées à la configuration du périphérique. Vos modifications sont ainsi conservées même après l'arrêt de l'appareil.
Utilisateurs et téléphones	Ouvre la fenêtre Utilisateurs et téléphones vous permettant de configurer les options pour la communication vocale.
Serveur VPN	Ouvre la fenêtre Serveur VPN permettant de configurer un serveur VPN pour la transmission des règles de sécurité à un périphérique.
Pare-feu et DMZ	Affiche la fenêtre Pare-feu et DMZ vous permettant de configurer un pare-feu ou de créer une DMZ.
Réseaux sans fil	Affiche la fenêtre Réseaux sans fil permettant de définir des critères de sécurité pour un contrôleur WLAN et les points d'accès qui y sont associés.

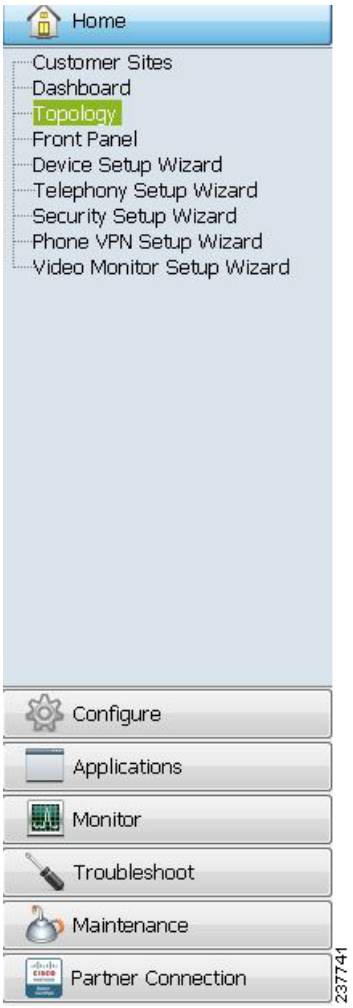
Icône	Action
Smartports	Ouvre la fenêtre Smartports dans laquelle vous configurez les ports et les périphériques en leur attribuant des profils.
Paramètres des ports du commutateur	Ouvre la fenêtre Paramètres des ports du commutateur dans laquelle vous pouvez afficher l'état des ports sur un périphérique sélectionné et modifier les paramètres des ports.
Inventaire	Ouvre la fenêtre Inventaire, qui affiche l'inventaire pour la communauté (types de périphérique, numéros de série, adresses IP et versions des logiciels) ou pour un périphérique isolé.
État	Affiche la fenêtre État vous permettant de surveiller une série de mesures relatives à *l'état* d'un périphérique afin d'éviter les temps d'arrêt et d'assurer le bon fonctionnement de votre réseau.
Notification d'événements	Affiche la fenêtre Notification d'événements qui décrit les conditions du réseau dont vous devez avoir connaissance et qui pourraient nécessiter votre intervention.
Tableau de bord	Affiche le Tableau de bord qui contient l'affichage graphique de l'état du système et de son fonctionnement, dont l'espace de stockage utilisé sur la mémoire flash de l'UC, l'utilisation du PoE, la température, les événements, la messagerie vocale, la mémoire et l'utilisation du processeur.
Topologie	Ouvre la fenêtre Topologie qui affiche notamment une carte du réseau des membres de la communauté en fonction des options de topologie que vous avez choisies.
Volet frontal	Ouvre la fenêtre Volet frontal qui affiche une liste hiérarchique des périphériques dans la communauté, une représentation graphique du câblage des périphériques et le statut de chaque périphérique et de ses ports.
Légende	Ouvre l'aide en ligne pour obtenir une explication des conventions graphiques utilisées dans CCA.
Aide pour la fenêtre active	Ouvre l'aide en ligne pour obtenir une explication de la fenêtre active. S'il n'y a pas de fenêtre active, l'aide affiche la rubrique *Introduction*.

Icône	Action
Feed-back	Affiche une page Web vous permettant de commenter votre expérience avec CCA.

Vous pouvez également saisir les termes dans le champ à droite de la barre d'outils et cliquer sur le bouton **Rechercher** pour effectuer une recherche dans l'aide en ligne.

Barre de fonctions

La barre de fonctions se trouve sur la gauche du bureau de CCA.



Les fonctions sont regroupées dans les menus suivants afin d'identifier les catégories de tâches :

- **Accueil** permet d'afficher le Tableau de bord, la Topologie et le Volet frontal. Cette fonction permet également d'accéder aux assistants de configuration des périphériques, de la téléphonie, des VPN, des réseaux sans fil, etc.
- **Configurer** permet de configurer les périphériques, les ports, le routage du réseau, les LAN sans fil, la sécurité et la voix.
- **Applications** permet d'activer et de configurer les options de configuration des Applications Smart ou tierces.
- **Superviser** permet d'assurer le suivi de votre réseau grâce aux rapports sur l'état du système et de la téléphonie ainsi qu'aux commandes de débogage de Cisco IOS et Cisco Unity Express (CUE).
- **Dépanner** permet de résoudre les problèmes de réseau ou de voix et de créer des journaux pouvant être utilisés par le Cisco Small Business Support Center afin de vous aider lors de la résolution des problèmes associés au système et au réseau.
- **Maintenance** permet d'assurer la maintenance de votre réseau, la mise à niveau de votre logiciel, la gestion des licences, des charges de téléphone et des fichiers de l'UC500.
- **Connexion aux partenaires** permet d'accéder à la communauté Cisco Small Business Support Community, à la page produit de l'UC500, aux flux RSS, aux téléchargements propres à l'UC500 et au site Partner Central sur Cisco.com.

Lorsque vous sélectionnez une fonction dans l'un de ces menus, la fenêtre relative à cette fonction s'affiche dans une nouvelle fenêtre.

Mode Standard et Mode masquage automatique

L'affichage de la barre de fonctions peut être défini en mode standard ou en mode masquage automatique :

- Si la barre de fonctions est en *mode standard*, il vous est possible de la réduire de manière à disposer de plus d'espace pour les fenêtres du bureau de CCA. Pour ce faire, pointez le curseur sur le bord droit de la barre de fonctions et faites glisser le curseur vers la gauche.
- Si la barre de fonctions est en mode *masquage automatique*, elle n'apparaît que lorsque vous déplacez le curseur vers le bord gauche de l'espace de travail de CCA. Elle disparaît à nouveau lorsque vous déplacez le curseur vers un autre endroit de l'espace de travail en dehors des limites de la barre de fonctions.

Pour définir le mode d'affichage de la barre de fonctions, sélectionnez **Système** > **Barre de fonctions** dans la barre de menus et sélectionnez l'option **Mode standard** ou **Mode masquage automatique**.

Bureau de CCA

Le bureau de CCA représente le point central de l'interface utilisateur. C'est là que vous exécutez les tâches suivantes :

- Affichage de l'**Tableau de bord**. Il s'agit d'une vue graphique de l'état du système avec des indications sur l'utilisation du processeur, du PoE, de l'espace de stockage et de la mémoire flash de l'UC500, la température, les alertes d'événements, l'état du VPN et la messagerie.
- Affichage de la **Fenêtre Topologie**, une carte du réseau représentant la communauté que gère CCA. L'information affichée renseigne à propos des nœuds, des liaisons et des périphériques voisins.
- Affichage du **Vue volet frontal**, une représentation des volets frontaux des périphériques dans la communauté. Vous pouvez cliquer sur les périphériques et ports affichés, et choisir les options de configuration à partir d'un menu contextuel.
- Affichage des assistants de configuration. Certains assistants de configuration, tels que l'Assistant de configuration de la téléphonie et l'Assistant de connectivité du SR520-T1, démarrent automatiquement lorsque vous vous connectez à un périphérique présentant une configuration par défaut.
- Introduire l'information pour configurer les fonctions réseau . Cette tâche peut s'exécuter au moyen des fenêtres de fonctions ou à l'aide du mode Guide.
- Afficher rapports et graphiques. Recherchez les termes Rapports et Graphiques dans les menus de la barre de fonctions. Ils sont associés à de nombreuses fonctions réseau et vocales proposées dans ces menus.

Il vous est possible de définir l'affichage par défaut lorsque CCA se connecte à un périphérique. Il est possible de lancer l'une ou l'autre vue, les deux vues ou aucune des deux. Voir la rubrique **Définition des préférences, page 54**.

Tableau de bord

Le Tableau de bord exige au moins la version 10.0.0.0 d'Adobe Flash Player et Microsoft Internet Explorer sur le PC exploitant CCA. Javascript doit être activé sur le navigateur Microsoft Internet Explorer.

Vue d'ensemble

Le Tableau de bord affiche la fenêtre principale lorsque vous vous connectez pour la première fois au périphérique ou au site client à l'aide de CCA. Il offre une interface intuitive, directe et graphique de l'état du système et de l'état des plateformes de la série Cisco Unified Communications 500 ainsi que des autres périphériques gérés.

Si vous fermez la fenêtre Tableau de bord, vous pourrez toujours l'afficher par la suite en accédant au menu **Accueil** > **Tableau de bord**.

Vous pouvez définir si le Tableau de bord doit automatiquement s'afficher lorsque vous êtes connecté(e) au réseau. Pour accéder à ce paramètre, utilisez le menu **Système** > **Préférences** et cliquez sur l'onglet Général. Sélectionnez ou annulez l'option **Afficher le Tableau de bord lors de la connexion au réseau**.

Utilisation du Tableau de bord

L'interface utilisateur du Tableau de bord se compose d'une série de fenêtres et d'une palette vous permettant de glisser-déposer les fenêtres vers la zone d'affichage principale :

- Cliquez sur **Afficher la palette** pour afficher la palette. L'élément est masqué par défaut.
- Utilisez les flèches Droite et Gauche de la palette pour parcourir les fenêtres disponibles.
- Glissez-déposez les icônes ou cliquez deux fois sur la palette pour placer les fenêtres dans la zone d'affichage.
- Placez la souris sur les éléments de la fenêtre pour afficher les infos-bulles contenant les valeurs numériques et les pourcentages.

Chaque fenêtre du Tableau de bord contient des commandes pour les fonctions suivantes :

- Réduction et agrandissement de la fenêtre affichée
- Sélection d'un périphérique différent à afficher, le cas échéant

- Mode de navigation en mode Présentation avec commande de lecture/pause

  En mode Présentation, l'affichage est mis à jour en fonction de l'état de l'instantané pour chaque périphérique selon l'intervalle de navigation défini. S'il n'y a qu'un seul périphérique, la sélection du mode Présentation n'a aucun effet sur l'affichage.

- Fermeture de la fenêtre et retour à la palette
- Configuration des paramètres de la fenêtre

  Par exemple, la fenêtre Température du Tableau de bord peut être configurée de telle sorte à afficher les valeurs en degrés Celsius ou Fahrenheit. Les intervalles pour l'actualisation des données et les présentations peuvent être configurés pour chaque fenêtre.

Pour accéder aux paramètres de configuration des fenêtres du Tableau de bord, cliquez sur l'icône Paramètres de la barre de fenêtre

Les modifications apportées au Tableau de bord sont enregistrées pour toutes les sessions.

État système et fenêtres d'état

Le tableau ci-dessous dresse la liste des états système et des fenêtres d'état disponibles.

Fenêtre	Description
État système	Affiche les informations générales sur le périphérique sélectionné : ▪ Nom de l'hôte et type de périphérique ▪ Adresse IP WAN, masque de sous-réseau et adresse IP de la passerelle ▪ Adresses IP du serveur DNS ▪ Version de Cisco IOS ▪ Durée active ▪ Date de la dernière mise à jour

Fenêtre	Description
Utilisation du processeur	Pourcentage de la capacité du processeur utilisée au cours des 5 dernières secondes, les 60 dernières secondes et les 5 dernières minutes pour le périphérique sélectionné.
Utilisation PoE	Pourcentage disponible et consommation des ports PoE du périphérique. Placez la souris sur le graphique pour afficher la consommation d'énergie en Watts. **REMARQUE** L'utilisation PoE ne s'affiche pas pour les commutateurs de la série ESW 500 avec PoE.
Utilisation de la mémoire flash	Pourcentage d'espace disponible et pourcentage d'espace utilisé sur la mémoire flash du périphérique sélectionné. Placez la souris sur le graphique pour afficher l'espace utilisé en Mo.
Utilisation de la mémoire	Pourcentage de la mémoire disponible et pourcentage utilisé pour le périphérique sélectionné. Placez la souris sur le graphique pour afficher la mémoire disponible en Mo.
Événements	Type et description des messages d'alerte relatifs à la notification des événements. Pour plus d'informations, allez dans **Superviser** > **Notification d'événements**. Vous pouvez aussi placer la souris sur les événements pour afficher une info-bulle contenant une description complète et des conseils.
Température	Pour les périphériques capables d'établir la température exacte en degrés Celsius ou Fahrenheit.

Fenêtre	Description
État de la messagerie	Affiche les informations sur l'état et le stockage système et des messageries, à savoir : ▪ La version de Cisco Unity Express (CUE) ▪ Le pourcentage (%) d'espace utilisé sur le système ▪ Les données par messagerie - L'identifiant utilisateur et le nom de groupement de postes associé à la messagerie - Poste - Le type : Personal ou GDM (General Delivery Mailbox) - La taille : volume de stockage affecté en minutes
État du VPN	Si EZVPN est configuré, il affiche l'adresse IP publique et l'état actuel : Actif - Actif ; Actif - En attente, Actif - Sans IKE, Panne - Négociation ou Panne. L'état du VPN est également accessible à partir de l'option **Superviser** > **Sécurité** > **État du VPN** .
Client sans fil (AP541N)	Pour obtenir un aperçu de l'état du client sans fil, sélectionnez l'option **Accueil** > **Tableau de bord** pour afficher le tableau de bord du système. Glissez-déposez ensuite le Client sans fil de la palette vers l'espace principal du Tableau de bord. L'élément Client sans fil du Tableau de bord affiche l'adresse MAC, l'adresse IP, le SSID, le type de protection et le type de périphérique pour les clients sans fil associés aux points d'accès AP541N. L'état du contrôleur sans fil et l'état de l'AP521 ne figurent pas dans le Tableau de bord.

Fenêtre Topologie

Cette fenêtre s'affiche lorsque vous effectuez l'une des opérations suivantes :

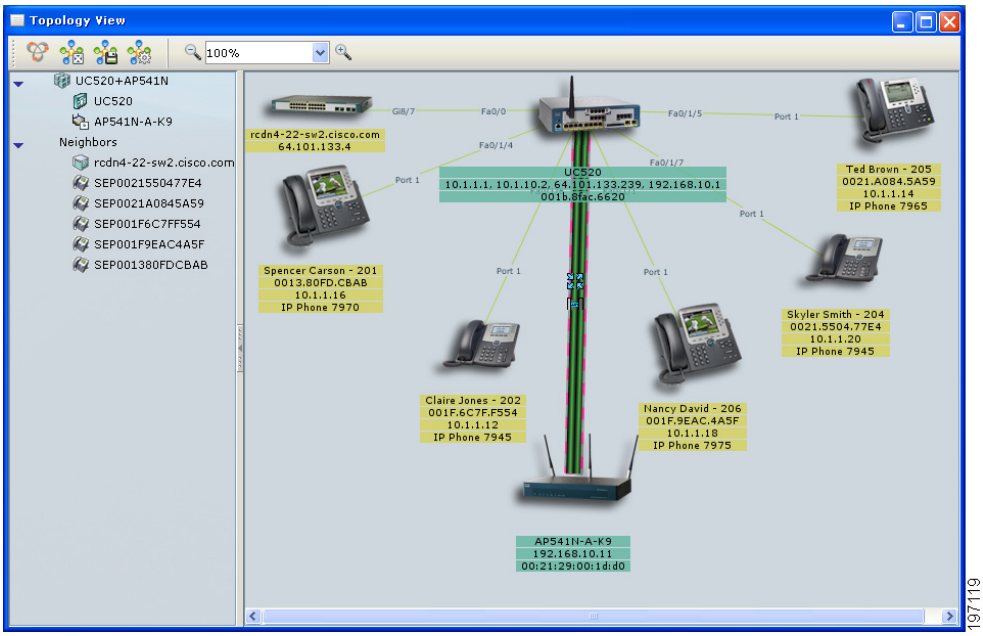
- Lorsque vous connectez CCA aux périphériques que vous souhaitez gérer.
- Sélectionnez **Accueil** > **Topologie** dans la barre de fonctions.
- Cliquez sur l'icône Fenêtre Topologie dans la barre d'outils.

Vue d'ensemble

Cette vue vous permet d'obtenir un aperçu de la topologie des périphériques que vous gérez et de leurs connexions. Utilisez les éléments qui la composent (**Barre d'outils**, **Volet gauche : périphériques du site et voisins** et **Volet droit - Carte de la topologie**) pour réaliser des **Tâches** destinées à manipuler l'affichage, l'enregistrer et vous donner des informations sur les périphériques qui s'y trouvent.

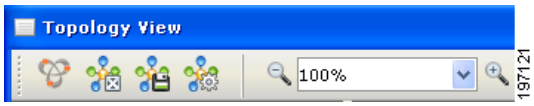
REMARQUE Les téléphones logiciels Cisco IP Communicator (CIPC) ne sont pas affichés dans la Fenêtre Topologie car ils ne contiennent aucune donnée CDP (Cisco Discovery Protocol).

Cliquez avec le bouton droit de la souris sur les icônes de la Fenêtre Topologie pour connaître les options permettant d'ajouter ou de supprimer un périphérique du site client, ouvrir l'utilitaire de configuration du périphérique ou pour effectuer d'autres tâches de gestion. Voir la rubrique **Tâches, page 37**.



Barre d'outils

La Fenêtre Topologie dispose de sa propre barre d'outils. Ce tableau décrit les actions entreprises par CCA lorsque vous cliquez sur les options de la barre d'outils.



Option	Utilisation
Exploration des périphériques Bonjour	Cliquez sur ce bouton pour détecter les caméras Cisco PVC2300 et WVC2300 ainsi que les imprimantes tierces prenant en charge le système Bonjour. Cliquez avec le bouton droit de la souris sur le périphérique Bonjour et utilisez l'Utilitaire de configuration pour gérer ces périphériques à l'aide des outils de gestion Web.
Disposition automatique	Redistribue l'espace et les informations de la fenêtre.
Enregistrer la présentation	Fige les modifications de la fenêtre Topologie.
Options de topologie	Cliquez pour ouvrir la fenêtre Options de topologie qui vous permet de contrôler les informations affichées dans la fenêtre. Vous pouvez par exemple contrôler le volume d'informations affiché sur les liaisons et les nœuds à l'aide des cases se trouvant sous l'onglet **Afficher les informations**. Voir la rubrique **Options de topologie, page 41**.

Option	Utilisation
Commandes de zoom	Lorsque cette vue s'affiche, le volet droit présente un grossissement de 100 %. Pour réduire la vue : ▪ Cliquez ou maintenez l'icône « - » de la loupe ▪ Appuyez sur la touche « - » du clavier ▪ Sélectionnez un pourcentage inférieur dans la liste déroulante ▪ Entrez un nombre inférieur à 100 dans le champ textuel. Pour zoomer à nouveau, utilisez l'une des techniques suivantes : ▪ Cliquez ou maintenez l'icône « + » de la loupe. ▪ Appuyez sur la touche « + » du clavier. ▪ Sélectionnez un pourcentage supérieur dans la liste déroulante. ▪ Entrez un nombre supérieur à 100 dans le champ textuel.

Vous pouvez sélectionner l'une des trois premières options du menu contextuel qui s'affiche lorsque vous cliquez dans l'arrière-plan du volet droit avec le bouton droit de la souris.

Volet gauche : périphériques du site et voisins

Le volet gauche contient *l'arborescence*. La liste contient le nom du site client ainsi et celui de chaque membre du site. Il y a aussi la liste des périphériques voisins des membres du site.

En présence d'un périphérique autonome, l'arborescence présente uniquement le périphérique et ses voisins.

Si vous n'utilisez pas de souris, utilisez la touche **Tab** pour sélectionner l'arborescence et utilisez les flèches Haut et Bas pour vous y déplacer.

Une fois que vous avez sélectionné un périphérique dans l'arborescence, le périphérique correspondant est sélectionné dans le volet droit. La fenêtre est automatiquement mise à jour afin d'afficher le périphérique.

Etat du périphérique

L'arborescence indique l'état des périphériques avec les couleurs suivantes :

Couleur	État
 Rouge	En panne ou non connecté
 Vert	Connecté et fonctionnel
 Bleu	Inconnu

Utilisation de la fenêtre contextuelle

Cliquez avec le bouton droit de la souris sur un périphérique ou appuyez sur les touches **MAJ-F10** dans le volet gauche pour afficher une fenêtre contextuelle. Ce menu se présente sous la forme d'une liste de tâches (par exemple, afficher les propriétés, modifier le nom d'hôte, redémarrer un périphérique ou afficher un graphique de bande passante) que vous pouvez réaliser avec le périphérique. Il s'agit de la même fenêtre contextuelle que celle qui s'ouvre lorsque vous cliquez avec le bouton droit de la souris sur un périphérique du volet droit.

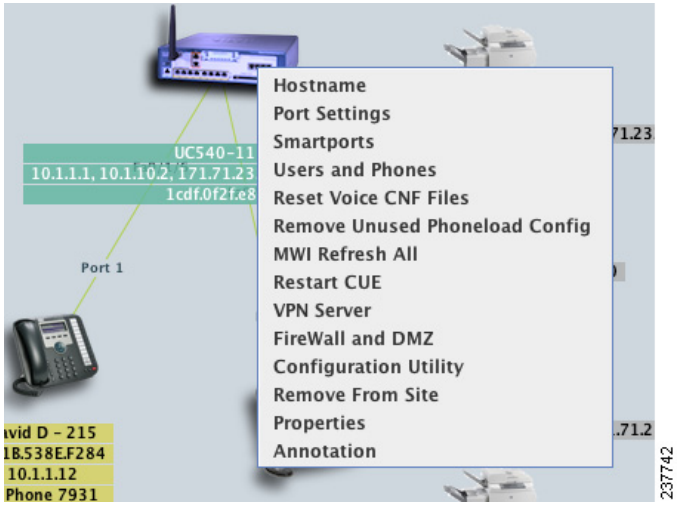
Volet droit - Carte de la topologie

Le volet droit contient la *carte de la topologie*. Elle présente les liaisons entre les périphériques ainsi que les informations les concernant. Les règles qui s'y appliquent sont les mêmes que celles du volet gauche :

- Le contenu varie selon que vous gérez un site client contenant plusieurs périphériques ou un périphérique autonome et si vous avez paramétré l'affichage de telle sorte à afficher les périphériques voisins dans la fenêtre Options de topologie.
- Cliquez avec le bouton droit de la souris sur l'icône du périphérique dans la fenêtre Topologie pour afficher les fenêtres vous permettant d'accomplir les tâches correspondantes. Vous pouvez réaliser des opérations

indépendantes des périphériques et destinées à modifier l'affichage de ce volet.

Par exemple, le menu suivant s'affiche lorsque vous cliquez avez le bouton droit sur l'UC500 dans la Fenêtre Topologie.



- L'état du périphérique est indiqué à l'aide des mêmes couleurs.

Tâches

Le tableau ci-dessous présente les tâches accessibles à partir de cette vue et la manière de les réaliser.

Tâche	Comment la réaliser
Réorganiser la présentation	Pour rendre les périphériques, les liaisons et les informations plus visibles, procédez comme suit : ▪ Déplacez les périphériques là où vous le souhaitez. ▪ *Sélectionnez les périphériques en série* en maintenant le bouton de la souris et en dessinant un rectangle autour d'un groupe d'éléments. Ensuite, en déplaçant un périphérique, vous les déplacerez tous.

Tâche	Comment la réaliser
Afficher les informations sur le périphérique et la liaison	Pour afficher les propriétés d'un commutateur ou d'une liaison, cliquez avec le bouton droit ou cliquez deux fois pour afficher le menu contextuel où vous pourrez sélectionner l'option **Propriétés**. Parmi les propriétés d'un périphérique figurent son nom, son type, son adresse IP, son adresse MAC ainsi que la version Cisco IOS en cours d'exécution. Les propriétés d'une liaison sont les identités des ports connectés et l'état de la liaison. Pour afficher la bande passante utilisée par un périphérique, cliquez avec le bouton droit ou cliquez deux fois pour afficher le menu contextuel où vous pourrez sélectionner l'option **Graphiques de bande passante**. Pour contrôler l'utilisation d'une liaison, cliquez avec le bouton droit ou cliquez deux fois pour afficher le menu contextuel où vous pourrez sélectionner l'option **Graphiques de liaison**.
Affichage des VLAN	Si vous gérez plusieurs périphériques sur un site client, vous pouvez afficher les liaisons des VLAN dans la fenêtre de topologie. Cliquez sur l'icône correspondante pour afficher la fenêtre Options de topologie et utilisez l'onglet **Afficher les VLAN**.
Ajouter des périphériques à un site client	Pour ajouter un périphérique à un site client, cliquez à l'aide du bouton droit de la souris ou cliquez deux fois sur le candidat pour sélectionner **Ajouter au site** dans le menu contextuel.
Supprimer des périphériques d'un site client	Pour supprimer un périphérique d'un site client, cliquez à l'aide du bouton droit de la souris sur le périphérique pour sélectionner **Supprimer du site** dans le menu contextuel.

Tâche	Comment la réaliser
Actualiser l'affichage	Lorsque le sondage réseau est actif, CCA sonde périodiquement les périphériques gérés et affiche la topologie réseau lorsque les périphériques sont supprimés ou ajoutés. Si vous savez qu'une modification a eu lieu et souhaitez visualiser les modifications entre deux sondages, cliquez sur l'icône **Actualiser** dans la barre d'outils. **REMARQUE** Pour activer ou désactiver le sondage réseau et modifier la fréquence d'interrogation, utilisez la fenêtre Préférences. Voir la rubrique **Définition des préférences, page 54**.
Réinitialisation des fichiers de configuration de la voix (CNF)	Sélectionnez l'option **Réinitialiser les fichiers vocaux CNF** pour que CCA recrée les fichiers de configuration XML pour les téléphones IP afin qu'ils puissent être actualisés et reconnaissent les nouveaux paramètres. Cela peut s'avérer nécessaire après la modification des fichiers de localisation du téléphone.
Suppression d'une configuration vocale inutilisée	Sélectionnez l'option **Supprimer configuration vocale inutilisée** pour supprimer la CLI non utilisée de la configuration.
Actualisation des MWI sur tous les téléphones	Sélectionnez l'option **Actualiser tous les MWI** pour actualiser les indicateurs de message en attente sur tous les téléphones afin d'obtenir une image actuelle de l'état des messageries.
Modifier un nom d'hôte	Cliquez avec le bouton droit de la souris sur le périphérique, choisissez **Nom de l'hôte** dans le menu contextuel et utilisez la fenêtre Nom de l'hôte.

Tâche	Comment la réaliser
Annotation d'objets et de liaisons	Vous pouvez ajouter un champ textuel (*annotation*) sous les périphériques et les nuages réseau ainsi qu'aux terminaisons des liaisons. Les annotations sont particulièrement utiles lorsqu'il s'agit d'afficher des informations qui n'apparaissent pas forcément sur la carte de topologie. Lorsque vous ajoutez un nuage réseau ou une liaison, la fenêtre Annotation s'affiche. Pour annoter un périphérique se trouvant déjà sur la carte, cliquez avec le bouton droit de la souris, sélectionnez l'option **Annotations** dans le menu contextuel et utilisez la fenêtre Annotation. Voir la rubrique **Annotations, page 43**. Si vous souhaitez masquer les annotations de la fenêtre Topologie, ouvrez la fenêtre Options de topologie et décochez l'option **Annotations** de l'onglet **Afficher les informations**.
Mise à jour du logiciel	Glissez et déposez le fichier image du logiciel de votre PC vers l'icône d'un périphérique. (Le périphérique doit être membre du site client.) Ce fichier peut se trouver sur un lecteur mappé ou réseau ainsi que sur un disque local. Pour mettre le logiciel à jour sur plusieurs périphériques, utilisez la fenêtre Mise à jour du logiciel.
Exploration des périphériques Bonjour	Cliquez sur l'icône Bonjour de la barre d'outils Topologie ou cliquez avec le bouton droit de la souris sur l'arrière-plan de la fenêtre Topologie et sélectionnez l'option **Explorer les périphériques Bonjour** pour détecter les caméras Cisco PVC2300 et WVC2300 ainsi que les imprimantes tierces prenant en charge le protocole Bonjour. Sélectionnez l'option Utilitaire de configuration pour gérer ces périphériques à l'aide des outils de gestion Web intégrés.

Tâche	Comment la réaliser
Ajout d'un nuage réseau	Cliquez avec le bouton droit de la souris sur l'arrière-plan de la topologie et sélectionnez l'option **Ajouter un nuage réseau** dans la fenêtre contextuelle. Attribuez un nom au nuage à l'aide de la fenêtre Annotation. Vous pourrez ensuite le déplacer vers n'importe quel endroit de la carte. Vous pouvez modifier la désignation ou supprimer le nuage en cliquant avec le bouton droit et en choisissant une action dans le menu.
Ajout d'une liaison	Vous pouvez ajouter manuellement une liaison à la carte. Pointez la souris vers le nœud d'origine de la liaison. Appuyez sur **Ctrl** et cliquez. Pointez la souris vers le nœud de destination. Appuyez à nouveau sur **Ctrl** et cliquez. Cliquez ensuite sur l'un des nœuds et sélectionnez l'option **Ajouter un lien** dans la fenêtre contextuelle. Les deux nœuds sont ainsi reliés et la fenêtre Annotation s'affiche. Utilisez les champs pour introduire des noms pour chaque terminaison.

Options de topologie

Cette fenêtre s'affiche lorsque vous cliquez sur l'icône Options de topologie dans la barre d'outils de la fenêtre Topologie. Cette fenêtre vous permet de définir ce que vous souhaitez afficher dans la fenêtre Topologie.

Chaque périphérique exploitant le protocole Cisco Discovery Protocol (CDP) s'affichera dans la topologie. Certains de ces périphériques ne peuvent pas être gérés avec Configuration Assistant.

CCA peut effectuer un démarrage croisé du gestionnaire de périphérique ou de l'utilitaire de configuration de certains périphériques tels que les routeurs sécurisés de la série SA500 et les commutateurs de la série ESW500. Pour démarrer le gestionnaire de périphérique natif, cliquez avec le bouton droit de la souris dans la Fenêtre Topologie et sélectionnez l'option **Utilitaire de configuration** dans la liste déroulante.

Cette fenêtre présente les onglets suivants :

- **Afficher les voisins** permet de sélectionner les périphériques voisins que vous souhaitez afficher.

- **Afficher les informations** permet de sélectionner les informations sur les liaisons et les noeuds que vous souhaitez afficher.
- **Afficher les VLAN** permet d'afficher les liaisons de VLAN dans la communauté et de sélectionner les couleurs qui les représentent.

Lorsque vous avez terminé de travailler dans cette fenêtre, cliquez sur **OK**.

Afficher les voisins

Les cases à cocher représentent les périphériques voisins que vous pouvez afficher :

- **Téléphones IP** : cochez cette case pour afficher les téléphones permettant la communication vocale sur un réseau IP.
- **Autres voisins** : cochez cette option pour afficher les périphériques voisins détectés par le protocole CDP (Cisco Discovery Protocol) (points d'accès et périphériques que CCA ne considère pas comme membres de la communauté).

Afficher les informations

Les cases à cocher suivantes contrôlent l'affichage des informations relatives aux liaisons et aux nœuds composant la Fenêtre Topologie :

- **Identifiant de l'interface** : cochez cette case si vous souhaitez afficher les identifiants des interfaces auxquelles les liaisons sont associées.
- **Vitesse réelle** : cochez cette case si vous souhaitez afficher les informations sur la vitesse de liaison, en opposition à sa vitesse d'administration.
- **Nom de l'hôte** : cochez cette case pour afficher les noms d'hôte des nœuds.
- **Adresse IP** : cochez cette case pour afficher les adresses IP des nœuds.
- **Adresse MAC** : cochez cette case pour afficher les adresses MAC des nœuds.
- **Annotations** : cochez cette case pour afficher les annotations des liaisons et des nœuds.

Afficher les VLAN

Suivez les étapes suivantes pour afficher les liaisons du VLAN dans la Fenêtre Topologie :

ETAPE 1 Dans le dossier VLAN, cliquez sur **Attribuer une couleur** pour le VLAN dont vous souhaitez mettre les liaisons en évidence.

ETAPE 2 Dans la fenêtre Sélection de la couleur, cliquez sur la couleur que vous souhaitez utiliser et terminez par **OK**. Le numéro du VLAN se déplace au-dessus du dossier du VLAN dans la liste des VLAN colorés. Le bouton **Attribuer une couleur** devient **Modifier la couleur** et indique la couleur sélectionnée.

ETAPE 3 Cochez la case à côté du numéro de VLAN afin d'activer la couleur dans la fenêtre Topologie. Si vous décochez ensuite la case, la couleur est désactivée.

Remarques :

- pour modifier la couleur de surbrillance d'un VLAN, cliquez sur le bouton **Modifier la couleur** et sélectionnez une couleur différente dans la fenêtre Sélection de la couleur.
- Pour supprimer la surbrillance pour un VLAN, cliquez sur **Supprimer la couleur**. Les boutons **Modifier la couleur** et **Supprimer la couleur** disparaissent et le numéro de VLAN revient au dossier présentant le bouton **Attribuer une couleur**.

Annotations

Cette fenêtre s'affiche dans les cas suivants :

- Clic droit sur un périphérique de la topologie et sélection de l'option Annotations dans le menu contextuel
- Ajout d'un nuage réseau
- Ajout d'un lien entre les nœuds dans la topologie (par exemple, entre un périphérique et un nuage réseau ou entre les périphériques).

Si vous annotez un nœud, introduisez une description dans le champ textuel ; par exemple, l'emplacement du périphérique. Les données s'affichent sous l'icône du nœud. Si vous annotez une liaison, entrez une description pour chaque terminaison. Lorsque vous avez terminé, cliquez sur **OK**.

Vous pouvez masquer des annotations dans la fenêtre Topologie en décochant la case Annotations sous l'onglet Afficher les informations de la fenêtre Options de topologie.

Vue volet frontal

Cette fenêtre s'affiche lorsque vous effectuez l'une des opérations suivantes :

- Lorsque vous spécifiez dans la fenêtre Préférences que vous souhaitez que la Vue volet frontal s'ouvre quand CCA est connecté. Voir la rubrique **Définition des préférences, page 54**.
- Lorsque vous sélectionnez **Accueil** > **Volet frontal** dans la barre de fonctions.
- Cliquez sur l'icône Vue volet frontal dans la barre d'outils.

Cette fenêtre est formée de deux parties liées : le **Volet gauche** et le **Volet droit**. Utilisez-les pour **Sélectionner les périphériques** et **Sélection de ports** des ports afin de pouvoir vérifier et modifier des configurations. Vous pouvez aussi **Organiser les périphériques** dans l'affichage. Pour voir les effets des modifications apportées, vous pouvez **Actualiser l'affichage**.

Volet gauche

Le volet gauche contient une arborescence qui indique les périphériques membres, inscrits en retrait sous le nom du site client. Une case apparaît à côté de chaque nom de périphérique. Cochez la case pour afficher le volet frontal du périphérique dans le volet droit.

Certains périphériques ne disposent pas d'une vue volet frontal. Certains périphériques inconnus n'affichent pas la vue volet frontal.

L'arborescence indique l'état des périphériques avec les couleurs suivantes :

- **Vert**. Le périphérique est connecté et fonctionnel.
- **Jaune**. Un dysfonctionnement est détecté. Déplacez le pointeur de la souris sur l'icône du périphérique afin de consulter la description.
- **Rouge**. Le périphérique est en panne ou non connecté.

Volet droit

Le volet droit affiche la vue Volet frontal des périphériques que vous avez choisis dans le volet gauche. Vous voyez leurs ports et emplacements de modules comme vous les verriez dans une armoire de répartition.

Sélectionner les périphériques

Vous pouvez sélectionner un périphérique de deux manières :

- En cliquant dans son volet frontal.

- En sélectionnant l'icône du périphérique dans l'arborescence.

Quand vous cliquez sur un périphérique, un rectangle jaune l'entoure, indiquant ainsi qu'il est sélectionné. Pour sélectionner plusieurs périphériques, maintenez la touche **Ctrl** et cliquez sur les périphériques que vous souhaitez sélectionner. Pour annuler la sélection d'un périphérique, maintenez la touche **Ctrl** et cliquez sur le périphérique concerné.

Vous pouvez sélectionner un groupe de périphériques puis cliquer à l'aide du bouton droit de la souris sur un périphérique pour afficher un menu contextuel. Utilisez le menu contextuel pour vérifier ou modifier les configurations du périphérique. Les options du menu contextuel ne s'appliquent qu'aux périphériques sélectionnés. Vous pouvez aussi utiliser les options de la barre de fonctions pour vérifier ou modifier les configurations du périphérique. Si une option de la barre de fonctions n'est pas applicable aux périphériques sélectionnés, la sélection est ignorée.

Sélection de ports

Ce tableau indique les différentes manières de sélectionner des ports.

REMARQUE les ports d'un contrôleur WLAN ne peuvent pas être sélectionnés.

Si vous souhaitez...	Procédez ainsi...
Sélectionner un port unique	Cliquez à l'aide du bouton droit ou gauche de la souris sur le port. Si vous cliquez à l'aide du bouton droit de la souris, un menu contextuel est également affiché.
Sélectionner tous les ports d'un périphérique.	Cliquez à l'aide du bouton droit de la souris sur n'importe quel port et choisissez **Sélectionner tous les ports** dans le menu contextuel.
Sélectionner plusieurs ports sur le même périphérique ou sur différents périphériques.	Utilisez une des méthodes suivantes : ▪ Maintenez enfoncée la touche **Ctrl** et cliquez sur les ports que vous souhaitez sélectionner. ▪ *Sélectionnez les périphériques en série* en maintenant le bouton de la souris et en dessinant un rectangle autour d'un groupe d'éléments. Maintenez la touche **Ctrl** pour ajouter plusieurs groupes de ports non adjacents à la sélection.

Pour annuler la sélection d'un port, maintenez la touche **Ctrl** et cliquez sur le port concerné.

Lorsque vous cliquez à l'aide du bouton droit de la souris pour sélectionner un port unique, un menu contextuel s'affiche. Pour voir le menu contextuel quand vous sélectionnez plusieurs ports, vous devez cliquer à l'aide du bouton droit de la souris sur l'un des ports. Utilisez le menu contextuel pour vérifier ou modifier les paramètres du port. Les éléments du menu contextuel ne s'appliquent qu'aux ports sélectionnés. Vous pouvez aussi utiliser les éléments de la barre de fonctions pour vérifier ou modifier les paramètres du port. Si un élément de la barre de fonctions n'est pas applicable aux ports sélectionnés, la sélection est ignorée.

Organiser les périphériques

Vous pouvez modifier l'ordre des périphériques de manière à refléter la configuration physique de votre armoire de répartition. Pour déplacer un périphérique, glissez-déposez son icône dans l'arborescence sur une nouvelle position.

Actualiser l'affichage

Pour actualiser la fenêtre Volet frontal, cliquez sur l'icône Actualiser dans la barre d'outils. Si vous savez qu'une modification a eu lieu dans la communauté, vous pourrez la voir immédiatement.

Icônes et images représentant l'état des périphériques et des liaisons

Cette rubrique présente les images et les couleurs qui apparaissent dans la fenêtre Topologie, le Volet frontal et les fenêtres de configuration. Les explications se répartissent dans les catégories suivantes :

- **Icônes du périphérique**
- **Icône représentant l'état du périphérique et couleurs**
- **Types de port**
- **Types de liaison**
- **État de la liaison**

Icônes du périphérique

Ces icônes s'affichent généralement dans les vues et les fenêtres de CCA.

- L'icône du périphérique est rouge lorsque le périphérique est en panne.
- Une icône Périphérique inconnu s'affiche lorsque CCA ne prend pas en charge un périphérique ou n'est pas compatible avec la version Cisco IOS en cours d'utilisation sur le périphérique.

Icône	Périphérique	Icône	Périphérique
	Site client		Routeur d'accès 800
	Plateforme Unified Communications 500 Series		Téléphone IP
	Commutateur (ESW 500 Series ou Catalyst Express CE520)		Contrôleur WLAN
	Point d'accès autonome		Point d'accès léger

Ces icônes peuvent également apparaître dans la topologie :

Icône	Périphérique	Icône	Périphérique
	Stack		Commutateur modulaire
	Commutateur de couche 3		Commutateur LRE
	Inconnu		Nuage réseau

Icône représentant l'état du périphérique et couleurs

Couleur de l'icône		Actif		Panne		Inconnu
Couleur		Membre ou périphérique indépendant		Candidats		Périphérique de périmètre

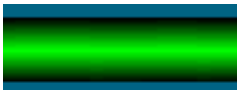
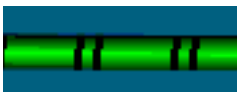
Types de port

RJ-45	RJ-45	RJ-11
Module SFP compact (small form-factor pluggable) (vide)		
Module SFP de fibre optique (LX, SX, ZX, CWDM, 100BASE-FX)		

Types de liaison

REMARQUE Les deux canaux représentent au moins deux liaisons. Si l'un d'entre eux est gris et l'autre vert, cela signifie qu'au moins une liaison est bloquée et qu'au moins une est active.

Icône/Type de liaison		Icône/Type de liaison	
	10 Mbit (bloqué)		Gigastack
	100 Mbit		Trunk
	1 Gbit		Routé

Icône/Type de liaison		Icône/Type de liaison	
	10 Gbit		Périmètre
	EtherChannel		Liaisons multiples
	Liaison ajoutée manuellement		

État de la liaison

Couleur de la liaison		Actif		Bloqué

Application et enregistrement de la configuration

La fenêtre Enregistrer la configuration s'affiche lorsque vous quittez Configuration Assistant ou sélectionnez **Configurer**>**Enregistrer la configuration** dans la barre de fonctions.

Vue d'ensemble

Lorsqu'un périphérique réseau sous Cisco IOS est actif, il présente deux configurations. La première est la configuration de démarrage qui est stockée dans la mémoire flash. La seconde représente la configuration en cours d'exécution qui est stockée dans la mémoire vive. Le périphérique utilise la configuration en cours d'exécution afin de définir son comportement.

- Lorsque vous cliquez sur **OK** ou **Appliquer** dans la fenêtre de configuration, vous apportez des modifications à la configuration en cours d'exécution. Ces modifications entrent immédiatement en vigueur.
- Lorsque vous sélectionnez **Configurer** > **Enregistrer la configuration** ou cliquez sur **OK** à l'invite vous demandant si vous souhaitez enregistrer la configuration à la fermeture, vous enregistrez les modifications apportées à la configuration de démarrage propre aux périphériques sélectionnés. Cela vous permet de faire en sorte que les modifications soient préservées en cas de redémarrage du périphérique.

Vous pouvez utiliser CCA pour définir la configuration en cours d'exécution comme configuration de démarrage. Les modifications apportées à la configuration en cours d'exécution seront donc permanentes.

L'enregistrement de la configuration en cours d'exécution ne concerne pas les modifications réalisées dans la fenêtre Topologie. Pour enregistrer les paramètres dans la fenêtre Topologie, utilisez l'option **Accueil**> **Topologie** et sélectionnez **Enregistrer la présentation** dans la barre d'outils de la Fenêtre Topologie.

Procédures

- Pour définir la configuration en cours d'exécution d'un périphérique géré comme configuration au démarrage, sélectionnez le périphérique dans la liste Nom de l'hôte et cliquez sur **Enregistrer**.
- Pour sauvegarder les configurations en cours pour les périphériques gérés, cliquez sur **Tous les périphériques** et cliquez sur **Enregistrer**.

Affichage et gestion des erreurs

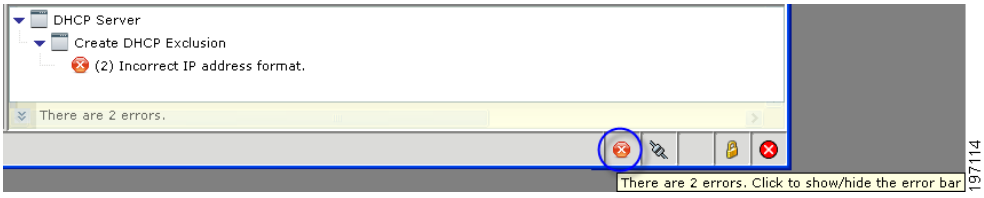
CCA vous indique que l'information que vous introduisez est valable en affichant une bordure verte.

- Toute information modifiée apparaît dans la barre d'état.
- Lorsque vous enregistrez une modification, le cadre vert disparaît.

Gestion des erreurs

Si vous introduisez des données erronées dans les champs de CCA :

- Un cadre rouge s'affiche autour des champs contenant des erreurs.
- Dans les fenêtres présentant des onglets, le nombre d'erreurs pour chaque onglet s'affiche en rouge sous chaque onglet.
- La barre de gestion des erreurs s'affiche automatiquement au bas de la fenêtre.



La barre de gestion des erreurs permet de rassembler les opérations d'affichage et de gestion des erreurs lors du paramétrage et de la validation de la configuration sous CCA.

Toutes les erreurs concernant les fenêtres ouvertes s'affichent avec le nom de la fenêtre, la fenêtre associée (si l'erreur s'affiche dans une fenêtre contextuelle) et le détail des messages d'erreur. Le nombre total d'erreurs pour toutes les fenêtre ouvertes s'affiche au bas de la barre de gestion des erreurs.

Tandis que vous résolvez les erreurs, la barre de gestion des erreurs est mise à jour. Lorsque tous les problèmes ont été résolus, la barre se ferme automatiquement.

Lorsque vous utilisez la barre de gestion des erreurs :

- Cliquez sur les flèches de la structure des fenêtres afin de parcourir les erreurs propres à chaque fenêtre.
- Cliquez sur le message d'erreur pour mettre la fenêtre en évidence et le champ contenant l'erreur en surbrillance.
- Pour redimensionner la barre de gestion des erreurs, cliquez avec le bouton gauche et déplacez la souris sur la bordure supérieure de la barre.
- Pour afficher ou masquer la barre de gestion des erreurs, cliquez sur l'icône d'erreur au bas de la fenêtre.

Si la fonction CLI Postview est activée (voir l'onglet Avancé de la fenêtre Préférences), les commandes de configuration envoyées à l'UC500 ou au SR500 s'affichent dans une fenêtre contextuelle. Voir la rubrique **Définition des préférences, page 54**.

Messages d'avertissement pour la voix

La fenêtre Messages d'avertissement pour la voix s'affiche lorsque vous tentez d'accéder ou de configurer des fonctions vocales et que votre système ne respecte pas certaines conditions.

Avant de continuer, veillez à ce que ces conditions soient respectées.

Message d'avertissement	Action requise	Fonction ou fenêtre associée
Rétablissez le système à sa configuration par défaut	Pour démarrer l'Assistant de configuration de la téléphonie, vous devez d'abord rétablir la configuration par défaut de l'UC500. Cela peut durer jusqu'à 20 minutes. Pour rétablir la configuration par défaut de l'UC500 : 1. Dans la barre de fonctions sur la gauche, sélectionnez **Maintenance** >**Redémarrer/Réinitialiser**. 2. Dans la fenêtre Redémarrer/Réinitialiser, sélectionnez Cisco UC500, cochez la case **Rétablir la configuration par défaut** et cliquez sur **OK**. 3. Au terme de la réinitialisation, redémarrez l'Assistant de configuration de la téléphonie.	Assistant de configuration de la téléphonie
Veillez à ce que votre PC soit directement connecté à un port LAN du routeur UC500	Pour démarrer l'Assistant de configuration de la téléphonie, le PC exploitant CCA doit être directement relié au port LAN de l'UC500 et obtenir l'adresse IP de l'UC500 à l'aide du protocole DHCP.	Assistant de configuration de la téléphonie

Message d'avertissement	Action requise	Fonction ou fenêtre associée
Désactivez les services TFTP tiers actifs sur votre PC	Si la fonction à laquelle vous tentez d'accéder exige de CCA qu'il utilise le service TFTP ou FTP pour le transfert des fichiers vers ou à partir de l'UC500, vous devrez d'abord désactiver les services TFTP ou FTP tiers actifs sur votre PC avant de continuer. Si vous utilisez un PC Windows, vous pouvez utiliser le Gestionnaire des tâches de Windows pour identifier ces applications et les fermer. Toutefois, ces services peuvent ne pas figurer sous l'onglet Applications du Gestionnaire des tâches. Vous pouvez aussi ouvrir une fenêtre de commande sur votre PC et introduire la commande `netstat` pour vérifier si ces services sont actifs et les identifier grâce au nom de l'exécutable ou à la référence de processus. c:\ **netstat -a -b** Une fois le processus TFTP ou FTP tiers localisé, allez dans l'onglet Processus du Gestionnaire des tâches Windows et fermez-le manuellement en mettant le processus en surbrillance dans la liste et en sélectionnant l'option **Fin de tâche**. Pour plus d'informations, consultez le manuel de votre système d'exploitation, de l'application TFTP ou de l'application FTP. En l'absence de services TFTP tiers, vérifiez le pare-feu et les paramètres de sécurité du réseau sur votre PC afin de vérifier si le trafic TFTP est autorisé entre le PC et l'UC500 ou essayez de redémarrer votre PC pour libérer les ports TFTP à partir d'une session antérieure de CCA.	Glissez-déposez les fichiers du PC vers la Fenêtre Topologie (images Cisco IOS, fichiers MoH, scripts B-ACD, scripts du standard automatique, etc.). Assistant de configuration de la téléphonie Configurer > Téléphonie > Gestion des appels > Standard automatique Configurer > Téléphonie > Gestion des appels > Basic ACD Configurer > Téléphonie > Utilisateurs et postes> Numérotation abrégée système Maintenance > Archive des configurations Maintenance > Mise à jour du logiciel Maintenance > Gestion des licences Maintenance > Redémarrer/ Réinitialiser (option Rétablissement des paramètres par défaut)

Définition des préférences

Pour configurer les préférences pour CCA, procédez comme suit :

- Sélectionnez **Système** > **Préférences** dans la barre de fonctions.
- Cliquez sur l'icône Préférences dans la barre d'outils.

Vue d'ensemble

Vous pouvez personnaliser la plupart des activités de CCA. Par exemple :

- Choisissez si vous souhaitez afficher la fenêtre Topologie, le Volet frontal ou le Tableau de bord lorsque vous connectez CCA à votre réseau.
- Activez ou désactivez le sondage réseau et indiquez la fréquence d'interrogation du périphérique géré par CCA en vue d'obtenir des données à jour.
- Précisez à quelle fréquence vérifier l'existence d'une nouvelle version de CCA sur Cisco.com.
- Précisez si vous souhaitez utiliser un serveur proxy pour télécharger les mises à jour de CCA sur Cisco.com.
- Précisez l'emplacement où Configuration Assistant doit archiver les configurations enregistrées sur les périphériques que vous administrez.
- Précisez les options de suivi de l'état de santé du système.
- Activez ou désactivez l'affichage des commandes Cisco IOS envoyées vers le routeur pour les changements de configuration de la téléphonie (fenêtre CLI Postview).
- Indiquez si le fichier Cisco.wav doit ou non être lu au démarrage.
- Choisissez l'image du bureau par défaut.
- Activez ou désactivez la collection et chargez les données d'utilisation de CCA vers Cisco.
- Activez ou désactivez l'affichage des CLI envoyées vers les périphériques ainsi que l'affichage de l'horodatage dans la console.

Lorsque vous quittez CCA, les préférences sont enregistrées dans un fichier intitulé `.user_preferences`. Le fichier est stocké à l'emplacement suivant :

`C:\Documents and Settings\<`*nom d'utilisateur*`>\.configuration assistant`

Vous pouvez copier ce fichier vers d'autres PC.

Les paramètres propres à chaque onglet de la fenêtre Préférences et les réglages par défaut sont expliqués dans les rubriques suivantes. Si vous modifiez les paramètres par défaut, cliquez sur **Définir les valeurs par défaut** pour les restaurer.

Général

Sous l'onglet Général, vous pouvez définir les préférences de sondage et de démarrage.

Paramètre	Description
Activer le sondage réseau	Le paramètre est désactivé par défaut. Lorsque cette option est active, CCA interroge périodiquement le réseau pour établir l'état du périphérique et détecter les nouveaux. Les informations ainsi obtenues permettent de mettre à jour les fenêtres Topologie, Volet frontal et nombre d'autres fenêtres de fonctions. Lorsque le sondage est désactivé, cliquez sur l'icône **Actualiser** dans la barre d'outils de CCA pour déclencher manuellement le sondage du réseau.
Fréquence d'interrogation du réseau	Lorsque le sondage réseau est actif, ce paramètre définit la fréquence à laquelle CCA analyse le réseau. La valeur par défaut est 5 minutes. Cette option n'est pas disponible lorsque la fonction de sondage réseau est désactivée.
Fréquence d'interrogation LED.	Cet élément définit la fréquence d'interrogation des LED des périphériques gérés par CCA. Pour chaque fréquence, CCA indique les informations de l'interface et les données d'alimentation redondante sous la forme de LED colorés dans la fenêtre Volet frontal. Vous pouvez cliquer sur le bouton à gauche de la fenêtre pour sélectionner le type d'information représenté par la couleur (état de la liaison, vitesse du port, état duplex, état de l'alimentation). La valeur par défaut est 3 minutes.

Paramètre	Description
Fréquence d'interrogation graphique.	Cet élément définit la fréquence d'interrogation des périphériques gérés par CCA afin d'obtenir des informations sur le périphérique et la connexion. Ces informations sont utilisées pour mettre à jour les graphiques de connexion et de bande passante. La valeur par défaut est 5 secondes.
Afficher la fenêtre Topologie lors de la connexion au réseau	Cet élément régit l'affichage de la fenêtre Topologie lorsque CCA est relié à un périphérique. La case est cochée par défaut.
Afficher la vue Volet frontal lors de la connexion au réseau.	Cet élément régit l'affichage du Volet frontal lorsque CCA est relié à un périphérique. La case est décochée par défaut.
Afficher le Tableau de bord lors de la connexion au réseau	Cet élément régit l'affichage de la fenêtre Topologie lorsque CCA est relié à un périphérique. La case est cochée par défaut.

Mise à jour de l'application

Permet de préciser à quelle fréquence vérifier l'existence d'une nouvelle version de CCA.

Dans la liste **Vérifier les mises à jour de l'application**, sélectionnez **Tous les mois**, **Chaque semaine** ou **Jamais**. Si vous sélectionnez **Jamais**, CCA ne fera aucun contrôle périodique. Cependant, vous pouvez vérifier manuellement en cliquant sur **Système** > **Mise à jour de l'application** dans la barre de menus.

Serveurs proxy

Cet onglet vous permet d'indiquer si vous souhaitez utiliser des serveurs proxy pour la connexion à Internet (notamment Cisco.com pour la récupération des mises à jours de CCA).

Pour mettre à niveau CCA vers une nouvelle version, suivez les étapes suivantes.

ETAPE 1 Cochez la case **Activer les serveurs proxy** afin d'activer l'échange par le biais de serveurs proxy. Si vous cochez cette case, vous avez accès aux autres champs.

ETAPE 2 Cochez la case **Utiliser les serveurs proxy pour gérer les périphériques** afin d'activer les échanges sur votre réseau par le biais de serveurs proxy.

ETAPE 3 Pour montrer que le trafic HTTP utilisera un serveur proxy, entrez les valeurs suivantes dans les champs **HTTP** :

- L'adresse IP ou le nom d'hôte du serveur proxy

  Vous pouvez utiliser un nom d'hôte pour identifier un serveur proxy si un serveur DNS a été défini pour la résolution du nom d'hôte.

- Le numéro du port HTTP

ETAPE 4 Pour montrer que le trafic HTTPS utilisera un serveur proxy, entrez les valeurs adéquates dans les champs **HTTPS**.

Archive des configurations

Cet onglet permet de définir les préférences quant à la sauvegarde d'une configuration enregistrée sur un périphérique.

Suivez les étapes ci-dessous :

ETAPE 1 Cochez la case **Enregistrer la configuration sur le périphérique avant la sauvegarde** si vous souhaitez que CCA enregistre la configuration en cours sur le périphérique avant de la sauvegarder.

ETAPE 2 Dans le champ **Répertoire de sauvegarde**, remplacez le chemin utilisé pour la sauvegarde des configurations si vous souhaitez les enregistrer à un autre endroit.

État

Cochez les cases concernant les différentes catégories que CCA doit contrôler.

La **Fréquence d'interrogation de l'état** vous permet de définir la fréquence des mises à jour des mesures figurant dans la fenêtre État et Détails de l'état.

Activité d'utilisation

La fonction de suivi Activité d'utilisation permet de fournir automatiquement des informations sur l'utilisation de CCA dans le déploiement des services Cisco SBCS. Les données partagées grâce à cette fonction permettent à Cisco d'améliorer la qualité du logiciel.

Le suivi de l'activité d'utilisation est activé par défaut conformément au Contrat de licence de l'utilisateur final (CLUF) de CCA. Pour afficher le CLUF, cliquez sur **Aide** > **À propos de** dans le menu principal de CCA et cliquez sur Contrat de licence de l'utilisateur final.

Annulez la sélection de l'option **Activer la collecte de l'activité d'utilisation** pour désactiver la collecte d'informations et la transmission de ces informations à Cisco.

Lorsque cette option est activée, seules les données d'utilisation sont rassemblées :

- Version de CCA et internationalisation
- Types de périphériques gérés par CCA
- Version logicielle pour chaque périphérique géré (par exemple : version Cisco IOS, version du microprogramme du commutateur et version logicielle Cisco Unity Express-CUE).
- Actions de l'utilisateur
  - Lancement des fenêtres de fonctions
  - Événements de navigation par onglets dans les fenêtres de fonctions et les boîtes de dialogue
- Quand CCA applique une configuration à un périphérique

  Aucune information propre à la configuration n'est enregistrée sauf en cas de modifications apportées par l'utilisateur à la configuration.
- L'adresse IP publique du PC sur lequel CCA est installé et à partir de laquelle les données sont envoyées.

  Il s'agit du WAN ou de l'adresse IP gérés et affectés par votre Fournisseur de services Internet au routeur ou au pare-feu sur votre site.
- Horodatage de chaque événement
- Utilisation du VLAN
  - Indique si l'adresse IP par défaut est utilisée ou non pour le VLAN1 sur l'UC500 (192.168.10.x). CCA n'enregistre pas l'adresse IP du VLAN1. Il vérifie uniquement si la valeur par défaut est utilisée.
  - Nombre total de VLAN
- Utilisation des Smartports : Type de profil Smartport appliqué
- Utilisation du VPN : Types de VPN actifs (EasyVPN, SSL VPN ou VPN de site à site). Les VPN téléphoniques ne sont pas pris en charge.

- Utilisation des trunks SIP
  - Indique si les trunks SIP sont actifs ou non
  - Si la fonction est activée, le fournisseur de trunk SIP est indiqué
- Utilisation sans fil
  - Indique si la fonction sans fil est active ou non
  - Type de sécurité sans fil utilisée
  - Total des SSID configurés
- Utilisation de la mémoire flash de l'UC500 : Espace disponible et espace total sur la mémoire flash en Mo

Les informations suivantes NE sont PAS collectées :

- Les noms des clients, les adresses ou toute autre donnée permettant l'identification des personnes
- Les numéros de série ou les identifiants
- Les noms d'hôte ou les adresses IP des périphériques se trouvant derrière le routeur ou le pare-feu de votre site
- Les numéros de téléphone ou toute autre information permettant d'identifier un client ou un VAR
- Les noms d'utilisateur ou les mots de passe Cisco.com
- Les noms d'utilisateur ou les mots de passe configurés sur le périphérique

Les données relatives à l'utilisation sont stockées dans un fichier texte sur le PC exécutant CCA. Elles sont ensuite envoyées à un serveur hébergé par Cisco par session. Une fois les informations envoyées, elles sont supprimées du PC de l'utilisateur.

Une alerte de notification d'événements est créée à chaque fois que les données relatives à l'utilisation sont envoyées.

Journalisation

Sous l'onglet Journalisation, vous pouvez définir les préférences d'affichage dans les fichiers journaux de CCA et la Console.

Paramètre	Description
Journalisation du contenu	Ces paramètres régissent l'affichage des données CLI dans les fichiers journaux et l'horodatage dans la Console de CCA. ▪ Les données CLI s'affichent par défaut dans les fichiers journaux de CCA. Cette option est active par défaut au lancement de l'application. Pour désactiver l'affichage des données CLI dans les fichiers journaux, désactivez l'option **Activer l'affichage des CLI dans le journal**. Si l'utilisateur quitte CCA et redémarre l'application, cette option est activée par défaut. ▪ Cette option est active par défaut au lancement de l'application. Pour désactiver l'horodatage dans la Console CCA, désactivez l'option **Activer l'affichage de l'horodatage dans la Console** (pour ouvrir la Console, appuyez sur F2). Si l'utilisateur quitte CCA et redémarre l'application, cette option est activée par défaut.

Avancé

Configurez les paramètres suivants sous l'onglet Avancé.

Paramètre	Description
Activer le son au démarrage	Cochez l'option **Activer le son au démarrage** si vous souhaitez entendre le son Cisco .wav au démarrage.
Activer CLI Postview pour les fonctions vocales de l'IOS	Cochez l'option **Activer CLI Postview pour les fonctions vocales de l'IOS** si vous souhaitez afficher la liste des commandes Cisco IOS envoyées au routeur après que des modifications aient été apportées à la fenêtre de configuration. Les commandes s'affichent dans une fenêtre contextuelle après l'application des modifications.

Paramètre	Description
Image d'arrière-plan du bureau	Pour sélectionnez un autre arrière-plan, cliquez sur **Parcourir** et accédez à l'emplacement du fichier souhaité sur le PC local. Cliquez ensuite sur **OK** ou sur **Appliquer**. Les images au format .png et .jpg sont prises en charge. Si l'image est trop grande, elle sera réduite. Si l'image est trop petite, elle sera affichée en mosaïque.

Notification des messages système

La fenêtre Notification des messages système s'affiche lorsque vous sélectionnez l'option **Système** > **Notification des messages système** dans la barre de menus de CCA.

Vous pouvez recevoir par e-mail des notifications de messages système que vous souhaitez. Les messages système peuvent concerner n'importe quel événement du site client, allant des urgences et des alertes (niveaux de gravité 0 et 1) aux messages d'information ou de débogage (niveaux de gravité 6 et 7).

Pour activer cette fonction, vous devez effectuer les opérations suivantes :

- Permettre à un serveur SMTP d'envoyer des notifications de messages système par e-mail
- Définir un nom pour la notification

Pour configurer notifications de messages système, procédez comme suit :

ETAPE 1 Dans le champ **Serveur E-mail (SMTP)**, introduisez le nom du serveur SMTP qui enverra les notifications.

ETAPE 2 Dans le champ **Adresse e-mail de l'expéditeur**, introduisez une adresse e-mail que le SMTP affichera comme expéditeur des notifications. Dans la terminologie SMTP, cette adresse est appelée adresse de retour.

ETAPE 3 Cliquez sur **E-mail de test** afin de tester la connexion entre le serveur SMTP et l'adresse e-mail de l'expéditeur. Si l'expéditeur reçoit l'e-mail test, cela signifie que la connexion a été vérifiée.

ETAPE 4 Cliquez sur **Créer** et utilisez la fenêtre Créer une notification. Voir la rubrique **Créer ou modifier une notification système, page 62**.

Lorsque vous avez terminé, le nom de la nouvelle notification apparaît dans la Liste des Notifications et la case Active est cochée.

ETAPE 5 Cliquez sur **OK** ou **Appliquer**.

Pour modifier les informations contenues sous un nom de notification, sélectionnez le nom, cliquez sur **Modifier**, et utilisez la fenêtre Modifier la notification.

Pour supprimer un nom de notification, sélectionnez le nom et cliquez sur **Supprimer**.

Créer ou modifier une notification système

Cette fenêtre s'affiche lorsque vous cliquez sur **Créer** ou **Modifier**dans la fenêtre Notification des messages système. Utilisez cette fonction pour les opérations suivantes :

- Nom de notification
- Adresse e-mail des destinataires
- Type de message en fonction du niveau de sécurité dont les destinataires souhaitent avoir connaissance

Pour créer ou modifier une notification système, procédez comme suit :

ETAPE 1 Introduisez ou modifiez un nom dans le champ **Nom de la notification**.

ETAPE 2 Introduisez ou modifiez une adresse e-mail dans le champ **Adresse e-mail**. Il s'agit de l'adresse à laquelle les destinataires recevront les notifications.

ETAPE 3 Indiquez les types de messages que les destinataires recevront en cochant les cases se trouvant à côté des niveaux de gravité relatifs à ces messages.

Si vous cochez un niveau de gravité supérieur à 3, les destinataires risquent d'obtenir davantage de notifications.

ETAPE 4 Cliquez sur **OK**.

Utilisation de l'aide en ligne

L'aide en ligne de CCA s'affiche dans une fenêtre distincte contenant les éléments suivants :

- Barre d'outils avec les boutons de navigation Précédent, Suivant et Accueil, un bouton Imprimer le PDF et la zone de texte Rechercher.
- Les liens vers la table des matières et l'index sur la gauche
  - La table des matières s'affiche par défaut. Cliquez sur le lien Index pour accéder à l'index de l'aide.
  - Cliquez sur les icônes représentant un livre pour agrandir ou réduire la liste des rubriques.
  - En mode Index, vous pouvez introduire un mot ou une phrase dans la zone de recherche au-dessus de la liste afin de rechercher l'entrée d'index.
- La rubrique d'aide active se trouve sur la droite

Pour de meilleurs résultats, activez JavaScript dans votre navigateur Internet Explorer. Le cas échéant, dans la Barre d'informations, choisissez l'option autorisant l'affichage du contenu bloqué afin que vous puissiez afficher et utiliser les commandes de navigation et d'interface de l'aide.

Accès à l'aide en ligne

Pour accéder à l'aide en ligne

- Cliquez sur **Aide** dans une fenêtre ou une boîte de dialogue
- Appuyez sur **F1** pour accéder à l'aide pour la fenêtre active
- Sélectionnez l'une des options du menu Aide dans la barre de menus en haut de la fenêtre principale :
  - **Table des matières**. Affiche la présentation de la rubrique CCA.
  - **Nouveautés**. Affiche les liens vers les informations relatives aux nouvelles fonctions de la dernière version et des versions antérieures.
  - **Aide pour la fenêtre active**. Affiche l'aide en ligne pour la fenêtre active. Si plusieurs fenêtres sont ouvertes, la fenêtre active est celle qui est actuellement utilisée.

Effectuer une recherche dans l'aide en ligne

Pour effectuer une recherche dans l'aide en ligne, entrez un mot ou une suite de mots dans la zone de texte en haut à droite de l'aide en ligne et cliquez sur **Rechercher**. Les correspondances partielles sont affichées mais les recherches à base de caractères jokers (par exemple : * et .) ne sont pas prises en charge.

Lorsque vous cliquez sur **Rechercher**, la page affiche les résultats de la recherche.

- Cliquez sur le lien permettant d'afficher la rubrique contenant les correspondances pour le terme recherché. Les correspondances sont surlignées.
- Cliquez sur l'icône pour afficher la rubrique dans une nouvelle fenêtre pour que vous puissiez facilement revenir à la page des résultats.

Ouvrir le fichier PDF de l'aide en ligne

Cliquez sur le bouton **PDF** de la barre d'outils de la fenêtre Aide pour afficher un document PDF contenant l'intégralité de l'aide en ligne au format PDF.

Cela vous permet d'enregistrer ou d'imprimer une copie de l'aide pour une consultation hors ligne.

Imprimer les rubriques d'aide

Cliquez sur le bouton **Imprimer** de la barre d'outils de la fenêtre Aide pour imprimer la rubrique active.

Pour imprimer les données des fenêtres de CCA, vous pouvez utiliser l'impression Java. Voir la rubrique **Impression des fenêtres, des rapports et des graphiques de CCA, page 65**.

Impression des fenêtres, des rapports et des graphiques de CCA

Pour imprimer une fenêtre de CCA, un affichage ou un graphique, suivez les étapes ci-dessous.

ETAPE 1 Activez l'objet que vous souhaitez imprimer.

ETAPE 2 Sélectionnez **Système** > **Imprimer** dans la barre de menus afin d'envoyer le fichier à imprimer vers une imprimante.

Lorsque vous imprimez une fenêtre, le résultat se présente sous la forme d'un rapport. Dans ce format, vous retrouvez toutes les données de la fenêtre comme si vous utilisiez la fonction **PrtSc** afin d'imprimer l'écran. La date et l'heure y figurent également et les pages sont numérotées.

Remarques

- Les fenêtres de l'Assistant de configuration de la téléphonie, de l'Assistant de configuration sans fil, du Gestionnaire multi-sites, de l'Assistant de configuration de la surveillance vidéo, de l'Assistant de configuration de la sécurité, de l'Assistant de configuration du téléphone VPN et du Tableau de bord ne peuvent pas être imprimées.
- Si l'objet que vous souhaitez imprimer est inactif en raison d'un message d'erreur, vous ne pourrez pas l'imprimer avant d'avoir fermé la boîte de dialogue et de l'avoir réactivé.
- Pour imprimer une sous-fenêtre (fenêtre secondaire qui s'affiche lorsque vous cliquez sur un bouton de la fenêtre principale), celle-ci doit être ouverte et active.
- Lors de l'impression de la fenêtre Topologie ou Volet frontal, la fenêtre Aperçu avant impression (**Système** > **Aperçu avant impression**) présente une option **Ajuster à la page**. Cochez cette option si vous souhaitez que tout soit imprimé sur une seule page.

2

Nouveautés

Pour plus d'informations sur les nouvelles fonctions et les périphériques pris en charge sous Cisco Configuration Assistant, consultez les rubriques suivantes :

- **Version actuelle, page 67**
- **Dernières versions, page 68**

Version actuelle

Version 3.0(1)

La version 3.0(1) de CCA permet de résoudre les erreurs rencontrées sous CCA 3.0.

Fonction	Description
Configuration de la fonction vocale	
Etat Mobilité de poste	Cette nouvelle fenêtre permet d'accéder aux données Mobilité de poste, de profil et d'état (**Superviser** > **Téléphonie** > **Etat Mobilité de poste**). Ces données sont en lecture seule. Pour configurer ces paramètres, voir **Mobilité de poste, page 343**.
Modification et amélioration de l'interface utilisateur	
Arrière-plan personnalisé	Permet à l'utilisateur de définir une image d'arrière-plan personnalisée à partir de l'option **Préférences...** du menu **Système.** Cliquez ensuite sur l'onglet **Avancé**. Pour configurer d'autres éléments pour CCA, accédez à la rubrique **Définition des préférences, page 54**.

Dernières versions

Version 3.0

La version 3.0 de CCA est une importante mise à niveau du logiciel. Elle comprend plusieurs nouvelles fonctions et autant de modifications de l'interface.

Voir les *Notes de version pour Cisco Configuration Assistant 3.0* pour obtenir la liste des problèmes connus résolus dans cette version et des données actualisées sur les paquets logiciels et de localisation de l'UC500.

Fonction	Description.
Compatibilité du matériel	
Modèle Cisco 69xx Prise en charge des téléphones IP	CCA 3.0 prend en charge la configuration des téléphones IP Cisco 6901, 6911, 6921, 6941 et 6961. Les mises à niveau du microprogramme des téléphones par glisser-déposer sont également possibles.
Paquet logiciel et de localisation	
Prise en charge de la version 8.1.0 du paquet logiciel de l'UC500	CCA 3.0 prend en charge la version 8.1.0 du paquet logiciel de l'UC500. Pour plus d'informations, consultez les *Notes de version pour la version 3.0 de Cisco Configuration Assistant*. Voir la rubrique **Paquets logiciels de l'UC500, page 546**.
Prise en charge du paquet de localisation pour l'UC500	CCA 3.0 prend en charge l'installation des fichiers de localisation à l'aide des paquets prévus pour l'UC500. Les paquets de localisation pour l'UC500 peuvent aussi être téléchargés à partir de Cisco.com à l'adresse www.cisco.com/go/uc500swpk. Chaque paquet de localisation contient des fichiers de langue, les fichiers de langue pour la messagerie, les sonneries réseau et les cadences pour une région donnée. Voir la rubrique **Paquets de localisation pour l'UC500, page 546**.
Configuration de la fonction vocale	
Mobilité de poste	Activez la fonction Mobilité de poste et configurez les paramètres généraux, les profils d'utilisateur et de téléphone pour la fonction MP. Cette fonction permet aux utilisateurs d'accéder à chaque téléphone MP ainsi qu'aux aspects de ligne, à la messagerie vocale et aux touches rapides. Voir la rubrique **Mobilité de poste, page 343**.
Postes flottants	Ajoutez les postes non associés à un téléphone physique. Voir la rubrique **Postes flottants, page 340**.
Notification par la messagerie vocale	Activez la notification des messages de la messagerie par e-mail ou par téléphone et définissez les paramètres des notifications. Voir la rubrique **Messagerie et notifications, page 374**.

Fonction	Description.
T.37 Fax vers e-mail	Enregistrez les messages T.37 Fax vers e-mail et transférez-le comme annexes. **T.37 Fax vers e-mail, page 454**.
Délai d'expiration SNR	Configurez les délais d'expiration pour la fonction Single Number Reach (SNR). La fenêtre SNR se trouve désormais sous l'option **Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Utilisateurs et téléphones**. Voir la rubrique **Single Number Reach (SNR), page 389**.
Délai d'expiration et rappel pour le parcage d'appels	Permet de définir les paramètres associés au délai d'expiration et au rappel pour les appels parqués. Voir la rubrique **Parcage d'appels, page 413**.
Alerte sonore pour la mise en attente des appels	Vous pouvez définir une sonnerie répétitive pour signaler à l'utilisateur lorsqu'un appel est mis en attente sur un téléphone IP Cisco. Voir la rubrique **Onglet Alerte d'appel en attente, page 361**.
Paramètres détaillés du port FXO	Permet de définir les paramètres de port FXO avancés pour les fonctions de compression-expansion, déconnexion de supervision, inversion de batterie, audio et temporisateurs. Il est aussi possible de copier les paramètres de port. Voir la rubrique **Configuration des paramètres des ports FXO, page 313**.
Bip pour enregistrement en direct	Permet de définir la durée du signal sonore et de l'intervalle pour la fonction Enregistrer en direct. Voir la rubrique **Enregistrer en direct, page 452**.
Importation améliorée pour les données globales des utilisateurs et des téléphones	Importez massivement les données des utilisateurs et des téléphones à l'aide de l'Assistant de configuration de la téléphonie ou de la fenêtre Utilisateurs et téléphones. Les procédures permettant de préparer et d'importer les données utilisateurs ont varié depuis les versions précédentes. Voir la rubrique **Importation des données du téléphone pour plusieurs utilisateurs (Importation massive), page 334**.

Fonction	Description.
Configuration du réseau	
Mappage NAT statique	Si la connexion WAN est associée à une adresse IP statique ou une adresse IP PPPoE négociée, vous pouvez configurer les mappages NAT statiques. Voir la rubrique **Fenêtre NAT (IP statique ou PPPoE avec IP statique), page 259**.
Etapes modifiées pour la création de VLAN	L'interface pour la création et la configuration des VLAN a été modifiée. Vous pouvez configurer l'adressage IP pour les VLAN à partir de la fenêtre VLAN et y configurer le VLAN voix par défaut. Voir la rubrique **VLANs, page 168**.
Maintenance	
Localisation de l'UC, installation du logiciel et mise à jour simplifiées	Un assistant d'installation distinct a été ajouté pour les mises à niveau de l'UC500. Il est accessible à partir de la fonction **Maintenance** > **Mise à jour du logiciel** > **UC500**. L'Assistant simplifie l'installation du logiciel et facilite la localisation. Voir la rubrique **Mises à jour des logiciels, page 548**.
Basculement entre les langues primaire et alternative pour le téléphone et la messagerie vocale	Les paramètres régionaux ont été simplifiés. Vous avez le choix entre les langues primaires et secondaires installées sur l'UC500 sans devoir réinstaller CUE. Voir les rubriques **Localisation de l'UC500 (paramètres hors USA/UK), page 569** et **Paramètres régionaux pour la téléphonie, page 302**.
Charger et télécharger les fichiers vers et à partir de la mémoire flash de l'UC500	La fenêtre Gestion des fichiers contient les options permettant de charger et télécharger les fichiers vers la mémoire flash de l'UC500. Voir la rubrique **Gestion des fichiers, page 570**.
Activer ou désactiver le sondage réseau	L'onglet Général de la fenêtre Préférences fournit désormais la possibilité d'activer ou désactiver le sondage réseau. Le paramètre est désactivé par défaut. Voir la rubrique **Général, page 55**.

Fonction	Description.
Modification et amélioration de l'interface utilisateur	
Modifications apportées au menu Configuration de la téléphonie	Les menus de la rubrique **Configurer** > **Téléphonie** ont été réorganisés et renommés. Voir la rubrique **Utilisateurs et téléphones, page 327**. Ces modifications concernent les éléments suivants : ▪ La fenêtre Voix a été renommée Utilisateurs et téléphones. Elle se trouve désormais sous **Configurer** > **Téléphonie** > **Utilisateurs et postes**. Les paramètres des onglets Système et Réseau ont été supprimés de la fenêtre Voix. Les paramètres du système vocal sont définis à partir de la fenêtre Paramètres système sous **Configurer** > **Téléphonie** > **Système**. ▪ La fenêtre Région se trouve désormais sous **Configurer** > **Téléphonie** > **Système**. ▪ La fenêtre Single Number Reach se trouve désormais sous **Configurer** > **Téléphonie** > **Utilisateurs et postes**. ▪ La fenêtre Numérotation abrégée système se trouve désormais sous **Configurer** > **Téléphonie** > **Utilisateurs et postes**. Les touches d'appel rapide pour les téléphones d'utilisateurs sont désormais paramétrées à partir de la fenêtre Utilisateurs et téléphones. ▪ La fenêtre Messagerie se trouve désormais sous **Configurer** > **Téléphonie** > **Utilisateurs et postes**. ▪ Les fenêtres Standard automatique, Programmes, Basic ACD, Service de nuit et Enregistrer en direct se trouvent désormais sous **Configurer** > **Téléphonie** > **Système**. ▪ La fenêtre Paramètres des ports analogiques a été renommée Ports FXS. Elle se trouve désormais sous **Configurer** > **Téléphonie** > **Ports et trunks**. ▪ Les fenêtres Gestionnaire multi-sites et Nombre d'appels maximum se trouvent désormais sous **Configurer** > **Téléphonie** > **Gestion de site**.

Version 2.2(6)

CCA 2.2(6) résout les problèmes rencontrés avec la version CCA 2.2(5) et assure la prise en charge du paquet logiciel 8.0.5 de l'UC500 qui contient notamment la version 8.0.3 de Cisco Unity Express (CUE).

Pour plus d'informations, consultez les *Notes de version pour la version 2.2(6) de Cisco Configuration Assistant* disponible sur Cisco.com.

Version 2.2(5)

La version 2.2(5) de CCA prend en charge ces périphériques et présente les améliorations ainsi que les modifications suivantes au niveau de l'interface.

Voir les *Notes de version pour Cisco Configuration Assistant 2.0 et les versions ultérieures* pour obtenir la liste des problèmes connus résolus dans cette version.

Fonction	Description.
Prise en charge de la version 8.0.4 du paquet logiciel de l'UC500	CCA 2.2(5) est compatible avec le paquet logiciel pour l'UC500 version 8.0.4. Pour plus d'informations sur les versions des composants du paquet logiciel, voir les *Notes de version pour Cisco Configuration Assistant 2.0 et les versions ultérieures*.
Prise en charge de Windows 7 (64-bits et 32 bits)	CCA peut désormais être utilisé sur des PC sous Microsoft Windows. Les versions de 64 et 32 bits sont prises en charge. Pour plus d'informations sur les restrictions associées à CCA et Windows 7, voir les *Notes de version pour Cisco Configuration Assistant 2.0 et les versions ultérieures*. **REMARQUE** Le contrôle de compte utilisateur de Windows 7 doit être désactivé afin de permettre les mises à niveau en glisser-déposer ainsi que les opérations sur les fichiers.
Contrôle de compatibilité de version CCA	Au démarrage de CCA, la fenêtre de conflit de version de CCA s'affiche si la version que vous utilisez est antérieure à celle qui a été utilisée pour configurer le système. Vous pouvez fermer la fenêtre ou opter pour la mise à jour vers une nouvelle version de CCA. Voir la rubrique **Contrôle de compatibilité de version CCA, page 20**.

Fonction	Description.
Nouveaux périphériques pris en charge :	Téléphones IP. CCA 2.2(5) prend désormais en charge les modèles de téléphone IP Cisco Small Business suivants : ▪ Cisco SPA 525G2 ▪ Cisco SPA 300, tous les modèles Les mises à niveau de charge de téléphone en glisser-déposer sont prises en charge pour ces nouveaux téléphones.
Intecom appelable	Vous pouvez configurer les intercoms appelables à l'aide de CCA. Ces éléments sont définis sous l'onglet Postes utilisateurs de la fenêtre (**Configurer** > **Téléphonie** > **Utilisateurs et postes**> **Utilisateurs et téléphones**). Pour de plus amples informations, consultez la rubrique **Intercom appelable, page 368**.
Intercoms Whisper	Vous pouvez configurer les intercoms Whisper à l'aide de CCA. Ces éléments sont définis sous l'onglet Postes utilisateurs de la fenêtre (**Configurer** > **Téléphonie** > **Utilisateurs et postes**> **Utilisateurs et téléphones**). Pour de plus amples informations, consultez la rubrique **Intercom Whisper, page 371**. La fonction Intercom Whisper est uniquement disponible sur les téléphones prenant en charge les lignes octales.
Conference Barge, Privacy et poste partagé à ligne octale	Vous pouvez configurer les paramètres de confidentialité pour Conference Barge à l'aide de CCA. cBarge et Privacy nécessitent la configuration de numéros de poste partagés avec ligne octale. cBarge et Privacy peuvent être configurés à l'aide de la fenêtre Conference Barge (**Configurer** > **Téléphonie** > **Fonctions vocales** > **Conference Barge**). Les postes de ligne octale partagée sont définis sous l'onglet Postes utilisateurs de la fenêtreVoix (**Configurer** > **Téléphonie** > **Utilisateurs et postes**> **Utilisateurs et téléphones**). Pour de plus amples informations, consultez la rubrique **Conference Barge, page 420**.

Fonction	Description.
Activation ou désactivation des tonalités d'arrivée et de départ pour les téléconférences	Vous pouvez désormais activer ou désactiver les tonalités émises lorsque les appelants rejoignent ou quittent une téléconférence. Pour accéder à ces paramètres, sélectionnez **Configurer** > **Téléphonie** >**Fonctionnalités voix** > **Conférence**. L'option Conférence à plusieurs doit être active.
Groupes de radiomessagerie combinés	CCA prend désormais en charge les groupes de radiomessagerie combinés. Cette fonction permet aux groupes de radiomessagerie d'être membres des groupes de radiomessagerie. Pour configurer les groupes de radiomessagerie, sélectionnez **Configurer** > **Téléphonie** > **Groupes de téléphones** > **Groupes de radiomessagerie** dans la barre de fonctions. Pour de plus amples informations, consultez la rubrique **Groupes de radiomessagerie, page 405**.
Poste de chevauchement sur la ligne SC	Vous pouvez configurer un poste de chevauchement pour la ligne du siège central (SC) à l'aide de CCA. Pour de plus amples informations, consultez la rubrique **Poste de chevauchement, page 366**.
Diagnostic de connectivité CUE	Dans la fenêtre Diagnostic de connectivité CUE (**Dépanner** > **Diagnostic CUE** > **Diagnostic de connectivité CUE**), vous pouvez vérifier la connexion avec le module CUE de l'UC500, générer des fichiers journaux et mettre en œuvre des tâches de récupération de sorte à activer un état connu sur le module. Pour de plus amples informations, consultez la rubrique **Diagnostic de connectivité CUE, page 629**.
Capture PCM	Dans la fenêtre Capture PCM (**Dépanner** > **Diagnostic téléphonie** > **Capture PCM**), vous pourrez effectuer une capture PCM pour résoudre les problèmes associés au son, comme une faible qualité sonore, une communication unidirectionnelle ou l'absence de son. Pour de plus amples informations, consultez la rubrique **Capture PCM, page 626**.

Fonction	Description.
Diagnostic de l'enregistrement des trunks SIP	La fenêtre Enregistrement de trunk SIP (**Dépanner** > **Diagnostic téléphonie** > **Enregistrement des trunks SIP**) affiche les données d'enregistrement SIP et fournit les outils de diagnostic pour le dépannage des problèmes d'inscription des trunks SIP. Pour de plus amples informations, consultez la rubrique **Enregistrement des trunks SIP, page 619**.
Nouveau script par défaut pour le SA	Le script **aa_sbcs_v03.aef** est à présent le script par défaut pour le Standard automatique. Cette version du script du SA permet le transfert des appels vers un numéro donné si l'appelant n'agit pas au terme de trois lectures du message d'accueil principal. Pour de plus amples informations, consultez la rubrique **Configuration du standard automatique, page 433**.

Fonction	Description.
Améliorations diverses de la fonction de téléphonie	Vous pouvez désormais activer ou désactiver le blocage des appels et définir les autorisations pour les téléphones de zone commune et les fax. Ces éléments sont définis sous l'onglet Postes utilisateurs de la fenêtre (**Configurer** > **Téléphonie** > **Utilisateurs et postes**> **Utilisateurs et téléphones**). Une option **Utiliser comme téléphone de télétravailleur** a été ajoutée à l'onglet Postes utilisateurs. Lorsque l'option est cochée, le point MTP (Media Termination Point) est configuré sur le téléphone sélectionné. Voir la rubrique **Postes utilisateurs, page 328**. Une option **Autoriser les appels vidéo** a été ajoutée à l'onglet Postes utilisateurs de la fenêtre Voix pour les téléphones prenant en charge la vidéo point à point. Lorsque l'option est cochée, la fonction Cisco Unified Voice Advantage (CUVA) est activée sur le téléphone sélectionné. Voir la rubrique **Postes utilisateurs, page 328**. Vous pouvez à présent **modifier la description s'affichant dans le coin supérieur droit de l'écran des téléphones IP**. Par exemple, vous pouvez modifier ce paramètre pour afficher le numéro DID (appel entrant direct) du téléphone. Dans les versions antérieures, CCA affichait toujours le prénom et le nom de l'utilisateur du téléphone pour cette zone. Ce paramètre est défini à partir de l'onglet Postes utilisateurs de la fenêtre Voix. Voir la rubrique **Postes utilisateurs, page 328**. CCA permet désormais de **désactiver la configuration des codes d'accès à la fonction STCAPP** sur les téléphones analogiques SCCP. Nous vous conseillons de désactiver les codes d'accès STCAPP pour éviter les conflits avec les codes d'accès configurés à l'aide des commandes fac du service de téléphonie. Pour accéder à ce paramètre, sélectionnez l'option **Dépanner** > **Téléphonie Diagnostic** > **Téléphones analogiques SCCP**. La désactivation des codes d'accès de la fonction STCAPP n'affecte pas les codes d'accès à la fonction définis à l'aide des commandes fac du service de téléphonie, car elles sont toujours actives. Voir la rubrique **Postes analogiques SCCP, page 628**.

Fonction	Description.
Prise en charge de la touche HLog pour les groupements de postes standard et BACD	Lorsqu'un groupement de postes BACD, standard ou un groupe d'appels est configuré, la touche HLog est ajoutée aux membres du groupe. Les agents et les membres du groupement de postes peuvent désormais se connecter ou se déconnecter d'un groupement de postes à l'aide de la touche **HLog**. La touche **HLog** s'affiche sur les téléphones du groupement de postes en cas de réception d'un appel. Les utilisateurs peuvent aussi utiliser la touche à partir de l'écran principal du téléphone en appuyant sur la touche **plus**. La touche **HLog** remplace la fonction DnD (Do Not Disturb - Ne pas déranger). DnD est moins polyvalent étant donné que l'abonné est indisponible d'une manière générale et pas seulement pour les appels du groupement de postes.

3

Configuration de base

Cette rubrique vous permet d'en savoir plus sur la connexion de Cisco Configuration Assistant (CCA) à un site client ou à un périphérique autonome afin d'entamer sa configuration. Les rubriques suivantes sont présentées :

- **Créer et gérer les sites clients**
- **Connexion à un site client ou à un périphérique autonome**
- **Utilisation des assistants de configuration de CCA**
  - **Quel assistant utiliser et quand ?**
  - **Assistant de configuration de la téléphonie**
  - **Assistant de configuration de la sécurité**
  - **Assistant de configuration sans fil**
  - **Assistant de configuration de périphérique**
  - **Utilitaire de configuration SR520-T1**
  - **Assistant de configuration du téléphone VPN**
  - **Assistant de configuration de la surveillance vidéo**
- **Sauvegarde et restauration d'une configuration de périphérique**
- **Utilisation de CCA avec Cisco Small Business Office Manager, page 123**
- **Ressources pour la planification et la mise en œuvre de votre solution SBCS**
- **Fonctions Cisco SBCS prises en charge par CCA**

Créer et gérer les sites clients

Cette rubrique vous permet d'en savoir plus sur la création et la gestion des sites clients à l'aide de CCA.

À propos des sites clients

La création d'un site client permet de gérer les périphériques Cisco Smart Business Communications System (SBCS) dans le même groupe logique, et ce, quels que soient leurs emplacements physiques et le logiciel installé. Vous pouvez créer, modifier, supprimer et gérer plusieurs sites clients.

Ce type de site vous permet de configurer et surveiller plusieurs périphériques tels que les UC500 et les SR500 dans une session unique sans devoir reconnecter chaque périphérique séparément. Le site client permet à CCA de mettre en œuvre des fonctions spécifiques, dont la synchronisation des VLAN sur plusieurs plateformes et les déploiements multi-sites.

Un site client peut contenir un maximum de 25 périphériques. Chaque périphérique doit disposer d'une adresse IP. Cisco Configuration Assistant utilise la fonction de recherche automatique des protocoles Cisco Discovery Protocol (CDP) et Bonjour pour trouver des périphériques réseau susceptibles de rejoindre le site et les y ajouter. Si le CDP n'est pas activé sur les périphériques, vous pouvez tout de même créer le site et ajouter les périphériques manuellement.

CCA vous permet de communiquer en toute sécurité avec tous les membres d'un site client. En cas de panne d'un membre du site, vous pouvez continuer à assurer la gestion des autres membres.

La plupart des périphériques réseau (routeurs, commutateurs et contrôleurs WLAN) peuvent faire partie d'un site client. Pour obtenir une liste spécifique des périphériques, veuillez consulter les *Notes de version pour Cisco Configuration Assistant*.

Les membres du site client, comme les routeurs et les points d'accès, prennent en charge plusieurs tâches réseau de base.

- Gestion des accès utilisateur
- Mise à jour du logiciel

- Enregistrement d'une configuration active
- Sauvegarde et restauration d'une configuration
- Gestion de l'heure système
- Réception des notifications des messages système
- Modification du numéro de port HTTP
- Réception du rapport d'inventaire

Planning du site client

Cette rubrique explique les lignes de conduite, les critères et les éléments à maîtriser avant de créer un site client.

Caractéristiques des candidats et des membres

Le terme "Membre" désigne les périphériques réseau qui appartiennent à une communauté. Les *candidats* sont des périphériques réseau qui ne font pas encore partie du site client.

Pour intégrer un site client, un candidat doit répondre aux critères suivants :

- Il doit être pris en charge par CCA
- Il doit disposer d'une adresse IP accessible à partir du PC exécutant CCA
- Les protocoles HTTP et HTTPS doivent être actifs sur les ports par défaut.

  L'accès à ces ports doit être possible si le périphérique se trouve derrière un pare-feu.

Restrictions pour les périphériques du site client

Le nombre maximal est limité à 25 pour les périphériques suivants :

- Plateformes UC500 (UC520, UC540 et UC560)
- Les commutateurs Cisco Small Business Pro ESW 500 (tous modèles et SKU confondus)
- Points d'accès sans fil Cisco AP541N
- Commutateurs Catalyst Express CE520
- Routeurs Cisco 800
- Routeurs Cisco 870

- Routeurs sécurisés Cisco SR500
- Systèmes de sécurité Cisco SA500
- Contrôleurs Cisco 526 Wireless Express
- Points d'accès autonomes Cisco AP521 Wireless Express. Il s'agit de points d'accès complets ne nécessitant aucun contrôleur Cisco 526 Mobility Controller.

Le nombre de téléphones IP ou de points d'accès légers (points d'accès gérés par un contrôleur WLAN) dans un site client n'est pas limité. Le nombre de sites clients pouvant être géré par CCA est illimité.

Outre la limite globale de 25 périphériques, il existe certaines limites propres au type de périphérique :

- Commutateurs Catalyst Express et Cisco Small Business Pro ESW 500 : maximum 15.
- Routeurs Cisco 800 et plateformes Unified Communications 500 : maximum 5.
- Contrôleurs Cisco 526 Wireless Express : maximum 2.
- Points d'accès sans fil Cisco AP541N et points d'accès autonomes Cisco AP521 avec points d'accès intégrés HWIC : maximum 10.

Si la limite globale ou la limite de périphériques est dépassée, vous ne pourrez pas gérer le site client. Vous devrez supprimer des périphériques en fonction des restrictions imposées.

Détection automatique de périphériques

En commençant par l'adresse IP du périphérique initial et les numéros de ports pour les protocoles HTTPS et HTTP, CCA exploite le protocole Cisco Discovery Protocol (CDP) pour dresser la liste des candidats pour le site client se trouvant dans un rayon de quatre bonds CDP par rapport au périphérique initial. Cisco Configuration Assistant peut détecter les périphériques candidats et membres sur plusieurs réseaux et VLAN s'ils disposent d'une adresse IP valable. Voir la rubrique **rubrique "Caractéristiques des candidats et des membres" à la page 81** pour connaître la liste des critères que les périphériques doivent respecter pour être détectés.

IMPORTANT Ne désactivez pas la fonction CDP sur les candidats, les membres ou les périphériques que CCA devra détecter.

Vous pouvez modifier la liste des périphériques détectés en fonction de vos besoins et les ajouter au site client. Si CCA ne détecte pas un périphérique réseau, vous pourrez l'ajouter manuellement.

Pour plus d'informations sur l'ajout des périphériques détectés à un site client ou pour ajouter manuellement ces périphériques à un site client, voir **rubrique "Ajouter un périphérique à un site client existant" à la page 89**.

Noms des sites clients

Lorsque vous créez un site client, CCA vous demande d'introduire un nom. Le nom peut contenir jusqu'à 64 caractères alphanumériques et n'est pas sensible à la casse.

Noms d'hôte

Vous pouvez modifier le nom d'hôte par défaut d'un membre d'un site client. Cette manipulation s'avérera particulièrement utile dans le cadre d'un déploiement multi-sites ou en présence de plusieurs périphériques d'un même type. Par exemple, les points d'accès ou commutateurs AP541N. Pour modifier le nom d'hôte d'un périphérique géré, allez dans **Configurer** > **Périphérique Propriétés** > **Nom de l'hôte**.

Mots de passe

Lorsque vous vous connectez à un site client, CCA vous invite à entrer le mot de passe affecté aux membres du site. Cisco Configuration Assistant tente d'utiliser ces mots de passe pour se connecter aux autres périphériques. Vous devrez introduire un mot de passe uniquement si le mot de passe préalablement saisi ne fonctionne pas pour le périphérique.

IMPORTANT Pour les périphériques Cisco IOS, le mot de passe pour le périphérique doit être identique à celui utilisé pour vous connecter au périphérique à l'aide de CCA.

Par exemple, si le site client contient 10 membres et que cinq d'entre eux ont un mot de passe en commun alors que les cinq autres sont associés à un mot de passe distinct, CCA vous invite à saisir le mot de passe à deux reprises, soit une fois pour chaque mot de passe. Cisco Configuration Assistant n'enregistre pas les mots de passe sur votre PC. Vous devrez donc les introduire à chaque fois que vous tentez de vous connecter à un site.

Protocoles de communication

Cisco Configuration Assistant utilise les protocoles HTTPS, HTTP, Telnet et SSH pour communiquer avec les périphériques. Le système tente d'utiliser le protocole HTTPS lorsqu'il détecte des périphériques voisins et lorsque des périphériques sont ajoutés manuellement à un site client. S'il échoue, il réessaie sous HTTP.

Le port HTTPS est le port 443 alors que le port HTTP correspond par défaut au port 80. Vous pouvez définir un port HTTP différent lorsque vous créez un site client. Utilisez alors la fenêtre Port HTTP pour modifier le port HTTP. Les paramètres des ports HTTPS et HTTP doivent être identiques pour tous les membres du site client.

Données du site client

Cisco Configuration Assistant enregistre toutes les données du périphérique, à savoir l'adresse IP, le nom d'hôte et le protocole de communication sur votre PC local. Lorsque CCA se connecte à un site client, il utilise les données stockées localement pour détecter les périphériques membres.

Si vous essayez d'utiliser un autre PC pour gérer un site client existant, les données relatives au périphérique membre ne sont pas disponibles. Vous devrez à nouveau créer le site client et ajouter les périphériques.

Créer un nouveau site client

La fenêtre Créer un nouveau site client s'affiche lorsque vous cliquez sur **Ajouter un site** sous l'onglet Sites clients de la fenêtre Sites clients ou Connexion.

Si vous débutez sous CCA ou si vous créez un site client pour la première fois, consultez la rubrique **Créer et gérer les sites clients, page 80** pour en savoir plus sur l'objet et les avantages de la création d'un site client pour gérer les périphériques sous CCA.

Utilisez cette fenêtre pour créer un nouveau site client et détecter les périphériques à ajouter au site client.

Procédures

Pour créer un site client, procédez comme suit :

ETAPE 1 Dans le volet **Données du site client**, introduisez le nom du site et sa description.

Le nom du site peut contenir jusqu'à 64 caractères. Vous pouvez utiliser les caractères A-Z, a-z, 0-9, - (tiret) et _ (soulignement).

Dans le champ **Description du site** , introduisez le nom de la société, le nom de l'entreprise ou tout autre texte. Le texte est intégré au SSID lorsque vous créez le SSID propre à votre réseau.

ETAPE 2 *Facultatif.* Cliquez sur **Options de connexion** si vous souhaitez réaliser les opérations suivantes :

- Introduire un numéro de port HTTP (dans le cas où les périphériques du site client n'utiliseraient pas le port 80 par défaut).
- Définir le mode d'accès pour la recherche de périphériques et en cas de connexion à un site client pour la première fois. La valeur par défaut est **Lecture seule** si vous êtes déjà connecté(e) à une communauté dont le mode d'accès est **Lecture seule**, sinon le mode est **Lecture/écriture**.

Voir la rubrique **Options de connexion, page 87**.

ETAPE 3 Dans la rubrique **Ajouter des périphériques au site**, sélectionnez l'option **Entrez une adresse IP** pour le périphérique ou **Exploration des périphériques**.

a. Pour rechercher et ajouter un périphérique autonome au site, sélectionnez l'option **Entrez une adresse IP** pour le périphérique et introduisez l'adresse IP du périphérique que vous souhaitez rechercher.

b. Pour rechercher et ajouter plusieurs périphériques au site, sélectionnez l'option **Exploration des périphériques**. Ce tableau dresse la liste des options affichées dans le menu **Exploration des périphériques**. Il fournit des explications sur les paramètres supplémentaires et décrit les résultats de la recherche et de l'affichage des données dans le tableau Périphériques.

Option	Éléments à introduire	Données affichées par CCA
Exploration des périphériques > À l'aide d'une adresse IP de départ	Adresse IP de départ d'un périphérique dont vous souhaitez ajouter les voisins à votre communauté	Informations relatives au périphérique que vous avez identifié et aux voisins que Cisco Discovery Protocol a détectés à l'aide d'un nombre de sauts égal à 4.
Exploration des périphériques > Dans un sous-réseau	Adresse IP et masque de sous-réseau identifiant un sous-réseau dont vous souhaitez ajouter les périphériques à votre site.	Informations relatives aux périphériques détectés sur le sous-réseau
Exploration des périphériques > Dans une plage d'adresses IP	Adresses IP de départ et de fin définissant une plage composée des périphériques que vous souhaitez ajouter à votre site.	Informations relatives aux périphériques détectés dans la plage d'adresses IP

ETAPE 4 Cliquez sur **Démarrer**.

ETAPE 5 Lors de la détection, le bouton **Démarrage** devient **Arrêter**. Cliquez sur ce bouton si vous souhaitez interrompre la recherche.

Voir **Détection automatique de périphériques, page 82** pour plus d'informations sur le processus de détection des périphériques.

ETAPE 6 Introduisez les codes d'accès pour chaque périphérique. Vous pourriez aussi être invité à accepter les certificats de sécurité pour certains périphériques.

IMPORTANT Pour les périphériques Cisco IOS, le mot de passe pour le périphérique doit être identique à celui utilisé pour vous connecter au périphérique à l'aide de CCA.

Pour de plus amples informations, consultez la rubrique **Mots de passe, page 83**.

REMARQUE Après trois tentatives infructueuses, l'icône du périphérique s'affiche en rouge dans la fenêtre Topologie et le message suivant s'affiche : "Inaccessible : l'autorisation a échoué." Pour retenter la connexion, sélectionnez l'option **Système** > **Connexion**. Vous êtes invité à fermer la session et à redémarrer CCA.

ETAPE 7 Si CCA ne détecte pas un périphérique que vous souhaitez ajouter à votre site client, réessayez l'étape 3 en utilisant une option d'**exploration** différente.

ETAPE 8 Repérez les lignes du tableau correspondant aux périphériques que vous *ne souhaitez pas* ajouter au site client et annulez la sélection.

Un maximum de 25 périphériques peut être sélectionné pour un site client. Ce tableau indique les limites relatives à certains types de périphériques d'un site client. Voir la rubrique **Restrictions pour les périphériques du site client, page 81**.

Les téléphones IP ne doivent pas être explicitement ajoutés à un site client.

ETAPE 9 Cliquez sur **OK** pour ajouter les périphériques sélectionnés au site client.

Le nouveau site client figure sous l'onglet Sites clients.

Options de connexion

Cette fenêtre s'affiche lorsque vous cliquez sur **Options de connexion** dans la fenêtre Créer un nouveau site client ou Modifier un site client.

- Lorsque vous créez un site client et détectez les périphériques à l'aide d'une adresse IP de départ, un sous-réseau ou une plage d'adresses IP, CCA utilise d'abord le protocole HTTPS pour se connecter. Si la connexion par HTTPS échoue, CCA retente la connexion à l'aide du protocole HTTP.

- Lorsque vous utilisez l'option Nom de l'hôte/Adresse IP pour vous connecter à un périphérique seul, CCA se connecte au périphérique à l'aide du protocole défini sous l'onglet Options avancées. Valeur par défaut : HTTPS.
- Lors des connexions suivantes au site client ou à un périphérique autonome, CCA utilise le même protocole que celui utilisé au cours de la détection.

Vous ne pouvez modifier le champ **Port HTTP** que si vous créez un site client. Le champ doit contenir le numéro du port HTTP que CCA utilisera pour communiquer avec les périphériques de la communauté.

Si vous introduisez un numéro de port HTTP autre que le port 80 par défaut, faites-le avant d'ajouter tout autre périphérique au site. Pour changer le numéro de port par la suite, utilisez la fenêtre Port HTTP.

Le numéro de port utilisé pour les connexions HTTPS, à savoir le port 443, ne peut pas être modifié.

Vous pouvez sélectionner un mode d'accès et un niveau de privilège si vous créez un site client. Votre sélection sera utilisée lors de la recherche de périphériques et en cas de connexion à un site client pour la première fois.

Lorsque vous avez terminé, cliquez sur **OK**.

Modifier un site client

Cette fenêtre s'affiche lorsque vous sélectionnez un site client et cliquez sur **Modifier** sous l'onglet Sites clients de la fenêtre Sites clients ou Connexion.

Dans la fenêtre Modifier un site client, vous pouvez ajouter ou supprimer les périphériques pour un site client. Vous pouvez aussi effectuer les opérations suivantes :

- Cliquer sur **Avancé** pour entrer un nouveau numéro de port HTTP si le port HTTP des périphériques du site client est modifié.
- Entrer ou modifier le nom de l'entreprise ou de l'organisation ainsi que tout descriptif figurant dans la section **Description du site**. Le texte est intégré au SSID lorsque vous créez le SSID propre à votre réseau.

Procédures

Pour ajouter ou supprimer un périphérique pour votre site client, suivez les étapes suivantes :

ETAPE 1 Dans la liste **Exploration**, sélectionnez une option. Complétez les champs sous la liste et cliquez ensuite sur **Démarrage**. Consultez la rubrique **Créer un nouveau site client, page 85** pour plus d'informations sur les options permettant de détecter et d'ajouter des périphériques au site.

ETAPE 2 Lors de la détection, le bouton **Démarrage** devient **Arrêter**. Cliquez sur ce bouton si vous souhaitez interrompre la recherche.

ETAPE 3 Si CCA ne détecte pas un périphérique que vous souhaitez ajouter à votre site client, réessayez l'étape 1 en utilisant une option d'**exploration** différente.

ETAPE 4 Repérez les lignes du tableau des périphériques reprenant les périphériques ajoutés que vous *ne souhaitez pas* voir figurer dans le site client et annulez la sélection. Un maximum de 25 périphériques peut être sélectionné pour un site client. Ce tableau indique les limites relatives à certains types de périphériques d'un site client. Voir **Restrictions pour les périphériques du site client, page 81** pour plus d'informations.

ETAPE 5 Pour supprimer les périphériques qui font déjà partie du site client, annulez la sélection des entrées correspondantes dans le tableau Périphériques.

ETAPE 6 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

ETAPE 7 Sélectionnez **Accueil** > **Fenêtre Topologie** pour afficher la fenêtre Topologie. Les icônes des nouveaux périphériques détectés s'affichent dans la fenêtre Topologie.

ETAPE 8 Pour ajouter un périphérique à un site client, cliquez à l'aide du bouton droit de la souris sur l'icône correspondante dans la fenêtre Topologie et sélectionnez **Ajouter au site** dans le menu contextuel.

Ajouter un périphérique à un site client existant

Vous pouvez ajouter un périphérique à un site client existant. Pour ce faire, cliquez sur l'icône du candidat dans la fenêtre Topologie et sélectionnez **Ajouter au site**. Vous devrez introduire le nom d'utilisateur et le mot de passe d'un administrateur.

Afficher la liste des périphériques composant un site client

Suivez les étapes suivantes pour afficher et dresser la liste des périphériques composant le site client et vérifier si le site contient les périphériques escomptés :

ETAPE 1 Sélectionnez **Accueil** > **Topologie** pour afficher la fenêtre Topologie.

ETAPE 2 Sélectionnez l'option **Superviser** > **Inventaire** pour afficher l'inventaire des périphériques composant le site client.

Le récapitulatif contient les références des périphériques, les numéros de série, les versions du logiciel, les données IP et l'emplacement.

ETAPE 3 Sélectionnez **Accueil** > **Panneau frontal** pour afficher le Panneau frontal.

ETAPE 4 Sélectionnez **Accueil** > **Tableau de bord** pour afficher le Tableau de bord.

Gestion des sites clients

Pour gérer les sites clients, sélectionnez l'option **Accueil** > **Sites clients** dans la barre de fonctions.

La fenêtre Sites clients affiche la liste des sites clients existants. Vous pourrez aussi y créer les sites, les modifier ou les supprimer.

Procédures

- Pour créer un site client, cliquez sur **Ajouter un site** pour afficher la fenêtre Créer un nouveau site client. Voir la rubrique **Créer un nouveau site client, page 85**.
- Pour modifier un site client, sélectionnez-le dans la liste et cliquez sur **Modifier le site** pour afficher la fenêtre Modifier un site client. Voir la rubrique **Modifier un site client, page 88**.
- Pour supprimer un site client, sélectionnez le site dans la liste et cliquez sur **Supprimer le site**.

Lorsque vous en avez terminé avec cette fenêtre, cliquez sur **OK**.

Connexion à un site client ou à un périphérique autonome

Au démarrage de CCA, deux fenêtres s'ouvrent : la fenêtre Cisco Configuration Assistant qui contient l'interface utilisateur complète et la fenêtre Connexion.

Vous pouvez également ouvrir la fenêtre Connexion en sélectionnant l'option **Système** > **Connexion** dans la barre de menus.

Cisco Configuration Assistant démarre en mode déconnecté ; il n'est donc connecté à aucun site client ni à aucun périphérique autonome. Dans ce mode, vous pouvez voir la barre de menus dans la fenêtre CCA et certains composants de la barre de fonctions. La barre de fonctions est créée et affiche les fonctions réseau uniquement lorsque CCA est connecté.

Les rubriques suivantes décrivent la manière d'utiliser chaque onglet de la fenêtre Connexion :

- **Onglet Sites clients, page 91**
- **Onglet Nom de l'hôte/adresse IP, page 93**
- **Onglet Options avancées, page 94**

Onglet Sites clients

Pour gérer et configurer plusieurs périphériques sur votre réseau en une même session, créez un site client.

ASTUCE Si vous débutez sous CCA ou si vous créez un site client pour la première fois, consultez la rubrique **Créer et gérer les sites clients, page 80** pour en savoir plus sur l'objet et les avantages de la création d'un site client pour gérer les périphériques sous CCA.

Sous l'onglet Sites clients, vous pouvez effectuer les opérations suivantes :

- Créer un nouveau site client et vous y connecter
- Se connecter à un site client en le sélectionnant dans la liste.
- Modifier ou supprimer un site client existant.

Pour créer et vous connecter à un nouveau site client, procédez comme suit :

ETAPE 1 Sélectionnez l'onglet Sites clients de la fenêtre Connexion et cliquez sur Ajouter un site. La fenêtre Créer un nouveau site client s'affiche.

ETAPE 2 Complétez les champs de la fenêtre Créer un nouveau site client, recherchez les périphériques et ajoutez-les au site en suivant les instructions de la rubrique **Créer un nouveau site client, page 85**.

ETAPE 3 Une fois que vous avez créé le site client, il s'affiche dans la liste sous l'onglet Sites clients de la fenêtre Connexion.

ETAPE 4 Cliquez sur **Connexion**.

Lorsque vous vous connectez à un site client, CCA affiche une fenêtre d'authentification. La fenêtre Périphérique s'affiche afin que vous introduisiez le mot de passe unique affecté aux membres de ce site.

ETAPE 5 Introduisez les codes d'accès pour chaque périphérique. Vous pourriez aussi être invité à accepter les certificats de sécurité pour certains périphériques.

IMPORTANT Pour les périphériques Cisco IOS, le mot de passe pour le périphérique doit être identique à celui utilisé pour vous connecter au périphérique à l'aide de CCA.

Pour de plus amples informations, consultez la rubrique **Mots de passe, page 83**.

REMARQUE Après trois tentatives infructueuses, l'icône du périphérique s'affiche en rouge dans la fenêtre Topologie et le message suivant s'affiche : "Inaccessible : l'autorisation a échoué." Pour retenter la connexion, sélectionnez l'option **Système** > **Connexion**. Vous êtes alors invité à fermer la session et à redémarrer CCA.

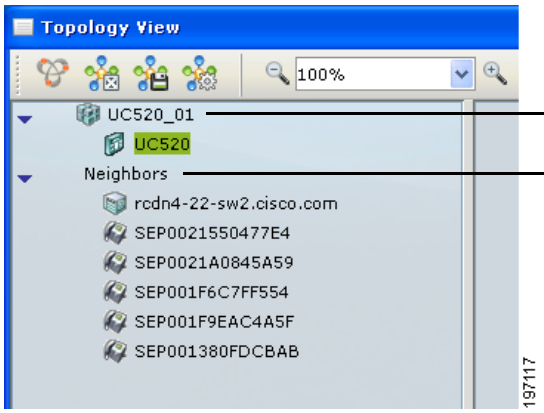
Si vous êtes correctement identifié, une session CCA est établie. Vous ne pouvez lancer qu'une session à la fois sur le PC.

Lorsque vous êtes connecté au site client, la barre d'état au bas de la fenêtre affiche le message "**Détection de la topologie**" tandis que CCA recherche les périphériques et prépare la topologie. Voir la rubrique **Fenêtre Topologie, page 33**.

Une fois que les données de topologie ont été chargées, les données de configuration de la voix sont introduites. La barre d'état au bas de la page affiche le message "**Chargement des données associées à la voix**".

Attendez la fin du chargement des données avant d'ouvrir une quelconque fenêtre associée à la voix ou à la téléphonie.

Les périphériques qui font partie de ce site sont repris dans le volet gauche de la fenêtre Topologie (commutateurs, points d'accès, etc.). Les téléphones et les périphériques qui ne font pas partie du site client sont repris dans la rubrique Voisins du volet gauche. Bien que les téléphones IP figurent sous la rubrique Voisins, ils sont configurés à l'aide de CCA.



Pour mettre fin à une session, fermez la fenêtre de CCA ou sélectionnez **Système** > **Quitter**. Vous devrez enregistrer les modifications apportées à la configuration au cours de la session afin de les appliquer à un périphérique ou à tous.

Pour modifier les paramètres d'un site existant, sélectionnez le site client dans la liste et cliquez sur **Modifier**. Voir la rubrique **Modifier un site client, page 88**.

Pour supprimer un site client, sélectionnez le site dans la liste et cliquez sur **Supprimer**.

Onglet Nom de l'hôte/adresse IP

Utilisez l'onglet Nom de l'hôte/Adresse IP lorsque vous voulez vous connecter ou gérer un périphérique autonome en introduisant son nom d'hôte ou son adresse IP.

Pour vous connecter à un périphérique seul, procédez comme suit :

ETAPE 1 Cliquez sur l'onglet **Nom de l'hôte/Adresse IP**, entrez ou sélectionnez un nom d'hôte ou une adresse IP correspondant au périphérique.

ETAPE 2 Cliquez sur **Connexion**.

ETAPE 3 Entrez le nom d'utilisateur et le mot de passe pour l'identification.

IMPORTANT Pour les périphériques Cisco IOS, le mot de passe pour le périphérique doit être identique à celui utilisé pour vous connecter au périphérique à l'aide de CCA.

Si vous êtes correctement identifié, une session CCA est établie. Vous ne pouvez lancer qu'une session à la fois sur le PC.

REMARQUE Après trois tentatives infructueuses, l'icône du périphérique s'affiche en rouge dans la fenêtre Topologie et le message suivant s'affiche : "Inaccessible : l'autorisation a échoué." Pour retenter la connexion, sélectionnez l'option **Système** > **Connexion**. Vous êtes alors invité à fermer la session et à redémarrer CCA.

Onglet Options avancées

Sous l'onglet **Options avancées**, vous pouvez choisir d'accorder un accès en **Lecture/Écriture** pour cette connexion.

Lorsque vous sélectionnez la valeur Lecture/Écriture, vous pouvez configurer les fonctions réseau sous CCA. Dans le cas contraire, sélectionnez Lecture seule et choisissez un niveau de privilège entre 1 et 15.

Le mode d'accès par défaut est Lecture/Écriture.

Utilisation des assistants de configuration de CCA

Outre l'interface de configuration en mode Expert, CCA dispose également d'assistants qui vous aident dans le paramétrage des solutions Cisco SBCS, des fonctions et des périphériques.

Pour accéder aux assistants de configuration de CCA, sélectionnez l'option **Accueil** dans la barre de fonctions.

Certains assistants sont uniquement accessibles si les périphériques font partie du site client auquel vous êtes connecté. Par exemple, si le site client ne dispose pas d'une fonction sans fil, l'option Assistant de configuration sans fil ne s'affiche pas.

Voir les rubriques suivantes :

- **Quel assistant utiliser et quand ?, page 95**
- **Assistant de configuration de la téléphonie, page 98**

Quel assistant utiliser et quand ?

Chaque assistant de configuration de CCA est conçu pour automatiser la configuration et la maintenance de périphériques, fonctions et types de déploiement spécifiques. Les assistants de configuration personnels sont rassemblés dans le tableau suivant.

Assistant	Fonction de l'assistant	Quand l'utiliser	Pour en savoir plus...
Assistant de configuration de la téléphonie	Pour un système Cisco SBCS/UC500, l'Assistant de configuration de la téléphonie configure les paramètres WAN et LAN de base, les paramètres régionaux, les paramètres système de la téléphonie, les trunks vocaux (sauf les trunks SIP), les ports vocaux, le Standard automatique, les plannings, les utilisateurs et les numéros de poste, le routage des appels entrants et les groupements de poste. L'assistant prend en charge toutes les plateformes UC500. Si l'UC500 se trouve derrière un routeur sécurisé SR500 ou un périphérique de sécurité SA500, l'assistant ajuste automatiquement les routages statiques et les ACL. Il annule ensuite le pare-feu de l'UC500.	Utilisez cet assistant pour la première configuration uniquement. L'assistant nécessite un UC500 présentant une configuration d'usine. Lancez l'Assistant de configuration de la téléphonie *avant* d'exécuter d'autres assistants de configuration de CCA. Si le routeur sécurisé SR520-T1 assure la connexion au WAN, vous devrez aussi exécuter l'Utilitaire de configuration du SR520-T1. Lancez l'Utilitaire de configuration du SR520-T1 *avant* d'exécuter l'Assistant de configuration de la téléphonie. Voir la rubrique **Utilitaire de configuration SR520-T1, page 108**. Pour les routeurs sécurisés ADSL/ Ethernet SR520 et les routeurs sécurisés SA 500, configurez la connexion WAN avant d'exécuter l'Assistant de configuration de la téléphonie.	**Assistant de configuration de la téléphonie, page 98**

Assistant	Fonction de l'assistant	Quand l'utiliser	Pour en savoir plus...
Assistant de configuration de la sécurité	L'Assistant de configuration de la sécurité est utilisé pour la configuration des déploiements de petite envergure exploitant des données uniquement en présence d'un dispositif de sécurité SA500 installé comme appareil périphérique, de commutateurs Cisco Small Business Pro et de points d'accès sans fil. Cet assistant permet de définir les paramètres de base pour le WAN, le LAN et le réseau sans fil sur les périphériques de sécurité SA 500. Il permet également d'automatiser la configuration des trunks pour les commutateurs Cisco Small Business Pro ESW 500 ou CE 520. Il synchronise les profils sans fil sur les points d'accès SA500 intégrés et les points d'accès externes AP541N qui font partie du même site client.	Utilisez cet assistant pour la première configuration d'un déploiement de données SA500. Vous pouvez également relancer l'assistant pour mettre à jour ces paramètres dans le cas d'un déploiement existant. L'assistant prend également en charge le *mode de transfert* qui vous permet d'effectuer une configuration préalable des paramètres sans le SA 500 et les autres périphériques reliés physiquement au réseau. Le mode de transfert vous permet d'exporter et d'importer la configuration vers et à partir d'un fichier local avant d'appliquer la configuration finale. Lancez cet assistant *avant* de configurer les fonctions de sécurité à l'aide de l'Utilitaire de configuration du SA 500.	**Assistant de configuration de la sécurité, page 101**
Assistant de configuration de périphérique	L'Assistant de configuration de périphérique fournit les instructions nécessaires à la connexion et la configuration des paramètres de base du périphérique tels que le nom d'hôte et l'adresse IP afin que la gestion puisse être assurée par CCA. Les périphériques suivants sont pris en charge : Commutateurs Cisco Catalyst Express CE520 Points d'accès autonomes Cisco AP521 Contrôleurs WLAN Cisco WLC526 Routeurs sécurisés ADSL/Ethernet Cisco SR520	Utilisez cet assistant pour la première configuration de ces périphériques.	**Assistant de configuration de périphérique, page 107**

Assistant	Fonction de l'assistant	Quand l'utiliser	Pour en savoir plus...
Assistant de configuration sans fil	L'Assistant de configuration sans fil configure et synchronise le réseau sans fil et les paramètres de profil pour les déploiement voix/sans fil ou les déploiements de réseaux de données uniquement en présence de plusieurs points d'accès. L'assistant prend en charge les points d'accès intégrés UC500, les points d'accès autonomes AP521, les téléphones IP SPA525G opérant en mode sans fil G et les points d'accès AP541N.	Utilisez cet assistant pour la première configuration et la synchronisation des profils sans fil pour les déploiements de réseaux vocaux ou de données sans fil pour les téléphones IP SPA525G et les PA pris en charge. Vous pouvez relancer l'assistant pour mettre à jour le réseau sans fil et les paramètres de profil.	**Assistant de configuration sans fil, page 104**
Assistant de configuration du téléphone VPN	L'Assistant de configuration du téléphone VPN permet de configurer les paramètres du client VPN sur les téléphones IP Cisco SPA525G ou SPA525G2 qui seront déployés en vue d'une utilisation sur un site distant. L'Assistant de configuration du téléphone VPN ne peut pas être utilisé pour les déploiements où l'UC500 se trouve derrière un périphérique de sécurité SA500.	Exécutez cet assistant sur le site principal afin d'automatiser la configuration du client VPN pour les téléphones IP SPA525G qui seront déployés sur les sites distants. Vous pouvez relancer l'assistant afin de mettre à jour ou de supprimer la configuration VPN existante sur les téléphones. Il est conseillé de lancer l'Assistant de configuration de la téléphonie *avant* d'exécuter l'Assistant VPN.	**Assistant de configuration du téléphone VPN, page 108**
Assistant de configuration de la surveillance vidéo	L'Assistant de configuration de la surveillance vidéo permet de configurer les paramètres des caméras et d'associer les caméras Cisco PVC2300/WVC2300 Business Internet aux téléphones IP SPA525G et SPA525G2. Cela permet aux utilisateurs d'afficher la vidéo obtenue de ces caméras grâce à l'écran intégré des téléphones IP SPA525G et SPA525G2.	L'assistant peut être utilisé pour la première configuration de la fonction de surveillance vidéo sur les téléphones SPA525G et les caméras IP PVC2300/WVC2300. Vous pouvez relancer l'assistant pour mettre à jour ces paramètres dans le cas d'une installation existante. Lancez l'Assistant de configuration de la téléphonie *avant* d'exécuter l'Assistant de configuration de la surveillance vidéo.	**Assistant de configuration de la surveillance vidéo, page 111**

Assistant	Fonction de l'assistant	Quand l'utiliser	Pour en savoir plus...
Gestionnaire multi-sites	Utilisez le Gestionnaire multi-sites pour configurer et gérer les déploiements des réseaux de données ou vocaux multi-sites Cisco SBCS.	Utilisez le Gestionnaire multi-sites pour la première configuration d'un déploiement multi-sites Cisco SBCS. Les configurations multi-sites hors bande existantes ne sont pas prises en charge par CCA. Vous pourrez également utiliser le Gestionnaire multi-sites pour ajouter, supprimer ou modifier les sites ou pour actualiser les paramètres dans le cadre d'un déploiement existant. Il est conseillé de lancer l'Assistant de configuration de la téléphonie *avant* d'exécuter le Gestionnaire multi-sites.	**Gestionnaire multi-sites, page 485**

Assistant de configuration de la téléphonie

Pour accéder à l'Assistant de configuration de la téléphonie, sélectionnez **Accueil** > **Assistant de configuration de la téléphonie** dans la barre de fonctions. Si l'UC500 se trouvant sur le site client présente la configuration par défaut, l'assistant s'exécute automatiquement.

L'Assistant de configuration de la téléphonie vous guide pas à pas lors de la configuration d'un système téléphonique de base.

L'assistant est prévu pour les installations initiales, lorsque vous rétablissez les paramètres d'usine pour les périphériques Cisco UC500 et lorsque vous remplacez complètement la configuration active.

Les paramètres suivants sont définis par le biais de l'assistant :

- Paramètres réseau de base, dont le type de connexion WAN
- Téléphones, utilisateurs et numéros de poste primaires
- Groupements de postes et groupes d'appel
- Paramètres de trunk (ISDN BRI, ISDN PRI et trunks analogiques) et numéros de téléphone
- Plan de numérotation local
- Routage des appels entrants
- Horaires d'ouverture

- Actions et invites du Standard automatique

Lorsque vous démarrez l'Assistant de configuration de la téléphonie, CCA détecte le nombre de licences logicielles, le paquet logiciel de l'UC500 et/ou la version de Cisco IOS.

L'Assistant de configuration de la téléphonie prend aussi en charge l'importation des données des utilisateurs et des téléphones. Pour plus d'informations sur la préparation des données pour l'importation, consultez la rubrique **Importation des données du téléphone pour plusieurs utilisateurs (Importation massive), page 334**.

Les boutons permettant d'accéder au mode Expert et aux fenêtres Mise à jour du logiciel et Gestion des licences sont prévus afin que vous puissiez effectuer les mises à jour du logiciel et/ou des licences avant de continuer. Cliquez sur ces boutons pour quitter l'assistant.

Avant de commencer

Avant de lancer l'Assistant de configuration de la téléphonie

- Si le PC sur lequel CCA est actif présente plusieurs cartes réseau (par exemple, une double carte réseau pour les connexions câblées et sans fil), veillez à n'en activer qu'une seule.
- Désactivez les pare-feu tiers et les services TFTP sur le PC exécutant CCA.
- Vérifiez le pare-feu et les paramètres de sécurité du réseau sur votre PC afin de vérifier si le trafic TFTP est autorisé entre le PC et l'UC500.
- Vérifiez si le PC exécutant Configuration Assistant est directement connecté au port LAN de l'UC500 et a obtenu l'adresse IP de l'UC500 par le protocole DHCP.
- Assurez-vous que les paramètres par défaut sont actifs sur l'UC500.
- Pour les paramètres régionaux autres que les États-Unis, téléchargez et installez les fichiers de localisation à l'emplacement adéquat.
- Veillez à rassembler toutes les données figurant à la page d'accueil de l'Assistant.
- Si l'UC500 se trouve derrière un dispositif de sécurité SA500 ou un routeur sécurisé SR500, reliez le WAN de l'UC500 au LAN du SA500 ou du SR500 avant d'exécuter l'Assistant de configuration de la téléphonie.

Utilisation de l'Assistant de configuration de la téléphonie

Pour accéder à l'assistant à partir de la barre de fonctions, utilisez l'option **Accueil** > **Assistant de configuration de la téléphonie**.

Les données configurées ne sont pas appliquées avant la dernière page de l'Assistant. Procédez comme suit pour revenir aux écrans précédents :

- Utilisez le bouton **Précédent**.
- Utilisez le volet de navigation sur la gauche pour accéder à la page souhaitée.
- Utilisez les liens de la page Récapitulatif. Puis, cliquez sur **Reprendre** pour revenir au récapitulatif.

Si les modifications apportées affectent d'autres paramètres configurés à l'aide de l'Assistant, les éléments de navigation signalés en rouge indiquent des erreurs qui doivent être corrigées avant de continuer.

Si vous cliquez sur **Appliquer la configuration**, les paramètres sélectionnés dans l'Assistant entrent en vigueur. Si vous quittez l'Assistant avant d'appliquer la configuration, les modifications ne seront pas effectives.

Une fois la configuration initiale établie à l'aide de l'Assistant et que vous avez vérifié si les principales fonctions réseau et voix sont opérationnelles, continuez à paramétrer les autres fonctions réseau, de sécurité et vocales à l'aide de l'interface de Cisco Configuration Assistant

Étapes suivantes

Les fonctions de téléphonie suivantes ne sont pas configurées à l'aide de l'Assistant de configuration de la téléphonie :

- Autorisations d'appel pour chaque téléphone (les autorisations d'appel sont illimitées pour les téléphones ajoutés à l'aide de l'Assistant)
- Blocage d'appel pour chaque téléphone (le blocage d'appel est désactivé pour les téléphones ajoutés à l'aide de l'Assistant)
- Interphones, lignes partagées, chevauchements et lignes octales.
- Lignes en mode Supervision et Surveillance
- Interface de trunk SIP
- Basic ACD (répartition automatique des appels)
- Conférence à plusieurs (ad hoc/Meet-Me)

- Service de nuit
- Numéros personnalisés pour le plan de numérotation sortant
- Groupes de trunks et priorités
- Numérotation abrégée système
- Groupes de radiomessagerie
- Groupes d'interception
- Numéros de poste pour le parc d'appels
- Conférence
- Mobilité de poste

Consultez l'aide en ligne de CCA et les autres rubriques de ce guide pour obtenir des informations sur la configuration de ces fonctions en mode Expert sous CCA.

Assistant de configuration de la sécurité

Pour accéder à l'Assistant de configuration de la sécurité, sélectionnez **Accueil** > **Assistant de configuration de la sécurité** dans la barre de fonctions.

REMARQUE L'Assistant de configuration de la sécurité est conçu pour les déploiements de réseaux de données uniquement en présence de dispositifs de sécurité SA500, de commutateurs ESW 500 et de points d'accès AP541. Si vous déployez une solution de téléphonie UC500, lancez l'Assistant de configuration de la téléphonie pour configurer le réseau.

L'Assistant de configuration de la sécurité peut être utilisé pour la configuration initiale ou pour modifier la configuration existante conformément aux rubriques suivantes.

- **Vue d'ensemble**
- **Transfert de la configuration**
- **Téléchargement et installation du dernier microprogramme pour les périphériques SA500, ESW500 et AP541N**
- **Utilisation de l'Assistant de configuration de la sécurité**
- **Étapes suivantes**

Vue d'ensemble

Les dispositifs de sécurité Cisco SA500 assurent la connectivité WAN, le routage, le pare-feu, l'accès à distance et l'accès sans fil pour les réseaux des petites entreprises.

L'Assistant de configuration de la sécurité vous guide au fil des étapes nécessaires à la configuration des paramètres du réseau sans fil pour les dispositifs de sécurité Cisco SA500 dans un réseau professionnel exploitant des données uniquement. L'assistant assure également la synchronisation des données de profil pour les points d'accès sans fil SA500 et AP541N membres du site client de CCA.

Lorsque vous appliquez la configuration à l'aide de l'assistant, CCA définit automatiquement les trunks 802.1q et synchronise les données du réseau LAN sans fil (WLAN) et les paramètres de profil invité pour les périphériques Cisco Small Business Pro tels que les commutateurs ESW 500 et les points d'accès AP541N.

Transfert de la configuration

Si CCA détecte que le site client auquel vous êtes connecté ne contient pas de SA500, l'assistant passe automatiquement en mode Transfert.

Dans ce mode, vous pouvez prédéfinir les paramètres et enregistrer votre progression à tout moment en sélectionnant l'option **Exporter la configuration vers un fichier**. Pour reprendre la configuration, relancez l'assistant et sélectionnez l'option **Importer la configuration à partir d'un fichier**.

Une fois le matériel disponible et que vous êtes connecté au site client, relancez l'assistant, importez la configuration préalablement enregistrée, apportez les modifications nécessaires et appliquez la configuration.

Téléchargement et installation du dernier microprogramme pour les périphériques SA500, ESW500 et AP541N

Si vous êtes relié à un site client CCA présentant un SA500, la version actuelle du périphérique s'affiche. La version 1.1.21 ou une version supérieure du microprogramme du SA500 est nécessaire.

Pour obtenir le dernier microprogramme de Cisco.com, suivez les liens suivants. Un identifiant est nécessaire pour accéder à cette rubrique du site.

- Les téléchargements disponibles pour les périphériques de sécurité SA500 sont disponibles sur www.cisco.com/go/sa500software.

- Pour les commutateurs ESW500, les liens pour le téléchargement sont disponibles sur www.cisco.com/go/esw500help. Cliquez sur l'onglet **Resources** et sélectionnez le lien Firmware sous **Firmware and Release Notes**.
- Pour les points d'accès AP541N, les téléchargements sont disponibles sur www.cisco.com/go/ap500software.

Lorsque vous avez terminé le téléchargement du logiciel, cliquez sur le bouton **Mise à jour du logiciel** dans l'assistant ou sélectionnez l'option **Maintenance** > **Mise à jour du logiciel** dans la barre de fonctions de CCA pour afficher la fenêtre Mise à jour du logiciel de CCA.

Suivez les consignes figurant dans l'aide en ligne de CCA pour mettre à niveau le microprogramme de ces périphériques. Voir la rubrique **Mises à jour des logiciels, page 548**.

Utilisation de l'Assistant de configuration de la sécurité

Pour lancer l'Assistant, sélectionnez **Accueil** > **Assistant de configuration de la sécurité** dans la barre de fonctions.

Suivez les consignes à l'écran pour configurer les paramètres suivants :

- Mot de passe de l'administrateur (pour des raisons de sécurité, le mot de passe par défaut "cisco" doit être modifié)
- Fuseau horaire, options de passage à l'heure d'été/hiver et serveurs NTP

  Vous ne pouvez pas définir directement l'heure système sur le SA500. Un serveur NTP est donc nécessaire. Les serveurs par défaut (0.us.pool.ntp.org et 1.us.pool.ntp.org) concernent les États-Unis.
- Connexion WAN (DHCP, IP statique ou PPPoE)
- VLAN de données
- Routages statiques
- Réseau sans fil invité
- SSID sans fil, Identifiant de VLAN et données de profil pour les réseaux de données et invités

  Lorsque vous appliquez la configuration, l'assistant synchronise les paramètres de profil sans fil en fonction du point d'accès intégré SA 520W et de tous les points d'accès AP541N présents sur le réseau. Pour être synchronisés, ces points d'accès doivent être membres du site client de CCA auquel vous êtes connecté.

La configuration existante est remplacée par la nouvelle.

La protection WPA2 avec chiffrement TKIP + CCMP est automatiquement définie pour le type de sécurité sans fil.

Vous pouvez relancer l'assistant à tout moment pour modifier ces paramètres.

Étapes suivantes

Lorsque vous en avez terminé avec l'Assistant de configuration de la sécurité, cliquez avec le bouton droit de la souris sur l'icône du SA500 dans la fenêtre Topologie et sélectionnez **Utilitaire de configuration** pour lancer le logiciel de gestion Web du SA 500.

L'Utilitaire de configuration du SA 500 vous permet de définir les fonctions de sécurité pour le site client, dont le pare-feu et la DMZ, le filtrage d'adresses, le système de prévention des intrusions (IPS), le transfert de port et la fonction SSL VPN. Ces fonctions ne sont pas configurées à l'aide de CCA.

Cisco ProtectLink Gateway est un service de sécurité hébergé permettant de bloquer le pourriel et de filtrer les URL afin d'éviter au contenu non désiré d'accéder à votre réseau d'entreprise. Suivez les consignes figurant dans le *Guide d'administration des dispositifs de sécurité Cisco SA500* pour obtenir un code d'activation et activer les services ProtectLink sur le SA 500. Pour en savoir plus, consultez www.cisco.com/go/protectlink.

Pour plus d'informations, consultez le *guide Cisco SA500 Series Security Appliances Administration Guide* disponible sur le site Cisco.com à l'adresse :

www.cisco.com/go/sa500

Cliquez sur l'onglet **Resources** et parcourez la rubrique **Technical Documentation** pour accéder au guide d'administration et aux autres liens utiles.

Assistant de configuration sans fil

Pour accéder à l'Assistant de configuration sans fil, sélectionnez **Accueil** > **Assistant de configuration sans fil** dans la barre de fonctions. L'option de menu Assistant de configuration sans fil est disponible uniquement si le site client auquel vous êtes connecté dispose d'une fonction sans fil.

- **Vue d'ensemble**
- **Avant de commencer**
- **Utilisation de l'Assistant de configuration sans fil**

Vue d'ensemble

Utilisez l'Assistant de configuration sans fil pour automatiser la configuration des paramètres sans fil pour plusieurs points d'accès ou pour configurer les solutions voix/sans fil Cisco SBCS en présence de téléphones Cisco SPA525G ou SPA525G2 fonctionnant en mode wireless-G. Les paramètres du réseau sans fil et de profil sont synchronisés sur tous les points d'accès et les téléphones SAP525G et SPA525G2 membres du site client. Tous les modèles UC500 sont pris en charge.

Les périphériques suivants sont pris en charge :

- Points d'accès UC500 intégrés
- Points d'accès Cisco Small Business Pro AP541N
- Points d'accès autonomes Cisco AP521

IMPORTANT Si la mise en cluster est activée pour les points d'accès AP541N faisant partie du site client CCA, ne lancez pas l'Assistant de configuration sans fil pour les configurer.

Si vous utilisez des points d'accès AP541N avec des téléphones SPA525G/SPA525G2, suivez les consignes de déploiement pour SBCS figurant dans le *Guide de déploiement voix/sans fil Cisco SBCS 2.0*. Le guide est disponible sur Cisco.com à l'adresse suivante :

www.cisco.com/en/US/docs/voice_ip_comm/sbcs/deployment_guides/voice_over_wireless/sbcs_20_vowifi_deployment_guide.pdf

Les téléphones Cisco 7921 et 7925 peuvent être utilisés avec les solutions sans fil SBCS 2.0 utilisant les points d'accès AP541N. Toutefois, l'Assistant de configuration sans fil ne synchronise pas automatiquement les paramètres de profil sans fil pour ces téléphones.

Si vous utilisez d'anciens points d'accès autonomes Cisco AP 521 avec des téléphones IP SPA525G/SPA525G2, suivez les modèles de référence et les lignes de conduite définies dans le *Guide de déploiement sans fil de Cisco SPA525G pour Cisco SBCS*. Le guide est disponible sur Cisco.com à l'adresse suivante :

www.cisco.com/en/US/docs/voice_ip_comm/sbcs/deployment_guides/spa525g_phone/sbcs_spa525g_wireless_deployment_guide.pdf

Avant de commencer

Votre système doit répondre aux critères suivants :

- CCA version 2.2(2) ou supérieure est nécessaire pour la prise en charge des points d'accès AP541N par l'Assistant de configuration sans fil.
- Les téléphones IP SPA525G doivent exécuter la version 7.1.3 du microprogramme ou une version supérieure
- Paquet logiciel UC500 7.0 ou supérieur
- Les points d'accès AP541N doivent exécuter la version 1.8.0 du microprogramme ou une version supérieure.
- Les téléphones SPA 525G/SPA525G2 qui seront connectés sans fil doivent être dotés d'une alimentation externe PA100.

Avant de lancer l'Assistant de configuration sans fil, vous devrez effectuer les opérations suivantes :

- Rassemblez les informations suivantes : Les SSID et les mots de passe (clés partagées) que vous souhaitez utiliser pour les données sans fil, la voix et les réseaux invités.
- Connectez les points d'accès externes (AP541N ou AP521s) à l'UC 500.
- Connectez les téléphones SPA525G/SPA525G2 directement côté LAN de l'UC500 pour la synchronisation du profil sans fil.
- Créez un site client CCA pour l'UC500, les téléphones et les points d'accès.
- Connectez-vous au site client et vérifiez si les points d'accès externes sont membres du site client.

Utilisation de l'Assistant de configuration sans fil

Pour lancer l'Assistant de configuration sans fil, connectez-vous au site client que vous avez créé et sélectionnez **Accueil** > **Assistant de configuration sans fil** dans la barre de fonctions.

Suivez les consignes à l'écran pour configurer les paramètres suivants :

- Activez le mode sans fil sur les téléphones SPA525G/SPA525G2.
- Configurez les SSID, les mots de passe (clés partagées) pour les données sans fil et les réseaux vocaux.
- Choisissez si vous souhaitez ou non diffuser le SSID.
- Activez le réseau invité (le cas échéant) et configurez le SSID ainsi que le mot de passe (clé partagée). Choisissez si vous souhaitez ou non activer la diffusion du SSID.

Les notes suivantes s'appliquent aux identifiants de VLAN configurés à l'aide de l'Assistant de configuration sans fil :

- L'identifiant de VLAN pour le réseau vocal est 1 (valeur réservée par CCA).
- L'identifiant de VLAN pour le réseau de données est 100 (valeur réservée par CCA).
- L'identifiant de VLAN pour le réseau invité est 25 (valeur réservée par CCA).
  - Si le SSID cisco-guest existe déjà sur un périphérique du site client et si l'identifiant de VLAN n'est pas 25, le SSID cisco-guest existant est supprimé et recréé, puis, la valeur de l'identifiant de VLAN est définie sur 25.
  - Si le SSID cisco-guest existe déjà sur un périphérique du site client et si l'identifiant de VLAN est 25, la configuration reste intacte.

L'assistant configure automatiquement les paramètres QoS des points d'accès AP541N et le chiffrement WPA2-PSK pour la sécurité sans fil. Vous ne devez pas définir ces options.

Vous pouvez relancer l'assistant à tout moment pour modifier ces paramètres. Chaque fois que vous lancez l'assistant, les valeurs existantes sont écrasées par les nouveaux paramètres.

Assistant de configuration de périphérique

Les nouveaux périphériques et ceux qui ont été réinitialisés doivent être configurés. Utilisez l'Assistant de configuration de périphérique pour faire en sorte que les périphériques puissent être pris en charge par CCA. Pour lancer l'Assistant, sélectionnez **Accueil** > **Assistant de configuration de périphérique** dans la barre de fonctions. Suivez les consignes à l'écran pour paramétrer le périphérique.

REMARQUE le routeur sécurisé Cisco SR520-T1 dispose de son propre utilitaire de configuration. L'utilitaire de configuration démarre automatiquement si le périphérique SR520-T1 est relié à un UC500 et s'il présente la configuration par défaut. Voir la rubrique **Utilitaire de configuration SR520-T1, page 108**.

Vous pouvez configurer ces périphériques à l'aide de l'Assistant de configuration de périphérique :

- Routeurs sécurisés ADSL/Ethernet Cisco SR520
- commutateurs CE520

- Points d'accès autonomes Cisco AP521
- Contrôleur LAN sans fil Cisco WLC526

Le point d'accès sans fil Cisco AP541N Dual-band Single-radio ne peut pas être configuré à l'aide de l'Assistant de configuration de périphérique.

Utilitaire de configuration SR520-T1

Si votre site comprend un routeur sécurisé SR520-T1 et s'il est réglé sur les paramètres par défaut, sélectionnez l'option **Accueil** > **Utilitaire de configuration SR520-T1** pour effectuer les opérations suivantes :

- Définir la connexion T1 WAN
- Modifier l'adresse IP par défaut du LAN0 au cours de la configuration initiale (*facultatif*)
- Afficher les données de diagnostic et exécuter les tests de ping pour vérifier la connectivité
- Mettre à niveau le logiciel du SR520-T1

Pour plus d'informations sur les prérequis et les procédures, consultez le guide *Cisco Small Business Pro SR520-T1 Secure Router Quick Start Guide* et le document *UC500 and SR520-T1 Secure Router Setup* disponibles sur Cisco.com.

Une fois la connexion T1 configurée, utilisez Configurer en mode Expert pour configurer les autres paramètres et fonctions tels que le NAT, le pare-feu et la DMZ, les comptes d'administration, le DNS, le nom d'hôte, le NTP, le SNMP, les routages statiques et les fonctions de sécurité sous licence (IPS, SSL VPN et filtrage d'URL).

Assistant de configuration du téléphone VPN

REMARQUE : L'Assistant de configuration du téléphone VPN ne peut pas être utilisé pour les déploiements où l'UC500 se trouve derrière un périphérique de sécurité SA500.

Pour accéder à l'Assistant de configuration du téléphone VPN, sélectionnez **Accueil** > **Assistant de configuration du téléphone VPN** dans la barre de fonctions. L'élément de menu Assistant de configuration du téléphone VPN est uniquement disponible si le site client auquel vous êtes connecté contient au moins un téléphone IP SPA525G ou SPA525G2.

Vue d'ensemble

L'Assistant de configuration du téléphone VPN permet de configurer les paramètres du client VPN sur les téléphones IP Cisco SPA525G ou SPA525G2 qui seront déployés en vue d'une utilisation sur un site distant.

- **Au bureau** : connectez les téléphones IP à l'UC500, configurez les postes d'utilisateur à l'aide de CCA et lancez l'assistant afin de configurer les paramètres VPN du client sur le téléphone et définir les comptes d'utilisateur VPN sur le serveur. Une fois configuré, le téléphone peut être débranché et envoyé vers un site distant.
- **Sur le site distant** : l'utilisateur distant connecte le téléphone au réseau du site distant et active le client VPN sur le téléphone. Le téléphone établit une connexion avec l'UC500 par un tunnel VPN sécurisé à l'aide des paramètres prédéfinis. Une fois connecté au VPN, le téléphone s'affiche comme n'importe quel autre téléphone du site principal et les appels entre le site principal et le site distant passent par le VPN.

Vous pouvez relancer l'Assistant de configuration du téléphone VPN si nécessaire afin d'ajouter, modifier ou supprimer les paramètres du client VPN sur les téléphones. Par exemple, pour redéployer un téléphone sur le site principal, configurer des téléphones VPN ou modifier l'utilisateur associé au téléphone.

Avant de commencer

Avant de lancer l'Assistant de configuration du téléphone VPN, votre système doit répondre aux critères suivants :

- Le serveur VPN SSL et les paramètres du client Anyconnect doivent être configurés pour le site. Si SSL VPN n'est pas configuré, vous devrez le faire pour continuer.

L'adresse IP statique de la connexion WAN est nécessaire pour la configuration du serveur SSL VPN. Vous devez aussi activer le mode Full Tunnel et installer le client SSL VPN Anyconnect pour Microsoft Windows. Le mode Split Tunnel n'est pas pris en charge pour le VPN téléphonique.

- Tous les téléphones IP à configurer pour le VPN doivent être dotés du dernier microprogramme. La version 7.4.2 ou une version supérieure est nécessaire.
- Les téléphones IP doivent être alimentés et connectés à l'UC500 par le port LAN de l'UC500 ou par un commutateur ou un point d'accès sans fil relié à l'UC500.
- Lors du calcul du total des connexions VPN simultanées requises pour un site client, veillez à inclure toutes les connexions VPN utilisées pour les VPN des téléphones IP.

  Les plateformes UC520 et UC540 prennent en charge 10 connexions VPN simultanées au maximum. Les plateformes UC560 prennent en charge 20 connexions VPN simultanées au maximum.
- Les téléphones IP doivent être inscrits sur l'UC500 et afficher un numéro de poste.
- Les paramètres de base pour le réseau et la téléphonie doivent être configurés pour le site client à l'aide de l'Assistant de configuration de la téléphonie ou du mode Expert de CCA.
- Par souci de simplicité, les paramètres relatifs aux postes utilisateurs tels que l'identifiant utilisateur du téléphone et les boutons doivent être configurés avant de lancer l'Assistant de configuration du téléphone VPN. Il s'agit d'une recommandation et non d'une obligation. Les paramètres des postes utilisateurs pourront être modifiés après que vous avez lancé l'Assistant de configuration du téléphone VPN.

Lancement et utilisation de l'Assistant de configuration du téléphone VPN

Pour lancer l'Assistant de configuration du téléphone VPN, sélectionnez **Accueil** > **Assistant de configuration du téléphone VPN**.

L'Assistant détecte les téléphones SPA525G et SPA525G2 reliés à l'UC500 et affiche l'adresse MAC, le numéro de poste et l'identifiant utilisateur du téléphone afin que vous puissiez facilement identifier les téléphones.

Suivez les instructions de l'Assistant pour sélectionner les téléphones. Entrez un nom d'utilisateur et un mot de passe pour le compte VPN à associer à ce téléphone.

Au fur et à mesure de la configuration de chaque téléphone, la colonne État est mise à jour et indique la réussite ou l'échec. Si la configuration échoue pour un téléphone, l'Assistant passe au téléphone suivant dans la liste.

Activation du VPN de téléphone sur le site distant

Sur le site distant, l'utilisateur du téléphone doit suivre les étapes suivantes afin de configurer son téléphone IP et le connecter au VPN.

ETAPE 1 Branchez le téléphone IP.

ETAPE 2 Reliez le téléphone au réseau du site distant (domicile ou bureau distant).

ETAPE 3 Attendez que le téléphone soit initialisé et obtienne l'adresse IP du réseau sur le site distant.

Le téléphone se connecte automatiquement au serveur VPN.

Si vous ne voulez pas que le serveur se connecte automatiquement au serveur VPN, paramétrez l'option **Connecter au démarrage** du téléphone IP SPA525G/SPA 525G2 sur **OFF**. Pour accéder à ce paramètre, appuyez sur le bouton **paramètres** du téléphone et accédez à l'option **Informations et paramètres**> **Configuration réseau** > **VPN**.

Pour plus d'informations sur les téléphones IP Cisco SPA525G/SPA525G2, rendez-vous à l'adresse suivante :

www.cisco.com/go/500phones

Modification des paramètres VPN du téléphone après l'installation initiale

Vous pouvez relancer l'Assistant de configuration du téléphone VPN pour configurer les paramètres VPN pour de nouveaux téléphones, modifier les paramètres VPN existants ou supprimer les paramètres VPN du téléphone.

Pour supprimer la configuration VPN des téléphones, relancez l'Assistant de configuration du téléphone VPN et annulez la sélection des téléphones dans la liste des téléphones disponibles avant d'appliquer la configuration.

Assistant de configuration de la surveillance vidéo

Pour accéder à l'Assistant de configuration de la surveillance vidéo, sélectionnez **Accueil** > **Assistant de configuration de la surveillance vidéo** dans la barre de fonctions.

L'option Assistant de configuration de la surveillance vidéo n'est disponible que si le site client auquel vous êtes connecté contient au moins un téléphone IP SPA525G ou SPA525G2 et une caméra Cisco PVC2300 ou WVC2300 Business Internet.

Vue d'ensemble

L'Assistant de configuration de la surveillance vidéo vous guide au fil des étapes permettant de configurer les paramètres des caméras et d'associer les caméras Cisco 2300 Business aux téléphones IP SAP 525G/SPA525G2. Cela permet aux utilisateurs d'afficher la vidéo obtenue de ces caméras grâce à l'écran intégré des téléphones IP SPA 525G/SPA525G2.

Chaque téléphone IP SPA 525G/SPA525G2 peut recevoir la vidéo d'un maximum de quatre (4) caméras Cisco 2300 Series Business Internet. Les modèles de caméra PVC2300 (câblée, PoE) et WVC2300 (sans fil, non PoE) sont pris en charge.

Les restrictions suivantes s'appliquent à la surveillance vidéo sur les téléphones SPA 525G/SPA525G2 :

- Lorsque vous regardez la vidéo sur un téléphone SPA 525G/SPA525G2, le téléphone peut toujours effectuer et recevoir des appels. Toutefois, les appels entrants ne modifient pas l'affichage et seul le témoin associé à la ligne appelée clignotera. Pour répondre aux appels entrants, appuyez simplement sur le bouton correspondant à la ligne.
- Si vous visualisez la vidéo sur le téléphone, l'application s'arrête lorsque vous effectuez un appel sortant. Elle ne redémarre pas forcément ensuite.
- Il n'y a pas de prise en charge audio entre le téléphone IP et la caméra.

- Vous ne pouvez pas à la fois activer le client VPN et la surveillance vidéo sur les téléphones SPA525G/SPA525G2.
- Le contrôle d'accès aux portes des téléphones SPA525G/SPA525G2 à l'aide des ports GPIO situés à l'arrière de la caméra n'est pas pris en charge.

Avant de commencer

Avant de lancer l'Assistant de configuration de la surveillance vidéo, veillez à ce que votre système respecte les critères suivants :

- Les paramètres de base pour le réseau et la téléphonie doivent être configurés pour le site client à l'aide de l'Assistant de configuration de la téléphonie ou du mode Expert de CCA.
- Les téléphones IP Cisco SPA525G/SPA525G2 doivent disposer de la version 7.4.3 du microprogramme ou d'une version supérieure. Ils doivent être membres du site client de CCA auquel vous êtes connecté. Voir la rubrique **Préparation des caméras et des téléphones IP pour la surveillance vidéo, page 116**.
- Les caméras Internet Cisco 2300 doivent disposer de la version 1.1.1.4 du microprogramme ou d'une version supérieure. Ils doivent être membres du site client de CCA auquel vous êtes connecté. Les caméras doivent disposer d'une adresse IP statique.

  Si vous utilisez des caméras WVC2300 (sans fil, non POE), le SSID par défaut (ciscosb) et les paramètres de profil sans fil doivent être configurés en fonction des points d'accès et de l'UC500.

  Pour savoir où télécharger le dernier microprogramme pour la caméra et comment mettre à niveau le microprogramme, voir **Préparation des caméras et des téléphones IP pour la surveillance vidéo, page 116**.
- Le PC exécutant CCA doit être relié à un site client CCA contenant l'UC500, les téléphones IP SPA525G/SPA525G2 et les caméras Cisco PVC2300/ WVC2300.

Lancement et utilisation de l'Assistant de configuration de la surveillance vidéo

ETAPE 1 Lorsque toutes les caméras sont intégrées au site client, sélectionnez **Accueil** > **Assistant de configuration de la surveillance vidéo** pour démarrer l'assistant.

ETAPE 2 Suivez les instructions à l'écran pour configurer les paramètres des caméras et associer les téléphones IP aux caméras.

a. Pour chaque caméra de la liste, vous pouvez modifier le nom et la description de l'emplacement, définir un nom d'utilisateur et un mot de passe ainsi qu'un numéro de poste.

   Le nom d'utilisateur et le mot de passe définis à l'aide de l'assistant permettent à CCA d'accéder à la caméra afin de créer des comptes dotés des privilèges de surveillance pour les caméras utilisées par les téléphones IP. Le numéro de téléphone défini dans le champ **Poste à appeler** désigne le numéro de poste ou de téléphone composé lorsque l'utilisateur appuie sur la touche **Appeler** de son téléphone IP alors qu'il visionne la vidéo sur la caméra.

b. Associer les téléphones IP SPA 525G/SPA525G2 aux caméras IP. Chaque téléphone SPA525G/SPA525G2 peut être associé à un maximum de quatre (4) caméras.

ETAPE 3 Passez les paramètres en revue et appliquez la configuration.

Les caméras et les téléphones IP qui y sont associés sont redémarrés au terme de la configuration.

IMPORTANT Suivez les consignes de la rubrique **Configuration des paramètres vidéo PVC2300/WVC2300, page 114** pour configurer les paramètres vidéo pour les caméras qui enverront la vidéo aux téléphones.

Configuration des paramètres vidéo PVC2300/WVC2300

Vous devez modifier les paramètres vidéo MJPEG des caméras WVC2300/PVC2300 au format requis pour l'intégration aux SPA525G.

Pour chaque caméra, effectuez les opérations suivantes pour configurer les paramètres vidéo.

ETAPE 1 Dans la fenêtre Topologie de CCA, cliquez avec le bouton droit de la souris sur l'icône de la caméra et sélectionnez l'Utilitaire de configuration.

ETAPE 2 Dans le menu de navigation gauche de l'utilitaire de configuration de la caméra, sélectionnez **Audio/Vidéo** > **Vidéo**.

ETAPE 3 Dans la rubrique **Paramètres MJPEG**, définissez les paramètres suivants :

Résolution : 320*240
Débit d'images max : 10 i/s
Contrôle de la qualité vidéo : Sélectionnez **Qualité fixe** et **Normal**.

ETAPE 4 Enregistrez la configuration et quittez l'utilitaire de configuration pour PVC2300/WVC2300.

IMPORTANT Les paramètres MJPEG pour la caméra ne peuvent pas être modifiés si la caméra est intégrée au téléphone SPA525G/SPA525G2. Si vous modifiez ces paramètres, le flux vidéo ne pourra pas être affiché sur le téléphone.

Affichage de la vidéo sur les téléphones IP SPA525G/SPA525G2

Une fois que les téléphones et les caméras ont redémarré, suivez les étapes suivantes pour afficher la vidéo sur les téléphones IP SPA525G.

ETAPE 1 Sur le téléphone SPA525G/SPA525G2, appuyez sur le bouton **paramètres**.

ETAPE 2 Utilisez les flèches Haut et Bas du téléphone pour accéder au menu Information et **paramètres** > **Surveillance vidéo** et cliquez sur le bouton de sélection central.

ETAPE 3 Sélectionnez une caméra dans la liste et cliquez sur la touche **Superviser**.

ETAPE 4 Lorsque le téléphone est relié à la caméra et affiche la vidéo, appuyez sur la touche **Appeler** pour appeler le poste défini à l'aide de l'Assistant.

Modification des paramètres de surveillance vidéo après l'installation initiale

Pour ajouter ou supprimer les téléphones et les caméras ou pour modifier les paramètres, vous pouvez relancer l'assistant.

Si vous utilisez des caméras IP sans fil, elles doivent présenter le même SSID que le réseau de données sur l'UC500 et les points d'accès. Les paramètres SSID sans fil peuvent être modifiés à l'aide de l'Utilitaire de configuration pour PVC2300/ WV2300 ou en utilisant CCA en mode Expert. Sélectionnez **Configurer** > **Sans fil** > **WLAN (SSID)** dans la barre de fonctions pour accéder à ces paramètres sous CCA.

Vous pouvez aussi afficher ou modifier les propriétés des caméras, dont les utilisateurs et les mots de passe, à l'aide de CCA.

Préparation des caméras et des téléphones IP pour la surveillance vidéo

Consultez les rubriques suivantes pour plus d'informations sur la mise à jour du microprogramme des caméras et des téléphones IP et préparer les téléphones et les caméras pour la surveillance vidéo :

- **Récupération du dernier microprogramme du téléphone SPA 525G/ SPA525G2**
- **Configuration des caméras Internet Cisco 2300**

Récupération du dernier microprogramme du téléphone SPA 525G/ SPA525G2

La version 7.4.3 ou une version supérieure du microprogramme du téléphone SPA 525G est nécessaire pour activer la vidéo sur les téléphones SPA 525G. La version 7.4.5 ou une version supérieure du microprogramme du téléphone SPA 525G2 est nécessaire pour activer la vidéo sur les téléphones SPA 525G2.

La version 7.4.3 du microprogramme du téléphone SPA 525G2 est incluse dans le paquet logiciel pour l'UC500 - version 8.0.1. Pour récupérer le logiciel, vous pouvez installer le paquet logiciel 8.0.1 sur l'UC500 ou télécharger la version 7.4.3 du SPA 525G ou une version supérieure sur Cisco.com et utiliser le glisser-déposer pour charger le microprogramme sur l'UC500.

Les téléphones SPA 525G2 sont équipés de série de la version 7.4.5 du microprogramme.

Configuration des caméras Internet Cisco 2300

Suivez les étapes suivantes pour configurer et préparer les caméras vidéo Cisco 2300 en vue d'une utilisation avec l'Assistant de configuration de la surveillance vidéo de CCA. Vous devrez effectuer les opérations suivantes

- Décompresser et configurer le matériel.
- Télécharger la dernière version du microprogramme sur Cisco.com.

- Relier votre PC à chaque caméra et lancer le CD d'installation fourni avec la caméra afin de configurer les paramètres de base.
- Affecter une adresse IP et mettre à niveau le microprogramme pour chaque caméra.
- Pour chaque caméra IP sans fil WVC2300, vous devrez configurer le SSID du réseau sans fil en fonction du SSID propre aux points d'accès et à l'UC500.
- Créer un site client sous CCA et ajouter les caméras au site de sorte à pouvoir utiliser CCA pour configurer les fonctions de vidéosurveillance sur les téléphones IP Cisco SPA 525G/SPA525G2.

ETAPE 1 Télécharger la version 1.1.1.4 ou une version supérieure des caméras Cisco 2300 Business Internet sur le PC exécutant CCA.

La version V1.1.1.4 ou une version supérieure du microprogramme de la caméra est nécessaire.

Le logiciel est disponible sur Cisco.com aux emplacements suivants :

- Page produit de Cisco PVC2300 et WVC2300 (version américaine du site Cisco.com uniquement).
  - **PVC2300** : www.cisco.com/go/pvc2300software
  - **WVC2300** : www.cisco.com/go/wvc2300software

  Sous l'onglet Resources (Ressources), accédez à la rubrique Firmware (Microprogramme) et cliquez sur **Download Firmware and Accept License Agreement for Cisco PVC2300 Business Internet Video Camera - Audio/PoE** (Télécharger le microprogramme et accepter le contrat de licence pour les caméras Cisco PVC2300 Business Internet - Audio/PoE) ou
  ou

  Download Firmware and Accept License Agreement for Cisco WVC2300 Wireless-G Business Internet Video Camera - Audio (Télécharger le microprogramme et accepter le contrat de licence pour les caméras Cisco WVC2300 Wireless-G Business Internet - Audio).

  Les fichiers sont intitulés PVC2300_Firmware.zip et WVC2300_Firmware.zip.
- Centre de téléchargement de logiciels Cisco (requiert des codes d'accès Cisco.com) à l'adresse

http://www.cisco.com/public/sw-center/index.shtml

Dans la liste Select a Product Category (Sélectionnez une catégorie de produit), choisissez **Security(Sécurité)** > **Cisco Physical Security (Sécurité physique Cisco)** > **Cisco Small Business Video Surveillance Cameras (Linksys Business Series) (Caméras de surveillance Cisco Small Business (série Lynksis Business)** et sélectionnez le modèle de caméra.

ETAPE 2 Décompressez les fichiers que vous avez téléchargés. **PVC2300_Firmware.zip**, **WVC2300_Firmware.zip**.

Lorsque vous mettez à niveau le microprogramme de la caméra à l'aide de CCA, vous devrez utiliser le fichier **WVC2300 FW_V111R04.bin** ou le fichier **PVC2300 FW_V111R04.bin** selon le modèle de caméra utilisé.

ETAPE 3 Décompressez et configurez le matériel décrit dans le *Guide de démarrage rapide pour les caméras Cisco PVC2300 et WVC2300 avec son*. Le guide est disponible sur Cisco.com à l'adresse suivante :

http://www.cisco.com/en/US/products/ps9944/prod_installation_guides_list.html

ETAPE 4 Connectez les caméras à l'UC500 conformément aux consignes figurant dans le *Guide de démarrage rapide* et raccordez-les à une source d'alimentation.

La caméra Cisco PVC2300 peut être reliée à un port PoE sur le commutateur UC500 ou ESW500. La caméra Cisco WVC2300 utilise un adaptateur secteur fourni avec la caméra.

ETAPE 5 Suivez les consignes figurant dans le *Guide d'administration pour les caméras Cisco PVC2300 et WVC2300 Business Internet avec son* si vous utilisez le CD d'installation pour installer le logiciel et configurer les paramètres de base.

- Acceptez le contrat de licence.
- Connectez-vous en tant qu'administrateur (les paramètres de connexion par défaut sont admin/admin).
- Configurez les paramètres de base de la caméra (nom, description, fuseau horaire, date et heure).
- A la page Paramètres réseau du programme d'installation, sélectionnez **Adresse IP fixe** pour le type de configuration et entrez une adresse IP statique à utiliser pour la caméra (192.168.10.x).

  Par défaut, les caméras PVC2300 et WVC2300 utilisent le protocole DHCP pour obtenir une adresse IP. Toutefois, une adresse IP statique doit être définie sur les caméras afin que l'adresse IP de la caméra corresponde

toujours à l'adresse IP de la caméra configurée sur les téléphones. L'Assistant de configuration de la surveillance vidéo récupère l'adresse IP configurée sur les caméras.

- Confirmez les paramètres et quittez l'assistant de configuration.
- Si vous configurez des caméras WVC2300 (sans fil, non PoE), suivez les instructions figurant dans le guide d'administration de la caméra pour configurer les paramètres sans fil. Le nom de réseau sans fil (SSID) et les paramètres de sécurité configurés sur les caméras doivent correspondre aux paramètres SSID du réseau de données définis sur les points d'accès et l'UC500.

ETAPE 6 Mettez à niveau le microprogramme de chaque caméra. La version 1.1.1 du microprogramme ou une version supérieure est nécessaire.

a. A partir du PC relié au réseau local (LAN), lancez le navigateur Web et connectez-vous aux caméras à l'aide de l'adresse IP statique affectée à la caméra (par exemple, 192.168.10.21).

b. Connectez-vous en tant qu'administrateur.

c. Cliquez sur **Configuration initiale** dans la barre d'outils.

d. Cliquez sur **Administration** > **Microprogramme**. La version active s'affiche. Si la version est préalable à la version 1.1.1,4, cliquez sur **Mettre à niveau** et suivez les instructions à l'écran.

e. Lorsque vous êtes invité à sélectionner le fichier pour la mise à niveau, accédez au fichier **WVC2300 FW_V111R04.bin** ou **PVC2300 FW_V111R04.bin** selon le modèle de caméra utilisé.

f. Répétez ces étapes pour chaque caméra.

ETAPE 7 Si vous ne l'avez pas encore fait, démarrez CCA et créez un site client.

ETAPE 8 Avec le PC exécutant CCA relié au LAN de l'UC 500, connectez-vous au site client contenant l'UC 500.

ETAPE 9 Sélectionnez **Accueil** > **Topologie** pour afficher la fenêtre Topologie.

Si les caméras auxquelles vous vous connectez ont déjà été mises à jour vers le logiciel adéquat, elles s'affichent dans la fenêtre Topologie.

ETAPE 10 Cliquez sur l'icône Actualiser de la fenêtre Topologie et cliquez avec le bouton droit sur chaque caméra pour sélectionner l'option **Ajouter au site**.

Vous êtes à présent prêt à lancer l'Assistant de configuration de la surveillance vidéo. Voir la rubrique **Lancement et utilisation de l'Assistant de configuration de la surveillance vidéo, page 114**.

Sauvegarde et restauration d'une configuration de périphérique

Pour accéder aux options de sauvegarde et de restauration, sélectionnez **Maintenance>** Archive de configuration dans la barre de fonctions.

Vue d'ensemble

Cette rubrique contient des instructions sur la sauvegarde de la configuration de démarrage de tous les périphériques ou d'un périphérique isolé sur votre PC ou sur un disque réseau. Vous y trouverez également les consignes pour restaurer une configuration sauvegardée.

Outre la configuration de démarrage, les fichiers et répertoires se trouvant sur la mémoire flash de l'UC500 sont eux aussi sauvegardés et restaurés :

- Configuration de la numérotation abrégée système
- fichier vlan.dat (configuration du VLAN)
- Répertoires de la mémoire flash pour les invites BACD, images pour l'écran du téléphone, fichiers audio (musique d'attente) et sonneries
  - flash:bacdprompts/
  - flash:Desktops/
  - flash:ringtones/
  - flash:media/

Si l'UC500 faisant l'objet de la sauvegarde dispose d'une structure récupérée d'une version antérieure, seuls la configuration de démarrage, la configuration du VLAN et les paramètres de numérotation rapide sont sauvegardés et restaurés.

Procédures

Cette partie couvre les rubriques suivantes :

- Pour sauvegarder une configuration, page 121
- Procédez comme suit pour restaurer une configuration à partir d'une sauvegarde :, page 121
- Préférences pour la sauvegarde, page 122

Pour sauvegarder une configuration

Suivez les étapes suivantes pour sauvegarder la configuration de démarrage des périphériques gérés ou de tous les périphériques :

ETAPE 1 Dans la fenêtre Archive des configuration, cliquez sur l'onglet **Sauvegarde**.

ETAPE 2 Dans la liste Nom de l'hôte, sélectionnez **Tous les périphériques** ou le périphérique que vous souhaitez sauvegarder.

ETAPE 3 Dans la zone de texte **Remarques concernant la sauvegarde**, entrez les informations qui vous permettront par la suite d'identifier la configuration enregistrée comme étant celle que vous souhaitez restaurer.

ETAPE 4 Cliquez sur **Sauvegarde**.

Les sauvegardes sont archivées vers le répertoire affiché dans le champ Répertoire de sauvegarde et l'événement est enregistré sous l'onglet Restaurer.

ASTUCE vous pouvez supprimer les configurations archivées qui s'accumulent dans le répertoire de sauvegarde. Le répertoire par défaut est C:\Documents and Settings\<*nom d'utilisateur*>\.configuration assistant\backups.

ETAPE 5 Cliquez sur **OK**.

Procédez comme suit pour restaurer une configuration à partir d'une sauvegarde :

IMPORTANT Vous ne pouvez restaurer la configuration que sur l'UC500 à partir duquel vous avez effectué la sauvegarde. Le transfert de la configuration d'un système UC500 à un autre n'est pas pris en charge.

Pour restaurer une configuration sauvegardée vers la configuration de démarrage d'un périphérique géré, suivez les étapes suivantes :

ETAPE 1 Dans la fenêtre Archive des configurations, sélectionnez le périphérique vers lequel vous souhaitez effectuer la restauration dans la liste Nom de l'hôte.

ETAPE 2 Cliquez sur un bouton pour définir le nombre de configurations sauvegardées à afficher dans la liste Configurations sauvegardées.

Le bouton du haut n'affiche que les configurations sauvegardées à partir du périphérique que vous avez sélectionné. Le bouton du milieu affiche les configurations sauvegardées à partir du périphérique que vous avez sélectionné à partir des autres périphériques du même type sur votre site client. Le bouton du bas affiche toutes les configurations sauvegardées dans le répertoire de sauvegarde.

ETAPE 3 Dans la liste Configurations sauvegardées, sélectionnez une configuration à restaurer.

Consultez la zone de texte Remarque concernant la sauvegarde pour vérifier si la configuration sélectionnée est bien celle souhaitée.

ETAPE 4 Cliquez sur **Restaurer**.

ETAPE 5 Cliquez sur **Redémarrer** pour redémarrer le périphérique une fois la configuration restaurée.

Préférences pour la sauvegarde

Pour effectuer une sauvegarde vers un répertoire distinct, cliquez sur **Préférences** dans la fenêtre Archive des configurations ou sélectionnez l'option **Système** > **Préférences** dans la barre de fonctions.

Dans la fenêtre Préférences, sélectionnez l'onglet Archives des configurations et introduisez un chemin ou un répertoire différent.

L'onglet permet également d'enregistrer automatiquement la configuration active avant la sauvegarde. Si vous ne sélectionnez pas cette option, CCA vous invite à enregistrer la configuration en cours si elle diffère de la configuration de démarrage.

Utilisation de CCA avec Cisco Small Business Office Manager

Cisco Small Business Office Manager est une application gratuite conçue pour le gérant d'une société ou un informaticien. Office Manager permet au gérant ou à l'informaticien d'effectuer des opérations de routine sur Cisco Smart Business Communications System.

Un partenaire de Cisco configure le système à l'aide de CCA, puis personnalise l'application Cisco Office Manager et la laisse sur place, ce qui permet à l'administrateur du site de modifier les paramètres vocaux et utilisateur du système, afficher les flux vidéo en provenance des caméras IP et visualiser l'état du réseau. Les partenaires Cisco peuvent collaborer avec leurs clients pour établir les fonctions dont l'administrateur du site a besoin.

Pour des informations sur le produit et télécharger le logiciel Office Manager, consultez le site www.cisco.com/go/officemanager.

Le manuel d'installation d'Office Manager est accessible à l'adresse :

www.cisco.com/en/US/products/ps11199/prod_installation_guides_list.html

Ressources pour la planification et la mise en œuvre de votre solution SBCS

Les ressources suivantes sont fournies par Cisco afin de permettre la planification et la mise en œuvre de votre solution SBCS :

- **Communauté Cisco Small Business Support Community, page 124**
- **Cisco Smart Designs, page 125**
- **Guides de référence pour les plateformes Cisco UC540 et UC560, page 125**

Communauté Cisco Small Business Support Community

Le site de la communauté Cisco Small Business Support Community offre les ressources destinées aux VAR et aux Partenaires afin de les aider dans la conception, la mise en œuvre et la maintenance des plateformes Cisco SBCS.

Pour accéder à la communauté Cisco Small Business Support, procédez comme suit :

- Dans CCA, Sélectionnez **Connexion aux partenaires**> **Cisco Small Business Support Community** ou
- Ouvrez le navigateur Web et accédez à l'adresse suivante :

  www.cisco.com/go/smallbizsupport

Parmi les ressources, vous trouverez les éléments suivants :

- Domaines d'assistance organisés en fonction du produit, de la technologie ou du pays

  Pour accéder à la zone d'assistance pour Cisco Smart Business Communications System/UC500, sélectionnez **Support Areas** > **Voice and Conferencing** > **SBCS/UC500.**
- Forums de discussion (nécessite une connexion à Cisco.com pour publier les messages, mais pas pour consulter les réponses)
- Formations, dont une médiathèque avec des vidéos à la demande et des didacticiels
- Liens vers les ressources Cisco :
  - Outils de vente et d'assistance technique
  - Outils de conception et de déploiement
  - Guide de configuration et notes sur l'application
  - Téléchargement de logiciels pour UC500
  - Informations sur la garantie SBCS
  - Small & Medium Business (SMB) University

Cisco Smart Designs

Les documents Smart Design de Cisco SBCS regroupent les meilleures pratiques en ce qui concerne la conception et la mise en œuvre des réseaux. Ces solutions simplifiées et préalablement testées sont conçues pour limiter la complexité et le risque tout en assurant le succès aux partenaires. Vous devrez vous connecter en tant que partenaire pour accéder au site.

Rendez-vous à l'adresse suivante pour afficher les documents SBCS Smart Design :

www.cisco.com/go/partner/smartdesigns

Guides de référence pour les plateformes Cisco UC540 et UC560

Pour en savoir plus sur les fonctions des plateformes UC540 et UC560, consultez les guides suivants disponibles sur Cisco.com.

- *Cisco Unified Communications 500 - Modèle 560 pour les petites entreprises : Guide de référence*

  www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps7293/reference_guide_c07-566560.html

- *Cisco Unified Communications 500 - Modèle 540 pour les petites entreprises : Guide de référence*

  www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps7293/C78-557768-00_540_platform_reference_guide_DS_v2a.html

Ces guides de référence présentent les codes des modèles, les interfaces et les modules disponibles, les éléments de licence, les fonctions de base pour les centrales d'appel, l'utilisation des ressources vocales pour les conférences et la conversion de code, la localisation et les données matérielles pour les modèles UC540 et UC560.

Fonctions Cisco SBCS prises en charge par CCA

Le *Guide de référence pour Cisco Smart Business Communications System* permet aux partenaires de Cisco de mieux comprendre les fonctions pouvant être configurées à l'aide des dernières versions de CCA. Ces informations sont classées par catégories (Voix, Commutation, Sans fil, Sécurité).

Ce guide est accessible à partir de l'onglet Resources (Ressources) de la page Cisco Smart Business Communications (www.cisco.com/go/sbcs). Sous CCA, cliquez sur **Connexion aux partenaires** > **Guide des fonctions SBCS** pour accéder au guide.

4

Propriétés du périphérique

Cette partie traite de la configuration des propriétés du périphérique suivantes :

- **Nom de l'hôte**
- **Heure système**
- **Fuseau horaire (dispositifs de sécurité SA 500 uniquement)**
- **Port HTTP**
- **Utilisateurs et mots de passe**
- **Accès aux périphériques distants (Telnet)**
- **SNMP**

Nom de l'hôte

Pour modifier le nom d'hôte d'un périphérique, procédez comme suit :

- Sélectionnez **Configurer** > **Propriétés du périphérique** > **Nom de l'hôte** dans la barre de fonctions.
- Lorsque vous cliquez sur un périphérique avec le bouton droit dans la fenêtre Topologie et sélectionnez l'option **Nom de l'hôte** dans le menu contextuel.

Vue d'ensemble

Vous pouvez attribuer un nom d'hôte à un membre sans nom d'un site client ou le modifier.

Le nom d'hôte s'affiche dans les invites système et dans le menu déroulant Nom de l'hôte dans les fenêtres de configuration de CCA.

La modification du nom n'est pas immédiatement effective. Un message s'affiche dans la barre d'état une fois que la modification est effective.

Procédures

Pour modifier le nom d'hôte d'un périphérique, procédez comme suit :

ETAPE 1 Dans la liste **Nom de l'hôte**, sélectionnez le périphérique dont vous souhaitez modifier le nom.

ETAPE 2 Si vous avez sélectionné un périphérique à partir de la fenêtre Topologie avant d'afficher la fenêtre Nom de l'hôte, le Nom de l'hôte sera prédéfini en fonction de votre sélection.

ETAPE 3 Dans le champ **Nouveau nom d'hôte**, introduisez un nom distinct pour le périphérique. La longueur maximale pour le nom d'hôte est de 31 caractères.

ETAPE 4 Cliquez sur **OK**. La fenêtre Topologie réapparaît et présente le nouveau nom du périphérique.

ETAPE 5 Cliquez sur **Configurer** > **Enregistrer la configuration** pour enregistrer la configuration.

Heure système

Pour définir l'heure système, sélectionnez l'option **Configurer** > **Propriétés du périphérique** > **Heure système**.

IMPORTANT Vous ne pouvez pas définir les paramètres de l'heure système pour le SA500 à partir de cette fenêtre. Pour configurer le fuseau horaire et les paramètres du serveur NTP pour le SA500, sélectionnez **Configurer** > **Propriétés du périphérique** > **Fuseau horaire**. Voir la rubrique **Fuseau horaire (dispositifs de sécurité SA 500 uniquement), page 134**.

Vue d'ensemble

Dans la fenêtre Heure système, vous pouvez effectuer les opérations suivantes :

- Configurer manuellement l'heure et le passage à l'heure d'été/d'hiver sur vos périphériques réseau ;
- Configurer le protocole NTP (protocole d'horloge réseau) de sorte que les périphériques procèdent à des mises à jour à partir d'un serveur NTP ;
- Synchroniser l'heure des périphériques en fonction de l'heure du PC ou de l'heure système d'un périphérique spécifique.

En règle générale, vous ne devez pas régler l'horloge système si le système est synchronisé par un mécanisme d'horloge extérieur (NTP). Si aucune autre source horaire n'est disponible, vous devez régler l'heure manuellement. L'heure spécifiée est relative au fuseau horaire configuré.

Consultez les rubriques suivantes pour plus d'informations :

- **Affichage de l'heure**
- **Définir l'heure système**
- **Synchroniser l'heure système**
- **Configurer le service NTP**

Affichage de l'heure

La fenêtre Heure système affiche automatiquement l'heure : heures (dans un format de 24 heures), minutes, fuseau horaire, mois, date et année pour tous les périphériques de la communauté.

Voici quelques exemples des formats d'heure et de date :

- Mois, jour et année : **Août/2/2005**.
- Heures et minutes : **9:00** (pour 9 h) ou **13:00** (pour 13 h).
- Fuseau horaire : **(GMT -10:00) Hawaï,** ce qui correspond à 10 heures avant l'heure de Greenwich.

Définir l'heure système

Dans la fenêtre Heure système, vous pouvez effectuer les opérations suivantes :

- Définir ou modifier l'heure sur un ou plusieurs périphériques.
- Synchroniser l'heure pour une série de périphériques d'un site client.

Pour régler ou modifier manuellement l'heure système d'un périphérique :

ETAPE 1 Sélectionnez la ligne correspondant au périphérique.

ETAPE 2 Sélectionnez le mois, le jour, l'année, l'heure et les minutes à l'aide des listes déroulantes se trouvant dans les cellules.

Votre sélection de l'heure doit être basée sur le format de 24 heures. Par exemple, pour 9 heures du matin, introduisez **09** ; pour 1 heure de l'après-midi, introduisez **13** ; pour minuit, introduisez **24**.

ETAPE 3 Sélectionnez le fuseau horaire dans les listes déroulantes.

Le temps universel coordonné (UTC) est pris en charge. UTC est identique à l'heure du méridien de Greenwich (GMT). Le décalage (différence entre l'UTC et le fuseau horaire du commutateur) peut être un nombre négatif ou positif.

Par exemple, l'heure du Pacifique présente un décalage de -8 heures, ce qui correspond à 8 heures avant l'UTC. Chaque fuseau horaire est affiché avec le décalage UTC et la plupart des villes et états dans cette région.

ETAPE 4 Sélectionnez **Ajustement automatique heure d'été / heure d'hiver** pour configurer le passage à l'heure d'été.

L'heure d'été est uniquement prise en charge aux États-Unis, au Canada, en Australie et en Europe. Elle commence le jour et l'heure fixés localement.

ETAPE 5 Cliquez sur **OK**.

Pour régler ou modifier manuellement l'heure système de plusieurs périphériques :

ETAPE 1 Sélectionnez les lignes correspondant aux périphériques.

ETAPE 2 Cliquez ensuite sur **Modifier**.

ETAPE 3 Complétez les données de la fenêtre Modifier l'heure système et cliquez sur **OK** pour enregistrer les données. Voir la rubrique **Modifier l'heure système, page 131**.

ETAPE 4 Cliquez sur **Appliquer** pour appliquer les modifications apportées dans la fenêtre Heure système.

ETAPE 5 Cliquez sur **Actualiser** pour mettre à jour la fenêtre.

Synchroniser l'heure système

Pour synchroniser l'heure pour une série de périphériques d'une communauté, procédez comme suit :

ETAPE 1 Cliquez sur **Synchronisation** pour synchroniser tous les périphériques du site. Pour synchroniser des périphériques donnés, sélectionnez-les et cliquez sur **Synchronisation**.

ETAPE 2 Complétez les données de la fenêtre Synchroniser l'heure système et cliquez sur **OK** pour enregistrer les modifications. Voir la rubrique **Synchroniser l'heure système, page 133**.

ETAPE 3 Cliquez sur **Appliquer** pour appliquer les modifications apportées dans la fenêtre Heure système.

ETAPE 4 Cliquez sur **Actualiser** pour mettre à jour la fenêtre Heure système.

Configurer le service NTP

Pour configurer un serveur NTP, procédez comme suit :

ETAPE 1 Dans la fenêtre Heure système, cliquez sur NTP.

ETAPE 2 Complétez les champs de la fenêtre Serveur de temps réseau. Voir la rubrique **Serveur de temps réseau, page 132**.

ETAPE 3 Cliquez sur **Appliquer** pour appliquer les modifications.

ETAPE 4 Cliquez sur **Actualiser** pour mettre à jour la fenêtre Heure système.

Pour de plus amples informations, consultez les rubriques suivantes :

- **Modifier l'heure système, page 131**
- **Synchroniser l'heure système, page 133**
- **Serveur de temps réseau, page 132**

Modifier l'heure système

Cette fenêtre s'affiche lorsque vous sélectionnez un ou plusieurs périphériques et que vous cliquez sur **Modifier** dans la fenêtre Heure système.

REMARQUE Si vous avez sélectionné plusieurs périphériques présentant des paramètres différents, les champs correspondant à ces paramètres sont vides. Si les périphériques sélectionnés présentent les mêmes périphériques, ceux-ci s'affichent.

ETAPE 1 Dans la zone **Date et heure**, sélectionnez le mois, le jour et l'année dans les listes déroulantes.

ETAPE 2 Sélectionnez l'heure et les minutes dans les listes déroulantes.

Votre sélection de l'heure doit être basée sur le format de 24 heures. Par exemple, pour 9 heures du matin, introduisez **09** ; pour 1 heure de l'après-midi, introduisez **13**.

ETAPE 3 Sélectionnez le fuseau horaire dans les listes déroulantes.

Le temps universel coordonné (UTC) est pris en charge. UTC est identique à l'heure du méridien de Greenwich (GMT). Le décalage (différence entre l'UTC et le fuseau horaire du commutateur) peut être un nombre négatif ou positif.

Par exemple, l'heure du Pacifique présente un décalage de -8 heures, ce qui correspond à 8 heures avant l'UTC. Chaque fuseau horaire est affiché avec le décalage UTC et la plupart des villes et états dans cette région.

ETAPE 4 Sélectionnez **Activer** dans le menu déroulant pour activer le passage automatique à l'heure d'été/hiver. Sélectionnez **Désactiver** pour désactiver cette fonction.

L'heure d'été est uniquement prise en charge aux États-Unis, au Canada, en Australie et en Europe. Elle commence le jour et l'heure fixés localement.

ETAPE 5 Quand vous avez terminé vos modifications, cliquez sur **OK**. La fenêtre Heure système s'affiche.

Serveur de temps réseau

Cette fenêtre s'affiche lorsque vous cliquez sur **NTP** dans la fenêtre Heure système.

Utilisez cette fenêtre pour configurer le client NTP (Network Time Protocol) si vous souhaitez qu'il envoie régulièrement des demandes d'heure locale vers un serveur NTP. Le serveur NTP synchronise ensuite l'horloge du système client avec l'horloge du serveur lorsque le périphérique le demande.

Pour augmenter la sécurité, vous pouvez configurer l'authentification NTP. Lorsque l'authentification NTP est définie, le périphérique met à jour l'heure uniquement si le serveur s'identifie correctement. Pour que l'authentification fonctionne correctement, vous devez d'abord obtenir les codes d'accès de l'administrateur du serveur et les introduire dans les champs Authentification NTP.

Voici comment faire pour configurer les périphériques pour qu'ils reçoivent les mises à jour de l'heure à partir d'un serveur NTP et pour configurer l'authentification NTP :

ETAPE 1 Dans le champ **Adresse IP**, introduisez l'adresse IP du serveur horaire.

ETAPE 2 *Facultatif* : dans le champ **Code**, introduisez le code à utiliser lorsque vous envoyez des paquets au serveur. Introduisez un nombre allant de 1 à 4294967295.

ETAPE 3 *Facultatif* : dans le champ **Valeur de la clé**, introduisez la clé secrète. Entrez 32 caractères au maximum. Les espaces ainsi que les caractères !, ", #, $, }, | et ~ ne sont pas admis.

ETAPE 4 *Facultatif* : dans le champ **Type de cryptage**, introduisez le numéro utilisé pour crypter la clé. Introduisez un nombre allant de 1 à 4294967295.

ETAPE 5 Cliquez sur **OK** pour fermer la fenêtre Serveur de temps réseau et revenir à la fenêtre Heure système.

Synchroniser l'heure système

Cette fenêtre s'affiche lorsque vous cliquez sur **Synchronisation** ou sélectionnez un ou plusieurs périphériques et que vous cliquez sur **Synchronisation** dans la fenêtre Heure système.

Vue d'ensemble

Cette fenêtre affiche l'heure actuelle sur le PC.

Vous pouvez synchroniser l'heure système de périphériques donnés avec l'heure système du PC. Vous pouvez aussi effectuer la synchronisation en fonction de l'heure système d'un périphérique donné. Vous pouvez aussi modifier les paramètres de fuseau horaire de certains périphériques.

Par exemple, si vous synchronisez l'heure système d'un périphérique à New York avec un périphérique à San Jose, lequel affiche 13 h (PST), au terme de la synchronisation, le périphérique de New York affichera 16 h EST. Toutefois, si vous cochez la case **Écraser le fuseau horaire**, le périphérique de New York affichera 13 h PST comme le périphérique de San Jose. L'heure locale est donc modifiée.

Procédures

Pour synchroniser l'heure système des périphériques sélectionnés avec l'heure du PC, procédez comme suit :

ETAPE 1 Sélectionnez **Synchronisation avec le PC**.

ETAPE 2 Sélectionnez **Écraser le fuseau horaire** si vous souhaitez modifier l'heure locale pour les périphériques sélectionnés.

ETAPE 3 Cliquez sur **OK** pour enregistrer vos modifications et revenir à la fenêtre Heure système.

Pour synchroniser l'heure système des périphériques sélectionnés en fonction de l'heure d'un périphérique donné, procédez comme suit :

ETAPE 1 Sélectionnez **Synchronisation avec le périphérique**.

ETAPE 2 Sélectionnez le périphérique avec lequel vous souhaitez effectuer la synchronisation dans la liste déroulante.

ETAPE 3 Sélectionnez **Écraser le fuseau horaire** si vous souhaitez modifier l'heure locale pour les périphériques sélectionnés.

Cliquez sur **OK** pour enregistrer vos modifications et revenir à la fenêtre Heure système.

Fuseau horaire (dispositifs de sécurité SA 500 uniquement)

La fenêtre Gestion du fuseau horaire s'affiche lorsque vous sélectionnez **Configurer** > **Propriétés du périphérique** > **Fuseau horaire** dans la barre de fonctions. Cette option s'affiche uniquement si vous êtes connecté à un dispositif de sécurité autonome de la série SA500 ou si le site client CCA en est équipé.

Vue d'ensemble

Dans la fenêtre Gestion du fuseau horaire, vous pouvez effectuer les opérations suivantes :

- Définir le fuseau horaire sur le SA500
- Choisir de passer automatiquement à l'heure d'été/hiver
- Indiquer si vous souhaitez utiliser les serveurs NTP par défaut pour les mises à jour de l'heure système ou entrer jusqu'à deux serveurs NTP personnalisés

- Afficher l'heure sur le SA500

Vous ne pouvez pas définir manuellement l'heure système sur le SA500.

Procédures

Pour configurer les paramètres de fuseau horaire sur le SA500, complétez les champs conformément au tableau ci-dessous et cliquez sur **OK** ou **Appliquer**.

Paramètre	Description
Nom de l'hôte	Nom d'hôte du SA500 que vous configurez. Valeur par défaut : SA500.
Fuseau horaire	Sélectionnez le fuseau horaire dans les listes déroulantes. Le temps universel coordonné (UTC) est pris en charge. UTC est identique à l'heure du méridien de Greenwich (GMT). Le décalage (différence entre l'UTC et le fuseau horaire du commutateur) peut être un nombre négatif ou positif. Par exemple, l'heure du Pacifique présente un décalage de -8 heures, ce qui correspond à 8 heures avant l'UTC. Chaque fuseau horaire est affiché avec le décalage UTC et la plupart des villes et états dans cette région.
Passage automatique à l'heure d'été/hiver	Lorsque cette case est cochée, le SA500 passe automatiquement à l'heure d'été/hiver. Le passage à l'heure d'été/hiver est uniquement pris en charge aux États-Unis, au Canada, en Australie et en Europe. Elle commence le jour et l'heure fixés localement.
Utiliser les serveurs NTP par défaut	Configurez le SA500 afin qu'il obtienne les mises à jour de l'heure à partir des serveurs NTP par défaut. Les serveurs par défaut sont `0.us.ntp.pool.org` et `1.us.ntp.pool.org`.
Utiliser les serveurs NTP personnalisés	Lorsque cette option est cochée, vous pouvez définir un maximum de deux serveurs NTP personnalisés pour la mise à jour de l'heure.

Paramètre	Description
Serveur NTP 1 **Serveur NTP 2**	Si l'option Utiliser les serveurs NTP personnalisés est cochée, entrez le nom d'hôte ou l'adresse IP publique des serveurs NTP dans ces champs.
Heure actuelle	Champ en lecture seule affichant la date et l'heure du SA500, par exemple, samedi, 1er janvier 2010, 22:24:24 (GMT +0000).

Port HTTP

Pour modifier le numéro de port HTTP pour tous les périphériques d'un site client, sélectionnez **Configurer** > **Propriétés du périphérique**> **Port HTTP** dans la barre de fonctions.

Vue d'ensemble

Configuration Assistant se connecte à n'importe quel périphérique du site client par le port HTTP ou HTTPS.

- Vous pouvez modifier le numéro de port HTTP mais vous ne pouvez pas modifier le numéro de port HTTPS.
- Le port par défaut 443 doit impérativement être utilisé pour le protocole HTTPS.

HTTPS fait en sorte que les échanges entre Configuration Assistant et les périphériques gérés soient cryptés. Vous ne pouvez utiliser le protocole HTTPS uniquement en présence d'une image chiffrée de Cisco IOS.

Une alerte s'affiche lorsque vous vous utilisez le protocole HTTPS pour vous connecter pour la première fois. Elle vous demande si vous acceptez un certificat indiquant que le périphérique connecté est un site de confiance. Vous avez le choix entre **Oui**, **Non**, **Toujours** et **Afficher le certificat**.

Choisissez **Oui** ou **Toujours** pour continuer. Vous ne serez plus averti au cours des sessions suivantes si vous sélectionnez **Toujours**.

Lorsque vous utilisez HTTPS, une icône s'affiche dans la barre d'état.

Procédures

Pour configurer le port HTTP, procédez comme suit :

ETAPE 1 Introduisez un autre numéro de port dans le champ **Port HTTP**. Le port par défaut est le 80. L'autre plage de valeurs possibles est comprise entre 1025 et 65535.

Cliquez sur **OK**. Le nouveau numéro de port HTTP se propage alors à tous les membres du site client.

Utilisateurs et mots de passe

Pour définir les mots de passe et associer les mots de passe à des noms d'utilisateurs et niveaux de privilège, choisissez **Configurer** > **Périphérique Propriétés** > **Utilisateurs et mots de passe**.

Vue d'ensemble

Vous pouvez gérer l'accès à CCA au moyen de mots de passe seuls ou de mots de passe couplés à des noms d'utilisateurs. Vous pouvez également associer un niveau de privilège à un mot de passe et à un nom d'utilisateur de manière à gérer l'accès en fonction de l'utilisateur.

Selon le type de périphérique que vous configurez, différents types de privilèges peuvent être affectés.

- Pour les dispositifs de sécurité Cisco Small Business Pro SA500, les niveaux de privilège disponibles sont : Invité (accès en lecture seule), Admin et Utilisateur SSL VPN.
- Point d'accès Cisco AP541N :
  - Vous ne pouvez pas ajouter d'utilisateurs, modifier le nom d'utilisateur de l'administrateur (cisco) ni le niveau de privilège correspondant (Admin).
  - Vous pouvez uniquement modifier le mot de passe par défaut de l'administrateur (cisco).
- Pour les caméras Internet PVC2300 et WVC2300 :
  - Différents privilèges sont disponibles (Admin, Supervision et Affichage).

  - Vous ne pouvez pas modifier le nom d'utilisateur par défaut de l'administrateur (admin), mais vous pouvez créer des utilisateurs disposant de privilèges de type Admin).

- Pour l'UC500 et les autres périphériques IOS, les niveaux de privilège varient de 1 à 15 :
  - Le niveau de privilège 15 donne un accès en lecture et en écriture. Les utilisateurs à ce niveau peuvent voir et configurer toutes les options de CCA.
  - Les niveaux de privilège 1 à 14 donnent l'accès en lecture seule. Les options de la barre de fonctions, de la barre d'outils, des menus contextuels et des fenêtres de fonctions qui peuvent modifier la configuration d'un périphérique ne sont pas affichées.

Pour définir les mots de passe et associer les mots de passe à des noms d'utilisateurs et niveaux de privilège, utilisez la fenêtre Utilisateurs et mots de passe.

Procédures

Dans la fenêtre Utilisateurs et mots de passe, vous pouvez effectuer les opérations suivantes :

- **Donner accès à tous les périphériques du site**
- **Accorder l'accès à un périphérique donné**

Commencez par sélectionner **Tous les périphériques** ou un périphérique spécifique dans la liste **Nom de l'hôte**.

Lorsque vous avez terminé de configurer les utilisateurs et les mots de passe, cliquez sur **OK**.

Donner accès à tous les périphériques du site

Pour accorder l'accès à tous les périphériques de votre site client, suivez les étapes suivantes :

ETAPE 1 Dans le champ **Nom d'utilisateur admin**, introduisez le nom qu'emploiera un administrateur pour accéder à tous les périphériques de la communauté.

ETAPE 2 Dans le champ **Mot de passe**, introduisez le mot de passe qu'emploiera l'administrateur. Votre entrée est cryptée et s'affiche sous forme d'astérisques.

ETAPE 3 Introduisez à nouveau le mot de passe dans le champ **Confirmer le mot de passe**.

Accorder l'accès à un périphérique donné

REMARQUE Le nom d'utilisateur, le mot de passe et les options d'accès au périphérique varient en fonction des périphériques sélectionnés. Si un onglet ne s'affiche pas pour un périphérique, c'est que l'option n'est pas prise en charge.

Utilisez les onglets suivants pour accorder l'accès à un périphérique donné :

- **Nom d'utilisateur/mot de passe local**permet d'associer les noms d'utilisateur et mots de passe à des niveaux de privilège
- **Authentification HTTP**permet de spécifier si les utilisateurs introduisent un nom d'utilisateur et un mot de passe ou uniquement un mot de passe pour accéder à Configuration Assistant.
- **Activer le mot de passe**permet d'associer les mots de passe à des niveaux de privilège
- **Mot de passe console/Telnet**permet d'associer les mots de passe à la ligne de commande et aux sessions Telnet

Nom d'utilisateur/mot de passe local

Cet onglet indique les noms d'utilisateur, les mots de passe et les niveaux de privilège qui leur sont associés. Les utilisateurs qui introduisent un nom d'utilisateur et un mot de passe dans cet onglet ont accès à CCA selon un niveau défini.

Les options relatives au nom d'utilisateur local et au mot de passe varient en fonction du périphérique que vous configurez.

Point d'accès Cisco AP541N :

- Vous ne pouvez pas ajouter d'utilisateurs, modifier le nom d'utilisateur de l'administrateur (cisco) ni le niveau de privilège correspondant (Admin).
- Vous pouvez uniquement modifier le mot de passe par défaut de l'administrateur (cisco).

Pour introduire une nouvelle ligne (un nouveau nom d'utilisateur, mot de passe et niveau de privilège), cliquez sur **Créer**. Utilisez ensuite la fenêtre Créer un nom d'utilisateur / un mot de passe local. Voir la rubrique **Créer utilisateur, page 141**.

Pour modifier le mot de passe ou un niveau de privilège d'un utilisateur, sélectionnez-le dans la liste, cliquez sur **Modifier** et utilisez la fenêtre Modifier un nom d'utilisateur / un mot de passe local.

Pour supprimer un enregistrement, sélectionnez-le et cliquez sur **Supprimer**.

Authentification HTTP

Sous cet onglet, cliquez sur **Activer le mot de passe** si vous souhaitez que les utilisateurs accèdent au périphérique sélectionné en introduisant uniquement un mot de passe. Cliquez sur **Nom d'utilisateur/mot de passe local** si vous souhaitez qu'ils introduisent un nom d'utilisateur et un mot de passe.

Veillez à utiliser également l'onglet **Activer le mot de passe** pour définir les mots de passe ou l'onglet **Nom d'utilisateur/mot de passe local** pour définir les noms d'utilisateur et les mots de passe.

Activer le mot de passe

Cet onglet indique les niveaux de privilège et les mots de passe. Les utilisateurs qui introduisent un mot de passe dans cet onglet ont accès à Configuration Assistant selon le niveau de privilège correspondant.

Pour créer un nouveau mot de passe et un niveau de privilège, cliquez sur **Créer**, et utilisez la fenêtre Créer le mot de passe d'activation.

REMARQUE si un mot de passe existe pour tous les niveaux de privilège de 1 à 15, le bouton **Créer** sera désactivé.

Pour modifier un mot de passe, sélectionnez-le et cliquez sur **Modifier**. Utilisez ensuite la fenêtre Modifier le mot de passe d'activation. Voir la rubrique **Modifier le mot de passe d'activation, page 143**.

Pour supprimer un mot de passe, sélectionnez-le et cliquez sur **Supprimer**. Le mot de passe et le niveau de privilège sont supprimés de l'onglet.

Mot de passe console/Telnet

Cet onglet affiche les mots de passe qui sont associés à la ligne de console et aux sessions Telnet.

Dans une session Telnet, un mot de passe Telnet donne un accès en lecture seule à un périphérique. La configuration du périphérique est impossible. En liaison Telnet avec le périphérique, les utilisateurs sont invités à introduire un mot de passe commun. Le nom d'utilisateur ne leur est pas demandé. Si vous n'entrez pas de mot de passe Telnet ou le supprimez, les utilisateurs seront invités à introduire leur nom d'utilisateur et leur mot de passe sous l'onglet **Nom d'utilisateur/mot de passe local**.

L'introduction du mot de passe pour la console vous donne un accès en lecture et en écriture. Si vous avez créé et activé un mot de passe, vous devez introduire celui-ci plutôt que le mot de passe console pour bénéficier d'un accès en lecture et en écriture.

Pour créer ou modifier des mots de passe, introduisez-les dans le champ **Mot de passe** et réintroduisez-les dans le champ **Confirmer le mot de passe**.

Créer utilisateur

Cette fenêtre s'affiche lorsque vous cliquez sur **Créer** sous l'onglet Nom d'utilisateur/mot de passe local dans la fenêtre Utilisateurs et mots de passe. Utilisez-la pour spécifier un nom d'utilisateur, un mot de passe et un niveau de privilège.

Les options disponibles varient en fonction du périphérique que vous configurez.

Suivez les étapes ci-dessous :

ETAPE 1 Dans le champ **Nom d'utilisateur**, introduisez le nom qu'emploiera un utilisateur pour accéder à Configuration Assistant.

ETAPE 2 Dans le champ **Mot de passe**, introduisez le mot de passe qu'emploiera l'utilisateur. La valeur est chiffrée.

ETAPE 3 Introduisez à nouveau le mot de passe dans le champ **Confirmation du mot de passe**.

ETAPE 4 Sélectionnez un niveau de privilège dans la liste Niveau de privilège. Selon le périphérique que vous configurez, plusieurs options s'affichent pour le Niveau de privilège.

Pour les plateformes UC500 et les autres périphériques IOS, le Niveau 15 attribue un accès en lecture et en écriture, les niveaux de 1 à 14 attribuent un accès en lecture seule.

Pour les dispositifs de sécurité SA500, vous pouvez définir le niveau Invité (pour un accès en lecture seule) et Utilisateur SSL VPN.

Pour les caméras Internet Cisco PVC2300 et WVC2300, faites votre choix parmi les niveaux de privilège suivants :

- **Admin** : permet à l'utilisateur d'administrer et de contrôler la caméra et la vidéo.
- **Supervision** : permet à l'utilisateur de piloter la caméra (panoramique/inclinaison manuelle, basculement en vision diurne/nocturne, activation des ports de sortie). Les utilisateurs intégrés à l'aide de l'Assistant de configuration de la surveillance vidéo se voient attribuer l'autorisation de niveau Supervision.
- **Affichage** : permet à l'utilisateur d'afficher la vidéo à l'aide d'un navigateur Web, d'un téléphone IP ou de toute autre application.

ETAPE 5 Cliquez sur **OK**. Une fois de retour à la fenêtre Utilisateurs et mots de passe, vous verrez une nouvelle entrée sous l'onglet Nom d'utilisateur/mot de passe local.

Modifier le mot de passe utilisateur

Cette fenêtre s'affiche lorsque vous sélectionnez une entrée et cliquez sur **Modifier** sous l'onglet Nom d'utilisateur/mot de passe local dans la fenêtre Utilisateurs et mots de passe. Elle vous permet de modifier le mot de passe et le niveau de privilège associé au nom d'utilisateur.

Suivez les étapes ci-dessous :

ETAPE 1 Si vous souhaitez modifier le mot de passe, entrez un nouveau mot de passe dans le champ **Mot de passe**. Votre entrée est cryptée et s'affiche sous forme d'astérisques.

ETAPE 2 Introduisez à nouveau le mot de passe dans le champ **Confirmer le mot de passe**.

ETAPE 3 Si vous souhaitez modifier le niveau de privilège, sélectionnez un autre niveau dans la liste Niveau de privilège.

ETAPE 4 Cliquez sur **OK**.

Modifier le mot de passe d'activation

Cette fenêtre s'affiche lorsque vous sélectionnez un mot de passe et cliquez sur **Modifier** sous l'onglet Activer le mot de passe dans la fenêtre Utilisateurs et mots de passe. Utilisez-la pour modifier le mot de passe du niveau de privilège.

Suivez les étapes ci-dessous :

ETAPE 1 Dans le champ **Mot de passe** de l'interface, introduisez un nouveau mot de passe pour le niveau de privilège correspondant. Votre entrée est cryptée et s'affiche sous forme d'astérisques.

ETAPE 2 Introduisez à nouveau le mot de passe dans le champ **Confirmation du mot de passe**.

ETAPE 3 Cliquez sur **OK**.

Accès aux périphériques distants (Telnet)

L'accès à distance par Telnet est toujours actif étant donné que CCA ne fonctionnera pas correctement sans accès à Telnet. La fenêtre Accès aux périphériques incluses dans les versions précédentes de CCA a été supprimée. CCA n'utilise plus le protocole SSH.

SNMP

Pour définir le protocole SNMP, sélectionnez l'option **Configurer** > **Propriétés du périphérique** > **Gestion SNMP**.

Vue d'ensemble

La gestion SNMP englobe les missions suivantes :

- Désactivation ou activation du SNMP sur un commutateur indépendant
- Réglage des options du système
- Ajout et suppression des chaînes de communauté
- Ajout et suppression des gestionnaires des interruptions
- Création d'affichages des objets MIB qui sont accessibles aux groupes d'utilisateurs
- Association des affichages aux groupes qui peuvent y avoir accès
- Association des groupes aux utilisateurs qui en font partie

Procédures

Cette fenêtre présente les onglets suivants :

- **Options système**permet d'attribuer des informations d'administration à un périphérique afin de l'identifier
- **Chaînes de communauté**permet d'ajouter et supprimer les chaînes de communauté
- **Gestionnaires d'interruption**permet d'ajouter et supprimer des gestionnaires d'interruption
- **Filtre (commutateurs ESW500)**permet de créer des ensembles d'interruptions pouvant être envoyés au gestionnaire d'interruption (commutateurs Cisco ESW 500 uniquement)
- **Affichages**permet de créer les affichages des objets MIB qui sont accessibles aux groupes d'utilisateurs
- **Groupes**permet d'associer les affichages aux groupes qui peuvent y avoir accès
- **Utilisateurs**permet d'associer les groupes aux utilisateurs qui en font partie

Les onglets disponibles et les options de configuration SNMP varient en fonction des périphériques. Certains périphériques ne prennent pas en charge toutes les options de configuration SNMP sous CCA.

Pour commencer :

- Sélectionnez le périphérique dans la liste **Nom de l'hôte**. Les onglets et leurs paramètres s'appliquent au périphérique sélectionné. Seuls les onglets **Affichages**, **Groupes** et **Utilisateurs** s'affichent si le périphérique prend en charge la version 3 ou supérieure de SNMP.
- Assurez-vous que la case **Activer SNMP** est activée.

Lorsque vous avez terminé l'introduction des paramètres sur les onglets, cliquez sur **OK**.

Options système

Bien que SNMP autorise un maximum de 255 caractères pour chaque champ dans cet onglet, Configuration Assistant tronque ces informations pour les raccourcir. Pour cette raison, nous recommandons de limiter la longueur du texte. Voir les étapes individuelles dans la procédure suivante pour les directives.

Pour attribuer les options système, procédez comme suit :

ETAPE 1 Dans le champ **Emplacement système**, introduisez l'emplacement physique du périphérique. La longueur maximum d'une entrée dans le champ **Emplacement système** est de 129 caractères.

ETAPE 2 Dans le champ **Contact système**, introduisez le nom ou l'entreprise responsable pour le périphérique. La longueur maximum d'une entrée dans le champ **Contact système** est de 129 caractères.

Chaînes de communauté

Les chaînes de communauté servent de mots de passe pour authentifier les messages SNMP. Chaque chaîne de communauté est soit en mode Lecture seule, ce qui permet d'afficher les informations sur l'objet MIB, ou en mode Lecture-Écriture, ce qui permet d'afficher et de modifier les informations sur l'objet MIB.

La première chaîne de communauté en mode Lecture seule et la première chaîne de communauté en mode Lecture-Écriture figurent dans la liste de la fenêtre Gestion SNMP. Étant donné qu'elles sont nécessaires au routage des paquets SNMP, elles ne doivent pas être supprimées des périphériques.

La configuration SNMP peut également contenir des chaînes de communauté définies par l'utilisateur.

Si votre mode d'accès est en lecture seule, vous ne voyez pas les chaînes de communauté dans cette liste.

Ajout de chaînes de communauté

Le périphérique sélectionné prend en charge un nombre illimité de chaînes de communauté de n'importe quelle longueur.

Procédez comme suit pour ajouter une nouvelle chaîne de communauté à un périphérique :

ETAPE 1 Dans le champ **Nouvelle chaîne**, entrez une chaîne de caractères.

ETAPE 2 Sélectionnez **RO** (Lecture seule) ou **RW** (Lecture-Écriture) pour définir le type de chaîne.

ETAPE 3 Cliquez sur **Ajouter** pour déplacer la nouvelle chaîne de communauté dans la liste **Chaînes actuelles**.

Suppression des chaînes de communauté

Ne supprimez pas la première chaîne de communauté en mode Lecture seule ni la première chaîne de communauté en mode Lecture-Écriture. Les chaînes sont nécessaires pour les fonctions SNMP.

Pour supprimer une chaîne de communauté existante :

ETAPE 1 Dans la liste **Chaînes existantes**, sélectionnez les chaînes de communauté qui doivent être supprimées.

ETAPE 2 Pour supprimer toutes les chaînes de communauté, cliquez sur **Sélectionner tout**.

ETAPE 3 Cliquez ensuite sur **Supprimer**.

Gestionnaires d'interruption

Un gestionnaire d'interruption est un poste de gestion qui reçoit des interruptions et les alertes système générées par un périphérique. Par défaut, aucun gestionnaire d'interruption n'est défini et aucune interruption n'est envoyée.

Afin de permettre au périphérique sélectionné d'envoyer des interruptions, cochez **Activer les interruptions**. Ensuite, cochez les cases en regard des types d'interruptions que vous souhaitez activer pour chaque IP cible.

Pour ajouter un nouveau gestionnaire d'interruption, effectuez les opérations suivantes :

ETAPE 1 Dans le champ **Adresse IP**, entrez l'adresse IP du nouveau gestionnaire d'interruption.

ETAPE 2 Dans le champ **Chaîne de communauté**, entrez la chaîne de communauté pour le nouveau gestionnaire d'interruption.

ETAPE 3 Dans le champ **Port UPD**, entrez le port UDP du gestionnaire d'interruption auquel les interruptions doivent être envoyées.

ETAPE 4 Pour envoyer chaque type d'interruption au gestionnaire d'interruption, cochez l'option **Envoyer toutes les interruptions**. Autrement, cochez seulement les types d'interruption que vous souhaitez envoyer.

ETAPE 5 Pour une description des types d'interruption, reportez-vous au guide de configuration du logiciel pour le périphérique sélectionné.

ETAPE 6 *Facultatif.* Si vous configurez un gestionnaire d'interruption sur un commutateur ESW 500, vous pouvez sélectionner un filtre pour le Gestionnaire d'interruption si des filtres ont été définis.

ETAPE 7 Cliquez sur **Ajouter** pour déplacer votre entrée dans la liste **Gestionnaires actuels**.

Si votre mode d'accès est en lecture seule, vous ne voyez pas les gestionnaires d'interruption et leurs chaînes de communauté dans cette liste.

Pour supprimer un gestionnaire d'interruption, procédez comme suit :

ETAPE 1 Dans la liste **Gestionnaires actuels**, sélectionnez les gestionnaires d'interruption qui doivent être supprimés.

ETAPE 2 Pour supprimer tous les gestionnaires des interruptions existants, cliquez sur **Sélectionner tout**.

ETAPE 3 Cliquez ensuite sur **Supprimer**.

Filtre (commutateurs ESW500)

L'onglet Filtre s'applique uniquement aux commutateurs Cisco Small Business Pro ESW 500.

Il vous permet de créer, modifier et supprimer les filtres SNMP. Le filtre SNMP définit un ensemble d'interruptions transmis au gestionnaire d'interruption. Les filtres créés à partir de cet onglet peuvent être sélectionnés sous l'onglet Gestionnaires d'interruption.

Pour créer un filtre, procédez comme suit :

ETAPE 1 Cliquez sur **Créer**.

ETAPE 2 Dans la fenêtre Créer un filtre pour les interruptions SNMP, entrez un nom composé de 1 à 30 caractères (les espaces ne sont pas autorisées). Après avoir validé les modifications, le nom s'affiche dans le menu Sélectionner le filtre de l'onglet Gestionnaires d'interruption.

ETAPE 3 Sélectionnez au moins un OID dans la liste Disponible et utilisez les boutons **Ajouter**, **Supprimer** et **Sélectionner tout** pour déplacer les OID de la liste Disponible à la liste Sélectionné.

ETAPE 4 Cliquez sur **OK** pour fermer la fenêtre Créer un filtre pour les interruptions SNMP.

ETAPE 5 Dans la fenêtre Gestion SNMP, cliquez sur **Appliquer** ou sur **OK**.

Pour supprimer un filtre, sélectionnez le filtre dans la liste et cliquez sur **Supprimer**. Vous pouvez uniquement supprimer les filtres inutilisés. Si le filtre est utilisé par un Gestionnaire d'interruption, vous serez invité(e) à supprimer le filtre du Gestionnaire d'interruption au préalable.

Pour modifier un filtre, sélectionnez le filtre dans la liste et cliquez sur **Modifier**.

Créer ou modifier un filtre SNMP (commutateurs ESW 500)

Cette fenêtre s'affiche lorsque vous sélectionnez l'option **Créer** ou **Modifier** sous l'onglet Filtre de la fenêtre Gestion SNMP pour les commutateurs Cisco ESW 500.

Cette fenêtre vous permet de créer et de modifier les filtres SNMP. Le filtre SNMP définit un ensemble d'interruptions transmis au gestionnaire d'interruption. Les filtres créés à partir de cet onglet peuvent être sélectionnés sous l'onglet Gestionnaires d'interruption de la fenêtre Gestion SNMP.

Pour créer ou modifier un filtre SNMP, procédez comme suit :

ETAPE 1 Entrez un **nom de filtre** composé de 1 à 30 caractères (les espaces ne sont pas autorisées). Après avoir validé les modifications, le nom s'affiche dans le menu Sélectionner le filtre de l'onglet Gestionnaires d'interruption.

ETAPE 2 Utilisez les boutons **Ajouter**, **Supprimer**, **Sélectionner tout** pour déplacer les OID de la liste Disponible vers la liste Sélectionné.

ETAPE 3 Cliquez sur **OK**.

Affichages

Cet onglet affiche les noms des affichages, les collections d'objets MIB pour lesquels les groupes d'utilisateurs peuvent avoir :

- Accès en lecture
- Accès en écriture
- Privilèges de notification

Pour créer un affichage et ajouter son nom dans cet onglet, cliquez sur **Créer** et utilisez la fenêtre Créer un affichage SNMP. Voir la rubrique **Créer un affichage SNMP, page 150**.

Pour modifier un affichage, sélectionnez-le et cliquez sur **Modifier**. Utilisez la fenêtre Modifier un affichage SNMP.

Si vous souhaitez supprimer un affichage, sélectionnez-le et cliquez sur **Supprimer**.

Vous ne pouvez pas supprimer ou modifier l'affichage **v1default**.

Créer un affichage SNMP

Cette fenêtre s'affiche lorsque vous cliquez sur **Créer** sous l'onglet Affichages dans la fenêtre SNMP.

Pour supprimer un affichage SNMP, procédez comme suit :

ETAPE 1 Entrez un nom pour l'affichage dans le champ **Nom de l'affichage**.

ETAPE 2 Sélectionnez un ou plusieurs objets OID (identifiant de l'objet MIB) dans la liste OID. Pour sélectionner tous les objets OID, cliquez sur **Sélectionner tout**.

ETAPE 3 Cliquez sur **Ajouter** pour déplacer les OID sélectionnées dans la liste OID incluses. Ce sont les OID qui constitueront le nouvel affichage. Pour remettre les OID dans la liste des OID, sélectionnez-les et cliquez sur **Supprimer**.

ETAPE 4 Cliquez sur **OK**. Le nom de l'affichage créé figure sous l'onglet Affichages de la fenêtre SNMP.

Modifier l'affichage SNMP

Cette fenêtre s'affiche lorsque vous sélectionnez un affichage et cliquez sur Modifier sous l'onglet Affichages dans la fenêtre SNMP.

Pour modifier un affichage SNMP, procédez comme suit :

ETAPE 1 Dans la liste OID, sélectionnez tous les objets OID que vous souhaitez ajouter à l'affichage. Cliquez ensuite sur **Ajouter**.

ETAPE 2 Dans la liste OID incluses, sélectionnez toutes les OID que vous souhaitez supprimer de l'affichage. Cliquez ensuite sur **Supprimer**.

ETAPE 3 Cliquez sur **OK**.

Groupes

Les colonnes de cet onglet ont les significations suivantes :

Colonne	Signification
Groupe	Nom d'un groupe d'utilisateurs
Niveau de sécurité	Les utilisateurs doivent-ils entrer un mot de passe (**Authentifier**) et le mot de passe doit-il être crypté (**Confidentialité**) ?
Mode lecture	Affichage pour lequel le groupe dispose d'un accès en lecture
Mode écriture	Affichage pour lequel le groupe dispose d'un accès en écriture
Mode notification	Affichage pour lequel le groupe dispose de privilèges de notification

Pour créer un groupe et ajouter ses attributs dans cet onglet, cliquez sur **Créer**, et utilisez la fenêtre Créer un groupe SNMP. Voir la rubrique **Créer un groupe SNMP, page 151**.

Pour modifier un groupe, sélectionnez-le et cliquez sur **Modifier**.Utilisez la fenêtre Modifier un groupe SNMP.

Si vous souhaitez supprimer un groupe, sélectionnez-le et cliquez sur **Supprimer**.

Vous ne pouvez pas supprimer ou modifier le groupe **v1default**.

Créer un groupe SNMP

Cette fenêtre s'affiche lorsque vous cliquez sur **Créer** sous l'onglet Groupes de la fenêtre SNMP. Utilisez-la pour spécifier les attributs d'un groupe d'utilisateurs SNMP.

Pour créer un groupe SNMP, procédez comme suit :

ETAPE 1 Dans le champ **Nom du groupe**, entrez un nom pour le nouveau groupe.

Vous pouvez entrer le nom d'un groupe qui existe déjà, si vous sélectionnez un niveau de sécurité différent. Un nom de groupe et un niveau de sécurité permettent d'identifier le groupe.

ETAPE 2 Dans la liste **Niveau de sécurité**, sélectionnez un niveau de sécurité.

- "NoAuthenticate" signifie qu'aucune authentification n'est requise pour les paquets.
- "Authentifier" signifie qu'une authentification du paquet est requise.
- "Confidentialité" signifie que le cryptage du paquet est requis. Cette option n'est disponible que si vous disposez d'un logiciel de cryptage.

ETAPE 3 *Facultatif* : Dans la liste Mode lecture, sélectionnez un affichage auquel le groupe aura un accès en lecture.

ETAPE 4 *Facultatif* : Dans la liste Mode écriture, sélectionnez un affichage auquel le groupe aura un accès en écriture.

ETAPE 5 *Facultatif* : Dans la liste Mode Notification, sélectionnez un affichage avec des notifications à envoyer au groupe.

ETAPE 6 Cliquez sur **OK**. Lorsque vous revenez à la fenêtre SNMP, une nouvelle entrée s'affiche sous l'onglet Groupes.

Modifier le groupe SNMP

Cette fenêtre s'affiche lorsque vous sélectionnez un groupe et cliquez sur **Modifier** sous l'onglet Groupes de la fenêtre SNMP.

Voici les attributs du groupe que vous pouvez modifier :

- L'affichage des objets MIB pour lesquels le groupe dispose d'un accès en lecture.
- L'affichage des objets MIB pour lesquels le groupe dispose d'un accès en écriture.
- L'affichage des objets MIB envoyés au groupe avec des notifications.

Pour de plus amples informations sur ces options d'affichage, reportez-vous à la rubrique **Créer un groupe SNMP**.

Lorsque vous avez terminé, cliquez sur **OK**.

Utilisateurs

Ce tableau explique ce que contient chaque colonne de cet onglet.

Colonne	Sommaire
Utilisateur	Noms des utilisateurs
Groupe	Groupe auquel les utilisateurs appartiennent
Algorithme d'authentification	Type d'algorithme qui est utilisé pour crypter le mot de passe d'authentification.

Pour affecter un utilisateur à un groupe et ajouter l'utilisateur à cet onglet, cliquez sur **Créer** et utilisez la fenêtre Créer un utilisateur SNMP. Voir la rubrique **Créer un utilisateur SNMP, page 153**.

Pour modifier les attributs d'un utilisateur, y compris le groupe auquel l'utilisateur appartient, sélectionnez l'utilisateur, cliquez sur **Modifier** et utilisez la fenêtre Modifier l'utilisateur SNMP.

Pour supprimer un utilisateur, sélectionnez l'utilisateur et cliquez sur **Supprimer**.

Créer un utilisateur SNMP

Cette fenêtre s'affiche lorsque vous cliquez sur **Créer** sous l'onglet Utilisateurs dans la fenêtre SNMP. Utilisez-la pour définir les attributs d'un utilisateur SNMP.

Pour créer un groupe SNMP, procédez comme suit :

ETAPE 1 Dans le champ **Nom d'utilisateur**, entrez un nom pour l'utilisateur.

ETAPE 2 Dans la liste **Nom du groupe**, sélectionnez le groupe auquel l'utilisateur appartient. (Le groupe doit d'abord être défini sous l'onglet Groupes).

ETAPE 3 *Facultatif* : dans la zone Authentification, effectuez les opérations suivantes si l'utilisateur a besoin d'un mot de passe d'authentification :

a. Sélectionnez un algorithme d'authentification dans la liste **Algorithme d'authentification**.

b. Entrez un mot de passe dans le champ **Mot de passe**. L'utilisateur devra l'introduire pour s'identifier.

c. Introduisez à nouveau le mot de passe dans le champ **Confirmer le mot de passe**.

ETAPE 4 Cliquez sur **OK**. Lorsque vous revenez à la fenêtre SNMP, l'onglet Utilisateurs affiche une nouvelle entrée.

Modifier l'utilisateur SNMP

Cette fenêtre s'affiche lorsque vous sélectionnez un utilisateur et cliquez sur Modifier sous l'onglet Utilisateurs dans la fenêtre SNMP.

Voici les attributs de l'utilisateur que vous pouvez modifier :

- Le groupe auquel l'utilisateur appartient, en sélectionnant un nom de groupe différent.
- L'algorithme d'authentification le cas échéant.
- Le mot de passe d'authentification et le mot de passe de confirmation le cas échéant.

Pour de plus amples informations sur ces options d'affichage, reportez-vous à la rubrique **Créer un utilisateur SNMP**.

Lorsque vous avez terminé, cliquez sur **OK**.

4

Paramètres des ports et du commutateur

Cette partie traite de la configuration des ports et des commutateurs. Elle comprend les rubriques suivantes :

Paramètres des ports du commutateur

Pour modifier les paramètres des ports du commutateur, procédez comme suit :

- Sélectionnez **Configurer** > **Ports** > **Paramètres des ports du commutateur** dans la barre de fonctions.
- Cliquez sur l'icône Ports du commutateur dans la barre d'outils.

Vue d'ensemble

Par défaut, tous les ports sont activés sur le commutateur. Les paramètres présentent les valeurs initiales. La Fenêtre Paramètres des ports affiche ces valeurs et vous permet de les modifier.

Certains types de ports négocient automatiquement les paramètres de configuration. Une erreur de négociation automatique peut se présenter dans les cas suivants :

- Lorsqu'un paramètre duplex manuel diffère de celui qui a été défini sur le port lié
- Lorsqu'un port est défini pour une négociation automatique et si le port relié est paramétré en full duplex sans négociation automatique

Une incohérence au niveau des ports Fast Ethernet provoque de moins bons résultats ou des erreurs de liaison. Sur les ports Gigabit Ethernet, la connexion n'a pas lieu et aucune statistique ne s'affiche.

Pour corriger les paramètres de ports non concordants, suivez l'une des propositions ci-dessous :

- Laissez les ports négocier automatiquement la vitesse et le duplex.
- Définissez manuellement les paramètres de vitesse et duplex pour les ports à chaque extrémité de la liaison.

Pour relier un périphérique Fast Ethernet distant qui ne prend pas en charge la négociation automatique, vous devrez paramétrer manuellement le duplex sur le périphérique local sur une valeur autre qu'**Auto**. La négociation de la vitesse peut se produire même si l'autre périphérique ne prend pas en charge la négociation automatique.

Pour relier un périphérique Gigabit Ethernet distant qui ne prend pas en charge la négociation automatique, désactivez la négociation automatique sur le périphérique local et faites en sorte que les paramètres duplex et de contrôle de flux soient compatibles avec le périphérique distant.

Procédures

Commencez par sélectionner un périphérique dans la liste **Nom de l'hôte**. Les informations sur les ports des périphériques sont disponibles à partir des onglets suivants :

- **Paramètres de configuration, page 157**affiche les valeurs que vous pouvez définir et modifier.
- **État d'exécution, page 160**affiche l'état actuel des ports.

Afin d'afficher un sous-ensemble des informations sur ces onglets, cliquez sur **Filtre** et utilisez la fenêtre Éditeur de filtre. Voir la rubrique **Filtre, page 162**.

Paramètres de configuration

Ce tableau explique les données de l'onglet.

Paramètres	Explication
Description	Description textuelle du port. Cliquez sur **Décrire** dans la fenêtre Paramètres des ports pour décrire plusieurs ports. Vous ne pouvez pas utiliser les caractères ? et /. Si vous avez sélectionné plusieurs ports, ce champ n'est pas disponible.
État	Permet d'activer ou de désactiver le port. La configuration peut différer de celle du moteur d'exécution. Par exemple, si aucun périphérique n'est relié au port, il peut être activé et présenter l'état d'exécution PANNE. Si vous modifiez d'autres paramètres sur un port désactivé, ils n'entrent en ligne de compte qu'une fois le port activé. Lorsque vous désactivez un port, une *interruption de liaison* est envoyée à la console de gestion si vous avez configuré un gestionnaire SNMP.
Duplex	Paramètres pour le duplex : full duplex, half duplex ou auto. Le mode auto est configuré par défaut sur les ports Gigabit Ethernet et GigaStack GBIC. Ces ports s'adaptent automatiquement aux particularités duplex du périphérique relié. Pour paramétrer le duplex sur une valeur qui n'est pas automatique, la vitesse doit également être définie. La valeur duplex doit être automatique si la vitesse du port est définie sur automatique et si le port fonctionne à une vitesse de 1000 Mbits/s. Les connexions de stack GigaStack GBIC fonctionnent en mode half duplex. Les connexions de stack GigaStack GBIC point-à-point fonctionnent en mode full duplex.

Paramètres	Explication
Vitesse	Paramètres pour les ports 10/100 Mbits/s et 10/100/1000 Mbits/s : ▪ *10* (les ports fonctionnent à une vitesse forcée de 10 Mbits/s) ▪ *100* (les ports fonctionnent à une vitesse forcée de 100 Mbits/s) ▪ *1000* (les ports fonctionnent à une vitesse forcée de 1000 Mbits/s) ▪ *auto* (les ports négocient et publient les vitesses disponibles.) ▪ *auto 10* (les ports négocient et publient une vitesse de 10 Mbits/s à l'autre extrémité de la liaison.) Non disponible sur les commutateurs ESW 500 . ▪ *auto 100* (les ports négocient et publient une vitesse de 100 Mbits/s à l'autre extrémité de la liaison.) Non disponible sur les commutateurs ESW 500 ▪ *auto 100 1000* (les ports négocient et publient des vitesses de 100 et 1000 Mbits/s à l'autre extrémité de la liaison.) ▪ *auto 10 1000* (les ports négocient et publient des vitesses de 10 et 1000 Mbits/s à l'autre extrémité de la liaison.) ▪ *auto 1000* (les ports négocient et publient une vitesse de 1000 Mbits/s à l'autre extrémité de la liaison.) ▪ *auto 10 100* (les ports négocient et publient des vitesses de 10 et 100 Mbits/s à l'autre extrémité de la liaison.) ▪ *auto 10 100 1000* (les ports négocient et publient une vitesse de 10, 100 et 1000 Mbits/s à l'autre extrémité de la liaison.) Les paramètres par défaut pour les ports 10/100 et 10/100/1000 Mbits/s sont automatiques. Les ports Ethernet s'adaptent automatiquement à la vitesse de transmission du périphérique relié. **REMARQUE** Vous ne pouvez pas modifier les vitesses de ces ports : ▪ 1000BASE-T, SX, LX/LH, ZX, DWDM et CWDM GBIC ▪ 1000BASE-SX, LX/LH, ZX et SFP CWDM ▪ XENPAK-10GB-LR, ER, CX4, SR et LX4

Paramètres	Explication
Alimentation	Ce paramètre concerne un port unique des commutateurs Catalyst Express 500 PoE ou ESW500. Sélectionnez **auto** si vous souhaitez que le port recherche un système d'alimentation et l'alimente. Sinon, sélectionnez **jamais**.
Auto MDIX	Commutateurs ESW500 uniquement. Affiche l'état de l'interface Media Dependent Interface (MDI)/ Media Dependent Interface avec Crossover (MDIX) sur le port du commutateur ESW 500. Les concentrateurs et les commutateurs sont délibérément câblés à l'inverse des stations terminales afin que lorsqu'un concentrateur ou un commutateur est relié à une station terminale, un câble Ethernet puisse être utilisé et les paires correctement associées. Lorsque deux concentrateurs ou commutateurs sont reliés ou lorsque deux stations terminales sont reliées, un câble simulateur de modem est utilisé afin que les paires soient correctement branchées. Faites un choix parmi les options suivantes : ▪ **Auto**. Utilisez cette option pour détecter automatiquement le type de câble. Il s'agit de la valeur par défaut. ▪ **MDIX**. Utilisez cette option pour les concentrateurs et les commutateurs. ▪ **MDI**. Utilisez cette option pour les stations terminales.

Pour modifier les paramètres de chaque port individuellement, cliquez sur la cellule du port que vous souhaitez modifier.

Pour modifier les paramètres d'un ou plusieurs ports, procédez comme suit :

ETAPE 1 Sélectionnez les ports dans la colonne Interface. Sélectionnez les éléments en maintenant la touche **Ctrl**.Vous pouvez aussi maintenir **MAJ** enfoncé et sélectionner la première et la dernière valeur de la plage qui vous intéresse.

ETAPE 2 Cliquez sur **Modifier** pour afficher la fenêtre Modifier paramètres des ports. Voir la rubrique **Modifier paramètres des ports, page 161**.

ETAPE 3 Complétez les champs de la fenêtre Modifier paramètres des ports.

ETAPE 4 Cliquez sur **OK** pour fermer la fenêtre et revenir à la fenêtre Paramètres des ports.

État d'exécution

Ce tableau explique les informations en lecture seule de l'onglet.

Colonne	Explication
Interface	Identifie le port : Fast Ethernet, Gigabit Ethernet, FDDI, le module ou le numéro de l'emplacement (0, 1, 2) et le numéro de port.
Description	Description de l'interface.
Lien Ethernet	État du port. Le port peut être actif, en panne ou en panne administrativement.
Duplex	État duplex du port (hybride, half, full). Affiche le mode duplex du port. Pour les commutateurs ESW 500, la valeur Full indique que l'interface prend en charge la transmission entre le périphérique et le client dans les deux sens simultanément. La valeur Half indique que l'interface prend en charge la transmission entre le périphérique et le client dans un sens à la fois.
Vitesse	Vitesse du port. Pour les ports Gigabit Ethernet, ce champ est en lecture seule et affiche *1000* (1000 Mbits/s).
État	Indique si l'alimentation est assurée pour le périphérique connecté.
Budget	Alimentation prévue pour le périphérique connecté.
Périphérique	Présente le type de périphérique obtenant l'alimentation électrique par le câble Ethernet de l'interface.
Classe	Classe IEEE du périphérique alimenté. La plupart des périphériques alimentés n'ont pas besoin de la totalité de la puissance du PoE (15,4 W). La valeur peut être comprise entre 0 et 4. 0 est la valeur par défaut. L'alimentation prévue pour le commutateur dépend de la classe IEEE.

Modifier paramètres des ports

La fenêtre Modifier paramètres des ports s'affiche lorsque vous sélectionnez plusieurs ports dans la fenêtre Paramètres des ports du commutateur.

Entrez ou sélectionnez les valeurs correspondant aux ports à modifier. Voir **Paramètres de configuration, page 157** pour obtenir une description des valeurs à introduire.

Si vous sélectionnez plusieurs ports et définissez des paramètres non valables pour le port sélectionné, le paramétrage en cours reste inchangé. Par exemple, si vous sélectionnez un port 10BaseT Ethernet, Fast Ethernet et Gigabit et ensuite une vitesse de 100 Mbits/s, le port Ethernet 10BaseT restera sur 10 Mbits/s alors que le port Gigabit restera quant à lui sur 1000 Mbits/s.

Cliquez sur **OK** pour fermer la fenêtre. Les modifications s'affichent dans la fenêtre Paramètres des ports.

Pour de plus amples informations, consultez les rubriques suivantes :

- **Paramètres de configuration, page 157**
- **État d'exécution, page 160**

Modifier les descriptions des ports

Pour ajouter ou modifier les descriptions de ports :

Sélectionnez un ou plusieurs ports. Si vous sélectionnez un port, cliquez dans la cellule de la colonne **Description** correspondant au port souhaité. Entrez le texte au niveau du curseur.

Si vous sélectionnez plusieurs ports :

ETAPE 1 Cliquez sur **Décrire** pour afficher la fenêtre Description simple du port.

ETAPE 2 Introduisez les paramètres dans la fenêtre. De la fenêtre Description simple du port, vous pouvez accéder à la fenêtre Description avancée du port qui vous permet de définir l'incrément automatique pour un maximum de 3 descripteurs.

ETAPE 3 Cliquez sur **OK** pour fermer la fenêtre.

Filtre

La fenêtre Filtre s'affiche lorsque vous cliquez sur **Filtre** dans une fenêtre de Configuration Assistant ou dans un assistant contenant le tableau. Les noms de colonne du tableau deviennent les noms de champ de cette fenêtre. Entrez les critères de sélection dans les champs afin de filtrer les lignes du tableau et ne laisser que celles qui vous intéressent.

Suivez les étapes ci-dessous :

ETAPE 1 Laissez le champ vide si vous ne souhaitez pas filtrer la colonne correspondante du tableau (donc, si vous ne souhaitez aucun critère de sélection pour cette colonne).

ETAPE 2 Pour utiliser un champ avec une liste déroulante, sélectionnez l'élément que Configuration Assistant devra rechercher dans la colonne correspondante.

ETAPE 3 Pour utiliser un champ de texte, entrez les caractères que Configuration Assistant devra rechercher dans la colonne correspondante. Utilisez un astérisque (*) pour représenter une chaîne de caractères d'une longueur indéterminée. Utilisez un point d'interrogation (?) pour représenter un seul caractère. Pour rechercher une chaîne entourée d'un nombre indéterminé de caractères, entrez **chaîne*.

Exemples

- Pour n'afficher que les interfaces activées pour la mise à jour dans la fenêtre Mise à jour du logiciel LRE, sélectionnez **activer** dans le champ **Mise à jour** de la fenêtre Éditeur de filtre de la boîte de dialogue Mise à jour du logiciel LRE.
- Pour n'afficher que les descriptions contenant la chaîne 1234 dans la fenêtre Paramètres des ports, entrez ***1234*** dans le champ **Description** de la fenêtre Éditeur de filtre pour la boîte de dialogue Paramètres des ports.

ETAPE 4 Cliquez sur **OK**. Vous revenez ensuite à la fenêtre précédente de Configuration Assistant ou de l'assistant où sont affichées les informations demandées.

Smartports

Pour configurer les connexions de port, vous devez appliquer des profils aux ports. Pour afficher la fenêtre Smartports et accéder aux paramètres, procédez comme suit :

- Sélectionnez **Configurer** > **Commutation** > **Smartports** dans la barre de fonctions.
- Cliquez sur l'icône Smartports dans la barre d'outils.
- Cliquez sur **Résoudre** dans la fenêtre Notification d'événements afin de résoudre un événement Smartports.

Vue d'ensemble

Les Smartports vous permettent de configurer les paramètres de sécurité essentiels, ainsi que les critères de disponibilité et de contrôle des connexions de vos ports réseau.

La fenêtre Smartports permet d'afficher le volet frontal des périphériques. Vous pouvez ainsi sélectionner les ports et y appliquer des profils. Vous pouvez configurer la liaison aux périphériques suivants :

Périphérique	Commentaire
Desktop	Hôte interne disposant d'un accès à Internet et aux sous-réseaux d'une entreprise.
Téléphone IP	Hôte de bout de ligne tel qu'un PC mis en cascade vers un téléphone IP.
Switch	Connexion entre commutateurs.
Router	Routeur d'accès ou plateforme UC 500.
Access point	Un point d'accès peut se connecter à des terminaux mobiles. Selon la configuration du point d'accès, les terminaux mobiles peuvent être des invités ou des hôtes Desktop.

Procédures

La fenêtre présente une image du volet frontal des périphériques de votre réseau. Si un port est connecté à un périphérique et si un profil y a été appliqué, l'icône du périphérique connecté au port s'affiche. Lorsque vous placez le curseur sur l'icône, Configuration Assistant identifie le type de périphérique connecté.

Pour appliquer des profils à d'autres ports connectés ou pour corriger un profil appliqué par erreur (indiqué par l'icône de conflit), procédez comme suit :

- Cliquez sur **Suggérer**. Les icônes des périphériques connectés clignotent au niveau des ports. La fenêtre Smartports suggérés s'affiche. Elle propose

les profils à appliquer aux ports. Voir la rubrique **Smartports suggérés, page 166**.

- Sélectionnez un port et cliquez sur **Modifier**. La fenêtre Modifier les profils de port s'affiche. Vous pouvez aussi utiliser cette fenêtre pour supprimer les profils Smartports ou pour appliquer des profils Smartports à des ports non reliés à des périphériques. Voir la rubrique **Modifier les profils de port, page 164**.

Remarques :

- Pour sélectionner plusieurs ports, maintenez la touche **Ctrl** et cliquez sur les ports souhaités. Vous pouvez aussi *sélectionner les ports en série* en maintenant le bouton de la souris et en dessinant un rectangle autour d'un groupe de ports. Maintenez la touche **Ctrl** pour sélectionner plusieurs séries distinctes.
- Si vous utilisez CCA pour définir un profil, le programme remplace les profils précédemment définis.

Lorsque vous revenez à la fenêtre Smartports, les icônes des périphériques s'affichent sur les ports pour lesquels les profils ont été sélectionnés. Si vous avez demandé à CCA de supprimer les profils, les icônes précédemment affichées disparaissent.

Pour visualiser les détails des ports configurés, cliquez sur **Détails** pour ouvrir la fenêtre Détails des profils du port. Voir la rubrique **Smartports suggérés, page 166**.

Pour de plus amples informations, consultez les rubriques suivantes :

- **Modifier les profils de port, page 164**
- **Détails des profils du port, page 166**
- **Smartports suggérés, page 166**

Modifier les profils de port

Cette fenêtre s'affiche lorsque vous sélectionnez un ou plusieurs ports sous l'onglet Configuration de port de la fenêtre Smartports et cliquez ensuite sur **Modifier**. Si vous avez sélectionné un port, le champ **Interface** présente le numéro de port. Si vous avez sélectionné plusieurs ports, le champ **Interface** indique **Multiple**.

Pour appliquer un profil aux ports sélectionnés, procédez comme suit :

Dans la liste **Profil**, sélectionnez le profil correspondant au périphérique que vous souhaitez connecter.

Périphérique	Commentaire
Desktop	Hôte interne disposant d'un accès à Internet et aux sous-réseaux d'une entreprise.
IP Phone+Desktop	Hôte de bout de ligne tel qu'un PC mis en cascade vers un téléphone IP.
Switch	Connexion entre commutateurs.
Router	Routeur d'accès ou plateforme UC500.
Access point	Un point d'accès peut se connecter à des terminaux mobiles. Selon la configuration du point d'accès, les terminaux mobiles peuvent être des invités ou des hôtes Desktop.

Si vous avez sélectionné un port Ethernet 10 Gigabits, seules les valeurs **Switch** et **Router** sont disponibles.

Remplissez la rubique **Attributs** en fonction du profil sélectionné.

Si vous avez sélectionné...	Suivez les étapes ci-dessous...
Desktop	Entrez le numéro d'un VLAN dans le champ **VLAN d'accès**. Il s'agit du VLAN qui assurera l'envoi des données entre le port et l'ordinateur de bureau.
IP Phone+Desktop	▪ Dans le champ **VLAN d'accès**, sélectionnez le VLAN pour les données (généralement VLAN1). Il s'agit du VLAN qui assurera l'envoi des données au départ et à destination du port. ▪ Dans le champ **VLAN voix**, sélectionnez le VLAN pour la voix (généralement cisco-voice). Il s'agit du VLAN qui assurera l'envoi et la réception des paquets vocaux du port.

Router ou Access Point	Entrez le numéro d'un VLAN natif dans le champ **VLAN natif**. Le port sera configuré comme un port trunk et le VLAN natif générera un trafic non balisé.
Switch	Entrez le numéro d'un VLAN natif dans le champ **VLAN natif**. Le port sera configuré comme un port trunk et le VLAN natif générera un trafic non balisé. Cochez la case **Autoriser uniquement les VLAN internes** pour autoriser tout le trafic en provenance de tous les VLAN à l'exception des VLAN de type Invité et DMZ. Si la case n'est pas cochée, le trafic sera autorisé pour tous les VLAN. Si aucun VLAN de type DMZ ou Invité n'est configuré, la case est grisée. Vous devez configurer un VLAN de type Invité ou DMZ pour activer cette case.

Pour supprimer un profil des ports sélectionnés, choisissez **aucun** dans la liste **Profil**. Les valeurs par défaut du port sont rétablies.

Lorsque vous avez terminé, cliquez sur **OK**. Vous revenez à la fenêtre Smartports.

Détails des profils du port

Cette fenêtre s'affiche lorsque vous cliquez sur **Détails** sous l'onglet Configuration de port de la fenêtre Smartports.

Si vous avez sélectionné des ports avant de cliquer sur **Détails**, vous pouvez développer les en-têtes des périphériques présentant les ports que vous avez sélectionnés. Si aucun port n'est sélectionné, les en-têtes s'affichent pour tous les périphériques de la fenêtre Smartports.

Les en-têtes du périphérique permettent d'accéder aux en-têtes complètes des ports qui donnent accès aux détails du profil. Si un profil est affecté à un port, le type de profil et les informations de configuration y afférant sont affichés. Si aucun profil n'est appliqué, la mention Aucun s'affiche.

Lorsque vous avez terminé, cliquez sur **OK**.

Smartports suggérés

Cette fenêtre s'affiche lorsque vous effectuez l'une des opérations suivantes :

- Clic sur **Suggérer** dans la fenêtre Smartports.

- Clic sur **Résoudre** dans la fenêtre Notification d'événements afin d'appliquer un profil Smartports.

Utilisez cette fenêtre pour les opérations suivantes :

- Configurer les VLAN en fonction des profils suggérés pour les téléphones IP, les commutateurs, les routeurs ou les points d'accès.
- Corriger les profils appliqués par erreur.

Pour attribuer un profil à un port, procédez comme suit :

ETAPE 1 Acceptez le profil dans la colonne Profil proposé.

Remarques **:**

- Configuration Assistant considère parfois le type de périphérique connecté comme un commutateur alors qu'il s'agit en fait d'un routeur ou vice-versa. Modifiez le profil du port si le type de profil proposé est incorrect.
- Si le périphérique connecté est un point d'accès, vous pouvez accepter le profil **Point d'accès** proposé ou modifier le profil du port.
- Configuration Assistant ne peut pas détecter les commutateurs ou les analyseurs de réseau connectés à un commutateur Cisco Express 500. Le cas échéant, aucun rôle ne sera suggéré pour ces liaisons.

ETAPE 2 Sélectionnez un VLAN (deux VLAN pour les téléphones IP). Ce tableau indique les VLAN correspondant à chaque type de périphérique.

Pour relier à	Vous devez sélectionner
Un téléphone IP et un ordinateur de bureau	Un VLAN d'accès et un VLAN vocal
Desktop	Un VLAN d'accès
Un commutateur	Le VLAN natif
Un routeur	Le VLAN natif
Un point d'accès	Le VLAN natif

Dans la liste des VLAN, sélectionnez le VLAN correspondant aux liaisons que vous configurez. Si le VLAN nécessaire ne figure pas dans la liste, il n'existe pas. Fermez cette fenêtre et le Gestionnaire Smartports, utilisez la fenêtre VLAN pour créer le VLAN et utilisez ensuite la fonction Smartports.

ETAPE 3 Lorsque vous avez terminé, cliquez sur **OK**.

ETAPE 4 Dans la fenêtre Smartports, cliquez sur **OK** pour appliquer les profils en fonction des VLAN configurés.

VLANs

Cette fenêtre s'affiche lorsque vous sélectionnez **Configurer** > **Commutation** > **VLANs** dans la barre de fonctions.

Lorsque vous sélectionnez un périphérique dans la liste **Nom d'hôte**, les données suivantes s'affichent pour chaque VLAN :

- Identifiant de VLAN
- Nom du VLAN
- Adresse IP, sous-réseau et masque de sous-réseau
- VLAN voix par défaut (indiqué par une flèche verte)

Si des périphériques synchronisés par le VLAN tels que des commutateurs UC500, ESW500 ou Catalyst Express CE520 font partie d'un site client, le sélecteur de périphériques **Nom d'hôte** affiche la valeur **Tous les UC5xx/CE/ESW**.

Consultez les rubriques suivantes pour plus d'informations sur les VLAN et les paramètres des VLAN :

- **Vue d'ensemble**
- **Remarques**
- **Procédures**

Vue d'ensemble

Vous pouvez créer des VLAN à partir des périphériques suivants :

- Tous les périphériques UC500
- Tous les périphériques SR500
- Tous les périphériques C8xx

Un VLAN (réseau local virtuel) est un réseau commuté segmenté par fonction logique, équipe de projet ou application quels que soient les emplacements physiques des utilisateurs. Les VLAN présentent les mêmes attributs que les LAN physiques.Vous pouvez cependant grouper les postes finaux même s'ils ne se trouvent pas dans le même segment du réseau local. N'importe quel port de commutateur peut faire partie d'un VLAN. Les paquets unicast, broadcast et multicast sont transférés et envoyés aux postes du VLAN uniquement.

Les VLAN définissent les domaines broadcast dans un réseau de Couche 2. Un domaine broadcast est composé de tous les périphériques qui recevront des trames broadcast provenant de n'importe quel périphérique de l'ensemble. Les domaines broadcast sont généralement liés par des routeurs parce que les routeurs ne transmettent pas de trames broadcast. Les commutateurs de Couche 2 créent des domaines broadcast basés sur la configuration du commutateur. Les commutateurs sont des ponts dotés de ports multiples qui vous permettent de créer des domaines broadcast multiples. Chaque domaine broadcast se présente comme un pont virtuel distinct au sein d'un commutateur.

Vous pouvez définir un ou plusieurs ponts virtuels au sein d'un commutateur. Chaque pont virtuel que vous créez dans le commutateur définit un nouveau domaine broadcast (VLAN). Le trafic ne peut pas passer directement vers un autre VLAN (entre des domaines broadcast) au sein du commutateur ou entre deux commutateurs. Pour relier deux VLAN différents, vous devez utiliser des routeurs ou des commutateurs de Couche 3.

Les commutateurs sont configurés par défaut avec un VLAN simple, dit "VLAN 1". Si vous souhaitez créer d'autres VLAN, utilisez la fenêtre VLAN. Vous pouvez également utiliser cette fenêtre pour modifier le nom d'un VLAN ou pour le supprimer.

Lorsque vous créez, modifiez ou supprimez un VLAN sur un commutateur ou une plateforme Unified Communications 500, votre action est automatiquement dupliquée sur tous les autres périphériques de ce type composant votre réseau. La duplication permet de préserver la configuration régulière des périphériques. Si vous ajoutez un périphérique à un site disposant déjà d'un VLAN associé, un conflit de VLAN se présentera entre les périphériques qui n'y sont pas associés. Dans ce cas, vous pouvez utiliser la fenêtre Synchronisation VLAN afin de rétablir la cohérence du VLAN. Voir la rubrique **Synchronisation VLAN, page 172**.

Remarques

Les restrictions suivantes s'appliquent à la création et à la configuration des VLAN :

- Au maximum, 15 VLAN peuvent être associés à un périphérique. Par défaut, tous les périphériques sont associés à VLAN 1.
- Seuls le nom et l'identifiant du VLAN sont synchronisés avec les commutateurs ESW500 et CE520.
- Dans un déploiement multi-sites, les VLAN peuvent uniquement être configurés sur l'UC500 local. Les modifications du VLAN apportées au niveau de l'UC500 local ne sont pas appliquées aux autres UC500 dans un déploiement multi-sites. Seuls les périphériques locaux sont synchronisés.

Procédures

Pour créer un VLAN, sélectionnez un **nom d'hôte** et cliquez sur **Créer**. Puis, complétez les champs dans la fenêtre Créer un VLAN. Voir la rubrique **Créer un VLAN, page 171**.

Pour modifier le nom, l'adresse IP, le sous-réseau et le masque de sous-réseau d'un VLAN, sélectionnez le VLAN dans cette fenêtre et cliquez sur **Modifier**. Voir la rubrique **Synchronisation VLAN, page 172**. Le VLAN 1 est réservé par CCA. Vous ne pouvez donc pas en modifier le nom ou l'identifiant.

Pour supprimer un VLAN, sélectionnez-le et cliquez sur **Supprimer**.

Lorsque vous avez terminé, cliquez sur **OK** ou sur **Appliquer**.

Pour de plus amples informations, consultez les rubriques suivantes :

- **Créer un VLAN, page 171**
- **Synchronisation VLAN, page 172**

Créer un VLAN

Cette fenêtre s'affiche lorsque vous cliquez sur **Créer** dans la fenêtre VLAN (**Configurer** > **Commutation** > **VLANs**).

Pour créer un VLAN, remplissez les champs de la fenêtre Créer un VLAN selon les indications ci-dessous, puis cliquez sur **OK**.

Une fois le VLAN créé, sélectionnez les options **Configurer** > **Routage** > **Serveur DHCP** pour créer une réserve DHCP, des plages d'exclusion DHCP et des liaisons DHCP selon vos besoins.

Paramètre	Description
Identifiant de VLAN	Entrez l'identifiant du VLAN. Utilisez un identifiant compris entre 2 et 1000. N'entrez pas le chiffre 1 car cet identifiant est réservé pour le VLAN de données par défaut.
Nom du VLAN	Le nom par défaut est VLANxxxx où xxxx représente quatre chiffres (y compris les zéros à gauche) équivalant à l'identifiant du VLAN. Vous pouvez utiliser cette valeur ou introduire un nom composé de 1 à 32 caractères. Le nom du VLAN doit être unique. Le VLAN voix par défaut doit être désigné par le nom "Cisco-Voice". Le nom de VLAN "Cisco-Voice" est réservé par CCA.
Choisir comme VLAN voix par défaut	Lorsque cette option est cochée, le VLAN est utilisé comme VLAN par défaut. Le VLAN voix par défaut est le VLAN100.
Adresse IP	Entrez l'adresse IP du VLAN. Si l'adresse IP du VLAN données ou voix par défaut est modifiée, le pare-feu, le NAT et les réserves DHCP le sont eux aussi. L'adresse IP ne peut pas être un doublon ni chevaucher une autre adresse IP existante.
Sous-réseau	Entrez le sous-réseau du VLAN.
Masque de sous-réseau	Entrez le masque de sous-réseau pour ce VLAN ou sélectionnez-en un dans la liste déroulante.

Synchronisation VLAN

Les périphériques de votre communauté doivent disposer des mêmes VLAN. Si ce n'est pas le cas, CCA affiche une icône d'événement sur la barre d'état et enregistre le conflit dans la fenêtre Notification d'événements. Si vous validez l'événement dans cette fenêtre et cliquez sur **Résoudre**, la fenêtre Synchronisation VLAN s'affiche. Vous résolvez les conflits VLAN dans cette fenêtre.

Ce tableau explique les colonnes de cette fenêtre.

Colonne	Explication
Identifiant de VLAN	Identifiants des VLAN en conflit.
Conflit	Description du conflit : ▪ N'existe pas Le VLAN n'est pas configuré sur tous les périphériques. ▪ Existe avec différents noms : Les identifiants de VLAN existent sur tous les périphériques mais les noms de VLAN ne correspondent pas.
Opération de résolution	Liste déroulante où figurent les opérations permettant de résoudre le conflit. Vous choisissez l'action qui correspond le mieux à vos besoins.

Lorsque vous avez choisi les actions pour les conflits de VLAN, cliquez sur **Résoudre**. Vos actions sont reproduites dans la fenêtre VLAN.

Vous ne pouvez pas cliquer sur **Résoudre** avant d'avoir choisi une action pour chaque conflit de VLAN.

Cliquez sur **Appliquer** dans la fenêtre VLAN pour sauvegarder les actions et y réaliser d'autres opérations, ou cliquez sur **OK** pour les sauvegarder et fermer la fenêtre.

Mise en miroir du port (commutateurs de la série ESW 500)

Pour configurer la mise en miroir de ports sur les commutateurs de la série Cisco ESW500, sélectionnez l'option **Configurer** > **Ports** > **Mise en miroir du port** dans la barre de fonctions.

Vue d'ensemble

La Mise en miroir du port permet de surveiller et de mettre en miroir le trafic réseau en envoyant des copies des paquets entrants et sortants d'un port à un port de contrôle. La Mise en miroir du port fait office d'outil diagnostic et/ou de débogage. Elle permet également d'assurer le suivi des performances du commutateur.

Les administrateurs réseau configurent la Mise en miroir du port en sélectionnant un port cible vers lequel seront copiés tous les paquets et jusqu'à 8 ports d'origine à partir desquels les paquets seront copiés.

Consignes importantes

- Avant de configurer la symétrie des ports sur les commutateurs de la série ESW 500, le profil Smartport du port cible doit être défini sur **Autre**.
- N'utilisez pas les ports de commutateur ou les ports de liaison ascendante pour la mise en miroir.
- Vous ne pouvez pas utiliser le même port comme port cible et port source.
- Les ports source et cible doivent se trouver sur le même commutateur.

Procédures

Pour configurer la Mise en miroir du port, effectuez la configuration selon les modalités ci-dessous et cliquez sur OK.

Paramètre	Description
Port de destination	Représente le port vers lequel le trafic source est mis en miroir.
Port source	Définit le port à partir duquel le trafic doit être analysé. Un maximum de 8 ports sources peuvent être sélectionnés.
Type	Désigne la configuration du port pour la mise en miroir. Les valeurs possibles sont les suivantes : ▪ **Réception uniquement**. Définit la symétrie des ports pour la réception de trafic uniquement sur le port sélectionné. ▪ **Transmission uniquement**. Définit la mise en miroir des ports de transmission. Il s'agit de la valeur par défaut. ▪ **Transmission et réception**. Définit la symétrie des ports pour les ports de réception et de transmission.

Protocole STP (commutateurs CE520)

Pour configurer le protocole STP pour les commutateurs CE520, sélectionnez l'option **Configurer** > **Commutation** > **STP**.

Vue d'ensemble

Le STP (Spanning Tree Protocol) est une technique standard de maintenance d'un réseau composé de plusieurs ponts ou commutateurs. Lorsque la topologie du réseau change, le STP empêche la création de boucles en plaçant des ports dans un état de transmission ou de blocage et reconfigure de manière transparente les ponts et les commutateurs. Chaque VLAN est traité comme un réseau séparé et une application séparée du STP est appliquée à chacun d'eux.

Le commutateur prend en charge le protocole PVST+ (per-VLAN spanning-tree) basé sur la norme IEEE 802.1D et les extensions Cisco brevetées.

Les paramètres STP sont déterminés pour chaque VLAN. Pour chaque application Spanning-Tree, vous pouvez configurer un ensemble d'options globales et un ensemble de paramètres de port. Le commutateur prend en charge jusqu'à 32 applications Spanning-Tree.

Vous pouvez configurer le STP comme suit :

- Modifier l'état STP pour le **désactiver** (ou l'**activer**) sur un ou plusieurs VLAN.
- Modifier les paramètres Spanning-Tree pour le commutateur racine.

Procédures

Cette fenêtre présente les onglets suivants :

- **État STP**permet de désactiver ou d'activer le protocole STP (Spanning Tree Protocol) sur un ou plusieurs VLAN
- **Racines actuelles**permet d'afficher les paramètres racines Spanning-Tree actuels

Commencez par sélectionner un commutateur dans la liste **Nom de l'hôte**. Les informations contenues dans les onglets s'appliquent au commutateur sélectionné.

Afin d'afficher un sous-ensemble des informations sur le port, cliquez sur **Filtre** et utilisez la fenêtre Éditeur de filtre (voir **Filtre, page 162**). Cliquez sur **Actualiser** pour sonder le périphérique et obtenir des données à jour.

Lorsque vous avez terminé la configuration STP, cliquez sur **OK**.

État STP

Cet onglet montre si le STP est activé pour chaque VLAN sur le commutateur. Le STP est activé par défaut. Cependant, en désactivant le STP, vous pouvez éviter un retard de 30 secondes lors du transfert de paquets à partir d'un port lors de la reconfiguration d'un commutateur.

Ce commutateur prend uniquement en charge le protocole PVST+ (per-VLAN spanning-tree plus) représenté par **pvst** dans la liste **Mode Spanning-Tree**.

IMPORTANT Désactivez uniquement le STP si vous êtes certain qu'il n'y a pas de boucle dans la topologie de votre réseau. Si le STP est désactivé et si des boucles sont présentes dans la topologie, les performances du réseau sont dégradées par un trafic excessif et une duplication indéfinie du paquet.

Pour activer ou désactiver le STP :

ETAPE 1 Dans la colonne **Identifiant de VLAN**, sélectionnez un ou plusieurs VLAN sur lesquels vous souhaitez activer ou désactiver le STP.

ETAPE 2 Dans la colonne **État Spanning-Tree**, sélectionnez **activer** dans la liste déroulante pour activer le STP pour chaque VLAN que vous avez sélectionné.

Sélectionnez **désactiver** pour désactiver le STP pour chaque VLAN que vous avez sélectionné.

Racines actuelles

Pour chaque VLAN, l'onglet **Racine actuelle** (onglet en lecture seule) affiche les paramètres STP sur le commutateur racine actuel. Ces paramètres, qui peuvent être définis sur un autre commutateur, établissent la configuration qui entre en vigueur lorsque le commutateur fonctionne en tant que racine VLAN.

Ces réglages sont définis dans le tableau ci-dessous.

Champ	Description
Identifiant de VLAN	Identifiant de VLAN auquel ces paramètres s'appliquent lorsque le commutateur agit en tant que racine.
Adresse MAC	Adresse MAC du commutateur racine.

Champ	Description
Priorité	Identifie le pont racine. Le commutateur avec la valeur la plus faible a la priorité et est sélectionné comme étant la racine. 32768 est la valeur par défaut.
Âge max	Détermine le nombre de secondes pendant lesquelles le commutateur attend sans recevoir de messages de configuration STP avant de tenter une reconfiguration. La valeur par défaut pour IEEE est de 20 secondes ; la valeur par défaut pour IBM est de 10 secondes.
Temps Hello	Détermine le nombre de secondes entre les messages de configuration STP. Pour IEEE et IBM, introduisez un nombre allant de 1 à 10. La valeur par défaut est 2 secondes.
Délai avant transmission	Détermine le nombre de secondes d'attente du port avant de passer d'un état d'apprentissage et d'écoute STP à l'état de transfert. Ce délai garantit qu'aucune boucle n'est formée avant que le commutateur transfère un paquet. La valeur par défaut pour IEEE est de 15 secondes ; la valeur par défaut pour IBM est de 4 secondes.
Coût de résolution racine	Mesure relative utilisée pour déterminer le chemin d'accès le plus favorable vers une destination. Voir **Table Coût de résolution, page 178** pour plus d'informations.
Port racine	Port auquel ces paramètres s'appliquent.
Pont racine	Si le commutateur est en fait la racine du STP pour ce VLAN, le champ affiche **Oui**. Autrement, le champ affiche **Non** et le port racine du périphérique figure dans la colonne Port racine. **REMARQUE** Chaque commutateur dans une application Spanning-Tree adopte les paramètres Hello, Délai et Âge max. du pont racine, quelle qu'en soit la configuration.

Table Coût de résolution

Ce tableau explique les paramètres par défaut pour le Coût de résolution pour différentes vitesses.

Coût de résolution	Vitesse
100	10 Mbits/s
19	100 Mbits/s
14	155 Mbits/s
4	1 Gbits/s
2	10 Gbits/s
1	Vitesses supérieures à 10 Gbits/s

IGMP Snooping (commutateurs CE520)

Pour activer et désactiver la fonction IGMP snooping et réaliser les opérations de configuration sur les commutateurs Cisco CE520, sélectionnez **Configurer** > **Commutation** > **IGMP Snooping** dans la barre de fonctions.

Vue d'ensemble

Vos commutateurs peuvent réduire les inondations de paquets IP multicast en limitant la transmission de ces paquets aux groupes de clients qui les demandent. Lorsque les clients (terminaux) adhèrent et quittent automatiquement les groupes qui reçoivent le trafic IP multicast, vos commutateurs peuvent modifier de manière dynamique leur transmission en fonction des requêtes Adhérer (join) et Quitter (leave). Le snooping du protocole IGMP (Internet Group Management Protocol) octroie ce contrôle aux commutateurs.

Procédures

La fenêtre IGM Snooping présente les paramètres suivants :

- Paramètres pour activer IGMP Snooping de manière générale et sur des VLAN isolés
- Groupes multicast pour afficher les groupes multicast
- Port du routeur multicast, pour afficher les ports du routeur multicast

Avant d'effectuer des sélections sous l'onglet Paramètres, sélectionnez un périphérique dans la liste Noms d'hôte. Tous les choix que vous effectuez dans cet onglet s'appliqueront au périphérique sélectionné.

Procédez comme suit pour modifier les paramètres :

ETAPE 1 Activer IGMP Snooping est coché par défaut. Annulez la sélection uniquement si vous souhaitez désactiver l'IGMP snooping sur tout le périphérique.

ETAPE 2 La table affiche les VLAN auxquels appartiennent les ports de commutation ainsi que les paramètres des VLAN. Par défaut, l'IGMP snooping est activé sur les VLAN. Pour modifier une valeur par défaut, cliquez sur **Modifier**, et utilisez la fenêtre Modifier les paramètres IGMP Snooping. Voir la rubrique **Modifier l'IGMP Snooping, page 179**.

ETAPE 3 Lorsque vous revenez à la fenêtre IGMP Snooping, cliquez sur **OK**.

Les informations de l'onglet Groupes multicast et de l'onglet Ports du routeur multicast sont disponibles en lecture seule et ne peuvent pas être modifiées.

Modifier l'IGMP Snooping

Cette fenêtre s'affiche lorsque vous sélectionnez un VLAN et cliquez sur **Modifier** dans la fenêtre IGMP Snooping tout en affichant l'onglet Paramètres. Utilisez cette fenêtre pour activer ou désactiver la fonction IGMP snooping sur le VLAN sélectionné.

Suivez les étapes ci-dessous :

ETAPE 1 Sélectionnez **Activer** ou **Désactiver** dans la liste État.

ETAPE 2 Lorsque vous avez effectué les modifications, cliquez sur **OK** pour fermer la fenêtre et revenir à la fenêtre IGMP Snooping.

Adresses MAC (commutateurs CE520)

Les commutateurs enregistrent l'adresse MAC (Media Access Control) des périphériques reliés dans une table d'adresses MAC. Vous pouvez assurer la gestion des adresses dans cette table en cliquant sur **Configurer** > **Commutation** > **Adresses MAC** dans la barre de fonctions.

Vue d'ensemble

Le périphérique acquiert l'adresse MAC des périphériques connectés, les identifiants VLAN et les numéros d'interface en lisant l'adresse source des paquets entrants. Quand une entrée est supprimée, le périphérique la détecte. Si le périphérique rencontre un paquet pour une destination inconnue, il inonde tous les ports du VLAN avec ce paquet.

Lorsque des stations sont ajoutées ou supprimées du réseau, le commutateur met à jour le tableau des adresses dynamiques en ajoutant de nouvelles entrées et en périmant celles qui ne sont pas utilisées. Le commutateur met aussi à jour le tableau des adresses en supprimant toutes les adresses associées au port sur lequel une modification d'adhésion VLAN a eu lieu.

Un commutateur peut acquérir une adresse dans plusieurs VLAN ; de plus, toute adresse acquise dans un VLAN peut être entrée comme adresse sécurisée dans un autre VLAN. Toute adresse acquise par le commutateur dans un VLAN est inconnue dans un autre VLAN jusqu'à ce que ce dernier acquière l'adresse.

Procédures

Pour afficher ou modifier la table des adresses MAC, suivez les étapes suivantes :

ETAPE 1 Dans la liste Nom de l'hôte, sélectionnez le commutateur dont vous souhaitez afficher les adresses MAC enregistrées.

Les colonnes du tableau ont les significations suivantes :

Colonne	Signification
Adresse MAC	Adresse MAC d'un périphérique attaché.
Identifiant de VLAN	Identifiant de VLAN configuré sur l'interface de sortie.
Interface de sortie	Interface à laquelle les paquets reçus doivent être transmis si l'adresse MAC de l'expéditeur correspond à celle de la colonne Adresse MAC.

ETAPE 2 *Facultatif*. Pour effacer les adresses et réinitialiser le tableau, cliquez sur **Enlever tout**.

ETAPE 3 Cliquez sur **OK** pour fermer la fenêtre.

Fenêtre Recherche de ports (commutateurs CE520)

Pour accéder à la fenêtre Recherche de ports, sélectionnez **Superviser** > **Rechercher** dans la barre de fonctions. Cette option est uniquement disponible en présence d'un commutateur Cisco CE520 sur le site client.

Vue d'ensemble

Vous pouvez rechercher des ports ou des périphériques sur votre réseau. Vous souhaitez peut-être connaître le type, l'état et la vitesse d'un port mais vous ne connaissez pas son numéro ou le périphérique auquel il est relié. Vous pouvez trouver rapidement les informations si vous connaissez la description qui a été saisie pour le port. Vous pouvez également rechercher les périphériques

connectés à un périphérique donné si vous connaissez l'adresse IP ou l'adresse MAC du périphérique en question. Pour rechercher des ports ou des périphériques, cliquez et entrez une valeur, une adresse IP ou MAC dans la fenêtre Rechercher.

Lorsque vous disposez des résultats de recherche du port, utilisez-les pour parcourir la fenêtre Paramètres des ports présentant les informations sur les paramètres de configuration et l'état de fonctionnement. Lorsque vous disposez des résultats de recherche, utilisez-les pour parcourir la fenêtre Topologie qui vous permet de localiser les périphériques connectés.

Procédures

Cette fenêtre vous permet de rechercher les ports disposant d'une description. Vous pouvez également rechercher les périphériques connectés à des périphériques donnés en entrant l'adresse IP ou l'adresse MAC du périphérique en question.

Suivez les étapes ci-dessous :

ETAPE 1 Dans le champ **Rechercher les ports avec description/adresse IP/adresse MAC**, entrez un mot ou une phrase, une adresse MAC ou une adresse IP. Les données introduites sont alors comparées à tous les périphériques de la communauté ou du cluster.

Entrez l'adresse MAC au format xxxx.xxxx.xxxx.xxxx ou xx:xx:xx:xx:xx:xx, où x représente un caractère hexadécimal (0-9, a-f, A-F).

ETAPE 2 Cliquez ensuite sur **Rechercher**.

Si vous entrez une description de port dans le champ Recherche, les ports correspondants s'affichent dans le champ Résultats de la recherche. Ces informations apparaissent dans le tableau suivant :

Colonne	Explication
Ports	Nom du périphérique et numéro de port pour les ports correspondant à la description.
Description	Description du port.

Si vous cliquez sur **Rechercher** alors qu'aucun texte n'a été entré dans le champ de recherche, Configuration Assistant présente une liste de tous les périphériques de la communauté à l'exception des contrôleurs WLAN et de leurs ports.

Si vous avez entré une adresse IP ou une adresse MAC dans le champ **Rechercher**, ces informations s'affichent dans le tableau suivant :

Colonne	Explication
Hôte	Nom du périphérique dont l'adresse IP ou MAC a été introduite dans le champ de recherche.
Adresse MAC	Adresse MAC du périphérique.
Adresse IP	Adresse IP du périphérique.
Description	Type de périphérique.

ETAPE 3 Lorsque vous avez terminé, cliquez sur **OK**.

EtherChannels (commutateurs CE520)

Pour afficher ou configurer des groupes de ports sur les commutateurs de la série Cisco Ce520, sélectionnez l'option **Configurer** > **Ports** > **EtherChannels** dans la barre de fonctions.

Vue d'ensemble

Les groupes de ports Fast EtherChannel et Gigabit EtherChannel assurent une liaison rapide entre commutateurs ou entre les commutateurs et les serveurs. Les groupes de ports assurent aussi une liaison redondante entre les commutateurs. Le commutateur considère le groupe de ports comme un seul port logique.Par conséquent, lorsque vous créez un groupe de ports, le commutateur utilise la configuration du premier port pour tous les autres ports du groupe. Une fois le groupe créé, la modification des paramètres STP ou VLAN d'un port du groupe fait varier les paramètres de tous les ports.

Un port de chaque groupe prend en charge les paquets multicast, broadcast et STP inconnus.

La fenêtre EtherChannels affiche les groupes de ports et vous permet d'effectuer les opérations suivantes :

- Créer des groupes de ports Fast EtherChannel et Gigabit EtherChannel
- Supprimer les ports d'un groupe de ports
- Modifier la méthode de transfert pour un groupe

Procédures

Cette fenêtre s'affiche lorsque vous sélectionnez l'option dans la barre de fonctions. Vous pouvez aussi cliquer ici pour l'activer. Utilisez cette fonction pour afficher les groupes de ports EtherChannel et pour effectuer les opérations suivantes :

- **Créer des groupes de ports**
- **Modifier des groupes de ports**
- **Supprimer des groupes de ports**

Commencez par sélectionner le périphérique local dans la liste Nom de l'hôte. Les informations figurant dans la zone Groupes de canaux s'appliquent au périphérique sélectionné.

Le champ Équilibre des charges est paramétré par défaut sur Adresse IP Source-Destination. Ce champ ne peut pas être modifié.

Votre sélection s'applique à chaque groupe de ports créé sur le commutateur.

Ce tableau explique les colonnes de la zone Groupes de canaux.

Colonne	Explication
Groupe	Nombre affecté au groupe de ports.
Ports	Ports appartenant au groupe.
État	Panne ou En cours d'utilisation. Vous pouvez également voir que le groupe contient des interfaces de couche 2.

Créer des groupes de ports

Vous pouvez créer jusqu'à 6 groupes de ports. Les ports qui constituent un groupe doivent être du même type.

Consultez la rubrique **Restrictions pour les groupes de ports, page 186** avant d'utiliser cette procédure.

Un groupe de ports peut contenir jusqu'à 16 ports s'ils se trouvent en mode LACP. Sinon, ce nombre est réduit à 8.

Par défaut, le commutateur transmet le trafic à un groupe de ports en fonction de l'adresse source du paquet. Si vous configurez une adresse statique pour un groupe de ports, configurez le commutateur afin de transférer les paquets en provenance des adresses statiques vers tous les ports du groupe afin d'éviter de perdre les paquets. Si vous configurez le groupe de ports de sorte à transférer les paquets en fonction de l'adresse de destination, configurez le commutateur de sorte à transférer les paquets destinés aux adresses statiques vers un seul port du groupe. Autrement, l'adresse de destination recevra des doublons.

Pour créer un groupe de ports, procédez comme suit :

ETAPE 1 Cliquez sur **Créer** et utilisez la fenêtre Créer EtherChannel. Voir la rubrique **Créer des groupes de ports, page 187**.

Vous pouvez créer un groupe de ports sur le périphérique local que vous avez sélectionné ou sur un périphérique distant.

Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

ETAPE 2 Cliquez sur **OK** pour fermer la fenêtre EtherChannels.

Modifier des groupes de ports

Vous pouvez modifier un groupe de ports en procédant comme suit :

- En ajoutant un port membre
- En supprimant un port membre
- En changeant le mode LACP d'un port membre

Pour effectuer ces opérations, suivez les consignes ci-dessous.

ETAPE 1 Dans la zone Groupes de canaux, sélectionnez la rangée du groupe que vous souhaitez modifier.

ETAPE 2 Cliquez sur **Modifier** et utilisez la fenêtre Modifier EtherChannel. Voir la rubrique **Créer des groupes de ports, page 187**.

Vous pouvez modifier un groupe de ports sur le périphérique local que vous avez sélectionné ou éventuellement sur un périphérique distant.

ETAPE 3 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

ETAPE 4 Cliquez sur **OK** pour fermer la fenêtre EtherChannels.

Supprimer des groupes de ports

Pour supprimer un groupe de ports, procédez comme suit :

ETAPE 1 Dans la zone Groupes de canaux, sélectionnez la rangée du groupe que vous souhaitez supprimer.

ETAPE 2 Cliquez sur **Supprimer**.

ETAPE 3 Cliquez sur **OK** pour fermer la fenêtre.

Restrictions pour les groupes de ports

N'importe quel port peut appartenir à un groupe de port. Toutefois, les restrictions suivantes s'appliquent :

- Le rôle Commutateur doit être appliqué au membre du groupe de ports.
- Aucun membre du groupe de ports ne peut être configuré pour la surveillance de port.

- Aucun membre du groupe de ports ne peut être destiné à la sécurité de port.
- Les membres du groupe de ports doivent appartenir au même groupe de VLAN et doivent tous disposer d'un accès statique, être multi-VLAN ou être des ports trunks.
- Les ports d'accès dynamiques ne peuvent pas être groupés avec d'autres ports même s'il s'agit d'autres ports d'accès dynamiques.
- Un port réseau ne peut pas se trouver dans un groupe de ports basés sur la destination.

Créer des groupes de ports

Cette fenêtre s'affiche lorsque vous cliquez sur Créer dans la fenêtre EtherChannels. Utilisez cette fonction pour affecter des ports locaux à un groupe de ports sur le périphérique sélectionné. Vous pouvez aussi affecter des ports distants à un groupe de ports sur un périphérique distant.

Seuls les ports présentant le profil de port "Commutateur" s'affichent dans cette fenêtre.

Suivez les étapes ci-dessous :

ETAPE 1 Si vous créez des groupes de ports sur un périphérique local et un périphérique distant, sélectionnez le périphérique distant dans la liste Périphérique distant. Le volet Ports distants présente les ports distants reliés aux ports du périphérique local.

Les options du périphérique distant sont identiques à celles du périphérique local. Lorsque vous sélectionnez les options pour le périphérique local, faites de même pour le périphérique distant.

ETAPE 2 Dans le champ **Groupe**, entrez le numéro du groupe de ports que vous créez.

ETAPE 3 Cochez la case sous "Dans groupe" pour chaque port destiné à faire partie du groupe.

ETAPE 4 Passez la colonne État. Elle présente l'état des ports uniquement dans la fenêtre Modifier EtherChannel.

ETAPE 5 Cliquez dans les cellules Mode des ports sélectionnés et choisissez l'une des valeurs suivantes :

- **LACP**. Le port peut former un ensemble de liaisons et initialiser le canal. L'ensemble est formé si l'autre extrémité utilise LACP en mode actif.
- **On (No LACP)**. Le port n'utilise pas le protocole LACP. L'EtherChannel est utilisable uniquement si le groupe de ports est relié à un autre groupe de ce mode.

ETAPE 6 Cliquez dans les cellules Priorité correspondant aux ports sélectionnés et entrez une priorité LACP si vous souhaitez modifier la valeur par défaut (32768 pour LACP).

Le port présentant la plus haute priorité envoie les paquets.

ETAPE 7 Cliquez sur **OK** pour fermer la fenêtre.

Le nouveau groupe de ports s'affiche dans la fenêtre EtherChannels.

Modifier le groupe de ports

Cette fenêtre s'affiche lorsque vous sélectionnez un groupe de ports et cliquez sur Modifier dans la fenêtre EtherChannels.

Voici les options pour les groupes de ports locaux et distants que vous pouvez modifier :

- Ports appartenant au groupe
- Mode du port
- Priorité du port

La colonne État présente les informations sur les ports qui vous aideront dans le choix des modifications. Voici les états qui s'affichent :

État	Signification
dans groupe de ports	Le port est actif dans le groupe de ports.
actif-en attente	Huit ports LACP (nombre maximum) sont déjà actifs.
suspendu	Le port ne fonctionne pas pour l'instant, sans doute en raison d'un conflit avec d'autres ports.
indépendant	Le port est relié à un port distant qui ne fait pas partie du groupe de ports.
panne	Le port ne fonctionne pas. Il peut être déconnecté ou présenter un problème de gestion.

ETAPE 8 Lorsque vous avez terminé, cliquez sur **OK**.

5

Routage et connexions réseau

Cette rubrique traite de la configuration du routage réseau. Elle se compose des sections suivantes :

- **Adresses IP**
- **Connexion Internet**
- **Serveur DHCP**
- **Routage statique**

Adresses IP

Pour gérer les adresses IP, sélectionnez **Configurer** > **Routage** > **Adresses IP** dans la barre de fonctions. Consultez les rubriques suivantes pour obtenir des informations sur l'activation et la configuration des adresses IP :

- **Vue d'ensemble**
- **Modification des VLAN par défaut**
- **Configuration de l'interface**
- **Configuration du périphérique**

ATTENTION Nous vous conseillons de ne pas configurer ces paramètres à l'aide d'une connexion WAN distante. Si la connexion WAN est interrompue, l'opération échouera et le système risque d'être inutilisable.

Vue d'ensemble

La fenêtre Adresses IP présente les onglets suivants :

- **Configuration de l'interface**permet d'affecter une adresse IP et un masque de sous-réseau à un VLAN. Ce faisant, le VLAN devient une SVI (interface virtuelle commutée). La création d'une SVI n'active pas le routage sur le périphérique.
- **Configuration du périphérique**permet d'associer un nom de domaine au périphérique sélectionné.

Modification des VLAN par défaut

Les VLAN par défaut sont définis de série pour ces périphériques :

- Pour l'UC500, la liste se compose des VLAN par défaut suivants :
  - **VLAN 1** : VLAN de données par défaut pour l'UC500.
  - **VLAN 100** : VLAN voix par défaut pour l'UC500.
  - **BV175** : VLAN de données sans fil pour l'UC500.
- Pour le SR520, la VLAN par défaut est **VLAN75**.
- Pour le SR520-T1, les VLAN par défaut sont **LAN0** (FastEthernet0) et **LAN1** (FastEthernet1).

Vous pouvez modifier l'adresse IP et le masque de sous-réseau pour ces VLAN par défaut sous l'onglet **Configuration de l'interface** de la fenêtre Adresses IP.

La configuration des VLAN de données et de voix par défaut pour l'UC500 peut être modifiée à l'aide de l'Assistant de configuration de la téléphonie, lequel devra être utilisé sur un système où les paramètres d'usine ont été rétablis à partir du Gestionnaire multi-sites.

ATTENTIONLa modification de l'adresse IP des VLAN de données et de voix par défaut au terme de la configuration initiale donne lieu à des modifications au niveau des autres paramètres de configuration. Une fois la configuration modifiée, vérifiez si le système fonctionne correctement.

Nous vous conseillons de ne pas configurer ces paramètres à l'aide d'une connexion WAN distante.

La modification du champ Réseau pour l'interface VLAN100 ou VLAN1 de l'onglet Réserves DHCP de la fenêtre Serveur DHCP (**Configurer** > **Routage** > **Serveur DHCP**) aura le même effet que la modification de l'adresse IP des VLAN de données et/ou de voix sur le périphérique.

IMPORTANT :

- Après avoir modifié l'adresse IP du VLAN par défaut, vous devrez définir manuellement les règles de mappage de ports NAT sous **Configurer** > **Sécurité** > **NAT**.
- Après avoir modifié l'adresse IP du VLAN de données par défaut sur l'UC500, vous devrez redémarrer les commutateurs ESW500 se trouvant sur le site client afin de renouveler la connexion DHCP de l'ESW 500. Cela peut également concerner d'autres périphériques du site.

Le tableau ci-dessous décrit les paramètres de configuration qui sont automatiquement mis à jour par CCA lorsque vous modifiez l'adresse IP de chacun des VLAN par défaut pour ces périphériques.

Périphérique	VLAN par défaut	Paramètres modifiés avec le VLAN
UC500	VLAN de données (VLAN 1)	L'adresse IP du VLAN de données (VLAN1 / BVI1) présente une nouvelle valeur. La plage d'exclusion d'adresses DHCP existante est supprimée et une nouvelle plage est intégrée sur la base de la nouvelle adresse IP du VLAN de données. La réserve d'adresses IP VPN existante est supprimée et une nouvelle réserve d'adresses IP VPN est intégrée sur la base de la nouvelle adresse IP du VLAN de données. Les dial-peers qui utilisent la cible de la session pour pointer vers le routage de l'adresse IP du VLAN de données existant sont modifiés de sorte à pointer vers le nouveau. Par exemple, si l'adresse du nouveau VLAN est 192.168.20.1, le dial-peer utilise la cible de session ipv4:192.168.20.1. Toutes les listes de contrôle d'accès (ACL) sont modifiées en vue d'être utilisées avec l'adresse IP du VLAN. Si l'UC500 se trouve derrière un SR500 : ▪ Toutes les ACL qui font référence au sous-réseau existant sont modifiées en fonction du nouveau. ▪ Les routages statiques au départ du SR500 vers l'UC500 qui font référence à l'adresse IP du VLAN de données existant sont modifiés de sorte à utiliser l'adresse IP du nouveau VLAN de données. Si l'UC500 se trouve derrière un dispositif de sécurité SA500 et que le SA500 présente des routages statiques vers le VLAN de données existant sur l'UC500, ces valeurs sont modifiées de telle sorte à pointer vers le nouveau VLAN de données.
UC500	VLAN vocal (VLAN100)	Le VLAN de données sans fil de l'UC-500 présente une nouvelle valeur (VLAN75/BVI75). Les paramètres des applications de contrôle SCCP sont modifiés en vue d'être utilisés avec la nouvelle adresse IP du VLAN vocal. Toutes les ACL de l'UC500 qui font référence à l'adresse IP du VLAN vocal sont modifiées en fonction du nouveau. Si l'UC500 se trouve derrière un SR500 ou un SA500, les ACL du SR500 ou du SA500 qui font référence à l'adresse IP du VLAN vocal existant sont modifiées en fonction du nouveau.

Périphérique	VLAN par défaut	Paramètres modifiés avec le VLAN
SR500 et SR520-T1	VLAN de données VLAN75 pour le SR500 FastEthernet0/0, FastEthernet0/1 pour le SR520-T1)	L'adresse IP du VLAN de données (VLAN75) présente une nouvelle valeur. La plage d'exclusion d'adresses DHCP existante est supprimée et une nouvelle plage est intégrée sur la base de la nouvelle adresse IP du VLAN de données. La réserve d'adresses IP VPN existante est supprimée et une nouvelle réserve d'adresses IP VPN est intégrée sur la base de la nouvelle adresse IP du VLAN de données. Toutes les listes de contrôle d'accès (ACL) sont modifiées en vue d'être utilisées avec l'adresse IP du VLAN. Si l'UC500 se trouve derrière un SR500 : ▪ Toutes les ACL qui font référence à l'adresse IP du VLAN de données existant sont modifiées en fonction du nouveau sous-réseau. ▪ Les routages statiques de l'UC500 qui font référence à l'adresse IP du VLAN de données existant sur le SR500 sont modifiés de sorte à utiliser l'adresse IP du nouveau VLAN de données. Les règles de conversion d'adresse réseau (NAT) du SR500 pour le transfert du trafic sur les ports 5060 (SIP) et 1720 (H323) sont modifiées de sorte à utiliser l'adresse IP du nouveau VLAN de données. Les routages par défaut pour l'UC500, s'il est connecté à un SR500 et à un site client, sont modifiés en fonction de la nouvelle valeur.

Configuration de l'interface

Commencez par sélectionner un périphérique dans la liste Nom de l'hôte.

Les noms des VLAN configurés sur le périphérique sélectionné sont affichés dans la colonne **Nom de l'interface**. Il peut s'agir des VLAN par défaut intégrés à la configuration d'usine d'un périphérique ou les VLAN que vous avez ajoutés.

- Pour affecter une nouvelle adresse IP, cliquez dans la colonne Adresse IP correspondant au périphérique sélectionné et entrez la nouvelle adresse IP.
- Pour affecter un nouveau masque de sous-réseau, cliquez dans la colonne Masque de sous-réseau correspondant au périphérique sélectionné et entrez la nouvelle valeur.

Cliquez sur **OK** ou **Appliquer** lorsque vous avez terminé.

Si vous êtes connecté au VLAN de données par défaut sur l'UC500 ou le SR500, vous perdrez la connexion à l'UC500 lorsque l'adresse IP du VLAN de données de l'UC 500 ou du SR500 est modifiée. Fermez et relancez ensuite CCA et connectez-vous au périphérique à l'aide de la nouvelle adresse IP.

Configuration du périphérique

ETAPE 1 Commencez par sélectionner un périphérique dans la liste Nom de l'hôte.

ETAPE 2 Dans le champ **Nom de domaine**, entrez un nom identifiant une région d'administration du réseau IP. Vous devrez peut-être demander ces informations à votre administrateur réseau. Quand le trafic réseau ne contient aucun nom de domaine, le nom que vous entrez est ajouté au nom du périphérique, puis ce nom complet est ajouté à la table des noms d'hôte du périphérique.

ETAPE 3 Cochez la case **Activer la recherche du domaine** pour autoriser les serveurs à transposer les noms de périphériques en adresses IP.

ETAPE 4 Dans le champ **Nouveau serveur**, entrez le nom d'un périphérique que vous souhaitez utiliser en tant que serveur de nom de domaine, puis cliquez sur **Ajouter**. Le périphérique est ajouté à la liste Serveurs actuels.

ETAPE 5 Pour cesser d'utiliser un périphérique en tant que serveur DNS, sélectionnez-le dans la liste **Serveurs actuels** et cliquez sur **Supprimer**.

ETAPE 6 Cliquez sur **OK** ou **Appliquer**.

Connexion Internet

La fenêtre Connexion Internet s'affiche lorsque vous sélectionnez **Configurer** > **Routage** > **Connexion Internet** dans la barre de fonctions.

Vue d'ensemble

La fenêtre Connexion Internet présente les deux onglets suivants :

- **Paramètres de connexion**: Pour l'activation et la configuration de la connexion Internet du WAN et la configuration des services de noms de domaine dynamique (DDNS).
- **Mise en forme du trafic**: Pour l'activation de la mise en forme du trafic et la configuration des paramètres QoS (recommandé pour les déploiements multi-sites).

Paramètres de connexion

À partir de cet onglet, vous pouvez activer et configurer la connexion Internet. Les types de connexion suivants sont pris en charge :

- **PPPoE** ou **PPPoE avec négociation d'adresse IP** : Le protocole PPPoE peut être utilisé par plusieurs hôtes sur une interface Ethernet partagée afin d'ouvrir des sessions PPP vers diverses cibles équipées d'au moins un modem de liaison. Si vous optez pour une adresse IP négociée, le routeur obtient l'adresse IP par une négociation PPP/IPCP (Protocole point-à-point/ protocole de contrôle d'IP).
- **Adresse IP statique** : configuration de l'interface pour l'utilisation d'une adresse IP statique.
- **DHCP** : configuration de l'interface pour l'obtention d'une adresse IP à partir d'un serveur DHCP.

Vous pouvez aussi configurer des options complémentaires pour le DDNS.

Pour activer et configurer la connexion Internet, procédez comme suit :

ETAPE 1 Sélectionnez un périphérique à configurer dans la liste Nom de l'hôte.

ETAPE 2 Sélectionnez une interface dans la liste Interfaces WAN.

ETAPE 3 Cliquez sur **Modifier** pour afficher la fenêtre Modifier la connexion Internet. Voir la rubrique **Modifier la connexion Internet, page 199**.

ETAPE 4 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Mise en forme du trafic

Cet onglet vous permet d'activer la mise en forme du trafic et de configurer les paramètres QoS.

Ces paramètres sont essentiellement utilisés pour la configuration du nombre maximum d'appels simultanés pour les déploiements multi-sites.

- Voir **Configuration de la qualité de service (QoS), page 506** pour plus d'informations et des recommandations sur la configuration du service QoS dans le cadre des déploiements multi-sites.
- Voir **Nombre d'appels maximum (Contrôle des admissions d'appel), page 513** pour plus d'informations sur la configuration du contrôle des admissions d'appel en fonction de ces paramètres.

Configurez les paramètres selon les indications du tableau suivant. Cliquez sur **OK** ou **Appliquer** pour terminer.

Paramètre	Description
Mise en forme du trafic	Activez ce paramètre pour activer le service QoS et la mise en forme du trafic.
Bande passante ascendante [kbps]	Lorsque la **Mise en forme du trafic** est active, définissez la bande passante ascendante en kb/s pour le site en fonction d'un test de vitesse de connexion ou du débit d'informations garanti (Committed Information Rate - CIR) établi dans le Contrat de niveau de service de votre fournisseur d'accès à Internet. Vous pouvez entrer des valeurs comprises entre 384 et 100000 kb/s. Par exemple, si la bande passante ascendante est de 1,8 Mb/s, entrez la valeur 1800. Si vous ne disposez pas des résultats des tests de vitesse ou CIR, entrez une valeur en kb/s correspondant à 80 % de la bande passante ascendante annoncée par votre fournisseur de services.
Réservation média (%)	Utilisez le curseur pour définir la fraction de bande passante disponible à affecter au trafic vocal (le cas échéant). Vous pouvez entrer des valeurs comprises entre 1 et 95 % (les 5 % restants sont réservés au signalement et autres éléments). Valeur par défaut : 50 %. En l'absence de trafic vocal sur le réseau, toute la bande passante disponible peut être utilisée pour le trafic de données.

Pour de plus amples informations, consultez la rubrique **Modifier la connexion Internet, page 199**.

Modifier la connexion Internet

Cette fenêtre s'affiche lorsque vous sélectionnez **Modifier** dans la fenêtre Connexion Internet.

Pour activer et configurer une connexion Internet sur une interface ou configurer les paramètres DDNS (facultatif), complétez les éléments ci-dessous et cliquez sur **OK**.

Paramètre	Description
Activer l'interface WAN	Lorsque cette option est cochée, la connexion Internet est active.
PPPoE	Cochez la case PPPoE pour sélectionner cette option pour la connexion Internet si votre fournisseur de services le demande. Si l'option PPPoE est cochée, configurez les paramètres correspondants. Vous obtiendrez les informations complémentaires de votre fournisseur de services. ▪ **Nom d'utilisateur** : nom d'utilisateur requis pour la connexion PPPoE. ▪ **Mot de passe** : mot de passe PAP/CHAP requis pour la connexion PPPoE. ▪ **Entrez à nouveau le mot de passe** : réintroduisez le mot de passe pour le confirmer.
IP négociée	Cette option n'est disponible qu'en présence d'une encapsulation PPPoE. Activez l'option **IP négociée** si votre fournisseur d'accès le préconise. Si vous choisissez **IP négociée**, le routeur obtient son adresse IP suite à une négociation d'adresses PPP/IPCP.

Paramètre	Description
IP statique	Cliquez sur **IP statique** pour utiliser l'adresse IP statique obtenue de votre fournisseur de services. Si vous choisissez l'option **IP statique**, vous devrez introduire les données ci-dessous. Vous obtiendrez les informations complémentaires de votre fournisseur de services. ▪ **Adresse IP Internet** ▪ **Masque de sous-réseau** ▪ **Passerelle par défaut** : adresse IP de la passerelle par défaut. ▪ **Adresse IP du serveur DHCP primaire** (requis) ▪ **Adresse IP du serveur DHCP secondaire** (facultatif) Si vous souhaitez par la suite modifier la connexion Internet afin d'utiliser le protocole DHCP au lieu d'une adresse IP statique, vous devrez au préalable supprimer les paramètres de configuration existants pour SSL VPN et VPN Server.
DHCP	Si vous sélectionnez l'option DHCP, le routeur emprunte une adresse IP d'un serveur DHCP distant.

Paramètre	Description
HTTP DDNS	
	Facultatif. Configurez les paramètres pour le service DDNS. Les sites exploitant le protocole DHCP pour obtenir une adresse IP de manière dynamique peuvent utiliser le service d'hébergement DDNS pour permettre l'association des adresses IP dynamiques (DHCP) à des noms d'hôtes statiques. Le DDNS peut également être configuré pour les périphériques dotés d'une adresse IP négociée pour le WAN. Les sites exploitant le protocole DHCP dans le cadre d'un déploiement multi-sites doivent configurer le protocole HTTP DDNS.
Fournisseur	Sélectionnez un fournisseur DDNS dans le menu déroulant. Vous devez créer votre compte DDNS auprès de l'un des fournisseurs suivants (hors Configuration Assistant). Les services d'hébergement DDNS suivant sont disponibles : ▪ cgi.tzo.com ▪ dup.hn.org ▪ members.dyndns.org ▪ members.easydns.com ▪ www.dynx.cx ▪ www.justlinux.com ▪ www.zoneedit.com
Nom de l'hôte	Nom d'hôte unique pour ce site obtenu du fournisseur de services DDNS. Il s'agit généralement d'un nom de domaine complet (FQDN), par exemple mon_hôte.mon_domaine.net, mais cela peut s'avérer différent en présence de certains services DDNS. Le nom d'hôte doit être enregistré. Ce champ n'est pas validé par Configuration Assistant. Veillez à introduire correctement le nom d'hôte selon les instructions de votre fournisseur DDNS. Si vous configurez un déploiement multi-sites, chaque site doit disposer d'un nom d'hôte DDNS unique.

Paramètre	Description
Nom d'utilisateur	Nom d'utilisateur pour le compte obtenu de votre fournisseur de services DDNS.
Mot de passe	Mot de passe pour le compte obtenu de votre fournisseur de services DDNS.
Confirmer le mot de passe	Réintroduisez le mot de passe pour le confirmer.

Pour de plus amples informations, consultez les rubriques suivantes :

- **Configuration du DDNS, page 505**
- **Configuration de la qualité de service (QoS), page 506**
- **Fonctions vocales prises en charge sur plusieurs sites, page 512**

Serveur DHCP

Pour configurer les paramètres du serveur DHCP, sélectionnez **Configurer** > **Routage** > **Serveur DHCP** dans la barre de fonctions.

Vue d'ensemble

Une réserve d'adresses IP DHCP (Dynamic Host Configuration Protocol) est une plage d'adresses IP qu'un serveur DHCP peut attribuer de manière dynamique aux périphériques clients. Étant donné que tous les clients ne sont pas forcément connectés en permanence, l'attribution d'adresses IP en fonction des besoins permet de réduire le nombre d'adresses IP nécessaires pour desservir un groupe de clients en utilisant la même adresse IP pour plusieurs clients à des moments différents.

Pour gérer une réserve d'adresses IP DHCP, vous pouvez procéder comme suit :

- Créez une réserve d'adresses IP DHCP permettant d'identifier la plage d'adresses IP pour cette réserve.
- Associez une adresse IP donnée de la réserve à une adresse MAC donnée afin de créer une adresse IP statique pour le périphérique client. (Certains clients demandent des adresses IP statiques afin d'assurer la liaison nécessaire aux applications actives.)

- Créez une exception pour une adresse IP donnée dans la réserve afin que le serveur DHCP ne l'affecte pas à un client. (Plusieurs adresses IP de la plage peuvent avoir été affectées par d'autres processus. Pour éviter les conflits, vous pouvez exclure ces adresses de la réserve.)

La plage de la réserve est calculée à partir du numéro de réseau et du masque de sous-réseau. Toutes les adresses IP disponibles au niveau du nœud sont comprises dans la réserve et mises à la disposition du serveur sauf en cas d'association à une adresse MAC spécifique ou si elles font l'objet d'une exception. Le serveur ignore en effet les adresses liées et les exceptions.

La fenêtre Serveur DHCP présente les onglets suivants :

- **Réserves DHCP**: permet d'afficher, créer, modifier ou supprimer une réserve DHCP d'adresses IP.
- **Liaisons DHCP**: permet d'associer manuellement les adresses IP de la réserve DHCP aux adresses MAC des clients.
- **Exclusions DHCP**: permet de définir l'adresse IP que le serveur DHCP ne doit pas affecter (ou exclure) des clients.

Réserves DHCP

Une réserve d'adresses IP DHCP (Dynamic Host Configuration Protocol) est une plage d'adresses IP qu'un serveur DHCP peut attribuer de manière dynamique aux périphériques clients.

Deux réserves DHCP par défaut sont créées pour l'UC500 : **phone** et **default**. Ces réserves DHCP par défaut peuvent être modifiées, mais les noms par défaut sont réservés. Ils ne peuvent donc pas être modifiés.

- La réserve **phone** est associée au VLAN vocal (VLAN 100) de l'UC500. Les adresses IP de la réserve DHCP "phone" sont affectées aux téléphones IP lors de l'enregistrement automatique.
- La réserve **data** est associée au VLAN de données (VLAN1) de l'UC500. Les adresses IP de cette réserve sont affectées aux périphériques du VLAN de données demandant une adresse IP au serveur DHCP.

Pour afficher les propriétés configurées pour une réserve DHCP, sélectionnez le nom de la réserve DHCP souhaitée.

Pour créer une réserve DHCP, cliquez sur **Créer** et utilisez la fenêtre Créer une réserve DHCP. Voir la rubrique **Créer une réserve DHCP, page 205**.

Pour modifier une réserve DHCP, sélectionnez la réserve DHCP, cliquez sur **Modifier** et utilisez la fenêtre Modifier une réserve DHCP. Voir la rubrique **Modifier une réserve DHCP, page 207**.

Pour supprimer une réserve DHCP, sélectionnez son nom et cliquez sur **Supprimer**. Une fenêtre s'affiche et vous indique que si vous continuez, vous allez supprimer la réserve DHCP.

Cliquez sur **OK** pour fermer la fenêtre.

Liaisons DHCP

Une fois la réserve DHCP créée, vous pouvez affecter manuellement les adresses IP à partir de cette réserve à des périphériques donnés en fonction de leur adresse MAC.

Pour créer une nouvelle liaison DHCP, cliquez sur **Créer** et utilisez la fenêtre Créer une liaison DHCP. Voir la rubrique **Créer une liaison DHCP, page 207**.

Pour modifier une liaison DHCP, sélectionnez le nom de la réserve, cliquez sur **Modifier** et utilisez la fenêtre Modifier une liaison DHCP. Voir la rubrique **Modifier la liaison DHCP, page 208**.

Pour supprimer une liaison DHCP, sélectionnez son nom et cliquez sur **Supprimer**. Une fenêtre s'affiche et vous indique que si vous continuez, vous allez supprimer la liaison DHCP.

Cliquez sur **OK** pour fermer la fenêtre.

Exclusions DHCP

Sous cet onglet, vous pouvez définir des adresses IP isolées ou des plages d'adresses IP à exclure de la réserve d'adresses DHCP. Ces adresses ne peuvent pas être affectées aux clients DHCP.

Pour créer une nouvelle exclusion DHCP, cliquez sur **Créer** et utilisez la fenêtre Créer une exclusion DHCP. Voir la rubrique **Créer une exclusion DHCP, page 205**.

Pour supprimer une exclusion DHCP, sélectionnez l'adresse IP et cliquez sur **Supprimer**.

Par défaut, ces adresses IP sont exclues des réserves DHCP :

- de 10.1.1.1 à 10.1.1.10 (réservées pour Cisco IOS et CUE)
- de 192.168.10.1 à 192.168.10.10 (réservées pour l'UC 500)
- adresses broadcast 10.1.1.255 et 192.168.10.255

Liaisons aux réserves DHCP

Vous pouvez utiliser deux types de liaisons aux réserves DHCP :

- Liaison automatique : le serveur DHCP créera l'association. Au terme du délai, le périphérique obtient une nouvelle adresse IP.
- Liaison manuelle : vous voulez que le périphérique utilise une adresse IP donnée. La liaison n'expire pas.

Créer une exclusion DHCP

Cette fenêtre s'affiche lorsque vous cliquez sur **Créer** sous l'onglet Exclusion IP DHCP dans la fenêtre Serveur DHCP.

Utilisez cette fenêtre pour ajouter une plage d'adresses IP DHCP à exclure.

Suivez les étapes ci-dessous :

ETAPE 1 Dans le champ **Adresse IP de départ**, entrez la première adresse IP DHCP de la plage d'adresses que le serveur DHCP ne doit pas affecter aux clients DHCP.

ETAPE 2 Dans le champ **Adresse IP de fin**, entrez la dernière adresse IP de la plage d'adresses que le serveur DHCP ne doit pas affecter aux clients DHCP.

ETAPE 3 Cliquez sur **OK**.

Créer une réserve DHCP

Cette fenêtre s'affiche lorsque vous cliquez sur **Créer** sous l'onglet Liaisons DHCP dans la fenêtre Serveur DHCP.

Cette fenêtre vous permet de créer une réserve DHCP et éventuellement indiquer les serveurs DNS, le nom de domaine, le routeur par défaut et les serveurs WINS (Windows Internet Naming Service).

Pour créer une réserve DHCP, configurez les paramètres ci-dessous et cliquez sur **OK**.

Paramètre	Description
Nom	Entrez le nom de la réserve DHCP. Sur l'UC500, le téléphone et les noms de la réserve DHCP de données sont réservés pour les VLAN de voix (VLAN100) et de données (VLAN1).
Réseau	Adresse IP de départ de la réserve DHCP. Si vous modifiez les paramètres réseau pour les réserves DHCP du téléphone et des données sur l'UC500, cela produit les mêmes résultats que la modification de l'adresse IP de ces VLAN par défaut. Voir la rubrique **Modification des VLAN par défaut, page 192**.
Masque de sous-réseau	Entrez le masque de sous-réseau.
Serveur DNS 1	Dans le champ **Serveur DNS 1**, introduisez l'adresse IP du serveur DNS. Les clients DHCP demandent aux serveurs DNS d'associer les noms d'hôte aux adresses IP.
Serveur DNS 2	*Facultatif*. Dans le champ **Serveur DNS 2**, introduisez l'adresse IP du deuxième serveur DNS.
Nom de domaine	Entrez le nom du domaine. Le nom de domaine d'un client DHCP place le client dans le domaine.
Serveur WINS 1, Serveur WINS 2	*Facultatif*. Dans les champs **WINS Server1** et **WINS Server2** , introduisez l'adresse IP du serveur WINS. Ces champs indiquent les serveurs WINS accessibles pour le client DHCP Microsoft.
Routeur par défaut	*Facultatif*. Dans le champ **Routeur par défaut**, entrez l'adresse IP de la passerelle par défaut. Au démarrage d'un client DHCP, le client commence à envoyer les paquets à la passerelle par défaut. L'adresse IP de la passerelle par défaut doit se trouver sur le même sous-réseau que le client.

Modifier une réserve DHCP

Cette fenêtre s'affiche lorsque vous cliquez sur **Modifier** sous l'onglet Réserves DHCP dans la fenêtre Serveur DHCP.

Cette fenêtre vous permet de modifier une réserve DHCP (serveurs DNS, nom de domaine, routeur par défaut et serveurs WINS).

Vous ne pouvez pas modifier le nom des réserves DHCP par défaut pour le téléphone et les données. Tous les autres paramètres peuvent être modifiés pour ces réserves.

Voir **Créer une réserve DHCP, page 205** pour une explication des champs de cette fenêtre.

Lorsque vous avez terminé, cliquez sur **OK**.

Créer une liaison DHCP

Cette fenêtre s'affiche lorsque vous cliquez sur **Créer** sous l'onglet Liaisons DHCP dans la fenêtre Serveur DHCP.

Pour créer une réserve DHCP, configurez les paramètres ci-dessous et cliquez sur **OK**.

Paramètre	Description
Nom	Introduisez un nom pour la réserve d'adresses DHCP.
Adresse IP de l'hôte	Entrez l'adresse IP de l'hôte.
Masque de réseau	Entrez le masque de sous-réseau de l'hôte.
Adresse MAC	Entrez l'adresse MAC. Elle représente l'adresse matérielle du client ou permet d'identifier le client sous la forme d'une notation hexadécimale. Par exemple, 01b7.0813.8811.66.
Nom du client	Entrez le nom du client au format ASCII standard. Le nom du client ne doit pas être le nom de domaine. Par exemple, *n'entrez pas* le nom "mars" sous la forme "mars.cisco.com".

Modifier la liaison DHCP

Cette fenêtre s'affiche lorsque vous cliquez sur **Modifier** sous l'onglet Liaisons DHCP dans la fenêtre Serveur DHCP.

Utilisez cette fenêtre pour modifier une liaison DHCP.

Voir **Créer une liaison DHCP, page 207** pour une explication des champs de cette fenêtre.

Lorsque vous avez terminé, cliquez sur **OK**.

Routage statique

Pour configurer les routages statiques, sélectionnez **Configurer** > **Routage** > **Routage statique** dans la barre de fonctions.

Cette fenêtre vous permet d'ajouter un routage statique ou de supprimer un routage statique du routeur.

Vue d'ensemble

Vous pouvez ajouter un routage statique à la table de routage statique d'un routeur.

- Le routage statique est codé dans la table de routage statique du périphérique. Chaque routage statique configuré ne peut être supprimé de cette table qu'en cas de suppression ou de remplacement.
- Le routage statique est prioritaire par rapport aux routages dynamiques. Il réduit les délais de traitement en définissant le routage d'un paquet de données. Les routages dynamiques sont obtenus par le périphérique à l'aide de protocoles de routage IP tels que RIP. Ils ont besoin d'un délai plus important et sont éliminés du tableau de routage s'ils ne sont pas actualisés.

Sur l'UC500, un routage statique est créé vers 10.1.10.1, qui correspond à l'interface Integrated-Service-Engine-0/0, le module CUE (Cisco Unity Express). Ne supprimez pas ce routage.

Procédures

Commencez par sélectionner un périphérique dans la liste Nom de l'hôte.

- Cliquez sur **Ajouter** et utilisez la fenêtre Ajouter un chemin statique pour ajouter un routage. Voir la rubrique **Ajouter un chemin statique, page 209**.

- Pour supprimer un routage statique, sélectionnez son nom et cliquez sur **Supprimer**.

Cliquez sur **OK** pour fermer la fenêtre.

Ajouter un chemin statique

Cette fenêtre s'affiche lorsque vous sélectionnez l'option **Ajouter** dans la fenêtre Routage statique.

Pour ajouter un routage statique à un routeur, configurez les paramètres ci-dessous et cliquez sur **OK** pour fermer la fenêtre et enregistrer vos modifications.

Paramètre	Description
IP de destination/ réseau	Entrez l'adresse IP du serveur cible.
Masque de sous-réseau	Entrez le masque de sous-réseau du serveur cible.
IP de la passerelle ou interface de sortie	Sélectionnez une interface dans la liste **Interface de sortie** ou l'option **Entrez l'adresse IP de la passerelle**. Si vous sélectionnez l'option **Entrez l'adresse IP de la passerelle**, entrez l'adresse IP de la passerelle ou l'interface de sortie dans la zone de texte inférieure.

6

Sans fil

Configuration Assistant fournit les outils permettant de configurer les points d'accès sans fil et les contrôleurs LAN sans fil sur votre système. Cette partie couvre les rubriques suivantes :

- **Configuration des paramètres du système sans fil sécurisé**
- **Convertir en LAP (Lightweight Access Point - point d'accès léger)**
- **Configuration du contrôleur WLAN**

Voir **Assistant de configuration sans fil, page 104** pour des informations sur l'utilisation de l'Assistant de configuration sans fil de CCA pour configurer les paramètres sans fil et synchroniser les paramètres de profil sans fil sur les points d'accès et les téléphones IP SPA525G.

Configuration des paramètres du système sans fil sécurisé

Pour configurer la protection de vos points d'accès sans fil, cliquez sur **Configurer** > **WLAN (SSID)** dans la barre de fonctions.

Dans la fenêtre WLAN (SSID), vous pouvez effectuer les opérations suivantes :

- Configurer les paramètres SSID pour la sécurité sans fil
- Choisir si vous souhaitez ou non diffuser le SSID
- Afficher les paramètres de sécurité que vous avez configurés sur le point d'accès
- Configurer les serveurs RADIUS
- Configurer les paramètres radio sans fil pour les points d'accès autonomes
- Configurer l'authentification pour les points d'accès AP541N
- Activer ou désactiver la carte sans fil pour les périphériques UC500 et SR500 avec fonctions sans fil

REMARQUE Pour désactiver la fonction sans fil sur les appareils UC500 et SR500 dotés de points d'accès intégrés, désactivez l'option **Activer l'interface sans fil** à la fenêtre WLAN (SSID). Par défaut, l'interface sans fil est activée pour ces plateformes.

Les paramètres sans fil varient en fonction du point d'accès que vous configurez :

- **Paramètres sans fil pour les points d'accès Cisco AP541N**
- **Paramètres sans fil pour les points d'accès Cisco AP521, UC500 ou SR500**

Paramètres sans fil pour les points d'accès Cisco AP541N

Les rubriques suivantes expliquent les paramètres de configuration sans fil pour chacun des trois onglets de la fenêtre WLAN (SSID) pour les points d'accès Cisco AP541N Single-radio Dual-band.

- **SSID**
- **Radius**
- **Authentification MAC**

REMARQUE Pour configurer les fonctions de l'AP541N qui ne sont pas encore gérées par CCA (mise en cluster par exemple), utilisez l'Utilitaire de configuration de l'AP541N. Pour accéder à cet utilitaire, cliquez avec le bouton droit de la souris sur l'icône de l'AP541N dans la Fenêtre Topologie de CCA et sélectionnez l'option Utilitaire de configuration dans le menu contextuel.

SSID

Sous l'onglet SSID, vous pouvez afficher, créer ou modifier les SSID et les paramètres associés pour les points d'accès AP541N.

Vous pouvez créer jusqu'à seize (16) SSID pour un même point d'accès AP541N.

- Pour créer un SSID, cliquez sur **Créer** pour ouvrir la fenêtre Créer ou modifier un SSID.
- Pour modifier les paramètres d'un SSID, sélectionnez le SSID dans la liste et cliquez sur **Modifier**.

Pour des informations détaillées sur les paramètres du SSID propres aux points d'accès AP541N, voir **Créer ou modifier un SSID pour les points d'accès Cisco AP541N, page 223**.

Ce tableau explique les paramètres affichés dans la fenêtre SSID.

Paramètre	Description
SSID	SSID configurés sur le point d'accès. Le nom du SSID ne peut pas être modifié une fois créé. Pour modifier le nom, supprimez le SSID et créez-en un autre avec un nouveau nom. Les SSID cisco-data (VLAN1) et cisco-voice (VLAN100) sont les valeurs par défaut pour le trafic de données et de voix. Par défaut, la protection de ces SSID est définie sur la valeur "Aucun". Pour modifier les paramètres de sécurité pour un SSID, sélectionnez le SSID dans la liste et cliquez sur **Modifier**.
VLAN	Affiche le VLAN associé au SSID.
Sécurité	Affiche le type de sécurité sans fil et les paramètres associés. Les types de sécurité suivants sont disponibles sur l'AP541N : ▪ Aucun ▪ WEP statique ▪ WEP dynamique ▪ WPA Personal ▪ WPA Enterprise Voir **Options de sécurité sans fil pour les périphériques AP541N, page 226** pour une description de chacun des paramètres.
Chiffrement	Affiche l'un des types de chiffrement suivants en fonction du type de sécurité sélectionné : Aucun, **WEP**, **AES** ou **TKIP** et **AES CCMP**.

Paramètre	Description
Authentification	Affiche les types d'authentification suivants en fonction du type de sécurité sélectionné : ▪ Aucun ▪ **authentification ouverte** ▪ **authentification ouverte avec EAP** ▪ **EAP réseau**
Type d'authentification MAC	Vous pouvez définir une liste globale contenant les adresses MAC pouvant ou non accéder au réseau. Faites un choix parmi les options suivantes : ▪ **Local** pour utiliser la liste d'authentification MAC définie sous l'onglet Authentification MAC. Voir la rubrique **Authentification MAC, page 216**. ▪ **Radius** pour utiliser la liste Authentification MAC définie sur le serveur RADIUS externe. ▪ **Désactivé** pour ne pas utiliser l'authentification MAC.

Radius

Sous l'onglet Radius, vous pouvez activer et configurer les paramètres généraux pour les serveurs RADIUS externes permettant d'assurer le suivi et d'authentifier les clients sans fil. Le point d'accès AP541N ne dispose pas d'un serveur RADIUS local.

Paramètre	Description
Adresse IP du serveur RADIUS	Entrez l'adresse du serveur RADIUS global primaire Lorsque le premier client sans fil tente de s'identifier sur le PA, le PA envoie une demande d'identification au serveur primaire. Si le serveur primaire répond à la demande d'identification, le PA continue à utiliser le serveur RADIUS comme serveur primaire et les demandes d'identification sont envoyées à l'adresse définie.

Paramètre	Description
Adresse IP RADIUS 1, Adresse IP RADIUS 2, Adresse IP RADIUS 3	Vous pouvez entrer jusqu'à trois adresses IPv4 pour les serveurs RADIUS de réserve. En cas d'échec de l'identification sur le serveur primaire, le système procède à un essai sur les serveurs de réserve. L'adresse doit être valable afin que le PA puissent tenter de contacter le serveur.
Clé RADIUS	La Clé RADIUS est le code partagé propre au serveur RADIUS global primaire. Vous pouvez introduire jusqu'à 63 caractères alphanumériques et spéciaux pour la clé RADIUS. Le code est sensible à la casse. Vous devrez configurer le même code sur le PA et sur votre serveur RADIUS. La clé RADIUS ne s'affiche pas en texte clair tandis que vous l'introduisez.
Clé RADIUS 1, Clé RADIUS 2, Clé RADIUS 3	Entrez la clé RADIUS associée à chaque serveur RADIUS de réserve configuré. Le serveur se trouvant à l'adresse IP RADIUS 1 utilise la Clé RADIUS 1, le serveur se trouvant à l'adresse IP RADIUS 2 utilise la Clé RADIUS 2, etc. Vous pouvez introduire jusqu'à 63 caractères alphanumériques et spéciaux pour la clé RADIUS. Le code est sensible à la casse. Vous devrez configurer le même code sur le PA et sur votre serveur RADIUS. La clé RADIUS ne s'affiche pas en texte clair tandis que vous l'introduisez.
Activer la gestion RADIUS	Activez cette option pour assurer le suivi et mesurer les ressources utilisées par un utilisateur donné ; par exemple, l'heure système, le volume de données envoyées et reçues, etc. Si vous activez la gestion RADIUS, elle est active sur le serveur RADIUS primaire et sur tous les serveurs de réserve.

Authentification MAC

Sous l'onglet Authentification MAC, vous pouvez définir une liste d'adresses MAC afin de contrôler l'accès au réseau par le biais du PA en fonction de l'adresse MAC du client sans fil. Vous pourrez également définir si les clients associés à ces adresses MAC sont autorisés ou non à accéder au réseau. Cette liste locale est utilisée lorsque le paramètre de la fonction **Authentification MAC** est défini sur Local pour un SSID configuré sur l'AP541N.

Pour configurer les paramètres de l'authentification MAC, procédez comme suit :

ETAPE 1 Sélectionnez le filtre à utiliser pour les clients dont les adresses MAC figurent dans la liste.

- Sélectionnez la valeur **Autoriser les adresses de la liste** pour n'autoriser l'accès qu'aux clients dont l'adresse MAC est définie dans la liste.
- Sélectionnez la valeur **Refuser les adresses de la liste** pour autoriser l'accès à tous les clients à l'exception de ceux dont l'adresse MAC est définie dans la liste.

ETAPE 2 Cliquez sur **Ajouter** pour ajouter une nouvelle ligne au tableau.

ETAPE 3 Cliquez n'importe où dans la ligne et introduisez l'adresse MAC à 12 chiffres du client à ajouter à la liste.

Entrez les adresses MAC au format `xxxx.xxxx.xxxx` (par exemple, `0101.FEFE.2345`). Les points sont introduits automatiquement au fil de la saisie. Évitez les deux points pour séparer les valeurs hexadécimales de l'adresse MAC.

ETAPE 4 Continuez à ajouter les adresses MAC à la liste en fonction des besoins.

ETAPE 5 Cliquez sur **OK** ou **Appliquer** lorsque vous avez terminé.

Pour supprimer une adresse MAC de la liste, mettez l'adresse en surbrillance et cliquez sur **Supprimer**. Cliquez ensuite sur **Appliquer** ou sur **OK**.

Paramètres sans fil pour les points d'accès Cisco AP521, UC500 ou SR500

Les rubriques suivantes expliquent les paramètres de configuration pour chacun des trois onglets de la fenêtre WLAN (SSID) :

- **Noms de réseau sans fil (SSID)**
- **Serveurs RADIUS**
- **Paramètres du point d'accès**

REMARQUE Les routeurs sécurisés SR500 dotés de points d'accès intégrés présentent des paramètres analogues, mais l'interface de configuration de ces paramètres ne présente pas d'onglets distincts. Voir les rubriques **Noms de réseau sans fil (SSID)** et **Serveurs RADIUS** pour plus d'informations sur ces paramètres.

Noms de réseau sans fil (SSID)

Vous pouvez définir des critères de sécurité pour votre **point d'accès autonome**. Les fonctions de sécurité permettent de protéger les échanges sans fil entre le point d'accès autonome et les autres périphériques sans fil en évitant tout accès non autorisé. Vous pouvez définir différents niveaux de sécurité et un cryptage pour votre point d'accès autonome. Les niveaux disponibles sont compris entre aucune sécurité et une sécurité élevée.

Le tableau suivant décrit les colonnes de cette fenêtre.

Paramètre	Description
SSID	SSID configurés sur le point d'accès.
VLAN	VLAN associé au SSID.
Activer l'interface sans fil	Cette option ne s'affiche que pour les périphériques UC500 et SR500 dotés de fonctions sans fil. Lorsque cette option est désactivée, l'interface sans fil de ces périphériques est désactivée. Vous pouvez toujours configurer les SSID et les paramètres lorsque l'interface sans fil est désactivée.

Paramètre	Description
Sécurité	Type de sécurité sans fil et paramètres associés : ▪ Pas de protection ▪ **WEP, page 230** ▪ **EAP, page 231** ▪ **LEAP, page 231** ▪ **WPA, page 232** ▪ **WPA-PSK, page 232** ▪ **WPA2, page 233** ▪ **WPA2-PSK, page 233** ▪ **MAC, page 233** ▪ **MAC et EAP, page 234** ▪ Inconnu : cette valeur s'affiche si le critère de sécurité a été configuré à l'aide de la ligne de commande et si ce dernier n'est pas pris en charge par l'Assistant de configuration.
Chiffrement	Type de chiffrement sans fil : ▪ Aucun (non recommandé) ▪ **WEP** ▪ Dynamique **WEP** ▪ **TKIP** ▪ **AES CCMP**
Authentification	Au moins un des types d'authentification suivants : ▪ **authentification ouverte** ▪ **authentification ouverte avec EAP** ▪ **EAP réseau** ▪ **WPA-PSK**

Procédez selon la méthode ci-dessous pour configurer les paramètres SSID et de sécurité sur vos points d'accès autonomes.

ETAPE 1 Dans la liste **Nom de l'hôte**, sélectionnez un point d'accès.

ETAPE 2 Pour créer un LAN sans fil et sélectionner les paramètres de sécurité, ouvrez l'onglet Noms de réseau sans fil (SSID), cliquez sur **Créer** et complétez la fenêtre Créer un WLAN. Voir la rubrique **Créer ou modifier un SSID de WLAN, page 223**.

Plusieurs WLAN permettent d'accéder à différents réseaux grâce à un seul point d'accès autonome.

Le nombre de SSID que vous pouvez créer varie en fonction du type de point d'accès. Par exemple, les périphériques SR500 prennent en charge un maximum de quatre (4) SSID.

ETAPE 3 Pour modifier une configuration, sélectionnez le WLAN et cliquez sur **Modifier**. Utilisez la fenêtre Modifier un WLAN. Voir la rubrique **Créer ou modifier un SSID de WLAN, page 223**.

ETAPE 4 Pour supprimer une configuration, sélectionnez le WLAN et cliquez sur **Supprimer**.

ETAPE 5 Pour désactiver la carte sans fil pour les périphériques Cisco UC500 et SR500, annulez l'option **Activer l'interface sans fil**. Vous pouvez toujours configurer les SSID lorsque l'interface sans fil est désactivée. Par défaut, l'interface sans fil est activée.

ETAPE 6 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Serveurs RADIUS

Dans l'onglet, vous pouvez effectuer les opérations suivantes :

- Configurer un serveur RADIUS local pour les clients sans fil, ajouter des utilisateurs au WLAN et configurer les mots de passe des utilisateurs, ou
- Activer et configurer un serveur RADIUS externe pour le suivi et l'identification des clients sans fil

Les options de configuration du serveur RADIUS (remote authentication dial-in user service) ne sont accessibles que si l'UC500 dispose d'un point d'accès intégré ou si le site client présente un contrôleur LAN sans fil.

Configurez les paramètres du serveur RADIUS selon la description fournie dans le tableau et cliquez sur **Appliquer** ou **OK**.

Colonne	Description
Nom de l'hôte	Sélectionnez un nom d'hôte dans la liste déroulante.
Serveur RADIUS externe	
Activer serveur RADIUS externe	Lorsque cette option est cochée, activez la configuration du serveur RADIUS externe de telle sorte à permettre l'identification des clients sans fil.
Adresse IP	Adresse IP du serveur RADIUS externe.
Code secret	Clé secrète partagée que le contrôleur WLAN ou le point d'accès utilise pour communiquer avec le serveur RADIUS externe.
Port d'authentification	Numéro de port pour l'identification du serveur RADIUS. 1812 est la valeur par défaut.
Port de gestion	Numéro de port pour la gestion du serveur RADIUS. 1813 est la valeur par défaut.
Serveur RADIUS local	
Activer le serveur RADIUS local	Lorsque cette option est cochée, vous activez la configuration du serveur RADIUS local de telle sorte à permettre l'identification des clients sans fil.
Code secret	Clé secrète partagée que le contrôleur WLAN ou le point d'accès utilise pour communiquer avec le serveur RADIUS local.
Utilisateurs	Nom d'utilisateur et mot de passe pour chaque client permettant une authentification à l'aide du serveur RADIUS local. Cliquez sur **Ajouter** pour ajouter une nouvelle ligne au tableau et introduire un nom d'utilisateur et un mot de passe.

Colonne	Description
Adresses MAC	Adresses MAC des clients permettant une authentification à l'aide du serveur RADIUS local. Cliquez sur **Ajouter** pour ajouter une nouvelle ligne au tableau et introduire l'adresse MAC au format xxxx.xxxx.xxxx.xxxx. Par exemple : 105b.aaab.99ac.0056

Paramètres du point d'accès

Configurez les paramètres du point d'accès selon la description fournie dans le tableau et cliquez sur **Appliquer** ou **OK**.

Paramètre	Description
Paramètres de canal La sélection des canaux radio disponibles est définie par votre domaine de gestion.	
Canal	Sélectionnez le canal radio à utiliser pour ce point d'accès. Lorsque la valeur Fréquence la moins sollicitée est sélectionnée pour ce canal, le périphérique recherche le canal radio le moins saturé et le sélectionne. Le périphérique effectue la recherche à la mise sous tension et dès que les paramètres sont modifiés. Vous pouvez aussi sélectionner des paramètres définis dans le menu déroulant Canal.
Paramètres du mode Mondial	
Activer le Mode Mondial Vous pouvez paramétrer le périphérique sans fil pour qu'il soit compatible avec le mode Mondial. Lorsque vous activez le mode Mondial, le périphérique sans fil ajoute des données de porteuse de voie à sa balise. Les périphériques clients en mode Mondial reçoivent les données de porteuse de voie et adaptent automatiquement leurs réglages. Par exemple, un périphérique client utilisé essentiellement au Japon utilisera le mode Mondial pour adapter les paramètres de canal et d'alimentation lorsqu'il rejoint un réseau en Italie.	

Paramètre	Description
Pays	Sélectionnez le pays principal pour le point d'accès.
Placement	Sélectionnez Intérieur, Extérieur ou Les deux pour désigner la position du point d'accès.

Niveau d'alimentation

Paramètres d'alimentation permettant de définir la puissance de la transmission radio.

La valeur par défaut est la plus élevée acceptée au sein de votre domaine de gestion. Les restrictions gouvernementales définissent la puissance maximale autorisée propre aux périphériques radio. Ce paramètre doit respecter les normes en vigueur pour le pays où vous utilisez le périphérique. Pour réduire les interférences, limitez la portée de votre point d'accès. Pour conserver la puissance, sélectionnez un paramètre inférieur.

Pour une radio 802.11g, la puissance de transmission se répartit entre l'Alimentation de l'émetteur CCK (dBm) et l'Alimentation de l'émetteur OFDM (dBm). Les paramètres d'alimentation peuvent être exprimés en mW ou en dBm selon la radio configurée. Le tableau de conversion de puissance (voir **Tableau de conversion de puissance, page 223**) permet la conversion en mW et dBm.

Puissance de l'émetteur CCK (dBm)	La modulation CCK est utilisée par la norme 802.11g pour les basses fréquences. Dans la plupart des cas, vous sélectionnerez la valeur maximale. Les valeurs disponibles oscillent entre 3 et 17 dBm.
Puissance de l'émetteur OFDM (dBm)	La modulation OFDM est utilisée par la norme 802.11g pour les débits de données élevés (plus de 20 Mbps). Dans la plupart des cas, vous sélectionnerez la valeur maximale. Les valeurs disponibles oscillent entre 3 et 17 dBm.
Alimentation client (dBm)	L'alimentation client définit le niveau de puissance maximal autorisé sur les périphériques clients associés au point d'accès. Lorsqu'un périphérique client s'associe au point d'accès, celui-ci envoie le paramètre de puissance maximale au client. Dans la plupart des cas, vous sélectionnerez la valeur maximale. Les valeurs disponibles oscillent entre 3 et 17 dBm.

Paramètre	Description
Paramètres d'antenne (périphériques UC520 et UC540 sans fil uniquement) Veillez à ne modifier ces paramètres d'antenne que si l'Assistance Cisco vous demande de le faire. Les dispositifs UC520 et UC540 sans fil ne disposent que d'une seule antenne.	
Antenne de réception	Pour les dispositifs UC520 et UC540 sans fil, le paramètre Antenne de réception doit être défini sur la valeur "**Primaire**t".
Antenne de transmission	Pour les dispositifs UC520 et UC540 sans fil, le paramètre Antenne de transmission doit être défini sur la valeur "**Primaire**t".

Tableau de conversion de puissance

Conversion approximative en nW et dBm																					
dBm	-1	2	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
mW	1	2	3	4	5	6	8	10	12	15	20	25	30	40	50	60	80	100	125	150	200	250

Créer ou modifier un SSID de WLAN

Cette fenêtre s'affiche lorsque vous cliquez sur **Créer** ou **Modifier** dans la fenêtre WLAN (SSID). Utilisez cette fenêtre pour créer un nouveau SSID et pour définir les paramètres de sécurité pour l'accès sans fil.

Les paramètres de la fenêtre WLAN (SSID) varient en fonction du point d'accès que vous configurez :

- **Créer ou modifier un SSID pour les points d'accès Cisco AP541N**
- **Créer ou modifier un SSID les SSID pour les points d'accès Cisco AP521 ou UC500**

Créer ou modifier un SSID pour les points d'accès Cisco AP541N

Pour créer un nouvel SSID pour un point d'accès Cisco AP541N, suivez les étapes suivantes :

ETAPE 1 Configurez les paramètres de base pour le SSID de l'AP541N selon les indications du tableau suivant.

Paramètre	Description
SSID	Dans le champ SSID, entrez un SSID. Le SSID peut contenir jusqu'à 32 caractères alphanumériques. Les guillemets (") ne sont pas autorisés.
Diffuser le SSID	Indiquez si vous souhaitez ou non que l'AP541N diffuse ou non le SSID. La diffusion du SSID est désactivée par défaut. Lorsque la diffusion du SSID est désactivée, le nom du réseau ne s'affiche pas dans la liste des réseaux disponibles sur le client. Le nom doit donc être correctement configuré sur le client afin qu'il puisse se connecter. Il suffit de désactiver la diffusion du SSID pour éviter toute connexion accidentelle des clients sur votre réseau. Cela n'empêche toutefois pas aux pirates de tenter de se connecter ou de surveiller le trafic non chiffré. En annulant la diffusion du SSID, vous offrez un niveau de protection minimal à un réseau exposé (réseau invité) dont le but est de faciliter l'accès aux clients et où aucune donnée sensible ne circule.
VLAN	Entrez l'ID du VLAN associé à ce SSID. Vous pouvez entrer des valeurs comprises entre 1 et 4094. Le VLAN par défaut pour le trafic vocal est le VLAN100 alors que le VLAN par défaut pour le trafic de données est le VLAN1. CCA ne vérifie pas si le VLAN existe sur le réseau. Vous devez donc veiller à introduire un identifiant de VLAN valable dans ce champ.

ETAPE 2 Dans la rubrique **Sécurité Paramètres** de cette fenêtre, sélectionnez le type de sécurité à utiliser pour ce SSID et configurez les paramètres supplémentaires nécessaires.

Les paramètres varient en fonction du type de sécurité sélectionné. Pour plus d'informations sur chaque type de protection et sur les paramètres associés, voir **Options de sécurité sans fil pour les périphériques AP541N, page 226**.

ETAPE 3 Sélectionnez le **type d'authentification MAC**.

Paramètre	Description
Désactivé	Ne pas utiliser l'authentification MAC.
Local	Utiliser la liste d'authentification MAC définie sous l'onglet Authentification MAC de la fenêtre Sans fil (SSID). Voir la rubrique **Authentification MAC, page 216**.
Radius	utiliser la liste Authentification MAC définie sur le serveur RADIUS externe.

ETAPE 4 Cliquez sur **OK** ou **Appliquer**.

Créer ou modifier un SSID les SSID pour les points d'accès Cisco AP521 ou UC500

Pour créer ou modifier les SSID pour les points d'accès Cisco AP521 et les points d'accès intégrés UC500, suivez les étapes suivantes :

ETAPE 1 Dans le champ **SSID**, entrez un SSID. Le SSID peut contenir jusqu'à 32 caractères alphanumériques.

ETAPE 2 Cochez **Broadcast dans une radiobalise** si vous souhaitez diffuser le SSID de sorte que les périphériques dépourvus de SSID puissent entrer en liaison avec le point d'accès autonome. Un seul SSID peut être inclus dans une radiobalise (SSID invité).

ETAPE 3 Dans le champ **VLAN**, introduisez ou sélectionnez l'identifiant du VLAN auquel vous souhaitez associer le SSID.

Si vous affectez un VLAN à un SSID, vous devez affecter un VLAN à chaque SSID. Il n'est pas possible que certains SSID soient affectés à des VLAN et d'autres à *aucun*.

ETAPE 4 Cochez la case **VLAN natif** si vous souhaitez que le VLAN soit le **VLAN natif**.

ETAPE 5 Dans la zone Paramètres de sécurité, sélectionnez les paramètres de sécurité dans la liste **Sécurité**. Les autres options de cette fenêtre dépendent de votre choix.

Vous pouvez sélectionner **Pas de protection**, **WEP**, **EAP**, **LEAP**, **WPA**, **WPA-PSK**, **WPA2**,**WPA2-PSK**, **MAC** ou **MAC et EAP**.

Voir **Options de sécurité sans fil pour les périphériques UC500W et AP521, page 230** pour une description de chacun des paramètres.

Configuration Assistant sélectionne automatiquement le type de chiffrement et d'authentification en fonction des critères de protection sélectionnés.

ETAPE 6 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Options de sécurité sans fil pour les périphériques AP541N

Cette rubrique décrit les options de sécurité sans fil et les paramètres connexes pour les points d'accès AP541N.

Aucun

Si vous sélectionnez l'option **Aucun** comme mode de sécurité, aucun paramètre supplémentaire ne doit être défini. Les données transférées vers ou à partir de ce point d'accès ne sont pas chiffrées et aucune identification n'est effectuée. Ce mode peut être utile lors de la configuration initiale du réseau ou lors du dépannage. Elle est cependant déconseillée lors de l'utilisation du réseau interne car il n'est pas sûr.

WEP statique

Le paramètre de sécurité **WEP statique** nécessite que le point d'accès autonome et le périphérique client (périphérique se connectant au périphérique sans fil tel qu'un ordinateur portable ou de bureau) partagent la même clé WEP afin de faire en sorte que les échanges demeurent confidentiels.

Le WEP statique n'est pas le mode le plus sûr, mais il offre plus de protection que l'option Aucun (texte brut).

Si l'option **WEP statique** est sélectionnée, configurez les paramètres suivants.

Paramètre	Description
Chiffrement	Lecture seule. Le chiffrement AES est utilisé.
Authentification	Lecture seule. Le chiffrement "network-eap" est utilisé.

Paramètre	Description
Longueur de la clé	Sélectionnez une clé à 64 ou 128 bits.
Type de clé	Sélectionnez l'option **ASCII** ou **HEX** (hexadécimal).
Key	Vous pouvez définir jusqu'à quatre clés WEP différentes. Pour chaque clé, entrez une suite de caractères. Utilisez le même nombre de caractères pour chaque clé. Il s'agit des clés WEP partagées par les postes utilisant le PA. Les clés introduites dépendent du type de clé sélectionné. **ASCII**. Comprend des lettres majuscules ou minuscules, des chiffres et des symboles tels que @ et #. **Hex**. Comprend des chiffres compris entre 0 et 9 et les lettres comprises entre A et F. Le nombre de caractères introduits dans les champs Clé dépendent de la longueur de la clé et du type de clé sélectionné. Par exemple, si vous utilisez une clé ASCII à 128 bits, la clé WEP doit contenir 13 caractères.

WEP dynamique

La fonction WEP dynamique permet de créer des clés dynamiques actualisées périodiquement.

Ce mode nécessite l'utilisation d'un serveur RADIUS externe afin d'identifier les utilisateurs. L'AP nécessite un serveur RADIUS compatible avec le protocole EAP tel que Microsoft Internet Authentication Server. Pour utiliser des clients Windows, le serveur d'authentification doit prendre en charge les protocoles Protected EAP (PEAP) et MSCHAP V2.

Si l'option WEP dynamique est sélectionnée, configurez les paramètres suivants.

Paramètre	Description
Chiffrement	Lecture seule. Le chiffrement AES est utilisé.
Authentification	Lecture seule. Le chiffrement "network-eap" est utilisé.

Paramètre	Description
Serveur actif	Affiche le serveur RADIUS actuellement utilisé. Vous pouvez mettre à jour manuellement le serveur en sélectionnant un autre serveur dans la liste déroulante. **REMARQUE** Le serveur actif n'est pas conservé au terme d'un redémarrage. Le premier serveur RADIUS configuré est sélectionné au redémarrage.
Fréquence d'actualisation de la clé de diffusion	Entrez une valeur pour définir la fréquence d'actualisation de la clé de diffusion pour les clients associés à cet SSID. Vous pouvez entrer des valeurs comprises entre 1 et 86400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.
Fréquence d'actualisation de la clé de session	Entrez une valeur pour définir la fréquence à laquelle le PA actualisera les clés de session (unicast) pour chaque client associé à cet SSID. La plage disponible est comprise entre 0 et 86400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.

WPA Personal

WPA Personal est un protocole Wi-Fi Alliance IEEE 802.11i comprenant un chiffrement AES-CCMP et TKIP. La version personnelle de WPA utilise une clé partagée (au lieu du protocole IEEE 802.1X) et la norme EAP comme pour le mode de sécurité WPA Enterprise. La clé partagée (PSK) est utilisée pour le contrôle initial des autorisations.

Ce mode de protection est rétrocompatible pour les clients sans fil prenant en charge le WPA d'origine.

Si l'option **WPA Personal** est sélectionnée, configurez les paramètres suivants.

Paramètre	Description
Chiffrement	Lecture seule. TKIP, AES-CCM IP est utilisé.
Authentification	Lecture seule. Le chiffrement "open-eap, network-eap" est utilisé.

Paramètre	Description
Key	Entrez la clé partagée pour la protection WPA Personal. La clé peut être composée de 8 à 63 caractères. Les caractères acceptés sont les lettres majuscules ou minuscules, des chiffres de 0 à 9 et des symboles tels que @ et #.
Fréquence d'actualisation de la clé de diffusion	Entrez une valeur comprise entre 0 et 86400 secondes pour définir la fréquence d'actualisation de la clé de diffusion (groupe) pour les clients qui y sont associés. La valeur 0 indique que la clé de diffusion n'est pas actualisée.

WPA Enterprise

WPA Enterprise avec RADIUS est une application de la norme Wi-Fi Alliance IEEE 802.11i qui comprend les mécanismes CCMP (AES) et TKIP. Le mode WPA Enterprise nécessite l'utilisation d'un serveur RADIUS externe afin d'identifier les utilisateurs.

Ce mode de protection est rétrocompatible avec les clients sans fil prenant en charge le protocole WPA d'origine.

Si l'option WPA Enterprise est sélectionnée, configurez les paramètres suivants.

Paramètre	Description
Chiffrement	Lecture seule. Les valeurs TKIP et AES-CCMP sont sélectionnées. Lorsque les valeurs TKIP et CCMP sont sélectionnées, les clients configurés pour utiliser la fonction WPA avec RADIUS doivent répondre à l'un des critères suivants : ▪ Une adresse IP RADIUS TKIP valable et une clé RADIUS ▪ Une adresse IP CCM (AES) valable et une clé RADIUS
Serveur actif	Affiche le serveur RADIUS actuellement utilisé. Vous pouvez mettre à jour manuellement le serveur en sélectionnant un autre serveur dans la liste déroulante. **REMARQUE** Le serveur actif n'est pas conservé au terme d'un redémarrage. Le premier serveur RADIUS configuré est sélectionné au redémarrage.

Paramètre	Description
Fréquence d'actualisation de la clé de diffusion	Entrez une valeur pour définir la fréquence d'actualisation de la clé de diffusion (groupe) pour les clients associés à ce PA. Vous pouvez entrer des valeurs comprises entre 1 et 86400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.
Fréquence d'actualisation de la clé de session	Entrez une valeur pour définir la fréquence à laquelle le PA actualisera les clés de session (unicast) pour chaque client associé. La plage disponible est comprise entre 0 et 86400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.

Options de sécurité sans fil pour les périphériques UC500W et AP521

Cette rubrique décrit les options de sécurité sans fil et les paramètres connexes pour les points d'accès AP521 et les plateformes UC500 disposant d'un point d'accès intégré.

Pas de protection

Il s'agit de l'option la moins sûre. Sélectionnez-la uniquement si le SSID est utilisé dans un lieu public (SSID invité) et associez-le à un VLAN limitant l'accès à votre réseau. Il n'existe aucun cryptage et l'authentification est de type **authentification ouverte**.

WEP

Ce paramètre de sécurité nécessite que le point d'accès autonome et le périphérique client (périphérique se connectant au périphérique sans fil tel qu'un ordinateur portable ou de bureau) partagent la même clé **WEP** afin de faire en sorte que les échanges demeurent confidentiels. Le type de chiffrement est WEP et le type d'authentification est **authentification ouverte**.

Pour définir ce type de protection, procédez comme suit :

ETAPE 1 Entrez une phrase de passe dans le champ **Phrase de passe** et sélectionnez le chiffrement dans la liste.

ETAPE 2 Cliquez sur **Générer**. Le champ qui se trouve à proximité de la liste **Clé** est rempli automatiquement. Vous pouvez modifier la clé en sélectionnant 1, 2, 3 ou 4 dans la liste **Clé**. La valeur par défaut est 1.

EAP

Le système de protection active l'authentification IEEE 802.1X et nécessite l'introduction de l'adresse IP et de la phrase secrète pour le serveur **RADIUS**. Le type de chiffrement est **WEP** dynamique et le type d'authentification est **authentification ouverte avec EAP**.

Si vous optez pour la protection EAP, les clients sans fil doivent utiliser les paramètres EAP (par exemple : EAP-TLS, EAP-FAST ou PEAP). Les clients sans fil ne peuvent pas utiliser les paramètres LEAP.

Pour définir ce type de protection, procédez comme suit :

ETAPE 1 Entrez l'adresse IP du serveur RADIUS.

ETAPE 2 Entrez la phrase secrète qui sera utilisée par le point d'accès autonome lors de la communication avec le serveur RADIUS.

LEAP

Le système de protection active l'authentification IEEE 802.1X et nécessite l'introduction de l'adresse IP et de la phrase secrète pour le serveur **RADIUS**. Le type de chiffrement est WEP dynamique et le type d'authentification est **authentification ouverte avec EAP** ou **EAP réseau**.

Remarques

- Si vous optez pour la protection LEAP, les clients sans fil doivent utiliser les paramètres LEAP.
- Configuration Assistant active à la fois l'authentification ouverte avec EAP et EAP réseau afin de permettre aux périphériques clients Cisco ou non d'entrer en liaison avec le point d'accès autonome grâce au même SSID que celui qui est utilisé pour l'authentification 802.1x.

Pour définir ce type de protection, procédez comme suit :

ETAPE 1 Entrez l'adresse IP du serveur RADIUS.

ETAPE 2 Entrez la phrase secrète qui sera utilisée par le point d'accès autonome lors de la communication avec le serveur RADIUS.

WPA

Ce paramètre est plus sûr par rapport à EAP. Il permet une authentification **WPA** et nécessite l'introduction de l'adresse IP et de la phrase secrète pour le serveur RADIUS. Les périphériques clients qui entrent en contact avec le point d'accès autonome par le biais de ce SSID doivent prendre en charge le WPA. Le type de chiffrement est **TKIP** et le type d'authentification est **authentification ouverte avec EAP** ou **EAP réseau**.

Configuration Assistant active à la fois l'**authentification ouverte avec EAP** et **EAP réseau** afin de permettre aux périphériques clients Cisco ou non d'entrer en liaison avec le point d'accès autonome grâce au même SSID que celui qui est utilisé pour l'authentification 802.1x.

Pour définir ce type de protection, procédez comme suit :

ETAPE 1 Entrez l'adresse IP du serveur RADIUS.

ETAPE 2 Entrez la phrase secrète qui sera utilisée par le point d'accès autonome lors de la communication avec le serveur RADIUS.

WPA-PSK

Sélectionnez ce critère de sécurité si vous souhaitez utiliser le chiffrement WPA sans avoir accès au serveur RADIUS. Le point d'accès autonome et le périphérique client doivent partager la même **WPA-PSK**. La clé peut être composée de 8 à 63 caractères. Le type de chiffrement est **TKIP** dynamique et le type d'authentification est **WPA-PSK**.

Pour activer cette protection, entrez une clé dans le champ **Clé partagée WPA**.

WPA2

Ce paramètre est plus sûr que WPA. Il permet une authentification **WPA2** et nécessite l'introduction de l'adresse IP et de la phrase secrète pour le serveur RADIUS. Les périphériques clients qui entrent en contact avec le point d'accès autonome par le biais de ce SSID doivent prendre en charge le WPA2. Le type de chiffrement est **AES CCMP** et le type d'authentification est **authentification ouverte avec EAP** ou **EAP réseau**.

Configuration Assistant active à la fois l'**authentification ouverte avec EAP** et **EAP réseau** afin de permettre aux périphériques clients Cisco ou non d'entrer en liaison avec le point d'accès autonome grâce au même SSID que celui qui est utilisé pour l'authentification 802.1x.

Pour définir ce type de protection, procédez comme suit :

ETAPE 1 Entrez l'adresse IP du serveur RADIUS.

ETAPE 2 Entrez la phrase secrète qui sera utilisée par le point d'accès autonome lors de la communication avec le serveur RADIUS.

WPA2-PSK

Sélectionnez ce critère de sécurité si vous souhaitez utiliser le chiffrement WPA2 sans avoir accès au serveur RADIUS. Le point d'accès autonome et le périphérique client doivent partager la même clé WPA2-PSK. La clé peut être composée de 8 à 63 caractères. Le type de chiffrement est **AES CCMP** et le type d'authentification est **WPA-PSK**.

Pour activer cette protection, entrez une clé dans le champ **Clé partagée WPA2** .

MAC

Sélectionnez ce critère de sécurité si vous souhaitez authentifier les périphériques clients à l'aide d'une identification MAC.

Il n'existe aucun cryptage et le type d'authentification est une authentification ouverte.

Pour définir ce type de protection, procédez comme suit :

ETAPE 1 Entrez l'adresse IP du serveur RADIUS.

ETAPE 2 Entrez la phrase secrète qui sera utilisée par le point d'accès autonome lors de la communication avec le serveur RADIUS.

MAC et EAP

Sélectionnez ce critère de sécurité si vous souhaitez authentifier les périphériques clients à l'aide d'une combinaison de l'identification MAC et EAP. Les périphériques clients qui entrent en contact avec le point d'accès par le biais de l'authentification ouverte IEEE 802.11 tenteront d'abord une authentification MAC. En cas de réussite, le périphérique client accède au réseau.Si le client utilise également l'authentification EAP, il tentera une authentification EAP. En cas d'échec de l'authentification MAC, le point d'accès attend l'authentification EAP.

Le type de cryptage est WEP dynamique et les types d'authentification sont authentification ouverte avec EAP et EAP réseau.

Configuration Assistant active à la fois l'**authentification ouverte avec EAP** et **EAP réseau** afin de permettre aux périphériques clients Cisco ou non d'entrer en liaison avec le point d'accès autonome grâce au même SSID que celui qui est utilisé pour l'authentification 802.1x.

Pour définir ce type de protection, procédez comme suit :

ETAPE 1 Entrez l'adresse IP du serveur RADIUS.

ETAPE 2 Entrez la phrase secrète qui sera utilisée par le point d'accès autonome lors de la communication avec le serveur RADIUS.

Fenêtre Résolution du VLAN invité

La fenêtre Résolution du VLAN invité s'affiche lorsqu'un VLAN invité est configuré sur un commutateur ESW 500 et si vous ouvrez la fenêtre WLAN (SSID) alors que le SR520 est défini comme hôte.

Cliquez sur **Résoudre** pour créer le VLAN invité sur le SR 520. Cliquez sur Annuler si vous ne souhaitez pas que CCA crée le VLAN invité sur le SR 520.

Convertir en LAP (Lightweight Access Point - point d'accès léger)

Cette fenêtre s'affiche lorsque vous sélectionnez **Configurer** > **Sans fil** > **Convertir en LAP** dans la barre de fonctions.

Vous pouvez convertir un **point d'accès autonome** en **point d'accès léger**. Le point d'accès léger s'associe à un contrôleur LAN sans fil. Le contrôleur assure la gestion de la configuration, du microprogramme et des transactions de commande telles que les identifications 802.1x. De plus, tout le trafic des données sans fil est acheminé par le contrôleur.

Pour convertir les points d'accès autonomes en point d'accès léger, sélectionnez et utilisez la fenêtre Convertir en LAP - voir **Convertir en LAP (Lightweight Access Point - point d'accès léger), page 235**). Vous pouvez sélectionner plusieurs points d'accès autonomes et les mettre à jour en une seule fois.

CCA ne prend pas en charge la conversion des points d'accès LAP en points d'accès autonomes. CCA ne pourra pas gérer les points d'accès LAP convertis en PA autonomes à l'aide de la ligne de commande Cisco IOS.

Ce tableau explique les paramètres de la fenêtre Convertir en LAP.

Paramètre	Explication
Périphérique	Affiche les icônes du périphérique et les noms d'hôte.
Convertir	Indique si le périphérique est sélectionné pour la **Conversion**.
Type de périphérique	Affiche le type de périphérique.
Version actuelle	Affiche la version de Cisco IOS.
Nom de l'image de récupération	Affiche le nom du fichier tar Cisco IOS repris dans la fenêtre Paramètres de conversion. Seul le nom du fichier s'affiche. Le chemin n'est pas indiqué.
État de conversion	Affiche l'état de la conversion et les messages de progression. Reportez-vous à la fenêtre État de conversion pour obtenir de plus amples détails.

Adresse IP	Affiche le paramètre relatif à l'adresse IP introduit dans la fenêtre Paramètres de conversion (statique ou DHCP).
Nom de l'hôte	Affiche le paramètre relatif au nom de l'hôte introduit dans la fenêtre Paramètres de conversion (Conserver ou Ne pas conserver).

Suivez les consignes suivantes pour convertir les points d'accès autonome en points d'accès légers :

ETAPE 1 Téléchargez les fichiers tar Cisco IOS que vous souhaitez utiliser pour convertir le point d'accès autonome.

ETAPE 2 Sélectionnez un ou plusieurs points d'accès autonomes.

ETAPE 3 Cliquez sur **Paramètres de conversion**.

ETAPE 4 Complétez les données de la fenêtre **Paramètres de conversion** et cliquez sur **OK** pour sauvegarder les données. Voir la rubrique **Paramètres de conversion., page 237**.

ETAPE 5 Cochez la case **Convertir** à côté de chaque périphérique que vous souhaitez convertir.

ETAPE 6 Cliquez sur **Convertir** pour commencer la mise à niveau.

L'image en cours sera supprimée et la nouvelle image sera téléchargée. Vous pouvez enregistrer l'ancienne image à l'aide de la ligne de commande.

ETAPE 7 Cliquez sur **État** pour afficher la fenêtre État de conversion. Cette fenêtre affiche la progression de la conversion. Voir la rubrique **État de conversion, page 238**.

Au terme du processus de conversion, une fenêtre de confirmation s'affiche. Les messages d'état indiquent les points d'accès convertis avec succès et les échecs.

ETAPE 8 Toutes les modifications sont automatiquement enregistrées dans la mémoire flash. Une minute plus tard, les périphériques sont rechargés et la nouvelle image s'exécute. Vous pouvez alors fermer la fenêtre Convertir en LAP.

Lors du rechargement, la liaison vers le périphérique est perdue.

Paramètres de conversion.

Cette fenêtre s'affiche lorsque vous sélectionnez un ou plusieurs **point d'accès autonome** dans la fenêtre Convertir en LAP et que vous cliquez sur **Paramètres de conversion**.

Sélectionnez l'option **Adresse IP DHCP** si vous souhaitez que le contrôleur WLAN affecte une nouvelle adresse IP au point d'accès léger après la conversion.

Sélectionnez l'option **Conserver le nom d'hôte** si vous souhaitez conserver le nom d'hôte pour le point d'accès léger après la conversion.

Choisissez **Standard** dans la liste **Mode** pour utiliser une image de conversion enregistrée localement. Sinon, sélectionnez **Serveur TFTP** distant.

Si vous sélectionnez **Standard**, entrez le nom de fichier de l'image de conversion dans le champ **Image de conversion**. Vous pouvez cliquer sur **Parcourir** pour trouver le fichier.

Si vous avez sélectionné **Serveur TFTP distant**, procédez comme suit :

ETAPE 1 Dans le champ **Image de conversion**, entrez le chemin complet et le nom du fichier pour l'image de conversion.

ETAPE 2 Dans le champ **Adresse IP du serveur TFTP**, introduisez l'adresse IP du serveur TFTP.

Pour réaliser des conversions groupées, votre serveur TFTP doit gérer plusieurs requêtes et sessions en même temps.

ETAPE 3 Dans le champ **Nom de domaine**, introduisez le nom de domaine.

ETAPE 4 Dans le champ **Adresse IP DNS**, entrez l'adresse **DNS**.

ETAPE 5 Cliquez sur **OK** pour enregistrer les modifications. Le nouveau paramétrage s'affiche dans la fenêtre Convertir en LAP.

État de conversion

Cette fenêtre s'affiche lorsque vous sélectionnez un ou plusieurs **point d'accès autonome** dans la fenêtre Convertir en LAP et que vous cliquez sur **État**. Cette fenêtre présente les messages détaillés dès leur création par le point d'accès autonome au cours de la conversion.

Ce tableau explique les messages d'état de la conversion.

Message	Explication
Cliquez sur le bouton **Paramètres de conversion** pour continuer.	La fenêtre Paramètres de conversion doit être complétée avant de procéder à la mise à jour du périphérique.
Cliquez sur le bouton **Convertir** pour mettre le périphérique à niveau.	Tous les paramètres sont définis pour la conversion du périphérique.
Détection de la taille totale de la mémoire flash.	Le processus de conversion vérifie l'espace disponible pour la conversion du périphérique.
Extraction du fichier d'informations à partir de l'image tar.	Le fichier image Cisco IOS extrait le fichier d'information.
Lecture du fichier info du fichier image tar.	Configuration Assistant lit les informations du fichier image (.tar) Cisco IOS pour obtenir des détails sur l'image Cisco IOS.
Le rechargement a commencé pour le périphérique.	Le périphérique est en cours de rechargement après une mise à jour réussie du logiciel. Même au terme du chargement, ce message s'affiche jusqu'à ce que la fenêtre ait été actualisée.
La conversion du périphérique a réussi.	La conversion a réussi.
Échec de la conversion du périphérique.	La conversion a échoué. Voir la fenêtre Détails pour de plus amples informations.
Conversion du périphérique en cours.	La conversion des périphériques a commencé.

Message	Explication
Conversion de périphérique annulée.	La conversion a été annulée.
Chargement de l'image.	L'image est en cours de chargement sur le périphérique.
Vérification de l'image IOS.	Le périphérique vérifie l'image.

Si l'espace disponible sur le périphérique est insuffisant pour l'installation d'une nouvelle image, un message contenant un lien vers la fenêtre Gestion des fichiers s'affiche. Vous pouvez utiliser la fenêtre Gestion des fichiers pour assurer la gestion de vos systèmes de fichiers et pour supprimer si nécessaire les anciennes images afin de libérer de l'espace pour les nouvelles.

Lorsque vous avez terminé, cliquez sur **OK**.

Configuration du contrôleur WLAN

Les rubriques de ce chapitre traitent des paramètres de configuration relatifs aux contrôleurs WLAN :

Configuration des interfaces sans fil pour un contrôleur WLAN

Si votre système comprend un contrôleur WLAN, sélectionnez l'option **Configurer** > **Interfaces sans fil** dans la barre de fonctions.

Vue d'ensemble

Vous pouvez configurer des interfaces sans fil dynamiques sur un contrôleur WLAN. Les interfaces sans fil dynamiques sont analogues aux VLAN pour les clients LAN sans fil. Un contrôleur peut prendre en charge jusqu'à huit interfaces dynamiques (VLAN).

Une interface sans fil présente plusieurs paramètres dont l'identifiant de VLAN, le port, l'adresse IP, le masque de sous-réseau, la passerelle par défaut (pour le sous-réseau IP) et le serveur DHCP.

Utilisez cette fenêtre pour afficher tous les paramètres de l'interface sans fil sur le contrôleur WLAN et pour configurer les interfaces dynamiques (définies par l'utilisateur) sur le contrôleur WLAN.

Procédures

Ce tableau explique les colonnes de la fenêtre Interfaces sans fil.

Colonne	Explication
Nom	Nom de l'interface sans fil, dont les interfaces dynamiques et statiques (gestion, gestionnaire PA et virtuel)
VLAN	VLAN associé à l'interface sans fil
Port	Numéro de port physique pour l'interface sans fil
Adresse IP	Adresse IP de l'interface sans fil

Procédez comme suit pour configurer une interface sans fil dynamique sur le contrôleur WLAN :

ETAPE 1 Dans la liste **Nom de l'hôte**, sélectionnez le contrôleur WLAN.

ETAPE 2 Pour créer une interface, cliquez sur **Créer** et complétez la fenêtre Créer une interface. Voir la rubrique **Créer une interface, page 241**.

Le contrôleur peut prendre en charge jusqu'à huit interfaces dynamiques.

Pour modifier une configuration, sélectionnez le nom de l'interface sans fil et cliquez sur **Modifier**. Utilisez la fenêtre Modifier l'interface.

Pour supprimer une configuration, sélectionnez le nom de l'interface sans fil et cliquez sur Supprimer.

REMARQUE Vous pouvez modifier et supprimer les interfaces dynamiques uniquement. Vous ne pouvez pas modifier ou supprimer les interfaces statiques.

Pour enregistrer vos modifications et fermer la fenêtre, cliquez sur **OK** dans la fenêtre Interfaces sans fil.

Créer une interface

Cette fenêtre s'affiche lorsque vous sélectionnez **Créer** dans la fenêtre Interfaces sans fil. Utilisez cette fenêtre pour créer une interface sans fil.

ETAPE 1 Dans le champ **Nom** de **l'interface**, introduisez un nom pour l'interface sans fil.

ETAPE 2 Dans le champ **Identifiant de VLAN**, introduisez l'identifiant du VLAN auquel vous souhaitez associer l'interface sans fil.

ETAPE 3 Dans la liste **Port**, sélectionnez un port pour l'interface sans fil.

ETAPE 4 Dans le champ **Adresse IP,** introduisez l'adresse IP de l'interface sans fil.

ETAPE 5 Dans la liste **Masque de sous-réseau**, sélectionnez le masque de sous-réseau pour l'interface sans fil.

ETAPE 6 Dans le champ **Adresse IP de la passerelle**, entrez l'adresse IP de la passerelle par défaut.

ETAPE 7 Dans le champ **Adresse IP du serveur DHCP**, entrez l'adresse IP du serveur DHCP.

ETAPE 8 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Modifier l'interface

Cette fenêtre s'affiche lorsque vous sélectionnez **Modifier** dans la fenêtre Interfaces sans fil. Cette fenêtre vous permet de modifier les paramètres d'une interface sans fil.

Suivez les étapes ci-dessous :

ETAPE 1 Dans le champ **Identifiant de VLAN**, introduisez l'identifiant du VLAN auquel vous souhaitez associer l'interface sans fil.

ETAPE 2 Dans la liste **Port**, sélectionnez un port pour l'interface sans fil.

ETAPE 3 Dans le champ **Adresse IP,** introduisez l'adresse IP de l'interface sans fil.

ETAPE 4 Dans la liste **Masque de sous-réseau**, sélectionnez le masque de sous-réseau pour l'interface sans fil.

ETAPE 5 Dans le champ **Adresse IP de la passerelle**, entrez l'adresse IP de la passerelle par défaut.

ETAPE 6 Dans le champ **Adresse IP du serveur DHCP**, entrez l'adresse IP du serveur DHCP.

ETAPE 7 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Affichage de l'état du client sans fil pour un contrôleur WLAN

Pour afficher l'état des clients sans fil définis sur un contrôleur WLAN, utilisez la fenêtre Clients sans fil.

Ce tableau explique les informations figurant dans les colonnes de cette fenêtre.

Colonne	Explication
Adresse MAC	Adresse MAC du client.

Colonne	Explication
État	État de la liaison du client : ▪ Inactif ▪ En attente ▪ Authentifié ▪ Associé ▪ Actif ▪ Économie d'énergie ▪ Non associé ▪ Exclure ▪ Recherche
Nom PA	Nom du point d'accès léger du client
SSID	SSID du client.
Radio	Type de client : ▪ 802.11a ▪ 802.11 b ▪ 802.11g
Authentifié	État de l'authentification du client (oui ou non)

Cliquez sur **OK** pour fermer la fenêtre.

Configurer les utilisateurs du WLAN

Vous pouvez configurer des utilisateurs sans fil sur un contrôleur WLAN. Vous pouvez aussi configurer les paramètres d'identification et les paramètres de connexion Web.

Les utilisateurs sans fil peuvent être invités ou non (par exemple, les employés).

Les utilisateurs invités ont accès à l'Internet et leur propre réseau sans compromettre la sécurité de votre réseau. Une date d'échéance est définie pour l'accès des utilisateurs invités.

Les utilisateurs non invités profitent d'un accès sécurisé au réseau. Ce type d'utilisateur n'est associé à aucune date d'expiration pour l'accès.

Cette fenêtre vous permet de configurer les utilisateurs sans fil pour un contrôleur WLAN ou afficher les paramètres de celui-ci.

Ce tableau explique les colonnes de la zone Utilisateurs du réseau sans fil (SSID).

Colonne	Explication
Nom d'utilisateur	Nom de l'utilisateur sans fil.
Utilisateur visiteur	État de l'utilisateur visiteur (oui ou non).
SSID	Nom SSID.
Heure de fin	Date d'expiration de l'accès de l'utilisateur invité.
Description	Description de l'utilisateur sans fil.

Procédez comme suit pour configurer les utilisateurs sans fil pour le contrôleur WLAN :

ETAPE 1 Dans la liste **Nom de l'hôte**, sélectionnez le contrôleur WLAN.

ETAPE 2 Pour créer un utilisateur visiteur ou non-visiteur, cliquez sur **Créer** et utilisez la fenêtre Créer un utilisateur WLAN. Voir la rubrique **Créer les utilisateurs du WLAN, page 245**.

ETAPE 3 Pour enregistrer vos modifications et fermer la fenêtre, cliquez sur **OK** dans la fenêtre Utilisateurs du WLAN.

Pour modifier un utilisateur sans fil, sélectionnez le nom d'utilisateur et cliquez sur Modifier. Utilisez la fenêtre Modifier un utilisateur WLAN.

Pour supprimer un utilisateur sans fil, sélectionnez l'utilisateur en question et cliquez sur **Supprimer**.

Les utilisateurs visiteurs sont supprimés automatiquement de la liste des utilisateurs du réseau sans fil lorsque vous ouvrez la fenêtre Utilisateurs du WLAN et que le délai Utilisateur visiteur a expiré. Si la fenêtre Utilisateurs du WLAN est déjà ouverte à la fin du délai prévu pour l'utilisateur et que vous tentez de modifier l'utilisateur visiteur, celui-ci sera supprimé de la liste Utilisateurs du réseau sans fil. Cliquez sur **Créer** pour créer un nouvel utilisateur visiteur.

Pour configurer la page de connexion des utilisateurs sans fil, cliquez sur **Configurer** dans le volet Connexion Web. Voir la rubrique **Connexion Web, page 248**.

Créer les utilisateurs du WLAN

Cette fenêtre s'affiche lorsque vous cliquez sur **Créer** dans la fenêtre Utilisateurs du WLAN. Utilisez cette fenêtre pour créer un utilisateur sans fil.

Vue d'ensemble

Vous pouvez configurer des utilisateurs sans fil sur un contrôleur WLAN. Vous pouvez aussi configurer les paramètres d'identification et les paramètres de connexion Web.

Les utilisateurs sans fil peuvent être invités ou non (par exemple, les employés).

Les utilisateurs invités ont accès à l'Internet et leur propre réseau sans compromettre la sécurité de votre réseau. Une date d'échéance est définie pour l'accès des utilisateurs invités.

Les utilisateurs non invités profitent d'un accès sécurisé au réseau. Ce type d'utilisateur n'est associé à aucune date d'expiration pour l'accès.

Procédures

Suivez les étapes ci-dessous :

ETAPE 1 Dans le champ **Nom d'utilisateur** de l'interface, introduisez un nom pour l'utilisateur sans fil. Vous pouvez introduire jusqu'à 24 caractères alphanumériques.

ETAPE 2 Dans le champ **Mot de passe** de l'interface, introduisez un mot de passe pour l'utilisateur sans fil. Vous pouvez introduire jusqu'à 24 caractères alphanumériques.

ETAPE 3 Dans le champ **Confirmer le mot de passe**, introduisez à nouveau le mot de passe.

ETAPE 4 Dans le champ **Description** de l'interface, introduisez une description pour l'utilisateur sans fil.

ETAPE 5 Si l'utilisateur sans fil n'est pas un visiteur, suivez les consignes suivantes :

a. Annulez la sélection de la case **Utilisateur Visiteur**.

b. Sélectionnez un SSID dans la liste SSID. Seuls les SSID présentant la valeur Web-Auth, WEP, WPA1-PSK ou WPA2-PSK s'affichent.

Si vous devez créer un SSID, cliquez sur **Ajouter un SSID** (prédéfini) pour afficher la fenêtre Ajouter un SSID (prédéfini). Voir la rubrique **Ajouter un SSID, page 247**

ETAPE 6 Si l'utilisateur sans fil n'est pas un visiteur, suivez les consignes suivantes :

a. Cochez la case **Utilisateur Visiteur**.

b. Sélectionnez un SSID dans la liste SSID. Seuls les SSID présentant la valeur Web-Auth s'affichent.

Si vous devez créer un SSID, cliquez sur **Ajouter un SSID** (prédéfini) pour afficher la fenêtre Ajouter un SSID (prédéfini). Voir la rubrique **Ajouter un SSID, page 247**.

ETAPE 7 Dans la zone **Heure de fin**, entrez la date d'expiration en sélectionnant l'année, le mois, le jour et l'heure. La date d'expiration maximale correspond à 30 jours à compter de la date du jour.

Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Modifier les utilisateurs du WLAN

Cette fenêtre s'affiche lorsque vous cliquez sur **Modifier** dans la fenêtre Utilisateurs du WLAN. Utilisez cette fenêtre pour définir les paramètres de l'utilisateur sans fil

Suivez les étapes ci-dessous :

ETAPE 1 Dans le champ **Mot de passe** de l'interface, introduisez un mot de passe pour l'utilisateur sans fil. Vous pouvez introduire jusqu'à 24 caractères alphanumériques.

ETAPE 2 Dans le champ **Confirmer le mot de passe**, introduisez à nouveau le mot de passe.

ETAPE 3 Dans le champ **Description** de l'interface, introduisez une description pour l'utilisateur sans fil.

ETAPE 4 Dans la liste **SSID**, sélectionnez un SSID.

ETAPE 5 Si l'utilisateur est un utilisateur visiteur, modifiez la date d'expiration dans la zone **Heure de fin** en sélectionnant la date et l'heure. La date d'expiration maximale correspond à 30 jours à compter de la date du jour.

ETAPE 6 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Ajouter un SSID

Cette fenêtre s'affiche lorsque vous sélectionnez **Ajouter un SSID** dans le volet SSID de la fenêtre Créer un utilisateur WLAN. Elle vous permet d'appliquer les paramètres SSID prédéfinis au contrôleur WLAN.

Configuration Assistant configure les VLAN et les SSID correspondants en fonction du type de protection défini. Une fois les paramètres du SSID appliqués au contrôleur de WLAN, vous pouvez modifier ou supprimer les WLAN correspondants de la fenêtre WLAN (SSID). Vous pouvez aussi modifier ou supprimer le VLAN correspondant de la fenêtre VLAN.

Procédez comme suit pour ajouter un SSID :

ETAPE 1 Sélectionnez un type de réseau sans fil dans la zone Sélection de WLAN. Les sélections possibles sont les suivantes :

- Données employé (Web-Auth et WPA1-PSK)
- Voix employé (Web-Auth et WPA2-PSK)

Si vous configurez un visiteur, l'option Visiteur (avec identification Web) est sélectionnée.

ETAPE 2 Selon la sélection de WLAN, entrez les données suivantes :

- **VLAN ID (2-1000)** : entrez l'identifiant du VLAN.
- **Nom de VLAN** : pour les réseaux de données, acceptez le nom prédéfini ou entrez un nom différent pour le VLAN. Pour les réseaux de type Voix et Invité, le champ présente un nom de VLAN prédéfini basé sur le type de WLAN sélectionné.
- **Adresse IP** : entrez l'adresse IP pour le VLAN.
- **Masque de sous-réseau** : sélectionnez le masque de sous-réseau pour le VLAN.
- **Adresse IP de la passerelle** : entrez l'adresse IP de la passerelle par défaut.

- **Adresse IP du serveur DHCP** : entrez l'adresse IP du serveur DHCP.
- **SSID** : acceptez le SSID par défaut (en fonction du nom de l'entreprise et de la sélection du WLAN) ou introduisez un SSID différent composé de 32 caractères alphanumériques maximum.
- **Clé partagée WPA1** (pour les réseaux de données) ou **Clé partagée WPA2** (pour les réseaux vocaux) : entrez une clé composée de 8 à 63 caractères.

ETAPE 3 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Connexion Web

Cette fenêtre s'affiche lorsque vous sélectionnez **Configurer** dans le volet Connexion Web de la fenêtre Utilisateurs du WLAN. Elle vous permet de personnaliser le contenu et l'aspect de la page Connexion Web pour les utilisateurs du WLAN.

Vue d'ensemble

La page de connexion est présentée pour la première fois aux utilisateurs Web accédant au WLAN lorsque la fonction d'identification Web est activée. Cisco offre une page de connexion par défaut qui peut être modifiée à l'aide de n'importe quel éditeur de texte HTML. Cependant, les champs Nom d'utilisateur et Mot de passe ne peuvent pas être modifiés et la méthode de validation doit être conservée. Une fois la page personnalisée créée, elle doit être intégrée à un fichier .tar contenant le code de la page et les images souhaitées.

Procédures

Procédez comme suit pour configurer la page de connexion :

ETAPE 1 Dans la liste **Nom de l'hôte**, sélectionnez le contrôleur WLAN.

ETAPE 2 Dans la zone **Authentification Web**, sélectionnez **Interne** ou **Personnalisé**.

ETAPE 3 Suivez les étapes suivantes si vous sélectionnez l'option **Interne** :

a. Dans la zone Logo Cisco, sélectionnez Afficher pour afficher le logo Cisco à la page de connexion ou sélectionnez Masquer pour masquer le logo. La valeur par défaut est Afficher.

b. Dans le champ Adresse de redirection après la connexion, entrez l'adresse vers laquelle l'utilisateur sera redirigé après la connexion. Entrez l'URL au format www.nomsociété.com (n'entrez pas http://) et jusqu'à 254 caractères.

c. Dans le champ Titre, entrez le titre ou une présentation de la page (jusqu'à 127 caractères). Le titre par défaut est "Bienvenue sur le réseau sans fil Cisco".

d. Dans le champ Message, entrez le message (jusqu'à 2047 caractères). Le message par défaut est "Cisco est ravie d'offrir une infrastructure LAN sans fil pour votre réseau. Veuillez vous connecter pour activer le réseau".

Cliquez sur **Définir par défaut** pour utiliser les paramètres par défaut.

ETAPE 4 Suivez les étapes suivantes si vous sélectionnez l'option **Personnalisé** :

a. Dans le champ Adresse IP du serveur TFTP, entrez l'adresse IP du serveur TFTP sur lequel se trouve le fichier utilisé pour l'identification Web personnalisée.

Le serveur TFTP ne peut pas être exécuté sur le même ordinateur que Cisco WCS étant donné que le serveur Cisco WCS et le serveur TFTP utilisent le même port de communication.

b. Dans le champ, **Nombre maximal de tentatives**, entrez le nombre de tentatives du contrôleur WLAN visant à charger le fichier d'identification Web à partir du serveur TFTP en cas d'échec. La valeur par défaut est 3.

c. Dans le champ **Délai d'expiration (en secondes** , entrez le délai d'expiration en secondes. Si le contrôleur WLAN ne peut pas télécharger le fichier au cours de ce délai, le chargement n'a pas lieu.

d. Dans le champ **Chemin de fichier**, entrez le chemin du fichier d'identification Web sur le serveur TFTP. La valeur par défaut est une barre oblique (/).

e. Dans le champ **Nom de fichier**, entrez le nom du fichier à transférer.

f. Cliquez sur **Télécharger** pour télécharger le fichier de connexion personnalisé.

ETAPE 5 Lorsque vous cliquez sur **OK** ou **Appliquer**, le téléchargement débute et le fichier de connexion personnalisé s'applique au périphérique.

Proxy DHCP

Pour configurer un proxy DHCP, sélectionnez **Configurer** > **Proxy DHCP** dans la barre de fonctions.

Le proxy DHCP aide les clients sans fil à obtenir une adresse IP du serveur DHCP. Le contrôleur WLAN obtient une demande de recherche DHCP du client sans fil et envoie la requête au serveur DHCP pour le compte du client sans fil. Lorsque vous activez le proxy DHCP, le contrôleur WLAN se place entre le client sans fil et le serveur DHCP jusqu'à ce que le client sans fil obtienne l'adresse IP.

Vous pouvez activer le proxy DHCP si vous avez configuré l'adresse du serveur DHCP sur tous les VLAN personnalisés pour ce périphérique.

Pour activer le proxy DHCP, procédez comme suit :

ETAPE 1 Sélectionnez un périphérique à configurer dans la liste **Nom de l'hôte**.

ETAPE 2 Cochez la case **Activer le proxy DHCP**.

ETAPE 3 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Tableau de bord pour le contrôleur sans fil

Si vous souhaitez obtenir des informations sur tous les contrôleurs WLAN de la communauté (par exemple, l'état du contrôleur du WLAN, l'état des radios 802.11b/g, le nombre de clients associés à un SSID), ouvrez le Tableau de bord pour le contrôleur sans fil. Cette fenêtre affiche de nombreuses informations sur le contrôleur WLAN, notamment :

- Récapitulatif système
- Informations et statistiques pour le point d'accès
- Statistiques du contrôleur WLAN

Cette fenêtre affiche de nombreuses statistiques relatives au contrôleur WLAN sous les onglets suivants : Système, Résumé du PA, WLAN, Statistiques du WLC et Statistiques du PA. Pour mettre les statistiques à jour, cliquez sur **Actualiser**.

Ce tableau présente les données relatives à la rubrique Système.

Colonne	Explication
Nom du contrôleur	Noms des contrôleurs.

Colonne	Explication
Temps de fonctionnement	Temps écoulé depuis le dernier redémarrage du contrôleur WLAN.
Température	Température interne au boîtier.
CPU	Utilisation totale du processus pour le contrôleur WLAN.
Mémoire	Mémoire totale du processus pour le contrôleur WLAN.

Ce tableau présente les données relatives à la rubrique Résumé du PA.

Colonne	Explication
Nom du contrôleur	Noms des contrôleurs.
Radios 802.11b/g	État des radios (marche / arrêt)
État du PA	État des points d'accès (marche / arrêt)

Ce tableau présente les données relatives à la rubrique WLAN.

Colonne	Explication
Nom du WLAN (nom du contrôleur)	Noms SSID des contrôleurs.
Clients	Nombre de clients associés au SSID.

Ce tableau présente les données relatives à la rubrique Statistiques du WLC. Vous pouvez afficher les données sous forme de totaux ou de pourcentages.

Colonne	Explication
Nom du contrôleur	Noms des contrôleurs.

Colonne	Explication
Paquets reçus sans erreur	Nombre total ou pourcentage des paquets reçus.
Élimination des paquets reçus	Nombre total ou pourcentage des paquets reçus éliminés.
Paquets transmis sans erreur	Nombre total ou pourcentage des paquets envoyés.
Paquets transmis éliminés	Nombre total ou pourcentage des paquets envoyés éliminés.

Ce tableau présente les données relatives à la rubrique Statistiques du PA.

Colonne	Explication
Nom du PA (nom du contrôleur)	Points d'accès associés aux contrôleurs de WLAN.
Décompte des trames de transmission	Nombre total de trames transmises.
Décompte des transmissions échouées	Total des trames non transmises.

Configurer les paramètres du serveur RADIUS pour les contrôleurs WLAN

La fenêtre Configurer les serveurs RADIUS s'affiche lorsque vous cliquez sur **Configurer** dans la zone Serveurs RADIUS de la fenêtre WLAN (SSID) d'un contrôleur WLAN.

Dans cette fenêtre, vous pouvez afficher les paramètres du serveur RADIUS pour le contrôleur WLAN et configurer jusqu'à deux serveurs RADIUS pour le contrôleur WLAN. Le tableau suivant décrit les colonnes de cette fenêtre.

Paramètre	Description
Adresse IP	Adresse IP du serveur RADIUS.
Port auth	Numéro de port pour l'identification du serveur RADIUS.
Priorité	Priorité du serveur RADIUS. Elle indique l'ordre dans lequel les serveurs sont utilisés si l'un des serveurs est inaccessible.
État	État (Activé ou Désactivé) du serveur RADIUS.

Pour configurer les serveurs RADIUS pour le contrôleur WLAN, procédez comme suit :

ETAPE 1 Dans la liste Nom de l'hôte, sélectionnez le contrôleur WLAN.

ETAPE 2 Cliquez sur **Créer** et complétez les paramètres de la fenêtre Créer un serveur RADIUS. Voir la rubrique **Fenêtre Créer un serveur RADIUS**.

Pour modifier l'état du serveur RADIUS, sélectionnez l'adresse IP du serveur RADIUS, cliquez sur **Modifier** et complétez les paramètres dans la fenêtre Modifier le serveur RADIUS. Voir la rubrique **Fenêtre Modifier le serveur RADIUS**.

Pour supprimer un serveur RADIUS configuré, sélectionnez l'adresse IP du serveur RADIUS et cliquez sur **Supprimer**.

Pour enregistrer vos modifications et fermer la fenêtre, cliquez sur **OK** dans la fenêtre Serveur RADIUS.

Fenêtre Créer un serveur RADIUS

Cette fenêtre s'affiche lorsque vous cliquez sur **Créer** dans la fenêtre Configurer le serveur RADIUS. Utilisez cette fenêtre pour définir les paramètres du serveur RADIUS.

Suivez les étapes ci-dessous.

ETAPE 1 Dans le champ **Adresse IP,** introduisez l'adresse IP du serveur RADIUS.

ETAPE 2 Dans le champ **Port auth**, entrez le numéro du port d'identification RADIUS. Le port d'authentification par défaut est le 1812.

ETAPE 3 Dans le champ **Clé secrète (ASCII)**, entrez le code que le contrôleur WLAN devra utiliser pour communiquer avec le serveur RADIUS.

ETAPE 4 Dans le champ **Confirmer la clé**, introduisez à nouveau le code.

ETAPE 5 Dans la liste **Code de priorité du serveur**, sélectionnez la priorité du serveur.

REMARQUE Chaque serveur RADIUS doit utiliser un code de priorité distinct.

ETAPE 6 Dans la liste **État admin**, sélectionnez l'option Activé ou Désactivé.

ETAPE 7 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Fenêtre Modifier le serveur RADIUS

Cette fenêtre s'affiche lorsque vous cliquez sur **Modifier** dans la fenêtre Configurer le serveur RADIUS. Utilisez cette fenêtre pour modifier l'état d'un serveur RADIUS.

Suivez les étapes ci-dessous :

ETAPE 1 Dans la liste **État admin**, sélectionnez l'option Activé ou Désactivé.

ETAPE 2 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

7

Fonctions de sécurité

Cette partie traite de la configuration des fonctions de sécurité de base suivantes :

- **NAT (Traduction d'adresse réseau)**
- **Serveur VPN**
- **Audit de sécurité**
- **Pare-feu et DMZ**
- **Paramètres de sécurité du réseau (commutateurs CE520)**
- **SSL VPN**
- **Système de prévention des intrusions (IPS)**
- **Filtrage d'URL (SR500)**

NAT (Traduction d'adresse réseau)

Pour activer ou désactiver la traduction d'adresse réseau (NAT), sélectionnez l'option **Configurer** > **Sécurité** > **NAT** dans la barre de fonctions.

Dans cette fenêtre, vous pouvez effectuer les opérations suivantes :

- Activer ou désactiver la fonction NAT (Traduction d'adresse réseau)
- Configurer le mappage de ports
- Configurer le transfert des ports

REMARQUE : L'interface utilisateur de la fenêtre NAT et les paramètres de configuration sont différents en fonction de l'affectation des adresses IP.

Pour plus d'informations sur les fonctions NAT et les paramètres de configuration, consultez les rubriques suivantes :

- **Vue d'ensemble**

- Fenêtre NAT (adresses IP affectées par DHCP)
- Fenêtre NAT (IP statique ou PPPoE avec IP statique)

Vue d'ensemble

Lorsqu'elle est active pour une interface, la fonction NAT (traduction d'adresses de réseau) assure le mappage des adresses IP privées de votre réseau local vers une adresse IP du réseau public en fonction d'un groupe d'adresses IP publiques défini.

Vous avez besoin d'une adresse IP valable, enregistrée, unique et publique pour vous connecter à l'Internet. Généralement, une entreprise ne dispose pas de suffisamment d'adresses IP publiques pour affecter une adresse IP publique à chaque client. Sans la fonction NAT, votre réserve d'adresses IP publiques serait insuffisante. La structure interne de votre réseau local s'affiche sur chaque client du réseau public. La fonction NAT vous permet d'utiliser une adresse IP publique afin d'offrir un accès Internet à plusieurs clients composant votre LAN.

Grâce à Configuration Assistant, vous pouvez associer chaque adresse IP publique affectée à l'interface de votre WAN à plusieurs adresses IP privées.

Les clients ne disposant pas des autorisations nécessaires pourront facilement se lancer à l'assaut de votre réseau si ces clients parviennent à définir la topologie de votre réseau grâce à vos adresses IP réseau. La fonction NAT permet de masquer vos adresses IP privées sur l'Internet. Si un pirate ne parvient pas à deviner la structure de votre réseau local à l'aide d'adresses IP, il sera d'autant plus difficile pour lui de le forcer.

Dans certains cas - par exemple lorsque vous configurez un UC500 en présence d'un trunk SIP derrière un routeur sécurisé SR500, les entrées NAT sont automatiquement créées par CCA.

REMARQUE Le protocole NAT prend uniquement en charge les interfaces Ethernet de couche 3. Il ne prend pas en charge les interfaces de port des commutateurs de couche 2. Pour activer le service NAT sur une interface externe (non approuvée), toutes les interfaces concernées seront sélectionnées comme étant des interfaces internes (de confiance).

NAT statique et NAT dynamique

Le NAT statique utilise des adresses IP liées entre elles de manière statique. En d'autres termes, l'administrateur peut établir une liaison individuelle entre les adresses IP privées et publiques. Les traductions statiques sont généralement utilisées pour permettre l'accès à un périphérique donné par le système

NAT. Par exemple, si un réseau dispose d'un serveur DNS interne devant communiquer avec un serveur DNS externe, l'administrateur mettra en place une conversion statique pour permettre la liaison. Le NAT permet ainsi le trafic entre des adresses statiques, certes, mais converties.

A l'inverse, le NAT dynamique associe des adresses IP privées à des adresses IP publiques. Le NAT dynamique utilise une réserve d'adresses publique qu'il affecte de manière périodique (premier arrivé, premier servi). Lorsqu'un hôte doté d'une adresse IP privée demande l'accès à Internet, le NAT dynamique sélectionne une adresse IP libre dans la réserve. Le NAT dynamique est particulièrement utile en présence d'un nombre d'adresses inférieur au nombre d'hôtes à convertir.

Fenêtre NAT (adresses IP affectées par DHCP)

Sélectionnez un périphérique sur lequel vous souhaitez activer la fonction NAT dans la liste **Nom de l'hôte**.

Pour activer la fonction de traduction d'adresse réseau, sélectionnez une interface externe (non approuvée) dans la liste **Interface externe**. Cliquez sur **Détails** pour afficher les données relatives à l'interface externe sélectionnée.

Pour créer une entrée pour chaque mappage de port, procédez comme suit :

ETAPE 1 Cliquez sur **Ajouter** pour ajouter un élément dans la fenêtre NAT.

ETAPE 2 Sélectionnez une application dans la liste déroulante :

- Serveur Web
- Serveur Web sécurisé
- Serveur de messagerie
- FTP
- SSH
- SFTP
- Autre (TCP)
- Autre (UDP)

ETAPE 3 Dans le champ **Adresse interne**, introduisez l'adresse IP utilisée par le serveur sur votre réseau interne. Cette adresse IP ne peut pas être utilisée en externe sur l'Internet.

ETAPE 4 Dans le champ **Port interne**, entrez un numéro de port pour le périphérique interne.Il s'agit du numéro de port utilisé par le serveur en cas de demande de service en provenance du réseau interne.

ETAPE 5 Dans le champ **Port traduit**, entrez un numéro de port que la fonction NAT utilisera pour la traduction. Le numéro de port est utilisé par le serveur pour accepter les demandes de service en provenance d'Internet.

Pour renforcer la sécurité en ajoutant un pare-feu, cliquez sur **Service pare-feu** et utilisez la fenêtre Pare-feu. Voir **Pare-feu, page 270** pour plus d'informations sur ces paramètres.

ETAPE 6 Cliquez sur **OK** ou **Appliquer**.

Pour supprimer un mappage de port, procédez comme suit :

ETAPE 1 Sélectionnez un élément dans la fenêtre.

ETAPE 2 Cliquez sur **Supprimer**.

ETAPE 3 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Vous pouvez supprimer les paramètres NAT d'un périphérique se trouvant derrière un autre périphérique NAT sur un réseau intégralement routé. Par exemple, lorsqu'un UC500 se trouve derrière un routeur sécurisé SR500, vous pouvez supprimer les paramètres NAT de l'UC500.

Pour supprimer une configuration NAT complète, procédez comme suit :

ETAPE 1 Cliquez sur **Supprimer les paramètres NAT**.

Si la table IP contient des valeurs, une fenêtre s'affiche et vous signale que si vous continuez, vous supprimerez les paramètres de configuration NAT. Cliquez sur **OK** pour fermer la fenêtre contextuelle et continuer.

ETAPE 2 Cliquez sur **OK** dans la fenêtre NAT.

Fenêtre NAT (IP statique ou PPPoE avec IP statique)

Les commandes de la fenêtre NAT (IP statique) ne sont actives qu'en présence d'une adresse IP statique (ou PPPoE avec IP statique) affectée à la connexion Internet (interface WAN).

La réserve NAT doit être introduite avant d'entrer des valeurs dans la table de mappage NAT statique.

- **Créer une réserve NAT**
- **Mappage NAT statique**

Créer une réserve NAT

Les adresses IP pour la réserve NAT proviennent du fournisseur d'accès à Internet (FAI). Vous pouvez ajouter jusqu'à 10 valeurs pour la réserve NAT.

Les utilisateurs ne peuvent pas entrer d'adresses IP dans la réserve NAT si celles-ci sont utilisées par l'interface WAN.

Créer une entrée de réserve NAT

ETAPE 1 Pour créer une entrée dans la réserve NAT, cliquez sur le bouton **Créer** se trouvant à proximité de la table. Vous afficherez ainsi une nouvelle fenêtre intitulée Créer une réserve NAT.

ETAPE 2 Introduisez un nom dans le champ **Nom de la réserve**.

ETAPE 3 Entrez l'adresse IP ou cliquez sur l'option **Définir une plage d'adresses**. Entrez alors une plage d'adresses IP.

REMARQUE : L'adresse réseau utilisée dans la réserve NAT doit se trouver dans le même sous-réseau que celui pour l'interface WAN.

ETAPE 4 Cliquez ensuite sur **OK**.

ETAPE 5 Après avoir introduit la réserve NAT, cliquez sur **Appliquer** ou sur **OK** pour appliquer la configuration. Vous pourrez ainsi installer la réserve NAT et ajouter les adresses IP comme IP secondaires pour l'interface WAN.

Supprimer une entrée de la réserve NAT

ETAPE 1 Pour supprimer une entrée de la table relative à la réserve NAT, sélectionnez l'entrée souhaitée et cliquez sur le bouton **Supprimer** à proximité de la table Réserve NAT.

Cette opération supprimera tous les mappages NAT statiques utilisant les adresses IP configurées pour cette réserve.

ETAPE 2 Cliquez sur **OK** ou **Appliquer**.

REMARQUE : Les adresses IP utilisées dans une réserve ne peuvent pas l'être dans une autre. Par ailleurs, chaque nom de réserve doit être unique.

Mappage NAT statique

Les consignes suivantes sont de rigueur pour la création de mappages NAT statiques :

- Chaque couple d'adresses IP doit être unique. Si une adresse IP et un port internes ou externes sont utilisés pour un mappage, l'adresse IP ne pourra pas être utilisée pour créer un autre mappage sans port défini. Par exemple, si le port interne 192.168.10.10:80 est mappé vers 171.71.236.176:80, vous pouvez aussi mapper 192.168.10.10 vers 171.71.236.175 ou 192.168.10.15 vers 171.71.236.176
- Le mappage NAT peut se composer d'une adresse IP uniquement ou d'une adresse IP et d'un numéro de port. Les numéros de port TCP/UDP connus sont repris dans le champ Port interne/externe. Vous pouvez entrer le numéro de port s'il n'est pas indiqué.
- L'adresse IP et le port internes ou externes utilisés pour un mappage ne peuvent pas être utilisés s'ils sont déjà associés à une autre adresse IP ou un autre port. Par exemple, si le port interne 192.168.10.10:80 est mappé vers le port externe 171.71.236.178:80, vous ne pouvez pas mapper 192.168.10.10:80 vers 171.71.236.176:80 ou 192.168.10.15:80 vers 171.71.236.178:80
- Vous ne pouvez pas créer un mappage statique à l'aide d'une seule adresse IP WAN. Vous pouvez en revanche créer un mappage en utilisant l'adresse IP WAN avec un port.

ETAPE 1 Pour créer un mappage NAT statique, cliquez sur le bouton **Créer** se trouvant à proximité de la table Mappage NAT statique.

ETAPE 2 Mapper les adresses IP internes et externes :

a. Entrez l'adresse IP interne souhaitée dans le champ **IP interne**.

b. Entrez l'adresse IP externe souhaitée dans le champ **IP externe**.

ETAPE 3 Cliquez sur **OK**. Vous reviendrez ensuite à la fenêtre NAT principale.

ETAPE 4 Cliquez sur **OK** ou **Appliquer**.

Serveur VPN

Pour configurer les paramètres du serveur VPN, sélectionnez **Configurer** > **Sécurité** > **VPN** dans la barre de fonctions.

ATTENTION Cisco conseille de ne pas configurer le serveur VPN sur une connexion WAN distante. Si la connexion WAN est interrompue, l'opération échouera et le système risque d'être inutilisable.

Vue d'ensemble

Le VPN (réseau privé virtuel) permet à un client distant d'accéder au réseau de l'entreprise.

Un VPN est nécessaire dans les cas suivants :

- Vous devez accéder au réseau SBCS à partir d'un ordinateur distant à l'extérieur du pare-feu de votre réseau.
- Vous pouvez utiliser CCA pour gérer un périphérique SBCS distant par Internet.

Vous pouvez autoriser un périphérique VPN distant à recevoir des règles IPsec envoyées par un serveur VPN. Vous pouvez aussi configurer un serveur VPN de sorte qu'il envoie des règles IPsec à un périphérique VPN distant.

Lorsque vous autorisez les clients VPN distants à recevoir les règles d'un serveur VPN, les utilisateurs peuvent demander une connexion à leur réseau d'entreprise par un tunnel VPN en introduisant un mot de passe. Lorsque la connexion est demandée et que l'utilisateur distant est authentifié, le serveur VPN transfère les

paramètres au client distant. Sinon, l'utilisateur doit introduire manuellement les paramètres IPSec afin de configurer le tunnel VPN. Les périphériques VPN distants comprennent les routeurs IOS Cisco, les dispositifs de sécurité Cisco et les clients VPN Cisco.

Un groupe *VPN* est un groupe de clients VPN partageant les mêmes données d'identification et de configuration. Les clés partagées et les certificats numériques sont utilisés afin d'identifier le client par rapport à un groupe. Les stratégies de groupe peuvent être configurées sur la base de données du routeur local ou sur un serveur RADIUS externe, voire à la fois sur un serveur local et un serveur externe.

Vous pouvez configurer une clé partagée pouvant identifier un client distant. La clé partagée renforce la sécurité des échanges entre le périphérique distant recevant les règles IPSec et un serveur. La clé partagée d'un périphérique distant doit correspondre à celle du serveur VPN.

REMARQUE CCA autorise un maximum de 10 connexions VPN pour l'UC520 et l'UC540. Pour l'UC560, il accepte jusqu'à 20 connexions VPN. Les connexions VPN utilisées pour EZVPN, SSL VPN, le Gestionnaire multi-sites et les VPN de téléphone SPA525G sont incluses dans ce total.

Accès réseau — Tunnel VPN

L'accès Internet est possible grâce au tunnel VPN. La connexion est plus sûre grâce à la protection VPN entre le client et le serveur. Les données Internet transitent du tunnel au serveur où les échanges avec Internet ont lieu tout en exploitant les protections offertes par le client et le serveur. Cette approche diffère de l'aiguillage de trafic où les données Internet sont envoyées et reçues en dehors du tunnel VPN et reposent uniquement des protections paramétrées sur le client.

Accès Internet - Aiguillage de trafic

Lorsque vous activez l'aiguillage de trafic sur un réseau distant, les échanges du client avec les périphériques locaux ou par Internet avec d'autres réseaux ne sont pas cryptés. Les données sont uniquement cryptées lorsque l'utilisateur communique avec un sous-réseau protégé, généralement le réseau de l'entreprise. Cela réduit les délais de traitement du périphérique et améliore les performances du réseau.

Par exemple, un télétravailleur utilise un PC client sur le VPN pour accéder au réseau de l'entreprise par le biais d'un routeur offrant une liaison Internet du site de télétravail au réseau d'entreprise grâce à un tunnel VPN. Il peut également y avoir d'autres ordinateurs chez le télétravailleur qui ne font pas partie du réseau d'entreprise et pour lesquels l'accès au VPN doit être interdit. Il s'agira notamment

des PC utilisés par le conjoint ou les enfants du télétravailleur. Ces PC ont besoin d'un accès à Internet. Les utilisateurs tendront à utiliser le routeur du télétravailleur pour éviter d'installer une seconde connexion à haut débit. Le tunnel IPsec peut être actif en permanence et utiliser le protocole IEEE 802.1x pour identifier les utilisateurs de l'entreprise qui tentent d'accéder au réseau depuis un site distant. Un serveur RADIUS au siège de l'entreprise contiendra la base de données des utilisateurs. Étant donné que le tunnel est en permanence disponible, le routeur distant pourra demander à la base de données de confirmer les autorisations 802.1x (nom d'utilisateur et mot de passe) du télétravailleur pour lui permettre d'accéder au VPN.

ATTENTION L'aiguillage de trafic peut présenter un risque lors de la configuration. Les clients VPN disposent d'un accès non sécurisé à Internet. Ils peuvent donc faire l'objet d'une attaque. Le pirate pourra ensuite accéder au réseau local de l'entreprise par le tunnel IPsec en utilisant l'identité du client VPN.

Procédures

Commencez par sélectionner un périphérique dans la liste **Nom de l'hôte**.

Configurez les paramètres de chacun des onglets de la fenêtre Serveur VPN :

- **Paramètres du serveur**
- **Comptes d'utilisateur**
- **Accès réseau**
- **Profil VPN**

Paramètres du serveur

Pour activer un serveur VPN, configurez les stratégies et les paramètres selon les éléments du tableau ci-dessous.

Au terme de la configuration des paramètres du serveur, cliquez sur **Appliquer** pour appliquer vos paramètres et cliquez sur **OK** pour quitter la fenêtre Serveur VPN. Vous pouvez aussi cliquer sur les onglets Comptes utilisateur et Accès réseau pour continuer la configuration des paramètres VPN.

Paramètre	Description
Interfaces du serveur VPN	Sélectionnez ou affichez les interfaces du serveur VPN. Si une seule interface est affichée, ce paramètre est en lecture seule.

Paramètre	Description
Groupe VPN	
Configurez les paramètres du groupe VPN. Un groupe *VPN* est un groupe de clients VPN partageant les mêmes données d'identification et de configuration.	
Nom du groupe VPN	Champ en lecture seule. Le nom de groupe VPN par défaut utilisé par Configuration Assistant est EZVPN_GROUP_1.
Nombre max. de connexions	Nombre maximum de clients pour le groupe VPN pouvant être relié au serveur VPN.
Clés partagées	Entrez la clé partagée pour l'identification des clients VPN et des périphériques VPN distants. Entrez ensuite une nouvelle fois la clé pour confirmer. La clé peut être composée de 8 à 127 caractères alphanumériques. Les espaces et les points d'interrogation (?) ne sont pas autorisés.
Plage IP à distance du VPN	Entrez l'adresse IP initiale et l'adresse IP finale afin de définir une plage d'adresses IP à partir desquelles une adresse IP disponible sera affectée à un utilisateur. Vous pouvez définir jusqu'à 10 adresses IP pour les plateformes UC520 et UC540. Jusqu'à 20 adresses IP peuvent être introduites pour les plateformes UC560.
DNS	
DNS primaire	Entrez l'adresse IP du serveur DNS primaire pour le serveur VPN.
DNS secondaire	Facultatif. Entrez l'adresse IP du serveur DNS secondaire pour le serveur VPN.

Pour supprimer un serveur VPN, procédez comme suit :

ETAPE 1 Cliquez sur **Supprimer**.

Une fenêtre s'affiche et vous indique que si vous continuez, vous allez supprimer les paramètres de configuration du serveur VPN.

ETAPE 2 Cliquez sur **Oui** pour supprimer les configurations du serveur VPN et fermer la fenêtre.

ETAPE 3 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Comptes d'utilisateur

Pour créer un compte d'utilisateur et définir un mot de passe pour les utilisateurs demandant une connexion par un tunnel VPN, cliquez sur **Créer** et utilisez la fenêtre **Ajouter un compte**. Voir la rubrique **Ajouter un compte, page 268**.

Pour supprimer un compte d'utilisateur, sélectionnez le compte en question et cliquez sur **Supprimer**.

Accès réseau

Pour activer l'accès réseau par le tunnel VPN pour un site distant, cochez la case **Autoriser l'accès Internet sur le site distant**.

Si vous autorisez l'accès à Internet par le tunnel VPN, l'aiguillage de trafic est désactivé.

Pour activer l'aiguillage de trafic et identifier les réseaux protégés par un cryptage, procédez comme suit :

ETAPE 1 Cochez la case **Activer l'aiguillage de trafic**.

Seul le trafic destiné au sous-réseau protégé sera crypté et transféré par le tunnel VPN au réseau domestique. Le reste du trafic est envoyé vers les sous-réseaux cibles sans cryptage et sans être protégés par un tunnel VPN.

ETAPE 2 Cliquez sur **Créer** et utilisez la fenêtre **Ajouter un réseau** (voir **Ajouter un réseau, page 268**).

Pour supprimer un sous-réseau protégé, procédez comme suit :

ETAPE 1 Sélectionnez le réseau et le masque.

ETAPE 2 Cliquez sur **Supprimer**.

Profil VPN

Sous l'onglet Profil VPN, vous pouvez exporter le fichier de configuration du profil (.PCF) que les utilisateurs du VPN pourront importer dans le client Cisco EZVPN afin de créer une nouvelle connexion.

Pour ce faire, l'UC500 doit avoir une adresse IP WAN statique.

Pour exporter un fichier PCF, cliquez sur **Exporter le profil VPN**. L'option Exporter le profil VPN s'affiche si vous n'avez pas défini les paramètres du serveur VPN. Enregistrez le fichier .pcf sur votre machine locale et distribuez le fichier à vos utilisateurs VPN.

Consignes pour l'importation du profil VPN

Les utilisateurs du VPN devront respecter les consignes suivantes pour importer le fichier PCF dans le client Cisco EZVPN.

ETAPE 1 Si nécessaire, téléchargez et installez le client Cisco EZVPN à partir du site Cisco.com à l'adresse www.cisco.com/go/vpnclient.

ETAPE 2 Démarrez le client Cisco EZVPN.

ETAPE 3 Dans le client VPN, cliquez sur l'icône Importer ou utilisez le menu **Connexion** > **Importer**. Accédez ensuite à l'emplacement où se trouve le fichier PCF sur votre machine. Le profil s'affiche sous la forme d'une nouvelle connexion.

ETAPE 4 Pour utiliser le profil, cliquez deux fois sur la nouvelle connexion et introduisez votre nom d'utilisateur et votre mot de passe associés au compte VPN.

VPN distant

Pour accéder à la configuration du VPN distant, sélectionnez **Configurer** > **Sécurité** > **VPN distant** dans la barre de fonctions.

REMARQUE Pour les routeurs sécurisés SR520-T1, le VPN distant est une fonction sous licence. Pour utiliser cette fonction de sécurité en toute légalité, vous devez acheter la licence FL-SR520-T1-SEC pour le SR520-T1. Contactez votre distributeur Cisco pour acheter la licence.

Pour activer les services du client sans fil VPN distant sur un routeur sécurisé SR500, suivez les étapes suivantes :

ETAPE 1 Commencez par sélectionner un périphérique dans la liste **Nom de l'hôte**.

ETAPE 2 Pour activer les services vocaux, cochez la case **Activer les services vocaux sur une connexion à distance**.

ETAPE 3 Dans le champ **Adresse IP autocommutateur privé**, entrez l'adresse IP de CME (Cisco Unified CallManager Express). Pour l'UC500, la valeur par défaut est 10.1.1.1.

ETAPE 4 Dans le champ **Serveur VPN** , introduisez l'adresse IP ou le nom de l'hôte du serveur ou du concentrateur VPN.

ETAPE 5 *Facultatif* : Dans le champ **Entrer la nouvelle clé partagée**, entrez la clé partagée pour identifier les tunnels cryptés.

La clé partagée doit contenir entre 8 et 127 caractères alphanumériques. Les espaces et les points d'interrogation (?) ne sont pas autorisés. Si la clé partagée est configurée sur le périphérique VPN distant, elle doit correspondre à celle du serveur VPN.

ETAPE 6 Dans le champ **Entrez à nouveau la nouvelle clé partagée**, réintroduisez la clé partagée.

ETAPE 7 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Pour supprimer l'autorisation d'un périphérique distant à recevoir les règles IPsec, procédez comme suit :

ETAPE 1 Cliquez sur **Supprimer**.

Une fenêtre s'affiche et vous indique que si vous continuez, vous allez supprimer les paramètres de configuration à distance du VPN.

ETAPE 2 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Établir un tunnel VPN (Instructions de connexion au client de l'utilisateur final)

Ces consignes indiquent comment un utilisateur connecté à un fournisseur de services à l'aide d'un routeur Cisco SR520 peut établir un tunnel VPN vers le réseau central. Ces instructions facilitent la tâche de l'administrateur système.

Pour établir un tunnel VPN entre un utilisateur distant et le réseau d'un site central, procédez comme suit :

ETAPE 1 Affichez un navigateur, Internet Explorer par exemple.

ETAPE 2 Dans le champ **Adresse**, introduisez l'adresse IP du serveur VPN. La fenêtre Outil d'activation du tunnel VPN s'affiche et vous permet de vous connecter à un réseau central à l'aide d'un VPN ou à Internet.

ETAPE 3 Pour vous connecter au réseau central, cliquez sur **Connexion.** La fenêtre Authentification pour l'activation du tunnel VPN s'affiche.

ETAPE 4 Cliquez sur **Continuer**. Le tunnel VPN est établi.

Ajouter un réseau

Cette fenêtre s'affiche lorsque vous cliquez sur **Créer** sous l'onglet Accès réseau dans la fenêtre Serveur VPN ou SSL VPN et que l'aiguillage de trafic est actif.

Elle vous permet d'ajouter les sous-réseaux pour lesquels les paquets sont aiguillés à partir des clients VPN ou SSL VPN. Seul le trafic destiné à ces sous-réseaux est envoyé par le tunnel VPN ou SSL VPN. Le reste du trafic en provenance des connexions clients n'est pas chiffré. Pour de plus amples informations, consultez la rubrique **Accès Internet - Aiguillage de trafic, page 262**.

Pour ajouter un réseau, procédez comme suit :

ETAPE 1 Dans le champ **Réseau**, entrez l'adresse IP du réseau.

ETAPE 2 Dans le champ **Masque joker**, choisissez un masque de sous-réseau.

ETAPE 3 Continuez à ajouter les sous-réseaux pour lesquels vous souhaitez un accès VPN ou SSL VPN.

ETAPE 4 Cliquez sur **OK** pour fermer la fenêtre.

Ajouter un compte

Cette fenêtre s'affiche lorsque vous cliquez sur **Créer** sous l'onglet Comptes d'utilisateur de la fenêtre Serveur VPN.

Cette fenêtre vous permet d'introduire les données d'identification dans la base de données locale.

Pour activer un compte, procédez comme suit :

ETAPE 1 Entrez un nom d'utilisateur dans le champ **Nom d'utilisateur**. Le nom d'utilisateur peut contenir jusqu'à 64 caractères alphanumériques. Les caractères suivants ne sont pas autorisés : (espace), +, #, %, /, \, ?, ; ,<, >, {, }, |, ^, ~, [,], ` et ".

Le compte d'administrateur est automatiquement activé comme utilisateur VPN.

Le compte d'utilisateur VPN par défaut ne peut pas être supprimé.

ETAPE 2 Introduisez le mot de passe dans le champ **Mot de passe** et validez-le dans le champ **Confirmer le mot de passe**. Le mot de passe peut contenir jusqu'à 25 caractères alphanumériques. La longueur minimale pour le mot de passe est de 6 caractères. Les caractères suivants ne sont pas autorisés : (espace), +, ?, /, \, <, >, #, %, {, }, |, ^, ~, [,], ` et ".

ETAPE 3 Cliquez sur **OK** pour fermer la fenêtre.

Pare-feu et DMZ

Pour configurer les paramètres Pare-feu et DMZ, sélectionnez **Configurer** > **Sécurité** > **Pare-feu et DMZ** dans la barre de fonctions.

ATTENTION Cisco conseille de ne pas configurer les paramètres du pare-feu et de la zone DMZ à l'aide d'une connexion WAN distante. Si la connexion WAN est interrompue, l'opération échouera et le système risque d'être inutilisable.

Vue d'ensemble

Vous pouvez renforcer la sécurité de votre réseau en configurant un pare-feu et une zone démilitarisée (DMZ) pour assurer la protection de votre réseau local.

- Si vous configurez un UC520, vous utilisez un pare-feu CBAC.
- Si vous configurez un SR520, vous utilisez un pare-feu de zone.

La stratégie du pare-feu CBAC est définie par la configuration de la liste de contrôle d'accès (ACL) sur les interfaces du routeur afin de définir le type de trafic autorisé sur une interface.

Le pare-feu de zone passe transforme le modèle d'inspection IOS Stateful en un modèle de configuration de zone où les interfaces du routeur sont affectées à des zones de sécurité et la stratégie d'inspection du pare-feu est appliquée au trafic se déplaçant entre les zones. (Consultez le document technique Conceptual Difference Between Cisco IOS Classic and Zone-Based Firewalls" publié sur le site Cisco.com pour plus d'informations.)

Gérez la sécurité de votre réseau en effectuant les opérations suivantes :

- Configurez un pare-feu afin de filtrer les paquets atteignant le routeur en fonction du niveau de sécurité sélectionné. Si un paquet répond aux critères, il peut traverser l'interface. Si le paquet ne respecte pas les critères définis par les paramètres de sécurité, le paquet est bloqué.
- Créez une zone démilitarisée (DMZ) où placer les serveurs publics de manière à les isoler. Vous profiterez ainsi d'une sécurité renforcée au niveau de votre réseau interne. La DMZ permet un accès public à l'Internet et un accès Internet aux serveurs accessibles. Vous devez d'abord créer un pare-feu avant de définir une zone démilitarisée.

Procédures

Sélectionnez un périphérique sur lequel vous souhaitez activer un pare-feu (voire une zone démilitarisée) dans la liste **Nom de l'hôte**.

Cette fenêtre présente les deux onglets suivants :

- **Pare-feu, page 270**
- **DMZ, page 272**

A partir de cette fenêtre, vous pouvez aussi cliquer sur **Service NAT** pour afficher la fenêtre NAT et configurer la traduction d'adresse réseau. Voir la rubrique **Fenêtre NAT (adresses IP affectées par DHCP), page 257**.

Pare-feu

Suivez la même procédure pour créer ou modifier un pare-feu. Suivez les étapes ci-dessous :

ETAPE 1 Sélectionnez une interface externe dans la liste **Interface/zone externe (non fiable)** ou une interface interne dans la liste **Interface/zone interne (fiable)**. Les interfaces externes vous permettent de vous connecter au WAN ou à l'Internet. Les

interfaces internes permettent une connexion au LAN. Les lignes de conduite suivantes s'appliquent dans les cas suivants :

- Si vous optez pour une interface externe, l'option **Interface/zone interne (fiable)** est grisée.
- Remarques :vous pouvez sélectionner plusieurs interfaces internes.
- Ne choisissez pas l'interface vous permettant d'accéder à Cisco Configuration Assistant et indiquée comme étant une interface externe (non fiable).
- Vous ne pouvez pas lancer Configuration Assistant Cisco à travers le pare-feu d'une interface externe (non fiable).
- Si vous sélectionnez une interface externe qui a déjà été sélectionnée comme interface interne ou DMZ, un message d'avertissement s'affiche.
- Si vous sélectionnez une interface interne qui a déjà été sélectionnée comme DMZ, un message d'avertissement s'affiche.

ETAPE 2 Déplacez le curseur **Niveau de sécurité** au niveau souhaité. Le curseur Niveau de sécurité est actif lorsque vous sélectionnez une interface. La zone **Description** dresse la liste des filtres pour chaque niveau de sécurité :

- **Élevé** : empêche l'utilisation de la messagerie instantanée et des applications point-à-point sur le réseau. Le pare-feu surveille le trafic HTTP et la messagerie et bloque tout trafic ne respectant pas le protocole de sécurité. Il renvoie le trafic TCP (Transmission Control Protocol) et UDP (User Datagram Protocol) pour les sessions démarrées dans le pare-feu.
- **Moyen** : contrôle l'utilisation de la messagerie instantanée, des applications point-à-point ainsi que le trafic HTTP et e-mail sur le réseau. Le pare-feu renvoie le trafic TCP et UDP pour les sessions démarrées dans le pare-feu.
- **Faible** : aucune surveillance du trafic. Le pare-feu renvoie le trafic TCP et UDP pour les sessions démarrées dans le pare-feu.

ETAPE 3 Dans le champ **DNS primaire**, introduisez l'adresse IP du serveur DNS (service de nom de domaine) primaire. Les restrictions suivantes s'appliquent :

- Si le DNS a été configuré par d'autres moyens, les adresses IP du DNS ne peuvent pas être configurées. Pour modifier la configuration DNS, utilisez l'onglet **Configuration du périphérique** de la fenêtre **Configurer** > **Propriétés du périphérique** > **Adresses IP**.
- Si un DNS a été configuré sur le périphérique, l'adresse IP du DNS s'affiche et vous ne pouvez pas entrer d'adresse IP pour le DNS.

- Si le curseur Niveau de sécurité est sur Moyen ou Haut et si aucun DNS n'a été configuré pour ce périphérique, vous devrez introduire l'adresse IP d'un DNS primaire.

ETAPE 4 *Facultatif* : dans le champ **DNS secondaire**, introduisez l'adresse IP du serveur DNS secondaire.

DMZ

Pour créer une zone démilitarisée (DMZ), procédez comme suit :

ETAPE 1 Sélectionnez une interface dans le menu **Interface DMZ**.

Si l'interface sélectionnée est une interface externe ou une interface interne correspondant à l'interface du pare-feu, un message d'avertissement s'affiche.

ETAPE 2 Cliquez sur **Créer** et utilisez la fenêtre Créer un service DMZ. Voir la rubrique **Créer un service DMZ, page 272**.

ETAPE 3 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Pour supprimer une DMZ, procédez comme suit :

ETAPE 1 Sélectionnez l'adresse IP.

ETAPE 2 Cliquez sur **Supprimer**. Une fenêtre de confirmation s'affiche.

ETAPE 3 Cliquez sur **Oui** pour fermer la fenêtre.

ETAPE 4 Cliquez sur **OK** dans la fenêtre Pare-feu et DMZ pour appliquer les modifications et fermer la fenêtre.

Créer un service DMZ

Cette fenêtre s'affiche lorsque vous cliquez sur **Créer** sous l'onglet DMZ dans la fenêtre Pare-feu et DMZ.

Utilisez cette fenêtre pour ajouter une zone démilitarisée (DMZ) à une interface. Vous devez d'abord configurer un pare-feu.

Suivez les étapes ci-dessous :

ETAPE 1 Pour définir la direction du trafic pour le service TCP ou UDP, entrez une adresse IP dans le champ **Adresse IP**. En cas d'activation du service NAT (traduction d'adresse réseau), entrez l'adresse traduite (inside global address - adresse interne globale).

ETAPE 2 Sélectionnez le type de serveur pris en charge dans la liste **Type de serveur**. Les types de serveur pris en charge sont :**FTP**, **Serveur Web**, **Serveur Web sécurisé**, **Serveur de messagerie**, **SSH** et **SFTP**.

ETAPE 3 Cliquez sur **OK** pour fermer la fenêtre.

Pare-feu - Modifier ACL

La fenêtre Pare-feu - Modifier ACL s'affiche dans les cas suivants :

- Le pare-feu est activé sur l'UC500.
- Les entrées personnalisées de la liste de contrôle d'accès ont été configurées hors-bande à l'aide de la ligne de commande IOS.
- Configuration Assistant détecte la configuration hors-bande lorsqu'il tente d'appliquer la configuration vocale.

Utilisez les commandes **Déplacer vers le haut** et **Déplacer vers le bas** de la fenêtre pour réorganiser les entrées de la liste de contrôle d'accès (ACL) en fonction de la situation. Cliquez ensuite sur **OK**.

Audit de sécurité

Pour réaliser un audit de sécurité, sélectionnez **Configurer** > **Sécurité** > **Audit de sécurité** dans la barre de fonctions.

Vue d'ensemble

Vous pouvez tester les règles de sécurité et activer les procédures de sécurité afin de sécuriser les services réseau. En évaluant la configuration de sécurité de votre routeur, vous pourrez tester les fonctions de sécurité stratégiques sur votre routeur afin de définir les risques potentiels. Vous pouvez accepter ou refuser les paramètres de sécurité recommandés.

Les conditions suivantes sont vérifiées. Vous pouvez modifier les paramètres suivants en fonction de vos besoins afin de régler les options de sécurité de votre réseau :

- Désactiver le service Finger
- Désactiver le service PAD
- Désactiver le service TCP pour les petits serveurs
- Désactiver le service UDP pour les petits serveurs
- Désactiver le service du serveur IP BOOTP
- Désactiver le service d'identification IP
- Désactiver le chemin de source IP
- Activer le service de cryptage de mot de passe
- Activer TCP keepalives pour les sessions Telnet entrantes
- Activer TCP keepalives pour les sessions Telnet sortantes
- Activer le numérotage de séquences et l'horodatage pour les débogages
- Activer IP CEF (Cisco Express Forwarding)
- Désactiver les ARP IP gratuits
- Définir la longueur minimale à moins de six caractères
- Définir le nombre de tentatives d'identification échouées à moins de trois
- Définir le délai TCP syncwait
- Activer la journalisation
- Désactiver SNMP
- Définir une affectation d'ordonnanceur
- Désactiver la redirection d'IP
- Désactiver IP Proxy ARP
- Désactiver le broadcast vers IP
- Désactiver le service MOP (Maintenance Operation Protocol)
- Désactiver les IP inaccessibles

- Désactiver la réponse de masque IP
- Désactiver les IP inaccessibles sur une interface vide
- Activer RPF unicast sur les interfaces externes
- Activer AAA

Procédures

Pour exécuter un audit de sécurité sur un périphérique, procédez comme suit :

ETAPE 1 Sélectionnez **Audit de sécurité** dans la liste **Sécurité** afin d'afficher le bouton de démarrage Audit de sécurité.

ETAPE 2 Dans la liste **Nom de l'hôte**, sélectionnez le périphérique à évaluer.

ETAPE 3 Pour afficher la liste des paramètres pour l'audit de sécurité ainsi que les actions recommandées, cliquez sur **Audit de sécurité**. La fenêtre Rapport d'audit de sécurité s'affiche.

ETAPE 4 Cette fenêtre vous permet de sélectionner les opérations à effectuer pour sécuriser votre réseau.

Le tableau indique quels paramètres de sécurité présentent les valeurs recommandées ainsi que celles qui ne le sont pas. Ces dernières représentent un risque pour la sécurité.

Pour exécuter la configuration de sécurité d'un périphérique, procédez comme suit :

ETAPE 1 Sélectionnez un périphérique à évaluer dans la liste **Nom de l'hôte**.

ETAPE 2 Pour configurer les paramètres de sécurité recommandés pour les paramètres ne présentant pas les valeurs recommandées, cliquez sur le bouton **Régler les problèmes de sécurité**. Pour définir les valeurs de sécurité par défaut, cliquez sur le bouton **Annuler les paramètres de sécurité**.

ETAPE 3 Pour définir les valeurs de sécurité recommandées, cochez les cases se trouvant dans la colonne **Réparer** correspondant aux paramètres de sécurité qui ont échoué à l'audit de sécurité.

ETAPE 4 Pour définir les valeurs de sécurité par défaut, cochez les cases de la colonne **Rétablir** correspondant au critère ayant passé le test. Pour sélectionner toutes les cases, cliquez sur **Sélectionner tout**.

ETAPE 5 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Paramètres de sécurité du réseau (commutateurs CE520)

Si au moins un commutateur Catalyst Express CE520 se trouve sur le site client, sélectionnez un niveau de sécurité pour les commutateurs en sélectionnant **Configurer** > **Sécurité** > **Paramètres de sécurité du réseau**.

Vue d'ensemble

Vos commutateurs Catalyst Express doivent présenter le même niveau de sécurité : faible, moyen ou élevé. Les niveaux se définissent comme suit :

- **Faible**. Contrôle de la prolifération broadcast et contrôle du nombre d'utilisateurs ayant accès au port.
- **Moyen**. Paramétrage Faible et table reprenant les adresses MAC pour lesquelles l'accès au port a été autorisé.
- **Élevé**. Paramétrage Faible et serveur RADIUS pour les accès autorisés des périphériques hôtes demandant l'autorisation.

Procédures

La fenêtre Paramètres de sécurité du réseau s'affiche dans les cas suivants :

- Lorsque vous cliquez sur **Résoudre** quand la fenêtre Notification d'événements présente un conflit au niveau des paramètres de sécurité du réseau.
- Lorsque vous sélectionnez **Configurer** > **Sécurité** > **Paramètres de sécurité du réseau** dans la barre de fonctions.

Le contenu de la fenêtre varie selon que vous définissez le niveau de sécurité de l'hôte sur Faible, Moyen ou Élevé.

La fenêtre Notification d'événements vous redirige vers cette fenêtre dans les cas suivants :

- Vos commutateurs Catalyst Express ne présentent pas le même niveau de sécurité. Pour résoudre ce conflit, définissez le niveau de sécurité sur Faible, Moyen ou Élevé et cliquez sur OK.

- La table d'identification MAC contient les adresses MAC nécessitant votre approbation. Pour effectuer cette tâche, consultez la rubrique Niveau de l'hôte : Moyen.
- La configuration du serveur RADIUS de vos commutateurs Catalyst Express est différente. Pour résoudre le conflit, consultez la rubrique Niveau de l'hôte : Élevé.

Niveau de l'hôte : Faible

Lorsque le niveau est Faible, Network Assistant utilise les fonctions de sécurité suivantes :

- Activer le contrôle de la prolifération broadcast pour tous les commutateurs Catalyst Express de la communauté.

  Le contrôle de la prolifération broadcast évite que les paquets n'engorgent le sous-réseau au détriment des performances du réseau. Une prolifération broadcast importante peut bloquer tout le trafic sur le réseau.

- Activer le contrôle de la sécurité des ports pour tous les commutateurs Catalyst Express de la communauté.

  Le contrôle de la sécurité des ports permet de limiter le nombre d'adresses MAC ayant un accès simultané à un port. Le nombre maximal d'adresses MAC dépend du profil Smartports configuré sur le port. Le tableau ci-dessous illustre la variation du nombre maximal en fonction du profil Smartports.

Profil Smartports	Nombre maximal d'adresses MAC
desktop	1
ipphone	3 si un VLAN vocal est configuré ; sinon, 2
access-point	30
switch	Aucune limite
router	Aucune limite
serveur	1
guest	30
diagnostic	Aucune limite

Profil Smartports	Nombre maximal d'adresses MAC
other	Aucune limite

Pour en savoir plus sur la fonction Smartports, voir **Smartports, page 162**.

Niveau de l'hôte : Moyen

Le niveau Moyen propose une fonction de sécurité supplémentaire : l'authentification MAC. Cela signifie que lorsqu'un ordinateur, un serveur, une imprimante, un téléphone IP, un point d'accès, un commutateur ou un routeur se connecte à la communauté par le biais d'un port Catalyst Express, son adresse MAC doit être ajoutée à la table d'authentification MAC afin que le périphérique puisse accéder à la communauté.

Vous devrez ajouter une adresse MAC à la table d'authentification MAC dans les cas suivants :

- Vous connectez un périphérique à un port du commutateur Catalyst Express.
- Pour approuver l'adresse MAC, sélectionnez oui dans la cellule Approuvé.
- Cliquez sur **Ajouter une adresse MAC** et utilisez la fenêtre Ajouter une adresse MAC. Voir la rubrique **Ajouter une adresse MAC, page 279**.

L'adresse MAC est toujours approuvée lorsqu'elle est ajoutée.

Pour modifier l'approbation d'une ou de plusieurs adresses MAC, sélectionnez-les et cliquez sur **Modifier**. Utilisez pour cela la fenêtre Modifier une adresse MAC. Vous pouvez aussi modifier l'approbation d'une adresse MAC simple en modifiant la cellule Approuvé. Voir la rubrique **Modifier une adresse MAC, page 279**.

Si vous souhaitez supprimer une ou plusieurs adresses MAC, sélectionnez-les et cliquez sur **Supprimer**.

Les tables d'authentification MAC des commutateurs Catalyst Express de votre réseau doivent être identiques. Si ce n'est pas le cas, vous devrez résoudre le conflit. Vous pouvez demander à Network Assistant de fusionner les tables ou de les réinitialiser.

Niveau de l'hôte : Élevé

Le niveau Élevé définit la configuration 802.1x sur les commutateurs Catalyst Express. Le protocole 802.1x est un protocole d'authentification nécessitant la production des noms d'utilisateur et des mots de passe afin que les hôtes puissent accéder au réseau. Ils sont ensuite transférés au serveur RADIUS qui assure le stockage des noms d'utilisateur et des mots de passe approuvés. Vous pouvez configurer le serveur RADIUS dans cette fenêtre.

REMARQUE l'authentification 802.1x s'applique uniquement aux demandes d'accès émanant des PC.

Lorsque vous utilisez un niveau Élevé, l'authentification MAC n'est plus nécessaire.Vous pouvez donc la désactiver.

Pour définir l'authentification 802.1x, procédez comme suit :

ETAPE 1 Entrez l'adresse IP du serveur RADIUS.

ETAPE 2 Entrez la clé RADIUS qui sera utilisée par les commutateurs Catalyst Express lors de la communication avec le serveur RADIUS.

ETAPE 3 Entrez un port UDP compris entre 0 et 65535 afin de définir l'autorisation RADIUS. Si vous disposez de la version 4.0 ou supérieure de Cisco Secure ACS, le port UDP par défaut est 1645. Pour les versions antérieures, il s'agit du 1812.

Ajouter une adresse MAC

Cette fenêtre s'affiche lorsque vous définissez un niveau de sécurité Moyen dans la fenêtre Paramètres de sécurité du réseau et cliquez ensuite sur **Ajouter une adresse MAC pré-approuvée**.

Entrez une adresse MAC dans le champ Adresse MAC et cliquez sur **OK**. L'adresse MAC s'affiche dans la fenêtre Paramètres de sécurité du réseau avec un état "oui".

Modifier une adresse MAC

Cette fenêtre s'affiche lorsque vous sélectionnez une ou plusieurs adresses MAC dans la fenêtre Paramètres de sécurité du réseau et cliquez sur **Modifier**.

Si vous sélectionnez une adresse MAC, celle-ci s'affiche dans la fenêtre. Si vous en sélectionnez plusieurs, la mention Adresse MAC : multiple s'affiche.

Dans la liste Approuver, sélectionnez oui ou non et cliquez sur **OK**. L'état des adresses MAC sélectionnées est automatiquement modifié.

SSL VPN

Pour accéder à la configuration SSL VPN, sélectionnez l'option **Configurer** > **Sécurité** > **SSL VPN**. SSL VPN peut être configuré sur les routeurs sécurisés de la gamme Cisco SR500 Series.

Pour activer et configurer la fonction SSL VPN, le routeur doit disposer d'une adresse IP statique.

REMARQUE Pour le routeur sécurisé SR520-T1, SSL VPN est une fonction sous licence. Pour utiliser cette fonction de sécurité en toute légalité, vous devez acheter la licence FL-SR520-T1-SEC pour le SR520-T1. Contactez votre distributeur Cisco pour acheter la licence.

REMARQUE La fonction SSL VPN pour le dispositif de sécurité Cisco SA500 n'est pas configurée à l'aide de CCA. Pour configurer SSL VPN sur le périphérique, utilisez l'utilitaire de configuration pour le dispositif de sécurité SA500.

ATTENTION Cisco conseille de ne pas configurer SSL VPN sur une connexion WAN distante. Si la connexion WAN est interrompue, l'opération échouera et le système risque d'être inutilisable.

Vue d'ensemble

Le SSL VPN (réseau privé virtuel SSL) permet une liaison à distance à partir de n'importe quel site relié à Internet grâce à un navigateur et au chiffrement SSL.

La fonction principale du SSL consiste à assurer la sécurité du trafic Internet. Le terme "sécurité" fait référence à la confidentialité, l'intégrité du message et l'identification. SSL permet de garantir la sécurité grâce au chiffrement, aux signatures numériques et aux certificats. Bien que l'accès à l'application soit soumis à certaines contraintes en présence de VPN IPSec, les VPN SSL permettent l'accès à de plus en plus de logiciels standard, des services Web tels que l'accès aux fichiers, la messagerie et les applications TCP (grâce à un client à télécharger).

Fonctions de base

La configuration SSL VPN par CCA autorise la configuration par défaut la meilleure qui soit.

Grâce à un navigateur sur lequel le protocole SSL est activé (Internet Explorer, Netscape ou assimilé), l'utilisateur peut établir un lien avec la passerelle SSL VPN. La requête initiale de l'utilisateur adressée à la passerelle SSL VPN le redirigera vers une page HTML où il devra se connecter. Le nom d'utilisateur et le mot de passe sont alors transmis à la passerelle où ils seront validés par le serveur RADIUS (Cisco ACS). L'accès ne sera autorisé que si l'identification est réussie.

Si la session est ouverte, elle est conservée grâce à l'envoi d'un cookie au navigateur de l'utilisateur. Ce cookie doit être intégré à toutes les requêtes HTTP ultérieures de l'utilisateur afin qu'il puisse être identifié sur la passerelle SSL VPN. Si le cookie est manquant ou incorrect, la session prend fin et l'utilisateur ne peut plus accéder au réseau de l'entreprise. Normalement, la session restera ouverte jusqu'à ce que l'utilisateur se déconnecte, la session arrive à terme ou la session est supprimée de la passerelle SSL VPN.

La configuration SSL VPN de base autorise un accès sécurisé sans client aux ressources Web privées ainsi qu'au contenu Web. Ce mode autorise l'accès au contenu à l'aide d'un navigateur Web (accès Internet, bases de données et outils en ligne exploitant une interface Web).

Lorsque la fonction SSL de base est configurée et que l'utilisateur s'est identifié pour ouvrir une session, le portail SSL VPN et la barre d'outils s'affichent dans le navigateur Web de l'utilisateur. À partir de cette page, il pourra accéder à tous les sites HTTP disponibles, consulter sa messagerie en ligne et parcourir les serveurs de fichiers CIFS (Common Internet File System).

REMARQUE Si votre système de blocage des fenêtres intempestives est actif, il est possible que la fenêtre contenant la barre d'outils SSL VPN ne s'affiche pas.

Fonctions avancées

Les options SSL VPN avancées donnent accès au mode SSL Client léger et au mode Client Full-tunnel.

- **Mode Client léger (transfert de port).** Le mode Client léger élargit l'étendue des fonctions de chiffrement du navigateur Web afin de permettre l'accès à distance des applications TCP en présence de ports statiques (Post Office Protocol version 3 (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access protocol (IMAP), Telnet et Secure Shell (SSH)).

En mode Client léger, l'utilisateur VPN télécharge un applet Java en cliquant sur le lien affiché sur le portail. L'applet Java fait office de proxy TCP sur le client pour les services configurés par l'administrateur de la passerelle de sécurité. Pour le téléchargement de l'applet, l'utilisateur doit disposer des droits d'administration.

- **Mode Full Tunnel**. Le mode Client Full Tunnel permet une prise en charge complète des applications grâce au client Cisco Anyconnect ou au client Cisco SSL VPN (SVC) qui font l'objet d'un téléchargement dynamique. Le mode Client Full Tunnel est un client pour le tunnel SSL VPN léger offrant une configuration centralisée pour un accès à la couche réseau de n'importe quelle application.

  En mode Client Full Tunnel, le tunnel SSL est utilisé pour déplacer les données entre les réseaux internes de la couche réseau (IP). Lorsque l'utilisateur se connecte à la passerelle SSL VPN, le client SSL VPN est automatiquement téléchargé et installé sur le PC de l'utilisateur final et la liaison au tunnel est établie. Une fois que la connexion est établie, l'utilisateur profite d'un accès VPN complet au réseau de l'entreprise. Le mode Full Tunel permet aussi la prise en charge de la voix.

  Lorsque le mode Full Tunnel est actif, le client SSL VPN Anyconnect doit être installé pour que le VPN puisse fonctionner.

  REMARQUE L'utilisateur VPN doit disposer des droits d'administration pour installer les applications sur son PC afin de permettre le téléchargement et l'installation automatiques du client SSL VPN.

  Vous devrez vous identifier sur le site Cisco.com pour télécharger le client. Vous trouverez le lien pour télécharger le logiciel sous l'onglet Avancé.

- **Aiguillage de trafic**. Lorsque vous activez l'aiguillage de trafic sur un réseau distant, les échanges du client avec les périphériques locaux ou par Internet avec d'autres réseaux ne sont pas cryptés. Les données sont uniquement cryptées lorsque l'utilisateur communique avec un sous-réseau protégé, généralement le réseau de l'entreprise. Cela réduit les délais de traitement du périphérique et améliore les performances du réseau.

ATTENTION L'aiguillage de trafic peut présenter un risque lors de la configuration. Les clients VPN disposent d'un accès non sécurisé à Internet. Ils peuvent donc faire l'objet d'une attaque. Le pirate pourra ensuite accéder au réseau local de l'entreprise par le tunnel IPsec en utilisant l'identité du client VPN.

Procédures

Commencez par sélectionner un périphérique dans la liste **Nom de l'hôte**.

Cette fenêtre présente les deux onglets suivants :

- **Simple**
- **Avancé**

Simple

Sous l'onglet Simple, vous devrez configurer les paramètres selon les données figurant dans le tableau suivant. Cliquez sur **OK** pour fermer la fenêtre.

Paramètre	Description
Certificat numérique	Sélectionnez le certificat numérique qui sera envoyé au client pour l'identification SSL. En l'absence du certificat numérique, cliquez sur **Créer certificat** pour en créer un.
Adresse IP	Ce champ en lecture seule contient l'adresse IP statique du WAN. Il s'agit de l'adresse IP qui sera utilisée pour accéder au portail VPN. **REMARQUE** Pour démarrer le SSL VPN à partir du PC client, entrez https://*adresse_IP* dans le champ **Adresse** du navigateur (utilisez "https" au lieu de "http").

Paramètre	Description
Sites Intranet	Liste des sites Intranet à afficher sur le portail du SSL VPN. Pour ajouter un site Intranet, procédez comme suit : 1. Cliquez sur **Ajouter** pour ajouter une nouvelle ligne au tableau. 2. Cliquez sur le champ **Étiquette** de la nouvelle ligne pour entrer un libellé à l'aide de caractères alphanumériques. Les caractères suivants ne sont pas autorisés : +, #, %, /, \, ?, ; ,<, >, {, }, |, ^, ~, [,], ` et ".  3. Cliquez sur le champ **URL** et entrez l'URL du site. Les caractères suivants ne sont pas autorisés : (espace), +, ?, /, \, <, >, #, %, {, }, |, ^, ~, [, ], ` et ". Pour supprimer un site Intranet, sélectionnez le site dans la liste et cliquez sur **Supprimer**.

Paramètre	Description
Comptes d'utilisateur	Liste des comptes utilisateur pour ce SSL VPN. Le compte d'administrateur est automatiquement activé comme utilisateur VPN. Le nombre maximum de comptes utilisateur est 10 pour les plateformes UC520 et UC540, et 20 pour l'UC560. **REMARQUE** CCA autorise un maximum de 10 connexions VPN pour l'UC520 et l'UC540. Pour l'UC560, il accepte jusqu'à 20 connexions VPN. Les connexions VPN utilisées pour EZVPN, SSL VPN, le Gestionnaire multi-sites et les VPN de téléphone SPA525G sont incluses dans ce total. Pour ajouter un compte utilisateur et définir un mot de passe pour les utilisateurs demandant l'accès par le tunnel VPN, procédez comme suit : 1. Cliquez sur **Ajouter** pour ajouter une nouvelle ligne au tableau. 2. Cliquez dans le champ **Nom d'utilisateur** de la nouvelle ligne et entrez l'identifiant pour le nouveau compte. 3. Cliquez dans le champ **Mot de passe** et entrez le mot de passe pour le compte utilisateur. Les caractères suivants ne sont pas autorisés : (espace), +, ?, /, \, <, >, #, %, {, }, |, ^, ~, [,], ` et ". Pour supprimer un compte utilisateur, sélectionnez le site dans la liste et cliquez sur **Supprimer**.

Avancé

Sous l'onglet Avancé, activez et configurez les paramètres avancés pour le SSL VPN selon les informations figurant dans le tableau suivant. Cliquez sur **OK** pour fermer la fenêtre.

Paramètre	Description	
Client léger	Activer ou désactiver le mode Client léger (transfert de port) pour le SSL VPN. Si la fonction Client léger n'est pas cochée, le mode Sans client est utilisé.	
	Configurer la liste de transfert des ports	Lorsque le client léger est actif, cliquez sur **Configurer le transfert des ports** pour activer l'accès à distance aux applications TCP comme la messagerie, Telnet et SSH avec ports statiques. Complétez les paramètres de la fenêtre Transfert des ports, selon les indications du **Configurer la liste de transfert des ports, page 288**.
Full Tunnel	Activer ou désactiver le mode Full Tunnel pour le SSL VPN. Le mode Full Tunnel fournit un client léger pour le tunnel SSL VPN et offrant un accès à la couche réseau de n'importe quelle application. Le client est automatiquement téléchargé et installé sur le PC client. Pour le mode Full Tunnel, le client SSL VPN doit être installé. L'utilisateur VPN doit disposer des droits d'administration pour installer les applications sur son PC afin de permettre le téléchargement et l'installation automatiques du client SSL VPN. Lorsque le mode Full Tunnel est actif, entrez une plage d'adresse IP que les clients pourront utiliser lorsqu'ils se connectent.	
	IP de départ	Entrez la première adresse IP de la plage.
	IP de fin	Entrez la dernière adresse IP de la plage.

Paramètre	Description	
Client SSL VPN	Lorsque le client Full Tunnel est actif, les options **Installer** et **Désinstaller** deviennent actives. **IMPORTANT** Lorsque le mode Full Tunnel est actif, le client SSL VPN doit être installé. Si le client n'est pas installé, un message d'erreur s'affiche. L'option Installer vous permet d'installer le logiciel client SSL VPN (déploiement du client Cisco Anyconnect sur les routeurs sécurisés SR520-T1 ou le client SSL VPN (SVC) sur les routeurs sécurisés SR520-ADSL/Ethernet).	
	Installer	Pour installer le logiciel client SSL VPN, cliquez sur **Installer**, puis sur **Naviguer** pour accéder à l'emplacement du fichier et cliquez ensuite sur **OK**. CCA prend en charge le paquet de déploiement Web actuel pour Windows. Vous trouverez un lien vers l'emplacement de téléchargement du paquet lorsque vous cliquez sur **Installer**. Vous devrez vous identifier sur le site Cisco.com pour télécharger le logiciel. Voir **Fenêtre Installer le logiciel SSL VPN Client, page 290** pour plus d'informations.
	Désinstaller	Pour désinstaller le client SSL VPN du routeur, cliquez sur **Désinstaller**.
	Laisser le logiciel client installé sur le PC client.	Cochez la case **Laisser le logiciel client installé sur le PC client** pour conserver le logiciel client sur le PC de l'utilisateur afin qu'il ne doive pas être téléchargé et installé à chaque fois que l'utilisateur se connecte au SSL VPN. **ASTUCE** Désactivez cette option si vous utilisez SSL VPN pour un accès à distance et que vous ne souhaitez pas conserver une copie du client sur d'autres PC.

Paramètre	Description	
Aiguillage de trafic	**Activer l'aiguillage de trafic**	Cochez cette option pour activer l'aiguillage de trafic. Seul le trafic destiné au sous-réseau protégé sera crypté et transféré par le tunnel SSL VPN au réseau domestique. Le reste du trafic est envoyé vers les sous-réseaux cibles sans cryptage et sans être protégés par un tunnel SSL VPN. Cliquez sur **Ajouter** pour définir les sous-réseaux locaux pour le trafic SSL VPN. Voir **Ajouter un réseau, page 268** pour une explication des champs de cette fenêtre. Pour supprimer un masque de sous-réseau de la liste, sélectionnez le sous-réseau et cliquez sur **Supprimer**.

Configurer la liste de transfert des ports

La fenêtre Transfert des ports s'affiche lorsque vous cliquez sur **Configurer la liste de transfert des ports** dans la fenêtre SSL VPN.

Vue d'ensemble

Lorsque le transfert des ports est actif, le fichier d'hôte du client SSL VPN est modifié afin d'associer l'application au numéro de port configuré dans la liste de transfert. La liste de transfert des ports établit les associations des numéros de ports sur le client distant aux adresses IP et aux ports des applications se trouvant derrière la passerelle SSL VPN.

Procédures

Pour ajouter une entrée à la liste Transfert des ports pour chaque serveur et chaque port mappé, cliquez sur **Ajouter**, définissez les paramètres pour chaque entrée selon les consignes ci-dessous et cliquez sur **OK** pour fermer la fenêtre et enregistrer vos paramètres.

Paramètre	Description
IP du serveur	Entrez une adresse IP utilisée par le serveur. Cette adresse IP ne peut pas être utilisée en externe sur l'Internet.

Paramètre	Description
Port du serveur	Entrez le numéro de port de l'application concerné par le transfert des ports (entre 1 et 65535). Il doit s'agir d'un port statique.
Port client	Entrez le numéro de port du client (entre 1 et 65535). Il doit s'agir d'un port statique.
Description	Ajoutez des informations sur l'élément relatif au transfert des ports (jusqu'à 1024 caractères). Ces données sont obligatoires pour les routeurs Cisco IOS.

Pour supprimer un mappage de port transféré, procédez comme suit :

ETAPE 1 Sélectionnez un élément dans la fenêtre.

ETAPE 2 Cliquez sur **Supprimer**.

ETAPE 3 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Ajouter un compte utilisateur

Cette fenêtre s'affiche lorsque vous cliquez sur **Ajouter** sous l'onglet Comptes d'utilisateur de la fenêtre SSL VPN.

Pour ajouter un compte utilisateur, configurez les paramètres selon les consignes ci-dessous et cliquez sur **OK** pour enregistrer les modifications et fermer la fenêtre.

REMARQUE Le compte d'administrateur correspond au compte d'utilisateur du SSL VPN. Il ne peut donc pas être supprimé.

Paramètre	Description
Nom d'utilisateur	Le nom d'utilisateur peut contenir jusqu'à 64 caractères alphanumériques. Les caractères suivants ne sont pas autorisés : (espace), +, #, %, /, \, ?, ; ,<, >, {, }, |, ^, ~, [,], ` et ".

Paramètre	Description
Mot de passe	Le mot de passe peut contenir jusqu'à 25 caractères alphanumériques. La longueur minimale pour le mot de passe est de 6 caractères. Les caractères suivants ne sont pas autorisés : (espace), +, ?, /, \, <, >, #, %, {, }, |, ^, ~, [,], ` et ".
Confirmer le mot de passe	Réintroduisez le mot de passe pour le confirmer.

Ajouter des sites Intranet

Cette fenêtre s'affiche lorsque vous cliquez sur **Ajouter** (Sites Intranet) dans la fenêtre SSL VPN.

Pour ajouter une adresse, configurez les paramètres selon les consignes ci-dessous et cliquez sur **OK** pour enregistrer les modifications et fermer la fenêtre.

Paramètre	Description
Étiquette de l'URL	Entrez une description de l'URL (caractères alphanumériques). Les caractères suivants ne sont pas autorisés : +, #, %, /, \, ?, ; ,<, >, {, }, |, ^, ~, [,], ` et ".
URL	Entrez l'adresse. Les caractères suivants ne sont pas autorisés : (espace), +, ?, /, \, <, >, #, %, {, }, |, ^, ~, [,], ` et ".

Fenêtre Installer le logiciel SSL VPN Client

Cette fenêtre s'affiche lorsque vous cliquez sur **Installer (Logiciel SSL VPN Client)** dans la fenêtre SSL VPN.

Utilisez cette fenêtre pour installer le logiciel SSL VPN Client sur le périphérique client. Vous pouvez aussi utiliser cette fenêtre pour télécharger la dernière version du logiciel SSL VPN Client. Vous devrez vous identifier sur le site Cisco.com pour télécharger le logiciel SSL VPN Client.

Pour installer le logiciel SSL VPN Client sur le périphérique client, suivez les consignes ci-dessous.

ETAPE 1 Téléchargez si nécessaire le client SSL VPN (SVC) ou le fichier de déploiement pour Cisco Anyconnect (.pkg) à partir du site Cisco.com grâce au lien fourni. Ce lien vous donne accès au paquet client Microsoft Windows compatible.

Si le paquet logiciel de l'UC500 8.1.0 est installé sur votre système, vous devez utiliser la version 2.5.1025 du paquet client Anyconnect Microsoft (win-2.5.1025-k9.pkg). La version 2.3.0254 du client Anyconnect est pas compatible avec la version de Cisco IOS contenue dans le paquet logiciel 8.1.0 de l'UC500.

ETAPE 2 Cliquez sur **Parcourir** pour accéder à l'emplacement du paquet logiciel SSL VPN Client ou Anyconnect sur votre PC.

ETAPE 3 Sélectionnez le fichier .pkg pour le SSL VPN Client.

ETAPE 4 Cliquez sur **OK** pour installer le paquet et revenir à la fenêtre SSL VPN.

Système de prévention des intrusions (IPS)

Pour configurer l'IPS sur les routeurs sécurisés SR500, sélectionnez l'option **Configurer** > **Sécurité** > **IPS** dans la barre de fonctions.

REMARQUE Pour le routeur sécurisé SR520-T1, IPS est une fonction sous licence. Pour utiliser cette fonction de sécurité en toute légalité, vous devez acheter la licence FL-SR520-T1-SEC pour le SR520-T1. Contactez votre distributeur Cisco pour acheter la licence.

Vue d'ensemble

Le système de prévention des intrusions surveille les activités du réseau ou du système afin de déceler les comportements malveillants ou non désirés. Il peut réagir en temps réel afin de bloquer ou d'empêcher ces activités.

L'IPS réseau opère en ligne afin de bloquer les codes malveillants et les attaques au niveau du trafic réseau. Lorsqu'une attaque est détectée, les paquets malveillants sont éliminés et le reste du trafic est conservé. À la différence des pare-feu traditionnels, l'IPS prend les décisions en matière de contrôle d'accès en fonction du contenu des applications plutôt que sur la base des adresses IP ou des ports.

Le système de prévention des intrusions de Cisco IOS est un système en ligne offrant une inspection rigoureuse des paquets et qui permet de contrer la plupart des attaques. Il prend en charge les fonctions suivantes :

- IPS peut être configuré pour les interfaces internes et externes réputées vulnérables aux attaques.
- Une fois les interfaces IPS configurées, vous devrez obtenir une clé publique et importer un paquet de signatures IPS (fichier de définition de signatures). La mise à jour des signatures IPS est possible pour les paquets SDM-IPS uniquement.
- Les mises à jour du paquet de signatures peuvent être importées après la configuration initiale.
- Les alertes IPS permettent de signaler aux utilisateurs les attaques et les alertes, les niveaux de risque et les actions entreprises.

REMARQUE La modification des signatures, le tableau de bord pour la sécurité IPS et le suivi de l'IPS ne sont pas pris en charge.

Procédures

Consultez les rubriques suivantes pour configurer les fonctions de l'IPS :

- **Configuration initiale de l'IPS, page 292**
- **Mise à jour des signatures IPS, page 294**
- **Alertes IPS, page 294**
- **Supprimer la configuration initiale de l'IPS, page 295**

Configuration initiale de l'IPS

La configuration initiale de l'IPS vous permet de sélectionner un périphérique sur lequel l'IPS pourra choisir les interfaces permettant l'analyse des paquets, l'obtention d'une clé publique, le téléchargement d'un paquet de signatures et l'installation du fichier de définition des signatures du paquet sur le routeur.

Pour configurer l'IPS, procédez comme suit :

ETAPE 1 Sélectionnez un périphérique sur lequel vous souhaitez activer l'IPS dans la liste **Nom de l'hôte**.

ETAPE 2 Configurer les interfaces

Pour configurer les interfaces pour IPS, sélectionnez une interface externe dans la liste **Interface/Zone externe (non fiable)** ou une interface interne dans la liste **Interface/Zone interne (fiable)**. Les interfaces disponibles détectées sur le routeur figurent dans les colonnes Interne et Externe du tableau.

Les termes *externe* et *interne* se rapportent au sens de la recherche des attaques visant les interfaces pour le paquet IPS (flux entrant ou sortant).

- Lorsque l'IPS est sélectionné pour une interface figurant dans la colonne **Externe** du tableau, l'IPS analyse uniquement les paquets sortants sur cette interface.
- De même, lorsque l'IPS est sélectionné pour une interface figurant dans la colonne **Interne** du tableau, l'IPS analyse uniquement les paquets entrants sur cette interface.
- Les interfaces peuvent être à la fois des interface internes et externes.

Vous pouvez activer l'analyse IPS pour les flux de paquets entrants ou sortants d'une interface. Le nombre d'interfaces pour lesquelles l'IPS peut être activé est illimité.

ETAPE 3 Télécharger une clé publique

Une fois les interfaces internes et externes configurées, cliquez sur le lien pour télécharger la clé publique de Cisco.com. Copiez et collez la partie **key-string** de la clé dans la zone de texte prévue à cet effet.

La clé publique est nécessaire. Elle s'intitule **realm-cisco.pub**.

ETAPE 4 Télécharger et installer un paquet de signatures.

Vous devrez introduire un compte d'utilisateur et un mot de passe afin de vous identifier sur Cisco.com.

Pour télécharger et installer un paquet de signatures IPS, procédez comme suit :

a. Cliquez sur **Installer SDF** pour afficher la fenêtre Télécharger le paquet de signatures. Vous y trouverez le lien pour télécharger le fichier de définition des signatures SDM-IPS.

b. Cliquez sur le lien de téléchargement pour accéder à Cisco.com et sélectionnez le paquet de signatures Cisco IOS SDM-IPS dans la liste des paquets de signatures SDM-IPS.

   Seuls les paquets SDM-IPS de la catégorie Basic (Simple) peuvent être utilisés avec le SR520. La catégorie Basic (simple) regroupe les fichiers de signature jusqu'à 128 Mo destinés aux routeurs jusqu'à 128 Mo.

c. Accédez à l'emplacement du fichier de signatures (.zip) sur votre PC.

d. Cliquez sur **OK** ou **Appliquer**.

Lorsque vous cliquez sur **OK** ou **Appliquer**, la configuration est envoyée au routeur. Tous les fichiers de configuration IPS sont placés dans le répertoire flash : flash:/ips/

Une fois que vous avez installé le paquet de signatures, les boutons **Supprimer la configuration IPS**, Mise à jour des signatures **IPS** et **Alerte IPS** s'activent.

Mise à jour des signatures IPS

La mise à jour des signatures est uniquement possible si l'IPS a bien été configuré et si le paquet de signatures a été téléchargé.

La mise à jour des signatures IPS est possible pour les paquets SDM-IPS uniquement. Sous l'onglet, Mise à jour des signatures IPS, vous pouvez importer les dernières signatures pour le paquet SDF sélectionné.

Pour importer les mises à jour des signatures pour l'IPS, procédez comme suit :

ETAPE 1 Dans la fenêtre IPS, cliquez sur l'onglet Mise à jour des signatures IPS.

ETAPE 2 Cliquez sur le lien pour accéder à Cisco.com et sélectionnez un paquet .sdf à télécharger.

ETAPE 3 Accédez à l'emplacement du fichier de signatures (.zip) sur votre PC.

ETAPE 4 Cliquez sur **Extraire les signatures** pour afficher les nouvelles signatures et les signatures mises à jour ainsi que les signatures déployées sur le routeur mais désactivées.

ETAPE 5 Cliquez sur **OK** pour charger les signatures affichées dans le tableau sur le routeur et mettre à jour la version du paquet SDF sur le routeur.

Alertes IPS

Le volet Alertes IPS affiche les intrusions détectées et les mesures prises ainsi que des informations sur l'alerte en question. Les informations suivantes s'affichent pour chaque alerte.

- ID de signature et description de l'attaque
- Évaluation du risque

- Action sur événement
- Adresse IP source et cible de l'attaque
- Nombre de tentatives réussies et de paquets abandonnés

Cliquez sur **Afficher les alertes** pour afficher la liste des alertes. Cliquez sur **Réinitialiser les alertes** pour effacer la liste.

Supprimer la configuration initiale de l'IPS

Pour supprimer la configuration active de l'IPS, cliquez sur **Supprimer la configuration IPS** et sélectionnez **OK** ou **Appliquer**.

Filtrage d'URL (SR500)

Pour configurer le filtrage d'URL sur les routeurs sécurisés SR500, sélectionnez l'option **Configurer** > **Sécurité** > **Filtrage d'URL** dans la barre de fonctions.

La configuration du pare-feu de zone (ZBF) doit être active avant que vous puissiez activer le filtrage d'URL.

REMARQUE Pour le routeur sécurisé SR520-T1, le filtrage d'URL est une fonction sous licence. Pour utiliser cette fonction de sécurité en toute légalité, vous devez acheter la licence FL-SR520-T1-SEC pour le SR520-T1. Contactez votre distributeur Cisco pour acheter la licence.

Vue d'ensemble

Le filtrage d'URL vous permet de contrôler l'accès aux sites Internet en autorisant ou refusant l'accès à certains sites sur la base de la liste des adresses. Vous pouvez conserver une liste d'adresses locales sur le routeur.

CCA ne prend en charge que les listes blanches ou noires (filtrage d'adresses C3PL). La liste noire/blanche est une liste d'adresses créée manuellement et gérée par l'équipe chargée de la sécurité du réseau d'une entreprise. Il n'y a pas d'adresses par défaut. Elle est définie par l'utilisateur. CCA ne prend pour l'instant pas en charge les serveurs tiers pour le filtrage des adresses.

La liste blanche/noire :

- Offre une solution de base si quelques adresses seulement doivent être bloquées.
- Permet à l'entreprise de gérer directement les adresses à bloquer conformément à la politique de l'entreprise.

- Exploite le matériel réseau existant.

Procédures

ETAPE 1 Sélectionnez un périphérique sur lequel vous souhaitez gérer le filtrage des adresses dans la liste **Nom de l'hôte**.

ETAPE 2 Définissez les options de filtre et gérez la liste des noms de domaine à filtrer :

a. Cochez la case **Activer** pour activer le filtrage des adresses.

   Lorsque le filtrage d'adresses est désactivé, vous pouvez toujours ajouter et supprimer les adresses de la liste des noms de domaine, mais le filtrage n'a pas lieu. Le filtrage d'URL est désactivé par défaut.

b. Vous pouvez bloquer l'accès à tous les domaines à l'exception de ceux figurant dans la liste ou autoriser l'accès à tous les domaines sauf ceux figurant dans la liste.

   Pour ajouter une adresse à la liste des noms de domaine, cliquez sur **Ajouter**, puis dans la ligne ajoutée et entrez le nom de domaine à filtrer. Les noms de domaine partiels sont pris en charge tant qu'ils peuvent être validés (par exemple, cisco.com est une adresse valable).

   Le nombre maximum d'adresses autorisées dans la liste est 100.

c. Continuez à ajouter et supprimer les noms de domaine selon vos besoins.

ETAPE 3 Cliquez sur **OK** ou **Appliquer**.

Une fois que vous aurez cliqué sur **OK** ou sur **Appliquer**, les noms de la liste ne pourront plus être modifiés. Vous devez supprimer le nom puis l'introduire à nouveau afin de le modifier.

Vous pouvez importer un fichier texte contenant la liste des adresses à filtrer ou exporter la liste active vers un fichier texte qui pourra ensuite être importé à partir d'un autre périphérique ou d'une autre application. Les consignes suivantes sont de rigueur pour la création des listes d'adresses :

- L'extension du fichier doit être .csv ou .txt.
- Les lignes commençant par "#" sont considérées comme des commentaires.
- Les doublons ne sont pas autorisés dans la liste.
- Une adresse est introduite par ligne comme le montre l'exemple suivant :

```
#Nom de domaine
www.cisco.com
www.yahoo.com
www.rediffmail.com
www.google.com
```

8

Paramètres du système téléphonique et paramètres régionaux

Cette rubrique traite de la configuration des paramètres système et régionaux pour la téléphonie. Les thèmes suivants y seront évoqués :

- **Initialisation du système vocal**
- **Paramètres du système vocal**
- **Paramètres régionaux pour la téléphonie**

IMPORTANT L'accès Telnet doit être activé pour pouvoir configurer les fonctions vocales.

Initialisation du système vocal

La fenêtre Initialisation voix s'affiche lorsque vous tentez d'afficher une fenêtre de configuration de la voix avant d'initialiser les paramètres vocaux au niveau du système.

Si vous n'utilisez pas l'Assistant de configuration de la téléphonie, vous devrez configurer ces paramètres avant de passer aux fonctions vocales.

Si la plateforme UC500 que vous configurez présente les réglages d'usine, utilisez l'Assistant de configuration de la téléphonie pour procéder au paramétrage et définir les paramètres des trunks. Pour de plus amples informations, consultez la rubrique **Assistant de configuration de la téléphonie, page 98**.

Une fois ces paramètres appliqués, le système n'est plus en mode par défaut. Vous ne pourrez dès lors plus alors utiliser l'Assistant de configuration de la téléphonie tant que vous n'aurez pas rétabli la configuration par défaut.

Lorsque vous avez terminé, cliquez sur **OK**. Vous pouvez aussi cliquer sur **Annuler**.

Champ	Description
Mode système	Choisissez entre les options **Autocommutateur privé** ou **Système d'appareils à clé** pour la gestion des appels. Autocommutateur privé est la valeur par défaut. Lorsque le **Mode système** est défini sur **Système d'appareils à clé**, le système est placé dans un mode hybride où les trunks SIP sont traités comme si le système se trouvait en mode Autocommutateur privé et les trunks locaux (FXO, BRI, PRI) sont considérés comme des lignes du système d'appareils à clé. Dans ce mode, les trunks FXO et les trunks T1/E1 CAS sont configurés comme étant des lignes de trunk directes. A la différence des versions antérieures de CCA (1.x), il n'y a pas de réelle différence entre les mode Système d'appareils à clé et Autocommutateur privé.
Nombre de chiffres par numéro interne	Définit la longueur du numéro de poste. La valeur par défaut est 3.
Numéro d'accès à la messagerie	Numéro interne pour accéder à la messagerie. Le nombre de chiffres composant le numéro de poste doit respecter la valeur **Nombre de chiffres par numéro interne**.

Paramètres du système vocal

Pour accéder aux paramètres du système vocal, sélectionnez l'option **Configurer** > **Téléphonie** > **Système** > **Paramètres système**.

Définissez les paramètres suivants dans la fenêtre Système :

- **Configuration matérielle**
- **Message système**
- **Paramètres du type de système**

Cliquez sur **OK** ou **Appliquer** lorsque vous avez terminé la configuration des paramètres.

Configuration matérielle

La configuration matérielle de l'UC500 est détectée et affichée dans le volet Configuration matérielle. CCA se limite aux paramètres de configuration pouvant être modifiés en fonction de la configuration matérielle du routeur. D'ordinaire, ces paramètres sont fixes.

Message système

Dans le champ Message système, entrez le message à afficher sur les téléphones (par exemple : le nom de l'entreprise). Le message peut contenir jusqu'à 31 caractères.

Si le champ Message système reste vide (s'il ne contient aucun texte alphanumérique), lorsque vous appliquez la configuration, le message n'est pas mis à jour et le message système affiché sur les téléphones reste tel quel.

Paramètres du type de système

Les Paramètres du type de système sont uniquement disponibles pour la configuration initiale.

- Ces paramètres peuvent également être définis à partir de l'Assistant de configuration de la téléphonie ou de la fenêtre Initialisation voix.
- Vous devez rétablir les paramètres d'usine sur l'UC500 afin de modifier ces valeurs.
- Une fois que ces paramètres sont définis, les champs passent en lecture seule.

Paramètre	Description
Type de système voix	Sélectionnez un type de système vocal (**Autocommutateur privé** ou **Systèmes d'appareils à clé**). Lorsque vous choisissez **Système d'appareils à clé**, le système est placé dans un mode hybride où les trunks SIP sont traités comme si le système se trouvait en mode Autocommutateur privé et les trunks locaux (FXO, BRI, PRI) sont considérés comme des lignes du système d'appareils à clé. Les trunks FXO et les trunks T1/E1 CAS sont configurés comme étant des lignes de trunk directes. Il n'y a aucune autre différence entre le mode Système d'appareils à clé et le mode Autocommutateur privé.
Nombre de chiffres par numéro interne	Entrez le nombre de chiffres composant les numéros de poste sur le site client. 3 est la valeur par défaut.

Paramètres régionaux pour la téléphonie

Pour configurer les paramètres régionaux pour la téléphonie, sélectionnez l'option **Configurer** > **Téléphonie** > **Système** > **Région** dans la barre de fonctions.

Dans cette fenêtre, vous pouvez effectuer les sélections suivantes :

- Pays pour les tonalités de progression d'appel
- Région et langue du téléphone
- Langue de la messagerie
- Format à utiliser pour l'affichage de la date et de l'heure sur les téléphones

La langue par défaut de l'UC500 est l'anglais (Etats-Unis). Avant de configurer les autres paramètres dans la fenêtre Région, vous devez télécharger le paquet logiciel adéquat pour l'UC500 et/ou les paquets de paramètres locaux qui contiennent tous les fichiers pour la localisation des téléphones et des messageries) afin de les installer sur l'UC500. Voir les rubriques **Localisation de l'UC500 (paramètres hors USA/UK), page 569** et **Installation du logiciel sur l'UC500, page 552**.

Vous pouvez installer jusqu'à deux langues sur l'UC500, mais une seule peut être active. Si deux langues sont installée, vous pouvez modifier la langue active à partir de cette fenêtre. Pour installer des langues supplémentaires, choisissez l'option **Maintenance** > **Mise à jour du logiciel** > **UC500**.

Configuration des paramètres régionaux

Dans la fenêtre Région, vous pouvez paramétrer les paramètres régionaux suivants pour la téléphonie. Lorsque vous avez terminé, cliquez sur **OK** ou sur **Appliquer**.

Paramètre	Description
Périphériques	
Nom de l'hôte	Veillez à sélectionner le nom d'hôte "UC500".
Tonalité de progression d'appel	
Pays	Sélectionnez la région adéquate afin de définir les tonalités et les cadences pour les téléphones.
Téléphones La région et la langue du téléphone qui s'affichent ici correspondent aux fichiers de langue et de localisation installés sur l'UC500. La valeur par défaut est Anglais US. Si vous n'avez installé aucune autre langue, aucune autre option n'est disponible. Pour installer des langues supplémentaires, choisissez l'option **Maintenance** > **Mise à jour du logiciel** > **UC500**. Voir la rubrique **Installation du logiciel sur l'UC500, page 552**.	
Région du téléphone	Sélectionnez le fichier contenant les paramètres locaux adéquats.
Langue du téléphone	Sélectionnez la langue qui s'affiche sur les téléphones.

Paramètre	Description
Messagerie	
Langue de la messagerie	Langue pour les invites de la messagerie. Sur un système présentant la configuration d'origine, seul l'anglais est disponible dans le menu déroulant Langue de la messagerie. Vous devez télécharger et installer les fichiers contenant les paramètres locaux adéquats pour l'UC500 afin de localiser la messagerie vocale. Pour installer des langues supplémentaires, choisissez l'option **Maintenance** > **Mise à jour du logiciel** > **UC500**. Consultez la rubrique **Installation du logiciel sur l'UC500, page 552** pour plus d'informations sur la localisation de la messagerie vocale lors de l'installation du logiciel sur l'UC500. Vous pouvez installer jusqu'à deux fichiers de langue, mais une seule langue ne peut être active.
Date et heure	
Format de date	Format d'affichage de la date sur le téléphone (jj-mm-aa, mm-jj-aa, aa-mm-jj, aa-jj-mm)
Format d'heure	Format d'affichage de l'heure sur le téléphone (12 ou 24 heures)
Autres paramètres Cette rubrique contient le plan de numérotation actif et le fuseau horaire ainsi que des informations sur le paramétrage de ces éléments sous CCA.	

9

Ports et trunks pour la voix

Cette partie traite de la configuration des ports et des trunks pour la voix. Les rubriques suivantes sont présentées :

- **Ports FXS**
- **Trunks PSTN**
- **Trunks SIP**
- **État de trunk**

Ports FXS

La fenêtre Ports FXS s'affiche lorsque vous choisissez l'option **Configurer** > **Téléphonie** > **Ports et trunks** > **Ports FXS** dans la barre de fonctions.

Vue d'ensemble

Dans la fenêtre Ports FXS, vous pouvez établir comment les ports FXS intégrés seront utilisés et sélectionner le type de signalement.

Les réglages pour les ports FXS/DID de la carte d'interface vocale (VIC) sont configurés dans la rubrique Ports et trunks de l'onglet Trunks PSTN (voir **FXS/DID (VIC uniquement), page 312**). Si les ports FXS de la carte d'interface vocale sont configurés à partir du volet Trunks PSTN, leur rôle peut être défini sur la valeur Téléphone ou fax de zone commune.

Procédures

Configurez les paramètres des ports FXS selon la description ci-dessous et cliquez sur **OK** pour appliquer la configuration.

Paramètres	Explication
Port FXS	Lecture seule. Affiche l'identifiant de port FXS, par exemple, 0/0/0.
Profil	Définit la manière dont le périphérique FXS sera utilisé et où il sera configuré. Faites un choix parmi les options suivantes : ▪ **Téléphone utilisateur**. Permet la définition des paramètres avancés du téléphone, comme la messagerie. Les ports sont de type SCCP et nécessitent une licence utilisateur. Les fonctions disponibles sont configurées à l'aide de la rubrique **Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Utilisateurs et téléphones** > **Postes utilisateurs**. ▪ **Téléphone de zone commune**. Le téléphone de zone commune est d'ordinaire un téléphone analogique placé dans un couloir ou une salle de pause. Les fonctions avancées telles que la messagerie vocale, le transfert d'appel, etc. ne sont pas disponibles sur ces téléphones. Les ports FXS affectés à ce profil sont définis sous l'onglet Postes analogiques de la fenêtre Utilisateurs et téléphones (**Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Utilisateurs et téléphones**). ▪ **Fax**. Permet l'utilisation de fonctions telles que Trunk SIP ou T.37 Fax vers e-mail puisqu'un paramétrage spécifique est nécessaire pour une prise en charge efficace des télécopies. (**Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Utilisateurs et téléphones**).
Description	*Facultatif*. Entrez une description pour le port FXS et son utilisation.
Signal	Sélectionnez l'option **Loop Start** ou **Ground Start** comme type de signal selon les consignes du fournisseur de services. La valeur par défaut est Loop Start.

Paramètres	Explication
Poste	Si un poste a été configuré, il s'affiche ici. Pour configurer un poste, sélectionnez l'option **Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Utilisateurs et téléphones**. Si un port se voit attribuer la fonction Téléphone ou fax de zone commune, sélectionnez l'onglet Postes analogiques et introduisez le numéro de poste. Si le port se voit attribuer le rôle Téléphone d'utilisateur, activez l'onglet Postes utilisateurs, sélectionnez le téléphone et cliquez sur **Modifier**.

Trunks PSTN

Pour accéder aux options de configuration du trunk PSTN, sélectionnez l'option **Configurer** > **Téléphonie** > **Ports et trunks** > **Trunks PSTN**. Les paramètres de trunks PSTN suivants peuvent aussi être configurés à l'aide de l'Assistant de configuration de la téléphonie.

Les paramètres et les options affichées sous les onglets de la fenêtre Tunks PSTN peuvent varier selon les types d'interface PSTN disponibles sur l'UC500 que vous configurez.

Consultez les rubriques suivantes pour obtenir des informations sur la configuration des interfaces PSTN.

- **FXO**
- **Interface BRI**
- **Interface T1/E1**
- **FXS/DID (VIC uniquement)**

FXO

Si des ports FXO sont disponibles sur le routeur, cet onglet affiche le nombre des ports FXO libres (lecture seule). Par exemple :

```
Total des ports : 4 (4 intégrés, 0 VIC)
```

Pour plus d'informations sur la configuration des ports FXO, voir **Configuration des paramètres des ports FXO, page 313**.

Pour plus d'informations sur l'affichage de l'état et la gestion des ports FXO, consultez la rubrique **État de trunk, page 326**.

Interface BRI

En présence d'une interface BRI sur le système, configurez les paramètres conformément au tableau suivant.

REMARQUE En présence d'un PRI RNIS, si celui-ci est sélectionné en présence d'au moins une interface BRI, vous devrez paramétrer l'option Type de commutateur RNIS. Le paramètre Type de commutateur permet de paramétrer le type de commutateur RNIS pour l'interface BRI afin d'éviter les conflits.

Paramètre	Description
Type de commutateur BRI	Sélectionnez l'un des types de commutateurs BRI suivants selon les consignes de votre fournisseur de services : Basic 5ESS, Basic DMS100, Basic NI, NTT, Basic 1TR6, Basic NET3, VN3, Basic QSIG.
Possibilités du support	Sélectionnez l'une des options suivantes selon les consignes de votre fournisseur de services : Aucun, Voix ou 3100 Hz.
TEI RNIS statique	Sélectionnez Aucun ou sélectionnez un nombre afin de configurer la valeur TEI (Terminal Endpoint Identifier) selon les indications de votre fournisseur de services. La valeur TEI représente les périphériques RNIS intégrés à un réseau RNIS et en constituant une terminaison. Les TEI permettent de faire la distinction entre plusieurs périphériques utilisant les mêmes liaisons RNIS.

Interface T1/E1

En présence d'une interface T1/E1, configurez les paramètres conformément au tableau suivant. Cliquez sur **OK** ou **Appliquer** pour terminer.

Sur les plateformes UC560, vous pouvez configurer jusqu'à deux (2) ports T1/E1. Ils peuvent se trouver sur une interface T1/E1 intégrée ou sur une interface T1/E1 installée à un emplacement VIC.

Paramètre	Description
Type de connexion	Cliquez sur le bouton **Type de connexion** pour faire un choix entre les valeurs T1 ou E1. Ce paramètre est uniquement disponible pour la configuration initiale. Une fois le paramètre défini, le champ passe en lecture seule. Les options T1/E1 s'affichent si le périphérique dispose d'un port vocal T1/E1.
Signalement de canal	Faites un choix parmi les options suivantes : ▪ PRI RNIS ▪ FXO ▪ FXS ▪ E&M ▪ FGD

Paramètre	Description
PRI RNIS	Si vous sélectionnez l'option PRI RNIS comme type de signalement de canal, configurez les paramètres suivants selon les consignes de votre fournisseur de services. ▪ Dans le menu **Type de commutateur**, sélectionnez le type de commutateur à configurer. Ce paramètre permet de définir le type de commutateur ISDN et le type de commutateur au niveau de l'interface. ▪ Dans le champ **Possibilités du support**, sélectionnez Aucun, Voix ou 3100 Hz. ▪ Dans le champ **Groupe PRI**, définissez la plage des intervalles de temps pour le groupe PRI RNIS. La plage par défaut pour T1 est comprise entre 1 et 24 intervalles. L'intervalle 24 (canal D) est toujours inclus. La plage d'intervalles de temps définie entre 24 et 24 n'est pas valable. La plage par défaut pour E1 est comprise entre 1 et 31 intervalles. L'intervalle 16 (canal D) est toujours inclus. La plage d'intervalles de temps définie entre 16 et 16 n'est pas valable.

Paramètre	Description
FGD (Utilisé pour les T1)	Si vous avez sélectionné la valeur FGD dans le menu Signalement de canal, suivez les consignes suivantes : ▪ Pour choisir un type de signal, cliquez sur EANA ou OS (services de l'opérateur). ▪ Pour utiliser des intervalles de temps distincts pour les appels entrants et sortants, cochez la case **Utiliser des groupes distincts pour les appels entrants et sortants**. ▪ Dans le champ **Intervalles de temps**, entrez la plage désirée. Si vous avez coché la case **Utiliser des groupes distincts pour les appels entrants et sortants**, entrez la plage des intervalles pour les appels entrants dans le champ **Intervalles de temps pour les groupes entrants** et entrez celle pour les appels sortants dans le champ **Intervalles de temps pour les groupes sortants**. La plage par défaut pour T1 est comprise entre 1 et 24 intervalles. L'intervalle 24 (canal D) est toujours inclus. La plage d'intervalles de temps définie entre 24 et 24 n'est pas valable.

Paramètre	Description
FXO **FXS** **E&M**	Si vous avez sélectionné la valeur FXO, FXS ou E&M dans le menu Signalement de canal, suivez les consignes suivantes : ▪ Sélectionnez le type de signal. ▪ Cochez la case **Utiliser des groupes distincts pour les appels entrants et sortants** pour utiliser des intervalles distincts pour les appels entrants et sortants. ▪ Dans le champ **Intervalles de temps**, entrez la plage désirée. Si vous avez coché la case **Utiliser des groupes distincts pour les appels entrants et sortants**, entrez la plage des intervalles pour les appels entrants dans le champ **Intervalles de temps pour les groupes entrants** et entrez celle pour les appels sortants dans le champ **Intervalles de temps pour les groupes sortants**. La plage par défaut pour T1 est comprise entre 1 et 24 intervalles. Il n'y a pas de canal D pour ces types de signalement T1. La plage par défaut pour E1 est comprise entre 1 et 31 intervalles. L'intervalle 16 (canal D) est toujours inclus. La plage d'intervalles de temps définie entre 16 et 16 n'est pas valable.

FXS/DID (VIC uniquement)

En présence d'une interface vocale FXS/DID (VIC), configurez les paramètres suivants pour chaque port.

REMARQUE : Pour configurer les ports FXS *intégrés*, sélectionnez l'option **Configurer** > **Téléphonie** > **Ports et trunks** > **Ports FXS** dans la barre de fonctions.

Paramètre	Description
Mode	Sélectionnez FXS ou DID

Paramètre	Description
Signal	Si le mode actif est **FXS**, sélectionnez l'option **Loop Start** ou **Ground Start** selon les consignes de votre fournisseur de services. Si le mode actif est **DID**, sélectionnez l'option **Immédiat**, **Wink Start** ou **Démarrage différé** selon les consignes de votre fournisseur de services.
Identifiant de l'appelant	Si le mode actif est FXS, entrez le numéro à afficher pour l'identifiant de l'appelant de ce port FXS. N/A si le mode est DID.
Poste	Si le mode actif est FXS, entrez le numéro à afficher pour le poste de ce port FXS. N/A si le mode est DID.
Bloquer les numéros interdits	Si le mode est **FXS**, cliquez sur **Activer** ou **Désactiver**. N/A si le mode est DID.
Autorisations	Si le mode actif est FXS, le champ est grisé tant que les champs Identifiant de l'appelant et Poste n'ont pas été remplis. Une fois complétés, vous avez le choix entre les valeurs **National, interne, local, international, sans restriction, local-plus** ou **National-plus**. N/A si le mode est DID.

Configuration des paramètres des ports FXO

Pour accéder au volet Trunk FXO à partir de la barre de fonctions, sélectionnez l'option **Configurer** > **Téléphonie** > **Ports et trunks** > **Trunks PSTN**> **Onglet FXO**.

Modifier les paramètres des ports FXO

Pour modifier les paramètres de port généraux ou régler le son et les minuteries pour le port sélectionné, choisissez l'option **Modifier les paramètres. (**Si vous cliquez deux fois sur la ligne sélectionnée, la fenêtre Modifier les paramètres s'affichera également.)

Les onglets disponibles pour la définition des ports FXO sont les suivants :

- **Onglet Général**

- Onglet Temporisateurs
- Onglet Audio

Onglet Général

Pour configurer les paramètres généraux des ports, complétez les champs conformément au tableau ci-dessous et cliquez sur **OK** ou **Appliquer**.

Contactez le fournisseur de service des lignes CO pour établir comment ces paramètres doivent être configurés pour un site donné.

Paramètre	Description
Type de signalement	Les interfaces FXO et FXS indiquent l'état "Décroché" ou "Raccroché" et l'occupation des lignes téléphoniques à l'aide de l'une des deux méthodes de signalement : loop-start ou ground-start. ▪ **Loop Start**. Active le signalement de type "Loop-start" sur le port sélectionné utilisé pour les interfaces FXO et FXS. Avec la fonction Loop-start, seul un des interlocuteurs peut raccrocher. Il s'agit de la valeur par défaut pour les ports de voix FXO et FXS. ▪ **Ground Start**. Permet de configurer le signalement de type "Ground-start" sur le port de voix utilisé pour les interfaces FXO et FXS. Le signalement "Ground-start" permet à chacune des parties de passer un appel et de raccrocher.
Type de compression-expansion	Définit la norme de compression-expansion utilisée pour la conversion des signaux analogiques et numériques en modulation par impulsions et codage. ▪ **u-law**. Définit la norme de codage u-law en vigueur en Amérique du Nord pour un port donné. Il s'agit de la valeur par défaut. ▪ **a-law**. Active la norme de codage a-law en vigueur en Europe.

Paramètre	Description
Déconnexion de supervision	Affecte uniquement le signalement de type "Loop-start" et est généralement utilisé pour les ports de voix. Les options de déconnexion de supervision sont désactivées lorsque l'option Ground Start est choisie comme type de signalement. Les options de déconnexion de supervision sont les suivantes : ▪ **Anytone** ▪ **Dualtone preconnect** ▪ **Dualtone mid-call** ▪ **Signal** Il s'agit de l'option de déconnexion de supervision par défaut pour le port FXO. Veuillez prendre contact avec l'Assistance Small Business Support Center pour obtenir de l'aide. Pour plus d'informations, sélectionnez l'option **Dépanner** > **Support technique**.
Autoriser l'inversion de batterie	La commande d'inversion de batterie concerne les ports de voix FXO et FXS. Les ports FXO inversent d'ordinaire la batterie en cas de connexion de l'appel. L'option Autoriser l'inversion de batterie permet de restaurer la fonction d'inversion active par défaut sur les ports de voix. Si un port FXO ou le port FXS correspondant ne prend pas en charge l'inversion de batterie, n'activez pas cette commande pour le port FXO. Le paramètre est actif par défaut.

Onglet Temporisateurs

Pour configurer les paramètres des temporisateurs, complétez les champs conformément au tableau ci-dessous et cliquez sur **OK** ou **Appliquer**.

Paramètre	Description
Mémoire tampon de la gigue du paquet	Le retard de lecture représente le temps écoulé entre la réception d'un paquet vocal par la mémoire tampon de la gigue sur le processeur de signal numérique (DSP) et la lecture de celui-ci sur le codec.
	Mode : ▪ **Adaptatif**. Lorsque la valeur Adaptatif est active pour le mode Retard de lecture, la taille de la mémoire tampon de la gigue et le retard de lecture est modifié pendant l'appel en fonction de l'état du réseau. Il s'agit de l'option par défaut pour le mode Retard de lecture. ▪ **Réparé**. Lorsque la valeur Réparé est active pour le mode Retard de lecture, la taille de la mémoire tampon de la gigue n'est pas modifiée pendant l'appel, mais un retard constant est ajouté.
	Nominal : Définit le temps de configuration initial et le retard minimal autorisé que le DSP peut introduire avant la lecture des paquets vocaux. La plage autorisée est comprise entre 40 et 250 millisecondes. La valeur par défaut est 60 millisecondes.
Temporisateur	Permet de définir les valeurs de la fonction Déconnexion de supervision pour le port. Ce paramètre est principalement utilisé pour vérifier si le décrochage est intentionnel.
	Temporisateur pour déconnexion de supervision : La plage autorisée est comprise entre 50 et 1500 millisecondes. La valeur par défaut est 350 millisecondes.

Paramètre	Description
Délais d'expiration	Attente avant libération : Définit le délai d'attente en cas d'erreur d'appel tandis que le routeur Cisco émet un signal de ligne occupée, de réattribution ou hors service. Au terme de ce délai, la séquence de libération s'effectue. La plage autorisée est comprise entre 1 et 3600 secondes. La valeur par défaut est 30 secondes.
	Déconnexion de l'appel : Définit la durée pendant laquelle le port de voix FXO reste connecté après que l'interlocuteur a raccroché en l'absence de réponse. La plage autorisée est comprise entre 0 et 120 secondes. La valeur par défaut est 60 secondes.

Onglet Audio

Pour configurer les paramètres audio, complétez les champs conformément au tableau ci-dessous et cliquez sur **OK** ou **Appliquer**.

.

Paramètre	Description
Couverture de file d'écho	Définit la couverture d'annulation de l'écho sur le port de voix. Cette fonction est principalement utilisée pour modifier la couverture de l'EC. Cette commande autorise l'annulation de la voix envoyée par l'interface et reçue sur cette même interface dans le délai défini. Si la boucle locale (la distance séparant l'interface et le matériel connecté produisant l'écho) est supérieure au délai, la valeur définie pour cette commande devra être augmentée. La plage autorisée pour le paquet logiciel 8.0 et les versions supérieures est [24 | 32 | 48 | 64 | 80 | 96 | 112 | 128] ms La plage autorisée pour toutes les versions précédentes est 24 | 32 | 48 | 64 | ms La valeur par défaut est 64 millisecondes.
	Activer l'annulation de l'écho : La commande d'activation de l'annulation de l'écho permet l'annulation de la voix envoyée à l'interface et reçue sur la même interface. Le son ainsi reçu est perçu par l'interlocuteur sous forme d'écho. La désactivation de la fonction d'annulation de l'écho pourrait rendre un signal d'écho audible à l'interlocuteur. Etant donné que l'annulation de l'écho est un processus invasif susceptible de dégrader la qualité de la voix, cette commande doit être désactivée si elle n'est pas nécessaire. La valeur par défaut est "activé". Il s'agit d'un paramètre de configuration avancé. Veuillez prendre contact avec l'Assistance Small Business Support Center pour obtenir de l'aide. Pour plus d'informations, sélectionnez l'option **Dépanner** > **Support technique**.

Paramètre	Description
Couverture de file d'écho (suite)	Activer non linéaire : Définit la commande non linéaire sur le port vocal. Cette fonction est utilisée avec la commande d'annulation d'écho. La fonction activée par cette commande est généralement présentée comme étant la suppression de l'écho résiduel. L'état par défaut est "activé" si la fonction d'annulation de l'écho est active. Il s'agit d'un paramètre de configuration avancé. Veuillez prendre contact avec l'Assistance Small Business Support Center pour obtenir de l'aide. Pour plus d'informations, sélectionnez l'option **Dépanner** > **Support technique**.
Gain d'entrée	Définit le gain d'entrée en décibel sur le port vocal et plus précisément lorsque l'utilisateur souhaite augmenter le gain d'un signal accédant au routeur. Si le niveau vocal est trop faible, l'utilisateur pourra augmenter le gain d'entrée. La plage autorisée est comprise entre -6 et +14 dB. La valeur par défaut est 0 dB.
Atténuation en sortie	Définit le niveau d'atténuation en décibel sur le port vocal et plus précisément lorsque l'utilisateur souhaite augmenter l'atténuation d'un signal quittant le routeur. Si le niveau vocal est trop élevé, l'utilisateur pourra augmenter l'atténuation. Si le niveau vocal est trop faible, l'utilisateur pourra diminuer l'atténuation. La plage autorisée est comprise entre -6 et +14 dB. La valeur par défaut est 3 dB.

Paramètre	Description
Impédance	Ce réglage définit l'impédance des interfaces analogiques. Pour régler l'impédance, sélectionnez l'une des options suivantes. ▪ **600c.** 600 ohms + 2.15 uF ▪ **600r.** Terminaison résistive 600 ohm ▪ **900c.** 900 ohms + 2.15 uF ▪ **900r.** Terminaison résistive 900 ohm ▪ **Complex 1.** 220 ohms + (820 ohms || 115 nF) ▪ **Complex 2**. 270 ohms + (750 ohms || 150 nF) ▪ **Complex 3.** 370 ohms + (620 ohms || 310 nF) ▪ **Complex 4.** 600r, ligne = 270 ohms + (750 ohms || 150 nF) ▪ **Complex 5.** 320 + (1050 ohms | 230 nF), ligne = 12 Kft ▪ **Complex 6.** 600r, ligne = 350 ohms + (1000 ohms || 210 nF) L'impédance par défaut dépend du pays. Pour l'Amérique du Nord, la valeur par défaut est 600r.

Copier les paramètres des ports FXO

Pour copier tous les paramètres d'un port vers d'autres, suivez les consignes suivantes.

ETAPE 1 Sous l'onglet FXO, cliquez sur la ligne du tableau correspondant au port que vous souhaitez copier.

ETAPE 2 Cliquez sur **Copier les paramètres**. La fenêtre Paramètres de copie du port FXO s'affiche. Elle contient les paramètres de port et les valeurs correspondantes.

ETAPE 3 Sous la rubrique "Copier les paramètres vers", sélectionnez les ports FXO cibles pour la copie des paramètres et cliquez sur **Ajouter**.

La liste Ports disponible est vide si tous les ports disposent déjà de paramètres identiques.

- Cliquez sur **Sélectionner tout** pour choisir les ports FXO disponibles.
- Cliquez sur **Supprimer** pour supprimer les ports FXO sélectionnés de la liste.

ETAPE 4 Cliquez sur **OK**.

ETAPE 5 Sous l'onglet FXO, cliquez sur **OK** ou **Appliquer** pour achever l'opération.

Trunks SIP

Pour configurer les trunks SIP, sélectionnez **Configurer** > **Téléphonie** > **Ports et Trunks** > **Trunks SIP** dans la barre de fonctions.

Les rubriques suivantes sont présentées :

- **Vue d'ensemble**
- **Onglet Trunks SIP**
- **Configuration du fournisseur de tunks SIP générique**
- **Onglet Options avancées**

Vue d'ensemble

Les paramètres de trunk SIP configurés à l'aide de cette fenêtre peuvent varier selon le fournisseur de services sélectionné. Les paramètres de trunk SIP doivent être obtenus du fournisseur de services de téléphonie par Internet (FSTI).

Si votre fournisseur de services de téléphonie par Internet ne figure pas dans la liste, utilisez le modèle général pour le fournisseur SIP afin de configurer le trunk SIP. Pour plus d'informations sur les paramètres automatiquement configurés par CCA à l'aide de ce modèle, consultez la rubrique **Configuration du fournisseur de tunks SIP générique, page 325**.

Sous l'onglet Options avancées, vous devez définir les adresses IP pouvant accéder à votre réseau VoIP.

Pour en savoir plus sur les trunks SIP sur les plateformes Cisco SBCS/UC500, consultez le lien suivant de la communauté Cisco Small Business :

https://supportforums.cisco.com/docs/DOC-9830/

Onglet Trunks SIP

Pour configurer les paramètres des trunks SIP, complétez les champs conformément au tableau ci-dessous et cliquez sur **OK** ou **Appliquer**.

Champ	Description
Fournisseur de services	Fournisseur de services trunk SIP auquel le routeur se connectera pour obtenir l'accès PSTN. Les fournisseurs de services certifiés Cisco sont repris dans la liste déroulante Fournisseur de services et associés au logo Cisco. Pour configurer les paramètres de trunk SIP pour les autres fournisseurs, sélectionnez l'option **Fournisseur de trunk SIP général** dans la liste déroulante Fournisseur de services et complétez les champs requis pour ce fournisseur de services Pour plus d'informations sur la configuration du fournisseur générique de trunks SIP, voir **Configuration du fournisseur de tunks SIP générique, page 325**. Les options **Ajouter** et **Supprimer** de la liste déroulante Fournisseur de services permettent d'importer ou supprimer les modèles personnalisés pour les fournisseurs de services. ▪ Les modèles intégrés pour les fournisseurs de services certifiés Cisco ne peuvent pas être supprimés. ▪ Les modèles à importer doivent être obtenus du fournisseur de services SIP. En cas d'ajout d'un nouveau modèle de fournisseur de services, celui-ci peut être sélectionné dans la liste Fournisseur de services et les paramètres de configuration propres au fournisseur de services s'affichent lorsque celui-ci est sélectionné. Pour les modèles personnalisés, la version et l'horodatage s'affichent.
Serveur proxy (primaire)	Adresse IP ou nom d'hôte DNS du serveur proxy SIP primaire pour le FSTI.
Serveur proxy (secondaire)	*Facultatif*. Adresse IP ou nom d'hôte DNS du serveur proxy SIP secondaire (backup) pour le FSTI.

Champ	Description
Serveur d'enregistrement	*Facultatif*. Adresse IP ou nom d'hôte DNS du serveur d'enregistrement SIP pour le FSTI. Ce champ est requis uniquement si le FSTI exige l'enregistrement des SIP.
Serveur proxy sortant	*Facultatif*. Adresse IP ou nom d'hôte DNS du système SBC pour le FSTI. Ce paramètre est nécessaire si l'adresse IP du SBCS du FSTI n'est pas le même que celui du serveur proxy du SIP.
Nombre d'appels maximum	*Facultatif*. Nombre d'appels simultanés autorisés pour le contrôle des admissions d'appel. Vous devez configurer ce paramètre si le FSTI exige de l'UC500 qu'il limite le nombre d'appels simultanés. Consultez votre FSTI pour savoir si ce paramètre est nécessaire. Le nombre d'appels simultanés est repris entre parenthèses (par exemple : [1-48]). Le nombre maximum d'appels simultanés est identique au nombre de licences de l'UC500. Lorsque vous modifiez ce paramètre, la valeur Nombre d'appels maximum introduite dans **Configurer** > **Téléphonie** > **Nombre d'appels maximum** est également mise à jour. Voir la rubrique **Nombre d'appels maximum (Contrôle des admissions d'appel), page 513**.
Nom de la société	*Facultatif*. Nom de l'entreprise du client à afficher pour l'identifiant de l'appelant. Ce champ est nécessaire si un identifiant de l'appelant doit être signalé pour les appels sortants. Dans la plupart des cas, cet élément est pris en charge par le FSTI. Consultez votre FSTI pour savoir si ce paramètre est nécessaire. Cette valeur est intégrée à l'en-tête de l'invite SIP.
Identification Digest	*Facultatif*. **Nom d'utilisateur** et **Mot de passe** pour l'enregistrement SIP ou l'appel. Ce paramètre est nécessaire en présence d'un serveur d'enregistrement SIP. Cochez la case **Afficher le mot de passe sous forme de texte brut** pour basculer l'affichage du mot de passe.

Champ	Description
Service de nom de domaine	*Facultatif.* **Nom de domaine SIP**. Nom de domaine pour le serveur SIP. Le nom de domaine SIP est propre aux services VoIP. *Facultatif.* **Adresse du serveur DNS**. Adresse IP du serveur DNS pour le serveur SIP. Vous pouvez configurer un serveur DNS si aucun n'a été configuré et si les noms de domaine sont utilisés pour la configuration des trunks SIP. Toutefois, l'emplacement réservé à la configuration du DNS se trouve sous l'onglet Configuration du périphérique dans la fenêtre Adresses IP (**Configurer** > **Routage** > **Adresses IP**).
Autorisations des utilisateurs	*Facultatif*. Ce champ est requis si le FSTI exige l'enregistrement SIP avec un nom d'utilisateur et un mot de passe unique par DID pour tous les DID associés à l'UC500. La plupart des FSTI n'enregistre que le numéro principal. Pour ajouter un ensemble d'autorisations pour les fournisseurs de services nécessitant une identification SIP par DID, procédez comme suit : 1. Cliquez sur **Ajouter** pour ajouter une nouvelle ligne au tableau. 2. Cliquez dans la colonne **Nom d'utilisateur** de la nouvelle ligne et entrez un nom d'utilisateur. En général, le champ Nom d'utilisateur contiendra un numéro PSTN au format E.164. 3. Cliquez dans la colonne **Mot de passe** de la nouvelle ligne et entrez le mot de passe communiqué par le fournisseur de services. 4. Cochez la case **Afficher le mot de passe sous forme de texte brut** pour basculer l'affichage du mot de passe en texte brut. 5. Répétez ces opérations pour ajouter d'autres autorisations.

Suivez les consignes suivantes pour supprimer un ensemble d'autorisations SIP par DID.

ETAPE 1 Cliquez dans la ligne du tableau correspondant à l'ensemble des autorisations que vous souhaitez supprimer.

ETAPE 2 Cliquez sur **Supprimer**.

ETAPE 3 Cliquez ensuite sur **Appliquer**.

Configuration du fournisseur de tunks SIP générique

Lorsque la fonction **Fournisseur de trunks SIP générique** est sélectionnée dans le modèle de fournisseur SIP, CCA affiche toutes les options paramétrables pour les trunks SIP.

Outre les options de configuration présentée, CCA configure automatiquement ces éléments pour les trunks SIP à l'aide du modèle générique :

- **Codec pour la voix** : G.711-ulaw
- **Codec pour le fax** : G.711
- **Données utiles DTMF** : 101
- **Enregistrement SIP** : Enregistre le numéro principal uniquement

Le modèle de trunk SIP générique n'est pas compatible avec tous les FSTI. Pour demander un modèle CCA pour un nouveau fournisseur SIP, consultez le lien suivant de la communauté Cisco Small Business :

https://supportforums.cisco.com/docs/DOC-9685/

Onglet Options avancées

Pour des raisons de sécurité, CCA bloque le trafic SIP en provenance des sources inconnues. Configurez les adresses IP supplémentaires si votre fournisseur utilise des passerelles SIP avec des adresses IP différentes des serveurs proxys définis sous l'onglet Trunks SIP.

Consultez votre fournisseur SIP pour connaître les adresses des passerelles SIP utilisées.

Pour configurer des adresses IP supplémentaires offrant un accès à votre réseau VoIP, suivez les étapes suivantes :

ETAPE 1 Cliquez sur **Ajouter** pour ajouter une nouvelle ligne au tableau.

ETAPE 2 Entrez l'adresse IP.

ETAPE 3 Configurez les adresses IP supplémentaires le cas échéant.

ETAPE 4 Cliquez sur **OK**.

État de trunk

La fenêtre Etat de trunk s'affiche lorsque vous choisissez l'option **Configurer** > **Téléphonie** > **Ports et trunks** > **Paramètres des ports trunks** dans la barre de fonctions.

Vue d'ensemble

Dans la fenêtre État de trunk, les options Port de trunk, État actuel et Action s'affichent.

La fenêtre Action permet d'arrêter les ports vocaux inactifs. Cela permet d'éviter l'envoi des appels vers les ports sélectionnés si aucun périphérique n'est connecté.

Lorsqu'un port vocal est arrêté, aucun appel ne peut lui être destiné. Toutefois, le port reste affiché comme option disponible dans les autres écrans de Configuration Assistant. La configuration peut être appliquée au port, mais le port doit être réactivé manuellement
avant de pouvoir commencer à utiliser cette configuration.

Procédures

Pour arrêter ou redémarrer un port trunk vocal, sélectionnez le port dans la liste et sélectionnez l'option **Réinitialiser le port** ou **Arrêter le port** dans le menu déroulant de la colonne Action. Cliquez ensuite sur **OK** ou **Appliquer**.

Pour réactiver un trunk vocal arrêté, sélectionnez le port dans la liste et sélectionnez l'option **Activer le port** dans le menu déroulant de la colonne Action. Cliquez ensuite sur **OK** ou **Appliquer**.

10

Utilisateurs et postes

Cette rubrique explique comment définir les paramètres pour les utilisateurs, les téléphones et les postes à partir de l'option **Configurer** > **Téléphonie** > **Utilisateurs et postes** de la barre de fonctions.

Les rubriques suivantes sont présentées :

- **Utilisateurs et téléphones**
- **Messagerie et notifications**
- **Single Number Reach (SNR)**
- **Numérotation abrégée système**

Utilisateurs et téléphones

Pour afficher la fenêtre Utilisateurs et téléphones, sélectionnez l'option **Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Utilisateurs et téléphones** dans la barre de fonctions.

Consultez les rubriques suivantes pour plus d'informations sur la configuration des options pour chaque onglet de la fenêtre Utilisateurs et téléphones :

- **Postes utilisateurs**
- **Postes flottants**
- **Mobilité de poste**
- **Postes analogiques**
- **Configurer l'affectation des boutons du téléphone**

Postes utilisateurs

Suivez les instructions pour :

- **Ajouter, modifier et supprimer des téléphones**
- **Importation des données du téléphone pour plusieurs utilisateurs (Importation massive)**

ASTUCE Cliquez avec le bouton gauche de la souris sur les en-têtes de colonne sous l'onglet Postes utilisateurs afin de réorganiser les colonnes de la vue. Vous pouvez aussi cliquer avec le bouton gauche de la souris sur les colonnes pour trier les données par ordre croissant ou décroissant.

Ajouter, modifier et supprimer des téléphones

Lorsque vous branchez un téléphone IP dans l'UC500, celui-ci l'enregistre automatiquement et lui attribue une adresse IP sur le VLAN vocal (VLAN100) par DHCP. Il détecte également l'adresse MAC du périphérique et l'affiche.

Vous pouvez aussi ajouter des téléphones et définir les paramètres correspondants. Plus tard, lorsque le téléphone sera branché, la configuration lui sera envoyée.

Les utilisateurs et les postes pour les téléphones reliés aux ports FXS associés à un profil Téléphone d'utilisateur sont également définis ici.

Pour de plus amples informations, consultez les rubriques suivantes :

- **Ajout d'un téléphone**
- **Modifier un téléphone**
- **Supprimer un téléphone**

Si vous ajoutez et prédéfinissez un grand nombre de téléphones, vous pouvez importer les données de manière globale. Pour plus d'informations sur l'importation massive, consultez la rubrique **Importation des données du téléphone pour plusieurs utilisateurs (Importation massive), page 334**.

Ajout d'un téléphone

Vous pouvez ajouter un téléphone et prédéfinir les paramètres avant que celui-ci soit effectivement branché au système.

Pour ajouter un téléphone et y associer un utilisateur, suivez les étapes suivantes :

ETAPE 1 Dans la fenêtre Utilisateurs et téléphones, cliquez sur le bouton **Ajouter** au bas de la fenêtre.

ETAPE 2 Configurez les paramètres suivants pour le nouveau téléphone.

Champ	Description
Informations sur le téléphone	
Adresse MAC	Entrez l'adresse MAC du téléphone IP.
Type de téléphone	Sélectionnez le modèle de téléphone IP dans la liste déroulante. Lorsque vous sélectionnez un type de téléphone, l'onglet Affectation de bouton est modifié et affiche le nombre de lignes correct pour le modèle sélectionné.
Module d'extension	*Facultatif*. Pour les téléphones compatibles avec les modules d'extension, le menu **Module d'extension** présente la liste de tous les modèles pris en charge. CCA ne détecte pas automatiquement les modules d'extension reliés aux téléphones. Si un ou plusieurs modules d'extension sont reliés à un téléphone, vous devrez les sélectionner manuellement. Les sélections "x2" de la liste montrent que deux modules d'extension sont reliés au téléphone. Lorsque vous sélectionnez un module d'extension dans la liste, les lignes sont ajoutées à la liste des boutons du module d'extension. L'image du téléphone est modifiée afin d'afficher le module d'extension.

Champ	Description
Autoriser les appels vidéo	Indiquez si vous souhaitez autoriser les appels vidéo pour ce téléphone. La fonction **Autoriser les appels vidéo** ne s'applique pas aux téléphones analogiques ni aux téléphones ATA. ▪ Lorsque l'option **Autoriser les appels vidéo** est cochée, la fonction Cisco Unified Voice Advantage (CUVA) est activée sur le téléphone afin d'autoriser les appels vidéo. Lorsqu'elle est associée à une caméra USB, la fonction CUVA permet à un ordinateur relié à un téléphone IP Cisco Unified ou au Cisco IP Communicator d'ajouter la vidéo aux appels internes effectués à l'aide du téléphone. ▪ Lorsque l'option **Autoriser les appels vidéo** est inactive, les appels vidéo ne sont pas autorisés pour le téléphone sélectionné. Si le paramètre a été modifié par rapport au réglage d'usine, la valeur est conservée si vous modifiez le type de téléphone. Dans la plupart des cas, vous ne modifierez que le type de téléphone lorsque vous ajoutez un téléphone non inscrit. Dans ce cas, vous devrez modifier manuellement le paramètre après avoir modifié le type de téléphone. Par défaut, la fonction **Autoriser les appels vidéo** n'est pas activée. **REMARQUE** Les téléphones IP SPA300 et SPA500 ne prennent pas en charge les appels vidéo.

Champ	Description
Utiliser comme téléphone de télétravailleur	Sélectionnez ou annulez la sélection de l'option **Utiliser comme téléphone de télétravailleur** pour activer ou désactiver la fonction MTP. Lorsque l'option **Utiliser comme téléphone de télétravailleur** est cochée, la fonction MTP (Media Termination Point) est configurée sur le téléphone de sorte que Cisco Unified CME puisse achever le flux multimédia. Le paramètre MTP amène l'UC500 à faire office de proxy. Les paquets sont transférés vers d'autres téléphones IP. L'adresse IP de l'UC500 figure dans le champ d'adresse source. La fonction MTP est généralement utilisée dans les déploiements de téléphonie destinés au télétravail. Lorsque l'option est inactive, le point MTP n'est pas configuré sur le téléphone sélectionné. La case **Utiliser comme téléphone de télétravailleur** ne s'affiche pas sur les téléphones logiciels Cisco IP Communicator (CIPC) puisque la fonction MTP est toujours configurée sur les téléphones CIPC.
Informations utilisateur	
Nom	Nom de l'utilisateur du téléphone. Le nom s'affiche dans l'annuaire et est utilisé par le service Appeler par nom du Standard automatique.
Prénom	Prénom de l'utilisateur du téléphone. Le prénom s'affiche dans l'annuaire et est utilisé par le service Appeler par nom du Standard automatique.
Identifiant utilisateur	Identifiant utilisateur de l'utilisateur du téléphone. Cet identifiant est utilisé lors de la connexion aux pages Options utilisateurs de Cisco Unity Express permettant de modifier les paramètres du téléphone.

Champ	Description
Mot de passe	Mot de passe pour le téléphone IP. Le mot de passe est obligatoire si la messagerie est active. Il est facultatif si la messagerie est inactive. Ce mot de passe est utilisé par l'utilisateur lors de la connexion aux pages Options utilisateurs de Cisco Unity Express permettant de modifier les paramètres du téléphone. Le mot de passe s'applique uniquement à l'interface Cisco Unity Express et IMAP (Internet Message Access Protocol). S'il s'agit d'un téléphone SCCP, ce champ s'applique également à l'interface de CME (Cisco Unified Communications Manager Express).
Mobilité de poste	
Activer Mobilité de poste	Si vous cochez cette case, la fonction Mobilité de poste est activée pour le téléphone. Cette case est activée uniquement en présence d'au moins un profil de téléphone configuré et disponible. Pour de plus amples informations, consultez la rubrique **Mobilité de poste, page 343**. **ATTENTION** S'il s'agit d'un utilisateur existant, la messagerie vocale, les boutons, les touches d'appel rapide et la configuration existants seront écrasés par le profil sélectionné dès que vous cliquerez sur OK.
Sélectionner le profil de déconnexion	Choisissez un profil de déconnexion pour ce téléphone. Pour de plus amples informations, consultez la rubrique **Mobilité de poste, page 343**. Le profil de téléphone définit les boutons affectés par défaut sur le téléphone en l'absence de connexion utilisateur pour la fonction Mobilité de poste.

Champ	Description
Affectations des boutons et touches d'appel rapide	
Affectations des boutons	Sélectionnez un **type de bouton** pour chaque bouton que vous souhaitez configurer sur le téléphone. Vous devez sélectionner un **Type de téléphone** avant de configurer les affectations. Le volet **Bouton<x>** affiche les paramètres qui doivent être configurés pour le type de bouton sélectionné. Pour les données détaillées des types de bouton qui doivent être affectés à chacun et les paramètres correspondants, consultez la rubrique **Configurer l'affectation des boutons du téléphone, page 356**.
Numérotation abrégée	Cliquez sur l'onglet **Numérotation abrégée** pour configurer les touches d'appel rapide pour le téléphone. Pour de plus amples informations, consultez la rubrique **Numérotation abrégée, page 337**.

ETAPE 3 Cliquez sur **OK**.

Modifier un téléphone

Après avoir ajouté le téléphone, suivez les étapes de la rubrique pour modifier les paramètres.

Lorsque le téléphone est relié physiquement à l'UC500, il est détecté et son adresse MAC figure dans la liste. Il ne récupère pas automatiquement son numéro de poste ni les données utilisateur par défaut. Vous devez modifier le téléphone et configurer les paramètres.

IMPORTANT Dans les versions de CCA préalables à la version 3.0, les téléphones se voyaient automatiquement affecter un numéro de poste et plusieurs données utilisateur, mais ce n'est plus le cas. Vous devez modifier les paramètres du téléphone pour ajouter la configuration requise une fois les téléphones branchés.

Lorsque l'onglet Postes utilisateurs est sélectionné pour la première fois, il affiche la liste de tous les téléphones utilisateurs. Les ports analogiques associés à un profil Téléphone utilisateur sont repris à la page Postes utilisateurs sous forme de Téléphones analogiques. L'adresse MAC, le modèle de téléphone, le premier numéro de poste, le prénom et le nom d'utilisateur ainsi que son identifiant sont repris pour chaque téléphone.

Pour modifier les paramètres du téléphone, procédez comme suit :

ETAPE 1 Cliquez sur un téléphone pour le sélectionner. Cliquez ensuite sur le bouton **Modifier** au bas de la fenêtre pour afficher les détails. Vous pouvez aussi cliquer deux fois sur un téléphone de la liste pour afficher les détails et les modifier.

ETAPE 2 Modifiez les paramètres si nécessaire. Pour plus d'informations sur les paramètres définis pour les téléphones, voir **Ajout d'un téléphone, page 328**.

ETAPE 3 Cliquez sur **OK** pour envoyer la configuration au périphérique.

Supprimer un téléphone

Pour supprimer des téléphones, procédez comme suit.

ETAPE 1 Débranchez les téléphones à supprimer.

ETAPE 2 Sélectionnez **Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Utilisateurs et téléphones** dans la barre de fonctions.

ETAPE 3 Dans la fenêtre Utilisateurs et postes, cliquez sur les téléphones que vous voulez supprimer pour les sélectionner.

ETAPE 4 Cliquez sur **Supprimer**. Tous les téléphones sélectionnés sont supprimés.

Importation des données du téléphone pour plusieurs utilisateurs (Importation massive)

Un fichier Microsoft Excel intitulé BulkUserImport.xls est prévu pour l'introduction des données des téléphones pour plusieurs utilisateurs. Ces données peuvent être exportées au format XML et importées à partir de CCA.

Si vous avez installé Configuration Assistant à l'emplacement par défaut, le fichier se trouve dans le répertoire suivant :

C:\Program Files\Cisco Systems\CiscoSMB\Cisco Configuration Assistant\appdata

Pour importer des données pour plusieurs téléphones et utilisateurs sous CCA, suivez les étapes suivantes.

ETAPE 1 Sur votre PC, localisez le fichier Excel `BulkUserImport.xls` dans le dossier appdata qui se trouve dans le dossier d'installation de CCA sur votre PC.

ETAPE 2 Cliquez sur **Activer les macros** à l'invite. Pour que l'importation se fasse correctement, les macros doivent être actives.

ETAPE 3 Faites une copie du fichier et attribuez-lui un nom différent.

ETAPE 4 Ouvrez le fichier et introduisez les données requises dans le fichier .xls. Toutes les données introduites doivent se trouver dans la table comprise dans la feuille de calcul.

Nom de champ	Description
Identifiant utilisateur	*Requis*. Identifiant utilisateur associé à ce téléphone.
Prénom Nom	*Requis*. Prénom et nom de l'utilisateur associé à ce téléphone. Les nom et prénom peuvent s'afficher sur le téléphone. Ils peuvent aussi être utilisés par le Standard automatique pour la fonction Appeler par poste. Ils figurent aussi dans les annuaires.
Type de téléphone	*Requis*. Dans la liste déroulante, sélectionnez le modèle de téléphone. Choisissez l'option /14 si un module d'extension doit être relié au téléphone. Choisissez l'option /14x2 si deux modules d'extension doivent être reliés.
Adresse MAC	*Requis*. Entrez l'adresse MAC du téléphone au format suivant : *nnnn.nnnn.nnnn* (par exemple, ABCD.1234.1234).
Poste	*Requis*. Entrez le numéro de poste à utiliser pour le premier numéro de poste du téléphone (bouton 1). Le nombre de chiffres doit correspondre à la longueur définie pour le site (les postes de longueur variable ne sont pas pris en charge).

Nom de champ	Description
Mot de passe	*Requis*. Mot de passe de l'utilisateur du téléphone.
Type de ligne	*Requis*. Sélectionnez Double ou Octale dans la liste déroulante.
Poste TSPR	*Requis*. Numéro de poste interne ou numéro de téléphone externe utilisé comme cible pour les appels restés sans réponse sur le poste principal. Lorsque vous introduisez un numéro externe, introduisez le numéro tel que vous le composeriez, sans oublier le code d'accès.
Poste CFB	*Requis*. Numéro de poste interne ou numéro de téléphone externe utilisé comme cible pour les appels lorsque le poste principal est occupé. Lorsque vous introduisez un numéro externe, introduisez le numéro tel que vous le composeriez, sans oublier le code d'accès.
Expiration TSPR	*Requis*. Délai en secondes avant le transfert des appels sans réponse vers la cible TSPR. La valeur par défaut est 20 secondes.

ETAPE 5 Cliquez sur le bouton **Generate XML** (Créer XML) du fichier .xls pour exporter les données vers un fichier XML.

Vous pouvez attribuer n'importe quel nom au fichier XML, mais il doit absolument avoir l'extension .xml.

ETAPE 6 Démarrez CCA et sélectionnez l'option **Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Utilisateurs et téléphones**.

ETAPE 7 Dans la fenêtre Utilisateurs et téléphones, cliquez sur le bouton **Importer** au bas de la fenêtre.

ETAPE 8 Cliquez sur **Parcourir** et accédez à l'emplacement du fichier XML contenant les données des téléphones et des utilisateurs.

ETAPE 9 Cliquez sur **OK** pour charger le fichier. CCA valide les données XML lorsque vous importez le fichier.

ETAPE 10 En cas d'erreur, vous devez les résoudre dans le fichier .xls, recréer le XML et ensuite
réimporter le fichier .xml à partir de CCA.

ETAPE 11 Lorsque vous avez terminé, cliquez sur **OK**.

Numérotation abrégée

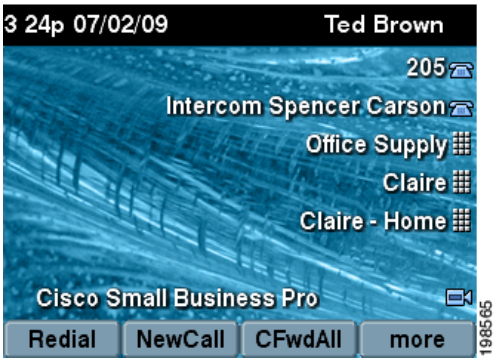
Pour plus d'information sur la configuration des touches d'appel rapide personnelles sur les téléphones des utilisateurs ou les profils MP, consultez les rubriques suivantes :

- **Vue d'ensemble**
- **Procédures**

Vue d'ensemble

Vous pouvez configurer les touches d'appel rapide personnelles pour des postes isolés, les téléphones Mobilité de poste (à l'aide du profil MP) et des utilisateurs de la fonction Mobilité de poste (par le profil utilisateur MP). Ces touches d'appel rapide sont accessibles à l'aide des boutons sur le téléphone ou à partir des menus du téléphone IP.

Par exemple, l'utilisateur Richard Dupont est affecté au poste 205. Le bouton 2 fait office d'interphone et trois numéros d'appel rapide personnels ont été configurés sur son téléphone. Boutons
Les boutons 3 à 5 correspondent à ces numéros d'appel rapide.



Les consignes suivantes concernent les numéros d'appel rapide personnels configurés à partir de cette fenêtre :

- Vous pouvez définir jusqu'à 55 numéros d'appel rapide personnels.
- Ces raccourcis sont appliqués dans l'ordre en commençant par le premier bouton disponible sur le téléphone de l'utilisateur.

- Les boutons d'appel rapide personnel ne peuvent pas être placés entre les boutons de ligne ou de fonction. Par exemple, si le bouton 1 est défini comme numéro de poste normal et le bouton 3 comme bouton d'interphone, le premier bouton d'appel rapide personnel doit être le bouton 4. Le raccourci ne pourra donc pas être affecté au bouton 2. Cela s'applique également aux boutons des téléphones dotés de modules d'extension.
- Si le nombre d'appels rapides est supérieur au nombre de boutons disponibles sur le téléphone IP de l'utilisateur, l'utilisateur pourra accéder aux autres raccourcis à l'aide du menu de son téléphone. Pour ce faire :
  - Il pourra appuyer sur la touche **Services** de son téléphone.
  - Il pourra choisir l'option **Mes applications** dans le menu URL de service CME.
  - Il pourra aussi choisir l'option **Touches d'appel rapide** dans le menu Mes applications.
- L'utilisateur du téléphone IP peut utiliser les fonctions d'appel rapide grâce à ces raccourcis. Pour utiliser les options d'appel rapide :
  - Lorsque le téléphone est décroché, appuyez sur le numéro correspondant au raccourci affiché dans le menu. Par exemple, pour appeler le 10e élément de la liste, l'utilisateur appuiera sur 1, puis sur 0.
  - Appuyez sur la touche **AbbrDial** pour effectuer l'appel.
- Les raccourcis que l'utilisateur ajoute à partir du menu **Services** de son téléphone s'affichent également dans la fenêtre Numérotation abrégée de CCA.
- Les téléphones IP sont automatiquement redémarrés dès que la configuration est validée.

Procédures

Pour ajouter, modifier ou supprimer des touches d'appel rapide pour les téléphones isolés ou les profils MP, suivez les étapes suivantes.

ETAPE 1 Sélectionnez **Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Utilisateurs et téléphones** dans la barre de fonctions.

ETAPE 2 Pour configurer des numéros d'appel rapide pour les utilisateurs standard, utilisez l'onglet Postes utilisateurs de la fenêtre Utilisateurs et téléphones.

Pour définir des numéros d'appel rapide pour les profils utilisateur ou de téléphone de type Mobilité de poste, utilisez l'onglet Mobilité de poste et sélectionnez le profil utilisateur ou le profil de téléphone. Cliquez ensuite sur l'onglet Numérotation abrégée.

ETAPE 3 Cliquez sur une ligne du tableau pour sélectionner un téléphone pour lequel vous souhaitez configurer un raccourci.

Vous pouvez trier les numéros par poste, par type de téléphone, par prénom, par nom, par ID utilisateur ou par adresse MAC.

ETAPE 4 Cliquez sur **Modifier**. La fenêtre Modifier téléphone s'affiche.

ETAPE 5 Dans la fenêtre Modifier téléphone, sélectionnez l'onglet Numérotation abrégée.

ETAPE 6 Sous l'onglet Numérotation abrégée, suivez les étapes suivantes pour ajouter une touche d'appel rapide.

a. Cliquez sur la ligne correspondant au numéro de la touche d'appel rapide que vous souhaitez ajouter ou modifier.

b. Entrez dans le champ **Numéro** le numéro de téléphone comme vous le composeriez normalement sans oublier les codes d'accès pour les appels externes et les préfixes éventuels.

Les jeux de caractères asiatiques à deux octets*ne sont pas* pris en charge pour les appels rapides.

Le champ **Numéro** n'accepte que les caractères suivants : chiffres de 0 à 9, A, B, C, D, #, * et +. Les lettres peuvent être utilisées pour les accès sécurisés ou les autres systèmes actifs sur le site du client.

c. Entrez un intitulé dans le champ **Etiquette**. Il désignera la touche d'appel rapide sur l'écran du téléphone.

ETAPE 7 Continuez à intégrer les touches d'appel rapide nécessaires.

ETAPE 8 Lorsque vous avez terminé, cliquez sur **OK**.

ETAPE 9 Les téléphones concernés sont automatiquement redémarrés. Les téléphones IP utilisés sont redémarrés au terme de l'appel en cours.

ETAPE 10 Pour supprimer une touche d'appel rapide, procédez comme suit :

a. Cliquez sur la ligne correspondant au numéro de la touche d'appel rapide que vous souhaitez supprimer.

b. Supprimez le numéro de téléphone dans le champ **Numéro**.

c. Supprimez les données dans le champ **Etiquette**.

ETAPE 11 Lorsque vous avez terminé, cliquez sur **OK**.

Les téléphones concernés sont automatiquement redémarrés. Les téléphones IP utilisés sont redémarrés au terme de l'appel en cours.

Postes flottants

Pour accéder aux paramètres de configuration pour les postes flottants, sélectionnez l'option **Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Utilisateurs et téléphones** et activez l'onglet Postes flottants.

Vue d'ensemble

Un poste flottant est un poste associé à aucun téléphone. Voici quelques exemples d'utilisation de cette fonction.

- Vous pouvez utiliser des postes flottants pour créer des messageries vocales associées à aucun téléphone. Les utilisateurs pourront ainsi accéder à leur messagerie vocale à partir de n'importe quel téléphone du système en composant simplement le numéro de la messagerie ou le code d'accès SDA. Ils devront alors introduire leur code PIN. Le code PIN pour accéder à la messagerie vocale est 1234. Les utilisateurs accédant pour la première fois à la messagerie vocale seront invités à modifier leur code PIN.
- Vous pouvez définir un poste flottant pour un employé mobile et faire en sorte que les appels soient transférés vers un numéro de téléphone portable.

  Le numéro faisant l'objet du transfert peut être modifié sans devoir changer le numéro de poste et le numéro réel (ici, le numéro de téléphone portable) n'est pas visible par l'appelant.

Vous pouvez associer un numéro DID à un poste flottant à l'aide de l'onglet Numérotation directe de la fenêtre Plan de numérotation en entrée (**Configurer** > **Téléphonie** > **Plan de numérotation** > **Entrant**).

Un poste flottant peut être affecté sous forme de :

- Poste pour le service de nuit.
- Cible d'une fonction **Transfert si pas de réponse vers** pour les appels adressés à un groupement de postes. Dans la liste **Transfert si pas de**

réponse vers, sélectionnez l'option **Autre numéro** et introduisez le numéro du poste flottant.

- Cible des appels transférés à partir du Standard automatique. Sélectionnez **Appeler un autre numéro** et introduisez le numéro de poste flottant.

Procédures

Pour ajouter ou modifier un poste flottant, procédez comme suit :

ETAPE 1 Sélectionnez **Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Utilisateurs et téléphones**.

ETAPE 2 Sélectionnez l'onglet Postes flottants.

ETAPE 3 Cliquez sur **Ajouter** ou sélectionnez un poste flottant existant dans la liste et cliquez sur **Modifier**. La fenêtre "Ajouter/modifier un poste flottant" s'affiche.

ETAPE 4 Définissez les paramètres conformément à la rubrique **Ajouter ou modifier des postes flottants**.

ETAPE 5 Cliquez sur **OK**.

Ajouter ou modifier des postes flottants

Pour créer un poste associé à aucun téléphone, définissez les paramètres conformément aux consignes ci-dessous et cliquez sur **OK**.

Paramètre	Description
Paramètres de poste	
Numéro	Numéro de poste à utiliser pour le poste flottant. Le numéro de poste doit être unique et contenir le nombre correct de numéros pour votre système.

Paramètre	Description
Numéro SDA	Si un numéro d'appel entrant direct (DID) a été associé à ce poste, il s'affiche ici. Sinon, la mention "Aucun DID mappé" s'affiche. Pour associer un numéro DID à un poste, utilisez la fonction **Configurer** > **Téléphonie** > **Plan de numérotation** > **Entrant** et sélectionnez l'onglet Numérotation directe. Dans la rubrique Appel direct vers les postes utilisateurs internes, cliquez sur **Ajouter** ou **Modifier** pour créer ou modifier les mappages entre le numéro DID souhaité et le poste flottant ou la plage de postes flottants.
Transfert d'appel : Tout	Permet de transférer tous les appels vers ce poste vers un numéro donné. Si le numéro est un poste externe, insérez les codes d'accès requis.
Activer la messagerie vocale	Créez une messagerie vocale pour ce poste. Lorsque cette fonction est active, les Informations utilisateur doivent être introduites.
Informations utilisateur Les informations utilisateur sont uniquement nécessaires si le service Appeler par nom du Standard automatique est requis ou si vous souhaitez activer la messagerie vocale pour un poste flottant.	
Prénom	Prénom de l'utilisateur associé à ce poste flottant. Il s'affiche dans l'annuaire et est utilisé par le service Appeler par nom du Standard automatique.
Nom	Nom de l'utilisateur associé à ce poste flottant. Il s'affiche dans l'annuaire et est utilisé par le service Appeler par nom du Standard automatique.
Identifiant utilisateur	Identifiant utilisateur associé à ce poste flottant. Cet identifiant est utilisé lors de la connexion aux pages Options utilisateurs de Cisco Unity Express permettant de modifier les paramètres de la messagerie.

Paramètre	Description
Mot de passe	Mot de passe de l'utilisateur associé à ce poste flottant. Ce mot de passe est utilisé lors de la connexion aux pages Options utilisateurs de Cisco Unity Express permettant de modifier les paramètres de la messagerie. Le mot de passe s'applique uniquement à l'interface Cisco Unity Express et IMAP (Internet Message Access Protocol). S'il s'agit d'un téléphone SCCP, ce champ s'applique également à l'interface de CME (Cisco Unified Communications Manager Express).
Réinitialiser les champs utilisateur	Permet de supprimer toutes les données utilisateur associées au poste flottant.

Mobilité de poste

La fonction Mobilité de poste (MP) permet d'offrir une mobilité aux utilisateurs finaux.

Un service de connexion permet aux utilisateurs des téléphones IP Cisco d'accéder à un téléphone sur lequel la fonction MP est active afin qu'ils puissent effectuer et recevoir des appels à l'aide de leur numéro personnel. Ils pourront par ailleurs profiter des fonctions d'appel rapide et d'une messagerie personnelle.

Pour plus d'informations sur la fonction Mobilité de poste et les paramètres associés à chaque onglet, consultez les rubriques suivantes :

- **Exemples de scénarios de déploiement pour la mobilité de poste**
- **Profil utilisateur MP**
- **Profil utilisateur MP**

Vue d'ensemble

Pour définir la fonction Mobilité de poste pour un site, vous devez effectuer les démarches suivantes :

- **Configurer les paramètres généraux.** Les paramètres généraux s'appliquent à tous les téléphones sur lesquels la fonction MP est active. Vous pouvez introduire jusqu'à 3 heures de déconnexion automatique. A une heure donnée, toutes les sessions MP actives sur les téléphones seront

automatiquement désactivées. Vous pouvez aussi indiquer si vous souhaitez que l'historique de l'utilisateur soit effacé lors de la déconnexion. Voir la rubrique **Paramètres généraux, page 348**.

- **Créer des profils d'utilisateur MP.** Le profil utilisateur MP permet d'affecter les boutons et les numéros d'appel rapide que l'utilisateur de la fonction MP verra lorsqu'il accède à un téléphone doté de cette fonction. Chaque utilisateur MP doit disposer d'un profil. Voir la rubrique **Profil utilisateur MP, page 346**.

  Créer des profils de téléphone MP. Le profil de téléphone MP définit les paramètres d'affectation des boutons et de numérotation abrégée pour les téléphones sur lesquels la fonction Mobilité de poste a été activée lorsqu'aucun utilisateur MP n'est branché sur le téléphone. Plusieurs téléphones peuvent être associés au même profil de téléphone. Voir la rubrique **Profil utilisateur MP, page 347**.

  * Le profil de téléphone CCA est également appelé Profil de déconnexion sous Cisco IOS.

- **Activer le service MP sur les téléphones IP sélectionnés.** La fonction Mobilité de poste est active sur le téléphone lorsqu'il est associé à un profil de téléphone. **Activer MP sur un téléphone, page 347**.

Exemples de scénarios de déploiement pour la mobilité de poste

Cette rubrique décrit quelques-uns des scénarios de déploiement les plus fréquents pour la mobilité de poste ainsi qu'une présentation des étapes de configuration pour chacun d'entre eux.

Scénario 1 : Les employés mobiles partagent les téléphones sur lesquels la fonction MP a été activée

Dans ce scénario, le service MP a été activé sur une réserve de téléphones IP. Les employés mobiles (par exemple, les commerciaux) partagent ces téléphones MP au lieu des téléphones de bureau standard lorsqu'ils sont en déplacement. Chaque employé mobile dispose d'une messagerie personnelle ainsi que des boutons et numéros d'appel rapide lorsqu'il se connecte à un téléphone MP.

Dans ce type de déploiement, vous devrez :

1. Créer un profil de téléphone MP définissant les affectations de bouton par défaut et les numéros d'appel rapide associés au téléphone lorsque personne n'y est connecté. Il s'agira généralement d'un profil très simple avec certaines restrictions d'appel. Voir la rubrique **Profil utilisateur MP, page 347**.
2. Activer le service MP pour chaque téléphone IP de la réserve commune en l'associant à un profil. Voir la rubrique **Activer MP sur un téléphone, page 347**.

3. Créer un profil utilisateur MP pour chaque employé mobile. Ce profil présentera les numéros de poste personnels et les touches d'appel rapide de l'employé. Pour chaque profil utilisateur MP, activez et affectez une messagerie personnelle au numéro principal de l'utilisateur. Voir la rubrique **Profil utilisateur MP, page 346**.

Scénario 2 : Les employés mobiles partagent des téléphones communs lorsqu'ils sont sur le site, mais ils disposent de leur propre téléphone IP en déplacement.

Dans ce scénario, le service MP est activé sur une réserve de téléphones de zone commune. Les employés mobiles partagent ces téléphones lorsqu'ils sont sur le site, mais ils disposent de leur propre téléphone IP en déplacement. Lorsqu'ils se connectent à un téléphone MP, les postes normaux et partagés personnels ainsi que les touches d'appel rapide sont identiques à ceux de leur téléphone IP principal. Ils peuvent accéder à leur messagerie personnelle à partir d'un téléphone MP, en plus de leur téléphone principal.

Dans ce type de déploiement, vous devrez :

1. Créer un profil de téléphone MP définissant les affectations de bouton par défaut et les numéros d'appel rapide associés au téléphone lorsque personne n'y est connecté. Il s'agira généralement d'un profil très simple avec certaines restrictions d'appel. **Profil utilisateur MP, page 347**.
2. Activer le service MP pour chaque téléphone IP de la réserve commune en l'associant à un profil MP que vous avez créé. **Activer MP sur un téléphone, page 347**.
3. Créer un profil d'utilisateur MP pour chaque employé mobile avec les affectations des boutons et les touches d'appel rapide correspondantes. Voir la rubrique **Profil utilisateur MP, page 346**.

   Pour que l'utilisateur MP utilise le même numéro de téléphone sur un téléphone MP et un téléphone IP standard, l'option Ligne partagée doit être utilisée pour le numéro principal. Pour accéder à la même messagerie vocale, la ligne partagée doit être associée à une messagerie partagée personnelle.

   Pour que l'utilisateur MP utilise le même numéro de téléphone et la même messagerie vocale sur un téléphone MP ainsi que sur son téléphone IP, la ligne partagée doit être utilisée comme numéro principal et disposer d'une fonction Messagerie vocale.

Eléments requis et restrictions

Les restrictions suivantes concernent la configuration de la fonction de mobilité de poste à l'aide de CCA :

- La version 8.0 ou une version supérieure de Cisco Unified CallManager Express (CME) est nécessaire.
- CCA prend uniquement en charge les types de ligne Normal et Partagé pour les profils Utilisateurs et téléphones.
- Le nombre maximal d'utilisateurs MP équivaut à trois fois le nombre de licences de téléphones pour la plateforme UC500 dont le client dispose (3 pauses).
- Si vous souhaitez qu'un utilisateur MP dispose aussi d'un téléphone, affectez le même numéro au profil MP et au téléphone à l'aide d'une ligne partagée. Configurez la messagerie pour la ligne partagée comme messagerie partagée personnelle.
- Les utilisateurs existants ne sont pas convertis automatiquement en utilisateurs Mobilité de poste. A l'inverse, les utilisateurs Mobilité de poste ne peuvent pas être automatiquement convertis en utilisateur de téléphone standard. Vous devez manuellement supprimer l'utilisateur de l'onglet Utilisateurs et postes et recréer l'utilisateur à l'aide d'un profil de l'onglet Mobilité de poste. La messagerie vocale existante sera supprimée.
- Aucune touche logicielle ne permet un accès direct à la fonction Mobilité de poste sur les téléphones MP. Les utilisateurs MP doivent accéder au menu de services CME sur leur téléphone et sélectionner le menu Mobilité de poste pour se connecter et se déconnecter.
- Un profil utilisateur ne peut être actif que sur un téléphone à la fois. Lorsqu'un utilisateur MP déjà connecté à un téléphone se connecte à un autre téléphone à l'aide du même profil, il est automatiquement déconnecté du premier.
- Le blocage d'appel après certaines heures n'est pas pris en charge.

Profil utilisateur MP

Le profil utilisateur MP permet d'affecter les boutons et les numéros d'appel rapide que l'utilisateur verra lorsqu'il accède à un téléphone doté de cette fonction MP.

Si une messagerie personnelle est nécessaire, elle devra être activée. Un identifiant utilisateur, un mot de passe, un prénom et un nom sont nécessaires lors de la création d'un profil utilisateur MP.

Pour créer ou modifier un profil utilisateur MP, procédez comme suit :

ETAPE 1 Sous l'onglet Mobilité de poste de la fenêtre Utilisateurs et téléphones, sélectionnez l'onglet Profils utilisateurs.

ETAPE 2 Cliquez sur **Ajouter** pour créer un nouveau profil utilisateur MP.

ETAPE 3 Pour modifier un profil utilisateur MP, localisez l'utilisateur dans la liste des profils, cliquez sur la ligne pour sélectionner le profil et cliquez ensuite sur **Modifier**.

ETAPE 4 Définissez les paramètres conformément à la rubrique **Ajouter un profil d'utilisateur Mobilité de poste, page 349**.

ETAPE 5 Cliquez sur **OK**.

Profil utilisateur MP

Le profil de téléphone MP définit les paramètres d'affectation des boutons et de numérotation abrégée pour les téléphones sur lesquels la fonction Mobilité de poste a été activée lorsqu'aucun utilisateur MP n'est branché sur le téléphone. Plusieurs téléphones peuvent être associés au même profil de téléphone.

Pour créer ou modifier un profil utilisateur MP, procédez comme suit :

ETAPE 1 Sous l'onglet Mobilité de poste de la fenêtre Utilisateurs et téléphones, sélectionnez l'onglet Profils de téléphone.

ETAPE 2 Cliquez sur **Ajouter** pour créer un nouveau profil de téléphone MP.

ETAPE 3 Pour modifier un profil de téléphone MP, localisez l'utilisateur dans la liste des profils, cliquez sur la ligne pour sélectionner le profil et cliquez ensuite sur **Modifier**.

ETAPE 4 Définissez les paramètres conformément à la rubrique **Ajouter un profil de téléphone Mobilité de poste, page 352**.

ETAPE 5 Cliquez sur **OK**.

Activer MP sur un téléphone

Pour activer la fonction Mobilité de poste sur un téléphone, procédez comme suit :

ETAPE 1 Sous l'onglet Postes utilisateurs de la fenêtre Utilisateurs et téléphones, cliquez sur un téléphone de la liste et ensuite sur **Modifier**. Vous pouvez aussi cliquer sur **Ajouter** pour ajouter un nouveau téléphone.

ETAPE 2 Dans la rubrique Mobilité de poste de la fenêtre Ajouter ou modifier les paramètres du téléphone, cochez l'option **Activer la mobilité de poste**.

Effectuez les opérations suivantes lorsque vous activez la mobilité de poste sur un téléphone :

- S'il s'agit d'un nouveau téléphone, l'intégralité du contenu des onglets relatifs aux utilisateurs et à l'affectation des lignes est grisé.
- Si un utilisateur est associé à un téléphone, toutes les données utilisateur, l'affectation des boutons et les numéros d'appel rapide sont réinitialisés et supprimés lors de l'application des modifications.
- Si l'utilisateur est actuellement associé à un téléphone doté d'une messagerie vocale personnelle, la messagerie est aussi supprimée lors de l'application de la configuration.

ETAPE 3 Dans la liste déroulante **Sélectionnez le profil de téléphone**, sélectionnez le profil de téléphone MP à associer.

Lorsque vous sélectionnez un profil de téléphone, la zone Informations utilisateur de la fenêtre est mise à jour afin d'afficher les données utilisateur configurées pour ce profil.

ETAPE 4 Cliquez sur **OK**.

Paramètres généraux

Configurez les paramètres de déconnexion généraux pour tous les téléphones MP de votre site conformément aux indications ci-dessous. Cliquez ensuite sur **OK**.

Paramètre	Description
Déconnexion automatique	Vous pouvez définir jusqu'à trois horaires de déconnexion automatique au format 24 heures. Ces paramètres s'appliquent à tous les téléphones sur lesquels la fonction MP est active. A l'heure indiquée, toutes les sessions MP actives sur les téléphones seront automatiquement désactivées. Si un appel est en cours à l'heure indiquée, la session prendra fin au terme de l'appel.
Réinitialiser l'historique des appels après la déconnexion de l'utilisateur	Si cette option est cochée, l'historique des appels de l'utilisateur connecté sera supprimé lorsque celui-ci se déconnecte ou en cas de déconnexion automatique.

Ajouter un profil d'utilisateur Mobilité de poste

Cette fenêtre s'affiche lorsque vous cliquez sur **Ajouter** ou **Modifier** sous l'onglet Profils utilisateurs du volet Mobilité de poste de la fenêtre Utilisateurs et téléphones. Vous pouvez aussi cliquer deux fois sur un profil utilisateur existant pour afficher cette fenêtre.

Le profil utilisateur MP permet d'affecter les boutons et les numéros d'appel rapide que l'utilisateur de la fonction MP verra lorsqu'il accède à un téléphone doté de cette fonction. Chaque utilisateur MP doit disposer d'un profil. Vous pouvez aussi choisir d'activer une messagerie personnelle pour l'utilisateur MP.

Définissez le profil utilisateur selon les indications ci-dessous et cliquez sur **OK**.

Paramètre	Description
Paramètres du profil	
Identifiant utilisateur **Mot de passe**	*Requis*. Introduisez l'identifiant utilisateur et le mot de passe pour vous connecter aux téléphones sur lesquels la fonction MP a été activée. Etant donné que l'utilisateur introduira un identifiant et un mot de passe à l'aide du clavier du téléphone, ceux-ci doivent rester courts. Ces identifiant et mot de passe donnent également accès à l'interface CUE.
Prénom **Nom**	*Requis*. Le prénom et le nom de l'utilisateur de la fonction MP sont aussi intégrés à l'annuaire et utilisés par le service "Appeler par nom" du Standard automatique.
Délai d'expiration automatique pour la déconnexion (minutes)	Entrez le temps d'attente (en minutes) avant que l'utilisateur soit automatiquement déconnecté.

Paramètre	Description
Activer le bouton Confidentialité	Lorsque l'option **Activer le bouton Confidentialité** est cochée, un bouton Confidentialité est affiché sur le téléphone. Le bouton Confidentialité est utilisé en mode Conference Barge (cBarge). Le bouton Confidentialité est automatiquement placé sur le téléphone par IOS sur la base des règles suivantes : ▪ Le bouton Confidentialité est affecté derrière la dernière ligne ou le dernier bouton de fonction. Il ne peut pas être placé entre les boutons de ligne ou de fonction. Par exemple, si les boutons 1 et 2 sont utilisés, le bouton Confidentialité est affecté au bouton 3. Si les boutons 1, 2 et 5 sont utilisés, le bouton Confidentialité est affecté au bouton 6, même si les boutons 3 à 4 ne sont pas utilisés. ▪ Si le téléphone ne comporte pas suffisamment de boutons, le bouton Confidentialité n'apparaîtra pas sur le téléphone.

Paramètre	Description
Détails	
Ligne	Sélectionnez l'onglet **Ligne** pour affecter les boutons au profil utilisateur MP. ▪ Pour ajouter ou supprimer des lignes de poste, définissez le nombre de postes souhaités dans le champ **Nombre de lignes de poste**. Vous pouvez introduire jusqu'à 69 postes. Pour chaque bouton : ▪ Sélectionnez un **Type de bouton** (**Normal** ou **Partagé**). Consultez les chapitres **Poste normal, page 356** et **Poste partagé, page 361** pour plus d'informations sur les options de configuration de ces types de bouton. ▪ Définissez les numéros de poste ou sélectionnez un poste partagé. ▪ Entrez une description du bouton. Cet intitulé s'affiche sur le téléphone. ▪ *Facultatif*. Cochez l'option **Messagerie** pour créer une messagerie pour ce poste.
Numérotation abrégée	Sélectionnez l'onglet Numérotation abrégée pour affecter les boutons au profil utilisateur MP. Pour de plus amples informations, consultez la rubrique **Numérotation abrégée, page 337**.

Ajouter un profil de téléphone Mobilité de poste

Cette fenêtre s'affiche lorsque vous cliquez sur **Ajouter** ou **Modifier** sous l'onglet Profils de téléphone du volet Mobilité de poste de la fenêtre Utilisateurs et téléphones.

Le profil de téléphone MP permet d'affecter les boutons et les numéros d'appel rapide que l'utilisateur verra lorsqu'aucun utilisateur MP n'utilise le téléphone.

Définissez le profil utilisateur selon les indications ci-dessous et cliquez sur **OK**.

Paramètre	Description
Paramètres du profil	
Identifiant utilisateur **Mot de passe**	*Facultatif*. L'identifiant utilisateur et le mot de passe sont nécessaires uniquement lorsque la messagerie vocale est active pour ce profil de téléphone. Ces identifiant et mot de passe donnent également accès à l'interface CUE.
Prénom **Nom**	*Facultatif*. Le prénom et le nom de l'utilisateur sont nécessaires uniquement lorsque la messagerie vocale est active pour ce profil de téléphone. Le cas échéant, le prénom et le nom de l'utilisateur de la fonction MP seront aussi intégrés à l'annuaire et utilisés par le service "Appeler par nom" du Standard automatique.

Paramètre	Description
Activer le bouton Confidentialité	Le bouton Confidentialité est utilisé en mode Conference Barge (cBarge). Le bouton Confidentialité est automatiquement placé sur le téléphone par IOS sur la base des règles suivantes : ▪ Le bouton Confidentialité est affecté derrière la dernière ligne ou le dernier bouton de fonction. Il ne peut pas être placé entre les boutons de ligne ou de fonction. Par exemple, si les boutons 1 et 2 sont utilisés, le bouton Confidentialité est affecté au bouton 3. Si les boutons 1, 2 et 5 sont utilisés, le bouton Confidentialité est affecté au bouton 6, même si les boutons 3 à 4 ne sont pas utilisés. ▪ Si le téléphone ne comporte pas suffisamment de boutons, le bouton Confidentialité n'apparaîtra pas sur le téléphone. Le bouton Confidentialité du profil de téléphone peut aussi être piloté à l'aide de la fenêtre **Téléphonie** > **Fonctionnalités voix** > **Conference Barge** une fois affecté à un téléphone.

Paramètre	Description
Détails	
Ligne	Sélectionnez l'onglet Ligne pour définir le nombre de lignes de poste et affecter les boutons au profil de téléphone MP. ▪ Pour ajouter ou supprimer des lignes de poste, définissez le nombre de postes souhaités dans le champ **Nombre de lignes de poste**. Cliquez ensuite sur **OK**. Vous pouvez ajouter jusqu'à 69 postes. ▪ Pour chaque bouton, sélectionnez un type, entrez ou sélectionnez le numéro de poste à affecter et une description du bouton. Vous pouvez uniquement ajouter des boutons de téléphone de type **Normal** et **Partagé**. Consultez les chapitres **Poste normal, page 356** et **Poste partagé, page 361** pour plus d'informations sur les options de configuration de ces boutons.
Numérotation abrégée	Sélectionnez l'onglet Numérotation abrégée pour affecter les boutons au profil de téléphone. Pour de plus amples informations, consultez la rubrique **Numérotation abrégée, page 337**.

Postes analogiques

Les ports repris sous l'onglet Postes analogiques sont les ports FXS pour lesquels le profil **Téléphone ou fax de zone commune** a été configuré dans la fenêtre **Configurer** > **Téléphonie** > **Ports et trunks** > **Ports FXS**. Parmi ces périphériques figurent les téléphones analogiques hérités et les télécopieurs.

Ces notes sont d'application lors de la configuration des numéros de poste analogiques :

- Entrez un numéro de poste dans le champ **Poste**.
- Les fonctions avancées telles que la messagerie vocale, le transfert d'appel, etc. ne sont pas disponibles sur les téléphones configurés comme étant des postes analogiques.

- Pour empêcher les utilisateurs d'appeler les numéros bloqués introduits dans le plan de numérotation sortant, cochez la case **Bloquer les numéros interdits**.
- Le paramètre **Autorisations** définit le type d'appel sortant pouvant être passé à partir de ce téléphone. Pour de plus amples informations, consultez la rubrique **Autorisations, page 359**.

Après avoir apporté les modifications dans la fenêtre, cliquez sur **Enregistrer les paramètres** pour appliquer la configuration.

Configurer l'affectation des boutons du téléphone

Pour plus d'informations sur les types de bouton pouvant être configurés sur le téléphone et pour plus d'informations sur les paramètres Bouton <x> (où <x> désigne le numéro de bouton), consultez les rubriques suivantes :

- **Poste normal, page 356**
- **Poste partagé, page 361**
- **Configuration d'une messagerie générique ou d'une messagerie partagée personnelle pour les postes partagés, page 363**
- **Superviser, page 364**
- **Surveillance, page 364**
- **Ligne CO, page 365**
- **Poste de chevauchement, page 366**
- **Intercom, page 367**
- **Intercom appelable, page 368**
- **Intercom Whisper, page 371**
- **Lignes octales, page 373**

Poste normal

Lorsqu'un bouton est défini comme étant un poste normal, un numéro de poste simple est affecté à ce bouton.

Pour configurer la rubrique **Bouton <x>** pour un bouton de poste normal, procédez comme suit :

ETAPE 1 Sélectionnez **Configurer** > **Téléphonie** > **Utilisateurs et postes** >**Utilisateurs et téléphones** dans la barre de fonctions et activez l'onglet Postes utilisateurs.

ETAPE 2 Cliquez sur un téléphone de la liste pour le sélectionner et cliquez sur le bouton **Modifier** pour afficher les données de configuration.

ETAPE 3 Sélectionnez l'onglet **Affectations des boutons**.

ETAPE 4 Choisissez un numéro de bouton.

ETAPE 5 Dans la rubrique **Bouton <x>**, configurez les paramètres du numéro de poste décrit ci-dessous.

Champ	Description
Type de bouton	Choisissez l'option **Normal** dans le menu déroulant.
Onglet Paramètres	
Poste	Entrez le numéro de poste souhaité pour cette ligne.
Désignation du bouton	Entrez l'intitulé souhaité pour ce bouton.
Description	Entrez une description du téléphone. Cette description s'affiche dans le coin supérieur droit du téléphone. Les caractères acceptés dans ce champ sont les caractères alphanumériques (A-Z, a-z, 0-9, espace, point (.), soulignement (_) et moins (-). Par exemple, votre client peut demander l'affichage du numéro de téléphone DID complet sur les téléphones. Vous pouvez modifier ce champ descriptif de sorte à afficher le numéro DID. Par exemple : 555 555-5555.

Champ	Description
Ligne double ou ligne octale	Type de ligne (double ou octale) La sélection ne concerne que les boutons de type Normal et Partagé. La valeur par défaut est Ligne octale, à condition que le téléphone prenne cette fonction en charge. Un numéro de répertoire de ligne octale prend en charge jusqu'à huit appels actifs, entrants ou sortants, sur un seul bouton. L'option Ligne octale n'est pas disponible pour les téléphones incompatibles avec cette fonction. Les lignes octales sont uniquement disponibles si l'UC500 exécute la version 12.4(20)T ou une version supérieure de Cisco IOS et en présence de la version 7.0(2) ou une version supérieure du logiciel de Cisco UC500. Pour de plus amples informations, consultez la rubrique **Lignes octales, page 373**. Un poste de ligne octale partagé est nécessaire pour permettre la fonction cBarge (Conference Barge). Voir la rubrique **Conference Barge, page 420**.
Activer la messagerie vocale	Cliquez pour activer ou désactiver la messagerie vocale. Si vous cochez l'option Messagerie pour la ligne normale, une messagerie personnelle est créée pour ce numéro de poste. Une seule messagerie est autorisée par utilisateur. La messagerie et son contenu ne sont pas supprimés lorsque vous réaffectez la messagerie à un autre poste.
Bloquer les numéros interdits	Pour empêcher les utilisateurs d'appeler les numéros bloqués introduits dans le plan de numérotation sortant, cochez la case **Bloquer les numéros interdits**.

Champ	Description
Autorisations	Ce paramètre définit le type d'appel sortant pouvant être passé à partir de ce téléphone. Les niveaux d'autorisation sont définis dans le plan de numérotation sortant (**Configurer** > **Téléphonie** > **Plan de numérotation** > **Plan de numérotation sortant et Gestion des appels sortants**). Faites un choix parmi les options suivantes : ▪ **Sans restriction**. Les appels sortants vers le SDA sont autorisés sans restrictions. ▪ **Interne**. Les appels sortants vers les numéros internes et les numéros d'urgence sont autorisés. Tous les autres appels sont interdits. ▪ **Local**. Les appels sortants vers les numéros locaux, internes et les numéros d'urgence sont autorisés. Les appels de type Local-plus, nationaux longue distance et les appels internationaux sont interdits. ▪ **Local-plus**. Les appels sortants pour les numéros locaux, internes et les numéros d'urgence ainsi que les numéros locaux définis dans le plan de numérotation sortant sont autorisés. ▪ **National**. Les appels sortants vers les numéros nationaux longue distance, les numéros locaux, internes et les numéros d'urgence sont autorisés. Les appels de type National-plus et les appels internationaux sont interdits. ▪ **National-plus**. Les appels sortants vers les numéros nationaux longue distance, locaux, internes et les numéros d'urgence ainsi que les numéros définis dans le plan de numérotation sortant sont autorisés. Les appels internationaux sont interdits. ▪ **International**. Les appels sortants pour les numéros internes, locaux, nationaux longue distance, les numéros d'urgence et les numéros internationaux sont autorisés.

Champ	Description
Transfert si occupé	Transfère les appels vers ce poste lorsque la ligne est occupée. Cliquez dans le champ et entrez un numéro de poste pour modifier les paramètres par défaut. Si la case Messagerie est cochée alors que le champ Transfert si occupé est vide, la valeur par défaut entre en vigueur (numéro de poste de la messagerie).
Transfert si pas de réponse	Transférer les appels entrants vers ce poste en cas d'absence de réponse. Cliquez dans le champ et entrez un numéro de poste pour modifier les paramètres par défaut. Si la case Messagerie est cochée alors que le champ Transfert si pas de réponse est vide, la valeur par défaut entre en vigueur (numéro de poste de la messagerie).
Expiration TSNR, secondes	Délai en secondes avant le transfert des appels sans réponse vers la cible Transfert si pas de réponse. La valeur par défaut est 20 secondes. **IMPORTANT** Si ce numéro de poste fait partie d'un groupe d'appel, la valeur **Expiration TSPR** définie doit être supérieure à la valeur d'expiration définie pour le groupe d'appel. Par exemple, si la valeur d'expiration pour le groupe d'appel auquel le poste appartient est de 10 secondes, définissez le délai d'expiration du numéro de poste sur au moins 11 secondes. Vous pouvez aussi réduire le délai d'expiration pour le groupe d'appel. Voir la rubrique **Appeler groupes d'appel, page 400**.
Numéro SDA	Champ en lecture seule signalant que le numéro SDA est associé à un numéro de poste spécifique du plan de numérotation entrant. Pour associer des numéros DID à des postes internes, sélectionnez l'option **Configurer** > **Téléphonie** > **Plan de numérotation** > *Entrant*. Activez l'onglet **Numérotation directe** et définissez les paramètres sous **Appel direct vers les postes utilisateurs internes**.

Champ	Description
Onglet Alerte d'appel en attente	
La fonction Alerte d'appel en attente permet de définir une sonnerie répétitive pour signaler à l'utilisateur lorsqu'un appel est mis en attente sur un téléphone IP Cisco.	
Alerte d'appel en attente	Sélectionnez l'un des paramètres suivants pour définir quand les tonalités signalant un appel en attente peuvent être entendues. ▪ **Aucun**. Les alertes sont désactivées. Il s'agit de la valeur par défaut. ▪ **Veille**. Les alertes sont émises lorsque le téléphone est en veille. ▪ **Veille ou occupé**. Les alertes sont émises lorsque le téléphone est en veille ou occupé. ▪ **Veille ou alerte partagée**. Les alertes sont émises uniquement lorsque le poste est en veille. Les alertes sont émises sur tous les téléphones partageant le numéro de poste.
Délai d'expiration	Nombre de secondes entre les alertes sonores. Introduisez une valeur comprise entre 15 et 300. Par exemple, si la valeur est de 25 secondes, la tonalité d'alerte est émise toutes les 25 secondes.

ETAPE 6 Cliquez sur **OK**.

Poste partagé

Vous pouvez configurer un poste partagé et ajouter un bouton correspondant à plusieurs téléphones afin que les appels entrants vers ce poste soient signalés sur tous les téléphones dotés de ce bouton.

Pour plus d'informations sur la création des messageries vocales pour les postes partagés, consultez la rubrique **Configuration d'une messagerie générique ou d'une messagerie partagée personnelle pour les postes partagés, page 363**.

Pour configurer un numéro de poste partagé, procédez comme suit :

ETAPE 1 Configurez les téléphones et les utilisateurs, conformément au point **Ajout d'un téléphone, page 328**.

ETAPE 2 Sélectionnez **Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Utilisateurs et téléphones** dans la barre de fonctions et activez l'onglet Postes utilisateurs.

ETAPE 3 Cliquez sur un téléphone pour le sélectionner. Cliquez ensuite sur le bouton **Modifier** au bas de la fenêtre pour afficher les détails.

ETAPE 4 Sélectionnez l'onglet **Affectations des boutons**.

ETAPE 5 Cliquez sur un numéro de bouton du tableau et réglez le type sur **Partager**.

ETAPE 6 Dans le champ **Poste** correspondant au bouton de ce téléphone, entrez ou sélectionnez le poste à utiliser pour la ligne partagée.

- Pour créer un nouveau poste partagé, introduisez le numéro de poste à utiliser.
- Pour affecter un poste partagé existant à un bouton donné, sélectionnez le numéro dans la liste déroulante.
- Si vous avez sélectionné Bouton 1 sur le téléphone pour le poste partagé, seuls les postes partagés correspondant au bouton 1 des autres téléphones figurent dans la liste.
- Si vous avez sélectionné un autre bouton, les numéros de poste autres que ceux associés au bouton 1 figurent dans la liste.

ETAPE 7 S'il s'agit d'un nouveau poste partagé, configurez la rubrique **Bouton <x>** correspondant à la ligne partagée conformément au chapitre **Poste normal, page 356**.

Les messageries sont gérées différemment en ce qui concerne les postes partagés. Pour de plus amples informations, consultez la rubrique **Configuration d'une messagerie générique ou d'une messagerie partagée personnelle pour les postes partagés, page 363**.

ETAPE 8 Dans le champ **Nom partagé**, entrez le numéro de poste utilisé pour ce poste partagé. Un nom doit être introduit si le poste partagé est associé à un bouton non primaire.

REMARQUE Le champ **Nom partagé** est désactivé si le poste partagé se trouve sur le bouton 1 du téléphone. Pour les postes associés au bouton 1, les données utilisateur correspondent à celles de l'utilisateur pour qui le poste partagé a été créé (à l'exception de l'identifiant et du mot de passe qui sont propres au téléphone).

ETAPE 9 Lorsque vous avez terminé, cliquez sur **OK**.

ETAPE 10 Effectuez des appels vers le poste partagé afin de vérifier si les paramétrages sont corrects.

Configuration d'une messagerie générique ou d'une messagerie partagée personnelle pour les postes partagés

Lorsque vous activez la messagerie pour un poste partagé, le type de messagerie créé par défaut est différent entre les postes partagés correspondant au bouton 1 du téléphone et ceux associés aux autres boutons :

- Si l'option **Activer messagerie** est cochée pour le bouton 1 d'un téléphone, une messagerie partagée personnelle est créée par défaut. Cette fonction est prévue pour les cas où un utilisateur dispose de plusieurs téléphones, mais souhaite une même messagerie accessible à partir de tous ces téléphones.
  Si pour une raison quelconque l'utilisateur disposant de plusieurs téléphones souhaite utiliser le bouton 1 pour cela, vous pouvez créer le poste partagé sur un autre. Accédez ensuite à l'onglet Boîtes de réception de la fenêtre Messagerie et faites de la messagerie générique une messagerie partagée personnelle. Sélectionnez enfin l'identifiant utilisateur dans la liste déroulante. Seuls les utilisateurs de cette ligne partagée ne disposant pas encore d'une messagerie personnelle figurent dans la liste. Après avoir défini une messagerie partagée personnelle et sélectionné un utilisateur, CCA supprime la messagerie générique et crée une messagerie personnelle pour le poste partagé sur la base de l'identifiant utilisateur.

  Vous pouvez également définir un poste normal pour l'utilisateur et lui affecter une messagerie personnelle. Vous pouvez ensuite définir le poste comme poste partagé à l'aide du même numéro de poste et activer la messagerie vocale. CCA conservera la messagerie personnelle et la réaffectera au poste partagé.

- Si l'option **Activer messagerie** est cochée pour un autre bouton d'un téléphone, une messagerie générique est créée par défaut. Lorsque vous affectez une messagerie générique à un poste partagé, l'utilisateur doit aussi disposer d'une messagerie personnelle afin de pouvoir accéder à la messagerie générique à l'aide de son code personnel.

  Lorsque vous ajoutez le poste partagé aux autres téléphones, veillez à activer la messagerie pour ce poste si vous voulez pouvoir accéder à la messagerie générique.

Superviser

Le bouton Superviser assure le suivi du poste défini uniquement.

L'état de ligne indique si la ligne est en attente ou utilisée. La réceptionniste pourra utiliser les boutons de supervision pour contrôler visuellement l'état des différents postes téléphoniques.

Pour configurer un bouton Superviser, procédez comme suit :

ETAPE 1 Sélectionnez **Configurer** > **Téléphonie** > **Utilisateurs et postes >Utilisateurs et téléphones** dans la barre de fonctions et activez l'onglet Postes utilisateurs.

ETAPE 2 Cliquez sur un téléphone de la liste pour le sélectionner et cliquez sur le bouton **Modifier** pour afficher les données de configuration.

ETAPE 3 Sélectionnez l'onglet **Affectations des boutons**.

ETAPE 4 Cliquez sur un numéro de bouton du tableau et réglez le **Type** sur **Superviser**.

ETAPE 5 Dans le volet **Bouton <x>** correspondant, sélectionnez le numéro de poste à superviser dans la liste déroulante. Les postes de parcage d'appels figurent dans la liste des numéros pouvant être supervisés.

L'étiquette du poste supervisé est automatiquement insérée dans le champ Étiquette du bouton Superviser.

ETAPE 6 Cliquez sur **OK**.

Surveillance

Le bouton Surveillance permet à l'utilisateur de surveiller toutes les lignes du téléphone correspondant au numéro de poste.

Le témoin d'état du bouton Surveillance devient rouge à chaque fois qu'une ligne du téléphone surveillé est utilisée, hors service ou en mode Ne pas déranger.

L'utilisateur du téléphone peut appuyer sur le bouton Surveillance pour accéder au numéro de poste surveillé. Aucun appel ne peut être envoyé ou reçu à l'aide d'un bouton de ligne en mode Surveillance. Les appels entrants sur un bouton de ligne en mode Surveillance ne sonnent pas et n'affichent ni l'identifiant de l'appelant ni l'identifiant de l'appelant en attente.

Pour configurer un bouton Surveillance, procédez comme suit :

ETAPE 1 Sélectionnez **Configurer** > **Téléphonie** > **Utilisateurs et postes >Utilisateurs et téléphones** dans la barre de fonctions et activez l'onglet Postes utilisateurs.

ETAPE 2 Cliquez sur un téléphone de la liste pour le sélectionner et cliquez sur le bouton **Modifier** pour afficher les données de configuration.

ETAPE 3 Sélectionnez l'onglet **Affectations des boutons**.

ETAPE 4 Cliquez sur un numéro de bouton du tableau et réglez le**Type** sur **Surveillance**.

ETAPE 5 Dans le volet **Bouton <x>** correspondant, sélectionnez le numéro de poste à surveiller dans la liste déroulante.

L'étiquette du poste surveillé est automatiquement insérée dans le champ Étiquette du bouton Surveillance.

ETAPE 6 Cliquez sur **OK**.

Ligne CO

Sélectionnez l'option Ligne CO si vous souhaitez affecter une ligne de siège central (Central Office) à ce bouton. Il s'agira d'une ligne de trunk directe. Vous ne pouvez pas affecter de messagerie à un bouton de ligne CO.

Pour configurer un bouton Ligne CO, procédez comme suit :

ETAPE 1 Sélectionnez **Configurer** > **Téléphonie** > **Utilisateurs et postes >Utilisateurs et téléphones** dans la barre de fonctions et activez l'onglet Postes utilisateurs.

ETAPE 2 Cliquez sur un téléphone de la liste pour le sélectionner et cliquez sur le bouton **Modifier** pour afficher les données de configuration.

ETAPE 3 Sélectionnez l'onglet **Affectations des boutons**.

ETAPE 4 Choisissez un numéro de bouton.

ETAPE 5 Dans le menu déroulant **Type** correspondant au bouton, sélectionnez l'option **Ligne CO** ; par exemple, **CO 1 (0/1/0)**.

Ces éléments correspondent aux lignes de trunk SDA directes reliées aux ports FXO. Modifiez le champ **Étiquette** afin de pouvoir identifier la ligne CO.

ETAPE 6 Dans le volet **Bouton <x>** correspondant, sélectionnez le numéro de ligne CO dans la liste déroulante.

ETAPE 7 Cliquez sur **OK**.

Poste de chevauchement

Un poste de chevauchement normal permet à plusieurs lignes (25 maximum) de se partager un même bouton sur un téléphone doté de plusieurs boutons. Les postes de chevauchement demandent au moins deux numéros de postes normaux, partagés ou de ligne CO.

CCA prend aussi en charge la configuration du chevauchement pour la ligne du siège central (SC). Cette configuration permet à la ligne du siège central de partager un bouton avec un poste standard. L'utilisateur peut alors répondre aux appels sur la ligne SC et afficher l'état de la ligne tout en pouvant passer et recevoir des appels à l'aide de son poste standard. Cette fonction est particulièrement utile sur les téléphones dotés d'un nombre limité de boutons.

REMARQUE Les lignes octales ne prennent pas en charge la fonction de chevauchement. En d'autres termes, les postes associés à des fonctions telles que Conférence ou Conference Barge (cBarge) ne peuvent pas faire l'objet d'un chevauchement.

Pour configurer un bouton Chevauchement, procédez comme suit :

ETAPE 1 Sélectionnez **Configurer** > **Téléphonie** > **Utilisateurs et postes >Utilisateurs et téléphones** dans la barre de fonctions et activez l'onglet Postes utilisateurs.

ETAPE 2 Cliquez sur un téléphone de la liste pour le sélectionner et cliquez sur le bouton **Modifier** pour afficher les données de configuration.

ETAPE 3 Sélectionnez l'onglet **Affectations des boutons**.

ETAPE 4 Cliquez sur un numéro de bouton dans le tableau et réglez le **Type** sur **Chevauchement**.

ETAPE 5 Dans le volet **Bouton <x>** correspondant, sélectionnez le numéro à utiliser pour le chevauchement dans la liste déroulante.

ETAPE 6 Dans la rubrique **Bouton <x>**, définissez les paramètres suivants :

a. Indiquez si vous souhaitez activer ou désactiver la mise en attente pour le poste de chevauchement. Si vous cochez l'option **Activer la mise en attente d'appels**, la fonction de mise en attente sera active sur le poste de chevauchement.

   Lorsque la mise en attente est active, si le chevauchement de poste est actif et

qu'un deuxième appel atteint le poste de chevauchement, la tonalité d'attente est activée et l'appel s'affiche à l'écran du téléphone IP.

b. Utilisez les boutons **Ajouter**, **Supprimer**, **Sélectionner tout** et **Sélectionner aucun** pour déplacer les postes partagés de la liste des Postes disponibles vers la liste des Postes sélectionnés.

   Vous devez sélectionner au moins deux (2) numéros de poste pour le bouton Chevauchement. Les postes de type Normal, Partagé et Ligne CO s'affichent dans la liste Postes disponibles.

c. Vous pouvez utiliser les flèches **Haut** et **Bas** pour réorganiser les numéros de poste dans la liste Postes sélectionnés.

d. *Facultatif*. Dans le champ **Désignation du bouton de chevauchement**, entrez un nom pour le poste. Il s'affichera sur le téléphone.

   Par défaut, la dénomination du premier numéro de poste de la liste Sélectionné est utilisée comme intitulé pour le bouton de chevauchement. Lorsque vous modifiez l'intitulé du bouton de chevauchement, vous modifiez également le libellé du premier numéro de poste.

ETAPE 7 Cliquez sur **OK**.

Intercom

Le bouton Intercom correspond à une ligne d'interphone entre deux téléphones IP.

- Plusieurs interphones peuvent être configurés sur un téléphone.
- Le bouton 1 ne peut pas être configuré comme interphone.

Pour configurer un bouton Intercom, procédez comme suit :

ETAPE 1 Sélectionnez **Configurer** > **Téléphonie** > **Utilisateurs et postes >Utilisateurs et téléphones** dans la barre de fonctions et activez l'onglet Postes utilisateurs.

ETAPE 2 Cliquez sur un téléphone de la liste pour le sélectionner et cliquez sur le bouton **Modifier** pour afficher les données de configuration.

ETAPE 3 Sélectionnez l'onglet **Affectations des boutons**.

ETAPE 4 Cliquez sur un numéro de bouton et choisissez le **Type Intercom**.

ETAPE 5 Dans la rubrique **Bouton <x>**, définissez les paramètres suivants :

a. Dans la liste déroulante **Utilisateur du bouton d'interphonie cible**, sélectionnez un utilisateur cible. Le bouton d'interphone se trouve alors sur le téléphone de l'utilisateur.

b. Dans la liste déroulante **Numéro du bouton d'interphonie cible**, sélectionnez un bouton disponible sur le téléphone ciblé par l'intercom.

c. Dans le champ **Etiquette pour l'utilisateur cible**, entrez le texte que vous souhaitez afficher sur le téléphone de l'utilisateur cible pour le bouton de l'intercom.

   Lorsque vous appuyez sur le bouton de l'intercom, ce texte s'affiche dans le champ De : du volet contenant les données d'appel sur le téléphone cible.

d. Dans le champ **Etiquette pour l'utilisateur actif**, entrez le texte que vous souhaitez afficher sur le téléphone de l'utilisateur pour le bouton de l'intercom.

   Lorsque vous appuyez sur le bouton Intercom, ce texte s'affiche dans le champ A : du volet contenant les données d'appel sur le téléphone cible.

ETAPE 6 Choisissez si vous souhaitez activer ou désactiver la fonction Silence pour l'intercom.

Lorsque la fonction **Muet** est active, le destinataire doit désactiver la fonction Muet sur son téléphone ou décrocher pour répondre.

Lorsque la fonction **Silence** est désactivée, les deux parties peuvent s'entendre dès que la communication est établie.

ETAPE 7 Cliquez sur **OK**.

Intercom appelable

Pour plus d'informations sur les intercoms appelables, consultez les rubriques suivantes :

- **Description de la fonction, page 368**
- **Téléphones non pris en charge, page 369**
- **Etapes de configuration, page 370**

Description de la fonction

Bouton d'interphone permettant à l'utilisateur d'appeler tout autre téléphone du système doté d'un bouton d'interphone appelable par la simple pression sur le bouton et l'appel du numéro de poste à joindre.

A la différence des intercoms standard et Whisper qui sont toujours configurés entre deux téléphones donnés, les utilisateurs peuvent appeler d'autres téléphones en appuyant sur le bouton d'intercom de leur téléphone et en composant le numéro de poste de l'intercom appelable.

Les intercoms appelables sont utilisés par les opérateurs ou le personnel administratif assurant l'assistance aux employés, à la différence des assistants administratifs qui prennent généralement en charge une ou deux personnes et disposent de boutons d'intercom propres à chacune d'elles. Lorsque cette fonction est utilisée, un bouton d'intercom appelable est configuré sur le téléphone de chaque utilisateur.

Un seul bouton d'interphone appelable peut être configuré par téléphone.

CCA ne permet pas d'associer un intercom appelable au bouton 1 d'un téléphone.

Vous pouvez configurer les intercoms appelables avec ou sans fonction Silence.

- Lorsque la fonction **Silence** est active pour l'intercom, le téléphone appelé répond automatiquement à l'appel à l'aide du haut-parleur et la fonction Silence est activée. Le téléphone sonne en cas de réponse automatique à un appel d'intercom afin d'avertir le destinataire.

  Pour répondre à l'appel et permettre un échange, le destinataire doit désactiver la fonction Silence en appuyant sur le bouton Silence de son téléphone ou, sur certains téléphones, en levant le combiné.

- Lorsque la fonction **Silence** est désactivée, les deux parties peuvent s'entendre dès que la communication est établie.

  L'avantage offert par la désactivation de la fonction Silence est que le destinataire d'un appel d'intercom peut parler et être entendu sans devoir désactiver la fonction Silence. Cependant, des sons ou des conversations émanant de l'environnement pourront être entendus dès que la connexion aura été établie.

Téléphones non pris en charge

Les intercoms appelables ne sont pas pris en charge sur les téléphones suivants :

- Téléphones analogiques
- ATA

Etapes de configuration

Pour configurer un bouton Intercom appelable, procédez comme suit :

ETAPE 1 Sélectionnez **Configurer** > **Téléphonie** > **Utilisateurs et postes >Utilisateurs et téléphones** dans la barre de fonctions et activez l'onglet Postes utilisateurs.

ETAPE 2 Cliquez sur un téléphone de la liste pour le sélectionner et cliquez sur le bouton **Modifier** pour afficher les données de configuration.

ETAPE 3 Sélectionnez l'onglet **Affectations des boutons**.

ETAPE 4 Dans la liste des boutons, cliquez sur une ligne du tableau pour sélectionner un bouton pour lequel vous souhaitez configurer la fonction Intercom appelable.

Un seul bouton d'interphone appelable peut être configuré par téléphone.

ETAPE 5 Dans le menu déroulant **Type**, sélectionnez l'option **Intercom appelable**.

ETAPE 6 Dans le volet **Intercom appelable** sur la droite, configurez les paramètres suivants :

a. Sélectionnez un numéro de poste dans le menu déroulant **Composition**. Il s'agit du numéro que les utilisateurs devront composer pour utiliser le téléphone comme intercom. Tous les numéros de poste standard définis sur le téléphone sont repris dans la liste.

b. Choisissez si vous souhaitez activer ou désactiver la fonction **Silence** pour les appels d'intercom.

   Lorsque la fonction **Silence** est activée, le téléphone appelé répond automatiquement à l'appel en mode Haut-parleur et la fonction Silence est activée. Le destinataire doit désactiver le bouton Silence pour pouvoir parler. Lorsque le bouton **Silence** est désactivé, les deux intervenants s'entendent immédiatement.

ETAPE 7 *Facultatif*. Dans la colonne **Etiquette** de la liste des boutons, modifiez l'intitulé du bouton de l'intercom appelable affiché sur le téléphone. La valeur par défaut est Dialable Intercom<*Ext*>.

ETAPE 8 Cliquez sur **OK**.

Intercom Whisper

L'intercom Whisper permet d'appeler un poste occupé. L'appelant peut uniquement être entendu par le destinataire. Pour de plus amples informations, consultez les rubriques suivantes :

- **Description de la fonction, page 371**
- **Eléments requis et restrictions, page 371**
- **Téléphones non pris en charge, page 372**
- **Procédures, page 372**

Description de la fonction

Pour passer un appel à l'aide de l'intercom Whisper, l'utilisateur doit appuyer sur le bouton Intercom Whisper de son téléphone.

- Le téléphone qui reçoit l'appel affiche le numéro de poste et le nom de la personne à l'origine de l'appel. Un signal sonore distinct est émis avant que le destinataire entende la voix de l'appelant. Le bouton Intercom Whisper passe à l'orange pour indiquer un flux unidirectionnel.
- Si le destinataire de l'intercom Whisper souhaite parler à l'appelant, il devra appuyer sur le bouton Intercom Whisper de son téléphone. Le bouton passera au vert pour indiquer un appel bidirectionnel.
- Lorsque le destinataire de l'appel à l'aide de l'intercom Whisper appuie sur le bouton Intercom Whisper pour parler, l'appel actif sur son téléphone est mis en attente.

Pour mettre fin à un appel à l'aide de l'intercom Whisper, l'utilisateur doit appuyer sur la touche **EndCall**.

Eléments requis et restrictions

Les critères et les restrictions suivantes s'appliquent aux intercoms Whisper configurés à l'aide de CCA :

- L'intercom Whisper nécessite Cisco Unified CME 7.1 et SCCP 12.0 ou des versions supérieures sur le téléphone IP.
- La fonction intercom Whisper exige CIPC 7.x ou une version supérieure sur les téléphones CIPC (Cisco IP Communicator).
- Le bouton Intercom Whisper permet de passer des appels uniquement vers un autre intercom Whisper.

- Un seul appel d'interphonie à la fois est autorisé (entrant ou sortant) sur le téléphone.

Téléphones non pris en charge

La fonction Intercom Whisper est uniquement disponible sur les téléphones prenant en charge les lignes octales. Les intercoms Whisper ne sont pas pris en charge sur les téléphones suivants :

- Téléphones FXS analogiques
- ATA
- Téléphones IP Cisco 7931 dotés d'un microprogramme dont la version est antérieure à 8.5(3)
- Téléphones IP de la série Cisco 3900
- Téléphones IP Cisco CP-521
- Téléphones IP Cisco SPA500 et SPA300
- Téléphones IP Cisco 7902, 7905, 7906, 7910, 7911 et 7912
- Téléphones IP Cisco 7940 et 7960

Procédures

Pour configurer un bouton d'intercom Whisper, procédez comme suit :

ETAPE 1 Sélectionnez **Configurer** > **Téléphonie** > **Utilisateurs et postes >Utilisateurs et téléphones** dans la barre de fonctions et activez l'onglet Postes utilisateurs.

ETAPE 2 Cliquez sur un téléphone de la liste pour le sélectionner et cliquez sur le bouton **Modifier** pour afficher les données de configuration.

ETAPE 3 Sélectionnez l'onglet **Affectations des boutons**.

ETAPE 4 Cliquez sur un numéro de bouton et choisissez le **Type Intercom Whisper**.

ETAPE 5 Dans la rubrique **Bouton <x>**, définissez les paramètres suivants :

a. Dans la liste déroulante **Utilisateur du bouton d'interphonie cible**, sélectionnez un utilisateur cible. Le bouton Intercom Whisper se trouve alors sur le téléphone de l'utilisateur.

b. Dans la liste déroulante **Numéro du bouton d'intercom Whisper**, sélectionnez un bouton disponible sur le téléphone ciblé par l'intercom Whisper.

c. Dans le champ **Etiquette pour l'utilisateur cible**, entrez le texte que vous souhaitez afficher sur le téléphone de l'utilisateur cible pour le bouton Intercom Whisper.

   Lorsque vous appuyez sur le bouton de l'intercom Whisper, ce texte s'affiche dans le champ De : du volet contenant les données d'appel sur le téléphone cible.

d. Dans le champ **Etiquette pour l'utilisateur actif**, entrez le texte que vous souhaitez afficher sur le téléphone de l'utilisateur pour le bouton de l'intercom Whisper.

   Lorsque vous appuyez sur le bouton de l'intercom Whisper, ce texte s'affiche dans le champ De : du volet contenant les données d'appel sur le téléphone cible.

ETAPE 6 Cliquez sur **OK**.

Lignes octales

Un numéro d'annuaire de ligne octale prend en charge jusqu'à huit appels actifs, entrants ou sortants, sur un seul bouton.

- A la différence du numéro d'annuaire de ligne double, qui est quant à lui partagé exclusivement par les téléphones (suite à la réponse à un appel, le téléphone détient les deux canaux propres au numéro d'annuaire de ligne double), le numéro d'annuaire de ligne octale peut répartir ses canaux entre plusieurs téléphones partageant le même numéro dans l'annuaire.
- Tous les téléphones sont autorisés à effectuer ou recevoir des appels sur les canaux en attente associés au numéro d'annuaire de ligne octale. Un numéro d'annuaire de ligne octale peut prendre en charge plusieurs appels. Les appels multiples vers un numéro d'annuaire de ligne octale sont signalés simultanément.
- Dès qu'un téléphone répond à un appel, la sonnerie s'interrompt sur le téléphone en question et la tonalité d'appel en attente est activée pour les autres appels entrants.
- Lorsque plusieurs téléphones se partagent un numéro d'annuaire de ligne octale, les appels entrants sont signalés sur les téléphones disponibles, lesquels peuvent ainsi prendre l'appel. Sur les téléphones occupés, l'appel est signalé grâce à la tonalité d'attente.

- Chaque téléphone partageant ce numéro d'annuaire peut prendre tout appel arrivé sur un numéro d'annuaire de ligne octale et mis en attente. Si un utilisateur effectue un transfert de communication ou crée une conférence, l'appel est verrouillé et les autres téléphones partageant le numéro d'annuaire de ligne octale ne pourront pas prendre la communication.
- Les appels manqués (appels sans réponse) ne sont pas affichés par défaut.
- Un poste de ligne octale partagé est nécessaire pour permettre la fonction cBarge (Conference Barge). Pour de plus amples informations, consultez la rubrique **Conference Barge, page 420**.

Les restrictions suivantes s'appliquent aux lignes octales :

- Les lignes octales ne prennent pas en charge la fonction de chevauchement. En d'autres termes, les postes associés à des fonctions telles que Conférence ou Conference Barge (cBarge) ne peuvent pas faire l'objet d'un chevauchement.
- Les lignes octales sont uniquement disponibles si l'UC500 exécute la version 12.4(20)T ou une version supérieure de Cisco IOS et en présence de la version 7.0(2) ou une version supérieure du logiciel Cisco Unified Communications Manager Express (CUCME). La mise à jour vers le dernier paquet logiciel de l'UC500 est recommandée.
- Certains téléphones IP Cisco ne prennent pas en charge les lignes octales.
- Les modèles de téléphone IP Cisco 7920, 7902, 7931G, CP-52xG, CP-52xSG et Cisco SPA500 ne prennent pas en charge les lignes octales.
- Les ports Cisco ATA et les ports analogiques FXS ne sont pas compatibles avec les lignes octales.

Messagerie et notifications

Cette rubrique explique comment configurer les fonctions de messagerie et de notification suivantes :

Pour configurer les paramètres de la messagerie vocale et de la boîte de réception, sélectionnez l'option **Configurer** > **Téléphonie** > **Utilisateurs et postes**> **Messagerie** dans la barre de fonctions. Consultez les rubriques suivantes pour plus d'informations sur l'activation et la configuration des fonctions de la messagerie vocale.

- **Vue d'ensemble**

- Consignes générales
- Configuration initiale
- Boîtes de réception
- Notifications

Vue d'ensemble

La fenêtre Messagerie vous permet de configurer les paramètres de base de la messagerie pour le site, d'afficher et de modifier l'espace réservé à la messagerie vocale (en minutes) pour chaque boîte de réception.

Consignes générales

Les consignes suivantes s'appliquent aux messageries vocales et aux notifications :

- Lorsque vous ajoutez des utilisateurs et des téléphones à l'aide de l'Assistant de configuration de la téléphonie, les messageries vocales sont créées si l'option correspondante est activée.
- Les utilisateurs pourront ainsi accéder à leur messagerie vocale à partir de n'importe quel téléphone du système en composant simplement le numéro de la messagerie ou le code d'accès SDA. Ils sont invités à introduire le code PIN de la messagerie afin d'y accéder. Le code PIN pour accéder à la messagerie vocale est 1234. Les utilisateurs accédant pour la première fois à la messagerie vocale seront invités à modifier leur code PIN.
- Lorsque vous ajoutez des utilisateurs en mode Expert ou en chargeant un fichier .xml, les messageries personnelles sont créées sur le système à condition que les paramètres **Transfert si occupé** ou **Transfert si pas de réponse** aient été associés à la messagerie pour chaque poste de type Normal. Ces éléments sont définis sous l'onglet Postes utilisateurs de la fenêtre Modifier téléphone (**Configurer** > **Téléphonie** > **Utilisateurs et postes**> **Utilisateurs et téléphones** > **Modifier téléphone**).
- Le paramètre par défaut pour les options **Transfert si occupé** ou **Transfert si pas de réponse** est Messagerie. En d'autres termes, si vous ajoutez un utilisateur et ne modifiez pas ces paramètres lors de l'opération, une messagerie vocale sera automatiquement créée pour l'utilisateur en question. Vous pourrez désactiver la messagerie par la suite à partir de l'onglet Postes utilisateurs de la fenêtre Modifier téléphone (**Configurer** > **Téléphonie** > **Utilisateurs et postes**> **Utilisateurs et téléphones** > **Modifier téléphone**).

- Lorsque vous modifiez les paramètres pour les options **Transfert si occupé** et **Transfert si pas de réponse** en passant de la valeur Messagerie à une autre, la messagerie de l'utilisateur demeure sur le système. Si vous voulez priver un utilisateur d'une messagerie vocale, vous devrez la désactiver manuellement à partir de l'onglet Postes utilisateurs de la fenêtre Modifier téléphone(**Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Utilisateurs et téléphones**> **Modifier téléphone**).
- Vous pouvez créer une messagerie par utilisateur et l'associer à n'importe quel numéro de poste de type Normal défini pour l'utilisateur ou à un poste personnel (partagé).
- Les messageries génériques sont créées pour les lignes partagées, les groupements de postes et les groupes d'appel lorsque la fonction **Transfert si pas de réponse vers** pour le groupe ou la ligne partagée est définie sur la valeur Messagerie. Vous pouvez aussi opter pour la création d'une messagerie partagée personnelle pour un poste partagé.

ASTUCE : Le Tableau de bord (**Accueil** > **Tableau de bord**) dispose d'une option **Etat de la messagerie** offrant un récapitulatif de l'espace utilisé, des informations et l'état propre à chaque messagerie.

Configuration initiale

L'onglet Configuration initiale vous permet de définir les paramètres de base pour la messagerie vocale d'un site :

- Numéro d'accès à la messagerie et numéro SDA
- Préfixe pour le transfert direct vers la messagerie
- Paramètres de site généraux pour activer la notification des messages par téléphone et/ou par e-mail
- Activation des fonctions VoiceView Express et LiveReply pour le site

Pour configurer les paramètres de la messagerie vocale, complétez les champs de l'onglet Configuration initiale conformément au tableau ci-dessous et cliquez sur **OK**.

Paramètre	Description
Numéros d'accès	
Numéro d'accès à la messagerie	Numéro de poste interne permettant d'accéder à la messagerie. Le numéro d'accès à la messagerie par défaut est le 399.
SDA de la Messagerie	*Facultatif*. Numéro SDA externe permettant d'accéder à la messagerie. Il doit s'agir d'un numéro E.164 complet. Ce numéro est celui que les appelants externes composent pour accéder à la messagerie. Le numéro SDA pour l'accès à la messagerie peut commencer par un caractère "+".
Fonctions de la messagerie vocale	
VoiceView Express	**VoiceView Express** permet aux utilisateurs d'interagir avec leur messagerie vocale Cisco Unity Express à l'aide de l'écran de leur téléphone IP et des touches s'y trouvant. Les utilisateurs peuvent gérer les options de leur messagerie, gérer les notifications, envoyer, écouter, enregistrer et gérer leurs messages vocaux. Cette fonction offre une alternative à l'interface utilisateur pour la téléphonie (TUI) et à l'interface Web. Le paramètre est activé par défaut.

Paramètre	Description
Live Reply	**Live Reply** permet aux abonnés Cisco Unity Express écoutant leurs messages vocaux par téléphone ou par Voice View Express de répondre aux messages en appuyant sur 4-4. Lorsque la fonction Live Reply est invoquée, Cisco Unity Express tente d'établir la liaison entre les deux parties. En cas de réussite, l'utilisateur est mis en contact avec son interlocuteur ou l'appel est transféré selon les règles définies par lui. Au terme de l'appel, la liaison à la messagerie prend fin. L'utilisateur n'est pas renvoyé vers la messagerie. Pour passer en revue les autres messages vocaux au terme d'une session LiveReply, l'utilisateur devra composer à nouveau le code d'accès à la messagerie. Le paramètre est désactivé par défaut.

Paramètre	Description
Lire l'identifiant de l'appelant pour les messages entrants	Active ou désactive la lecture de l'identifiant de l'appelant pour les messages entrants vers la messagerie. Lorsque la fonction **Lire l'identifiant de l'appelant pour les messages entrants** est active et qu'un message est reçu sur la messagerie vocale, selon que l'appel entrant provient d'un numéro interne ou externe : ▪ **Appels internes**. Si l'identifiant de l'appelant correspond à une valeur du répertoire local, le système cite le nom de l'appelant à partir du répertoire local lorsque le destinataire écoute le message. ▪ **Appels externes**. Si l'identifiant de l'appelant ne correspond pas à une valeur de l'annuaire local, le système cite le numéro de l'appelant lorsque le destinataire écoute le message. Pour les appels externes, le système ne vérifie pas si les données de l'appelant sont valables. Cette fonction dépend de la configuration du siège central et de la configuration des trunks entrants. Un appel externe provient de tout téléphone ne figurant pas dans le répertoire local. Les sources possibles pour les appels externes sont la compagnie locale des téléphones, un téléphone IP ou une passerelle H.323. Ces sources doivent être configurées pour présenter l'identifiant de l'appelant à la messagerie vocale.

Paramètre	Description
Transfert direct	

Paramètre	Description
Activer le transfert direct vers la messagerie	Cochez cette option pour activer le **transfert direct vers la messagerie vocale** et définir un **préfixe pour le transfert vers la messagerie vocale**. Le **Préfixe pour le transfert vers la messagerie vocale** peut être un chiffre compris entre Le préfixe est utilisé par le Standard automatique et par les utilisateurs qui ne disposent pas d'une touche spécifique pour transférer les appels vers leur messagerie. Le préfixe doit être différent du code d'accès au standard pour les appels extérieurs et du premier numéro d'un poste interne. Lorsque cette fonction est activée, le Standard automatique est mis à jour de sorte à intégrer l'option propre au transfert direct vers la messagerie vocale. Lorsque vous activez ou désactivez la fonction **Transfert direct vers la messagerie vocale**, les téléphones IP sont réinitialisés et les touches sont ajoutées ou supprimées selon le cas. Lorsque la fonction **Transfert direct vers la messagerie vocale** est active, les utilisateurs des téléphones IP disposant de la touche **TrnsferVM** peuvent transférer les appels directement vers une messagerie personnelle ou de groupe en procédant comme suit : 1. En appuyant sur la touche **TrnsferVM** de leur téléphone. 2. En introduisant le numéro de poste propre à la messagerie personnelle ou de groupe. 3. En appuyant à nouveau sur la touche **TrnsferVM** pour effectuer le transfert. Les utilisateurs ne disposant pas de la touche permettant le transfert vers la messagerie peuvent effectuer l'opération de la manière suivante : 1. Appuyez sur la touche **Trnsfer**. 2. Entrez le préfixe pour le transfert vers la messagerie, suivi du numéro de poste de l'utilisateur. Par exemple, si le préfixe est le 6 et que vous souhaitez transférer un message vers le numéro 201, vous devrez appuyer sur la touche **Trnsfer** et terminer par 6201.

Paramètre	Description
Notification par la messagerie vocale Activer et configurer les paramètres en vigueur sur le site en ce qui concerne les notifications en provenance de la messagerie vocale.	
Activer la notification par la messagerie vocale	Cette fonction est désactivée par défaut. Vous devez cocher l'option Activer la notification par la messagerie vocale avant de configurer les paramètres du site relatifs aux notifications pour la messagerie et les téléphones ainsi que pour activer les notifications pour vos utilisateurs. Désactiver les notifications de la messagerie vocale. Si les notifications ne sont pas actives et que vous cochez cette option, CCA réinitialisera les paramètres de notification.

Paramètre	Description
Programme de notification	Indiquez quand le système doit envoyer la notification : ▪ Cliquez sur **De 8 à 17 h** du lundi au vendredi Ou ▪ Cliquez sur **24 h/24** et 7 j/7.
Notification par e-mail	Définissez les paramètres suivants pour activer et configurer l'envoi des notifications de la messagerie vocale par e-mail. ▪ Cochez l'option **Activer la notification par e-mail** pour envoyer les notifications par e-mail pour le site. ▪ Dans le champ **Adresse de réponse pour les e-mails sortants :** , introduisez l'adresse e-mail qui s'affichera dans le champ De : pour les e-mails envoyés par le système de messagerie. ▪ Dans le champ **Adresse du serveur SMTP**, introduisez le nom d'hôte ou l'adresse IP du serveur SMTP que la messagerie devra utiliser pour envoyer les notifications. Vous devez *activer le service DNS* pour pouvoir utiliser un nom d'hôte. ▪ Entrez le numéro de **port du serveur SMTP**. ▪ Si le serveur SMTP exige une authentification, cochez l'option **Authentification nécessaire** et introduisez le nom d'utilisateur et le mot de passe correspondants.
Notification par téléphone	L'option **Autoriser les destinataires de la notification à accéder à la fenêtre de connexion à la messagerie** doit être cochée si vous souhaitez permettre l'envoi des notifications de la messagerie vers des téléphones. Cette option est désactivée par défaut.

Boîtes de réception

Sous l'onglet Boîtes de réception se trouvent les données relatives à l'espace disponible et un récapitulatif des messageries personnelles et de groupe.

Définissez les paramètres de la messagerie conformément à la description ci-dessous. Cliquez ensuite sur **OK**.

Champ	Description	
Espace	Espace libre et espace utilisé par la messagerie (en minutes) pour le système.	
Récapitulatif	Récapitulatif pour chaque messagerie vocale.	
	Nom (Identifiant utilisateur)	Identifiant utilisateur du téléphone, identifiant du groupe (par exemple : hunt1 ou blast1) ou ligne partagée pour la messagerie sélectionnée.
	Poste	Poste utilisateur, numéro pilote pour le groupement de postes ou le groupe d'appel, numéro de la ligne partagée pour la messagerie sélectionnée.
	Boîte de réception	État de la messagerie (Activée ou Aucun).
	Taille	Taille de la messagerie, en minutes.

Champ	Description	
Messagerie, Paramètres	Affichez ou modifiez les paramètres de la messagerie sélectionnée.	
	Poste	En présence d'une messagerie personnelle, le champ affiche le poste utilisateur qui y est associé.
	Type	Personnel ou Générique. Vous pouvez modifier une messagerie générique créée pour un poste partagé et la transformer en messagerie partagée personnelle en changeant simplement le type et en sélectionnant un utilisateur dans la liste déroulante. Seuls les utilisateurs de cette ligne partagée ne disposant pas encore d'une messagerie personnelle figurent dans la liste. Une messagerie partagée personnelle ne peut pas être convertie en messagerie générique. Si le type de messagerie associé à un poste partagé est Partagée personnelle, la seule manière de revenir à la messagerie générique consiste à supprimer l'utilisateur associé à la messagerie personnelle, appliquer la configuration et recréer ensuite l'utilisateur.
	Taille	Affichez ou modifiez le volume de stockage affecté à la messagerie (de 4 à 90 minutes). La valeur par défaut est 12 minutes.

Notifications

Si les notifications de la messagerie vocales sont actives et configurées pour le site, les options de l'onglet Notifications vous permettent de sélectionner le numéro de poste doté d'une messagerie vocale et de configurer les paramètres relatifs aux notifications par e-mail et par téléphone.

Les notifications associées à la messagerie vocale et aux télécopies peuvent être envoyées vers un téléphone (par exemple, le téléphone de l'utilisateur, un téléphone mobile ou un autre numéro professionnel) ou vers la boîte e-mail.

Pour chaque utilisateur, vous pouvez effectuer les opérations suivantes :

- Activer les notifications par téléphone, par e-mail ou les deux.
- Définir si les messages vocaux et les télécopies doivent être annexés aux notifications envoyées (les télécopies sont annexées au format .TIFF).
- Définir un niveau de notification distinct pour les messages téléphoniques et les e-mails. Vous pouvez décider d'envoyer des notifications pour tous les messages vocaux ou uniquement pour les messages signalés comme étant urgents. L'option Urgent ne s'applique qu'aux messages vocaux, pas aux télécopies.

Les fonctions de notification suivantes pour la messagerie vocale ne sont pas prises en charge par CCA :

- Programme de notification
- Préfixe et suffixe pour le message de notification
- Délai de connexion
- Table contenant les restrictions associées à certains numéros de téléphone que les utilisateurs de la messagerie peuvent utiliser pour envoyer des notifications.
- Notification de messages en cascade

Pour ajouter des utilisateurs ou modifier les paramètres de notification pour des utilisateurs existants, suivez les étapes suivantes.

ETAPE 1 Sélectionnez **Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Messagerie** dans la barre de fonctions et activez l'onglet Notifications.

ETAPE 2 Si vous ajoutez un nouvel utilisateur et un poste, cliquez sur **Ajouter**.

ETAPE 3 Pour modifier les paramètres d'un utilisateur et d'un poste, sélectionnez l'utilisateur dans la liste et cliquez sur **Modifier**.

ETAPE 4 Définissez les paramètres conformément à la rubrique **Ajouter et modifier un utilisateur pour les notifications, page 387**.

ETAPE 5 Cliquez sur **OK**.

Ajouter et modifier un utilisateur pour les notifications

La fenêtre Ajouter/modifier un utilisateur des notifications s'affiche lorsque vous cliquez sur **Ajouter** ou **Modifier** sous l'onglet Notification de la fenêtre Messagerie (**Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Messagerie**).

Pour définir les paramètres de la messagerie vocale par e-mail et par téléphone pour un numéro de poste, configurez les paramètres ci-dessous et cliquez sur **OK**.

Paramètre	Description
Poste	Sélectionnez un Numéro de poste disponible dans la liste déroulante. Seuls les numéros de poste associés à une messagerie sont repris dans la liste. Il peut s'agir de messageries personnelles ou génériques.
Nom d'utilisateur (lecture seule)	Lorsque vous sélectionnez un numéro de poste, le nom, le prénom et l'identifiant de l'utilisateur s'affichent ici. S'il s'agit de postes partagés, l'option Ligne partagée s'affiche.
Notification par e-mail Cette fonction permet de définir l'envoi de notifications relatives aux messages vocaux ou aux télécopies par e-mail pour la messagerie associée à ce poste.	
Avertir l'utilisateur de la présence d'un nouveau message vocal par e-mail	Lorsque cette option est active, l'arrivée des nouveaux messages vocaux ou des fax est signalée par e-mail.
Adresse e-mail	Introduisez l'adresse à laquelle les notifications sont envoyées. L'adresse peut contenir jusqu'à 129 caractères.

Paramètre	Description
Annexe	Si vous cochez l'option **Associer le fichier de messagerie vocale à l'e-mail**, le message ou la télécopie est annexé à la notification envoyée. Chaque message vocal est annexé au format .wav. Il s'agit d'un fichier .wav G711 mu-law, 8 KHz, 8 bits, mono. Les fax sont annexés au format .TIFF. Cette option est désactivée par défaut. Les messages privés ne sont jamais annexés aux e-mails.
Niveau de notification	Faites un choix parmi les options suivantes : ▪ Message vocal urgent uniquement (ne s'applique pas aux fax). ▪ Tous les messages. Choisissez cette option si la fonction T.37 Fax vers e-mail est active et si vous souhaitez que les utilisateurs soient avertis de la présence de fax par e-mail et que ceux-ci soient annexés au message.
Notification par téléphone	
Avertir l'utilisateur de la présence d'un nouveau message par téléphone	Lorsque cette option est active, l'arrivée des nouveaux messages vocaux ou des fax est signalée par téléphone.
Type de téléphone	Faites un choix parmi les types suivants : ▪ Téléphone mobile ▪ Téléphone domicile ▪ Téléphone travail
Numéro de téléphone	Introduisez le numéro de téléphone auquel les notifications seront envoyées. Lorsque vous introduisez un numéro extérieur, veillez à intégrer les codes d'accès (le cas échéant).

Paramètre	Description
Chiffres supplémentaires	Le système compose ces numéros en cas de réponse à l'appel sortant. Ces numéros sont considérés comme des chiffres DTMF. Par exemple, les numéros supplémentaires peuvent être utilisés lors de l'envoi des appels vers un système de radiomessagerie ou vers un répondeur automatique. Vous pouvez introduire jusqu'à 64 chiffres. Les chiffres supplémentaires sont des chiffres compris entre 0 et 9, # (dièse), * (astérisque) et + (plus).
Niveau de notification	Faites un choix parmi les options suivantes : ▪ Message vocal urgent uniquement (ne s'applique pas aux fax). ▪ Tous les messages. Choisissez cette option si la fonction T.37 Fax vers e-mail est active et si vous souhaitez que les utilisateurs soient avertis de la présence de fax par e-mail et que ceux-ci soient annexés au message.

Single Number Reach (SNR)

Cette fenêtre s'affiche lorsque vous sélectionnez **Configurer** > **Téléphonie**>**Utilisateurs et postes**> **Single Number Reach** dans la barre de fonctions.

La fonction Single number reach (SNR) permet aux utilisateurs d'être joignables sur deux numéros : un numéro de poste normal sur leur téléphone IP et un numéro SDA. Les interfaces BRI, PRI, FXO et SIP sont prises en charge.

REMARQUE Pour les numéros SNR passant par les trunks SIP, l'identifiant de l'appelant peut différer de celui de la personne à l'origine de l'appel car celui-ci est défini par l'ITSP. L'identifiant de l'appelant correspondra d'ordinaire au numéro SDA principal défini pour le trunk SIP. La plupart des ITSP exigent des identifiants mappés explicitement vers leurs comptes afin d'éviter toute fraude. Si l'identifiant de l'appelant originel n'est pas remplacé par celui de l'ITSP, l'appel destiné au SNR échouera.

Vue d'ensemble

La fonction Single Number Reach (SNR) permet à l'utilisateur de répondre à un appel entrant sur son téléphone IP ou sur un site distant (à l'aide d'un téléphone mobile par exemple) et de prendre des appels en cours sur son téléphone de bureau ou distant sans perdre la liaison. Cela permet aux appelants d'utiliser un numéro unique pour contacter l'utilisateur du téléphone. Les appels restés sans réponse peuvent être transférés vers la messagerie.

Parmi les destinations distantes, les périphériques suivants :

- Téléphones mobiles (cellulaires)
- Smartphones
- Les téléphones IP ne doivent pas appartenir au même routeur Cisco Unified CME que le téléphone de bureau.
- Les numéros de téléphone principaux du SDA
- Les interfaces PRI, BRI, SIP et FXO sont prises en charge par le SDA.

Les appels entrants vers les postes SNR sont d'abord signalés par Cisco Unified CME sur le téléphone IP de bureau. S'il n'y a pas de réponse dans le délai prévu, celui-ci est signalé sur le numéro distant alors que le téléphone IP sonne toujours. Les appels sans réponse sont envoyés vers le numéro de messagerie défini.

L'utilisateur du téléphone IP dispose des options pour la gestion des appels sur le poste SNR :

- **Renvoyer l'appel du téléphone distant**. Renvoyer manuellement l'appel vers le poste SNR en appuyant sur la touche **Reprendre**, ce qui permet de raccrocher à partir du téléphone distant.
- **Envoyer l'appel vers un téléphone distant.** Envoyer l'appel vers un téléphone distant en utilisant la touche **Mobilité**. En cours d'appel, l'utilisateur peut appuyer sur la touche **Mobilité** et sélectionner l'option "Envoyer l'appel vers mobile". L'appel est transféré vers un téléphone mobile.
- **Activer ou désactiver Single Number Reach**. Lorsque le téléphone IP est en attente, l'utilisateur peut activer/désactiver la fonction SNR à l'aide de la touche Mobilité. Si l'utilisateur désactive la fonction SNR, l'appel n'est pas signalé sur le numéro distant.

Les utilisateurs du téléphone IP peuvent modifier les paramètres SNR directement à partir du téléphone à l'aide du menu accessible à l'aide du bouton **Services**. Vous devez activer cette fonction sur le téléphone pour permettre à un utilisateur d'accéder à l'interface.

Restrictions

Les restrictions suivantes s'appliquent à la configuration et aux fonctions SNR :

- Chaque téléphone IP ne prend en charge qu'un seul numéro SNR.
- L'utilisation simultanée de la fonction SNR et de l'application T.37 Détection de télécopies n'est pas prise en charge.
- Vous ne pouvez pas configurer le système SNR sur un poste faisant partie d'un groupement de postes.
- La fonction SNR n'est pas prise en charge sur les composants suivants :
  - Téléphones FXS analogiques commandés par SCCP
  - Appels vidéo
  - Téléphones SCCP sans touches programmables. Dans certains cas, la fonction SNR sera activée sur ces téléphones. Etant donné qu'ils ne sont pas pourvus de touches programmables, la fonction Mobilité est inutilisable.

Pour plus d'informations sur la fonction SNR et sur les restrictions, consultez le *Guide de l'administrateur pour Cisco Communications Manager Express System* disponible sur Cisco.com à l'adresse suivante :

www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeadm.html

Caractéristiques techniques de la plateforme SBCS

Cette fonction est prise en charge sur le CME 7.1 et disponible sur la version 7.1.1-EA ou supérieure du paquet logiciel de l'UC500.

Procédures de configuration et paramètres

Pour activer la fonction SNR pour un ou plusieurs utilisateurs, ou pour modifier les paramètres, suivez les consignes suivantes :

ETAPE 1 Sélectionnez **Configurer > Téléphonie > Utilisateurs et postes > Single Number Reach** dans la barre de fonctions.

ETAPE 2 Cliquez sur **Ajouter** ou **Modifier**. La fenêtre Ajouter un utilisateur SNR ou Modifier l'utilisateur SNR s'affiche.

ETAPE 3 Définissez les paramètres de l'utilisateur SNR conformément à la rubrique **Ajouter un utilisateur SNR, page 392** ou **Modifier un utilisateur SNR, page 394**.

ETAPE 4 Cliquez sur **OK**.

Ajouter un utilisateur SNR

Cette fenêtre s'affiche lorsque vous sélectionnez l'option **Ajouter** dans la fenêtre Single Number Reach.

Pour ajouter un utilisateur SNR, procédez comme suit :

ETAPE 1 Configurez les paramètres suivants pour chaque utilisateur SNR.

Paramètre	Description
Nom d'utilisateur	Sélectionnez un utilisateur dans la liste déroulante.
Adresse MAC	*Lecture seule*. Ce champ contient l'adresse MAC du téléphone associé au poste de l'utilisateur sélectionné lors de la création de l'utilisateur SNR.

Paramètre	Description
Poste	Lorsque vous sélectionnez un utilisateur, le menu déroulant contient la liste des postes disponibles sur le téléphone de l'utilisateur et pouvant être utilisés pour la fonction SNR. Si le numéro de poste choisi correspond à une ligne partagée, le texte (Ligne partagée) s'affiche à droite du numéro de poste. Sélectionnez le numéro de poste à utiliser pour la fonction SNR. Si l'utilisateur sélectionné dispose déjà d'une fonction SNR configurée sur un poste, un message d'avertissement s'affiche. Un seul numéro de poste peut être configuré par téléphone pour la fonction SNR.
Destination distante	Entrez ou modifiez le numéro de téléphone pour la destination distante. Lorsque vous introduisez le numéro distant, entrez le numéro exactement comme vous le composeriez normalement en y intégrant les codes d'accès, les numéros interurbains et les autres numéros.
Paramètres de retard et délai d'expiration	
Délai avant l'appel de la cible distante (s)	Ce délai représente la durée en secondes au cours de laquelle l'appel est signalé sur le téléphone IP avant de passer au téléphone distant. Introduisez une durée comprise entre de 1 et 10 secondes. La valeur par défaut est 5 secondes.
Délai de transfert d'appel vers la messagerie vocale (sec)	Durée en secondes pendant laquelle l'appel est signalé sur le téléphone IP et sur le téléphone distant avant son transfert vers la messagerie vocale. Introduisez une durée comprise entre de 5 et 60 secondes. La valeur par défaut est 30 secondes.

ETAPE 2 Cliquez sur **OK**.

Modifier un utilisateur SNR

Cette fenêtre s'affiche lorsque vous cliquez sur **Modifier** dans la fenêtre SNR (**Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Single Number Reach**).

Vous pouvez modifier le numéro de la cible distante et les durées relatives à la fonction SNR.

Si vous souhaitez modifier le poste associé à l'utilisateur SNR, vous devez supprimer l'utilisateur SNR, ajouter à nouveau l'utilisateur et sélectionner un poste différent.

Pour modifier les paramètres de l'utilisateur SNR, procédez comme suit :

ETAPE 1 Modifiez les paramètres de l'utilisateur SNR selon les indications du tableau suivant.

Paramètre	Description
Nom d'utilisateur	*Lecture seule*. Ce champ affiche le nom et le prénom de l'utilisateur associé à ce poste.
Adresse MAC	*Lecture seule.*Ce champ affiche l'adresse MAC du téléphone associé au poste SNR.
Poste	*Lecture seule*. Ce champ affiche le poste sélectionné lors de l'ajout de l'utilisateur SNR.
Destination distante	Modifiez le numéro de téléphone pour la destination distante. Lorsque vous modifiez le numéro distant, entrez le numéro exactement comme vous le composeriez normalement en y intégrant les codes d'accès, les numéros interurbains et les autres numéros.
Membres de la ligne partagée	Lecture seule. Si le poste est une ligne partagée, cette section contient la liste des utilisateurs.

Paramètre	Description
Paramètres de retard et délai d'expiration	
Délai avant l'appel de la cible distante (s)	Ce délai représente la durée en secondes au cours de laquelle l'appel est signalé sur le téléphone IP avant de passer au téléphone distant. Introduisez une durée comprise entre de 1 et 10 secondes. La valeur par défaut est 5 secondes.
Délai de transfert d'appel vers la messagerie vocale (sec)	Durée en secondes pendant laquelle l'appel est signalé sur le téléphone IP et sur le téléphone distant avant son transfert vers la messagerie vocale. Introduisez une durée comprise entre de 5 et 60 secondes. La valeur par défaut est 30 secondes.

ETAPE 2 Cliquez sur **OK**.

Numérotation abrégée système

Pour configurer la numérotation abrégée système, sélectionnez **Configurer** > **Téléphonie** > **Utilisateurs et postes**> **Numérotation abrégée système** dans la barre de fonctions.

La fenêtre Numérotation abrégée système vous permet de définir les numéros d'appel rapide nationaux.

Vue d'ensemble

Vous pouvez créer une liste des numéros les plus fréquents pour tous les téléphones. L'utilisateur peut ainsi rapidement composer le numéro d'une liste grâce à la fonction d'appel rapide.

Les utilisateurs peuvent accéder à ces raccourcis à partir du menu **Services locaux** > **Numéros d'appel rapide locaux** de leur téléphone.

Vous pouvez ajouter, modifier ou supprimer les raccourcis. Les numéros peuvent être déplacés vers le haut ou vers le bas. Ils s'affichent à l'écran du téléphone selon l'ordre de la liste. Vous pouvez introduire jusqu'à 32 raccourcis d'appel dans la liste.

Procédures

Pour activer un menu pour les appels rapides locaux pour tous les téléphones IP, effectuez les opérations suivantes :

ETAPE 1 Cliquez sur **Ajouter**.

ETAPE 2 Dans le champ **Nom**, entrez le nom correspondant au raccourci.

ETAPE 3 Dans le champ **Numéro de téléphone**, entrez le numéro correspondant au raccourci.

ETAPE 4 Pour réorganiser les numéros dans la liste, sélectionnez l'entrée et cliquez sur la flèche Haut ou Bas. Les numéros sont repris dans l'ordre dans lequel ils sont affichés sur le téléphone.

ETAPE 5 Pour supprimer un numéro d'appel rapide du menu, sélectionnez le numéro et cliquez sur **Supprimer** dans le volet Numéros d'appel rapide locaux.

Si la liste a atteint son volume maximal, le bouton **Ajouter** est grisé.

11

Groupes de téléphones

Cette rubrique contient les instructions pour la configuration des types de groupes de téléphone suivants :

- **Groupement de postes**
- **Appeler groupes d'appel**
- **Groupes d'interception**
- **Groupes de radiomessagerie**

Pour configurer les groupes de téléphones, sélectionnez **Configurer** > **Téléphonie** > **Groupes de téléphones** dans la barre de fonctions.

Groupement de postes

Pour configurer les groupements de postes, sélectionnez **Configurer** > **Téléphonie** > **Groupes de téléphones**> **Groupements de postes** dans la barre de fonctions.

Vue d'ensemble

Utilisez les groupements de postes pour gérer la répartition des appels entrants vers un groupe de postes prédéfini (membres). Le type de groupement de postes définit l'ordre dans lequel les membres du groupement de postes reçoivent les appels.

Vous pouvez définir jusqu'à 10 groupements de postes sur le système. Chaque groupement de postes doit contenir entre 1 et 32 membres.

Une fois les groupements de postes configurés, vous pourrez les sélectionner comme cibles pour le routage des appels entrants, le Standard automatique, le transfert d'appel et pour toute autre fonction de téléphonie.

Lorsque vous configurez un groupement de postes, la touche **HLog** s'ajoute aux téléphones membres du groupe. Les membres du groupement de postes peuvent se connecter ou se déconnecter du groupe à l'aide de la touche **HLog**. La touche **HLog** s'affiche sur les téléphones du groupement de postes en cas de réception d'un appel. Les utilisateurs peuvent aussi utiliser la touche à partir de l'écran principal du téléphone en appuyant sur la touche **plus**. La touche **HLog** remplace la fonction DnD (Do Not Disturb - Ne pas déranger). DnD est moins polyvalent étant donné que l'abonné est indisponible d'une manière générale et pas seulement pour les appels du groupement de postes.

Restrictions

Les restrictions suivantes s'appliquent à la configuration des groupements de postes :

▪ Un téléphone sur lequel la fonction SNR a été activée ne peut pas être membre d'un groupement de postes.

Procédures

Pour activer et configurer un groupement de postes, configurez les paramètres selon les consignes ci-dessous et cliquez sur **OK** ou **Appliquer**.

Paramètre	Description
Activer	Le groupement de postes associé est actif lorsque cette case est cochée.
N° pilote	Numéro pilote pour le groupement de postes. Il s'agit du numéro permettant d'atteindre le groupement de postes. Utilisez le numéro de poste par défaut pour le numéro pilote ou cliquez dans le champ pour le modifier.
Description	*Facultatif.* Description désignant le groupement de postes. La description est uniquement utilisée dans la fenêtre Groupement de postes. Dans les autres parties de l'interface utilisateur de CCA, le groupement de postes est désigné par son numéro et le numéro pilote. Par exemple : hunt1 (502).

Paramètre	Description
Type de recherche	Définit l'ordre dans lequel les appels sont répartis vers les membres du groupement de postes. Faites un choix parmi les options suivantes : ▪ **Séquentiel** : la recherche débute toujours par le numéro pilote du groupe et passe ensuite aux autres numéros du groupe selon l'ordre dans lequel ils sont affichés, de haut en bas, dans la liste Membres. ▪ **Plus longtemps disponible** : les appels sont transférés vers le numéro qui est resté le plus longtemps en attente d'après l'horodatage du dernier appel pris en charge à partir du poste en question. Si le poste n'est pas disponible, le système passe au poste suivant. ▪ **Poste** : groupe de recherche dans lequel le premier groupe appelé est sélectionné sur une base périodique.
Membres	Désigne les membres du groupement de postes Tous les postes sur lesquels l'appel est signalé lorsqu'il atteint le numéro pilote. 1. Cliquez sur **Membres** pour afficher la liste des utilisateurs disponibles et sélectionnés au bas de la fenêtre Groupements de postes. 2. Utilisez les boutons **Ajouter** et **Supprimer** pour déplacer les membres de la liste Disponible à la liste Sélection. Maintenez la touche CTRL ou MAJ enfoncée pour effectuer des sélections multiples. 3. Utilisez les flèches **Haut** et **Bas** pour modifier l'ordre de routage des appels vers le groupement de postes.
Délai d'expiration (sec)	Délai (en secondes) au terme duquel un appel resté sans réponse est redirigé vers le numéro suivant de la liste (valeur comprise entre 5 et 20 secondes).

Paramètre	Description
Transfert si pas de réponse vers	Cible des appels transférés au sein du groupement de postes. Vous avez le choix entre les options suivantes : **Aucun**, **Standard automatique**, **Messagerie**, **Poste**, **Groupement de postes**, **Groupe d'appel**, **B-ACD** ou **Autre numéro**. Si vous sélectionnez l'option **Messagerie** comme cible pour l'option **Transfert si pas de réponse vers**, une messagerie générique est créée pour le groupe. Pour afficher les données relatives à la messagerie générique ou modifier sa taille, utilisez l'option **Configurer** > **Téléphonie** > **Messagerie vocale** et sélectionnez l'onglet **Boîtes de réception**.

Appeler groupes d'appel

Pour configurer les groupes d'appel, sélectionnez **Configurer** > **Téléphonie** > **Groupes de téléphones** > **Appeler groupes d'appel** dans la barre de fonctions.

Vue d'ensemble

Un groupe d'appel est un groupe de téléphones où les appels vers un numéro pilote sont signalés sur plusieurs téléphones. Cette fonction permet également de définir un scénario Single Number Reach où l'appel vers le poste d'un utilisateur est également signalé sur un autre numéro (par exemple, un numéro de portable ou le numéro du domicile) ou sur un autre poste.

Vous pouvez définir jusqu'à 10 groupes d'appel sur le système. Chaque groupe d'appel doit contenir entre 2 et 32 membres.

Une fois les groupes d'appel configurés, vous pourrez les sélectionner comme cibles pour le routage des appels entrants, le Standard automatique, le transfert d'appel et pour toute autre fonction de téléphonie.

Lorsque vous configurez un groupe d'appel, la touche **HLog** s'ajoute aux téléphones membres du groupe. Les membres du groupement de postes peuvent se connecter ou se déconnecter du groupe à l'aide de la touche **HLog**. La touche **HLog** s'affiche sur les téléphones du groupe d'appel en cas de réception d'un appel. Les utilisateurs peuvent aussi utiliser la touche à partir de l'écran principal

du téléphone en appuyant sur la touche **plus**. La touche **HLog** remplace la fonction DnD (Do Not Disturb - Ne pas déranger). DnD est moins polyvalent étant donné que l'abonné est indisponible d'une manière générale et pas seulement pour les appels du groupe d'appels.

Procédures

Pour activer et configurer un groupement de postes, configurez les paramètres selon les consignes ci-dessous et cliquez sur **OK** ou **Appliquer**.

Paramètre	Description
Activer	Le groupe d'appels associé est actif lorsque cette case est cochée.
N° pilote	Numéro pilote pour le groupe d'appel. Il s'agit du numéro permettant d'atteindre le groupe d'appel. Utilisez le numéro de poste par défaut pour le numéro pilote ou cliquez dans le champ pour le modifier.

Paramètre	Description
Membres	Désigne les membres du groupe d'appel. Tous les postes sur lesquels l'appel est signalé lorsqu'il atteint le numéro pilote. 1. Cliquez sur **Membres** pour afficher la liste des utilisateurs disponibles et sélectionnés au bas de la fenêtre Groupe d'appel. 2. Utilisez les boutons **Ajouter** et **Supprimer** pour déplacer les membres de la liste Disponible à la liste Sélection. Maintenez la touche CTRL ou MAJ enfoncée pour effectuer des sélections multiples. Pour ajouter un numéro SDA externe (par exemple, un numéro de téléphone portable ou le numéro de votre domicile) à la liste des membres disponibles et le déplacer dans la sélection, procédez comme suit : 1. Dans le champ **Autre numéro**, entrez le numéro de téléphone comme vous le composeriez sur un téléphone normal, préfixes et codes d'accès compris (jusqu'à 16 numéros). 2. Cliquez sur le bouton **Ajouter** à droite du champ **Autre numéro** pour le déplacer vers la liste Disponible. 3. Cliquez sur la touche fléchée **Ajouter** pour déplacer le numéro introduit à la liste Sélection. Pour supprimer un numéro externe de la liste Sélection, cliquez sur la flèche **Supprimer** pour le déplacer vers la liste Disponible. Lorsque vous fermez la fenêtre Groupes d'appel ou sélectionnez un autre groupe d'appel à configurer, les numéros externes ajoutés à la liste Disponible qui ne sont pas déplacés vers la liste Sélection sont retirés de la liste Disponible. Lorsque vous ouvrez ensuite la sélection des membres, les numéros externes ne figurent pas dans la liste Disponible.

Paramètre	Description
Délai d'expiration (sec)	Délai (en secondes) au terme duquel un appel resté sans réponse est redirigé vers le numéro suivant de la liste **Transfert si pas de réponse vers** (valeur comprise entre 5 et 20 secondes). Le délai d'expiration par défaut est 16 secondes. **IMPORTANT** La valeur **Délai d'expiration** pour le groupe d'appel doit être inférieure à celle de CFNA, et ce, pour tous les numéros de poste qui en font partie. Réduisez la valeur du délai d'expiration pour le groupe d'appel, augmentez la valeur CFNA pour les postes membres.
Transfert si pas de réponse vers	Cible des appels transférés au sein du groupement de postes. Vous avez le choix entre les options suivantes : **Aucun**, **Standard automatique**, **Messagerie, Poste**, **Groupement de postes**, **Groupe d'appel**, **B-ACD** ou **Autre numéro**. Si vous sélectionnez l'option **Messagerie** comme cible pour l'option **Transfert si pas de réponse vers**, une messagerie générique est créée pour le groupe. Pour afficher les données relatives à la messagerie générique ou modifier sa taille, utilisez l'option **Configurer** > **Téléphonie** > **Messagerie vocale** et sélectionnez l'onglet **Boîtes de réception**.
Numéro	Numéro correspondant à la cible définie dans l'option **Transfert si pas de réponse vers** : ▪ Si vous avez sélectionné **Standard automatique** et que plusieurs standards automatiques sont configurés pour le site, sélectionnez le standard souhaité. ▪ Si vous avez sélectionné **Autre numéro**, entrez le numéro dans le champ **Numéro** comme vous le composeriez sans oublier les préfixes et codes d'accès. ▪ Si vous avez sélectionné **Poste**, sélectionnez un numéro de poste dans la liste figurant dans le champ **Numéro**. ▪ Si vous avez sélectionné **Groupement de postes, Groupe d'appel** ou **B-ACD**, sélectionnez un groupe ou un service B-ACD dans la liste affichée dans le champ **Numéro**.

Groupes d'interception

Pour configurer les groupes d'interception, sélectionnez **Configurer** > **Téléphonie** > **Groupes de téléphones** > **Groupes d'interception** dans la barre de fonctions.

Vue d'ensemble

Créez des groupes d'interception pour configurer un groupe de numéros de poste pouvant répondre aux appels signalés sur les postes appartenant au même groupe d'interception en appuyant sur la touche **GPickUp** du téléphone IP. Appuyez ensuite sur la touche *.

Les remarques suivantes s'appliquent aux fonctions d'interception d'appel sur les plateformes SBCS :

- Chaque utilisateur peut répondre à un appel entrant en appuyant sur la touche PickUp de son téléphone et en introduisant le numéro de poste. Aucune configuration n'est nécessaire.
- Chaque utilisateur peut répondre à un appel signalé sur un poste du groupe en appuyant sur la touche **GPickUp** de son téléphone et en introduisant le code d'interception du groupe.
- Si le téléphone de l'utilisateur et le numéro de poste sur lequel l'appel est signalé se trouvent dans le même groupe d'interception, l'utilisateur pourra prendre l'appel en appuyant sur la touche **GPickUp** et ensuite sur la touche * de son téléphone. Si un seul groupe d'interception est configuré sur le système, l'utilisateur est automatiquement connecté. Il ne doit donc pas appuyer sur la touche *.

Procédures

Pour activer et configurer un groupe d'interception, configurez les membres selon les consignes ci-dessous et cliquez sur **OK** ou **Appliquer**.

Paramètre	Description
Membres	Définissez les postes intégrés au groupe d'interception. 1. Cliquez sur **Membres** pour afficher la liste des postes disponibles et sélectionnés au bas de la fenêtre Groupes d'interception. 2. Utilisez les boutons **Ajouter**, **Supprimer** ou **Sélectionner tout** pour déplacer les postes sélectionnés de la liste Disponible vers la liste Sélection. Maintenez la touche CTRL ou MAJ enfoncée pour effectuer des sélections multiples.

Groupes de radiomessagerie

Pour configurer les groupes de radiomessagerie, sélectionnez **Configurer** > **Téléphonie** > **Groupes de téléphones** > **Groupes de radiomessagerie** dans la barre de fonctions.

La configuration des groupes de radiomessagerie fait l'objet des rubriques suivantes :

Vue d'ensemble

Vous pouvez créer des groupes de radiomessagerie permettant aux utilisateurs de diffuser les annonces aux groupes de téléphones IP Cisco grâce au haut-parleur du téléphone. Vous pouvez créer jusqu'à 10 groupes de radiomessagerie.

Seuls les téléphones IP Cisco peuvent être membres des groupes de radiomessagerie.

Vous pouvez aussi créer des groupes de radiomessagerie combinés. Un groupe de radiomessagerie combiné peut contenir d'autres groupes de radiomessagerie ou un ensemble de téléphones individuels et de groupes de radiomessagerie. Par exemple, un téléphone se trouvant dans un bureau immobilier est susceptible de recevoir des messages destinés au service de gestion des biens alors qu'un autre téléphone devra recevoir les messages destinés au service commercial. Par ailleurs, les deux téléphones devront recevoir les messages envoyés à tous les employés.

La marche à suivre pour la configuration d'un groupe de radiomessagerie se présente comme suit :

1. Tout d'abord, créez les groupes de radiomessagerie nécessaires et affectez les téléphones.
2. Créez le groupe de radiomessagerie combiné et ajoutez les téléphones membres du groupe combiné uniquement.
3. Ajoutez les groupes de radiomessagerie isolés créés à l'étape 1 au groupe de radiomessagerie combiné.

Un groupe de radiomessagerie peut être membre de plusieurs groupes de radiomessagerie, mais un téléphone ne peut être affecté qu'à un seul groupe. Un seul niveau d'intégration est pris en charge pour les groupes de radiomessagerie. Voir **Groupes de radiomessagerie combinés, page 409** pour plus d'exemples.

Création d'un groupe de radiomessagerie simple (téléphones individuels uniquement)

Pour activer et configurer un groupe de radiomessagerie contenant un ou plusieurs téléphones individuels, suivez les étapes suivantes :

ETAPE 1 Activez la configuration pour le groupe que vous souhaitez créer en cochant l'option **Activer**.

ETAPE 2 Dans le champ **Numéro de radiomessagerie**, entrez le numéro de poste à utiliser pour le groupe de radiomessagerie ou utilisez les valeurs par défaut. La plage de

numéros de postes par défaut pour les groupes de radiomessagerie est comprise entre 101 et 110.

Il s'agit du poste permettant d'atteindre le groupe de radiomessagerie.

ETAPE 3 *Facultatif*. Entrez une **description** désignant le groupe de radiomessagerie. La description est uniquement utilisée pour la fenêtre Groupes de radiomessagerie. Elle ne s'affiche pas sur les téléphones.

ETAPE 4 Ajoutez les numéros de téléphone des membres au groupe de radiomessagerie.

a. Cliquez sur l'onglet Téléphones au bas de la page. La liste Disponible affiche l'identifiant et l'adresse MAC de chaque téléphone qui ne fait pas actuellement partie d'un groupe de radiomessagerie.

b. Cliquez sur l'identifiant d'un utilisateur dans la liste **Disponible** et utilisez les boutons **Ajouter** et **Supprimer** pour déplacer les membres de ou vers la liste **Sélection**. Maintenez la touche CTRL ou MAJ enfoncée pour effectuer des sélections multiples.

ETAPE 5 Cliquez sur **Appliquer** ou **OK** pour créer le groupe de radiomessagerie.

La colonne Membres est mise à jour et affiche le nombre de téléphones faisant partie du groupe.

Création d'un groupe de radiomessagerie combiné

Pour créer un groupe de radiomessagerie contenant d'autres groupes, suivez les étapes suivantes :

ETAPE 1 Créez les groupes de radiomessagerie que vous souhaitez ajouter au groupe combiné et indiquez les téléphones individuels qui feront partie du groupe combiné.

Voir la rubrique **Création d'un groupe de radiomessagerie simple (téléphones individuels uniquement), page 406**.

ETAPE 2 Activez la configuration du groupe combiné en cochant l'option **Activer** pour le nouveau groupe.

ETAPE 3 Dans le champ **Numéro de radiomessagerie**, entrez le numéro de poste à utiliser pour le groupe de radiomessagerie ou utilisez les valeurs par défaut. La plage de numéros de postes par défaut pour les groupes de radiomessagerie est comprise entre 101 et 110.

Il s'agit du poste permettant d'atteindre le groupe de radiomessagerie.

ETAPE 4 *Facultatif*. Entrez une description désignant le groupe de radiomessagerie. La description est uniquement utilisée pour la fenêtre Groupes de radiomessagerie. Elle ne s'affiche pas sur les téléphones.

ETAPE 5 Ajoutez les groupes de radiomessagerie et les téléphones au groupe de radiomessagerie.

a. Pour ajouter des téléphones, cliquez sur l'onglet Téléphones au bas de la page. La liste Disponible affiche l'identifiant et l'adresse MAC de chaque téléphone qui ne fait pas actuellement partie d'un groupe de radiomessagerie.

   Cliquez sur l'identifiant d'un utilisateur dans la liste Disponible et utilisez les boutons **Ajouter** et **Supprimer** pour déplacer les membres de ou vers la liste Sélection.

b. Pour ajouter des groupes de radiomessagerie, cliquez sur l'onglet **Groupes** au bas de la page. Sélectionnez le groupe dans la liste Disponible et utilisez les boutons **Ajouter** et **Supprimer** pour déplacer les membres de ou vers la liste Sélection.

Un groupe de radiomessagerie peut être membre de plusieurs groupes de radiomessagerie, mais un téléphone ne peut être affecté qu'à un seul groupe.

Maintenez la touche CTRL ou MAJ enfoncée pour effectuer des sélections multiples.

La colonne Membres est mise à jour et affiche le nombre de téléphones ou de groupes de radiomessagerie faisant partie du groupe.

ETAPE 6 *Facultatif*. Pour afficher les liens entre les groupes ou vérifier les problèmes de configuration dans les groupes de radiomessagerie combinés, cliquez sur **Afficher la dépendance de groupe**. Voir la rubrique **Affichage des dépendances des groupes de radiomessagerie, page 411**.

ETAPE 7 Cliquez sur **OK** ou **Appliquer**.

Modifier un groupe de radiomessagerie

Pour modifier un groupe de radiomessagerie, cliquez sur le bouton **Téléphones (n) et Groupes (n)** correspondant au groupe que vous souhaitez modifier.

Les onglets Téléphones et Groupes sont mis à jour et affichent la liste des téléphones IP disponibles et sélectionnés ainsi que les groupes correspondant au groupe de radiomessagerie à modifier.

Utilisez les boutons **Ajouter** et **Supprimer** pour modifier les membres du groupe et cliquez sur **OK** ou **Appliquer**.

Supprimer un groupe de radiomessagerie

Pour supprimer un groupe de radiomessagerie, annulez la sélection du paramètre **Activer** correspondant au groupe que vous voulez supprimer et cliquez sur **OK** ou **Appliquer**.

Avant de supprimer un groupe, cliquez sur **Afficher la dépendance de groupe** pour savoir quels groupes sont membres d'autres groupes.

ASTUCE Si le groupe que vous supprimez fait partie d'un groupe de radiomessagerie combiné, il est automatiquement supprimé du groupe de radiomessagerie. Dans ce cas, vous pourrez mettre à jour la description introduite pour que le groupe de radiomessagerie combiné tienne compte des modifications.

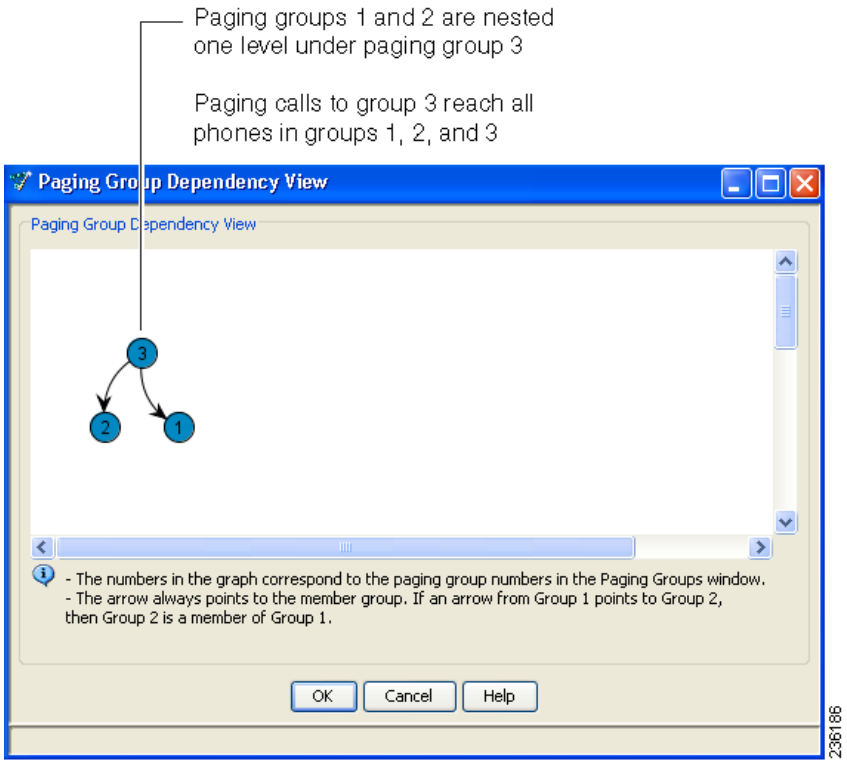
Groupes de radiomessagerie combinés

Les groupes de radiomessagerie combinés sont pris en charge jusqu'à un niveau inférieur.

Le scénario suivant présente des groupes de radiomessagerie avec un niveau d'intégration :

- Imaginons que les groupes de radiomessagerie n° 1 et 2 ne contiennent que des téléphones et que le groupe n° 3 contienne les groupes 1 et 2 et quelques téléphones. Dans ce cas, il n'existe qu'un seul niveau d'intégration.
- Un appel de radiomessagerie destiné au groupe 3 atteindra tous les téléphones des groupes 1, 2 et 3.

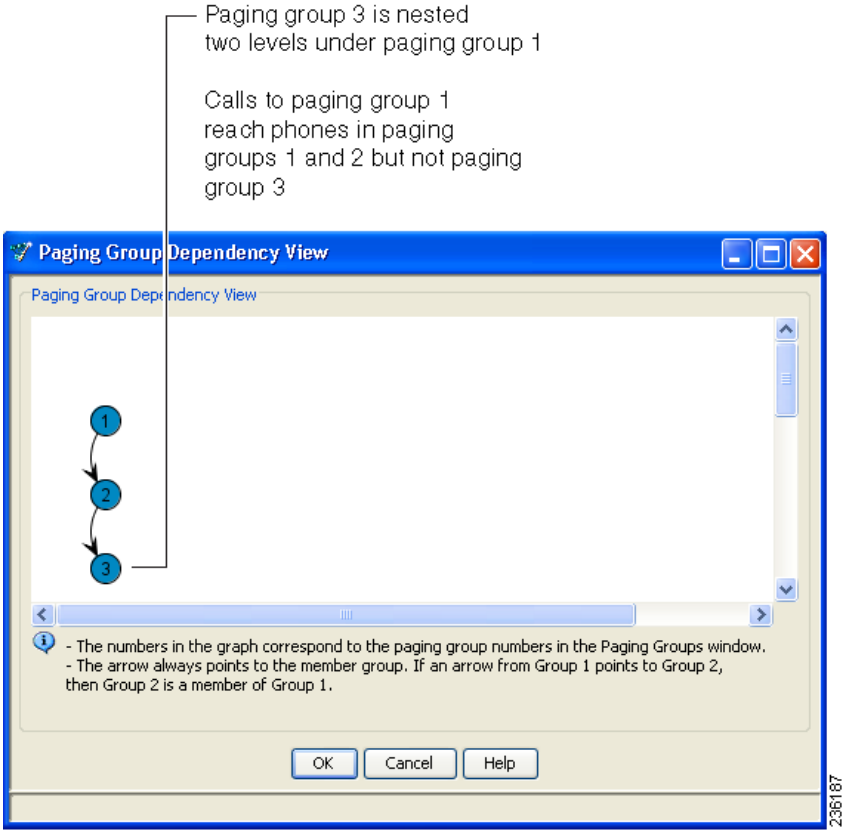
L'affichage des dépendances du groupe de radiomessagerie pour ce scénario est présenté ci-dessous :



Le scénario suivant présente des groupes de radiomessagerie combinés avec deux niveaux d'intégration :

- Imaginons que le groupe de radiomessagerie n° 1 contienne le groupe 2 qui contient le groupe 3. Dans ce cas, il y a deux niveaux d'intégration.
- Un appel de radiomessagerie destiné au groupe 1 atteindra tous les téléphones des groupes 1 et 2, mais pas ceux du groupe 3.

L'affichage des dépendances du groupe de radiomessagerie pour ce scénario est présenté ci-dessous :



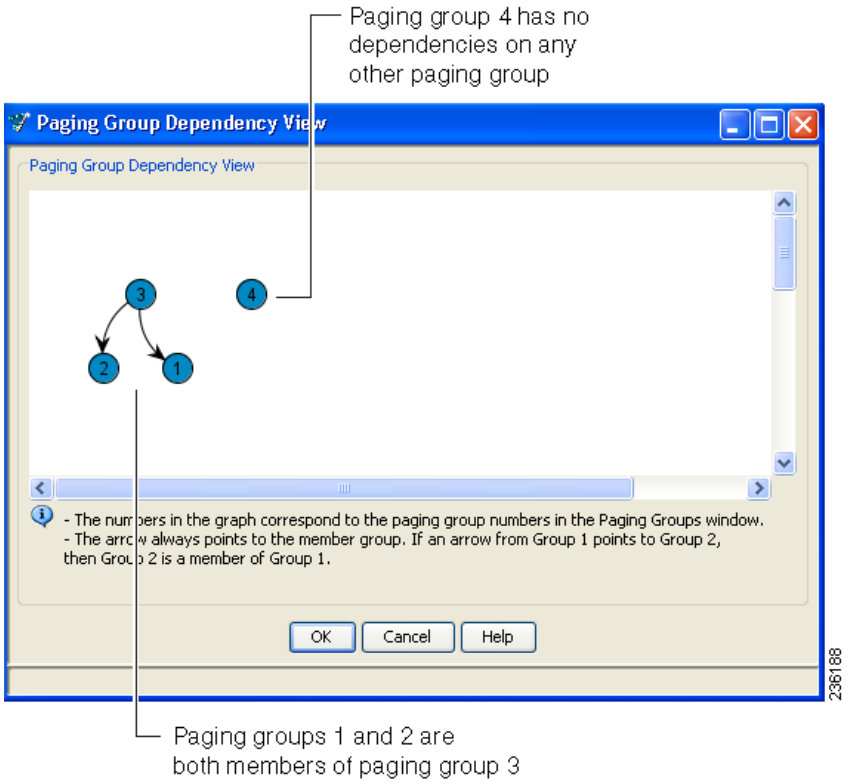
Affichage des dépendances des groupes de radiomessagerie

La fenêtre Dépendances des groupes de radiomessagerie s'affiche lorsque vous cliquez sur **Afficher la dépendance de groupe** dans la fenêtre Groupes de radiomessagerie (**Configurer** > **Téléphonie** > **Groupes de téléphones** > **Groupes de radiomessagerie**).

Cette fenêtre contient un graphique qui vous permet de savoir quels groupes sont membres d'autres groupes. Comme l'indique l'exemple ci-dessous :

- Les chiffres présentés correspondent au nombre de groupes de radiomessagerie repris dans la fenêtre Groupes de radiomessagerie.
- Les flèches indiquent quels groupes appartiennent à d'autres groupes. La flèche pointe toujours vers le groupe membre.

Certains schémas d'appartenance des groupes de radiomessagerie sont présentés ci-dessous.



12

Fonctions vocales

Les thèmes évoqués dans cette rubrique permettent de configurer les fonctions vocales suivantes :

- **Parcage d'appels**
- **Téléconférence**
- **Conference Barge**
- **Musique d'attente**

IMPORTANT L'accès Telnet doit être activé pour pouvoir configurer les fonctions vocales.

Parcage d'appels

Pour configurer le parcage d'appels, sélectionnez **Configurer** > **Téléphonie** > **Fonctionnalités voix** > **Parcage**d'appels dans la barre de fonctions.

Vue d'ensemble

La fonction Parcage d'appels permet de définir un emplacement temporaire pour les appels entrants. Lorsqu'un appel est parqué, il est transféré et mis en attente jusqu'à ce qu'il soit récupéré par un autre employé grâce à la fonction Interception d'appel. Le message "<*Numéro de poste pour le parc d'appels*"> s'affiche à l'écran du téléphone à l'origine du parcage. Pour récupérer un appel parqué, les autres utilisateurs peuvent appeler le poste de parcage d'appel.

- Une sonnerie de rappel d'une seconde est émise à intervalles réguliers et le message "Numéro de poste <*pour le parc d'appels*>" s'affiche à l'écran du téléphone à l'origine du parcage. La sonnerie et le message sont uniquement envoyés au téléphone à l'origine du parcage.
- Vous pouvez activer la fonction Délai d'expiration et rappel pour établir l'action à entreprendre lorsque le délai d'expiration est écoulé. Le délai d'expiration correspond au nombre de tentatives multiplié par le nombre de secondes composant l'intervalle de rappel. L'appel peut être transféré vers

le poste à l'origine du parcage, transféré vers un autre poste ou abandonné.

Lorsque la fonction Délai d'expiration et rappel est active, vous pouvez aussi définir le nombre de rappels, l'intervalle de rappel, le délai pour les différentes tentatives et le nombre de tentatives. Au terme du délai, l'action prévue pour le parcage d'appels a lieu.

Restrictions et lignes de conduite

Les restrictions et lignes de conduite suivantes s'appliquent au parc d'appels :

- Un seul appel peut être parqué pour chaque numéro de poste réservé au parcage d'appels.
- Les téléphones dépourvus de touches programmables ne peuvent pas être utilisés pour le parcage d'appels.

Procédures

Pour créer un nouvel emplacement de parcage d'appels, cliquez sur **Créer** et remplissez les champs conformément à la rubrique **Créer ou modifier un emplacement de parcage d'appels, page 414**. Dans la fenêtre Parcage d'appels, cliquez sur **OK** ou sur **Appliquer** pour envoyer la configuration à l'UC500.

Pour modifier un emplacement, cliquez sur celui-ci dans la liste pour le sélectionner. Cliquez ensuite sur **Modifier** et modifiez les paramètres conformément aux indications de la rubrique **Créer ou modifier un emplacement de parcage d'appels, page 414**. Dans la fenêtre Parcage d'appels, cliquez sur **OK** ou sur **Appliquer** pour envoyer la configuration à l'UC500.

Pour supprimer un emplacement, cliquez sur celui-ci dans la liste pour le sélectionner. Cliquez ensuite sur **Supprimer**, puis sur **OK** à l'affichage du message de confirmation. Dans la fenêtre Parcage d'appels, cliquez sur **OK** ou sur **Appliquer** pour envoyer la configuration à l'UC500.

Créer ou modifier un emplacement de parcage d'appels

Pour créer ou modifier un emplacement de parcage d'appels, procédez comme suit :

ETAPE 1 Dans le champ **Numéro de poste**, entrez le numéro de poste utilisé pour l'emplacement de parcage d'appel.

ETAPE 2 Dans le champ **Etiquette d'emplacement**, introduisez une description pour chaque emplacement de parcage.

ETAPE 3 Si nécessaire, cochez l'option **Activer le délai d'expiration et le rappel** pour activer la fonction Délai d'expiration et rappel pour le parcage d'appel.

ETAPE 4 Si la fonction **Activer le délai d'expiration et le rappel** est active, configurez les paramètres suivants.

Paramètre	Description
Intervalle de rappel (sec)	Nombre de secondes d'attente entre les rappels relatifs au parcage d'appels. La valeur par défaut est 120 secondes.
Nombre de rappels	Nombre de rappels envoyés au téléphone à l'origine du parcage. Le nombre par défaut est 2. Le délai d'expiration correspond au nombre de tentatives multiplié par le nombre de secondes composant l'intervalle de rappel. Par exemple, si vous définissez un intervalle de 20 secondes avec 3 tentatives, l'appel pourra être parqué pendant 60 secondes maximum avant la fin du délai d'expiration et l'exécution de la commande correspondante.
A la fin du délai	Permet d'établir l'action entreprise au terme du délai d'expiration. Faites un choix parmi les options suivantes : ▪ **Rappeler le poste qui a effectué le parcage d'appel** (valeur par défaut) ▪ **Transfert vers le poste**. Si vous sélectionnez cette option, accédez à la fenêtre **Poste de transfert**, définissez le **Délai pour les tentatives** et le **Nombre de tentatives**. ▪ **Déconnecter l'appel**.
Poste de transfert	Si vous avez choisi l'option **Transfert vers le poste**, introduisez le numéro de poste (vous pourriez par exemple introduire un numéro pilote pour un groupement de postes ou tout autre numéro de poste).
Délai pour les tentatives (s)	Entrez le délai d'attente en secondes entre les tentatives de transfert d'un appel parqué. Le nombre de tentatives est défini par le paramètre **Nombre de tentatives**. La valeur par défaut est 120 secondes.
Nombre de tentatives	Introduisez le nombre de tentatives pour le transfert d'un appel parqué. Le nombre par défaut est 2.

ETAPE 5 Cliquez sur **OK**.

Téléconférence

Pour configurer la conférence à plusieurs, sélectionnez **Configurer** > **Téléphonie** > **Fonctionnalités voix** > **Conférence** dans la barre de fonctions.

Pour plus d'informations sur la configuration de la conférence, consultez les rubriques suivantes :

- **Vue d'ensemble, page 417**
- **Activation et configuration d'une conférence à plusieurs (MeetMe et Ad Hoc), page 419**
- **Restrictions et remarques relatives à la conférence à plusieurs, page 420**
- **Conference Barge, page 420**

Vue d'ensemble

Dans la fenêtre Conférence, choisissez d'activer la conférence à plusieurs et configurez les options.

REMARQUE La conférence à plusieurs doit être activée pour pouvoir utiliser les fonctions Conference Barge (cBarge) et Confidentialité.

Lorsque la conférence à plusieurs est activée :

- Les ressources logicielles sont utilisées pour la téléconférence.
- Vous pouvez définir le nombre maximal d'appels tridirectionnels simultanés autorisés sur le système.

Lorsque la conférence à plusieurs est active :

- Les ressources matérielles (DSP) sont utilisées.

  Configuration Assistant détecte automatiquement la plateforme UC500 que vous configurez et définit le nombre de participants pris en charge pour les sessions de conférence et les conférences simultanées de type Meet-Me et Ad Hoc.

Les plateformes Cisco UC500 prenant en charge au moins 24 utilisateurs disposent de deux fois le volume de ressources matérielles. Elles peuvent donc prendre en charge un grand nombre de participants et de sessions.

REMARQUE La conférence matérielle est désactivée en l'absence de ressources suffisantes. Par exemple, ce type de conférence pourra être désactivé si une carte T1/E1 complémentaire est ajoutée à un boîtier UC500 de 16 unités car les ports vocaux exploitent des ressources provenant du même groupe de ressources affecté à la conférence matérielle.

- Vous pouvez configurer la conférence MeetMe ou Ad hoc.
  - Une *conférence ad hoc* est une conférence au cours de laquelle un participant appelle un autre et chacun accepte d'ajouter une troisième personne à la discussion.
  - La *conférence MeetMe* permet aux intervenants d'appeler un numéro MeetMee prédéfini.

    Le créateur de la conférence se déconnecte, appuie sur la touche **MeetMe** de son téléphone, entend un signal de confirmation et compose le numéro MeetMe. Une fois que la conférence a démarré, les autres participants rejoignent la conférence en appelant le numéro MeetMe.

    Lorsque vous configurez la conférence MeetMe, tous les utilisateurs sont autorisés à organiser des conférences MeetMe. Le créateur de la conférence MeetMe peut utiliser la touche **ConfList** pour dresser la liste de tous les participants, **RmLstC** pour supprimer le dernier appelant et supprimer un participant.

    Les touches MeetMe sont configurées et appliquées aux téléphones dès que la conférence à plusieurs est active et que les numéros MeetMe ont été configurés.
  - Vous pouvez activer ou désactiver les tonalités émises lorsque les appelants rejoignent ou quittent une téléconférence. L'élément est désactivé par défaut.

Activation et configuration d'une conférence à plusieurs (MeetMe et Ad Hoc)

Pour activer et configurer la fonction de conférence à plusieurs participants, procédez comme suit :

ETAPE 1 Dans la fenêtre Conférence, choisissez d'activer la conférence à plusieurs.

- Cochez la case **Activer la conférence à plusieurs** pour autoriser la conférence à plusieurs participants (nécessite des ressources matérielles suffisantes).
  - Lorsque cette option est sélectionnée, la conférence Ad Hoc ou MeetMe peut être configurée.
  - Le nombre maximal de sessions configurables dépend du nombre de ressources matérielles disponibles pour la plateforme UC500 à configurer.
- Si vous n'activez pas la conférence à plusieurs, activez l'option **Nombre max. de sessions à 3**
  pour définir le nombre maximal de conférences Ad hoc tridirectionnelles que vous souhaitez autoriser.
  - Lorsque cette option est sélectionnée, les ressources logicielles de Cisco IOS sont utilisées pour la téléconférence. Les ressources matérielles ne sont pas nécessaires. Cette option est utilisée lorsque la fonction de conférence matérielle est désactivée ou n'est pas configurée.
  - Chaque conférence peut accueillir jusqu'à 3 participants.

ETAPE 2 Si l'option **Activer la conférence à plusieurs** est cochée, configurez les paramètres suivants :

a. Choisissez un **mode** : G711 (mode simple) ou G711/G729 (mode mixte).

   Le paramètre **Mode** définit le volume des ressources matérielles par appel affectées à chaque conférence. Le mode G711 exploite moins de ressources matérielles que le mode G711/G729.

   Le mode G711 est conseillé pour les déploiements exploitant uniquement des trunks locaux. Le mode mixte (G711/G729) est conseillé pour les déploiements couvrant des trunks SIP à condition que le fournisseur de services SIP prenne en charge la norme G729.

b. Sous **Paramètres de tonalité**, vous pouvez activer ou désactiver les tonalités émises lorsque les appelants rejoignent ou quittent une téléconférence.

Par défaut, les sons émis à l'arrivée ou au départ d'un participant sont désactivés. Lorsque la conférence à plusieurs est désactivée, les paramètres de tonalité le sont aussi.

c. Utilisez le menu déroulant pour sélectionner le **nombre maximum de participants** par conférence.

d. Utilisez le curseur sur la droite du menu **Sessions** pour répartir les sessions entre les options Ad hoc et Meet-Me. Le nombre total de sessions doit être inférieur ou égal au nombre maximum de sessions simultanées.

e. Modifiez les numéros de poste Meet-Me ou conservez les valeurs par défaut.

ETAPE 3 Cliquez sur **OK** ou **Appliquer**.

Restrictions et remarques relatives à la conférence à plusieurs

- Si vous installez une carte VIC à 8 ou 16 utilisateurs et que la conférence matérielle Ad hoc est déjà configurée pour le périphérique, avant l'installation de la carte VIC à l'aide de CCA, vous devrez rétablir la conférence logicielle en annulant la sélection de l'option **Activer la conférence à plusieurs** et en cliquant sur **Appliquer**.
- En cas de configuration DSP hors bande (par exemple, codage), la conférence à plusieurs n'est pas disponible. Vous devrez supprimer la configuration hors bande ou continuer la configuration hors bande.

Conference Barge

Pour configurer la fonction Conference Barge (cBarge) et un bouton Confidentialité supplémentaire sur les téléphones cBarge, sélectionnez **Configurer** > **Téléphonie** > **Fonctionnalités voix** > **Conference Barge** dans la barre de fonctions.

IMPORTANT La conférence à plusieurs doit être activée pour pouvoir utiliser les fonctions Conference Barge (cBarge) et Confidentialité. cBarge peut uniquement être activé sur les téléphones IP présentant au moins un numéro de ligne octale partagé.

Pour plus d'informations sur les fonctions cBarge et Confidentialité, consultez les rubriques suivantes :

- **Description des fonctions Conference Barge et Confidentialité, page 421**

Description des fonctions Conference Barge et Confidentialité

La fonction cBarge permet aux utilisateurs disposant de lignes octales sur leur téléphone d'appuyer sur la touche **cBarge** pour intégrer un appel en cours sur la ligne octale en question. Lorsqu'une tierce personne rejoint la discussion, une conférence Ad hoc est mise en place. D'autres utilisateurs pour qui la fonction cBarge est également configurée pour la même ligne octale peuvent accéder à la conférence (selon le nombre maximal d'utilisateurs défini). Les éléments suivants s'appliquent à la fonction cBarge :

- **Nombre max. de sessions cBarge**. Le nombre maximum de téléconférences cBarge actives est identique au nombre maximal de sessions Ad hoc autorisé sur votre système. Ces données sont visibles sous l'onglet Conférence.
- **Nombre maximal de participants cBarge par session**. Une conférence cBarge accepte un nombre maximal donné de participants. Cette valeur est définie sous la rubrique Conférence Ad hoc de votre plateforme UC500. Ces données sont visibles sous l'onglet Conférence.
- Si aucune conférence Ad hoc n'est disponible ou si le nombre maximal de participants a été atteint, la requête cBarge est rejetée et un message d'erreur s'affiche sur le téléphone à l'origine de l'appel.
- La conférence demeure effective tant qu'il reste au moins trois participants sur la ligne. Si seulement deux participants restent en ligne, ils sont redirigés vers un appel standard afin de libérer les ressources nécessaires à la conférence.
- Lorsque le destinataire de l'appel effectue un parcage d'appel ou associe l'appel à un autre, le module cBarge et les autres participants restent en ligne.

La fonction Confidentialité est associée à la fonction cBarge. Cette fonction permet aux utilisateurs disposant d'un module cBarge pour un numéro de poste partagé de bloquer les autres utilisateurs partageant le numéro de poste de voir les données d'appel, de reprendre l'appel ou d'intégrer un appel visant un numéro de poste partagé. Le téléphone doit présenter un bouton disponible pour pouvoir activer cette fonction.

Lorsque la fonction de confidentialité est configurée pour un téléphone doté de la fonction cBarge à l'aide de CCA :

- Un bouton Confidentialité est intégré au téléphone. Si aucun bouton de ligne n'est disponible, un message s'affiche dans la barre d'erreur de CCA.
- L'utilisateur peut appuyer sur le bouton Confidentialité de son téléphone pour activer ou désactiver la fonction.
- Lorsque la fonction de confidentialité est active, le bouton Confidentialité présent sur le téléphone de l'utilisateur devient orange.

Utilisation et exemples des fonctions cBarge et Confidentialité

Utilisation. Imaginons que l'Utilisateur A et l'Utilisateur B aient tous deux le numéro de poste 222 affecté à un bouton sur leur téléphone respectif. Le numéro 222 fait référence à un poste de ligne octale partagé. La fonction cBarge est active pour le poste 222 sur les deux téléphones et la fonction Confidentialité est désactivée.

La touche **cBarge** est accessible dès que l'Utilisateur A appuie sur le bouton de ligne pour le poste 222 afin de répondre à un appel entrant sur la ligne partagée. Tandis que l'Utilisateur A est en ligne sur le poste 222, l'utilisateur B peut appuyer sur la touche **cBarge** de son téléphone pour accéder à une conversation avec l'Utilisateur A et son interlocuteur à l'aide du numéro de poste 222. Cette démarche peut être effectuée en interne en créant une conférence Ad hoc entre l'Utilisateur A, l'Utilisateur B et l'autre partie sur le numéro de poste 222.

Pour aller plus loin :

- Si un troisième utilisateur, l'Utilisateur C, dispose également d'un numéro de poste de ligne octale sur son téléphone, il pourra lui aussi appuyer sur la touche **cBarge** de son téléphone pour accéder à la conférence.
- Si l'Utilisateur A appuie sur la touche Confidentialité de son téléphone et active ainsi la fonction de confidentialité, la touche **cBarge** ne sera pas accessible aux utilisateurs disposant du numéro de poste 222 sur leur téléphone. Aucun autre utilisateur ne pourra donc rejoindre l'appel.

Les fonctions cBarge et Confidentialité peuvent être activées ou désactivées sur les téléphones partageant le même numéro de poste sur une ligne octale. Lorsque la fonction cBarge est désactivée, la fonction de confidentialité reste accessible. Voici quelques exemples.

Exemple 1. Dans un environnement professionnel, tous les téléphones des employés partageant le même numéro de poste sur une ligne octale peuvent disposer d'une fonction cBarge et Confidentialité.

Téléphones/ Utilisateurs	cBarge	Confidentialité	Résultats de la configuration
Tous les téléphones	Activé	Activé	Chaque utilisateur du numéro de poste partagé peut accéder à n'importe quel appel effectué sur ce numéro de poste et/ou définir les options de confidentialité pour les appels effectués sur ce poste.

Exemple 2. Dans un environnement où un responsable et plusieurs employés partagent le même numéro de poste sur une ligne octale, les fonctions cBarge et Confidentialité peuvent être configurées selon l'exemple ci-dessous.

Téléphones/ Utilisateurs	cBarge	Confidentialité	Résultats de la configuration
Téléphone du responsable	Activé	Désactivé	Le superviseur peut accéder aux appels de ses employés effectués sur le numéro de poste de ligne octale partagé. L'option de confidentialité ne doit pas être activée sur le téléphone du responsable étant donné qu'aucun employé ne pourra accéder à un appel effectué sur ce numéro de poste.
Téléphones des employés	Désactivé	Désactivé	Les employés disposant de ce numéro de poste partagé ne peuvent pas accéder aux appels ni définir les options de confidentialité pour les appels effectués sur ce poste.

Exemple 3. Dans un bureau où un directeur dispose de plusieurs responsables supervisant un petit groupe d'employés, vous pouvez configurer les options cBarge et Confidentialité de la manière suivante :

Téléphones/ Utilisateurs	cBarge	Confidentialité	Résultats de la configuration
Téléphone du directeur	Activé	Activé	Le directeur peut accéder aux appels effectués sur le numéro de poste partagé par les responsables ou les employés. Seul le directeur peut effectuer des appels privés à partir de ce poste.
Téléphones des responsables	Activé	Désactivé	Le superviseur peut accéder aux appels de ses employés effectués sur le numéro de poste de ligne octale partagé. Il ne peut cependant pas accéder aux appels du directeur lorsque l'option Confidentialité est active.
Téléphones des employés	Désactivé	Désactivé	Les employés disposant de ce numéro de poste partagé ne peuvent pas accéder aux appels ni définir les options de confidentialité pour les appels effectués sur ce poste.

Eléments nécessaires aux fonctions cBarge et Confidentialité

Avant de configurer les fonctions Conference Barge et Confidentialité, votre système doit répondre aux critères suivants :

- La version 7.0.2 ou une version supérieure du paquet logiciel de l'UC500 est nécessaire pour veiller à ce que les versions requises de Cisco IOS et CUE soient installées (IOS 12.4(20)T2 et CUE 7.0 ou des versions supérieures). Pour les téléphones Cisco 7931, le paquet logiciel UC500 8.0.4 est requis.
- La conférence à plusieurs doit être activée. Les conférences Ad hoc et les participants doivent être configurés avant de définir les paramètres des fonctions cBarge et Confidentialité. Voir la rubrique **Téléconférence, page 417**.
- Les numéros de poste partagés pour les lignes octales doivent être configurés sur les téléphones avant de pouvoir configurer les fonctions cBarge et Confidentialité. Voir la rubrique **Configuration des numéros de poste de ligne octale partagée, page 425**.

Téléphones non pris en charge

Les fonctions cBarge et Confidentialité ne peuvent pas être configurées sur les téléphones dotés d'un seul bouton et les téléphones ne prenant pas en charge les numéros de répertoire pour les lignes octales partagées (NR). Les téléphones ne prenant pas en charge les NR de ligne octale partagée sont définis ci-dessous :

- Téléphones FXS analogiques
- ATA
- Téléphones Cisco 7935,7936,7937 et 39xx
  Les téléphones 7931 *sont* pris en charge.
- Téléphones IP Cisco CP-521
- Téléphones IP Cisco CP-52xG
- Téléphones IP Cisco 7902, 7905, 7906, 7910, 7911, 7912, 7920 et 7985
- Tous les téléphones SPA500 (SPA501G, SPA525G, SPA525G2 et SPA50x)
- Téléphones IP Cisco SPA300
- Téléphones analogiques SCCP (VG224)

Configuration des numéros de poste de ligne octale partagée

Pour de plus amples informations sur les lignes octales consultez la rubrique **Lignes octales, page 373**.

Pour configurer un numéro de poste de ligne octale partagée sur un téléphone de sorte que la fonction **cBarge** puisse être activée sur un téléphone, suivez les étapes suivantes.

ETAPE 1 Suivez les instructions de la rubrique **Poste partagé, page 361**.

ETAPE 2 Veillez à configurer le type de ligne sur l'option **Ligne octale** lorsque vous configurez les options de ligne pour le bouton Partagé du téléphone.

ETAPE 3 Une fois le numéro de poste créé pour la ligne octale partagée, affectez cette ligne à un bouton pour chaque téléphone où les fonctions cBarge et Confidentialité sont actives.

Pour obtenir la liste des téléphones incompatibles avec cette fonction, consultez la rubrique **Téléphones non pris en charge, page 425**.

ETAPE 4 Cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre Utilisateurs et téléphones.

Configuration de la fonction Conference Barge et des fonctions de confidentialité

Une fois la conférence à plusieurs activée et les numéros de poste de ligne octale partagée définis sur les téléphones, suivez les étapes suivantes pour configurer les fonctions cBarge et Confidentialité pour ces numéros de poste.

ETAPE 1 Dans la barre de fonctions sur la gauche, sélectionnez l'option **Configurer** > **Téléphonie** > **Fonctionnalités voix** >**Conference Barge**.

Tous les téléphones dotés d'un numéro de poste de ligne octale partagée. Les fonctions cBarge et Confidentialité sont désactivées par défaut sur ces numéros de poste.

ETAPE 2 Pour chaque téléphone, indiquez si vous souhaitez activer les fonctions cBarge et Confidentialité.

Les fonctions cBarge et Confidentialité peuvent être activées ou désactivées sur les téléphones partageant le même numéro de poste sur une ligne octale. Pour obtenir des exemples d'utilisation, voir **Utilisation et exemples des fonctions cBarge et Confidentialité, page 422**.

Pour activer la fonction de confidentialité pour une ligne octale, un bouton de ligne doit être disponible. En l'absence de bouton de ligne disponible sur le téléphone, la barre d'erreur affiche le message "Impossible d'activer la fonction de confidentialité pour <*Prénom Nom*> (*nom d'utilisateur*) car aucun bouton de ligne n'est disponible."

ETAPE 3 Cliquez sur **OK** ou **Appliquer**.

Suppression de la fonction cBarge et Confidentialité sur le téléphone d'un utilisateur

Pour supprimer la fonction cBarge et Confidentialité à partir d'un téléphone, procédez comme suit :

ETAPE 1 Dans la barre de fonctions sur la gauche, sélectionnez l'option **Configurer** > **Téléphonie** > **Fonctionnalités voix** >**Conference Barge**.

ETAPE 2 Localisez l'utilisateur dans la liste.

ETAPE 3 Pour supprimer la fonction cBarge du téléphone de l'utilisateur, sélectionnez l'option **Désactivé** dans la liste déroulante de la colonne cBarge.

ETAPE 4 Pour supprimer la fonction Confidentialité du téléphone de l'utilisateur, sélectionnez l'option **Désactivé** dans la liste déroulante de la colonne Confidentialité.

ETAPE 5 Cliquez sur **OK** ou **Appliquer**.

Musique d'attente

Pour configurer la musique d'attente, sélectionnez **Configurer** > **Téléphonie** > **Fonctionnalités voix**> **Musique d'attente** dans la barre de fonctions.

Vue d'ensemble

La fonction Musique d'attente permet d'intégrer une musique en provenance d'une source de diffusion en direct externe ou d'un fichier .wav stocké dans la mémoire flash de l'UC500 lorsqu'un appel est mis en attente.

Procédures

Pour configurer la musique d'attente, procédez comme suit :

ETAPE 1 Dans le champ **Fichier audio**, sélectionnez **Aucun** ou sélectionnez un fichier audio.

ETAPE 2 Indiquez si vous souhaitez activer la musique d'attente pour les appels internes et/ou activer la musique d'attente à partir d'une source externe reliée au port Musique d'attente de l'UC500.

- Lorsque l'option **Activer la musique d'attente pour les appels internes** est activée, la musique d'attente est émise lors des appels internes d'un téléphone IP à un autre mis en attente. Dans le cas contraire, les appelants internes entendront la tonalité de mise en attente.

- Lorsque l'option **Activer le port pour la musique d'attente externe** est cochée, la musique d'attente est automatiquement activée pour les appels internes. Cette fonction ne peut pas être désactivée. Si un fichier audio a été sélectionné et que le port correspondant a été activé, la musique en provenance de la source externe est prioritaire. Le fichier audio sélectionné prend le relais en cas de défaillance ou d'indisponibilité de la source externe.
- La musique d'attente est toujours active pour le SDA et le trunk SIP, même si la fonction est désactivée pour les appels internes. Pour désactiver la musique d'attente pour les appels du SDA et du trunk SIP, annulez la sélection des options et sélectionnez Aucun comme fichier audio.

ETAPE 3 Cliquez sur **Appliquer**.

Pour charger une musique d'attente personnalisée (fichier .au) sur l'UC500, procédez comme suit :

ETAPE 1 Sélectionnez **Accueil** > **Topologie** pour afficher la fenêtre Topologie.

ETAPE 2 Glissez et déposez le fichier audio à partir de votre Bureau vers l'icône de l'UC500 dans la fenêtre Topologie.

Le fichier audio doit être au format .au.

Une fois le fichier chargé, il est accessible dans la liste Fichier audio.

Pour de plus amples informations sur la création d'un fichier audio personnalisé comme musique d'attente, consultez le guide *Cisco Unified Communications Manager Express System Administrator Guide* disponible sur Cisco.com.

13

Gestion des appels

Les rubriques suivantes sont présentées :

- **Programmes**
- **Standard automatique**
- **Répartition des appels (B-ACD)**
- **Service de nuit**
- **Enregistrer en direct**
- **T.37 Fax vers e-mail**

Programmes

Pour paramétrer les programmes, sélectionnez l'option **Configurer** > **Téléphonie** > **Gestion des appels** > **Programmes**.

Les heures de bureau, les vacances et le service de nuit sont gérés grâce aux onglets de la fenêtre Programmes.

- **Heures de bureau**
- **Congés**
- **Programme du service de nuit**

Heures de bureau

Le programme des heures de bureau établit les heures d'ouverture et de fermeture. Cela autorise la configuration de différentes invites sur le **Standard automatique**. Il pourra ainsi réaliser différentes opérations en fonction des heures d'ouverture et de fermeture. Vous pouvez définir jusqu'à quatre horaires différents.

Si vous utilisez plusieurs standards automatiques, vous pourrez définir un horaire différent pour chacun d'entre eux. Vous pouvez définir les heures d'ouverture et de fermeture pour chaque jour de la semaine par incrément de 30 minutes.

Pour activer et définir un horaire, procédez comme suit :

ETAPE 1 Sélectionnez un horaire dans la liste sur la gauche de l'onglet.

ETAPE 2 Cliquez sur **Activer le programme des heures de bureau** pour activer et ouvrir l'horaire sélectionné afin de le modifier.

ETAPE 3 Modifiez le nom de l'horaire et entrez un nom plus précis. Le nom par défaut est systemschedule.

ETAPE 4 Utilisez le menu déroulant en haut de la fenêtre pour définir les heures d'ouverture et de fermeture en vigueur pour les différents jours de la semaine. Cliquez ensuite sur **Mettre à jour tableau** pour actualiser l'affichage.

Vous pouvez aussi cocher les cases du tableau pour définir les heures d'ouverture.

Les heures associées à une coche correspondent aux heures d'ouverture.

ETAPE 5 Cliquez sur **OK** ou **Appliquer**.

Congés

Vous pouvez définir jusqu'à 26 jours de congé par an, pour l'année en cours ou pour la suivante. Toutefois, si le service de nuit est aussi défini, celui-ci ne sera activé que pour les 15 premiers jours de congé introduits (un message d'avertissement s'affiche si le service de nuit est actif et que vous ajoutez plus de 15 jours de congé). Pour les congés définis, le **Standard automatique** active les invites et les actions définies pour les heures de fermeture. **Service de nuit** est activé s'il est configuré pour le site.

Vous pouvez aussi modifier ou supprimer les congés existants ou copier les congés de l'année en cours vers l'année suivante. Lorsque vous copiez les congés de l'année en cours à l'année suivante, si la même date s'affiche pour les deux années, l'entrée pour l'année en cours est utilisée.

REMARQUE Vous ne pouvez pas modifier l'année d'un congé existant. Supprimez le congé pour le rajouter ensuite si vous devez modifier l'année.

Pour ajouter une année, procédez comme suit :

ETAPE 1 Dans la fenêtre Programmes, sélectionnez l'année en cours ou l'année suivante.

ETAPE 2 Cliquez sur **Ajouter** pour afficher la fenêtre Ajouter congé (voir **Ajouter congé, page 431**).

ETAPE 3 Lorsque vous en avez terminé avec l'ajout des congés, cliquez sur **OK**.

Ajouter congé

Cette fenêtre s'affiche lorsque vous cliquez sur **Ajouter congé** dans la fenêtre Programmes.

Pour ajouter un congé, procédez comme suit :

ETAPE 1 Cliquez sur l'icône Calendrier et sélectionner une date pour l'année active.

ETAPE 2 Utilisez les flèches Suivant (>) et Précédent (<) pour accéder aux autres mois du calendrier.

ETAPE 3 Entrez une description du congé. La description peut contenir jusqu'à 64 caractères.

ETAPE 4 Cliquez sur **OK**.

Programme du service de nuit

Définissez les heures d'activation du Service de nuit pour chaque jour de la semaine.

Une fois que vous avez configuré le programme pour le service de nuit, allez dans **Configurer** > **Téléphonie** > **Gestion des appels** > **Service de nuit** pour activer et configurer la fonction.

Pendant les heures du service de nuit :

- Le service de nuit est activé pour les téléphones et numéros de poste définis.
- Les appels vers les postes prévoyant un transfert d'appel après leurs heures de bureau sont automatiquement transférés vers le numéro en question.

Pendant les congés, le service de nuit est activé s'il est configuré pour le site.

Pour configurer les heures du Service de nuit, procédez comme suit :

ETAPE 1 Sélectionnez un jour de la semaine dans le menu déroulant ou cliquez sur la ligne correspondant au jour de la semaine concerné dans la fenêtre Programme du service de nuit.

ETAPE 2 Utilisez les menus déroulants **de** et **à** pour définir les heures pour la journée en question. Cliquez sur **Supprimer** pour réinitialiser les horaires.

ETAPE 3 Cliquez sur **Ajouter** pour ajouter des horaires. Passez cette étape si vous supprimez des heures.

ETAPE 4 Continuez la sélection des jours de la semaine pour définir les horaires du service de nuit.

Utilisez l'option **Copier la ligne sélectionnée vers** pour copier les paramètres d'un jour à l'autre pour la semaine ou le week-end.

Exemple : si vous souhaitez que le service de nuit soit actif de 16h00 à 9h00 du lundi au vendredi et 24 heures les samedis et dimanches, définissez les heures de début et de fin comme suit :

Jour	Heure de début (HH:MM)	Heure de fin (HH:MM)
Lundi	**17:00**	**8:00**
Mardi	**17:00**	**8:00**
Mercredi	**17:00**	**8:00**
Jeudi	**17:00**	**8:00**
Vendredi	**17:00**	**8:00**
Samedi	**9:00**	**8:00**
Dimanche	**9:00**	**8:00**

ETAPE 5 Cliquez sur **OK** ou **Appliquer**.

Pour de plus amples informations, consultez les rubriques suivantes :

- **Standard automatique, page 433**
- **Service de nuit, page 449**

Standard automatique

Pour configurer un Standard automatique et gérer les invites et les scripts, sélectionnez l'option **Configurer** > **Téléphonie** > **Gestion des appels**> **Standard automatique**.

Les rubriques suivantes sont présentées :

- **Prérequis**
- **Configuration du standard automatique**
- **Gestion des invites**
- **Gestion des scripts**

Prérequis

Avant de définir la configuration et les invites du Standard automatique, vous devez avoir défini les fonctions de téléphonie suivantes :

REMARQUE L'accès Telnet doit être activé pour pouvoir configurer les fonctions du Standard automatique.

- Numéros de poste et comptes de messagerie associés
- Plan de numérotation et fonctionnalités voix associées
- Programmes des heures de bureau et des congés
- Paramètres du service Basic ACD (le cas échéant)
- Préfixe pour le transfert vers la messagerie vocale si l'option **Transfert direct vers la messagerie vocale** est utilisée comme option pour le Standard automatique.

Configuration du standard automatique

L'onglet Standard automatique affiche les options permettant d'activer ou de désactiver le standard automatique. Il offre également le choix entre la configuration d'un système standard avec un seul niveau de menus (par défaut) ou un système sur plusieurs niveaux avec des menus intermédiaires.

Pour les consignes sur la configuration du Standard automatique, consultez les opérations suivantes :

Modes du standard automatique

Trois modes sont disponibles pour le Standard automatique :

- **Off**. Lorsque le mode Standard automatique est désactivé (**Off**), les paramètres par défaut sont utilisés et le Script SA est défini sur aa.aef.

  Si vous choisissez de désactiver le Standard automatique en optant pour le mode **Off**, les associations du plan de numérotation aux numéros SDA externes du SA et aux numéros de postes internes du SA seront supprimées. Il est possible que les fonctions vocales référençant le Standard automatique (numéro principal, groupements de postes et groupes d'appel) doivent être modifiées.

- **Standard**. Le mode Standard automatique **standard** vous permet de configurer jusqu'à 3 standards automatiques avec une arborescence de menus distincte pour chacun. Voir la rubrique **Configuration d'un standard automatique standard, page 434**.

- **Multi-niveaux**. Le mode Standard automatique **multi-niveaux** vous permet de configurer le SA afin d'offrir aux appelants un menu principal avec un maximum de trois menus intermédiaires. Voir la rubrique **Configuration d'un standard automatique multi-niveaux, page 437**.

Lorsque vous modifiez le mode Standard automatique, la configuration existante du Standard automatique n'est pas conservée. Vous devez définir tous les paramètres si vous changez de mode.

Configuration d'un standard automatique standard

Pour configurer un standard automatique standard, procédez comme suit :

ETAPE 1 Dans le champ **Mode**, veillez à sélectionner l'option **Standard**.

ETAPE 2 Dans le champ **Nombre de standards automatiques**, sélectionnez le nombre de standards automatiques à configurer.

ETAPE 3 Dans le champ **Numéro du SA**, entrez le numéro de poste à contacter pour accéder aux fonctions générales du standard automatique.

Il s'agit généralement du numéro de poste principal pour le bureau. Lorsque quelqu'un appelle ce numéro, le script du Standard automatique s'exécute. Le numéro du SA doit être unique pour tout le système. La numéro de poste par défaut pour le SA est le 398.

ETAPE 4 Dans le champ **Numéro SDA SA**, entrez le numéro SDA à contacter pour accéder aux fonctions générales du standard automatique.

Le numéro SDA peut commencer par un caractère "+".

ETAPE 5 Dans le champ **Script SA**, sélectionnez le script SA qui sera exécuté lors de l'activation du Standard automatique.

Les scripts CCA et les scripts système sont affichés.

- **aa_sbcs_v03.aef** est le script par défaut. Il s'agit d'un script avancé prenant en charge les menus SA multi-niveaux et permettant la configuration d'actions et d'invites distinctes pour les heures de bureau et les heures de fermeture d'après les programmes définis pour les paramètres Heures de bureau et Congé. Il prend également en charge les options **Composer par numéro** et **Autoriser le transfert externe** ainsi que le basculement vers un numéro personnalisé (**Pas de choix, transférer vers**) si l'appelant ne réagit pas aux invites du menu après trois annonces.
- **aa_sbcs_v02.aef** a la même fonction que **aa_sbcs_v03.aef** à l'exception du champ **Pas de choix, transférer vers**.
- **aa.aef** et **aasimple.aef** sont les scripts système par défaut déployés dans le cadre de Cisco Unity Express (CUE). Lorsque l'un de ces scripts est sélectionné, CCA permet uniquement la configuration des paramètres de base (Numéro du SA, Numéro SDA SA, Script SA).
- **aa_transfer2.aef** est une version mise à jour du script aa_transfer.aef prenant en charge deux options principales complémentaires (**#** et *****) et l'action **Lire invite**.

Vous pouvez charger des scripts personnalisés. Toutefois, pour les scripts personnalisés, CCA configure uniquement le numéro du SA et le numéro SDA SA. Voir la rubrique **Gestion des scripts, page 440**. Ces étapes de configuration ne s'appliquent que lorsque le script du standard automatique **aa_sbcs_v02.aef** ou **aa_sbcs_v03.aef** est sélectionné.

La migration entre les scripts SA n'est pas prise en charge. Lorsque vous modifiez le script SA, la configuration existante du Standard automatique n'est pas conservée.

ETAPE 6 Dans le champ **Programme des heures de bureau**, sélectionnez les heures d'ouverture pour le Standard automatique.

ETAPE 7 Vous pouvez également activer les fonctions **Composer par numéro à tout moment** et **Autoriser le transfert externe**. Lorsque la fonction **Composer par numéro à tout moment** est active, les appelants peuvent entrer le numéro du destinataire à tout moment pour passer l'appel.

ETAPE 8 Si vous utilisez le script **aa_sbcs_v03.aef**, vous pouvez entrer un numéro dans le champ **Pas de choix, transférer vers**. Il peut s'agir d'un numéro PSTN externe ou d'un numéro de poste interne.

- Lorsque vous introduisez un numéro PSTN externe, introduisez le numéro tel que vous le composeriez, sans oublier le code d'accès.
- Si vous définissez un numéro de poste interne, veillez à introduire correctement le numéro de poste. CCA ne vérifie pas si le numéro de poste est valable pour votre système.

Si vous définissez un numéro pour l'option **Pas de choix, transférer vers** et que l'appelant n'appuie pas sur l'une des touches associées à une action, le menu principal est répété à deux reprises avant que l'appel soit redirigé vers le numéro indiqué.

Si vous ne définissez aucun numéro dans ce champ et que l'appelant n'appuie pas sur l'une des touches associées à une action, le menu principal est répété à deux reprises avant que l'appel soit interrompu.

ETAPE 9 Effectuez les mêmes opérations pour configurer les invites et les actions pour les **Heures de bureau** et les **Heures de fermeture**.

a. Dans le champ **Invite de menu**, sélectionnez le fichier .wav correspondant à l'invite diffusée lors de l'activation du Standard automatique.

b. (*Facultatif*) Vous pouvez aussi cliquer sur **Enregistrer** pour utiliser la fonction d'enregistrement et de lecture de CCA afin d'enregistrer les invites de menu.

c. Définissez les actions principales. Pour chaque action que vous souhaitez définir, effectuez les opérations suivantes :

- Cliquez sur la colonne **Mode** pour sélectionner le type d'action.
- Cliquez dans la colonne **Paramètres** pour définir les paramètres d'entrée (le cas échéant).

Par exemple, pour que le SA renvoie l'appel vers un groupement de postes dès que l'utilisateur appuie sur la touche 4, sélectionnez l'option **Appeler groupement de postes** dans la colonne **Mode** et sélectionnez ensuite un groupement de postes dans la liste des groupements de postes figurant dans la colonne **Paramètre**.

Vous avez le choix entre les actions suivantes : **Appeler groupe d'appels**, **Appeler groupement de postes**, **Appeler la messagerie**, **Transférer vers la messagerie**, **Transférer vers Basic ACD**, **Appeler le poste**, **Lire invite**, **Appeler par nom**, **Appeler par numéro**, **Appeler un autre numéro** et **Aucun**.

Si un numéro externe est défini pour l'option **Appeler un autre numéro**, veillez à ce que le numéro soit introduit de la manière dont il sera composé, avec les codes d'accès ou les codes pour les appels interurbains (le cas échéant).

ETAPE 10 Cliquez sur **OK** ou **Appliquer**.

Configuration d'un standard automatique multi-niveaux

Le mode Standard automatique **multi-niveaux** vous permet de configurer le SA afin d'offrir aux appelants un menu principal avec un maximum de trois menus intermédiaires.

Si vous optez pour plusieurs standards automatiques (jusque 3), des onglets supplémentaires s'affichent pour configurer chacun d'entre eux. Les étapes de configuration sont les mêmes.

La configuration du standard multi-niveaux et de ses sous-menus est identique à la configuration d'un **Standard automatique standard**. Les exceptions suivantes subsistent cependant :

- Pour la configuration du menu principal, le script par défaut du standard automatique (**aa_sbcs_v03.aef**) est toujours utilisé et l'option de sélection du script n'est pas disponible.
- Pour les sous-menus, le script aa_transfer2.aef est toujours utilisé et l'option de sélection du script n'est pas disponible.
- L'option supplémentaire **Menu d'appel** s'affiche afin que vous puissiez définir les codes permettant de passer du menu principal aux menus intermédiaires.

Pour des informations détaillées sur la configuration des autres paramètres, voir **Configuration d'un standard automatique standard, page 434**.

Gestion des invites

L'onglet Gestion des invites vous permet d'effectuer les opérations suivantes :

- Créer des invites à l'aide des techniques suivantes :
  - **Enregistrer l'invite avec l'enregistreur de CCA**. Cette méthode vous permet d'enregistrer et de lire les invites à partir de CCA grâce au magnétophone intégré. Voir la rubrique **Enregistrer l'invite avec l'enregistreur, page 439**.
  - **Charger des invites préalablement enregistrées à partir d'un PC**. Vous pouvez enregistrer ou lire des fichiers .wav sur votre PC et les charger sur CUE. Le fichier .wav doit être enregistré au format mono G.711 u-law, 8 bits et 8 kHz sous Windows ou G.711 u-law, 8 bits et 44100 Hz sous Mac. L'invite ne peut pas dépasser les 60 secondes. Voir la rubrique **Charger les invites, page 439**.
  - **Utilisez le CUE Greeting Management System pour enregistrer les invites à partir d'un téléphone.** Pour utiliser cette méthode, vous devez configurer un numéro de poste pour la gestion des invites du SA sur CUE et affecter les privilèges de gestion des invites aux utilisateurs. L'enregistrement à partir du téléphone évite le recours à un PC ou un logiciel audio pour gérer les invites.

    Le numéro de poste pour la gestion des invites est celui que les utilisateurs disposant des autorisations nécessaires doivent composer pour enregistrer ou supprimer les invites. Lorsqu'un utilisateur doté des autorisations nécessaires compose ce numéro, il doit introduire son numéro de poste et le code d'accès à la messagerie pour se connecter. Voir **Activation de l'enregistrement des invites par téléphone et affectation des privilèges de gestion des invites aux utilisateurs, page 439**.
- Chargement des invites. Voir la rubrique **Charger les invites, page 439**.
- Modification du nom de l'invite.

  Les noms de fichier pour les invites personnalisées enregistrées à l'aide du téléphone ou à l'aide du magnétophone intégré sont enregistrées selon le modèle suivant User_Prompt_<*date_heure*>.wav.

  Pour renommer une invite de manière à pouvoir facilement la reconnaître, cliquez sur le **nom de l'invite** dans la liste des invites disponibles. Modifiez le nom et cliquez sur **OK**.
- Suppression des invites.

Pour supprimer une invite, cliquez sur le **nom de l'invite** dans la liste des Invites disponibles. Cliquez sur **Supprimer** et cliquez sur **OK**.

Enregistrer l'invite avec l'enregistreur

Procédez comme suit pour enregistrer des invites pour le Standard automatique ou pour Basic ACD à l'aide du magnétophone intégré :

ETAPE 1 Cliquez sur l'onglet Gestion des invites dans la fenêtre Standard automatique.

ETAPE 2 Dans le volet **Créer des invites, Enregistrer avec l'enregistreur** de l'onglet Gestion des invites, cliquez sur **Ouvrir**.

ETAPE 3 Utilisez le magnétophone intégré et enregistrez l'invite. Voir la rubrique **Magnétophone, page 440**.

Charger les invites

Pour charger un fichier d'invite enregistré à partir de votre PC, procédez comme suit :

ETAPE 1 Cliquez sur l'onglet Gestion des invites dans la fenêtre Standard automatique.

ETAPE 2 Dans le volet **Invites disponibles** de la fenêtre **Gestion des invites**, cliquez sur **Ajouter**.

ETAPE 3 Cliquez sur **Parcourir** pour accéder au dossier où se trouve le fichier d'invite sur votre PC.

ETAPE 4 *Facultatif* : Utilisez les commandes **Lire invite** pour écouter l'invite.

ETAPE 5 Cliquez sur **OK**.

Activation de l'enregistrement des invites par téléphone et affectation des privilèges de gestion des invites aux utilisateurs

Pour activer l'enregistrement des invites avec un téléphone et affecter des privilèges de gestion des invites aux utilisateurs, procédez comme suit :

ETAPE 1 Cliquez sur l'onglet Gestion des invites dans la fenêtre Standard automatique.

ETAPE 2 Dans le champ **Poste d'enregistrement des invites**, entrez le numéro de poste utilisé pour l'enregistrement des invites.

ETAPE 3 Dans le champ **Administrateurs des invites**, cliquez sur **Utilisateurs**.

ETAPE 4 Dans la fenêtre **Affecter les privilèges de l'invite aux utilisateurs**, utilisez les flèches **Ajouter** et **Supprimer** ou utilisez la fonction **Sélectionner tout** pour gérer la liste des utilisateurs sélectionnés.

ETAPE 5 Cliquez sur **OK**.

Magnétophone

Cette fenêtre s'affiche lorsque vous cliquez sur **Enregistrer** sous l'onglet Gestion des invites du Standard automatique ou lorsque vous cliquez sur **Enregistrer** dans la fenêtre Créer/modifier les paramètres Basic ACD.

Procédez comme suit pour enregistrer des invites pour le Standard automatique ou pour Basic ACD à l'aide du magnétophone intégré :

ETAPE 1 Cliquez sur **Enregistrer** et enregistrez votre message. Vous pouvez faire une pause, revenir en arrière et arrêter l'enregistrement.

ETAPE 2 Lorsque vous êtes satisfait de votre enregistrement, cliquez sur **Parcourir** pour accéder à l'emplacement où vous souhaitez enregistrer le fichier .wav sur votre PC et entrez un nom de fichier pour l'invite.

ETAPE 3 Cliquez sur **OK**. Lorsque vous cliquez sur **OK**, CCA ferme le magnétophone et enregistre un nouveau fichier d'invite sur vote PC.

Gestion des scripts

Vous pouvez charger, renommer et supprimer des scripts personnalisés créés à l'aide de l'éditeur de scripts SA CUE.

Vous pouvez utiliser jusqu'à deux scripts SA personnalisés. Un maximum de 12 scripts est autorisé. Cependant, dix d'entre eux sont réservés pour CCA et les scripts par défaut de CUE. Ils ne peuvent donc pas être supprimés.

Pour les scripts personnalisés, CCA configure uniquement le numéro du SA et le numéro SDA SA. Vous devez utiliser l'interface de CUE pour configurer les autres paramètres de script.

Les scripts SA pris en charge par CCA (aa_transfer2.aef, aa_sbcs_v02.aef et aa_sbcs_v03.aef) et les scripts SA CUE par défaut (aa.aef et aasimple.aef) ne peuvent pas être supprimés, modifiés, renommés ou écrasés.

Pour plus d'informations sur la création des scripts SA CUE, reportez-vous au guide intitulé *Cisco Unity Express Guide to Writing and Editing Scripts* disponible sur Cisco.com.

Procédures

Pour charger un script SA personnalisé, suivez les étapes suivantes :

ETAPE 1 Cliquez sur l'onglet Gestion des scripts dans la fenêtre Standard automatique et cliquez sur **Ajouter**.

ETAPE 2 Cliquez sur **Parcourir** pour accéder au dossier où se trouve le fichier sur votre PC.

ETAPE 3 Cliquez sur **OK**.

Pour supprimer un script SA personnalisé, suivez les étapes suivantes :

ETAPE 1 Cliquez sur l'onglet Gestion des scripts dans la fenêtre Standard automatique et cliquez sur un script dans la liste Invites disponibles pour le sélectionner.

ETAPE 2 Cliquez sur **Supprimer**.

Vous ne pouvez pas supprimer les scripts en cours d'utilisation par le Standard automatique.

Répartition des appels (B-ACD)

Pour configurer la fonction Basic ACD, sélectionnez **Configurer** > **Téléphonie** > **Gestion des appels** > **Basic ACD** dans la barre de fonctions.

Cette partie couvre les rubriques suivantes :

- **Vue d'ensemble**
- **Avant de commencer**
- **Créer/modifier les paramètres Basic ACD**

- **Configuration du service Basic ACD**
- **Paramètres des rapports du groupement de postes**

Vue d'ensemble

La fonction Basic ACD permet de répondre et de répartir automatiquement les appels entrants grâce à des menus interactifs et des groupements de postes.

L'application Basic ACD se compose d'une file d'appels et d'un maximum de 10 services Basic ACD. Pour chaque service Basic ACD, vous pouvez configurer un numéro pilote, les paramètres des groupements de postes, les invites, la cible des appels restés sans réponse, le délai d'expiration, le nombre de rappels, etc.

Le flux d'appels Basic ACD mis en oeuvre sous Configuration Assistant se limite au *mode drop-through* où le Standard automatique fait office de point d'entrée principal alors que le contrôle est transmis au système Basic ACD pour les menus secondaires.

Lorsque le Standard automatique est en mode Drop-through, il envoie les appels entrants directement à la file d'appels sans détailler le menu aux appelants. Une fois dans la file, l'appelant entend une tonalité si un agent est disponible ou la musique d'attente si tous les agents sont occupés. En présence d'une invite pour le mode Drop-through, l'appelant entend l'invite avant d'être renvoyé dans la file d'attente. L'invite est simplement un message de bienvenue. Par exemple : "Merci d'avoir appelé XYZ. Nous répondrons à votre appel dans quelques instants." Les clients ne peuvent pas faire de choix en mode Drop-through. Les appels sont simplement pris en charge et acheminés vers une file d'attente.

Les fonctions B-ACD de la plateforme UC500 sont reprises dans la liste ci-dessous :

- Jusqu'à 10 groupements de postes B-ACD (files d'appel)
- Jusqu'à 30 appels autorisés dans chaque file
- Un maximum de 20 agents peuvent être membres du groupement de poste B-ACD

A partir de la version 2.5, CCA ajoute la touche **HLog** aux téléphones B-ACD. Les agents peuvent désormais se connecter ou se déconnecter d'un groupement de postes B-ACD à l'aide de la touche **HLog**. La touche **HLog** s'affiche sur les téléphones des agents en cas de réception d'un appel par le groupement de postes B-ACD. Les utilisateurs peuvent aussi utiliser la touche à partir de l'écran

principal du téléphone en appuyant sur la touche **plus**. La touche **HLog** remplace l'utilisation de la fonction DnD (Do Not Disturb - Ne pas déranger). DnD est moins polyvalent étant donné que l'abonné est indisponible d'une manière générale et pas seulement pour les appels du groupement B-ACD.

Voir **Créer/modifier les paramètres Basic ACD, page 444** pour une explication des paramètres affichés dans la fenêtre Basic ACD contenant les services configurés.

Avant de commencer

Avant de configurer Basic ACD :

- Établissez le flux d'appels et les options à présenter aux appelants.
- Établissez les invites nécessaires et celles qui doivent être personnalisées.
- Veillez à ce que les téléphones et les utilisateurs soient configurés.
- Lorsque vous configurez Basic ACD, Configuration Assistant crée automatiquement des groupements de postes pour la prise en charge du transfert d'appel Basic ACD. Les paramètres de ces groupements de postes sont configurés à partir de la fenêtre Créer/modifier les paramètres Basic ACD.
- Configurez les paramètres de base du standard automatique. Après avoir paramétré la fonction Basic ACD, vous pourrez sélectionner l'option **Transférer vers Basic ACD**, ce qui permet au service B-ACD de prendre le contrôle.

Configuration du service Basic ACD

Pour configurer un service Basic ACD, procédez comme suit :

ETAPE 1 Dans le volet **Récapitulatif des paramètres de base** de la fenêtre Basic ACD, cliquez sur **Créer** ou **Modifier**. La fenêtre Créer/modifier les paramètres Basic s'affiche.

ETAPE 2 Configurez les paramètres du service, des groupements de postes et des invites à partir de la fenêtre Créer/modifier les paramètres Basic ACD. Voir **Créer/modifier les paramètres Basic ACD, page 444** pour plus d'informations sur ces paramètres.

ETAPE 3 Cliquez sur **OK** ou **Appliquer** et fermez la fenêtre Basic ACD.

Une fois que vous avez créé le service et le groupement de postes local, l'option **Transférer vers Basic ACD** est disponible dans la fenêtre Standard automatique. Sélectionnez cette action pour définir la touche permettant au Standard automatique de passer les commandes au service Basic ACD lorsque l'appelant appuie sur la touche en question.

Effectuez les opérations suivantes pour associer un service Basic ACD à un bouton à l'aide du Standard automatique :

Cette procédure suppose que vous ayez déjà configuré les messages d'accueil de base pour le Standard automatique, les programmes et les invites.

ETAPE 1 Accédez à la fonction **Configurer** > **Téléphonie** > **Gestion des appels** > **Standard automatique**.

ETAPE 2 Sélectionnez l'onglet Standard automatique.

ETAPE 3 Désignez la touche que les appelants devront utiliser pour être automatiquement transférés au service Basic ACD que vous venez de configurer et sélectionnez l'option **Transférer vers Basic ACD** dans le champ **Mode**.

Le champ Paramètre est automatiquement mis à jour et affiche le numéro de poste pilote pour le service Basic ACD. Par exemple : **701 (aaService0)**.

Créer/modifier les paramètres Basic ACD

La fenêtre Créer/modifier les paramètres Basic ACD s'affiche lorsque vous cliquez sur **Créer** ou **Modifier** dans la fenêtre Basic ACD (**Configurer** > **Téléphonie** > **Gestion des appels** > **Basic ACD**).

Paramètres de service

Configurez les paramètres de service ci-dessous pour chaque service Basic ACD. Vous pouvez configurer jusqu'à 10 services Basic ACD.

Paramètre	Description
Numéro pilote	Numéro de poste correspondant au service Basic ACD. Il s'agit du numéro composé par le Standard automatique lors de l'action Transférer vers Basic ACD.

Paramètre	Description
Transfert si pas de réponse vers	Cible des appels restés sans réponse effectués par le groupement de postes B-ACD, soit parce que tous les agents sont déconnectés ou occupés, soit parce que la limite maximale autorisée a été dépassée. Les appels non pris en charge peuvent être transférés aux fonctions suivantes : Standard automatique, Groupement de postes, Groupe d'appels, Messagerie, Numéro de poste interne, Autre numéro (numéro PSTN externe).
Tonalité Ligne occupée après x secondes	Nombre de secondes d'attente avant l'émission de la tonalité Ligne occupée par le système Basic ACD. Il s'agit du laps de temps séparant le moment où l'appelant rejoint la file d'attente B-ACD et la répétition du message d'accueil. Ce même intervalle est utilisé entre les répétitions du message d'accueil. Vous pouvez entrer des valeurs comprises entre 30 et 120 secondes. La valeur par défaut est 60 secondes. Le fichier associé par défaut au signal Ligne occupée est en_bacd_allagentsbusy.au.
Transfert si pas de réponse en x secondes	Durée maximale de la tentative d'appel avant son transfert vers la cible définie dans le champ **Transfert si pas de réponse vers**. Il s'agit de la durée maximale au cours de laquelle l'appel peut rester dans la file. Vous pouvez entrer des valeurs comprises entre 60 et 3600 secondes. La valeur par défaut est 600 secondes.
Nombre d'essais en x secondes	Nombre de secondes d'attente avant le renvoi de l'appel vers le groupement de postes local pour le service B-ACD.
Transférer vers Invite B-ACD	*Facultatif*. Nom du fichier correspondant au message Transférer vers l'invite B-ACD.
Message d'accueil	*Facultatif*. Nom du fichier correspondant au message d'accueil pour la fonction B-ACD.
Nombre maximal de tentatives avant l'abandon	Nombre d'essais pour atteindre la cible définie dans le champ **Transfert si pas de réponse vers** avant l'abandon de l'appel. En cas d'abandon, le message de fin d'appel pour la fonction Basic ACD est exécuté. Vous pouvez entrer des valeurs comprises entre 1 et 3. La valeur par défaut est 1.

Paramètres du groupement de postes

Configurez les paramètres du groupement de postes pour chaque service Basic ACD. Le groupement de postes créé pour la fonction Basic ACD est local.

Paramètre	Description
Type de groupement	Définit l'ordre dans lequel les appels sont répartis vers les membres du groupement de postes Basic ACD. Faites un choix parmi les types suivants : ▪ **séquentiel**. Les appels sont routés vers les membres du groupement de postes Basic ACD dans l'ordre indiqué dans la fenêtre Membres. ▪ **poste**. Les appels sont envoyés vers les membres du groupement de postes Basic ACD sur une base périodique. ▪ **plus longtemps disponible**. Les appels sont envoyés vers le membre du groupement de postes Basic ACD disponible depuis le plus longtemps.
Membres	Cliquez sur **Membres** pour afficher une fenêtre permettant de sélectionner les téléphones et les utilisateurs qui y sont associés comme membres du groupement de postes Basic ACD. Voir la rubrique **Membres du groupement de postes, page 447**.
Délai d'expiration du groupement	Nombre de secondes avant le renvoi d'un appel resté sans réponse et destiné à un membre du groupement de postes vers le membre suivant selon les critères définis pour l'option Type de groupement. La valeur par défaut est 8 secondes.
Activer la déconnexion automatique	Lorsque cette option est activée, la déconnexion automatique est active. Lorsque la valeur **Tentatives avant la déconnexion** est dépassée, le téléphone de l'agent est automatiquement déconnecté du groupement de postes Basic ACD.

Paramètre	Description
Message à afficher lorsque tous les agents sont déconnectés	Message à afficher lorsque tous les agents (membres du groupement de postes) sont déconnectés. La valeur par défaut est Tous les agents sont déconnectés. Le message peut contenir jusqu'à 39 caractères.
Tentatives avant la déconnexion	Nombre maximum d'appels restés sans réponse pour le membre du groupement de postes B-ACD (de 1 à 20) avant la déconnexion automatique. La valeur par défaut est 3.

Invites

Pour gérer les invites Basic ACD, configurez les paramètres ci-dessous. Lorsque vous avez terminé, cliquez sur **OK** ou sur **Appliquer**.

Paramètre	Description
Message d'accueil	Sélectionnez une des invites Basic ACD par défaut dans la liste ou cliquez sur **Enregistrer** pour enregistrer une invite personnalisée à l'aide du magnétophone intégré.
Invite Transférer vers Basic ACD	Sélectionnez une des invites Basic ACD par défaut dans la liste ou cliquez sur **Enregistrer** pour enregistrer une invite personnalisée à l'aide du magnétophone intégré.

Membres du groupement de postes

La fenêtre s'affiche lorsque vous cliquez sur le bouton **Membres** de la fenêtre Créer/modifier les paramètres Basic ACD.

Suivez les étapes suivantes pour créer ou modifier la liste des membres du groupement de postes et leur téléphone :

ETAPE 1 Cliquez sur un utilisateur dans la liste Disponible ou Sélectionné. Maintenez les touches CTRL ou MAJ pour sélectionner plusieurs utilisateurs dans chaque liste.

ETAPE 2 Utilisez les boutons **Ajouter**, **Supprimer**, **Sélectionner tout** pour déplacer les utilisateurs sélectionnés de la liste Disponible vers la liste Sélectionné.

ETAPE 3 Utilisez les flèches **Haut** et **Bas** pour réorganiser les membres du groupement de postes.

ETAPE 4 Cliquez sur **OK** pour enregistrer les modifications.

Paramètres des rapports du groupement de postes

Les fonctions de base Basic ACD exploitent le système de création de rapport CME B-ACD pour créer des rapports simples au format CSV exploitables sous un tableur.

Pour activer la fonction de rapport Basic ACD et configurer les paramètres du groupement de postes, complétez les champs de la rubrique Paramètres des rapports du groupement de postes selon les instructions ci-dessous.

Lorsque vous avez terminé de configurer les paramètres des rapports pour le groupement de postes, cliquez sur **OK** ou sur **Appliquer**.

Paramètre	Description
Activer le rapport CME	Lorsque cette option est cochée, la création de rapports de groupement de postes Basic ACD est possible. Cette fonction est désactivée par défaut.
Emplacement du rapport CME	Emplacement du serveur TFTP ou FTP et répertoire des rapports Basic ACD. Le format est le suivant :**tftp://** *<Adresse IP serveur>/<dossier>/<nom de fichier>* ou **ftp:**//*<Adresse IP serveur>/<dossier>/<nom de fichier>*. Par exemple : **tftp://192.168.10.1/bacdrpts/mybacd**
Nombre de rapports	Nombre de rapports au format CSV qui seront créés. Vous pouvez entrer des valeurs comprises entre 1 et 200.
Fréquence des rapports (heures)	Fréquence de production des rapports, en heures. Vous pouvez entrer des valeurs comprises entre 1 et 84.
Chargement manuel des rapports	Lorsque la création de rapports CME est active, cliquez sur *Chargement manuel des rapports* pour activer immédiatement l'envoi des données vers l'emplacement défini sur le serveur TFTP. Cette option n'est pas disponible lorsque la fonction de création de rapport CME est désactivée.

Service de nuit

Pour configurer le Service de nuit, sélectionnez **Configurer** > **Téléphonie** > **Gestion des appels**> **Service de nuit** dans la barre de fonctions.

Avant d'activer le Service de nuit, vous devez définir un programme spécifique sous l'onglet Service de nuit de la fenêtre Programmes (**Configurer** > **Téléphonie** > **Gestion des appels** > **Programmes**). Voir la rubrique **Programme du service de nuit, page 431**.

Vue d'ensemble

Vous pouvez définir jusqu'à quatre postes pour le service de nuit. Chaque poste peut être associé à un code de transfert d'appel ou à une sonnerie de nuit.

En présence d'un code de transfert d'appel pour un poste de nuit, les appels entrants vers ce poste sont transférés vers le numéro indiqué pour le service de nuit.

La sonnerie de nuit vous permet d'assurer la prise en charge des postes dépourvus d'opérateur au cours du service de nuit. Pendant le service de nuit, les appels entrants sont signalés sur les postes associés au service de nuit par le biais d'une sonnerie particulière. Les utilisateurs des téléphones du service de nuit peuvent décrocher pour répondre aux appels entrants.

Pour configurer les téléphones du service de nuit, au moins un poste doit être associé à la sonnerie de nuit.

L'utilisateur peut introduire un code de nuit pour activer ou désactiver le service sur un téléphone affecté au service de nuit. Le code permet l'activation ou la désactivation du service de nuit sur les téléphones équipés de cette fonction.

Les restrictions suivantes s'appliquent au service de nuit :

- Les téléphones analogiques ne reçoivent pas les notifications du service de nuit. Cependant, les numéros de poste pour les téléphones analogiques configurés avec un profil Téléphone d'utilisateur peuvent être configurés de manière à être surveillés pendant le service de nuit.
- Les téléphones IP dépourvus de touches logicielles peuvent être associés à des codes d'accès permettant de prendre les appels à partir du poste du service de nuit.

Procédures

Pour configurer un transfert d'appel sur un poste pour le service de nuit, procédez comme suit :

ETAPE 1 Dans le champ **Numéro de poste**, sélectionnez un numéro disponible dans la liste.

ETAPE 2 Dans le champ **Type de réponse**, sélectionnez l'option **transfert appel service nuit**.

ETAPE 3 Entrez un numéro dans le champ **Transférer à numéro**.

Les appels entrants vers ce numéro pendant le service de nuit seront transférés vers le numéro indiqué.

Il peut s'agir d'un numéro SDA externe ou d'un numéro de poste. Lorsque vous introduisez un numéro SDA externe, introduisez le numéro tel que vous le composeriez, sans oublier le code d'accès.

ETAPE 4 Répétez les étapes 1 à 3 pour associer un transfert d'appel vers d'autres postes pour le service de nuit.

ETAPE 5 Cliquez sur **OK** ou **Appliquer**.

Pour activer la sonnerie de nuit pendant le Service de nuit, procédez comme suit :

ETAPE 1 Dans le champ **Numéro de poste**, sélectionnez un numéro disponible dans la liste.

ETAPE 2 Dans le champ **Type de réponse**, sélectionnez l'option **sonnerie de nuit**.

ETAPE 3 Cliquez sur le bouton **Téléphones du service de nuit** pour afficher la fenêtre contenant les téléphones sélectionnés.

ETAPE 4 Sélectionnez les téléphones dans la liste.

ETAPE 5 Cliquez sur **Ajouter**.

ETAPE 6 Cliquez sur **OK** ou **Appliquer**.

Pour configurer le code du service de nuit, procédez comme suit :

ETAPE 1 Dans le champ **Code du service de nuit**, entrez le code permettant de passer au service de nuit.

Vous pouvez introduire jusqu'à 15 chiffres. CCA ajoute automatiquement un astérisque (*) comme préfixe.

Lorsque vous sélectionnez un code pour basculer en Service de nuit, sachez que plusieurs codes d'activation par défaut (utilisés essentiellement pour les lignes analogiques) sont envoyés à l'UC500 par CCA. Pour éviter le chevauchement de ces codes d'activation, le code du Service de nuit devrait commencer par *2, *7, *8 ou *9.

ETAPE 2 Cliquez sur **OK** ou **Appliquer**.

Pour supprimer un poste du service de nuit, entrez dans le champ **Numéro de poste** la valeur **Aucun** et validez les modifications. Vous pouvez aussi sélectionner un numéro de poste distinct et modifier les autres paramètres.

Pour modifier la liste des téléphones accessibles pour le service de nuit, cliquez sur **Téléphones du service de nuit** et utilisez les boutons **Ajouter**, **Supprimer** et **Sélectionner tout** pour modifier la liste Téléphones sélectionnés. Appliquez ensuite les modifications.

Pour de plus amples informations, consultez les rubriques suivantes :

- **Téléphones du service de nuit, page 451**
- **Programme du service de nuit, page 431**

Téléphones du service de nuit

Cette fenêtre s'affiche lorsque vous cliquez sur **Téléphones du service de nuit** dans la fenêtre Service de nuit.

Sélectionnez les téléphones dans la liste **Disponible** et utilisez les boutons **Ajouter**, **Supprimer** et **Sélectionner tout** pour déplacer les éléments de la liste Disponible à la liste Téléphones sélectionnés.

Les téléphones sélectionnés sont activés pour le service de nuit. Les appels entrants y seront donc signalés pendant le service de nuit. Les utilisateurs des téléphones du service de nuit peuvent alors appuyer sur le bouton **GPickUP** de leur téléphone pour répondre aux appels entrants.

Lorsque vous avez terminé la sélection des téléphones, cliquez sur **OK**.

Pour de plus amples informations, consultez les rubriques suivantes :

- **Service de nuit, page 449**
- **Programme du service de nuit, page 431**

Enregistrer en direct

Cette fenêtre s'affiche lorsque vous sélectionnez **Configurer** > **Téléphonie** > **Gestion des appels> Enregistrer en direct** dans la barre de fonctions.

Vue d'ensemble

Le module Enregistrer en direct permet aux utilisateurs d'enregistrer les conversations et de les conserver sous forme de messages dans leur messagerie. Ils pourront ensuite l'écouter ou le transférer à une autre messagerie vocale. Par défaut, cette fonction est désactivée.

Les utilisateurs du téléphone peuvent lancer une session Enregistrer en direct en appuyant sur la touche **LiveRcd** de leur téléphone IP pendant l'appel. Le système établit alors une téléconférence entre le numéro de pilote de la fonction Enregistrer en direct configuré et l'interlocuteur enregistré.

Des tonalités se font entendre périodiquement afin de signaler que l'appel est enregistré. Vous pouvez activer ou désactiver ces tonalités. Vous pouvez aussi définir la durée et l'intervalle.

Les remarques générales suivantes s'appliquent à la fonction Enregistrer en direct :

- Les appelants externes ne peuvent pas utiliser cette fonction car elle nécessite le numéro de poste de l'appelant.
- Les messages de la fonction Enregistrer en direct ne donnent lieu à aucune notification lorsqu'ils sont transmis vers la messagerie.
- La durée des messages enregistrés en direct se limite à l'espace libre de la messagerie vocale de l'abonné.

Procédures

Pour activer et configurer la fonction d'enregistrement en direct, procédez comme suit :

ETAPE 1 Configurez les **paramètres de l'enregistrement en direct** :

a. Cochez la case **Activer l'enregistrement en direct** pour activer cette fonction.

b. Dans le champ Numéro pilote, entrez le numéro de poste pilote pour l'enregistrement en direct.

   Ce numéro de poste est utilisé pour transférer tous les appels entrants vers le numéro pilote de la messagerie vocale. Tous les appels envoyés vers le numéro pilote de la messagerie vocale à partir de ce numéro contourneront le message d'accueil de la messagerie. Si l'appelant dispose d'une messagerie, l'enregistrement démarre immédiatement.

ETAPE 2 Configurez les **paramètres de tonalité pour l'enregistrement en direct** :

a. L'option **Durée du bip** définit la durée du bip en millisecondes. Cette valeur peut être comprise entre 50 et 1000 millisecondes. La valeur par défaut est 250 secondes.

b. L'option **Intervalle de bip** définit la durée en secondes entre la fin d'un bip et le début du suivant. Cette valeur peut être comprise entre 1 et 30 secondes. La valeur par défaut est 15 secondes.

ETAPE 3 Cliquez sur **OK** ou **Appliquer**.

T.37 Fax vers e-mail

Pour configurer la fonction T.37 Fax vers e-mail, sélectionnez l'option **Configurer** > **Téléphonie** > **Gestion des appels** > **T.37 Fax vers e-mail** dans la barre de fonctions.

Pour en savoir plus sur les fonctions et les paramètres de configuration T.37 Fax vers e-mail, consultez les rubriques suivantes :

- **Vue d'ensemble**
- **Restrictions**
- **Prérequis pour la configuration de la fonction T.37 Fax**
- **Activer la fonction T.37 Fax vers e-mail et configurer les services**
- **Configuration des boîtes de réception pour les fax entrants**

Vue d'ensemble

T.37 est une norme ITU utilisée pour l'envoi des télécopies par e-mail. La fonction T.37 Fax vers e-mail de CCA permet à l'UC500 de faire office de passerelle lors des échanges avec les télécopieurs standard. Elle convertit les télécopies en messages électroniques et inversement. Chez Cisco, cette fonction s'appelle aussi T.37 Enregistrement et transfert de fax.

La fonction T.37 Fax vers e-mail de CCA vous permet de configurer l'UC500 et la messagerie pour profiter des fonctions suivantes :

- **Services de fax entrants** à l'aide de l'application On Ramp.

  Grâce à CCA, vous pourrez configurer les messageries qui recevront les fax entrants. Les fax enregistrés pourront être transférés sous forme d'annexes ou envoyés vers une imprimante. Les télécopies sont converties en fichiers images au format TIFF. Vous pouvez configurer les messageries pour une prise en charge des télécopies uniquement (tous les appels entrants seront considérés comme des télécopies) ou pour la voix et les fax (les appels entrants peuvent être des appels vocaux ou des fax).

  CCA configure les messageries vocales pour les utilisateurs, les groupes et les postes flottants (poste non associé à un téléphone ou à un groupe). Toutes les messageries vocales, dont celles associées à des postes flottants peuvent recevoir et stocker les télécopies à condition d'être associées à un numéro de téléphone entrant sur un trunk PSTN.

- **Détection des appels vocaux et des télécopies** à l'aide de l'application de détection des appels vocaux et des télécopies.

  La détection des appels vocaux et des télécopies permet d'établir si un appel entrant est en fait un appel vocal ou un fax. Cela vous permet d'utiliser un même numéro d'appel entrant pour les appels vocaux et les télécopies.

- **Impression de fax** à l'aide de l'application Off Ramp. Cette fonction permet aux utilisateurs d'utiliser l'Interface utilisateur de la téléphonie (TUI) pour transférer les fax conservés dans la messagerie vocale vers un télécopieur local en vue de leur impression.

- **Recevoir les fax sous forme d'e-mails**. Grâce à CCA, vous pouvez associer les services T.37 Fax vers e-mail à un service de notification par la messagerie vocale ou IMAP de sorte que les utilisateurs soient avertis de l'arrivée d'une télécopie par téléphone ou par e-mail. Le fax pourra par ailleurs être annexé à l'e-mail.

- **Enregistrer des invites personnalisées ou utiliser les invites par défaut pour les appels entrants vers les lignes paramétrées pour la réception des appels vocaux et des fax.** Vous pouvez utiliser les invites par défaut pour les appels entrants vers les lignes assurant la détection des appels vocaux et des télécopies. Vous pouvez aussi définir des invites personnalisées. Les invites par défaut sont disponibles en anglais, espagnol et chinois.

CCA comprend les applications de serveur vocal interactif (SVI) pour les télécopies, la détection de télécopie et l'impression de télécopies. Ces applications se présentent sous la forme de scripts TCL (Tool Command Language) et sont chargées dans la mémoire flash de l'UC500 lors de l'application de la configuration T.37 Fax vers e-mail. Les invites présentées par défaut aux utilisateurs pour les appels entrants vers les lignes paramétrées pour une détection des appels vocaux et des télécopies sont chargées sur la mémoire flash lorsque vous appliquez la configuration.

Les scripts TCL et les invites par défaut se trouvent dans le dossier `flash:applications/faxmail` de la mémoire flash de l'UC500. Les invites personnalisées se trouvent dans le dossier `flash:applications/faxmail/custom` de la mémoire flash.

Restrictions

Les restrictions suivantes concernent la configuration de la fonction T.37 Fax vers e-mail sous CCA :

- Seules les boîtes de réception associées aux numéros de téléphone entrants sur les trunks PSTN peuvent recevoir des fax entrants. Les trunks SIP ne sont pas pris en charge.
- La détection des appels vocaux et des fax ne fonctionne pas avec tous les télécopieurs ni avec tous les modes de fonctionnement. Il est possible que des tonalités ne soient pas correctement détectées en présence de télécopieurs en mode manuel.
- L'utilisation simultanée d'une fonction T.37 Détection de télécopies et d'une fonction SNR n'est pas possible.
- Les téléphones dépourvus de l'interface TUI (Telephony User Interface) ne peuvent pas être utilisés pour le transfert des télécopies vers un télécopieur local en vue de les imprimer.

Prérequis pour la configuration de la fonction T.37 Fax

Avant d'activer et de configurer la fonction T.37 Fax, les réglages suivants doivent être effectués :

- Configurez les utilisateurs, les postes et les messageries vocales sur le système.

  Pour ce faire, utilisez l'option **Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Utilisateurs et téléphones** et sélectionnez l'onglet Postes utilisateurs ou Postes flottants. Les messageries vocales pour les groupements de postes et les groupes d'appel sont créées lorsque l'option Transfert si pas de réponse vers est associée à la valeur Messagerie dans la fenêtre Groupes de téléphone (**Configurer** > **Téléphonie** > **Groupes de téléphones**).
- Seules les messageries vocales associées aux numéros de téléphone entrants sur les trunks PSTN peuvent recevoir des fax entrants. Vous devez créer un plan de numérotation en entrée pour chaque poste doté d'une messagerie vocale configuré pour recevoir les fax entrants.

  Pour ce faire, allez dans **Configurer** > **Téléphonie** > **Plan de numérotation** > **Entrant**. En ce qui concerne le type de destination pour les options Appels entrants FXO ou Appel direct vers le standard automatique, les groupes ou l'opérateur, sélectionnez OPERATOR (Opérateur) ou HUNT_GROUP (Groupement de postes).
- Si vous souhaitez activer la fonction d'impression de fax, un télécopieur doit être relié au port FXS de l'UC500 et ce port doit être associé à un profil FAX.

Pour ce faire, allez dans **Configurer** > **Téléphonie** > **Ports et trunks** > **Ports FXS**.

- Pour intégrer les notifications par la messagerie vocale à l'option T.37 Fax vers e-mail de sorte que les utilisateurs reçoivent un message avec le fax en annexe, allez dans **Configurer** > **Téléphonie** > **Utilisateurs et téléphones** > **Messagerie vocale** et configurez les notifications pour les messageries pouvant recevoir les fax entrants.

  Pour plus d'informations sur la marche à suivre, consultez la rubrique **Notifications, page 385**.

  REMARQUE : Pour recevoir un avis par e-mail ou par téléphone de l'arrivée d'un fax, la valeur Tous les messages doit être définie pour l'option Niveau de notification.

- Vous pouvez aussi activer la messagerie unifiée de CCA pour associer les fonctions T.37 Fax vers e-mail et IMAP. Pour activer la messagerie unifiée, allez dans **Applications** > **Smart Applications** > **Smart Applications Manager**. Voir la rubrique **Messagerie unifiée (IMAP), page 525**.

Activer la fonction T.37 Fax vers e-mail et configurer les services

Dans l'onglet Services, vous pouvez effectuer les opérations suivantes :

- Activer la fonction T.37 Fax vers e-mail
- Configurer les paramètres d'invite pour la détection des appels vocaux et des télécopies
- Définir l'imprimante par défaut pour l'impression des fax

Pour activer et configurer les paramètres de la fonction T.37 Fax vers e-mail, suivez les consignes suivantes :

ETAPE 1 Dans le menu déroulant Nom de l'hôte, sélectionnez l'UC500.

ETAPE 2 Cochez la case **Activer Fax vers e-mail**.

ETAPE 3 Complétez les champs de l'onglet Services, selon les indications du tableau suivant.

Paramètres	Description
Fax entrant uniquement	La rubrique "Fax entrant uniquement" affiche la version de l'application "Application fax uniquement (On Ramp)". Si la fonction T.37 Fax vers e-mail n'a pas été définie pour le système, le message "Installation en attente (version 2.0.1.3)" s'affiche. L'application On Ramp sera chargée et installée sur l'UC500 lorsque vous appliquez la configuration.
Appels et fax entrants	La détection des appels vocaux et des télécopies permet d'établir si un appel entrant est en fait un appel vocal ou un fax. Cela vous permet d'utiliser un même numéro d'appel entrant pour les appels vocaux et les télécopies. CCA configure la détection de télécopie de telle sorte que l'appel ne doit pas être connecté. En présence d'une tonalité de fax, il est pris en charge comme une télécopie. Si aucune tonalité de fax n'est détectée, il est considéré comme un appel vocal normal. La version de l'application de détection des appels vocaux et des fax installée s'affiche ici. Si la fonction T.37 Fax vers e-mail n'a pas été définie pour le système, le message "Installation en attente" et la version de l'application s'affichent. L'application de détection des appels vocaux et des fax sera chargée et installée sur l'UC500 lorsque vous appliquez la configuration.

Paramètres	Description
Appels et fax entrants (suite)	**Invite pour les appels entrants** La procédure de détection peut différer les appels jusqu'à 9 secondes. Les invites système par défaut sont prévues pour alerter les appelants et leur permettre d'éviter tout retard. Ils pourront ainsi être mis en communication directement ou envoyer un fax. Vous pouvez aussi enregistrer une invite personnalisée pour cela (par exemple, si l'invite doit être lue en plusieurs langues). L'invite système par défaut est "To send a fax, press the START key on your fax machine now. For voice calls, press any key or stay on the line." (Pour envoyer un fax, appuyez sur la touche DEMARRER de votre télécopieur maintenant. Pour les appels vocaux, appuyez sur n'importe quelle touche ou restez en ligne). Faites un choix parmi les options suivantes : ▪ **Personnalisé**. Permet d'enregistrer une invite personnalisée pour les appels entrants. Si cette option est sélectionnée, cliquez sur **Ajouter un fichier** pour enregistrer et charger une invite personnalisée. ▪ **Système (chinois)**. Permet d'utiliser les invites système par défaut en chinois. ▪ **Système (anglais)**. Permet d'utiliser les invites système par défaut en anglais. Il s'agit de la valeur par défaut. ▪ **Système (espagnol)**. Permet d'utiliser les invites système par défaut en espagnol. ▪ **Aucun**. Choisissez cette option si vous n'utilisez pas la détection des appels vocaux ou des fax (les messageries recevant les fax entrants présentent le paramètre "Fax uniquement"). Le serveur TFTP intégré à CCA est utilisé pour le chargement et le téléchargement des invites système. Vérifiez si les paramètres du pare-feu de votre PC autorisent le trafic TFTP au départ et à destination de l'UC500 et s'il n'y a pas de serveurs TFTP tiers sur votre PC. Pour plus d'informations sur l'enregistrement des invites avec l'enregistreur d'invites de CCA, consultez la rubrique **Magnétophone, page 440**.

Paramètres	Description
Impression de fax	**Fichier d'invite personnalisé (facultatif)** Affiche le nom de fichier de l'invite enregistrée pour les appels entrants. Ce menu ne s'affiche que si une invite personnalisée a été enregistrée.
	Les fax peuvent être imprimés sur n'importe quel numéro appelable ou sur l'imprimante fax par défaut. Si vous souhaitez activer la fonction d'impression de fax, un télécopieur doit être relié au port FXS de l'UC500 et ce port doit être associé à un profil FAX. Pour ce faire, allez dans **Configurer** > **Téléphonie** > **Ports et trunks** > **Ports FXS**. Seuls les ports FXS associés à un profil Fax peuvent être sélectionnés. La version de l'application d'impression de fax Off Ramp installée s'affiche aussi. Si la fonction T.37 Fax vers e-mail n'a pas été définie pour le système, le message "Installation en attente (version 2.0.1.1)" s'affiche. L'application d'impression de fax Off Ramp sera chargée et installée sur l'UC500 lorsque vous appliquez la configuration.
	Imprimante fax par défaut Configuration d'une imprimante de fax par défaut : 1. Définissez l'imprimante à utiliser par défaut. 2. Cliquez sur **OK** ou **Appliquer**.

Configuration des boîtes de réception pour les fax entrants

Les fax entrants peuvent être stockés et transférés vers les messageries. Toutes les messageries peuvent recevoir des fax à condition qu'elles disposent d'un plan de numérotation en entrée. La même messagerie est utilisée pour le stockage des fax et des messages vocaux.

Vous pouvez désactiver le fax sans porter atteinte aux messages existants de la messagerie. Lorsque la fonction de télécopie est désactivée pour une messagerie, le système rejette les fax en provenance d'un télécopieur.

Les messageries assurant un transfert vers les boîtes e-mail peuvent recevoir les fax sous forme d'e-mails. Pour configurer ce type de transfert, allez dans le menu **Téléphonie** > **Utilisateurs et postes** > **Messagerie** et sélectionnez l'onglet Notifications pour activer la notification par e-mail.

REMARQUE : La messagerie unifiée peut aussi être utilisée pour recevoir les fax sous forme d'e-mail. Pour activer la messagerie unifiée, allez dans **Applications** > **Smart Applications** > **Smart Applications Manager**.

Ajoutez les messageries pour recevoir les fax entrants

Seules les messageries associées à des numéros entrants sur les trunks PSTN peuvent être ajoutées. Pour configurer les numéros entrants, allez dans la rubrique **Téléphonie** > **Plan de numérotation** > **Entrant**.

Suivez les étapes suivantes pour ajouter les messageries qui réceptionneront les fax entrants :

ETAPE 1 Cliquez sur l'onglet **Ajouter** sous l'onglet Boîtes de réception de la fenêtre T.37 Fax vers e-mail. La fenêtre "Ajouter les messageries pour recevoir les fax entrants" s'affiche.

ETAPE 2 Dans la fenêtre "Ajouter les messageries pour recevoir les fax entrants", cliquez sur **Ajouter**, **Supprimer** et **Sélectionner tout** pour déplacer les utilisateurs entre les listes Messageries disponibles et Messageries sélectionnées.

ETAPE 3 Cliquez sur **OK** pour revenir à la fenêtre T.37 Fax vers e-mail.

Supprimer des messageries de la liste

Suivez les étapes suivantes pour supprimer les messageries qui réceptionneront les fax entrants :

ETAPE 1 Sélectionnez la messagerie souhaitée sous l'onglet Boîtes de réception.

ETAPE 2 Cliquez sur **Supprimer**.

ETAPE 3 Cliquez sur **OK** ou **Appliquer**.

14

Plan de numérotation

Cette partie concerne la configuration des plans de numérotation entrant et sortant. Elle se compose des rubriques suivantes :

- **Plan de numérotation entrant**
- **Plan de numérotation sortant**
- **Groupes de trunks PSTN**
- **Modèles du plan de numérotation**

Plan de numérotation entrant

Pour configurer le plan de numérotation en entrée, sélectionnez **Configurer** > **Téléphonie** > **Plan de numérotation** > **Entrant** dans la barre de fonctions.

Avant de commencer

Avant de configurer les paramètres du plan de numérotation pour la numérotation directe et les appels entrants FXO, vérifiez si les réglages de la fenêtre Trunks PSTN ont été définis pour les trunks BRI, PRI et FXO (**Configurer** > **Téléphonie** > **Ports et trunks** > **Trunks PSTN**). En présence de trunks SIP, veillez à les configurer (**Configurer** > **Téléphonie** > **Ports et trunks** > **Trunks SIP**). Le Standard automatique, les groupements de postes et les groupes d'appel doivent eux aussi être configurés afin qu'ils soient accessibles pour les appels entrants FXO et les numéros DID.

La fenêtre Plan de numérotation en entrée présente les onglets suivants :

- **Appels entrants FXO**
- **Numérotation directe**

Appels entrants FXO

Sous l'onglet Appels entrants FXO, vous pouvez sélectionner la cible des appels entrants sur les ports FXO.

Pour définir la cible des appels entrants vers les ports FXO, sélectionnez le port FXO dans la liste, modifiez les paramètres en fonction des éléments ci-dessous et cliquez sur **OK** ou **Appliquer**.

Champ	Description
Description	Description du port FXO. Vous pouvez modifier la valeur par défaut, laquelle correspond au numéro de port FXO. Par exemple : 4 FXO-0/0/1.
Trunk	Champ en lecture seule affichant le numéro de port FXO. Par exemple : 4 FXO-0/0/1.
Type de destination	Cible des appels entrants vers ce trunk FXO. Faites un choix parmi les options suivantes : ▪ CO_LINE (ligne de trunk SDA directe pour le siège central) ▪ OPERATOR ▪ AUTO_ATTENDANT ▪ BLAST_GROUP ▪ HUNT_GROUP ▪ B_ACD (numéro de poste pour le service Basic ACD)

Champ	Description
Destination	Si vous sélectionnez l'option AUTO_ATTENDANT, HUNT_GROUP, BLAST_GROUP ou B_ACD comme type de poste, sélectionnez le numéro de poste ou le groupe correspondant dans la liste parmi ceux configurés sur votre système. Si vous sélectionnez l'option Operator comme type de poste, introduisez le numéro de poste à utiliser par l'opérateur pour le site. Si vous sélectionnez l'option CO_LINE, une description en lecture seule s'affiche. Par exemple : Direct Trunk Line - CO1.

Numérotation directe

Sous l'onglet Numérotation directe, définissez les règles de transposition pour l'association des numéros SDA entrants aux postes internes. Deux types de transpositions peuvent être définis :

- **Appel direct vers les postes utilisateurs internes.** Configurez les numéros d'appel entrant direct (DID) afin qu'ils soient signalés sur les postes internes. Réalisez ainsi des associations individuelles entre un numéro d'appel entrant direct et un poste interne. Voir la rubrique **Appel direct vers les postes utilisateurs internes, page 465**.
- **Appel direct vers le standard automatique, les groupes ou l'opérateur.** Configurez un numéro DID ou une plage de numéros DID afin qu'ils soient signalés par un groupement de postes, un groupe d'appel, un service Basic ACD, un Standard automatique ou le poste de l'opérateur. Voir la rubrique **Appel direct vers le standard automatique, les groupes ou l'opérateur, page 468**.

IMPORTANT Pour les trunks SIP, les associations DID relatives au standard automatique et aux numéros de la messagerie vocale doivent être configurées à l'aide des paramètres des fenêtres Standard automatique et Messagerie et non à l'aide des paramètres DID de la fenêtre Plan de numérotation en entrée.

Appel direct vers les postes utilisateurs internes

Cette fenêtre s'affiche lorsque vous cliquez sur **Ajouter** dans la zone Appel direct vers les postes utilisateurs internes de la fenêtre Plan de numérotation en entrée.

Vue d'ensemble

Cette fenêtre vous permet de faire en sorte que les numéros DID (appel entrant direct) soient signalés sur les postes utilisateurs internes. Pour ce faire, des règles de conversion doivent être établies afin de définir le lien entre chaque numéro DID et le numéro de poste correspondant. Chaque numéro DID est associé à un numéro de poste interne.

Le numéro DID fourni par votre opérateur peut se composer d'un nombre variable de chiffres. Contactez votre opérateur pour connaître les DID affectés à votre installation.

Le nombre maximum de règles de conversion DID est fixé à 15. Toutefois, une seule règle de conversion peut être utilisée pour associer une plage de numéros DID à des postes internes (v. exemple).

Paramètres de conversion DID	
Paramètre	**Valeur**
Début de plage DID	9725551000
Fin de plage DID	9725551005
Début de numéro interne	200
Fin de numéro interne	205
Résultat de la configuration	
Appels entrants vers ce numéro DID	**Appel signalé sur le poste**
972-555-1000	Poste 200
972-555-1001	Poste 201
972-555-1002	Poste 202
972-555-1003	Poste 203
972-555-1004	Poste 204

Procédures

Pour définir une règle de conversion pour un appel direct vers les postes utilisateurs internes, cliquez sur **Ajouter**, complétez les champs de la fenêtre Appel direct vers les postes utilisateurs internes selon les consignes ci-dessous et cliquez sur **OK** ou **Appliquer**.

Champ	Description
Description	Description de l'association du poste DID.
Trunks	Sélectionnez le type de trunk numérique dans la liste correspondant à l'opérateur fournissant les numéros DID. Par exemple, Trunk SIP, Trunk BRI ou Trunk PRI.

Champ	Description
Numéros d'appel entrant direct	Numéros SDA à associer aux postes internes. ▪ Pour n'associer qu'un seul numéro, entrez le même numéro dans le champ **Début de plage DID** et **Fin de plage DID**. ▪ Pour associer une plage de numéros, entrez les numéros de début et de fin de la plage. ▪ Le numéro DID peut commencer par un caractère "+".
Numéros internes	Numéros de poste internes à associer aux numéros DID. ▪ Pour n'associer qu'un seul numéro, entrez le même numéro dans le champ **Début de numéro interne** et **Fin de numéro interne**. ▪ Pour associer une plage de numéros, entrez les numéros de début et de fin de la plage. ▪ Le nombre de postes internes définis par la plage doit correspondre aux numéros DID définis dans la plage correspondante.

Appel direct vers le standard automatique, les groupes ou l'opérateur

Cette fenêtre s'affiche lorsque vous cliquez sur **Ajouter** dans la zone Appel direct vers le standard automatique, les groupes ou l'opérateur de la fenêtre Plan de numérotation en entrée.

Elle vous permet de créer les conversions DID permettant d'associer au moins un numéro SDA en entrée à un Standard automatique, un groupement de postes, un groupe d'appel, un service Basic ACD ou un opérateur.

Pour configurer la numérotation directe d'au moins un numéro SDA vers un groupement de postes, un groupe d'appel, un service Basic ACD, un opérateur ou le Standard automatique, cliquez sur **Ajouter**, complétez les champs de la fenêtre **Appel direct vers le standard automatique, les groupes ou l'opérateur** selon les indications ci-dessous et cliquez sur **OK** ou **Appliquer**.

Champ	Description
Description	Description de l'association du poste DID.
Trunks	Sélectionnez le type de trunk vocal dans la liste correspondant à l'opérateur fournissant les numéros DID. Par exemple, Trunk SIP, Trunk BRI ou Trunk PRI.
Numéros d'appel entrant direct	Numéros SDA à associer aux postes internes. ▪ Pour n'associer qu'un seul numéro, entrez le même numéro dans le champ **Début de plage DID** et **Fin de plage DID**. ▪ Pour associer une plage de numéros, entrez les numéros de début et de fin de la plage. ▪ Le numéro DID peut commencer par un caractère "+".
Type de destination	Faites un choix parmi les options suivantes : Si un type de cible ne figure pas dans la liste, c'est qu'aucun poste de ce type n'a été défini sur le système. ▪ OPERATOR ▪ AUTO_ATTENDANT ▪ BLAST_GROUP ▪ HUNT_GROUP ▪ B_ACD (numéro de poste pour le service Basic ACD)
Destination	Si vous sélectionnez l'option AUTO_ATTENDANT, HUNT_GROUP, BLAST_GROUP ou B_ACD comme type de poste, sélectionnez le numéro de poste ou le groupe correspondant dans la liste parmi ceux configurés sur votre système. Si vous sélectionnez l'option Operator comme type de poste, introduisez le numéro de poste à utiliser par l'opérateur pour le site.

Plan de numérotation sortant

Cette fenêtre s'affiche lorsque vous sélectionnez **Configurer** > **Téléphonie** > **Plan de numérotation** > **Sortant** dans la barre de fonctions.

REMARQUE L'accès Telnet doit être activé pour pouvoir configurer les fonctions du plan de numérotation.

La fenêtre Plan de numérotation sortant présente les onglets suivants :

- **Gestion des appels sortants**
- **Groupes de trunks PSTN**
- **Identifiant de l'appelant**

Gestion des appels sortants

Sous l'onglet Gestion des appels sortants, vous pouvez effectuer les opérations suivantes :

- **Sélectionnez les paramètres locaux du modèle de numérotation**
- **Définir le Code d'accès par défaut et le Délai d'expiration de la saisie.**
- **Configurer les numéros sortants**
- **Ajouter ou modifier un numéro sortant**

Sélectionnez les paramètres locaux du modèle de numérotation

Dans le menu Paramètres locaux du modèle de numérotation, sélectionnez l'une des options suivantes :

- Un modèle de numérotation pour des paramètres locaux spécifiques. Par exemple : Modèle : Australie ou Modèle : Amérique du Nord.

  Les régions suivantes disposent de modèles intégrés : Argentine, Australie, Autriche, Belgique, Brésil, Chili, Chine, Colombie, France, Allemagne, Indonésie, Irlande, Italie, Japon, Malaisie, Mexique, Pays-Bas (6 ou 7 chiffres), Nouvelle-Zélande, Amérique du Nord (7 et 10 chiffres), Norvège, Philippines, Singapour, Slovénie, Espagne, Suisse, R-U, Taïwan, Thaïlande et Venezuela.

  Pour l'Amérique du Nord, des modèles de plan de numérotation à 7 et 10 chiffres sont fournis afin que vous ne deviez pas modifier manuellement le plan de numérotation pour les numéros locaux. Un modèle à 6 et 7 chiffres a également été prévu pour les Pays-Bas.

- Définir de nouveaux paramètres locaux (crée un nouveau modèle de numérotation vierge).
- Modèle personnalisé basé sur l'un des modèles par défaut modifié ou modèle personnalisé importé.

Lorsque vous sélectionnez les paramètres locaux du modèle de numérotation, l'onglet est mis à jour et affiche les numéros sortants définis pour la zone sélectionnée. Si vous avez sélectionné **Définir nouveaux paramètres régionaux**, tous les numéros sortants sont vierges.

Une fois que vous avez ajouté ou modifié l'un des numéros sortants dans le modèle par défaut d'une zone, un nouveau plan de numérotation est défini afin de conserver l'intégrité du modèle original.

Lorsque vous appliquez pour la première fois un modèle de plan de numérotation sortant, si ce modèle contient des numéros bloqués, le système vous demande si vous souhaitez activer ou désactiver de manière générale le blocage d'appel sur tous les téléphones. Cette option globale ne s'affiche que pendant la configuration du plan de numérotation. Si vous ajoutez ou supprimez des numéros bloqués une fois le modèle appliqué, l'option d'activation/désactivation n'est pas disponible. Le blocage d'appel sur les téléphones ajoutés après l'application du modèle de plan de numérotation devra être défini manuellement sous l'onglet Postes utilisateurs de la fenêtre Voix.

Pour de plus amples informations, consultez la rubrique **Modèles du plan de numérotation, page 477**.

Définir le Code d'accès par défaut et le Délai d'expiration de la saisie.

Le code d'accès est un code à un chiffre que les utilisateurs doivent composer pour effectuer les appels externes. Dans le champ **Code d'accès**, entrez un seul chiffre compris entre 0 et 9 ou utilisez la valeur par défaut (9). Vous pourrez ainsi définir le code d'accès par défaut.

Si vous modifiez le code d'accès par défaut pour un plan de numérotation existant, Configuration Assistant affiche une fenêtre vous demandant si vous souhaitez que le code d'accès par défaut soit appliqué à tous les numéros sortants. Sélectionnez **Oui** pour mettre à jour tous les numéros sortants du plan de numérotation existant.

Dans le champ **Délai d'expiration de la saisie**, entrez l'attente en secondes (de 2 à 120) pour la saisie des données par l'utilisateur ou optez pour la valeur par défaut, à savoir 5.

Configurer les numéros sortants

ATTENTION Toute modification apportée à la configuration du plan de numérotation devra être testée au niveau des numéros sortants. Les erreurs éventuelles risquent d'empêcher les clients d'effectuer des appels.

Cisco vous conseille vivement d'utiliser un véritable téléphone IP pour tester le plan de numérotation sortant après l'application de la configuration. CCA vérifie la présence de conflits au niveau de l'UC500. Toutefois, il ne peut pas déceler les incompatibilités avec le fournisseur Telco.

Par exemple, en Amérique du Nord, certains fournisseurs Telco exigent que le préfixe d'accès au PSTN soit envoyé au Bureau central alors que d'autres exigent l'abandon du code d'accès.

Vous devrez sans doute **Ajouter ou modifier un numéro sortant** à/de votre plan de numérotation pour effectuer les opérations suivantes :

- **Modifier les autorisations pour certains types d'appel.**

  Empêcher certains utilisateurs de composer certains numéros (blocage d'appel).
  Le blocage d'appel permet de bloquer les appels vers certains numéros. Lorsqu'un utilisateur tente de passer un appel vers un numéro bloqué, une tonalité "Occupé" se fait entendre pendant environ 10 secondes. L'appel prend fin et la ligne redevient disponible. Le blocage d'appel peut être activé et désactivé sur n'importe quel type de téléphone à l'exception des téléphones SIP. Le blocage d'appel est contrôlé séparément en fonction des autorisations des utilisateurs. Il doit être activé par téléphone à partir de la fenêtre Options complémentaires de l'onglet Utilisateur de la fenêtre Voix. Pour de plus amples informations, consultez la rubrique **Exemple de blocage d'appel, page 476**.

  Les autorisations d'appel et les numéros interdits du plan de numérotation ne s'appliquent pas aux lignes de trunk du Bureau central. Les options **Bloquer les appels interdits** et **Autorisations** ne sont pas disponibles pour les lignes du Bureau central.

  L'Assistant de configuration de la téléphonie n'active pas le blocage d'appel de manière générale sur les téléphones utilisateurs lors de l'application du modèle du plan de numérotation. Au terme des opérations, vous devrez configurer manuellement le blocage d'appel pour chaque téléphone.

- **Autorisez les utilisateurs à effectuer des appels vers des numéros spécifiques au-delà des permissions standard qui leur sont affectées.** Par exemple, les utilisateurs pouvant composer les numéros de type National-plus doivent aussi pouvoir composer un numéro international afin d'atteindre le siège central de l'entreprise. Dans ce cas, vous pouvez ajouter un numéro sortant dans ce but et l'associer à la permission de type National-plus.
- **Modifiez la liste des trunks pour qu'elle achemine les appels vers le trunk adéquat par ordre de préférence.** Par exemple, si vous sélectionnez l'option PSTN uniquement pour la liste des trunks associée aux numéros locaux et local-plus, tous les appels de type local/local-plus ainsi que les appels d'urgence seront redirigés vers les trunks PSTN. Si vous sélectionnez SIP puis PSTN comme type de trunk pour les appels de type International et International-plus, ceux-ci seront d'abord routés vers les trunks SIP disponibles (puisqu'ils sont libres) et redirigés vers les trunks PSTN le cas échéant.

Ajouter ou modifier un numéro sortant

Pour ajouter un numéro sortant, cliquez sur **Ajouter numéro** pour insérer une nouvelle ligne dans le tableau. Configurez les paramètres en fonction du tableau suivant et cliquez ensuite sur **OK** ou **Appliquer**.

Champ	Description
Autorisations	Niveau d'autorisation pour le numéro sortant. Vous pouvez aussi définir les schémas pour le blocage d'appel. Chaque numéro sortant est associé à un niveau d'autorisation. Le niveau d'autorisation correspond aux paramètres **Autorisations** et **Bloquer les appels interdits** configurés pour chaque téléphone. Les niveaux d'autorisation sont cumulés (voir ci-dessous) : ▪ **Bloqué**. Numéro interdit. Lorsque la fonction **Bloquer les numéros interdits** est active pour un téléphone, les appels vers ces numéros sont impossibles. ▪ **Urgence**. Numéro sortant pour les appels d'urgence. Les numéros d'appel d'urgence sont inclus dans tous les niveaux d'autorisation. ▪ **Gratuit**. Numéros d'appel gratuits inclus à tous les niveaux d'autorisation. ▪ **Local**. Comprend les appels d'urgence, gratuits et locaux. ▪ **Local-plus**. Comprend les appels d'urgence, gratuits, locaux et de type Local-plus. ▪ **National** comprend les numéros de type Urgence, Gratuit, Local, Local-plus et National ▪ **National-plus**. Comprend les numéros de type Urgence, Gratuit, Local, Local-plus, National et National-plus. ▪ **International**. Comprend les numéros de type Urgence, Gratuit, Local, Local-plus, National, National-plus et International. ▪ **International-plus**. Comprend les numéros de type Urgence, Gratuit, Local, Local-plus, National, National-plus, International et International-plus. ▪ **Sans restriction**. Comprend tous les niveaux d'autorisation à l'exception des numéros bloqués.

Champ	Description
Description	Description de la règle relative aux numéros sortants. Pour les appels bloqués, la description est toujours "Numéro interdit". Elle s'affiche automatiquement.
Code d'accès	Code d'accès au numéro sortant (le cas échéant). Dans la plupart des cas, il s'agira du code d'accès par défaut défini pour les appels sortants. Vous pouvez aussi entrer un code d'accès différent pour un numéro sortant.
Commence par	Numéro ou modèle à respecter. ▪ Le modèle doit être unique. ▪ Les numéros et modèles sont mis en correspondance en commençant par le premier chiffre. ▪ Un numéro comprenant le modèle mais qui ne commence pas par lui n'est pas mis en correspondance. ▪ Lorsque vous définissez un modèle, le "x" désigne tout chiffre compris entre 0 et 9. Une série de chiffres entre crochets ([089]) désigne chacun de ces chiffres. ▪ Vous pouvez aussi définir une plage. Par exemple, [2-9] désigne tout chiffre compris entre 2 et 9.
Nombre de chiffres	Entrez le nombre de chiffres composant le numéro ou sélectionnez **Variable**. Le nombre de chiffres ne peut pas être inférieur au préfixe défini dans le champ **Commence par** ni dépasser 15.
Modèle de numérotation	Alors que vous introduisez des modèles dans le champ **Commence par**, la colonne **Modèle de numérotation** du tableau est mise à jour afin d'afficher le modèle de numérotation correspondant, code d'accès compris. La colonne **Modèle de numérotation** est en lecture seule.
Priorité du trunk	Les paramètres de priorité du trunk vous permettent d'affecter un degré de priorité au trunk sortant associé au coût le plus bas pour un type d'appel donné. Définissez une priorité pour le numéro sortant. Parmi les options disponibles **PSTN uniquement**, **SIP uniquement**, **PSTN, puis SIP**, **SIP, puis PSTN** ou **Aucun**.

Champ	Description
Définition de la priorité	*Facultatif*. Cliquez sur le bouton **Définition de la priorité** pour afficher la fenêtre Détails de la liste de trunks qui vous permet d'afficher ou de modifier les paramètres de la liste des trunks. Pour modifier les paramètres de la liste des trunks, procédez comme suit : 1. Cliquez dans la colonne **Préférence** correspondant au trunk dont vous souhaitez modifier la priorité et sélectionnez une priorité comprise entre 1 (la plus élevée) et 10 (la plus faible). 2. Cliquez sur **Ajouter un trunk** pour ajouter les groupes de trunks configurés sur le système et qui n'ont pas été ajoutés aux numéros sortants lorsqu'ils ont été créés. Lorsqu'un trunk est créé, vous pouvez choisir de l'ajouter à la liste des trunks pour tous les numéros sortants. Si vous n'avez pas choisi de l'ajouter lors de sa création, utilisez cette option pour l'ajouter à un numéro sortant. 3. Cliquez sur **Supprimer le trunk** pour supprimer un trunk de la liste (par exemple, vous pouvez supprimer un trunk SIP si vous souhaitez que tous les appels soient routés par les ports reliés au SDA). 4. L'option **Transférer le code d'accès** indique si le code d'accès composé par l'utilisateur est transféré ou non au trunk. La valeur par défaut pour l'option Transférer le code d'accès est Non. Ne modifiez pas ce champ à moins que votre fournisseur de services vous le demande. 5. Cliquez sur **OK**.

Pour modifier un numéro sortant, sélectionnez le numéro que vous souhaitez modifier, cliquez sur la ligne pour le sélectionner, apportez les modifications et cliquez sur **OK**.

Pour supprimer un numéro sortant, sélectionnez le numéro que vous souhaitez supprimer, cliquez sur la ligne pour le sélectionner, cliquez sur **Supprimer** et cliquez sur **OK**.

Exemple de blocage d'appel

Pour paramétrer le Plan de numérotation de sorte que les appels sortants vers les appels commençant par 1976 soient bloqués pour le plan de numérotation nord-américain, suivez les étapes suivantes :

ETAPE 1 Dans la fenêtre Numéros sortants, cliquez sur **Ajouter numéro**.

ETAPE 2 Dans le menu **Autorisations**, sélectionnez **Bloqué** et entrez le code d'accès.

ETAPE 3 Entrez la valeur 1976 dans le champ **Commence par**.

ETAPE 4 Entrez la valeur 11 dans le champ **Nombre de chiffres**.

ETAPE 5 Les champs **Liste de trunks** et **Définition de la priorité** ne s'appliquent pas aux numéros bloqués.

ETAPE 6 Cliquez sur **OK**.

Une fois que vous avez modifié le plan de numérotation pour y ajouter les numéros bloqués, vous devrez activer la fonction **Bloquer les appels interdits** pour chaque téléphone sur lesquels vous souhaitez bloquer ces numéros. Pour accéder à cette fonction, sélectionnez **Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Utilisateurs et téléphones**. Ouvrez l'onglet Postes utilisateurs et paramétrez le blocage d'appel pour chaque bouton Normal ou Ligne partagée de votre téléphone.

Modèles du plan de numérotation

Grâce aux modèles du plan de numérotation, Configuration Assistant permet de modifier le plan de numérotation sortant afin de répondre aux normes régionales. Sous l'onglet Gestion des appels sortants, vous pouvez effectuer les opérations suivantes :

- **Définir de nouveaux paramètres régionaux** non basés sur un modèle existant. Pour définir de nouveaux paramètres régionaux, sélectionnez l'option **Définir nouveaux paramètres régionaux** dans le menu Paramètres locaux du modèle de numérotation. Vous créerez ainsi un nouveau modèle de numérotation vierge.
- **Importer un modèle.** Lors de l'importation d'un modèle, celui-ci est copié vers l'emplacement contenant les modèles de Configuration Assistant. Lors des démarrages successifs, Configuration Assistant affiche le nouveau modèle comme option supplémentaire dans le menu Paramètres locaux du modèle de numérotation. Pour importer un modèle, cliquez sur **Importer un modèle**.
- **Exporter de nouveaux paramètres régionaux ou une configuration existante vers un modèle**. Lorsqu'un modèle est exporté, vous êtes invité(e) à introduire un nom unique le désignant. Il est enregistré au même emplacement que les modèles intégrés de Configuration Assistant. Lors

des démarrages successifs, Configuration Assistant affiche le modèle exporté comme option supplémentaire dans le menu Paramètres locaux du modèle de numérotation sous l'onglet Gestion des appels sortants. Pour exporter des paramètres régionaux ou une configuration existante vers un nouveau modèle, cliquez sur **Exporter comme modèle**.

- **Supprimer des paramètres régionaux**. Pour supprimer des paramètres régionaux, sélectionnez l'option **Supprimer paramètres régionaux** dans le menu Paramètres locaux du modèle de numérotation. Utilisez les flèches de la fenêtre Supprimer le modèle des paramètres régionaux pour déplacer les modèles disponibles vers la liste des modèles supprimés. Cliquez ensuite sur **OK**. Cliquez sur **OK** pour confirmer la suppression.

Groupes de trunks PSTN

Les groupes de trunks PSTN permettent de constituer des groupes logiques de ports vocaux offrant davantage de flexibilité dans le choix des ports vocaux destinés aux appels sortants.

REMARQUE La fonction Routage à plus faible coût faisant l'objet de cette rubrique concerne la sélection manuelle d'un trunk PSTN ou SIP à l'aide d'un code d'accès prédéfini.

Le paramètre Routage à plus faible coût vous permet de choisir le trunk sortant associé au coût le plus bas pour un type d'appel donné.

Configuration Assistant assure la prise en charge du routage à plus faible coût et offre les possibilités suivantes :

- Configurer la priorité des trunks pour les numéros sortants
- Affecter un schéma de groupement pour les ports vocaux dans un groupe de trunks
- Créer et gérer les nouveaux groupes de trunks PSTN pour former des groupes logiques de ports vocaux

Pour créer un nouveau groupe de trunks PSTN personnalisé, sélectionnez l'onglet Groupe de trunks PSTN et cliquez sur **Ajouter**. Voir la rubrique **Paramètres du groupe de trunks, page 483**.

Identifiant de l'appelant

Consultez les rubriques suivantes pour savoir comment configurer les paramètres d'identification de l'appelant.

- **Définir le code de blocage d'identification de l'appelant**
- **Définir l'identifiant de l'appelant affiché par défaut pour chaque groupe de trunks PSTN**

- **Vous pouvez remplacer l'identifiant de l'appelant par défaut par des numéros de poste spécifiques.**

Définir le code de blocage d'identification de l'appelant

Le **code de blocage d'identification de l'appelant** se compose de quatre chiffres. Les utilisateurs peuvent introduire ce code avant d'effectuer un appel. Le code doit commencer par un astérisque (par exemple : *111).

Les utilisateurs doivent composer ce code pour que leur numéro ne s'affiche pas sur le téléphone de leur interlocuteur. L'identifiant de l'appelant est envoyé, mais les paramètres de présentation sont définis sur "limité" de sorte que l'identifiant en question ne s'affiche pas.

Pour configurer le code, entrez un nombre à trois chiffres dans le champ "Code de blocage d'identification de l'appelant" et cliquez sur **Appliquer** ou **OK**.

CCA insère automatiquement l'astérisque (*). Par exemple, si vous introduisez le code 222, les utilisateurs devront composer *222 pour bloquer l'affichage de leur numéro lors d'un appel.

Définir l'identifiant de l'appelant affiché par défaut pour chaque groupe de trunks PSTN

Le Numéro principal du standard pour l'identifiant de l'appelant est le numéro d'identification de l'appelant affiché par défaut pour tous les appels sortants en provenance d'un SIP ou d'un groupe de trunks PSTN.

L'onglet Identifiant de l'appelant contient la liste de tous les groupes de trunks PSTN par défaut et personnalisés configurés sur le système ainsi que le numéro principal du standard pour l'identifiant de l'appelant actuellement configuré pour chaque groupe de trunks. Par défaut, le numéro principal du standard pour l'identifiant de l'appelant utilise le numéro PSTN principal défini lors de la création du trunk.

Pour modifier l'ID de l'appelant pour un groupe de trunks, procédez comme suit :

ETAPE 1 Sous l'onglet Identifiant de l'appelant de la fenêtre Plan de numérotation sortant, cliquez sur un groupe de trunks PSTN pour le sélectionner.

ETAPE 2 Cliquez sur le champ **Numéro principal du standard pour l'identifiant de l'appelant** correspondant au groupe de trunks PSTN sélectionné.

ETAPE 3 Entrez un numéro de téléphone à afficher pour l'identifiant de l'appelant. Le numéro peut contenir jusqu'à 15 chiffres. Le numéro peut commencer par un caractère "+".

ETAPE 4 Cliquez sur **OK** ou **Appliquer**.

Vous pouvez remplacer l'identifiant de l'appelant par défaut par des numéros de poste spécifiques. Voir la rubrique **Vous pouvez remplacer l'identifiant de l'appelant par défaut par des numéros de poste spécifiques., page 480**.

Vous pouvez remplacer l'identifiant de l'appelant par défaut par des numéros de poste spécifiques.

Pour modifier l'ID de l'appelant par défaut pour certains postes, procédez comme suit :

ETAPE 1 Sous l'onglet Identifiant de l'appelant de la fenêtre Plan de numérotation sortant, cliquez sur un groupe de trunks PSTN pour le sélectionner.

ETAPE 2 Cliquez sur **Ajouter**.

La fenêtre Ajouter un identifiant de l'appelant pour les postes internes s'affiche. Complétez les paramètres de la fenêtre selon les indications de la rubrique **Ajouter un identifiant de l'appelant pour les postes internes, page 480**.

Vous pouvez entrer jusqu'à 14 identifiants de l'appelant.

ETAPE 3 Cliquez sur **OK** ou **Appliquer**.

Pour modifier les paramètres d'identifiant de l'appelant existants, mettez l'élément en surbrillance dans la liste et cliquez sur **Modifier**.

Ajouter un identifiant de l'appelant pour les postes internes

Cette fenêtre s'affiche lorsque vous sélectionnez un groupe de trunks PSTN sous l'onglet Identifiant de l'appelant de la fenêtre Plan de numérotation sortant et cliquez ensuite sur **Ajouter** ou **Modifier**.

Configurez les paramètres de l'identifiant de l'appelant pour les postes internes selon les consignes ci-dessous et cliquez sur **OK**. Vous pouvez entrer jusqu'à 14 identifiants de l'appelant. En définissant une plage de postes internes à associer à un ou plusieurs numéros d'identification de l'appelant, vous pouvez réduire le nombre d'entrées utilisées.

Champ	Description
Numéro initial pour la plage de postes internes **Numéro final pour la plage de postes internes**	Entrez le numéro initial et le numéro final de la plage de postes internes afin de remplacer l'identifiant de l'appelant par défaut par une plage de valeurs. Pour écraser l'identifiant de l'appelant par défaut par un numéro de poste, entrez le même numéro de poste dans les champs Numéro initial pour la plage de postes internes et Numéro final pour la plage de postes internes.
Numéro initial pour l'identification de l'appelant **Numéro final pour l'identification de l'appelant**	Entrez le numéro initial et le numéro final afin de remplacer l'identifiant de l'appelant par défaut par une plage de postes internes. Les numéros peuvent commencer par un signe "+". Toutefois, si le signe "+" est utilisé comme premier caractère, il doit aussi être utilisé comme élément de fin. Si vous associez une plage de numéros de postes internes à une plage de numéros de l'appelant, les derniers chiffres doivent correspondre. Par exemple, si vous entrez les valeurs 205 et 210 comme numéro initial et numéro final pour les postes internes, les numéros d'identification de l'appelant de début et de fin doivent se terminer par 05 et 10. Pour un groupe de trunks PSTN, les plages d'extension internes ne peuvent pas se chevaucher. Pour remplacer l'identifiant de l'appelant par défaut par un numéro de poste unique ou pour afficher le même identifiant de l'appelant pour une plage de numéros, entrez le même chiffre dans les champs Numéro initial pour l'identification de l'appelant et Numéro final pour l'identification de l'appelant.

Exemples :

Pour remplacer les numéros d'identification de l'appelant pour les postes 205 à 225 par des numéros de 12229990005 à 12229990005, procédez comme suit :

- Entrez la valeur 205 dans le champ Numéro initial pour la plage de postes internes.
- Entrez la valeur 225 dans le champ Numéro final pour la plage de postes internes.
- Entrez la valeur 12229990005 dans le champ Numéro initial pour l'identification de l'appelant.
- Entrez la valeur 12229990025 dans le champ Numéro final pour l'identification de l'appelant.

Pour afficher la valeur 12229991200 comme identifiant de l'appelant pour les numéros de poste interne compris entre 200 et 230 :

- Entrez la valeur 200 dans le champ Numéro initial pour la plage de postes internes.
- Entrez la valeur 230 dans le champ Numéro final pour la plage de postes internes.
- Entrez la valeur 12229991200 dans le champ Numéro initial pour l'identification de l'appelant et dans le champ Numéro final pour l'identification de l'appelant.

Pour remplacer les numéros d'identification de l'appelant pour les postes 505 par le numéro 12229991100, procédez comme suit :

- Entrez la valeur 505 dans le champ Numéro initial pour la plage de postes internes et dans le champ Numéro final pour la plage de postes internes.
- Entrez la valeur 12229991100 dans le champ Numéro initial pour l'identification de l'appelant et dans le champ Numéro final pour l'identification de l'appelant.

Paramètres du groupe de trunks

Cette fenêtre s'affiche lorsque vous cliquez sur **Ajouter** ou **Modifier** sous l'onglet Groupe de trunks PSTN de la fenêtre Plan de numérotation sortant.

Tous les ports vocaux sont placés dans les groupes par défaut sur la base du type de SKU. Par exemple, ALL_FXO ou ALL_ BRI. Ces groupes par défaut peuvent être modifiés.

Lorsque vous créez un nouveau groupe de trunks PSTN, vous devez faire un choix entre l'ajout du nouveau trunk comme option pour tous les numéros sortants ou l'ajout du groupe de trunks aux numéros sélectionnés selon les besoins.

Lorsque vous créez un nouveau trunk SIP ou un groupe de trunks T1/E1, vous êtes invité à introduire le numéro SDA principal correspondant à ces trunks. Le numéro SDA principal est nécessaire pour tous les groupes de trunks qui ne sont pas vides. Si vous créez un groupe de trunks sans affecter de ports vocaux en tant que membres, le numéro SDA principal n'est pas nécessaire. Si des ports vocaux sont affectés à ce groupe de trunks, il est nécessaire.

Pour créer ou modifier un groupe de trunks SDA, configurez les paramètres ci-dessous et cliquez sur **OK**.

Champ	Description
Groupe de trunks	Description du groupe de trunks.

Champ	Description
Modèle de groupement de postes	Le modèle de groupement de postes établit comment les ports vocaux membres sont sélectionnés pour les appels sortants. Les options suivantes sont disponibles : ▪ **séquentiel**. Sélectionne le port vocal prioritaire. ▪ **périodique**. Sélectionne le port vocal suivant présentant des emplacements libres. ▪ **aléatoire**. Sélectionne un emplacement de manière aléatoire. ▪ **plus longtemps disponible**. Sélectionne le port vocal présentant l'emplacement disponible depuis le plus longtemps. ▪ **le moins longtemps disponible**. Sélectionne le port vocal présentant l'emplacement disponible depuis le moins longtemps.
Type de trunk	Sélectionnez un type de trunk dans la liste des types de trunk disponible sur votre système.
Membres du groupe de trunks	Sélectionnez les membres du groupe de trunks dans la liste des ports vocaux disponibles pour le type de trunk sélectionné. Un port vocal ne peut appartenir qu'à un seul groupe de trunks PSTN. Vous ne pouvez pas mélanger les différents types de trunk PSTN dans un même groupe. Par exemple, un port FXO analogique ne peut pas être membre d'un groupe de trunks contenant des ports BRI ISDN. Utilisez les flèches **Haut** et **Bas** pour réorganiser la liste des ports vocaux si le modèle de groupement sélectionné est séquentiel ou périodique.

15

Gestion de site

Les rubriques suivantes sont présentées :

- **Gestionnaire multi-sites**
- **Nombre d'appels maximum (Contrôle des admissions d'appel)**

Gestionnaire multi-sites

Le Gestionnaire multi-sites vous permet de configurer, gérer et assurer le suivi d'un maximum de 5 sites clients Cisco SBCS reliés par un VPN Full-mesh.

Cette fonction permet aux utilisateurs finaux des sites connectés d'effectuer des appels inter-sites à l'aide de la fonction d'appel abrégé et de partager des données à l'aide d'une connexion WAN sécurisée. Les déploiements multi-sites sont parfaitement adaptés aux petites entreprises réparties sur 5 sites tout au plus.

Les modèles de déploiement pris en charge comprennent les sites clients dotés d'un seul UC500 ou d'un UC500 placé derrière un routeur sécurisé Cisco SR500 pour les fonctions de sécurité avancées.

- **Critères et consignes pour la conception multi-sites**
- **Procédures de configuration multi-sites**
- **Suivi de l'état multi-sites**
- **Fonctions vocales prises en charge sur plusieurs sites**

Critères et consignes pour la conception multi-sites

Seules les topologies de réseau suivantes sont prises en charge pour les sites clients isolés participant à un déploiement multi-sites. Chacune de ces topologies peut être combinée tant que le nombre total des sites reste inférieur ou égal à 5. Les sites sont configurés avec un VPN Full-mesh. Dès lors, chaque site dispose d'un lien direct avec chaque autre.

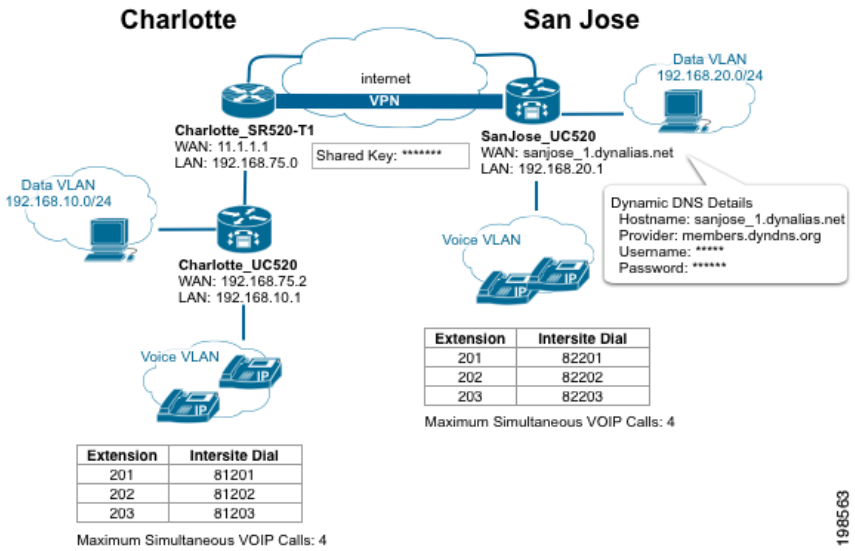
- Un seul UC500 relié au WAN.
- Un seul routeur sécurisé SR520-T1 associé à un UC500. Le SR520-T1 est relié au WAN et offre des fonctions de sécurité avancées alors que l'UC500 est responsable de la voix et des données pour le site. Pour ce type de déploiement, le VLAN de données doit être unique pour le SR520-T1 et l'UC500.

  Dans la version actuelle, le routeur sécurisé SR520-T1 peut être utilisé pour les déploiements multi-sites Cisco SBCS configurés à l'aide de CCA.

IMPORTANT Chaque site *doit* disposer d'un UC500 pour la voix et les données. Le Gestionnaire multi-sites ne peut pas être utilisé pour configurer l'un des types de déploiement suivants :

- Un routeur SR520-T1 autonome sous forme de site
- Un VPN de données uniquement et de site à site entre deux routeurs sécurisés SR500 ou plus
- Un téléphone distant derrière un SR520-T1 sans UC500

Ce schéma présente un exemple simple de déploiement avec deux sites illustrant les topologies prises en charge et certains critères de conception évoqués dans ce chapitre.



L'exemple ci-dessus représente les éléments principaux d'une configuration multi-sites :

- **Topologie du site**. Le site de Charlotte offre un exemple de site doté d'un UC500 placé derrière un SR520-T1 alors que le site de San Jose ne dispose que d'un UC500.
- **L'adresse IP du VLAN de données doit être unique**. Étant donné que les adresses IP du VLAN doivent être uniques pour tous les sites pour chaque UC500 ainsi que pour chaque SR520-T1, l'adresse IP du VLAN de données pour l'UC500 du site de Charlotte est 192.168.10.1/24 alors que l'adresse IP du VLAN de données pour l'UC 500 de San Jose est 192.168.20.1/24. L'adresse IP du VLAN pour le SR520-T1 de Charlotte est 192.168.75.0/24 et il n'y a pas de SR520-T1 sur le site de San Jose (sinon une adresse IP unique pour le VLAN de données serait nécessaire).
- **Plan de numérotation et numérotation inter-sites**. Pour cette configuration, nous avons opté pour le chiffre "8" comme préfixe de numérotation inter-sites. Le code pour le site de Charlotte est 1 alors que celui pour le site de San Jose est 2. Comme l'indique l'exemple, les utilisateurs forment le *Préfixe d'appel inter-sites + Code du site + numéro*

de poste pour contacter les autres sites. La limite est fixée à trois chiffres pour les numéros de poste. Bien que tous les sites ne doivent pas forcément présenter le même nombre de chiffres pour les numéros de poste, cette approche est conseillée afin de faciliter l'utilisation et la configuration.

- **L'adresse IP statique ou WAN DHCP est pris en charge**. Le site de Charlotte a utilisé une adresse IP WAN statique alors que celui de San Jose utilise le protocole DHCP. Puisque le DHCP est utilisé, Dynamic DNS (DDNS) est configuré pour San Jose.
- **Identification du VPN Full-mesh avec clé partagée**. Une clé partagée globale identique est définie pour chaque site afin de permettre l'identification par le tunnel VPN.
- **Contrôle des admissions d'appel**. Les deux sites sont configurés pour autoriser un maximum de
  4 appels simultanés sur le WAN.

Le tableau dresse la liste et décrit les critères de conception en vigueur pour le site ainsi que les consignes de manière plus détaillée.

IMPORTANT la configuration hors-bande n'est pas prise en charge par le Gestionnaire multi-sites. Vous pouvez supprimer la configuration multi-sites hors-bande avant d'utiliser le Gestionnaire multi-sites.

Élément de configuration	Critères/consignes
Nombre de sites	Jusqu'à 5 sites dans une topologie Full-mesh.

Élément de configuration	Critères/consignes
Nombre de tunnels IPsec	Pour les plateformes UC520 et UC540, chaque site client prend en charge jusqu'à 10 tunnels IPsec. Pour les plateformes UC560, chaque site client prend en charge jusqu'à 20 tunnels IPsec. Cela comprend les tunnels EZVPN, SSL VPN, les tunnels VPN multi-sites et les tunnels VPN pour les téléphones SPA525G. Lorsqu'un site fait partie d'un déploiement multi-sites, *N-1* de ces tunnels VPN sont utilisés pour un VPN Full-mesh de site à site (*N* correspond au nombre de sites). Par exemple, si le déploiement d'une plateforme UC540 couvre 4 sites, 3 tunnels IPsec sont utilisés pour le VPN Full-mesh de site à site, ce qui laissera 7 tunnels disponibles pour le protocole EZVPN et/ou SSL VPN.
Pare-feu	Pare-feu de zone (ZBF) Cisco sur le SR500 ou règle CBAC Cisco IOS pour l'UC500. Les pare-feu tiers ne sont pas pris en charge.
Adressage du VLAN de données	L'adresse IP du VLAN de données pour chaque UC500 et SR520-T1 doit être unique pour tous les sites. Si chaque site présente les paramètres d'usine, vous devez veiller à modifier l'adresse du VLAN de données par défaut au cours de la configuration initiale pour chaque membre du site afin qu'il soit véritablement unique. Utilisez l'Assistant de configuration de la téléphonie pour configurer les paramètres initiaux. Si l'un des sites distants présente une adresse IP de VLAN existante qui n'est pas unique, vous devrez modifier l'adresse. Pour les sites ne présentant pas la configuration d'usine, vous pouvez effectuer cette opération à l'aide du Gestionnaire multi-sites. Après avoir modifié l'adresse IP du VLAN de données, vous perdrez la liaison avec l'UC 500 et devrez lui demander une nouvelle adresse IP. Pour ce faire, allez dans **Démarrer** > **Exécuter** sur votre PC et entrez **`cmd`** pour afficher la ligne de commande. A l'invite de commande, entrez **`ipconfig /renew`**.

Élément de configuration	Critères/consignes
Type de connexion WAN	Les sites peuvent utiliser l'adresse IP DHCP avec DDNS ou statique. Pour les sites utilisant le protocole DHCP pour obtenir de manière dynamique l'adresse IP, le DDNS (Dynamic Domain Name Service) ou toute autre méthode d'enregistrement DNS devra être utilisée pour gérer les adresses dynamiques. Lorsque vous configurez le DDNS, le nom du fournisseur DDNS, le nom d'hôte pour chaque site et les codes d'accès (nom d'utilisateur et mot de passe) devront être introduits dans le cadre de la configuration de la connexion multi-sites. Voir la rubrique **Configuration du DDNS, page 505**. Le nom d'hôte DDNS doit être propre à chaque site.

Élément de configuration	Critères/consignes
Service d'hébergement DDNS (Dynamic DNS)	Le DDNS doit être configuré pour les sites offrant des connexions WAN DHCP faisant partie d'un déploiement multi-sites. Les sites associés à une adresse IP statique ne sont pas nécessaires pour la configuration du DDNS. Ces services d'hébergement DDNS peuvent être sélectionnés dans la rubrique HTTP DDNS de la fenêtre Connexion Internet (**Configurer** > **Routage** > **Connexion Internet > Modifier > Paramètres de connexion**). ▪ cgi.tzo.com ▪ dup.hn.org ▪ members.dyndns.org ▪ members.easydns.com ▪ www.dynx.cx ▪ www.justlinux.com ▪ www.zoneedit.com Les comptes pour ces fournisseurs DDNS doivent être définis hors de Configuration Assistant. **ASTUCE** Cisco vous conseille d'effectuer la mise à niveau de la version gratuite à la version payante ou premium auprès de votre fournisseur de services DDNS. Par exemple, certaines versions gratuites expirent suite à l'absence d'activité (par exemple, si l'adresse IP n'est pas mise à niveau au bout de 30 jours). En cas d'annulation de la prise en charge DNS pour le nom de domaine, les tunnels VPN ne seront plus fonctionnels ou risquent de ne plus démarrer, ce qui provoquerait des pannes.
Mise en forme du trafic/Qualité de service (QoS)	*Facultatif*. Bien que ce réglage soit facultatif, il n'en demeure pas moins conseillé. Les sites dotés d'une bande passante limitée doivent permettre la mise en forme de trafic et configurer les paramètres QoS pour les déploiements multi-sites.

Élément de configuration	Critères/consignes
Codec	Vous pouvez utiliser le codec G.711 ou G.729 pour les appels inter-sites. Le codec G.729 offre une compression supérieure, ce qui permet d'économiser de la bande passante et limiter la qualité de certains types de son tels que la musique d'attente.
Contrôle des admissions d'appel	*Facultatif.* Configurez la valeur Nombre d'appels maximum (nombre maximal d'appels simultanés) pour assurer la qualité de la voix pour les appels inter-sites et les appels VoIP en évitant une surcharge de la connexion Internet. Configuration Assistant utilise les paramètres QoS actifs pour la bande passante ascendante, la priorité des codecs et la réservation de la bande passante pour les supports vocaux afin de fournir des recommandations pour le contrôle des admissions d'appel.
Plan de numérotation	Définissez un **Préfixe d'appel inter-sites** pour les appels d'un site à l'autre. Pour appeler un autre site, les utilisateurs du téléphone doivent composer les numéros suivants : *Préfixe d'appel inter-sites + Code du site + Numéro de poste* Cette fonction offre une certaine flexibilité dans l'affectation des numéros de poste aux sites. Le préfixe déjà utilisé ne peut pas être sélectionné.
Longueur du numéro de poste	Il est conseillé d'utiliser le même nombre de chiffres pour le numéro de poste.
Nom de l'hôte	Pour éviter toute confusion lors de la sélection du nom de l'hôte dans les menus de Configuration Assistant, il est conseillé d'opter pour des noms d'hôte unique pour tous les sites. Le nom d'hôte système s'affiche dans les menus de sélection de Configuration Assistant et dans les invites du système.

Procédures de configuration multi-sites

Les rubriques de ce chapitre traitent des procédures de configuration multi-sites pour les configurations prises en charge.

Si vous n'avez pas encore configuré les connexions multi-sites sur l'UC500, la fenêtre initiale offre un aperçu des étapes de configuration avec les options suivantes :

- **Définir manuellement les paramètres multi-sites** Sélectionnez cette option pour accéder à l'onglet Configuration multi-sites. Voir la rubrique **Ajout et configuration de sites, page 495**.
- **Importer le fichier de configuration multi-sites**. Choisissez cette option pour importer les paramètres de site exportés vers un fichier de configuration sur un autre site. Voir la rubrique **Exportation et importation de sites, page 508**.

REMARQUE Toutes les procédures de configuration multi-sites considèrent que le PC exécutant Configuration Assistant est connecté à un port Ethernet de l'UC 500 et a obtenu l'adresse IP de l'UC500. Lorsque l'UC500 se trouve derrière un routeur sécurisé SR520-T1, connectez-le directement à l'UC500 et utilisez le protocole DHCP pour obtenir une adresse IP de l'UC500.

- **Critères et consignes pour la conception multi-sites**
- **Critères pour la configuration multi-sites**
- **Ajout et configuration de sites**
- **Configuration du DDNS**
- **Configuration de la qualité de service (QoS)**
- **Nombre d'appels maximum (Contrôle des admissions d'appel)**
- **Exportation et importation de sites**
- **Modifier un site après la configuration initiale**
- **Supprimer un site**

Critères pour la configuration multi-sites

Vous devez respecter plusieurs conditions pour configurer les liaisons multi-sites. Pour de plus amples informations, consultez la rubrique **Fonctions vocales prises en charge sur plusieurs sites, page 512**.

- La configuration de base pour la voix et les données doit être établie sur l'UC500 à l'aide de l'Assistant de configuration de la téléphonie (recommandé pour les sites configurés à partir des paramètres par défaut) ou de Configuration Assistant en mode Expert. Cela comprend les éléments suivants :
  - Connexion Internet
  - L'adresse IP du VLAN de données pour chaque UC500 et SR520-T1 doit être unique pour tous les sites. Si ce n'est pas le cas, vous pourrez la modifier par la suite grâce au Gestionnaire multi-sites.
  - Paramètres d'initialisation du système vocal, comme le code d'accès par défaut pour les appels extérieurs (**Configurer** > **Téléphonie** > **Plan de numérotation** > **Sortant** > **Gestion des appels sortants**).
  - La téléphonie locale doit au moins être configurée pour permettre les appels au sein du site de préférence à l'aide de l'Assistant de configuration de la téléphonie.
- Vous devez configurer ces paramètres si le routeur sécurisé SR500 est le périphérique de périmètre (à savoir si l'UC500 du site est placé derrière le SR500) :
  - Connexion WAN Si vous utilisez un routeur sécurisé SR520-T1, vous devez exécuter l'utilitaire de connexion T1 avant de lancer l'Assistant de configuration de la téléphonie.
  - Le pare-feu et le NAT sont désactivés sur l'UC500. Lorsque vous exécutez l'Assistant de configuration de la téléphonie, vous y êtes automatiquement invité(e) dans le cadre de la configuration.
  - L'UC500 présente l'adresse IP WAN statique 192.168.x.2 où x est obtenu du VLAN75 de données du SR500.
  - Le SR500 peut acheminer les données vers l'UC500 (chemin statique simple vers le VLAN1 de données). Lorsque vous lancez l'Assistant de configuration de la téléphonie, ces chemins sont automatiquement établis.
  - Le SR500 doit présenter une configuration d'adresse unique à l'échelle du réseau pour le VLAN75.
- Pour les sites utilisant une connexion DHCP WAN, les informations suivantes sont nécessaires pour la configuration du DDNS :
  - Nom du fournisseur DDNS

- Nom d'hôte unique pour chaque site
- Nom d'utilisateur et mot de passe pour le fournisseur DDNS

Ajout et configuration de sites

Vue d'ensemble

Si vous configurez des connexions multi-sites pour les sites dotés de plateformes UC500 et SR500 avec les réglages par défaut, les étapes conseillées pour la configuration des connexions entre les sites sont les suivantes.

1. Si vous utilisez un routeur sécurisé SR520-T1 comme élément périphérique, vous *devez* exécuter l'utilitaire de connexion T1 avant de lancer l'Assistant de configuration de la téléphonie. Consultez le *Guide de démarrage rapide pour Cisco Small Business Pro SR520-T1* et la note d'application pour la configuration de l'*UC500 et du routeur sécurisé SR520-T1* pour obtenir les instructions.
2. Sur le premier site :
   a. Vérifiez si la configuration de base pour la voix et les données est définie sur l'UC500.
   b. Lancez Configuration Assistant et configurez la Mise en forme du trafic/ Quality of Service, le nombre d'appels maximum (Contrôle des admissions d'appel) et les paramètres DDNS si nécessaire. Pour les sites dotés d'une connexion WAN DHCP, le DDNS doit être défini afin de lancer le Gestionnaire multi-sites.
   c. Démarrez le Gestionnaire multi-sites (**Configurer** > **Téléphonie** > **Gestion de site** > **Gestionnaire multi-sites**) et configurez les paramètres généraux pour les options multi-sites :
      - Clé partagée pour l'identification du tunnel VPN
      - Préfixe de numérotation inter-sites
      - Codec à utiliser pour les appels VoIP de site à site (G.711 ou G.729)
   d. Configurez les paramètres multi-sites pour le premier site :
      - Nom du site
      - Index du site
      - Nombre de chiffres par numéro de poste.

e. Ajoutez les autres sites distants et configurez les paramètres multi-sites de base :

- Nom du site
- IP du WAN ou nom de domaine complet (FQDN)
- Adressage interne (VLAN de données pour l'UC500 que le site dispose ou non d'un SR520-T1)
- Modèle de numérotation de site (ID de site et chiffres par numéro de poste)

f. Exportez les paramètres de configuration multi-sites configurés ci-avant et appliquez la configuration.

3. Sur le deuxième site et chaque site restant (jusqu'à 5 sites).

a. Vérifiez si la configuration de base pour la voix et les données est définie sur l'UC500.

b. Configurez la mise en forme du trafic/QoS, le nombre d'appels maximum et les paramètres DDNS si nécessaire.

c. Activez le Gestionnaire multi-sites et importez le fichier de configuration multi-sites créé et exporté à partir du premier site.

d. Configurez la même clé partagée sur les sites distants.

Si vous connectez un ou plusieurs sites existants, les étapes sont similaires à l'exception de l'utilisation de l'Assistant de configuration de la téléphonie car vous devrez définir la configuration en mode Expert. Si vous devez modifier l'adresse IP par défaut du VLAN de données pour le SR520-T1 ou l'UC500, vous pouvez le faire à l'aide du Gestionnaire multi-sites lors de l'importation des données du site.

Procédures

ETAPE 1 Vérifiez si les critères définis dans le chapitre **Critères pour la configuration multi-sites, page 493** sont respectés.

ETAPE 2 Vérifiez si le PC exécutant Configuration Assistant est directement connecté à l'UC500 et a obtenu l'adresse IP de l'UC500.

ETAPE 3 Démarrez Configuration Assistant et connectez-vous au premier site à configurer.

ETAPE 4 Dans la barre de fonctions, sélectionnez l'option **Configurer** > **Téléphonie** > **Gestion de site** > **Gestionnaire multi-sites**.

ETAPE 5 Sélectionnez l'onglet Configuration multi-sites.

ETAPE 6 Configurez les **paramètres généraux** pour tous les sites.

Paramètre	Description
Clé partagée pour authentification	Entrez une clé partagée pour l'identification des sites distants. Utilisez une clé partagée respectueuse des critères en vigueur pour la définition des mots de passe. Vous pouvez entrer entre 8 et 127 caractères. Les espaces et les points d'interrogation ne sont pas pris en charge. Cochez la case **Afficher la clé** pour afficher la clé partagée en texte brut. Cochez la case **Autoriser l'exportation de la clé** pour autoriser l'exportation de la clé partagée en texte brut dans le fichier de configuration. **IMPORTANT** La clé partagée *doit* être la même pour tous les sites. Par défaut, la clé partagée n'est pas exportée dans la configuration multi-sites. Si vous choisissez d'exporter la clé, elle est exportée sous forme de texte brut. Si la clé partagée n'est pas exportée, vous devrez la réintroduire manuellement lors de l'importation des données de configuration multi-sites à partir d'autres sites.
Codec	Codec de prédilection pour les appels inter-sites. Faites votre choix parmi les options suivantes : ▪ **G711** : Le codec G711 est sélectionné. ▪ **G729** : Le codec G729 est sélectionné.

Paramètre	Description
Préfixe de numérotation inter-sites	Sélectionnez un préfixe dans la liste déroulante. Le système détecte les préfixes utilisés par le plan de numérotation et n'affiche que les choix disponibles. Il s'agit du numéro que les utilisateurs doivent composer pour passer un appel à un autre site. Pour appeler des sites distants, les utilisateurs composent le *Préfixe d'appel inter-sites + Code du site + Numéro de poste* Par exemple, si le préfixe pour les appels inter-sites est le 7 et que l'utilisateur du site 1 souhaite appeler le poste 307 sur le site 2, l'utilisateur devra composer le numéro 72307.

ETAPE 7 Passez en revue et modifiez les paramètres multi-sites pour le premier site. Il s'agit du site avec lequel vous êtes mis en connexion.

Pour entamer la modification des paramètres du site, cliquez sur **Modifier**. Voir **Paramètres de site, page 502** pour plus d'informations.

Les informations s'affichent à partir du site auquel vous êtes connecté(e).

Paramètre	Description
Adresse WAN	Lecture seule. Adresse IP WAN du site.
Adresse du VLAN de données de l'UC500	Lecture seule. Adresse IP du VLAN de données de l'UC500 pour ce site.
Masque de sous-réseau du VLAN de données de l'UC500	Lecture seule. Masque de sous-réseau du VLAN de données de l'UC500 pour ce site.
Adresse du VLAN de données pour le SR500	Lecture seule. Adresse IP du VLAN de données du SR520-T1 si un SR520-T1 fait partie du site client
Masque de sous-réseau du VLAN de données du SR500	Lecture seule. Adresse IP du VLAN de données du SR520-T1 si un SR520-T1 fait partie du site client
Modèle de numérotation du site	Champ en lecture seule affichant le modèle que les membres du site doivent respecter pour passer des appels inter-sites par le WAN.
Connecté à ce site Cliquez sur **Afficher les options de configuration supplémentaires** pour afficher l'état (**Configuré** ou **Non configuré**) des paramètres supplémentaires qu'il pourrait être utile de définir pour le site.	

Paramètre	Description
DDNS	*Facultatif*. Configuration du DNS dynamique. Indique si un DDNS est configuré ou non pour ce site. Si le DDNS n'est pas configuré et que vous utilisez le DHCP, vous devrez le paramétrer avant de lancer le Gestionnaire multi-sites. Cliquez sur le lien **Configuré** ou **Non configuré** pour afficher la fenêtre Connexion Internet où vous pourrez modifier ces paramètres. Voir la rubrique **Configuration du DDNS, page 505**.
Mise en forme du trafic WAN	*Facultatif, mais fortement conseillé.* Indique si la mise en forme du trafic et le QoS ont été paramétrés pour le site. Tous ces paramètres sont facultatifs mais ils sont fortement recommandés pour tous les sites, surtout pour ceux associés à une faible bande passante. Cela permet de définir la priorité de la voix sur les données si nécessaire. Cliquez sur le lien **Configuré** ou **Non configuré** pour afficher la fenêtre Connexion Internet où vous pourrez modifier ces paramètres. Voir la rubrique **Configuration de la qualité de service (QoS), page 506**.
Contrôle des admissions d'appel	Indique si le Contrôle des admissions d'appel est configuré ou non pour ce site. Les paramètres de contrôle des admissions d'appel définissent le nombre maximum d'appels pour un site. Si le Contrôle des admissions d'appel n'est pas configuré, sélectionnez l'option **Configurer** > **Téléphonie** > **Nombre d'appels maximum** dans la barre de fonctions pour accéder aux options de configuration. Voir la rubrique **Nombre d'appels maximum (Contrôle des admissions d'appel), page 513**.

ETAPE 8 Une fois que vous avez passé en revue et configuré les paramètres pour le premier site, cliquez sur **Ajouter un site** et configurez les paramètres pour les autres sites concernés par le déploiement.

Voir la rubrique **Paramètres de site, page 502**.

ETAPE 9 Lorsque vous avez terminé d'ajouter et de configurer tous les sites distants, cliquez sur **Appliquer**.

Le bouton **Appliquer** est grisé si l'un des paramètres nécessaires n'est pas configuré (par exemple, la clé partagée).

Une fois que les modifications ont été appliquées, le bouton **Exporter le fichier de configuration multi-sites** est actif.

ETAPE 10 Cliquez sur **Exporter le fichier de configuration multi-sites**.

Le bouton **Exporter le fichier de configuration multi-sites** est grisé tant que vous n'avez pas appliqué la configuration.

ETAPE 11 Enregistrez le fichier de configuration sur votre PC. Vous pouvez utiliser le nom de fichier par défaut ou définir un nom de fichier distinct.

IMPORTANT Ne modifiez pas le fichier de configuration XML. Les modifications apportées aux paramètres de configuration multi-sites exportées doivent être effectuées par le Gestionnaire multi-sites et réimportées à partir des différents sites faisant partie de la configuration. Voir la rubrique **Exportation de sites, page 508**.

ETAPE 12 Cliquez sur **OK**.

ETAPE 13 Enregistrez les modifications apportées à la configuration de démarrage de tous les périphériques du site client :

- Cliquez sur **Configurer** > **Enregistrer la configuration** ou
- Cliquez sur **Enregistrer** à l'invite s'affichant à la fermeture de Configuration Assistant.

ETAPE 14 Importez le fichier de configuration multi-sites que vous venez d'exporter vers chaque site à l'aide des procédures décrites dans **Importation de sites, page 509**.

Une fois les paramètres importés et appliqués à tous les sites distants, les tunnels VPN s'afficheront.

Jusqu'à trois minutes peuvent s'avérer nécessaires pour que la liaison avec les tunnels puisse être établie.

Pour activer les tunnels IPsec manuellement, sélectionnez l'onglet État multi-sites et cliquez sur **Connecter à tous les sites**.

Paramètres de site

La fenêtre Paramètres de site s'affiche lorsque vous effectuez les opérations suivantes :

- Lorsque vous cliquez sur **Ajouter un site** dans la fenêtre Gestionnaire multi-sites.
- Lorsque vous cliquez sur **Modifier** (Crayon) dans la fenêtre Gestionnaire multi-sites pour modifier les paramètres des sites.

Lorsque vous ajoutez ou modifiez les paramètres selon les données reprises dans le tableau et cliquez sur **OK** pour revenir au Gestionnaire multi-sites.

Les modifications apportées à la configuration du site donneront lieu à des appels manqués et à l'interruption du trafic de données au cours de la configuration.

Paramètre	Description
Données du site	
Nom du site	Description du site.
Adresse IP WAN ou domaine	Adresse IP publique (en présence d'une adresse IP statique) ou nom de domaine complet pour le site (pour le DDNS).
Adressage interne Si vous êtes directement connecté(e) à ce site, les données d'adressage interne sont obtenues à partir de la configuration de périphérique active. Vous pouvez modifier l'adresse IP du VLAN de données pour l'UC500 ou le SR520-T1, auquel cas une fenêtre d'avertissement s'affichera. ▪ Vous êtes invité(e) à vérifier ou obtenir l'adresse IP sur votre PC avant de redémarrer Configuration Assistant et de vous connecter à votre site client. ▪ Aucune configuration multi-sites n'est appliquée au cours de la modification. Vous devez utiliser le Gestionnaire multi-sites et configurer ou réimporter vos paramètres multi-sites une fois que le VLAN aura été mis à jour.	
Adresse IP du VLAN de données de l'UC500	Adresse IP du VLAN de données sur l'UC500. Par exemple, 182.168.30.5.
Masque de sous-réseau du VLAN de données de l'UC500	Masque de sous-réseau pour le VLAN de données sur l'UC500. Par exemple, 255.255.255.0. Si vous êtes directement connecté(e) à ce site, les données sont obtenues à partir de la configuration active.
Le site utilise le SR500 comme périphérique WAN	Cochez cette option si l'UC500 se trouve derrière un routeur sécurisé SR520-T1.
Adresse réseau du VLAN de données du SR500	Adresse IP du VLAN de données sur le SR520-T1. Si vous êtes directement connecté(e) à ce site, les données sont obtenues à partir de la configuration active.

Paramètre	Description
Masque de sous-réseau du VLAN de données du SR500	Masque de sous-réseau pour le VLAN de données sur le SR520-T1. Si vous êtes directement connecté(e) à ce site, les données sont obtenues à partir de la configuration active.
Modèle de numérotation du site	
Préfixe de numérotation inter-sites	Ce champ en lecture seule affiche le préfixe à numéro unique configuré pour les appels inter-sites. Il s'agit de la configuration globale pour tous les sites.
Chiffres par numéro de poste	Nombre de chiffres utilisés pour les numéros de poste interne (longueur du numéro de poste).
Identifiant de site	Introduisez un nombre allant de 1 à 5 permettant l'identification du site. Il s'agit de l'identifiant de site utilisé pour la numérotation inter-sites. Pour appeler ce site, les utilisateurs se trouvant sur les sites distants doivent utiliser ce format : *Préfixe d'appel inter-sites + Code du site + Numéro de poste* Par exemple, si le préfixe pour les appels inter-sites est le 7 et que l'utilisateur du site 1 souhaite appeler le poste 307 sur le site 2, l'utilisateur devra composer le numéro 72307.
Modèle de numérotation résultant	Ce champ en lecture seule contient le modèle de numérotation pour le site d'après les valeurs configurées pour le préfixe de numérotation inter-sites, le code de site et le nombre de chiffres composant le numéro de poste.

Configuration du DDNS

Le DDNS est uniquement nécessaire pour les sites utilisant le DHCP afin d'obtenir une adresse IP WAN ou des sites utilisant le PPoE avec une négociation d'adresse IP.

Procédure

ETAPE 1 Sélectionnez **Configurer** > **Routage** > **Connexion Internet** et ouvrez la fenêtre Modifier la connexion Internet.

ETAPE 2 Complétez le volet **HTTP DDNS** de la fenêtre Modifier la connexion Internet en introduisant les valeurs suivantes :

Champ	Description
Fournisseur	Sélectionnez un fournisseur DDNS dans le menu déroulant. Le compte pour ce fournisseur DDNS doit être défini hors de Configuration Assistant.
Nom de l'hôte	Nom d'hôte unique pour ce site obtenu du fournisseur de services DDNS. Il s'agit généralement d'un nom de domaine complet (FQDN), par exemple mon_hôte.mon_domaine.net, mais cela peut s'avérer différent en présence de certains services DDNS. Le nom d'hôte doit être enregistré. Ce champ n'est pas validé par Configuration Assistant. Veillez à introduire correctement le nom d'hôte selon les instructions de votre fournisseur DDNS. Si vous configurez un déploiement multi-sites, chaque site doit disposer d'un nom d'hôte DDNS unique.
Nom d'utilisateur	Nom d'utilisateur pour le compte obtenu de votre fournisseur de services DDNS.
Mot de passe/ Confirmer le mot de passe	Mot de passe pour le compte obtenu de votre fournisseur de services DDNS. Réintroduisez le mot de passe pour le confirmer.

ETAPE 3 Cliquez sur **OK**.

ETAPE 4 Vérifiez si la modification de la configuration du site a bien déclenché la mise à jour du DNS pour le fournisseur de services DDNS.

Configuration de la qualité de service (QoS)

Les paramètres relatifs à la qualité de service (QoS) pour les déploiements multi-sites vous permettent d'effectuer les opérations suivantes :

- Activer la mise en forme du trafic
- Définir le volume de bande passante pour le chargement disponible pour chaque site
- Définir le pourcentage de bande passante du WAN affecté au trafic VoIP sur le réseau (le cas échéant)
- Utiliser le contrôle des admissions d'appel pour faire en sorte que le nombre d'appels ne dépasse pas l'affectation de la bande passante afin d'éviter toute dégradation.

Lorsque QoS est actif et configuré :

- La priorité est assurée pour le trafic vocal, du moins jusqu'au pourcentage de la bande passante établi à cette fin. Lorsque le trafic vocal dépasse ce pourcentage, le son peut être de moindre qualité pour tous les appels VoIP.
- Le reste de bande passante disponible sur le WAN est utilisé pour l'autre trafic.
- En l'absence de trafic vocal sur le réseau, toute la bande passante disponible peut être utilisée pour le trafic de données.

Consignes importantes

Les consignes suivantes concernent la configuration de QoS :

- Configurez les paramètres QoS avant de définir la valeur Nombre d'appels maximum de sorte que Configuration Assistant puisse établir les paramètres recommandés pour CAC.
- La configuration QoS est facultative, mais fortement recommandée. L'élément est désactivé par défaut.
- QoS doit être configuré séparément pour chaque site. Cet élément ne fait pas partie de la configuration multi-sites exportée grâce au Gestionnaire multi-sites.

- QoS est toujours configuré sur le périphérique connecté à l'Internet.
  - Si l'UC500 est directement connecté au WAN, configurez le QoS sur l'UC500.
  - Si l'UC500 se trouve derrière un SR520-T1, configurez QoS sur le SR520-T1.
- Définissez la bande passante ascendante pour le site en fonction d'un test de vitesse de connexion fiable ou du débit d'informations garanti (Commited Information Rate - CIR) établi dans le Contrat de niveau de service de votre fournisseur d'accès à Internet.

  Si vous n'avez pas accès au CIR et aux résultats du test, définissez une bande passante ascendante représentant environ 80 % de la bande passante ascendante annoncée par votre fournisseur de services.

  Si vous optez pour une valeur supérieure, vous risquez de rencontrer des problèmes au niveau de la qualité du son.

Procédures

ETAPE 1 Accédez à l'option **Configurer** > **Routage** > **Connexion Internet**.

ETAPE 2 Dans le menu **Nom de l'hôte**, sélectionnez le nom d'hôte d'un périphérique relié à Internet (l'UC500 ou le SR520-T1).

ETAPE 3 Cliquez sur une connexion pour la sélectionner.

ETAPE 4 Cliquez ensuite sur **Modifier**.

ETAPE 5 Dans la fenêtre Modifier la connexion Internet, cliquez sur l'onglet Mise en forme du trafic.

ETAPE 6 Cochez la case **Mise en forme du trafic** pour activer la mise en forme.

ETAPE 7 Dans le champ **Bande passante ascendante [kbps]**, définissez la bande passante ascendante pour le site en fonction d'un test de vitesse de connexion fiable ou du débit d'informations garanti (Commited Information Rate - CIR) établi dans le Contrat de niveau de service de votre fournisseur d'accès à Internet. Par exemple, si la vitesse de chargement est de 1,8 Mbps, entrez la valeur 1800 pour la bande passante ascendante.

Vous pouvez entrer des valeurs comprises entre 384 kbps et 100000 kbps.

Si vous ne disposez pas des résultats des tests de vitesse, entrez une valeur en kbps correspondant à 80 % de la bande passante ascendante annoncée par votre fournisseur de services.

ETAPE 8 Dans le champ **Réservation média**, utilisez le curseur pour définir la fraction de bande passante disponible à affecter aux supports vocaux (le cas échéant). Vous pouvez entrer des valeurs comprises entre 1 et 95 % (les 5 % restants sont réservés au signalement et autres éléments). Valeur par défaut : 50 %.

ETAPE 9 Cliquez sur **OK** ou **Appliquer**.

ETAPE 10 Cliquez sur **Configurer** > **Enregistrer la configuration** pour enregistrer la configuration.

Exportation et importation de sites

Une fois les paramètres de connexion configurés pour chaque site, les paramètres sont exportés vers un fichier XML pouvant être importé vers d'autres sites.

Exportation de sites

Pour chaque site, ces paramètres sont exportés :

- Nom du site et index
- Préfixe d'appel inter-sites et nombre de chiffres composant les numéros de poste
- Adresse IP publique ou nom d'hôte pour le site
- Adresse IP et masque de sous-réseau du LAN de données pour le périphérique de périmètre sur le réseau (SR500 ou UC500)
- Adresse IP et masque de sous-réseau de l'UC500 s'il se trouve derrière un routeur sécurisé SR500.

IMPORTANT Pour des raisons de sécurité, la **clé partagée** utilisée pour l'identification du site *n'est pas* incluse dans le fichier de configuration par défaut.

- Si la clé partagée n'est pas exportée dans le fichier de configuration, vous devrez l'introduire manuellement pour chaque site.
- Vous pouvez inclure la clé partagée dans les données de site exportées. La clé partagée est exportée sous forme de texte brut (moins sûr).

Ne modifiez ni ne supprimez les paramètres du fichier XML. Les modifications apportées aux paramètres de configuration doivent être effectuées à l'aide de Configuration Assistant.

Pour exporter les paramètres de connexion multi-sites, procédez comme suit :

ETAPE 1 Cliquez sur **Exporter le fichier de configuration multi-sites**.

ETAPE 2 Enregistrez le fichier de configuration sur votre PC exécutant Configuration Assistant.

Importation de sites

Pour importer les paramètres de connexion multi-sites, procédez comme suit :

ETAPE 1 Connectez le PC sous Configuration Assistant directement au port LAN de l'UC500 pour le site et veillez à ce que le PC ait obtenu l'adresse IP de l'UC500.

ETAPE 2 Démarrez Configuration Assistant et connectez-vous au site.

ETAPE 3 Sélectionnez l'option **Configurer** > **Téléphonie** > **Gestion de site** > **Gestionnaire multi-sites** dans la barre de fonction pour ouvrir le Gestionnaire multi-sites.

ETAPE 4 Si vous n'avez pas encore configuré les connexions multi-sites, cliquez sur **Importer les paramètres de connexion multi-sites** à la page qui s'affiche pour le Gestionnaire multi-sites.

Si vous réimportez les paramètres, cliquez sur **Importer le site** dans la fenêtre principale du Gestionnaire multi-sites.

ETAPE 5 Parcourez l'arborescence jusqu'à l'emplacement choisi pour le fichier de configuration exporté et cliquez sur **OK**.

ETAPE 6 Sélectionnez le site à importer et cliquez sur **OK**.

ETAPE 7 Si les paramètres de site ne correspondent pas à la configuration active du site, Configuration Assistant détecte les différences au niveau de la configuration et vous demande si vous souhaitez effectuer la mise à jour.

Si l'adresse IP du LAN de données doit être reconfigurée sur l'UC500, vous perdrez la liaison avec Configuration Assistant et devrez vous reconnecter à l'aide d'une nouvelle adresse IP.

Modifier un site après la configuration initiale

Vous pouvez modifier les paramètres du site après la configuration initiale. Si tel est le cas, vous devrez effectuer les opérations suivantes :

- Exporter la nouvelle configuration.
- Importer la nouvelle configuration vers tous les sites.

Supprimer un site

Pour supprimer un site d'une configuration multi-sites, suivez les étapes suivantes.

ETAPE 1 Démarrez Configuration Assistant et sélectionnez l'option **Configurer** > **Téléphonie** > **Gestion de site** > **Gestionnaire multi-sites**.

ETAPE 2 Dans la fenêtre Gestionnaire multi-sites, sélectionnez l'onglet Configuration multi-sites.

ETAPE 3 Sélectionnez le site que vous souhaitez supprimer et cliquez sur **Supprimer**.

ETAPE 4 Cliquez sur **OK** pour confirmer la suppression.

ETAPE 5 Cliquez sur **OK** ou **Appliquer**.

Pour supprimer l'intégralité de la configuration multi-sites du périphérique auquel vous êtes connecté(e), suivez les étapes suivantes :

ETAPE 1 Démarrez Configuration Assistant et sélectionnez l'option **Configurer** > **Téléphonie** > **Gestion de site** > **Gestionnaire multi-sites**.

ETAPE 2 Dans la fenêtre Gestionnaire multi-sites, sélectionnez l'onglet Configuration multi-sites.

ETAPE 3 Cliquez sur **Supprimer la configuration multi-sites**. Cette option se trouve dans le coin inférieur droit de la fenêtre Gestionnaire multi-sites. L'option **Supprimer la configuration multi-sites** ne s'affiche que si le Gestionnaire multi-sites détecte une configuration existante (à savoir une configuration qui a au moins été appliquée une fois).

ETAPE 4 Cliquez sur **OK** lorsque le système vous demande si vous souhaitez supprimer l'intégralité de la configuration.

Lorsque vous cliquez sur **OK**, toute la configuration est supprimée du périphérique. La fenêtre Gestionnaire multi-sites est actualisée afin d'afficher la page initiale par défaut sans les paramètres de configuration.

Suivi de l'état multi-sites

Pour surveiller les connexions de tunnel VPN multi-sites et afficher les données de diagnostic, procédez comme suit :

- Sélectionnez l'option **Superviser** > **État multi-sites** dans la barre d'outils ou
- Cliquez sur l'onglet État multi-sites dans le Gestionnaire multi-sites.

La fenêtre État multi-sites se compose de deux parties :

- **Récapitulatif de l'état du tunnel VPN**
- **Détail de l'état du tunnel VPN**

Récapitulatif de l'état du tunnel VPN

Le volet Récapitulatif de l'état du tunnel VPN affiche l'état de chaque connexion aux tunnels VPN pour tous les sites déployés. Si la configuration multi-sites n'a pas été importée et appliquée à un site, la mention "La configuration du site n'a pas encore été appliquée" s'affiche.

Cliquez sur **Connecter à tous les sites** pour afficher manuellement tous les tunnels VPN pour tous les sites.

Détail de l'état du tunnel VPN

Le volet **Détail de l'état du tunnel VPN** affiche le résultat de la commande Cisco IOS **show crypto session detail**. Cette commande dresse la liste de toutes les sessions VPN actives ainsi que des éléments IKE (Internet Key Exchange) et IPsec SA (associations de sécurité) pour chaque session VPN.

Notez les éléments suivants dans le résultat ci-dessous :

- **État de la session**. Affiche l'état du tunnel. Lorsque le tunnel devient actif, l'état est DOWN-NEGOTIATING. Lorsque le tunnel est actif, l'état peut être UP-ACTIVE, UP-NO-IKE ou UP-IDLE. Si l'état de la session est DOWN, le tunnel n'existe pas.
- **FLUX IPSEC**. Informations en direct sur le flux de trafic IPsec. Les adresses IP correspondent aux adresses IP du VLAN de données et aux masques de sous-réseau configurés pour l'UC 500 et le SR 500.

```
État actuel de la session de chiffrement

Code : C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface : Serial1/0:1
--> État de la session : UP-NO-IKE
Poste : 10.130.2.2 port 500 fvrf: (aucun) ivrf: (aucun)
      Desc : (aucun)
      Phase1_id: (aucun)
--> IPSEC FLOW: permit ip 192.168.30.0/255.255.255.0 192.168.20.0/
255.255.255.0
        SA actifs : 2, origin: crypto map
        Inbound:  #pkts dec'ed 335 drop 0 life (KB/Sec) 4429573/683
        Outbound: #pkts enc'ed 335 drop 0 life (KB/Sec) 4429573/683
--> IPSEC FLOW: permit ip 192.168.75.0/255.255.255.0 192.168.20.0/
255.255.255.0
        SA actifs : 0, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0

Interface : Serial1/0:1
État de la session :. UP-NO-IKE
Poste : 10.130.1.2 port 500 fvrf: (aucun) ivrf: (aucun)
      Desc : (aucun)
      Phase1_id: (aucun)
--> IPSEC FLOW: permit ip 192.168.75.0/255.255.255.0 192.168.10.0/
255.255.255.0
        SA actifs : 0, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 0 drop 1 life (KB/Sec) 0/0
--> IPSEC FLOW: permit ip 192.168.30.0/255.255.255.0 192.168.10.0/
255.255.255.0
        SA actifs : 2, origin: crypto map
        Inbound:  #pkts dec'ed 725 drop 0 life (KB/Sec) 4492717/470
        Outbound: #pkts enc'ed 707 drop 1 life (KB/Sec) 4492717/470
. . .
```

Fonctions vocales prises en charge sur plusieurs sites

Le tableau ci-dessous dresse la liste des fonctions vocales les plus fréquentes prises en charge par plusieurs sites en présence d'une configuration multi-sites.

Fonction vocale	Prise en charge sur plusieurs sites
Appel abrégé de base d'un site à un autre	Oui
Transfert d'appel entre les sites	Oui

Fonction vocale	Prise en charge sur plusieurs sites
Téléconférence entre les sites	Oui
Radiomessagerie et parc d'appels entre les sites	Non
Transfert de messages vocaux entre les sites	Non
Standard automatique	Partiel Le Standard automatique peut transférer les appels vers d'autres numéros de poste sur le site grâce à la numérotation abrégée.
Fax entre les sites	Oui
Mobilité de poste entre les sites	Non
Groupements de postes configurés entre les sites	Non* La fonction Groupe d'appel prend en charge la valeur "Autre" qui permet la configuration des groupes d'appel sur plusieurs sites.
Répertoire partagé sur plusieurs sites	Non

Nombre d'appels maximum (Contrôle des admissions d'appel)

Pour accéder aux options de contrôle des admissions d'appel, sélectionnez l'option **Configurer** > **Téléphonie** > **Gestion de site** > **Nombre d'appels maximum**.

Vue d'ensemble

Les paramètres de contrôle des admissions d'appel définissent le nombre maximum d'appels simultanés sur le réseau étendu. Lorsque le contrôle des admissions d'appel est actif et configuré, il concerne tous les appels parcourant le WAN. Cela comprend notamment les appels inter-sites dans un déploiement multi-sites et les appels SIP.

Configurez les paramètres Mise en forme du trafic/QoS avant de définir la valeur Nombre d'appels maximum de sorte que Configuration Assistant puisse établir les paramètres recommandés pour CAC sur la base de ces éléments.

Si vous modifiez la configuration, la valeur **Nombre d'appels maximum** définie à la fenêtre Trunk SIP est elle aussi mise à jour (**Configurer** > **Téléphonie** > **Ports et trunks** > **Trunks SIP)**. Voir la rubrique **Trunks SIP, page 321**.

Procédures

Pour configurer les paramètres de Contrôle des admissions d'appel, procédez comme suit :

ETAPE 1 Sélectionnez l'option **Configurer** > **Téléphonie** > **Gestion de site** > **Nombre d'appels maximum** dans la barre de fonctions pour afficher la fenêtre Nombre d'appels maximum.

ETAPE 2 Sélectionnez un périphérique dans la liste Nom de l'hôte.

ETAPE 3 Dans le champ Nombre d'appels maximum, entrez le nombre maximal d'appels simultanés autorisés.

Si vous entrez la valeur 0, le contrôle des admissions d'appel est désactivé.

Si la fonction QoS est activée et configurée pour le site, procédez comme suit :

- La zone **Mise en forme du trafic actuel** affiche des informations en lecture seule sur les paramètres de mise en forme du trafic actifs sur le système (bande passante ascendante en kbps et pourcentage de la bande passante du WAN garantie pour les appels VoIP).
- La zone **Plages d'appels maximales** présente les valeurs Recommandée, Sensible, Dégradée pour la valeur Nombre d'appels maximum d'après les paramètres QoS en vigueur.

Si le QoS n'est pas actif, sélectionnez l'option **Configurer** > **Routage** > **Connexion Internet** dans la barre de fonctions et sélectionnez la connexion WAN. Cliquez sur **Modifier** et sélectionnez l'onglet Mise en forme du trafic.

ATTENTION Si vous sélectionnez un nombre dans la plage Sensible ou Dégradée pour le paramètre Nombre d'appels maximum, vous risquez de réduire la qualité des appels VoIP (notamment les appels inter-sites) si vous dépassez la bande passante disponible.

ETAPE 4 Entrez le nombre maximum d'appels pour ce site.

ETAPE 5 Cliquez sur **OK**.

16

Applications

Cisco Configuration Assistant permet l'activation et la configuration de Cisco SBCS Smart Applications et d'autres applications tierces pour les plateformes UC500.

Pour certaines applications, des options de configuration sont nécessaires pour l'activation et l'utilisation.

Les rubriques suivantes fournissent des indications sur l'activation et la configuration des paramètres pour les applications Cisco SBCS.

- **Paramètres généraux**
- **Smart Applications Manager**
- **Configuration propre aux applications**

Pour des informations sur les applications tierces Cisco SBCS, rejoignez la communauté Cisco Small Business Support Community à l'adresse

https://supportforums.cisco.com/docs/DOC-9780/

Paramètres généraux

Certaines applications, telles que Cisco WebEx PhoneConnect ou les applications SBCS tierces, nécessitent la configuration des paramètres système généraux. Pour accéder aux paramètres généraux des applications, sélectionnez **Applications** > **Paramètres généraux** dans la barre de fonctions.

Les paramètres généraux pouvant être définis sont décrits dans les rubriques suivantes :

- **URL d'identification**
- **Accès au menu de services**
- **Comptabilisation des appels**

- **Authentification HTTPS**

Pour de plus amples informations sur les paramètres généraux des applications, consultez le manuel de l'application que vous tentez de configurer.

URL d'identification

Cette fenêtre s'affiche lorsque vous sélectionnez **Applications** > **Paramètres généraux** > **URL d'identification** dans la barre de fonctions.

Ce paramètre définit l'URL d'identification CME requise pour une application Cisco SBCS Smart Application ou une application tierce.

Voici quelques exemples d'URL d'identification :

- VoiceView Express

  http://10.1.10.1/voiceview/authentication/authenticate.do

- WebEx PhoneConnect

  http://10.1.10.2/CCMCIP/authenticate.asp.

Une seule URL d'identification peut être utilisée à la fois. Pour configurer une URL d'application et d'identification différente, vous devrez d'abord désactiver l'application exploitant ce paramètre. Vous devrez par exemple désactiver WebEx PhoneConnect si vous souhaitez configurer une adresse d'identification afin d'intégrer une application tierce.

REMARQUE Certaines URL d'identification sont compatibles avec plusieurs applications Cisco SBCS. Par exemple, l'URL d'identification VoiceView Express est également compatible avec l'URL TimeCardView. L'URL de l'application WebEx PhoneConnect est compatible avec VoiceView Express et TimeCardView. Ces applications peuvent être activées simultanément si les ressources sont suffisantes.

Lorsque vous accédez pour la première fois à la fenêtre URL d'identification, l'URL d'identification pour VoiceView Express s'affiche. Ceci est dû au fait que les paramètres par défaut pour VoiceView Express sont **activés**. Configuration Assistant définit automatiquement l'URL d'identification de l'application et l'URL des services CME pour VoiceView Express lorsque le système vocal est initialisé. Pour activer ou désactiver VoiceView Express, sélectionnez l'option **Configurer** > **Téléphonie** > **Utilisateurs et postes** > **Messagerie** et cliquez sur l'onglet Configuration.

Certaines applications n'ont pas besoin d'une URL d'identification. Consultez le manuel de l'application que vous configurez pour connaître l'adresse à introduire. Certaines applications configurent automatiquement l'URL lorsqu'elles sont actives.

Cliquez sur **OK** ou **Appliquer** une fois l'URL d'identification introduite.

Accès au menu de services

Cette fenêtre s'affiche lorsque vous sélectionnez **Applications** > **Paramètres généraux** > **Accès au menu de services** dans la barre de fonctions.

- **Vue d'ensemble**
- **Ajouter une URL de service CME**
- **Modifier ou supprimer une URL de service CME**

Vue d'ensemble

Dans la fenêtre Accès au menu de services, vous pouvez définir le nom de l'élément de menu ainsi que l'URL du service CME et organiser les éléments de menu sur les téléphones IP pour les URL de service paramétrables. Celles-ci sont utilisées par les applications telles que WebEx PhoneConnect, TimeCardView et d'autres applications tierces. Ces éléments de menu s'affichent lorsque l'utilisateur appuie sur le bouton **services** de son téléphone IP.

Vous pouvez configurer jusqu'à 8 URL de service.

Utilisez les flèches **Haut** et **Bas** pour modifier l'ordre d'affichage dans le menu **Services** du téléphone IP.

Seul l'ordre des URL de service CME peut être modifié. Dans le menu **Services** du téléphone IP Cisco, l'URL de service CME s'affiche toujours en premier lieu. Elle est suivie des URL de service CME personnalisables, Mobilité de poste et Mes applications.

IMPORTANT Consultez le manuel de l'application que vous configurez pour définir l'adresse à introduire.

- Certaines applications, telles que WebEx PhoneConnect et VoiceView Express, configurent automatiquement l'URL pour vous.
- Si une URL de service est automatiquement configurée par une application dès son activation, l'URL de service est automatiquement supprimée de la liste lorsque l'application est désactivée. Vous ne pouvez pas modifier ou supprimer les URL de service configurées par ces applications.

Ajouter une URL de service CME

Pour ajouter une nouvelle URL de service CME, procédez comme suit :

ETAPE 1 Cliquez sur **Ajouter** pour ajouter une nouvelle ligne au tableau.

ETAPE 2 Paramétrez le nom de service et l'URL.

Paramètre	Description
Nom de menu	Nom de menu pour le service CME affiché dans le menu Services des téléphones IP Cisco. Le nom de menu peut contenir jusqu'à 15 caractères. Il ne peut contenir aucun espace ni caractère spécial.
URL	URL de service CME, par exemple : http://10.1.10.1/WebExPhone/MainMenu

ETAPE 3 Si plusieurs URL de service CME figurent dans la liste, utilisez les flèches **Haut** et **Bas** pour réorganiser les éléments.

ETAPE 4 Cliquez sur **OK**.

Modifier ou supprimer une URL de service CME

Vous ne pouvez pas modifier ni supprimer les URL de service par défaut automatiquement configurées par les applications SBCS telles que VoiceView Express, TimeCardView ou WebEx PhoneConnect. Vous pouvez cependant désactiver ces applications afin de supprimer les URL de service.

Les URL de service définies par l'utilisateur peuvent quant à elles être supprimées ou modifiées.

- Pour modifier une URL de service personnalisée, cliquez dans la colonne Nom de menu ou URL dans la zone contenant l'URL. Apportez les modifications et cliquez sur **OK** ou **Appliquer**.
- Pour supprimer une URL de service personnalisée, sélectionnez l'adresse dans la liste et cliquez sur **Supprimer**.

Comptabilisation des appels

La fenêtre Comptabilisation des appels s'affiche lorsque vous sélectionnez **Applications** > **Paramètres généraux** > **Comptabilisation des appels** dans la barre de fonctions.

Vue d'ensemble

Cette fenêtre vous permet d'activer ou de désactiver la collecte des données d'appel (CDR) et de définir l'emplacement du serveur TFTP ou FTP externe où les CDR sont stockés ainsi que l'emplacement de sauvegarde sur la mémoire de l'UC500. Ces paramètres sont utilisés conjointement aux applications de comptabilisation des appels qui rassemblent les CDR pour les stocker sur un serveur FTP externe.

Les sauvegardes des fichiers CDR sont conservées dans le dossier cdr/ de la mémoire flash de l'UC500. Cliquez sur **Copier CDR vers fichier** pour copier manuellement les CDR vers l'emplacement de sauvegarde prévu sur la mémoire flash.

Pour plus d'informations, consultez le manuel de l'application de comptabilisation des appels que vous configurez.

Procédures

Configurez les paramètres généraux pour les applications de comptabilisation des appels selon les indications du tableau suivant : Cliquez sur **OK** ou **Appliquer** lorsque vous avez terminé.

Paramètre	Description
Serveur de comptabilisation des appels	
Adresse du FTP	Définit l'emplacement principal pour le stockage des CDR créés pour la comptabilisation. Entrez un chemin/nom pour le fichier à stocker sur le serveur FTP. Par exemple : ftpserver01/cdrs
Nom d'utilisateur	Nom d'utilisateur pour l'identification du serveur FTP
Mot de passe	Mot de passe pour l'identification du serveur FTP

Paramètre	Description
Sauvegarde sur la mémoire flash	

Nom de la sauvegarde sur la mémoire flash	Nom du fichier de base utilisé pour les sauvegardes des CDR dans le dossier \cdr\ de la mémoire flash de l'UC500 (par exemple : `cdr_backups`). Le nom de fichier peut contenir jusqu'à 15 caractères. Les espaces et les caractères spéciaux ne sont pas autorisés.
	
	Le fichier de sauvegarde CDR se voit attribuer un nom unique lors de sa création. Le nom d'hôte du routeur et l'horodatage sont annexés au nom de fichier selon le format *<nom de fichier>.<nom d'hôte>.<horodatage>*.
	
	Par exemple, si le **nom de fichier de sauvegarde sur la mémoire flash** est `cdr_backups`, le chemin et le nom de fichier seront définis selon le format suivant :
	
	`flash:/cdr/`
	`cdr_backups.UC520.07_25_2009_18_15_10.346`

Copier CDR vers fichier	Cliquez sur **Copier CDR vers fichier** pour copier manuellement les données CDR en attente vers l'emplacement de sauvegarde prévu sur la mémoire flash de l'UC500. Un nouveau fichier de sauvegarde est créé sur la mémoire flash lorsque vous cliquez sur **Copier CDR vers fichier**.

Authentification HTTPS

Cette fenêtre s'affiche lorsque vous sélectionnez **Applications** > **Paramètres généraux** > **Authentification HTTPS** dans la barre de fonctions.

Certaines applications, telles que Cisco WebEx PhoneConnect, exigent que vous activiez la liaison HTTPS et introduisiez un nom d'utilisateur et un mot de passe.

Pour plus d'informations, consultez le manuel de l'application que vous configurez.

Configurez les paramètres **Authentification HTTPS** selon les indications du tableau suivant. Cliquez sur **OK** ou **Appliquer** lorsque vous avez terminé.

Paramètre	Description
Activer la communication HTTPS	Lorsque cette fonction est active (cochée), le certificat privé HTTPS utilisé pour la connexion à l'interface PhoneConnect Web Services est créé. Cette option doit être cochée pour WebEx PhoneConnect.
Nom	Nom d'utilisateur pour l'identification HTTPS. Le nom d'utilisateur peut contenir jusqu'à 15 caractères. Les espaces et les caractères spéciaux ne sont pas autorisés. Le paramètre est vide par défaut. Requis pour WebEx PhoneConnect.
Mot de passe	Mot de passe pour l'identification HTTPS. Le mot de passe peut contenir jusqu'à 15 caractères alphanumériques. Les espaces et les caractères spéciaux ne sont pas autorisés. Le paramètre est vide par défaut. Requis pour WebEx PhoneConnect.

Smart Applications Manager

Pour accéder aux options permettant d'activer ou de désactiver les Smart Applications, sélectionnez l'option **Applications** > **Smart Applications Manager** dans la barre de fonctions.

Vue d'ensemble

Dans Smart Applications Manager, vous pouvez activer, désactiver et configurer Cisco SBCS Smart Applications. Ces applications exploitent le module CUE de la plateforme UC500. Vous pouvez aussi voir l'intégralité des ressources disponibles, les ressources requises pour chaque application et l'usage pour chaque application. Les applications accessibles à partir de cette fenêtre sont notamment les suivantes :

- Messagerie unifiée
- Cisco WebEx PhoneConnect
- Cisco TimeCardView

Les ressources système utilisées par l'application sont représentées par un nombre de crédits. Un total de 100 crédits est disponible pour le système. Le nombre total de crédits requis pour chaque application correspond au nombre minimum de crédits nécessaires pour exécuter l'application, sur la base de la mémoire du processeur et de l'espace disque. Certaines applications telles que la visiotéléphonie et l'enregistrement en direct n'exigent aucun crédit. Configuration Assistant affiche une erreur si vous tentez d'activer une application alors que vous ne disposez pas du nombre de ressources nécessaires.

Pour activer ou désactiver une application, procédez comme suit :

ETAPE 1 Dans la liste Applications affichée sur la gauche, cliquez sur l'application que vous souhaitez activer.

Une courte description de l'application s'affichera.

ETAPE 2 Cliquez sur **Configurer** pour accéder aux options permettant d'activer et de configurer l'application.

Consultez les rubriques suivantes pour obtenir des informations sur la configuration de Cisco SBCS Smart Applications :

- **Messagerie unifiée (IMAP), page 525**
- **Cisco WebEx PhoneConnect, page 526**
- **TimeCardView, page 539**.

ETAPE 3 Cliquez sur **OK** ou **Appliquer** lorsque vous avez terminé la configuration des paramètres des applications.

Configuration propre aux applications

Les thèmes abordés dans cette partie offrent un aperçu de chaque application et des consignes pour la configuration des options propres à l'application.

- **Messagerie unifiée (IMAP)**
- **Visiotéléphonie**
- **Cisco WebEx PhoneConnect**
- **TimeCardView**

Messagerie unifiée (IMAP)

La fenêtre Configuration de la messagerie unifiée s'affiche lorsque vous sélectionnez l'option Messagerie unifiée dans la liste Applications de la fenêtre Smart Applications Manager et cliquez sur **Configurer**.

Vue d'ensemble

La Messagerie unifiée permet aux utilisateurs de la messagerie vocale d'obtenir un panorama complet de leurs courriers électroniques et de leurs messages vocaux à partir d'un même client de messagerie grâce au protocole IMAP. Les utilisateurs pourront supprimer les messages vocaux ou les marquer comme lus ou non lus à l'instar des e-mails. Les messages vocaux sont téléchargés sous forme d'annexes aux courriers électroniques. Les utilisateurs peuvent accéder aux messages vocaux par le réseau ou les télécharger de manière sélective. Par défaut, cette fonction est désactivée.

Procédures

Activation ou désactivation de la messagerie unifiée

Pour activer ou désactiver la messagerie unifiée, cochez la case **Activer la messagerie unifiée** et cliquez sur **OK** pour revenir à la fenêtre Smart Applications Manager.

Configuration du client IMAP

Pour que l'utilisateur puisse profiter de cette fonction, son client de messagerie (par exemple, Microsoft Outlook) doit être configuré de sorte à utiliser le protocole IMAP. Lorsque vous configurez le client pour utiliser IMAP, respectez les consignes suivantes :

- Utilisez l'adresse IP du module Cisco Unity Express (CUE) (10.1.10.1) pour l'adresse IP du serveur IMAP.
- Le nom d'utilisateur et le mot de passe configurés sur le client IMAP et utilisés pour l'authentification doivent correspondre au nom d'utilisateur et au mot de passe de l'utilisateur configuré sous Cisco Configuration Assistant.

Visiotéléphonie

La solution Cisco Unified Video Advantage (CUVA) de SBCS permet aux utilisateurs d'effectuer des appels de visiotéléphonie de poste à poste grâce aux téléphones IP Cisco prenant en charge la vidéo.

La visiotéléphonie est activée par défaut. Pour désactiver cette fonction, désactivez l'option **Activer la visiotéléphonie** et cliquez sur **OK**.

Vous pourrez établir si les appels vidéo sont autorisés sur certains téléphones en activant ou désactivant l'option **Autoriser les appels vidéo** pour chacun d'entre eux. Voir la rubrique **Autoriser les appels vidéo, page 330**.

Cisco WebEx PhoneConnect

WebEx PhoneConnect est conçu pour les clients qui souhaitent un accès rapide et simple aux réunions WebEx à partir de leur téléphone IP sans devoir utiliser leur PC de bureau. WebEx PhoneConnect automatise le processus de sorte que les utilisateurs de téléphones IP puissent rejoindre la discussion lors d'une conférence WebEx par une simple pression sur une touche de leur téléphone IP. Cette partie couvre les rubriques suivantes :

- **A propos de Cisco WebEx PhoneConnect**
- **Caractéristiques techniques de la plateforme SBCS**
- **Documents connexes**
- **Données du compte Administrateur du site WebEx**
- **Procédures**

A propos de Cisco WebEx PhoneConnect

Une fois que l'utilisateur WebEx est associé à un téléphone IP grâce à WebEx PhoneConnect, une application simple s'affiche à l'écran de leur téléphone IP Cisco. Elle lui permet d'effectuer les opérations suivantes :

- Dresser la liste des conférences WebEx qu'il anime
- Dresser la liste des conférences WebEx auxquelles il est invité par d'autres utilisateurs de téléphones IP de son entreprise (les utilisateurs doivent partager le même routeur UC 500).
- Obtenir des alertes visuelles et sonores sur son téléphone IP lorsqu'il est l'heure d'intégrer la réunion
- Paramétrer les rappels pour les conférences
- Utiliser un raccourci pour participer à une réunion

Les utilisateurs WebEx ayant accès au client WebEx Connect à partir d'un ordinateur de bureau peuvent utiliser la fonction Click-to-Call de leur téléphone IP pour appeler automatiquement un membre de sa liste d'amis WebEx Connect.

Caractéristiques techniques de la plateforme SBCS

Composant	Version
Cisco Configuration Assistant (CCA)	2.0 ou supérieur
Paquet logiciel de l'UC500	7.0(3) ou supérieur
Cisco IOS	12.4(20)T2 ou supérieur Cisco Unified Communications Manager Express (CME) 7.0 ou supérieur
Cisco Unity Express (CUE)	CUE 7.0 ou supérieur
Téléphones IP Cisco pris en charge	Téléphones IP Cisco Unified 794x, 796x et 797x Téléphones sans fil Cisco Unified 7921 et 7925 Téléphone IP Cisco Unified 7937 Téléphone IP Cisco Unified 524G Téléphone IP Cisco Unified 521G Téléphones IP Cisco SPA525G et SPA525G2 Client pour téléphone logiciel Cisco IP Communicator (CIPC)

Documents connexes

Pour de plus amples informations sur la configuration et la gestion de WebEx PhoneConnect, consultez le *Guide d'administration de Cisco WebEx PhoneConnect*.

Les informations et les instructions pour l'utilisateur final figurent dans le *Guide de référence rapide pour Cisco WebEx PhoneConnect*.

Données du compte Administrateur du site WebEx

Avant d'activer et de configurer l'application WebEx PhoneConnect, votre client doit disposer d'un compte WebEx de type Petite entreprise ou en obtenir un auprès d'un administrateur.

- Votre client devra vous fournir les coordonnées du service WebEx (ID de l'administrateur et mot de passe, ID de site et adresse de site).

  CCA utilise ces données pour se connecter au site WebEx du client et pour associer les comptes d'utilisateur WebEx du client à l'application WebEx PhoneConnect.

- Vous devez connaître les règles en matière de mot de passe pour le site.

  Lorsqu'un site WebEx est configuré, l'administrateur du site peut définir les règles pour le mot de passe. Ces règles établissent les critères à respecter pour les mots de passe, à savoir le nombre minimum et maximum de caractères, la difficulté du mot de passe, les caractères à éviter, etc. Tous les mots de passe des utilisateurs WebEx doivent respecter ces critères.

Avant de commencer

Avant de configurer WebEx PhoneConnect, veillez à respecter les conditions suivantes :

- Les numéros de téléphone et les numéros de poste doivent être configurés sur le système (**Configurer** > **Téléphonie** > **Utilisateurs et postes > Utilisateurs et téléphones** > **Postes utilisateurs**).
- Le Plan de numérotation et les trunks vocaux doivent être configurés et les appels entrants/sortants doivent fonctionner.
- L'adresse IP du serveur DNS doit être configurée. WebEx PhoneConnect doit utiliser l'adresse IP du serveur DNS du fournisseur d'accès pour localiser le serveur webex.com.
- Le serveur NTP doit être configuré (facultatif, mais conseillé pour la synchronisation des heures des réunions et des alertes).

Procédures

Lisez la rubrique suivante pour obtenir une description des étapes de configuration. Pour obtenir des informations plus détaillées, consultez le *Guide d'administration pour Cisco WebEx PhoneConnect* disponible sur Cisco.com.

Pour configurer Cisco WebEx PhoneConnect, procédez comme suit :

ETAPE 1 Démarrez Cisco Configuration Assistant et connectez-vous à l'UC 500.

ETAPE 2 Sélectionnez **Applications > Paramètres généraux > URL d'identification** dans la barre de fonctions. Configurez les éléments suivants dans la fenêtre URL d'identification :

a. Vérifiez si l'adresse `http://10.1.10.2/CCMCIP/authenticate.asp` est utilisée. Apportez les modifications si ce n'est pas le cas.

b. Cliquez sur **OK**.

ETAPE 3 Sélectionnez **Applications** > **Paramètres généraux** > **Authentification HTTPS** dans la barre de fonctions.

ETAPE 4 Configurez les éléments suivants dans la fenêtre Authentification HTTPS :

a. Cochez la case **Activer la communication HTTPS** (requis).

b. Entrez un nom d'utilisateur et un mot de passe pour l'identification HTTPS (requis).

c. Cliquez sur **OK**.

Les valeurs pour le champ URL de service CME sont intégrées automatiquement pour WebEx PhoneConnect dès l'activation de l'application PhoneConnect.

ETAPE 5 Accédez à **Applications** > **Smart Applications Manager**.

ETAPE 6 Cliquez sur **WebEx Phone Connect** pour sélectionner l'application et ensuite sur **Configurer**. La fenêtre de connexion pour la configuration de PhoneConnect s'affiche.

ETAPE 7 Dans la fenêtre de connexion pour la configuration de PhoneConnect, entrez le nom d'utilisateur de l'administrateur WebEx du client, le mot de passe, l'identifiant du site et l'adresse du site. Cliquez ensuite sur **OK**. Voir la rubrique **Fenêtre de connexion pour la configuration de PhoneConnect, page 530**.

Une fois que les codes d'accès ont été vérifiés, la fenêtre principale de l'application PhoneConnect s'affiche. Elle contient les informations relatives au site WebEx.

ETAPE 8 Dans la fenêtre principale de l'application PhoneConnect, cochez la case **Activer** en haut de la fenêtre et configurez les paramètres du site. Voir la rubrique **Fenêtre principale de l'application PhoneConnect, page 530**.

ETAPE 9 Ajoutez des utilisateurs et activez WebEx PhoneConnect sur leur téléphone IP Cisco selon les instructions figurant dans le *Guide d'administration pour Cisco WebEx PhoneConnect*. Voir la rubrique **Fenêtre principale de l'application PhoneConnect, page 530**.

ETAPE 10 Cliquez sur **OK** pour appliquer les paramètres du site et fermer la fenêtre.

ETAPE 11 Cliquez sur **OK** dans la fenêtre Smart Applications Manager.

Voir **Configuration de site avancée pour PhoneConnect, page 537** pour obtenir des informations sur les paramètres supplémentaires à configurer.

Fenêtre de connexion pour la configuration de PhoneConnect

Pour configurer PhoneConnect, vous devez d'abord vous connecter en tant qu'administrateur sur le site WebEx (voir ci-dessous).

Paramètre	Description
ID utilisateur	Identifiant de l'administrateur pour le site WebEx. Également appelé "ID WebEx".
Mot de passe	Mot de passe de l'administrateur pour le site WebEx.
ID site	Numéro du site WebEx (les caractères textuels ne sont pas acceptés dans ce champ).
Nom du site	Nom du site WebEx (première chaîne de caractères affichée sur le site WebEx). Par exemple, si l'adresse du site WebEx est http://acme.webex.com, entrez "acme" comme nom de site.

Lorsque vous avez terminé d'introduire les codes d'accès, cliquez sur **OK**.

Fenêtre principale de l'application PhoneConnect

Cette fenêtre s'affiche lorsque vous avez correctement introduit les codes de l'administrateur après avoir cliqué sur **Options de configuration** pour WebEx PhoneConnect dans la fenêtre Smart Applications Manager.

Configurez les paramètres de la fenêtre principale de l'application PhoneConnect selon les indications ci-dessous. Cliquez sur **OK** ou **Appliquer** lorsque vous avez terminé.

Paramètre	Description
Données de l'administrateur chez le client Coordonnées de l'administrateur du site WebEx.	
Prénom	Prénom de l'administrateur pour le site WebEx.
Nom	Nom de l'administrateur pour le site WebEx.
E-mail	Adresse e-mail de l'administrateur pour le site WebEx.
Société	Nom de l'entreprise de l'administrateur pour le site WebEx.
Téléphone	Numéro de téléphone de l'entreprise de l'administrateur pour le site WebEx.
Coordonnées des utilisateurs WebEx	
ID utilisateur	Requis. Il s'agit du code utilisateur pour le compte WebEx que l'utilisateur doit introduire lorsqu'il se connecte au service WebEx afin de planifier et parcourir les réunions ainsi que pour y participer. Format recommandé : *<ID utilisateur du téléphone>@<admindomain>*.com Tous les utilisateurs WebEx créés par PhoneConnect doivent utiliser le format d'adresse e-mail correspondant à leur ID utilisateur. Les comptes d'utilisateur WebEx créés avant l'activation de PhoneConnect peuvent continuer à utiliser le format d'identifiant existant. Si les utilisateurs de votre client partagent le même domaine de messagerie, mieux vaut ajouter le domaine de messagerie après l'identifiant du téléphone et utiliser cette combinaison comme identifiant utilisateur (par exemple : mdupont@durant.com).

Paramètre	Description
Mot de passe	Requis. Il s'agit du mot de passe que l'utilisateur doit introduire lorsqu'il se connecte au service WebEx afin d'animer, participer ou parcourir les réunions. Lorsqu'un site WebEx est configuré, l'administrateur du site peut définir les règles pour le mot de passe. Les règles établissent des critères pour les mots de passe des utilisateurs : nombre de caractères, mots de passe interdits, etc. Tous les mots de passe des utilisateurs doivent respecter les règles en vigueur pour le site WebEx de votre client. Veillez à signaler aux utilisateurs tout changement de mot de passe.
E-mail	Requis. Il s'agit de l'adresse e-mail à laquelle les invitations aux réunions WebEx et les avis WebEx seront envoyés. Si l'utilisateur n'a pas d'adresse e-mail (par exemple, si l'utilisateur désigne une salle de conférence), le format suivant est recommandé : <*ID utilisateur du téléphone*>@<*admindomain*>.com où <*ID utilisateur du téléphone*> correspond à l'ID utilisateur du téléphone repris dans le champ Utilisateur du téléphone associé.
Nom	Requis. Prénom de l'utilisateur pour le site WebEx.
Prénom	Requis. Nom de l'utilisateur pour le site WebEx.
Téléphone associé	Lecture seule. Affiche l'identifiant utilisateur du téléphone associé au compte WebEx. Si aucun identifiant n'est associé à l'utilisateur de WebEx PhoneConnect, la valeur -Aucun- s'affiche.

Paramètre	Description
Sélectionner le téléphone	Cliquez sur **Sélectionner le téléphone** pour afficher une boîte de dialogue permettant la sélection du téléphone à associer au compte utilisateur WebEx et l'activation de l'application PhoneConnect sur le téléphone. Voir la rubrique **Sélectionner le téléphone, page 536**. Si l'utilisateur dispose d'un compte WebEx, si un téléphone a été configuré sur le système et si PhoneConnect n'est pas actif sur son téléphone, vous pouvez utiliser l'option Sélectionner le téléphone pour activer la fonction PhoneConnect sur le téléphone. **IMPORTANT** : Si vous modifiez un compte utilisateur WebEx afin d'activer PhoneConnect, vous devez affecter à l'utilisateur WebEx un nouveau mot de passe (cet élément est important afin de permettre à PhoneConnect d'identifier l'utilisateur). Veillez à envoyer le nouveau mot de passe pour le compte WebEx à l'utilisateur.
Ajouter	Permet d'insérer une nouvelle ligne à la liste des utilisateurs WebEx afin d'ajouter un nouvel utilisateur.
Supprimer	Permet de supprimer l'utilisateur WebEx sélectionné. L'utilisateur passe en mode "Désactivé" sur le site WebEx. Une fois le compte utilisateur supprimé, l'utilisateur n'a plus accès à WebEx ou WebEx PhoneConnect. L'utilisateur ne recevra plus les invitations aux conférences ni les alertes. Il ne pourra plus participer ni animer les conférences WebEx à partir du site WebEx. Pour réintroduire un utilisateur supprimé (par exemple, si l'utilisateur quitte l'entreprise et la réintègre ensuite), vous pouvez utiliser son ancien identifiant ainsi que les données du compte. Vous devez toutefois créer un mot de passe car WebEx peut être paramétré de telle sorte à refuser un mot de passe identique à l'un des trois derniers utilisés sous WebEx.

Paramètre	Description
Copier à partir du périphérique	**Copier à partir du périphérique** représente un autre moyen d'ajouter des utilisateurs WebEx. Cliquez sur **Copier à partir du périphérique** pour afficher une fenêtre qui vous permettra de sélectionner les utilisateurs à associer à ce compte WebEx. Le prénom, le nom, le mot de passe et le téléphone de chaque utilisateur sont copiés vers la liste des utilisateurs WebEx. Les champs réservés à l'identifiant utilisateur et à l'adresse e-mail demeurent vierges. Voir la rubrique **Copier à partir du périphérique, page 536**.
Données de configuration du site client	
Installation des fichiers de langue	Ajoutez une nouvelle langue pour le navigateur et les alertes WebEx PhoneConnect des utilisateurs des téléphones IP. Seuls les écrans des téléphones WebEx PhoneConnect sont concernés par cette procédure. Voir la rubrique **Installer un fichier de langue pour WebEx PhoneConnect, page 538**.
Configuration avancée	Accédez aux paramètres de configuration avancés. Voir la rubrique **Configuration de site avancée pour PhoneConnect, page 537**.
Configuration de l'accès à une conférence	
Préférence pour l'accès à une conférence	Utilisez un numéro gratuit ou payant pour rejoindre les conférences WebEx. La valeur par défaut est Gratuit.
Préfixe pour les appels sortants	Numéros à composer pour obtenir la ligne extérieure. La valeur par défaut est le code d'accès pour les appels sortants défini sur le système. Vous pouvez modifier ce paramètre.
Conversion de numéro d'accès à la conférence - Numéro gratuit ou numéro payant Selon l'origine de l'appel, le plan de numérotation sortant et le format du numéro d'accès à la conférence, vous pourrez utiliser ces paramètres pour supprimer ou remplacer les préfixes tels que les codes nationaux, locaux ou internationaux.	

Paramètre	Description
Numéro fourni par WebEx	Lecture seule. Numéro de téléphone fourni par WebEx pour le site.
Nombre de numéros à supprimer à l'avant	Nombre de numéros à supprimer du numéro fourni par WebEx. Ce champ est obligatoire et ne peut dès lors pas rester vierge. La valeur par défaut est 0. Entrez le nombre de chiffres à supprimer ou remplacer afin de respecter les critères définis pour le numéro d'appel sortant.
Ajouter des chiffres à l'avant	Chiffres à ajouter avant le numéro d'appel fourni par WebEx. Le code peut contenir jusqu'à 20 chiffres. La valeur par défaut est Aucun (vide). Entrez les chiffres à ajouter avant le numéro. Par exemple, un préfixe différent de celui composant le numéro fourni par WebEx. Vous ne devez pas ajouter le préfixe pour appel sortant (code d'accès). Le préfixe pour appel sortant est automatiquement ajouté devant le numéro.
Nombre de numéros à composer	Numéro à appeler après l'ajout et la suppression de chiffres et l'intégration du préfixe d'appel sortant. Le numéro affiché est en lecture seule et créé à l'aide du Préfixe pour les appels sortants ainsi que les valeurs introduites dans les champs Préfixe pour les appels sortants et Supprimer/Ajouter des chiffres. Vérifiez si le numéro correspond à celui que les utilisateurs composent pour joindre le service WebEx.

Sélectionner le téléphone

Cette fenêtre s'affiche lorsque vous cliquez sur l'option **Sélectionner le téléphone** dans la liste des utilisateurs WebEx de la fenêtre principale de l'application PhoneConnect.

ETAPE 1 Dans la fenêtre Sélectionner le téléphone, sélectionnez un téléphone dans la liste pour l'associer à l'utilisateur WebEx PhoneConnect.

Seuls les téléphones permettant l'accès à PhoneConnect sont repris dans la liste.

ETAPE 2 Cliquez sur **OK** pour revenir à la fenêtre principale de l'application PhoneConnect.

Copier à partir du périphérique

Cette fenêtre s'affiche lorsque vous cliquez sur l'option **Copier à partir du périphérique** dans la liste des utilisateurs WebEx de la fenêtre principale de l'application PhoneConnect.

L'option **Copier à partir du périphérique** permet d'ajouter facilement des comptes WebEx et d'activer PhoneConnect pour les utilisateurs existants. Lorsque vous utilisez la fonction **Copier à partir du périphérique**, les valeurs intégrées au préalable sont automatiquement copiées dans les champs du compte utilisateur WebEx adéquat.

Pour utiliser la fonction **Copier à partir du périphérique**, procédez comme suit :

ETAPE 1 Sélectionnez au moins un utilisateur auquel vous souhaitez associer un compte WebEx. Seuls les téléphones non associés à un compte utilisateur WebEx sont repris dans la liste.

ETAPE 2 Cliquez sur **Sélectionner tout** ou utilisez la combinaison CTRL+clic ou MAJ+clic pour sélectionner plusieurs utilisateurs.

ETAPE 3 Cliquez sur **Ajouter** pour déplacer les utilisateurs vers la sélection.

ETAPE 4 Cliquez sur **OK**.

L'identifiant utilisateur, le prénom, le nom, l'adresse e-mail et le téléphone associé à chaque utilisateur existant sont copiés vers les listes d'utilisateurs WebEx de la fenêtre principale de l'application PhoneConnect. Le mot de passe reste vide.

ETAPE 5 Dans la fenêtre principale de l'application PhoneConnect, vous devrez localiser les utilisateurs que vous venez d'ajouter et remplir le champ mot de passe.

Dès qu'un téléphone IP est associé à un utilisateur WebEx, il peut exploiter le système PhoneConnect. Les téléphones IP ne doivent pas redémarrer. Les menus ouverts sur les téléphones doivent être fermés pour afficher les modifications.

Configuration de site avancée pour PhoneConnect

Pour accéder aux paramètres de configuration avancée de WebEx PhoneConnect, cliquez sur **Configuration de site avancée** dans la fenêtre principale de l'application PhoneConnect.

Vous pourrez utiliser les paramètres par défaut dans la plupart des cas. Vous devrez apporter des modifications si vous rencontrez des problèmes avec WebEx PhoneConnect.

Configurez les paramètres de site avancés pour l'application WebEx PhoneConnect selon les consignes ci-dessous. Cliquez sur **OK** ou **Appliquer** lorsque vous avez terminé la configuration des paramètres du téléphone.

Paramètre	Description
Configuration de la temporisation de l'application	
Contrôle de la présence de nouvelles conférences (minutes)	Fréquence des sondages des conférences WebEx. La valeur par défaut est 4 minutes. Si vous diminuez la fréquence sous 4 minutes, vous risquez de compromettre les performances de Cisco Unity Express (CUE).
Délai avant la communication de la référence de la conférence (secondes)	Délai d'attente du système en secondes après la pression sur le bouton d'appel du téléphone IP avant la saisie automatique de la référence de la conférence. La valeur par défaut (10 secondes) se base sur la liaison au trunk FXO/BRI/PRI. Cette valeur peut être augmentée à 7 secondes en cas d'utilisation des trunks SIP. Cet intervalle devra sans doute être augmenté dans le cas des appels internationaux. Cela n'a aucune influence sur les performances.

Paramètre	Description
Délais entre les numéros (millisecondes)	Vitesse à laquelle les numéros sont composés lors de l'introduction de la référence de la conférence. La valeur par défaut est 200 ms. Vous devrez sans doute augmenter l'intervalle selon la destination de l'appel (par exemple, en cas d'appel international). Cela n'a aucune influence sur les performances.
Réinitialiser les données du site WebEx	Cliquez sur **Réinitialiser les données du site WebEx** pour supprimer toutes les données relatives au site WebEx de l'UC500. Cela n'affecte pas le site du service WebEx ou les données de compte. Cette opération supprime les paramètres de l'application WebEx PhoneConnect et les données de site stockées sur le Cisco UC500. L'application PhoneConnect est supprimée de tous les téléphones des utilisateurs. Cela peut s'avérer nécessaire notamment dans les cas où des données de site erronées seraient importées vers l'UC500, lorsque le site WebEx varie, lorsque le site n'est plus actif ou lorsque les données du site de démonstration doivent être supprimées.

Installer un fichier de langue pour WebEx PhoneConnect

Pour installer un nouveau fichier de langue pour WebEx PhoneConnect, cliquez sur **Installer un fichier de langue** dans la fenêtre principale de l'application PhoneConnect.

WebEx PhoneConnect prend en charge la localisation de l'interface des téléphones IP pour le navigateur WebEx PhoneConnect et pour les alertes. Entre chaque version, Cisco prévoit la prise en charge de nouvelles langues. Vous pouvez mettre à jour l'application WebEx PhoneConnect en y intégrant de nouvelles langues grâce à la fonction Installer un fichier de langue. Une fois que le fichier de langue est installé et que la langue est sélectionnée dans Configuration Assistant, tous les menus du téléphone IP pour WebEx PhoneConnect s'afficheront dans la langue sélectionnée.

Avant de commencer, vous devrez localiser l'UC500 en fonction de la région et de la langue souhaitées (**Configurer** > **Téléphonie** > **Système** > **Région**) et télécharger ensuite le fichier de localisation WebEx correspondant à la langue en question.

REMARQUE WebEx PhoneConnect ne prend pas en charge les fonctions d'écrasement du fichier de localisation de l'UC500. WebEx PhoneConnect n'affiche que la langue par défaut sélectionnée.

Suivez les étapes suivantes pour ajouter une nouvelle langue à WebEx PhoneConnect.

ETAPE 1 Dans le champ **Fichier à installer**, accédez au fichier de langue que vous souhaitez installer et cliquez sur **Ouvrir**.

ETAPE 2 Cliquez sur **Installer**. Le nouveau fichier de langue se déplace vers la liste Fichiers de langue installés. Vous pouvez écraser un fichier de langue existant mais ne pouvez pas le supprimer.

ETAPE 3 Cliquez sur **OK** pour déployer le fichier de langue vers le dossier de localisation de CME et revenir à la fenêtre principale de l'application PhoneConnect.

Vous pouvez redémarrer le module CUE sur l'UC500.

ETAPE 4 Pour redémarrer le module CUE de l'UC500, ouvrez la Fenêtre Topologie, cliquez avec le bouton droit sur l'UC500 et sélectionnez l'option **Redémarrer CUE** dans le menu.

Le redémarrage CUE peut prendre de 10 à 15 minutes. Au cours de cette période, la messagerie, le Standard automatique et les autres applications exigeant une connexion à CUE ne seront pas disponibles.

TimeCardView

Cette fenêtre s'affiche lorsque vous sélectionnez l'option TimeCardView dans la liste Applications de la fenêtre Smart Applications Manager et cliquez sur **Configurer**.

IMPORTANT Cette rubrique ne concerne que la configuration de TimeCardView et du serveur de paiement des salaires pouvant être effectuée par Configuration Assistant. Pour de plus amples informations, consultez les documents repris dans la section **Manuels pour TimeCardView, page 540**.

TimeCardView est un système de suivi du temps et des présences destinés aux utilisateurs de téléphone IP reliés aux plateformes Cisco SBCS.

- **Vue d'ensemble**
- **Manuels pour TimeCardView**
- **Caractéristiques techniques de la plateforme SBCS**
- **Configuration de TimeCard**
- **Configuration du serveur de paiement des salaires**

Vue d'ensemble

TimeCardView assure automatiquement le suivi des heures de travail des employés et permet aux superviseurs d'afficher leur état en temps réel. Il permet le suivi et la validation en ligne des horaires et la création de rapports destinés aux superviseurs et aux responsables du paiement des salaires. Ces rapports sont accessibles par le Client Historique et rapports, lesquels pourront être exportés aux formats .csv ou .xls.

TimeCardView permet aux employés d'utiliser un téléphone Cisco Unified IP relié à Cisco Unity Express pour assurer automatiquement le suivi des heures de travail (début et fin de pause, pause-déjeuner et pauses-café) et passer en revue les heures relatives aux pauses, journées, semaines et mois.

Les superviseurs et les responsables du paiement des salaires utilisent TimeCardView pour définir les limites de temps que les employés doivent respecter, afficher l'état des pauses et valider les fiches de présence.

TimeCardView pourra éventuellement être combiné aux logiciels de comptabilité tels que Inuit QuickBooks de sorte que les données des fiches de présence soient facilement transmises au système de comptabilité.

REMARQUE TimeCardView n'est pas pris en charge par tous les modèles de téléphone IP Cisco. Le nombre maximum d'utilisateurs TimeCardView est limité au nombre maximum d'utilisateurs pouvant être pris en charge par la plateforme Cisco SBCS.

Manuels pour TimeCardView

Les manuels pour TimeCardView suivants sont disponibles sur Cisco.com :

- Pour de plus amples informations sur la configuration de TimeCardView et la gestion des utilisateurs, consultez le guide *TimeCardView 7.0*.
- Les informations et les instructions pour l'utilisateur final figurent dans le *Guide de référence rapide pour TimeCardView 7.0*.

Caractéristiques techniques de la plateforme SBCS

- Cisco Configuration Assistant (CCA) 2.0 ou supérieur
- Paquet logiciel UC500 7.0(3) ou supérieur
  - Cisco IOS 12.4(20)T2 ou supérieur
  - Cisco Unified Communications Manager Express (CME) 7.0 ou supérieur
  - Cisco Unity Express (CUE) CUE 7.0.1 ou supérieur

Configuration de TimeCard

Sous l'onglet Configuration TimeCard, vous pouvez configurer les paramètres d'administration de l'application TimeCardView selon les consignes ci-dessous. Cliquez sur **OK** ou **Appliquer** lorsque vous avez terminé.

Paramètre	Description
Nombre max. de sessions	Nombre maximum de sessions TimeCardView, soit 2 ou 8 en fonction de la plateforme. 2 est la valeur par défaut.
E-mails de notification	Adresse e-mail à la norme RFC-2822 utilisée pour les e-mails de notification de l'application (par exemple : nom@société.com).
Délai d'expiration de l'application de téléphone IP du superviseur (60-600 secondes)	Laps de temps (en secondes) s'écoulant avant la déconnexion automatique du superviseur défini par le système.
Délai d'expiration de l'application de téléphone IP de l'employé (60-600 secondes)	Laps de temps (en secondes) s'écoulant avant la déconnexion automatique de l'employé défini par le système.
Durée max. d'une journée de travail (1-1440 minutes)	Durée maximale en minutes au cours de laquelle l'employé peut rester au travail.

Paramètre	Description
Durée max. des heures supplémentaires sur une journée (0-1440 minutes)	Nombre maximum de minutes supplémentaires par joueur autorisé pour l'employé. Si vous modifiez la valeur par défaut, n'oubliez pas de limiter le nombre des heures de travail standard. Dans le cas contraire, les employés ne pourront pas cumuler d'heures supplémentaires. 0 est la valeur par défaut.
Durée max. d'une journée en pause (1-1440 minutes)	Durée maximale en minutes au cours de laquelle l'employé peut rester au travail. 1440 est la valeur par défaut.
Durée max. des pauses sur une journée (1-1440 minutes)	Durée maximale en minutes au cours de laquelle l'employé peut rester en pause. 1440 est la valeur par défaut.
Durée max. du déjeuner sur une pause (1-1440 minutes)	Durée maximale en minutes au cours de laquelle l'employé peut rester en pause-déjeuner. 1440 est la valeur par défaut.
Début du travail	Jour débutant la semaine de travail. Lundi est la valeur par défaut.

Configuration du serveur de paiement des salaires

Sous l'onglet Configuration du serveur de paiement des salaires, complétez les champs décrits ci-dessous si vous souhaitez intégrer Intuit Quick Books à TimeCardView. Lorsque vous avez terminé la configuration des paramètres du serveur, cliquez sur **OK**.

Paramètre	Description
Configuration du serveur Quick Books	
Nom de l'hôte	Serveur de paiement des salaires QuickBooks. Adresse IP ou nom DNS du serveur de paiement des salaires.
Port	Numéro de port du serveur Quick Books. La valeur par défaut est 57343.

Paramètre	Description
Programmes de synchronisation	
Jour de la semaine	Jour de la semaine pour la synchronisation des données TimeCardView et QuickBooks. Valeur par défaut : Quotidien
Heure (HH:MM 24-hr)	Heure de la synchronisation. Valeur par défaut : (aucun) Exemple : 23:00
Fiches de présence comprises	Possibilité d'inclure toutes les fiches ou uniquement les fiches validées. Sélectionner tout ou Approuvé Valeur par défaut : Toutes les fiches de présence
Purger les programmes	
Nombre de jours entre les purges	Nombre de jours minimum entre les purges de la base de données. Plage de valeurs : 1 - 365 jours Valeur par défaut : 90
Jours de conservation	Nombre de jours minimum de conservation des données. Plage de valeurs : 1 - 365 jours Valeur par défaut : 90

17

Maintenance

Cette partie traite des opérations de maintenance pouvant être effectuées à l'aide de Configuration Assistant.

- **Paquets logiciels et paquets de localisation pour Cisco UC500**
- **Afficher les données de version du logiciel et les propriétés du périphérique**
- **Mises à jour des logiciels**
- **Mise à niveau de la messagerie (UC560)**
- **Gestion des fichiers**
- **Redémarrer/réinitialiser les périphériques**
- **Localisation de l'UC500 (paramètres hors USA/UK)**
- **Gestion des licences**
- **Gestion des charges de téléphone**

Voir **Sauvegarde et restauration d'une configuration de périphérique, page 120** pour les instructions sur l'utilisation des fonctions de sauvegarde et de restauration accessibles à partir de l'option Maintenance de la barre de fonctions.

Paquets logiciels et paquets de localisation pour Cisco UC500

Consultez les rubriques suivantes pour en savoir plus à propos du logiciel et des paquets de localisation pour l'UC500 :

- **Paquets logiciels de l'UC500**
- **Paquets de localisation pour l'UC500**
- **Téléchargement des paquets logiciels et des paquets de localisation pour Cisco UC500**

Paquets logiciels de l'UC500

Les paquets logiciels pour l'UC500 sont des fichiers .zip volumineux contenant tous les fichiers nécessaires pour la plateforme UC500 ainsi que les fichiers de localisation. La langue par défaut de l'UC500 est l'anglais (Etats-Unis).

D'autres paquets logiciels sont disponibles pour les plateformes UC520, UC540 et UC560. Vous devez télécharger le fichier .zip correspondant à votre plateforme UC500.

Le paquet logiciel de l'UC500 contient tous les fichiers nécessaires ainsi que les fichiers de langue et de téléphone pour l'anglais (Etats-Unis). Les fichiers s'intitulent UC5xx_8.1.0 .zip.

Chaque fichier .zip contient plusieurs fichiers .TAR pour le composant de l'UC500, à savoir :

- L'image Cisco IOS pour la plateforme UC500
- Les fichiers du microprogramme du téléphone IP
- Les fichiers Communications Manager Express (CME)
- Le logiciel de la messagerie vocale Cisco Unity Express (CUE)
- Configuration d'usine pour tous les SKU
- Les fichiers pour les invites et les scripts Basic ACD, les sonneries et les images pour le bureau
- Fichiers de localisation par défaut (Angalis US) :
  - Fichiers régionaux du téléphone et de langue
  - Fichiers de langue pour la messagerie vocale

Voir *Notes de version pour Cisco Configuration Assistant* pour connaître la compatibilité et obtenir les données de version pour les paquets logiciels de l'UC500.

Paquets de localisation pour l'UC500

Les paquets de localisation pour l'UC500 peuvent aussi être téléchargés à cette adresse. Les paquets de localisation contiennent le logiciel nécessaire à la localisation des messageries et des téléphones (paramètres régionaux pour les téléphones Cisco 79xx, SPA525, SPA50x et CP-52x).

En d'autres termes, vous devez uniquement télécharger un fichier pour localiser la messagerie et tous les modèles de téléphone pris en charge.

Un paquet de localisation peut être fourni lors de l'installation du logiciel sur l'UC500 par le biais de CCA afin que vous puissiez installer une autre langue sur l'UC500. Vous pouvez installer jusqu'à deux langues : une langue active et une langue alternative.

Pour de plus amples informations, consultez la rubrique **Installation du logiciel sur l'UC500, page 552**.

Téléchargement des paquets logiciels et des paquets de localisation pour Cisco UC500

Utilisez l'une des méthodes suivantes pour télécharger un paquet logiciel ou un paquet de localisation pour l'UC 500 :

- Dans CCA, sélectionnez l'option **Connexion aux partenaires** > **Téléchargements de logiciels pour UC500** dans la barre de fonctions.
- Ouvrez le navigateur Web et accédez à l'adresse suivante :

  www.cisco.com/web/go/uc500swpk

Les utilisateurs disposant d'un Contrat de service Cisco peuvent accéder aux dernières versions du logiciel publiées par Cisco. Les partenaires qui ne disposent pas du Contrat de service pour Cisco UC500 peuvent télécharger la dernière version du logiciel pour l'UC500 dans les 30 jours suivant l'achat du produit chez un Partenaire Cisco agréé. Les utilisateurs peuvent ainsi obtenir la dernière version du logiciel pour l'UC500 en vue du déploiement initial du produit.

L'accès au logiciel à cette fin nécessite un compte Cisco.com valable. Toutes les mises à jour du logiciel suivantes publiées par Cisco au-delà de ce délai de 30 jours nécessitent un contrat de service valable.

Afficher les données de version du logiciel et les propriétés du périphérique

Vous pouvez consulter les données de version du logiciel SBCS de l'UC500 et du microprogramme des périphériques connectés à partir de divers emplacements.

- La fonction État système du Tableau de bord affiche la version Cisco IOS.
- Sélectionnez **Superviser** > **Téléphonie** > **Paquet logiciel** pour afficher les données de version relatives au paquet logiciel installé pour l'UC500, à savoir les versions Cisco IOS, CME, CUE, les charges de microprogramme compatibles avec le téléphone, et l'état CUE.
- Cliquez avec le bouton droit de la souris sur un périphérique de la Fenêtre Topologie pour en afficher les propriétés, à savoir le nom d'hôte, l'adresse IP, l'adresse MAC et la version du logiciel (par exemple, l'image Cisco IOS) propre au périphérique.

  Lorsque vous cliquez avec le bouton droit de la souris sur un téléphone IP, le type de téléphone (modèle), l'état, le nom et le prénom de l'utilisateur, les types de bouton, les numéros de poste et les intitulés de bouton s'affichent.

Mises à jour des logiciels

Pour accéder à la fenêtre Mise à jour du logiciel, sélectionnez **Maintenance** > **Mise à jour du logiciel** dans la barre de fonctions.

- Pour en savoir plus sur la mise à niveau des logiciels des périphériques qui font partie de votre site client (commutateurs, points d'accès sans fil, routeurs ou dispositifs de sécurité), consultez la rubrique **Mise à niveau du microprogramme du périphérique, page 548**.
- Pour en savoir plus sur la mise à niveau du logiciel sur l'UC500, consultez la rubrique **Installation du logiciel sur l'UC500, page 552**.

Mise à niveau du microprogramme du périphérique

La fenêtre Mise à jour du logiciel s'affiche lorsque vous sélectionnez l'option **Maintenance** > **Mise à jour du logiciel** > **Routeur/Commutateur/Ssécurité** dans la barre de fonctions de CCA.

Pour en savoir plus sur la mise à niveau du logiciel sur les périphériques gérés par CCA sur le site client, consultez les rubriques suivantes :

- **Informations de la fenêtre Mise à jour du logiciel**
- **Procédures**

Informations de la fenêtre Mise à jour du logiciel

Ce tableau explique les colonnes de la fenêtre Mise à jour du logiciel.

Colonne	Explication
Périphérique	Affiche les icônes du périphérique et les noms d'hôte.
Mise à jour	Cochez la case Mise à jour correspondant aux périphériques qui doivent être mis à jour lorsque vous cliquez sur le bouton **Mise à jour**. Vous pouvez sélectionner plusieurs périphériques du même type.
Type de périphérique	Affiche le type de périphérique.
Version actuelle	Affiche la version du logiciel actuellement installé sur le périphérique.
Nouveau nom d'image	Affiche le nom de l'image reprise dans la fenêtre Paramètres de mise à jour. Seul le nom du fichier s'affiche. Le chemin n'est pas indiqué.
État de la mise à jour	Si vous n'avez pas défini les paramètres de mise à jour, ce champ affiche le message "Cliquez sur le bouton des Paramètres de mise à jour pour continuer." Une fois l'installation lancée, ce champ affiche l'état de la mise à jour et les messages de progression. Voir **Messages sur l'état de la mise à jour, page 554** pour plus d'informations.

Procédures

Avant de commencer, téléchargez l'image logicielle que vous souhaitez installer.

Suivez les étapes suivantes pour installer ou mettre à niveau le logiciel sur les périphériques du site client de CCA.

ETAPE 1 Dans la fenêtre Mise à jour du logiciel, sélectionnez au moins un périphérique d'une même plateforme.

ETAPE 2 Cliquez sur **Paramètres de mise à jour**.

ETAPE 3 Complétez les données de la fenêtre Paramètres de mise à jour et cliquez sur **OK** pour sauvegarder les valeurs. Voir la rubrique **Paramètres de mise à jour, page 551**.

ETAPE 4 Si vous souhaitez mettre à jour plusieurs types de périphérique, répétez les étapes 1 à 4 pour chaque type.

ETAPE 5 Cochez la case **Mise à jour** à côté de chaque périphérique que vous souhaitez mettre à niveau.

ETAPE 6 Cliquez sur **Mise à jour** pour commencer la mise à niveau.

ETAPE 7 Cliquez sur **État** pour afficher la fenêtre État de la mise à jour du logiciel. Cette fenêtre affiche la progression de la mise à niveau.

Au terme du processus de mise à niveau pour tous les périphériques sélectionnés, une fenêtre de confirmation s'affiche. Les messages d'état indiquent les périphériques mis à jour avec succès et les échecs. Voir la rubrique **Messages sur l'état de la mise à jour, page 554**.

ETAPE 8 Cliquez sur **OK**. Vous êtes invité(e) à recharger les périphériques correctement mis à jour.

ETAPE 9 Cliquez sur **Oui** pour les recharger et sur **Non** si vous ne souhaitez pas recharger les périphériques. Les périphériques n'utilisent pas la mise à jour tant qu'ils n'ont pas été rechargés.

ETAPE 10 Vous pouvez aussi cliquer sur **Recharger les périphériques mis à jour** afin de recharger les périphériques sélectionnés après la mise à niveau.

Toutes les modifications sont automatiquement enregistrées dans la mémoire flash. Une minute plus tard, les périphériques sont rechargés et la nouvelle image s'exécute. Vous pouvez alors fermer la fenêtre Mise à jour du logiciel.

- Vous pouvez gérer les périphériques de la communauté dès leur redémarrage.
- Lors du rechargement, la liaison au périphérique est perdue.

Paramètres de mise à jour

Cette fenêtre s'affiche lorsque vous sélectionnez un ou plusieurs périphériques dans la fenêtre Mise à jour du logiciel et que vous cliquez sur **Paramètres de mise à jour**. Elle vous permet de définir les paramètres de mise à jour pour les périphériques se trouvant sur la même plateforme.

Configurez les paramètres de mise à jour selon les indications du tableau suivant. Lorsque vous êtes prêt(e) à continuer, cliquez sur **OK**. Sinon, cliquez sur **Annuler**.

Paramètre	Description
Périphérique	Lecture seule. Affiche le nom du périphérique sélectionné.
Image	Cliquez sur **Parcourir** pour localiser l'image du logiciel à utiliser pour la mise à niveau.
Mode	Sur certains périphériques, vous avez le choix entre le mode **Standard** ou **TFTP**. ▪ Utilisez le mode *standard* si les images de mise à niveau sont stockées en local. ▪ Utilisez le mode *Serveur TFTP distant* si les images CUE ou IOS pour la mise à niveau sont stockées sur un serveur distant. Pour effectuer la mise à niveau en mode Serveur TFTP distant, vous avez besoin d'un serveur TFTP dédié sur une station de travail Unix ou sur un autre PC. Vous pouvez utiliser n'importe quelle application TFTP sur le serveur. Si vous avez sélectionné **Serveur TFTP distant**, procédez comme suit : ▪ Dans le champ **Fichier image**, entrez le chemin complet et le nom du fichier image Cisco IOS. ▪ Dans le champ **Adresse IP du serveur TFTP**, introduisez l'adresse IP du serveur TFTP. Vous pouvez sélectionner plusieurs membres de la communauté et mettre à jour les images Cisco IOS. Pour réaliser des mises à jour groupées, votre serveur TFTP doit gérer plusieurs requêtes et sessions en même temps.

Installation du logiciel sur l'UC500

L'assistant d'installation du logiciel de l'UC500 s'affiche lorsque vous sélectionnez l'option **Maintenance** > **Mise à jour du logiciel** > **UC500**.

Pour en savoir plus sur la préparation de l'installation du logiciel de l'UC500, consultez les rubriques suivantes :

- **Assistant d'installation du logiciel de l'UC500**
- **Préparation de l'installation du logiciel sur l'UC500**
- **Messages sur l'état de la mise à jour**

ATTENTION Cisco conseille de ne pas procéder à la mise à niveau du logiciel à partir d'une connexion WAN distante. Si la connexion WAN est interrompue, l'opération échouera et le système ou le périphérique risque d'être inutilisable.

Assistant d'installation du logiciel de l'UC500

Grâce à l'Assistant d'installation du logiciel de l'UC500, vous pouvez effectuer les opérations suivantes :

- Installer un paquet logiciel pour l'UC500

  Il s'agit du meilleur moyen d'installer et de mettre à niveau le logiciel de l'UC500. Si vous utilisez cette méthode, sélectionnez **Tout** lorsque vous sélectionnez les paramètres de mise à niveau. Le paquet logiciel de l'UC500 comprend Cisco IOS, CUE, les charges de téléphone CME, les scripts pour le standard automatique et Basic ACD, les paramètres locaux et les fichiers de langue en anglais US pour les téléphones et la messagerie, ainsi que les fichiers d'aide.

- Installer un paquet contenant les paramètres locaux pour l'UC500
- Mettre à niveau uniquement l'image de Cisco IOS sur l'UC500
- Mettre à niveau uniquement le logiciel de la messagerie Cisco IOS sur l'UC500

REMARQUE Lorsque vous téléchargez des images CUE ou IOS à partir de Cisco.com, utilisez la version .tar des images Cisco IOS et un paquet CUE pour le logiciel de messagerie CUE.

Suivez les consignes à l'écran pour configurer les paramètres suivants :

Préparation de l'installation du logiciel sur l'UC500

Pour éviter les problèmes d'installation, de mise à jour et autres, lisez attentivement cette partie et vérifiez si le système est prêt pour la mise à niveau en effectuant les opérations suivantes.

- Vérifiez si votre PC répond aux critères d'utilisation de CCA. Voir la rubrique **Configuration minimale requise, page 17**.
- Si le PC exécutant Configuration Assistant dispose d'une double carte réseau, veillez à ce qu'une seule carte soit active.
- Désactivez les services FTP/TFTP actifs sur votre PC.

  Avant la mise à niveau, désactivez les services TFTP tiers actifs sur votre PC. Le serveur TFTP de CCA permet de transférer les images et les fichiers de votre PC au périphérique à mettre à jour. Un seul serveur TFTP à la fois peut accéder au port TFTP.

  Sur le PC exécutant CCA, ouvrez une fenêtre de commande et exécutez la commande `netstat -a` pour voir si certains services FTP ou TFTP sont actifs. Vous ne devriez pas voir les ports 21, 69, FTP ou TFTP dans le résultat. Si c'est le cas, interrompez ces processus ou services.

  En l'absence de services TFTP actifs, essayez de redémarrer votre PC pour libérer les ports TFTP qui pourraient toujours être employés par une session antérieure de CCA.
- Vérifiez si le PC a obtenu une adresse DHCP de l'UC500 et si la passerelle par défaut est correctement paramétrée.

  Sur le PC exécutant CCA, ouvrez une fenêtre de commande et exécutez la commande `ipconfig /all`. L'adresse IP de la passerelle par défaut affichée parmi les résultats doit être obtenue de l'UC500 (valeur par défaut : 192.168.10.1).
- Tout pare-feu installé sur le PC exécutant CCA doit être configuré de telle sorte à autoriser l'accès TFTP et FTP à partir et vers l'UC500.

  Le pare-feu actif sur votre PC peut être amené à bloquer la liaison entre le module CUE sur l'UC500 et CCA, ce qui risque de provoquer l'échec de la mise à niveau.

  Si vous désactivez le pare-feu actif sur le PC pendant la mise à niveau, veillez à le réactiver au terme de l'opération.

- Vérifiez l'état de l'interface CUE. Pour ce faire, sélectionnez l'option **Dépanner** > **Diagnostic CUE > Diagnostic de connectivité CUE** dans la barre de fonctions et cliquez sur **Vérifier l'état**. La mention "`Integrated-Service-Engine0/0 is up, line protocol is up`" (Integrated-Service-Engine0/0 est actif, le protocole de ligne est actif) devrait s'afficher dans la rubrique "afficher les interfaces" située en haut de la fenêtre de résultat si le module d'interface CUE est actif.

État de la mise à jour du logiciel

Cette fenêtre s'affiche lorsque vous sélectionnez un périphérique et cliquez sur **État** dans la fenêtre Mise à jour du logiciel. Cette fenêtre présente les messages détaillés lors de leur apparition au cours de la mise à jour.

Si l'espace disponible sur le périphérique est insuffisant pour l'installation d'une nouvelle image, un message contenant un lien vers la fenêtre Gestion des fichiers s'affiche. Vous pouvez utiliser la fenêtre Gestion des fichiers pour assurer la gestion de vos systèmes de fichiers et pour supprimer si nécessaire les anciennes images afin de libérer de l'espace pour les nouvelles.

Messages sur l'état de la mise à jour

Ce tableau explique les messages d'état de la mise à jour.

Message	Explication
Cliquez sur le bouton Paramètres de mise à jour pour continuer.	La fenêtre Paramètres de mise à jour doit être complétée avant de procéder à la mise à jour du périphérique.
Cliquez sur le bouton Mise à jour pour mettre le périphérique à jour.	Tous les paramètres sont définis pour la mise à jour du périphérique.
Le rechargement a commencé pour le périphérique.	Le périphérique est en cours de rechargement après une mise à jour réussie du logiciel. Même au terme du chargement, ce message s'affiche jusqu'à ce que la fenêtre ait été actualisée.
La mise à jour du logiciel a été réalisée avec succès.	La mise à jour du logiciel a réussi.

Message	Explication
Échec lors de la mise à jour du logiciel.	La mise à jour du logiciel a échoué. Voir la fenêtre État pour de plus amples informations. **IMPORTANT** En cas d'échec de la mise à niveau, vérifiez si vous avez accompli toutes les tâches figurant dans le **Préparation de l'installation du logiciel sur l'UC500, page 553**.
La mise à jour du logiciel est en cours.	La mise à niveau des périphériques a commencé.
Chargement de l'image.	L'image est en cours de chargement sur le périphérique.
Vérification de l'image	Le périphérique vérifie l'image.

Mise à niveau de la messagerie (UC560)

La plateforme UC560 permet la mise à niveau de la carte Compact Flash de la Messagerie de sa taille par défaut (2 Go) à une capacité de 4 ou 8 Go en vue d'élargir la capacité de stockage de la messagerie vocale. Une fois que la carte Compact Flash est remplacée et que l'UC560 a redémarré, vous êtes invité à installer le logiciel de la messagerie et les fichiers de langue sur la nouvelle carte de la messagerie.

Consultez les rubriques suivantes pour plus d'informations :

- **Préparation de la mise à niveau de la messagerie**
- **Remplacement de la carte Compact Flash de la messagerie sur l'UC560 et réalisation de la mise à niveau de la messagerie**

Préparation de la mise à niveau de la messagerie

Avant d'effectuer la mise à niveau de la messagerie :

- Si le PC exécutant Configuration Assistant dispose d'une double carte réseau, veillez à ce qu'une seule carte soit active.
- Tout pare-feu installé sur le PC exécutant CCA doit être configuré de telle sorte à autoriser l'accès TFTP et FTP à partir et vers l'UC500.

- Arrêtez les serveurs TFTP ou FTP tiers actifs sur l'ordinateur exécutant CCA.
- En l'absence de services TFTP actifs, essayez de redémarrer votre PC pour libérer les ports TFTP qui pourraient toujours être employés par une session antérieure de CCA.
- Si les réglages d'usine ne sont pas actifs sur l'UC500 :
  - Enregistrez la configuration la configuration en cours comme configuration de démarrage. Voir la rubrique **Application et enregistrement de la configuration, page 49**.
  - Sauvegardez la configuration active de l'UC500 et **Sauvegarde et restauration d'une configuration de périphérique, page 120**.
- Vérifiez si vous avez bien téléchargé le dernier paquet logiciel de l'UC500 pour la plateforme correspondante (par ex. : UC560-8.0.0.zip ou une version supérieure) sur le PC exécutant CCA. Le paquet logiciel contient la dernière version du logiciel de la messagerie CUE (fichier SCUE*.zip).
- Si vous souhaitez une autre langue qu'Anglais US ou installer les fichiers pour une langue alternative, vous devez aussi télécharger les paquets de paramètres locaux correspondants. Voir la rubrique **Paquets de localisation pour l'UC500, page 546**.

  Pour télécharger les paquets de paramètres locaux pour l'UC500, utilisez la page www.cisco.com/go/uc500swpk.
- Vous pouvez aussi télécharger des copies des fichiers personnalisés à partir de la mémoire flash de l'UC500 vers votre PC à partir de la fenêtre Gestion des fichiers de CCA (**Maintenance** > **Gestion des fichiers**. Voir la rubrique **Gestion des fichiers, page 570**.

Remplacement de la carte Compact Flash de la messagerie sur l'UC560 et réalisation de la mise à niveau de la messagerie

Vous pouvez commander chez Cisco une nouvelle carte Compact Flash d'une capacité supérieure pour la messagerie de l'UC560 (UC500-8GB correspond à la carte de 8 Go et UC500-4GB à la carte de 4 Go).

AVERTISSEMENT Avant d'installer la nouvelle carte Compact Flash sur l'UC560, vous devrez enregistrer et sauvegarder la configuration de l'UC560 et ensuite débrancher l'UC560. Dans le cas contraire, le système risque d'être inutilisable et vous risquez de perdre des données.

Suivez les étapes suivantes pour remplacer la carte Compact Flash de la messagerie sur l'UC560 et réaliser la mise à niveau de la messagerie à l'aide de CCA.

ETAPE 1 Vérifiez si vous avez effectué les opérations reprises dans la rubrique **Préparation de la mise à niveau de la messagerie, page 555**.

ETAPE 2 Mettez l'UC560 hors tension.

ETAPE 3 Repérez la fente pour la carte Compact Flash de la messagerie et retirez la carte s'y trouvant.

ETAPE 4 Insérez la nouvelle carte dans la fente.

ETAPE 5 Mettez l'UC560 sous tension.

ETAPE 6 Alors que le PC exécutant CCA est relié à l'entrée LAN de l'UC500, démarrez CCA et connectez-vous à l'UC560.

CCA détecte la nouvelle carte pour la messagerie. Il affiche un message vous informant qu'aucun logiciel CUE n'est installé pour la messagerie et vous demande si vous souhaitez l'installer.

- Si vous sélectionnez l'option **Oui**, la fenêtre Mise à niveau de la messagerie s'affiche.
- Si vous sélectionnez l'option **Non** ou fermez la fenêtre, vous pourrez toujours y accéder à partir de la barre de fonctions à l'aide du menu **Maintenance** > **Mise à jour du logiciel** > **UC500**.

Étant donné que la nouvelle carte ne contient aucun logiciel ni aucune donnée, les fonctions vocales ne sont pas disponibles tant que vous n'aurez pas effectué la mise à niveau de la messagerie vocale.

ETAPE 7 Suivez les instructions de l'Assistant d'installation du logiciel de l'UC500 pour installer le logiciel de la messagerie et les fichiers de langue. Sélectionnez l'option **Logiciel de messagerie vocale**.

La procédure de mise à niveau dure environ 30 minutes.

CCA restaure la dernière sauvegarde au terme de l'installation du logiciel.

ETAPE 8 Pour vérifier si l'installation a été correctement effectuée, procédez comme suit :

- Ouvrez la fenêtre Messagerie (**Configurer** > **Téléphonie** > **Messagerie vocale**) et vérifiez si les données relatives à l'espace de stockage de la carte correspondent à la capacité de la nouvelle carte.
- Effectuez les appels, laissez les messages vocaux et écoutez les messages pour vérifier si la messagerie fonctionne correctement.
- Récupérez les anciens messages afin de vérifier s'ils sont toujours bien accessibles.

ETAPE 9 Cliquez sur **Configurer** > **Enregistrer la configuration** pour enregistrer la configuration.

ETAPE 10 Sauvegardez la nouvelle configuration (**Maintenance** > **Archive des configurations**, **Sauvegarde**).

.

Gestion des licences

Pour gérer les licences, sélectionnez **Maintenance** > **Gestion des licences** dans la barre de fonctions.

Les options de gestion des licences varient selon les plateformes UC520 et UC540. Ces options sont analysées plus en détail dans les rubriques suivantes :

- **Vue d'ensemble, page 558**
- **Types de licence, page 559**
- **Gestion des licences de l'UC520, page 560**
- **Gestion des licences de l'UC540 et de l'UC560, page 562**

Vue d'ensemble

Les licences Cisco sont prises en charge sur les plateformes de la série UC 500. Elles peuvent donc être modifiées. Par exemple, un système associé à une licence pour 8 utilisateurs pouvant prendre en charge 16 utilisateurs peut évoluer vers une licence pour 16 utilisateurs. Les licences peuvent également être revues à la baisse.

Les téléphones IP sont enregistrés en fonction de la disponibilité de la licence propre à chaque téléphone. Sur les plateformes UC520, lorsqu'une licence est réduite suite à une échéance ou à une configuration effectuée par l'utilisateur et que le nombre de téléphones enregistrés dépasse le nombre de licences utilisateur, le système se recharge.

Les fonctions de licence suivantes du logiciel sont disponibles :

- Les licences d'évaluation, d'extension, permanentes et de période de grâce sont prises en charge sur l'UC520.
- Les licences d'évaluation et permanentes sont prises en charge sur l'UC540 et l'UC560. L'UC540 et l'UC560 exploitent les mises à niveau de type PAK (code d'autorisation produit) pour les licences.
- Les installations et les échéances sont gérées par le système de suivi des licences.

Types de licence

Configuration Assistant prend en charge les quatre types de licence décrits dans cette rubrique.

Type de licence	Description
Licence d'évaluation	Les licences d'évaluation ne sont pas verrouillées sur les nœuds. Il s'agit de licences contrôlées associées à une image IOS et valables pour une durée déterminée. La licence est uniquement utilisée en l'absence de licence permanente, d'extension ou de période de grâce pour une fonction donnée. Vous devez accepter le contrat de licence de l'utilisateur final avant d'utiliser cette licence. Chaque fois que vous vous connectez ou actualisez le réseau, Configuration Assistant vous avertit de l'état d'une licence temporaire à l'aide de la fenêtre Notification des événements. Vous êtes également averti(e) lorsque l'une des fonctions arrive à échéance dans les 10 jours au plus, auquel cas le système vous conseille d'installer une licence permanente.

Type de licence	Description
Licence permanente	Les licences permanentes sont dépendantes des nœuds et ne sont associées à aucune période d'utilisation. Elles sont obtenues par le biais du portail de licence Cisco. Pour les plateformes UC520, vous devez accepter le CLUF dans le cadre de l'installation de la licence.
Licence d'extension	UC520 uniquement. Les licences d'extension sont des licences contrôlées verrouillées sur les noeuds et émises par le portail de licence Cisco. Pour les plateformes UC520, vous devez accepter le CLUF dans le cadre de l'installation de la licence.
Licence de période de grâce	UC520 uniquement. Les licences de période de grâce sont des licences dépendantes du nœud et émises par le portail de licence Cisco dans le cadre d'une demande de nouvel hébergement d'une licence. Ces licences sont installées sur le périphérique dans le cadre du nouvel hébergement. Vous devez accepter le CLUF dans le cadre du nouvel hébergement pour ce type de licence.

Gestion des licences de l'UC520

Pour afficher les données de licence ou installer une licence, sélectionnez **Maintenance** > **Gestion des licences** dans la barre de fonctions.

Ce tableau dresse la liste des licences de l'UC520 affichées dans cette fenêtre.

Paramètre	Description
Périphérique/Fonction	Affiche les périphériques disponibles et les licences utilisateurs actives.
Identifiant du périphérique	Lecture seule. Affiche l'identifiant de périphérique pour l'UC520. Par exemple : UC520W-FXO-K9:FFH104001MR.
Capacités actuelles	Nombre de licences utilisateurs installées sur l'UC520.
Capacités maximales	Nombre de licences utilisateurs prises en charge par le kit de développement de l'UC520.

Paramètre	Description
Type de licence	La licence peut être permanente, d'évaluation, d'extension ou de période de grâce.
Période d'expiration	Pour les licences permanentes, la valeur À vie est toujours affichée dans la rubrique Période d'expiration. Pour les licences d'évaluation, la Période d'expiration représente la durée résiduelle avant l'expiration de la licence.
Action	Parmi les options disponibles, **Aucun** ou **Sélectionnez le fichier de licence**.

Pour installer une **licence** d'évaluation, procédez comme suit :

ETAPE 1 Dans la fenêtre Gestion des licences, cliquez sur le périphérique UC500 pour lequel vous souhaitez installer la licence d'évaluation.

ETAPE 2 Dans la liste Action du périphérique, sélectionnez **Licence d'évaluation**.

ETAPE 3 Cliquez sur **Appliquer** ou **OK** pour installer les licences. Les champs connexes sont mis à jour.

Pour installer une licence **permanente** ou **d'extension**, procédez comme suit :

ETAPE 1 Dans la liste Action du périphérique, sélectionnez l'option **Sélectionnez le fichier de licence**. La fenêtre Charger le fichier de licence s'affiche.

ETAPE 2 Cliquez sur **Parcourir** pour accéder à l'emplacement du fichier de licence et cliquez ensuite sur **OK**. Voir la rubrique **Charger le fichier de licence, page 567**.

Pour annuler la mise à niveau de la licence, cliquez sur **Actualiser** avant de cliquer sur **Appliquer** ou sur **OK**. L'installation est annulée et l'état d'origine de la licence s'affiche.

ETAPE 3 Cliquez sur **Appliquer** ou **OK** pour installer la licence. Les champs connexes sont mis à jour.

Lorsque les licences sont correctement installées, la colonne Caractéristiques est mise à jour en fonction des nouvelles licences.

Gestion des licences de l'UC540 et de l'UC560

La gestion des licences pour l'UC540 et l'UC560 prend également en charge le système de code d'autorisation produit (PAK) pour les mises à niveau. Pour plus d'informations, consultez la section suivante, **Actions de gestion des licences, page 563**.

Ce tableau dresse la liste des licences de l'UC540 affichées dans cette fenêtre.

Paramètre	Description
Périphérique/Fonction	Affiche les périphériques disponibles et les licences installées. Les licences propres au périphérique UC540 et de l'UC560 sont citées comme Licence utilisateur Pro.
Identifiant du périphérique	Lecture seule. Affiche l'identifiant de périphérique pour l'UC540 ou l'UC560. Par exemple : UC540W-FXO-K9:FFH104001MR.
Capacités actuelles	Nombre de licences installées sur l'UC540 ou l'UC560.
Capacités maximales	Nombre maximal de licences prises en charge. Pour l'UC540, la valeur est 32. L'UC560 prend en charge jusqu'à 104 licences utilisateur.
Type de licence	Pour l'UC540, la valeur peut être Permanente ou Évaluation. Les licences peuvent être actives ou inactives.
Période d'expiration	Pour les licences permanentes, la valeur À vie est toujours affichée dans la rubrique Période d'expiration. Pour les licences d'évaluation, la Période d'expiration représente la durée résiduelle avant l'expiration de la licence.

Paramètre	Description
Action	Pour les licences actives, cliquez sur **Gérer** pour ouvrir la fenêtre Détails de la gestion des licences qui vous permet d'installer, mettre à niveau, transférer, activer et désactiver les licences. Voir la rubrique **Actions de gestion des licences, page 563**.

Actions de gestion des licences

Cette fenêtre s'affiche lorsque vous sélectionnez l'UC540 ou l'UC560 dans la fenêtre Gestion des licences, sélectionnez une licence et cliquez sur **Gérer**.

Vue d'ensemble

La plateforme UC540 est livrée par défaut avec 8 licences permanentes installées et actives. L'UC560 est quant à elle dotée de 16 licences permanentes installées et actives. Ces licences installée de série ne peuvent pas être transférées, révoquées ou modifiées.

Le nombre maximum de licences utilisateurs pour la plateforme UC540 est 32. Le nombre maximum de licences utilisateur autorisé pour l'UC560 est 104. Des licences supplémentaires peuvent être ajoutées par groupes de 8 à l'aide d'un code d'autorisation produit (PAK) ou d'un fichier de licence. Si le nombre maximum de licences est déjà installé, la fonction de mise à niveau d'une licence à partir d'un code d'autorisation produit (PAK) et les options d'installation de licences sont désactivées.

Les champs de configuration affichés dans cette fenêtre varient en fonction des opérations de gestion des licences effectuées. Les actions suivantes peuvent être effectuées :

- **Mettre à jour la licence à l'aide du Code d'autorisation produit (PAK), page 564**
- **Transférer la licence vers ou à partir de ce périphérique, page 565**
- **Installer une licence à partir d'un fichier, page 567**
- **Activer ou désactiver la licence d'évaluation, page 567**

Mettre à jour la licence à l'aide du Code d'autorisation produit (PAK)

Sélectionnez l'option **Mettre à jour la licence à l'aide du Code d'autorisation produit (PAK)** si vous souhaitez installer des licences supplémentaires à l'aide d'un PAK. Cette option n'est pas disponible si le nombre maximum de licences est déjà installé.

La base de données SWIFT (Software Infrastructure and Fulfillment Technology) est consultée et modifiée en cas de mise à niveau des licences.

Pour installer une licence de mise à niveau à l'aide d'un code d'autorisation produit (PAK), procédez comme suit :

ETAPE 1 Dans le volet **Actions** de la fenêtre, sélectionnez **Mettre à jour la licence à l'aide du Code d'autorisation produit (PAK)**.

L'identifiant du périphérique en haut de l'écran affiche l'identifiant propre au périphérique UC540.

ETAPE 2 Entrez les paramètres ci-dessous dans le volet **Détails de l'action** de la fenêtre.

Paramètres	Description
Utilisateur Cisco.com	Introduisez votre identifiant Cisco.com.
Mot de passe Cisco.com	Introduisez votre mot de passe Cisco.com.
Adresse e-mail	Introduisez une adresse e-mail valable. Il s'agit de l'adresse à laquelle SWIFT envoie les notifications.
Nombre de codes d'autorisation produit (PAK) à installer	Sélectionnez le nombre de codes d'autorisation produit (PAK) à installer dans la liste déroulante (de 1 à 3 pour l'UC540 et de 1 à 8 pour l'UC560.
PAK-1 à PAK-3 (UC540) **PAK-1 à PAK-8 (UC560)**	Entrez le code d'autorisation produit pour chaque licence à installer.

ETAPE 3 Cliquez sur **OK** pour fermer la fenêtre Actions de gestion des licences et revenir à la fenêtre Gestion des licences.

Transférer la licence vers ou à partir de ce périphérique

Sélectionnez l'option **Transférer la licence vers ou à partir de ce périphérique** si vous souhaitez effectuer l'une des opérations suivantes :

- Révoquer et supprimer les licences du périphérique UC540 ou UC560 et les enregistrer dans un fichier ;
- Transférer une licence préalablement enregistrée vers un autre périphérique UC540 ou UC560.

Lorsque vous supprimez les licences d'un UC540 ou UC560, les phénomènes suivants se produisent :

- Les licences sont enregistrées dans un fichier sur le PC exécutant Configuration Assistant.
- L'emplacement s'affiche dans la fenêtre Actions de gestion des licences.

Lorsque vous transférez la licence vers un autre UC540 ou UC560, veillez à ce que le fichier se trouve sur le PC exécutant Configuration Assistant. Utilisez le même PC pour supprimer et transférer les licences ou copier le fichier de licence enregistré au même emplacement sur le PC qui sera utilisé pour le transfert de la licence.

La base de données SWIFT (Software Infrastructure and Fulfillment Technology) est consultée et mise à jour en cas de révocation et de transfert des licences.

Pour supprimer les licences de l'UC540 ou de l'UC560 et les transférer vers un autre UC540 ou UC560, suivez les étapes suivantes :

ETAPE 1 Dans la section **Actions** de la fenêtre Actions de gestion des licences, sélectionnez l'option **Transférer la licence vers ou à partir de ce périphérique**.

ETAPE 2 Entrez les paramètres ci-dessous dans le volet **Détails de l'action** de la fenêtre.

Paramètres	Description
Nom d'utilisateur Cisco.com	Introduisez votre identifiant Cisco.com.
Mot de passe Cisco.com	Introduisez votre mot de passe Cisco.com.

Paramètres	Description
Adresse e-mail	Introduisez une adresse e-mail valable. Il s'agit de l'adresse à laquelle SWIFT (Software Infrastructure and Fulfillment Technology) envoie les notifications.
Type de transfert	Sélectionnez l'option **Supprimer la licence et enregistrer pour le transfert**.

ETAPE 3 Lorsque vous cliquez sur **OK**, le système se connecte à la base de données SWIFT et révoque la licence. La licence est supprimée de l'UC540 ou de l'UC560 et enregistrée dans un fichier sur le PC exécutant Configuration Assistant.

L'emplacement du fichier sur le PC local s'affiche dans la fenêtre Actions de gestion des licences.

Pour installer une licence préalablement enregistrée et transférée vers un autre UC540 ou UC560, suivez les étapes suivantes :

ETAPE 1 Dans la section **Actions** de la fenêtre, sélectionnez l'option **Transférer la licence vers ou à partir de ce périphérique**.

ETAPE 2 Entrez les paramètres ci-dessous dans le volet **Détails de l'action** de la fenêtre.

Paramètres	Description
Nom d'utilisateur Cisco.com	Introduisez votre identifiant Cisco.com.
Mot de passe Cisco.com	Introduisez votre mot de passe Cisco.com.
Type de transfert	Sélectionnez l'option **Transférer la licence préalablement enregistrée**. Choisissez la licence à installer dans la liste déroulante **Licences détectées**. Lors de la détection de licences, Configuration Assistant effectue la recherche uniquement à l'emplacement où la licence a été préalablement enregistrée.

ETAPE 3 Cliquez sur **OK** pour installer la licence et fermer la fenêtre Actions de gestion des licences. Vous reviendrez ainsi à la fenêtre Gestion des licences.

Installer une licence à partir d'un fichier

Sélectionnez l'option **Installer un fichier de licence** si vous souhaitez installer manuellement une licence à l'aide d'un fichier de licence.

Pour installer une licence à partir d'un fichier, procédez comme suit :

ETAPE 1 Dans la section **Actions** de la fenêtre, sélectionnez l'option **Installer une licence à partir d'un fichier**.

ETAPE 2 Dans la section **Détails de l'action**, cliquez sur **Parcourir** et localisez le fichier à installer. Cliquez ensuite sur **OK**. Voir la rubrique **Charger le fichier de licence, page 567**.

ETAPE 3 Cliquez sur **Appliquer** ou sur **OK** pour installer la licence et fermer la fenêtre Actions de gestion des licences.

Activer ou désactiver la licence d'évaluation

Pour activer ou désactiver une licence, sélectionnez **Activer une licence d'évaluation** ou **Désactiver une licence d'évaluation** et cliquez sur **OK**. Aucune autre information n'est nécessaire.

Charger le fichier de licence

La fenêtre Charger le fichier de licence s'affiche lorsque vous gérez les licences sur un UC520 et sélectionnez l'option **Sélectionner un fichier de licence** dans la liste déroulante Actions de la fenêtre Gestion des licences.

Cliquez sur **Parcourir** pour accéder à l'emplacement du fichier de licence et cliquez ensuite sur **OK** pour charger le fichier de licence.

Le fichier de licence est au format .lic ou .xml.

Redémarrer/réinitialiser les périphériques

Pour accéder à la fenêtre Redémarrer/Réinitialiser, sélectionnez **Maintenance** > **Redémarrer/Réinitialiser** dans la barre de fonctions.

Vue d'ensemble

Vous pouvez *redémarrer* les périphériques de votre site client ou *rétablir* les paramètres d'usine.

- Le redémarrage d'un périphérique permet de sauvegarder le fichier de configuration actif et de le redémarrer. Le périphérique n'est pas accessible pendant le redémarrage et la liaison entre le périphérique et les terminaisons est interrompue pendant un court laps de temps.
- La réinitialisation du périphérique permet de rétablir sa configuration par défaut. Une fois la configuration d'usine rétablie, vous pouvez utiliser l'un des assistants de configuration de périphérique pour définir la configuration ou reconfigurer manuellement le périphérique.

REMARQUE Lors de la réinitialisation d'un périphérique, le serveur DHCP peut affecter une nouvelle adresse IP au périphérique réinitialisé. Le cas échéant, la fenêtre Topologie de CCA indique que le périphérique est inaccessible. Cliquez avec le bouton droit de la souris dans la Fenêtre Topologie et sélectionnez l'option **Ajouter au site** pour ajouter le périphérique et sa nouvelle adresse IP au site client.

Procédures

Pour redémarrer ou réinitialiser un périphérique sur votre site client, suivez les étapes suivantes :

ETAPE 1 Dans la fenêtre Redémarrer/Réinitialiser, sélectionnez le périphérique que vous souhaitez redémarrer ou réinitialiser.

ETAPE 2 Faites un choix parmi les options suivantes :

- Cochez la case **Redémarrer**.
- Cochez l'option **Rétablissement des paramètres par défaut**.
- Cochez les deux options.

ETAPE 3 Cliquez sur **OK**.

Pour redémarrer CUE

Pour l'UC500, vous pouvez aussi choisir de redémarrer le module Cisco Unity Express uniquement. Les applications de messagerie, de standard automatique et autres s'exécutent sur le module CUE.

ATTENTION Vous ne devez redémarrer le module CUE que si le Cisco Technical Assistance Center (TAC) vous le demande afin de résoudre un problème spécifique ou dans le cadre d'une démarche connexe sous Configuration Assistant ; par exemple, pour forcer la relecture des fichiers de langue installés pour l'application Cisco WebEx PhoneConnect.

Le redémarrage CUE peut prendre de 10 à 15 minutes. Au cours de cette période, la messagerie, le standard automatique et les applications de téléphonie telles que Cisco WebEx PhoneConnect et TimeCardView ne sont pas disponibles.

Pour redémarrer le module CUE, sélectionnez l'option **Accueil** > **Topologie** pour afficher la fenêtre Topologie et cliquez avec le bouton droit sur le module UC500 de la Fenêtre Topologie et sélectionnez l'option **Redémarrer CUE** dans le menu.

ASTUCE Pour accéder aux outils de diagnostic et de dépannage CUE, accédez à l'option **Dépanner** > **Diagnostic de téléphonie** > **Diagnostic CUE** > **Diagnostic de connectivité CUE**. Pour de plus amples informations, consultez la rubrique **Diagnostic de connectivité CUE, page 629**.

Localisation de l'UC500 (paramètres hors USA/UK)

La langue par défaut de l'UC500 est l'anglais (Etats-Unis).

Pour localiser l'UC500, les téléphones et la messagerie en installant des paramètres régionaux adaptés, suivez les étapes suivantes :

ETAPE 1 Téléchargez le dernier paquet logiciel pour l'UC500 et les paquets de contenant les paramètres régionaux souhaités.

Voir la rubrique **Téléchargement des paquets logiciels et des paquets de localisation pour Cisco UC500, page 547**.

ETAPE 2 Pour installer ces éléments, sélectionnez l'option **Maintenance** > **Mise à jour du logiciel** > **UC500** et suivez les consignes à l'écran.

Voir la rubrique **Installation du logiciel sur l'UC500, page 552**.

ETAPE 3 Dans la fenêtre Plan de numérotation sortant, sélectionnez les paramètres locaux du modèle de numérotation correspondant ou chargez un modèle personnalisé.

Voir la rubrique **Plan de numérotation sortant, page 470**.

Gestion des fichiers

Pour gérer le système de fichiers sur la carte-mémoire de l'UC500 ou le système de fichiers des autres périphériques, sélectionnez l'option **Maintenance** > **Gestion des fichiers** dans la barre de fonctions.

ASTUCE La fonction Utilisation de la mémoire flash affichée sur le Tableau de bord fournit des indications sur le pourcentage de mémoire utilisée sur la carte. Pour accéder au Tableau de bord, sélectionnez **Accueil** > **Tableau de bord** dans la barre de fonctions. Vous pouvez supprimer des charges de téléphone de la mémoire flash afin de libérer de l'espace si nécessaire. Voir la rubrique **Gestion des charges de téléphone, page 576**.

Vue d'ensemble

Dans la fenêtre Gestion des fichiers, vous pouvez effectuer les opérations suivantes :

- Vous pouvez afficher le système de fichiers de n'importe quel périphérique Cisco IOS relié à un réseau actif.
- Vous pouvez réaliser des opérations de gestion de fichiers de base sur ces systèmes.
- Vous pouvez supprimer des fichiers de la mémoire flash.

  Par exemple, lors de la mise à niveau du logiciel, il est possible que vous ne disposiez pas de l'espace nécessaire à l'installation de l'image. Vous pouvez donc supprimer l'ancienne image pour faire de la place pour la nouvelle.
- Vous pouvez charger et télécharger les fichiers vers et à partir de la mémoire flash.

Procédures

La fenêtre Gestion des fichiers présente les onglets suivants :

- **Vue d'ensemble**
- **Fichiers**

Vue d'ensemble

Ce tableau explique les colonnes de l'onglet **Vue d'ensemble**.

Colonne	Explication
Périphérique / Système de fichiers	Dresse la liste des périphériques sélectionnés et le système de fichiers actif sur ces périphériques.
État	L'état du système de fichiers ne peut être que l'un des suivants : ▪ **Vide** - Aucun état à signaler. ▪ **Broyage nécessaire** - Certains fichiers supprimés se trouvent sur un système de fichiers de classe B. ▪ **Broyage en cours** - Nettoyage en cours des fichiers marqués pour la suppression. ▪ **Système de fichiers en cours d'utilisation** - Les données relatives au système de fichiers ne sont pas disponibles. Cliquez sur **Actualiser** pour réessayer. ▪ **Système de fichiers saturé** - Il ne reste aucun espace libre dans le système de fichiers. ▪ **Système de fichiers vide** - Il n'y a aucun fichier dans le système de fichiers. ▪ **Le système de fichiers est en lecture seule** - Le système de fichiers est verrouillé et ne peut pas être modifié. Cela est souvent dû au verrouillage de la carte Compact Flash.
Capacité	Taille du système de fichiers au méga-octet (Mo) près.

Colonne	Explication
Espace libre	Nombre de méga-octets libres dans le système de fichiers au Mo près.
Pourcentage d'espace libre	Fraction du système de fichiers non utilisée.
Fichiers	Nombre de fichiers dans le système de fichiers. Les répertoires des systèmes de fichiers de classe C et les fichiers supprimés des systèmes de fichiers de classe B sont comptabilisés comme des fichiers.

Fichiers

Ce tableau explique les colonnes de l'onglet **Fichiers**.

Colonne	Explication
Périphérique / Système de fichiers	Dresse la liste des périphériques sélectionnés et le système de fichiers actif sur ces périphériques. Une liste des répertoires et des fichiers s'affiche sous chaque système de fichiers.
Broyage	Cette action n'est disponible qu'en présence d'un fichier supprimé sur un périphérique disposant d'un système de fichiers de classe B. Cochez la case pour supprimer définitivement les fichiers supprimés du système. La case à cocher n'est pas disponible si le système de fichiers est en lecture seule ou en l'absence de fichiers supprimés.
Taille	Donne la taille des différents fichiers exprimée en Ko.
Type	Dresse la liste des différents types de fichiers le cas échéant. Parmi les types de fichiers les plus répandus, vous trouverez Image système, Image Cisco IOS et Configuration.
Modifié	Indique la date et l'heure de modification du fichier.
Supprimer	Cochez la case correspondant à un fichier pour la supprimer. En présence d'un système de fichiers de classe B et si le fichier a déjà été marqué pour suppression, la case sera déjà cochée.
Restaurer	S'affiche uniquement pour les périphériques présentant des systèmes de fichiers de classe B et des fichiers supprimés. Cochez les cases pour sélectionner les fichiers à restaurer.

Chargement, téléchargement et suppression de fichiers sur la mémoire flash

Vous pouvez charger et décharger les fichiers à partir et vers la carte Compact Flash de l'UC500 ou des autres périphériques Cisco IOS gérés par CCA. Par exemple, vous pouvez charger des fichiers de sonnerie, des images pour le bureau, des musiques d'attente, des scripts personnalisés pour le standard automatique ou les fichiers d'assistance conseillés par le service technique de Cisco. Vous pouvez télécharger des copies des fichiers de la carte vers votre machine afin de les archiver ou de les charger sur un autre périphérique.

IMPORTANT CCA utilise un service FTP propre pour transférer les fichiers de votre PC à la carte Compact Flash et vice-versa, pour l'UC500 et les autres périphériques Cisco IOS gérés. Vous devez désactiver tous les services FTP tiers actifs sur votre PC avant de transférer les fichiers. En l'absence de services FTP tiers, vérifiez le pare-feu et les paramètres de sécurité du réseau sur votre PC afin de vérifier si le trafic FTP est autorisé entre le PC et le périphérique. Vous pouvez aussi essayer de redémarrer votre PC.

Pour charger un fichier à partir de votre machine locale vers la carte Compact Flash d'un périphérique Cisco IOS, suivez les étapes suivantes.

ETAPE 1 Dans la fenêtre Gestion des fichiers, sélectionnez l'onglet **Fichiers**.

ETAPE 2 Dans l'arborescence **Périphérique/Système de fichiers**, sélectionnez le périphérique et accédez à l'emplacement sur la carte flash où vous souhaitez charger le fichier.

Veillez à charger le fichier à l'emplacement adéquat sur la mémoire flash. Par exemple, les fichiers audio pour la musique d'attente sont chargés dans le dossier `flash:\media`. Pour plus d'informations, consultez le dossier Cisco Unified CME sur Cisco.com.

ETAPE 3 Cliquez sur **Charger**.

Pour télécharger une copie des fichiers de la carte d'un périphérique Cisco IOS vers votre machine locale, suivez les étapes suivantes.

ETAPE 1 Dans la fenêtre Gestion des fichiers, sélectionnez l'onglet **Fichiers**.

ETAPE 2 Dans l'arborescence **Périphérique/Système de fichiers**, sélectionnez un périphérique et accédez au dossier de la mémoire flash contenant le fichier ou les fichiers que vous souhaitez télécharger.

ETAPE 3 Cliquez sur les noms des fichiers que vous souhaitez télécharger.

Vous pouvez utiliser les commandes CTRL-clic gauche et MAJ-clic gauche pour sélectionner plusieurs fichiers.

Le bouton **Télécharger** n'est pas actif tant que vous n'avez pas sélectionné au moins un fichier.

ETAPE 4 Cliquez sur **Télécharger**.

Pour supprimer des fichiers de la carte d'un périphérique Cisco IOS, suivez les étapes suivantes.

ATTENTION Ne supprimez pas l'image de démarrage du système ni aucun des fichiers suivants : vlan.dat, config.txt, env_vars, private_config.txt et system_env_vars.

ETAPE 1 Dans la fenêtre Gestion des fichiers, sélectionnez l'onglet **Fichiers**.

ETAPE 2 Dans l'arborescence **Périphérique/Système de fichiers**, accédez au dossier de la mémoire flash contenant le fichier ou les fichiers qui contient les dossiers ou fichiers que vous souhaitez effacer.

ETAPE 3 Cochez la case se trouvant sur la même ligne que le fichier ou le dossier que vous souhaitez supprimer.

Vous pouvez sélectionner plusieurs fichiers ou dossiers. Lorsque vous sélectionnez un dossier, tous les fichiers qu'il contient ainsi que ses sous-dossiers seront supprimés.

ETAPE 4 Cliquez ensuite sur **Appliquer**.

ETAPE 5 Si vous souhaitez définitivement supprimer le fichier d'un système de classe B, procédez au broyage du système de fichiers où il se trouve.

ETAPE 6 Procédez comme suit pour restaurer un fichier qui n'a pas été définitivement supprimé lors du broyage :

a. Cochez la case se trouvant sur la même ligne que le fichier que vous souhaitez restaurer.

b. Cliquez ensuite sur **Appliquer**.

ETAPE 7 Suivez ces étapes afin de broyer un système de fichiers de classe B :

a. Cochez la case se trouvant sur la même ligne que le système de fichiers que vous souhaitez broyer.

b. Cliquez ensuite sur **Appliquer**.

Lors du broyage d'un système de fichier, si certains fichiers ont été marqués pour une restauration, ces fichiers seront restaurés avant le broyage. Les fichiers marqués pour suppression sont supprimés avant le broyage. Le broyage peut prendre un certain temps.

Gestion des charges de téléphone

Pour accéder aux options de gestion des charges de téléphone, sélectionnez l'option **Maintenance** > **Gestion des charges de téléphone**.

- **Vue d'ensemble**
- **Supprimer les charges de téléphone**
- **Charger les charges de téléphone**
- **Mise à niveau des téléphones par glisser-déposer (SPA500, SPA300, 6900 et certains téléphones IP de la série 7900)**

Vue d'ensemble

Les onglets de la fenêtre Gestion des charges de téléphone vous permettent d'effectuer les opérations suivantes :

- Remplacer ou ajouter les charges de téléphone sur la carte-mémoire de l'UC500 en définissant un paquet logiciel pour l'UC500. Les charges du téléphone sont extraites du paquet logiciel et chargées sur l'UC500.
- Supprimer les charges du téléphone de la carte-mémoire de l'UC500 pour optimiser l'espace.
- Remplacer une charge de téléphone donnée en supprimant la version active et en chargeant une nouvelle version.

Pour charger les fichiers de charges du téléphone sur l'UC500, vous devez désactiver les serveurs TFTP ou FTP actifs sur le PC exécutant Configuration Assistant.

Supprimer les charges de téléphone

Sous l'onglet Supprimer les charges de téléphone, toutes les charges de téléphone de la mémoire flash de l'UC500 s'affichent dans la liste.

- Une case s'affiche dans la colonne Sélectionner pour chaque charge de téléphone disponible dans la mémoire de l'UC500.
- Les charges de téléphone non utilisées sur le système sont cochées et peuvent être supprimées en toute sécurité.
- Les charges de téléphone déjà actives sur votre système ne sont pas sélectionnées.

Pour supprimer une charge de téléphone, procédez comme suit :

ETAPE 1 Cliquez sur une ligne du tableau correspondant au téléphone pour la mettre en surbrillance.

ETAPE 2 Veillez à ce que la case **Sélectionner** correspondant au téléphone soit bien cochée.

Cliquez sur **Supprimer**.

ETAPE 3 Répétez les étapes ci-dessous pour les autres charges de téléphone.

Tandis que vous supprimez les charges de téléphone, le champ **Espace disponible sur la mémoire flash** est mis à jour afin d'afficher un aperçu de l'espace disponible après la suppression.

ETAPE 4 Lorsque vous en avez terminé avec la suppression des charges de téléphone, cliquez sur **OK**.

Charger les charges de téléphone

Pour charger les charges de téléphone vers l'UC500, suivez les étapes ci-dessous :

ETAPE 1 Cliquez sur **Parcourir** et accédez au paquet logiciel au format .zip de l'UC500 contenant les charges de téléphone que vous souhaitez charger ; par exemple `UC520-7.0.3.zip` ou `UC540-7.1.1.zip`.

Une fois le paquet logiciel sélectionné pour l'UC500, CCA analyse les charges de téléphone du paquet logiciel et celles utilisées sur votre système.

Au terme de l'analyse, la liste des charges de téléphone disponibles dans l'image définie s'affiche. Les charges de téléphone déjà actives sur votre système sont sélectionnées pour le chargement.

Cochez la case dans la colonne **Sélectionner** pour sélectionner ou annuler la sélection des charges de téléphone.

REMARQUE Les charges de téléphone 521_524 pour les téléphones CP 500 ne peuvent pas être sélectionnées. Vous devez appliquer la dernière mise à jour pour que ces téléphones fonctionnent correctement.

ETAPE 2 Cliquez sur **Charger** pour charger les charges de téléphone sélectionnées sur l'UC500.

ETAPE 3 Cliquez sur **OK** pour fermer la fenêtre Gestion des charges de téléphone.

Mise à niveau des téléphones par glisser-déposer (SPA500, SPA300, 6900 et certains téléphones IP de la série 7900)

La méthode de mise à niveau des charges de téléphone par glisser-déposer permet la mise à niveau des téléphones IP suivants :

- Téléphones IP Cisco 6901, 6911, 6921, 6941et 6961 (le modèle 6945 n'est pas pris en charge)
- Téléphones IP Cisco SPA500 (dont SPA525G et SPA525G2)
- Téléphones IP Cisco SPA 300
- Téléphones IP Cisco 7975, 7970, 7971, 7945, 7965, 7942, 7962, 7941, 7961, 7931, 7911, et 7906

Les lignes de conduite et les notes suivantes concernent la mise à niveau des charges de téléphone par glisser-déposer :

- Cette méthode est uniquement prise en charge par les téléphones ci-dessus. CCA affiche un message s'il ne reconnaît pas le fichier de charge de téléphone.
- Pour les téléphones Cisco de la série 79xx, vous devrez extraire les fichiers à partir du fichier .zip. Pour les téléphones Cisco SPA 500 et 300, vous devrez extraire le fichier .bin à partir du dossier compressé avant de le glisser-déposer dans la topologie. Les charges de téléphone pour les modèles Cisco 7921 et 7925 sont inclus dans des fichiers .tar que vous pouvez glisser-déposer vers l'icône de l'UC500.
- Vous ne pouvez pas glisser-déposer plus d'un fichier à la fois.
- Les charges de téléphone sont copiées vers le dossier `flash:phones/` se trouvant dans la mémoire Flash de l'UC500 et intégrées au sous-dossier correspondant au modèle de téléphone. Par exemple : `flash:phones/525` ou `flash:phones/5x5`.
- Une fois le microprogramme téléchargé, il peut être pris en charge à l'aide de la fenêtre Gestion des charges de téléphone sous CCA.

Pour mettre à niveau les téléphones IP Cisco par glisser-déposer, suivez les étapes ci-dessous :

ETAPE 1 Téléchargez le logiciel à partir de cisco.com. Un identifiant est nécessaire pour accéder à cette rubrique du site.

ETAPE 2 Démarrez CCA et connectez-vous au site client ou à l'UC500.

ETAPE 3 Sélectionnez **Accueil** > **Topologie** pour afficher la fenêtre Topologie si ce n'est pas encore fait.

ETAPE 4 Sur le PC exécutant CCA, localisez le fichier contenant le microprogramme du téléphone que vous avez téléchargé sur Cisco.com. Par exemple : `spa525g-7-4-3.bin`.

ETAPE 5 Dans la fenêtre Topologie, utilisez la souris pour déplacer le fichier de charge du téléphone (.zip ou .bin) à partir de votre PC et déposez-le sur l'icône de l'UC500.

Si CCA considère que le fichier est correct, une fenêtre s'affiche et vous invite à charger le fichier.

ETAPE 6 Cliquez sur **Charger**. La fenêtre affiche la progression du chargement et de la mise à niveau.

Au terme de la mise à niveau, vous serez invité à redémarrer tous les téléphones concernés.

Pour redémarrer le téléphone à l'aide de CCA, ouvrez la fenêtre Topologie, cliquez avec le bouton droit sur l'icône du téléphone et sélectionnez l'option **Redémarrer**.

18

Supervision

Consultez cette rubrique pour tout savoir sur les rapports et les données de diagnostic relatifs aux périphériques du site client. Pour accéder aux options de supervision, sélectionnez **Superviser** dans la barre de fonctions.

Les catégories de rapport et les outils de supervision suivants sont disponibles :

- **Réseau**
- **Sécurité**
- **Téléphonie**
- **Inventaire**
- **État**
- **Notification d'événements**
- **Journal système**
- **Messages système**
- **État multi-sites**

Réseau

Pour accéder aux options de supervision de l'état du réseau, sélectionnez **Superviser**> **Réseau** dans la barre de fonctions. Les rapports de supervision du réseau et les outils suivants sont disponibles :

- **Statistiques des ports**
- **Graphiques de bande passante**
- **Graphiques de liaison**
- **Utilisation sans fil**
- **État T1/E1/BRI**
- **DNS et hôtes**

Statistiques des ports

Pour accéder à la fenêtre Statistiques des ports, sélectionnez **Superviser** > **Réseau** > **Statistiques des ports** dans la barre de fonctions.

Les statistiques des ports sont disponibles pour les commutateurs Cisco ESW500 Series et les commutateurs Cisco CE520 uniquement.

Dans la fenêtre Statistiques des ports, vous pouvez afficher les données relatives aux ports, à savoir les statistiques sur la qualité de la liaison, les paquets abandonnés et le nombre total d'erreurs. Pour afficher un récapitulatif graphique des statistiques des ports, utilisez la fenêtre **Graphiques de bande passante**.

- Pour afficher ces statistiques pour les ports d'un périphérique donné, sélectionnez-le dans la liste Nom de l'hôte.
- Pour mettre les statistiques à jour, cliquez sur **Actualiser**.
- Pour réinitialiser les statistiques pour tous les ports du périphérique sélectionné, cliquez sur **Effacer les compteurs**.
- Cliquez sur **Enregistrer le rapport** pour enregistrer le rapport sur le disque local. Dans la fenêtre qui s'affiche, vous pouvez sélectionner le dossier de destination du rapport.

Ce tableau explique les informations figurant sous chaque onglet. Vue d'ensemble, Détails de transmission et Détails de réception.

Onglet	Colonne	Explication
Vue d'ensemble	Interface	Nom de l'interface de port (par exemple, sur un commutateur ESW-540-8P, les interfaces sont numérotées de g1 à g9.
	Description du port	Commutateurs ESW500 uniquement. Description textuelle du port, s'il est configuré sur le commutateur.
	Taux de transmission	Taux de transmission actuel en Mbits/s. Il comprend la transmission des paquets erronés ainsi que la retransmission en raison des collisions caractérisant les opérations en half-duplex.
	Taux de réception	Taux de réception actuel en Mbits/s. Il comprend les octets des paquets erronés, rejetés et sans destination.
	Utilisation de la bande passante de transmission	Pourcentage d'utilisation de la bande passante pour les transmissions en fonction du taux de transmission actuel et de la vitesse réelle.
	Utilisation de la bande passante de réception	Pourcentage d'utilisation de la bande passante pour la réception en fonction du taux de réception actuel et de la vitesse réelle.
	Taux de transmission de paquets	Taux de transmission actuel des paquets mis en forme. Comprend les paquets unicast, multicast et broadcast.
	Taux de réception de paquets	Taux de réception actuel des paquets mis en forme. Comprend les paquets unicast, multicast et broadcast.
	Taux de transmission de paquets multicast/ broadcast	Taux de transmission actuel des paquets multicast et broadcast mis en forme. Les paquets unicast ne sont pas pris en compte.
	Taux de réception de paquets multicast/ broadcast	Taux de réception actuel des paquets multicast et broadcast mis en forme. Les paquets unicast ne sont pas pris en compte.
	Total des paquets rejetés	Nombre total de paquets rejetés (transmission et réception).

Onglet	Colonne	Explication
Vue d'ensemble	Total des paquets erronés	Nombre total de paquets présentant des erreurs (transmission et réception).
Transmission de paquets	Interface	Nom de l'interface de port (par exemple, sur un commutateur ESW-540-8P, les interfaces sont numérotées de g1 à g9.
	Description du port	Commutateurs ESW500 uniquement. Description textuelle du port, s'il est configuré sur le commutateur.
	Unicast	Total des paquets unicast mis en forme transmis par un port. Exclut les paquets transmis avec des erreurs ou avec des adresses multicast ou broadcast cibles.
	Multicast	Total des paquets multicast mis en forme transmis par un port. Exclut les paquets transmis avec des erreurs ou avec des adresses unicast ou broadcast cibles.
	Diffusion	Total des paquets broadcast mis en forme transmis par un port. Exclut les paquets transmis avec des erreurs ou avec des adresses unicast ou multicast cibles.
	Total des paquets en collision	Total des paquets transmis avec succès après de 1 à 15 collisions. Comprend les paquets de tous les types d'adresse de destination et exclut les paquets rejetés en raison de ressources insuffisantes ou de collisions tardives.
	Paquets en collision en trop	Total des paquets non transmis après 16 collisions. Comprend les paquets pour tous les types d'adresse cible.
	Collision tardive	Nombre total de paquets rejetés en raison de collisions tardives détectées au cours de la transmission. Comprend tous les paquets présentant une collision après la transmission du 64e octet du paquet. Le préambule et le SFD ne sont pas repris dans ce décompte.

Onglet	Colonne	Explication
Réception de paquets	Interface	Nom de l'interface de port (par exemple, sur un commutateur ESW-540-8P, les interfaces sont numérotées de g1 à g9.
	Description du port	Commutateurs ESW500 uniquement. Description textuelle du port, s'il est configuré sur le commutateur.
	Unicast	Total des paquets unicast mis en forme reçus par un port. Exclut les paquets reçus avec des erreurs ou avec des adresses multicast ou broadcast cibles ou des paquets de trop grande ou trop petite taille. Les paquets rejetés ou sans destination sont également exclus.
	Multicast	Total des paquets multicast mis en forme reçus par un port. Exclut les paquets reçus avec des erreurs ou avec des adresses unicast ou broadcast cibles ou des paquets de trop grande ou trop petite taille. Les paquets rejetés ou sans destination sont également exclus.
	Broadcast	Total des paquets broadcast mis en forme reçus par un port. Exclut les paquets reçus avec des erreurs ou avec des adresses unicast ou multicast cibles ou des paquets de trop grande ou trop petite taille. Les paquets rejetés ou sans destination sont également exclus.
	Ignoré	Total des paquets rejetés en raison d'une bande passante ou d'une mémoire tampon en réception insuffisante ou parce que les règles de transfert indiquent qu'ils ne peuvent pas être envoyés.

Onglet	Colonne	Explication
Paquets reçus	Erreurs d'alignement	Nombre total des paquets reçus présentant des erreurs d'alignement. Comprend tous les paquets reçus et présentant une erreur FCS et un nombre d'octets non entier.
	Erreurs FCS	Nombre total de paquets reçus présentant des erreurs FCS. Exclut les paquets de trop petite taille présentant des erreurs FCS.
	Fragments de collision	Nombre total de trames de moins de 64 octets présentant un nombre entier d'octets et de mauvaises valeurs FCS.
	Paquets de trop petite taille	Nombre total de paquets reçus de moins de 64 octets présentant de bonnes valeurs FCS.
	Paquets de trop grande taille	Nombre total de paquets reçus de plus de 1518 octets présentant de bonnes valeurs FCS.

Graphiques de bande passante

Utilisez la fenêtre Graphiques de bande passante pour voir une estimation du trafic passant dans le périphérique que vous avez choisi dans la liste Nom de l'hôte. Les graphiques de bande passante sont disponibles uniquement pour les commutateurs CE520.

Pour afficher un graphique de bande passante pour un commutateur CE520, effectuez une des opérations suivantes :

- Cliquez à l'aide du bouton droit de la souris sur un membre du site dans la fenêtre Volet frontal et choisissez Graphiques de bande passante dans le menu contextuel.
- Cliquez à l'aide du bouton droit de la souris ou cliquez deux fois sur un membre du site dans la fenêtre Topologie et sélectionnez l'option Graphiques de bande passante dans le menu contextuel.
- Sélectionnez un membre du site dans une des fenêtres et choisissez **Superviser** > **Réseau** > **Graphiques de bande passante** dans la barre de fonctions.

Vue d'ensemble

Pour un commutateur Catalyst Express 500 sélectionné, un graphique de bande passante vous fournit les estimations suivantes :

- Le pourcentage de bande passante utilisé, à partir de l'affichage du graphique
- Le pourcentage de bande passante utilisé au cours de la dernière minute, au cours de la dernière heure, journée ou des deux dernières semaines.

Procédures

Cette fenêtre présente les onglets suivants :

- **Série chronologique**présente le pourcentage de bande passante utilisé, à partir du moment où la fenêtre s'affiche
- **Tendances**indique le pourcentage de bande passante utilisé pendant la minute passée ou une période d'une heure, d'un jour ou de deux semaines.

Série chronologique

Vous pouvez manipuler le graphique de cet onglet des manières suivantes :

- Sélectionner le type de graphique affiché
- Modifier les incréments de l'axe x
- Modifier l'intervalle d'interrogation
- Vous déplacer sur l'axe x

Sélectionner le type de graphique affiché

Dans la liste Type, cliquez sur Ligne ou Barre pour sélectionner un type de graphique. Dans un graphique à ligne, les points de données sont reliés par une ligne. Dans un graphique à barres, les points de données sont indiqués par la hauteur des barres.

Modifier les incréments de l'axe x

Par défaut, les intervalles de temps sur l'axe x sont de deux minutes. Pour raccourcir ou rallonger les intervalles, cliquez sur les boutons de Zoom.

Modifier la fréquence d'interrogation

À intervalle régulier, Configuration Assistant demande aux périphériques pris en charge de recueillir des informations sur le périphérique et la connexion. Cet intervalle est appelé Fréquence d'interrogation graphique. Pour le configurer, ouvrez la fenêtre Préférences et cliquez sur l'onglet Général, puis choisissez une valeur pour le champ Fréquence d'interrogation graphique.

Remarque : lorsque le niveau de trafic d'un périphérique chute considérablement, vous ne verrez pas de changement dans le graphique pendant au moins 15 minutes, quelle que soit la configuration de la fréquence d'interrogation graphique.

Vous déplacer sur l'axe x

La barre de défilement au bas du graphique vous permet de déplacer l'affichage afin de visualiser les points hors du graphique. Vous pouvez ensuite revenir vers la droite afin d'afficher les données les plus récentes.

Remarque : Le graphique est mis à jour chaque fois que le périphérique est interrogé. Vous pouvez modifier l'intervalle d'interrogation (la fréquence de collecte des données) en sélectionnant et en utilisant la fenêtre Préférences.

Tendances

Le graphique de cet onglet concerne l'ancienne utilisation de la bande passante. Vous voyez donc les données historiques quand vous ouvrez cet onglet - par défaut, les données de bande passante du périphérique relatives aux 60 dernières secondes. En cliquant sur les boutons Tendances de l'onglet, vous pouvez aussi voir les données relatives aux 60 dernières minutes, 24 dernières heures ou aux 14 derniers jours. Les données apparaissent toujours sous forme de graphique à barres. Les intervalles de l'axe x sont fixés pour chaque graphique de tendance ; vous pouvez les allonger ou les écourter en cliquant sur les différents boutons.

Graphiques de liaison

Les graphiques de liaison sont disponibles pour les commutateurs Cisco ESW500 Series et les commutateurs Cisco CE520 uniquement.

Pour afficher un graphique de liaison, une extrémité de la liaison doit se connecter à un port d'un périphérique membre. Vous ne pouvez pas afficher le graphique de liaison concernant des périphériques candidats.

Pour afficher un graphique de bande passante, procédez comme suit :

- Sélectionnez **Superviser** > **Réseau** > **Graphiques de liaison** dans la barre de fonctions.
- Cliquez sur un lien dans la fenêtre Topologie et sélectionnez l'option **Graphiques de liaison** dans le menu contextuel.

REMARQUE Vous pouvez modifier l'intervalle d'interrogation en sélectionnant et en utilisant la fenêtre Préférences.

Vue d'ensemble

Les graphiques de liaison présentent les éléments suivants :

- Pourcentage de bande passante utilisé
- Nombre d'octets transmis et reçus
- Nombre de paquets transmis et reçus (répartis en paquets broadcast/multicast et unicast)
- Total des erreurs et des paquets abandonnés

Dans la fenêtre Graphiques de liaison, vous pouvez effectuer les opérations suivantes :

- **Sélectionner les types de données affichées**
- **Sélectionner le type de graphique affiché**
- **Modifier les incréments des axes**
- **Visualiser une longue plage de données**

Procédures

Pour sélectionner un port différent de celui affiché dans le champ **Interface**, surfrappez, utilisez les boutons de défilement ou cliquez sur l'icône de sélection de port. Si vous optez pour cette dernière solution, la fenêtre Sélectionner l'interface s'ouvre pour afficher le panneau frontal du périphérique. Cliquez pour sélectionner le port et cliquez ensuite sur **OK**. Voir la rubrique **Sélectionner l'interface, page 592**.

Sélectionner les types de données affichées

Pour sélectionner un type de données, cliquez sur **% d'utilisation**, **Paquets transmis / reçus**, **Méthodes de transfert des paquets** ou **Interruptions et erreurs des paquets** dans la liste **Données**. Les résultats pour chaque sélection font l'objet du tableau ci-dessous :

Type de données	Résultats
% d'utilisation	Affiche le pourcentage de bande passante utilisé sur le port correspondant au lien. Par exemple, si la bande passante de la liaison est 100 Mbits/s et si 20 Mo sont utilisés à un moment donné, le graphique indique 20 % pour ce moment.

Type de données	Résultats
Paquets transmis / reçus	Affiche deux graphiques : transmis (rouge) et reçus (bleu). Le graphique Octets transmis indique le nombre d'octets transmis sur le port correspondant à la liaison. Le graphique Octets reçus indique le nombre d'octets reçus sur le port correspondant à la liaison.
Méthodes de transfert des paquets	Affiche deux graphiques : Paquets broadcast/multicast (rouge) et Paquets unicast (bleu). Le graphique Paquets broadcast/multicast indique le nombre de paquets broadcast et multicast reçus et transmis sur le port correspondant au lien. Le graphique Paquets unicast indique le nombre de paquets unicast reçus et transmis sur le port correspondant à la liaison.
Interruptions et erreurs des paquets	Affiche deux graphiques : Total des erreurs (bleu) et Total des paquets interrompus (rouge). Le graphique Total des erreurs affiche le nombre total des paquets présentant des erreurs recensés sur le port depuis la dernière réinitialisation des compteurs. Le graphique Total des paquets interrompus indique le nombre total de paquets interrompus sur le port correspondant à la liaison. Les paquets sont interrompus en raison du manque de mémoire tampon ou de bande passante ou à cause d'un filtre défini par l'utilisateur sur le périphérique.

Sélectionner le type de graphique affiché

Dans la liste **Type**, cliquez sur **Ligne**, **Barre**, **Histogramme**, **Secteur** ou **Zone de stack** pour sélectionner un type de graphique. La présentation de chaque graphique fait l'objet du tableau.

Type de graphique	Présentation
Ligne	Les points représentant les données sont reliés par une droite.
Barre	Les points de données sont représentés par la hauteur des barres.
Histogramme	Graphique composé de plusieurs barres de couleurs différentes et empilées.
Secteur	Les points de données sont reliés par une ligne et la surface sous cette ligne est pleine.
Zone de stack	Graphique composé de plusieurs surfaces de couleurs différentes et empilées.

Modifier les incréments des axes

Par défaut, les intervalles de temps sur l'axe x sont de deux minutes. Pour raccourcir ou rallonger les intervalles, cliquez sur les boutons de **Zoom**.

Cochez **Échelle logarithmique** si vous préférez une croissance logarithmique et non arithmétique.

Visualiser une longue plage de données

La barre de défilement au bas du graphique vous permet de déplacer l'affichage afin de visualiser les points qui seraient sortis du graphique. Vous pouvez ensuite revenir vers la droite afin d'afficher les données les plus récentes.

REMARQUE Le graphique est mis à jour chaque fois que le périphérique est interrogé. Vous pouvez modifier l'intervalle d'interrogation (la fréquence de collecte des données) à l'aide de la fenêtre Préférences.

Sélectionner l'interface

Cette fenêtre s'affiche lorsque vous cliquez sur l'icône correspondante dans une fenêtre de Configuration Assistant. Elle présente le panneau frontal du commutateur sélectionné. Utilisez la fenêtre pour sélectionner une interface sur le commutateur.

Suivez les étapes ci-dessous :

ETAPE 1 Cliquez sur l'interface que vous souhaitez utiliser.

Les interfaces inaccessibles sont grisées.

ETAPE 2 Cliquez sur **OK**. Vous revenez ensuite à la fenêtre de Configuration Assistant. Le numéro de l'interface sélectionnée s'affiche dans le champ Interface.

Utilisation sans fil

Pour accéder au rapport d'utilisation sans fil, sélectionnez **Superviser** > **Réseau> Utilisation sans fil** dans la barre de fonctions.

Les données d'état pour ces clients sans fil sont uniquement disponibles pour les périphériques suivants :

- Plateformes Cisco UC500 et routeurs sécurisés Cisco SR500 avec point d'accès intégré
- Points d'accès autonomes Cisco AP521
- Points d'accès Dual-band Single-radio Cisco AP541N

L'état du contrôleur WLAN n'est pas affiché.

Sélectionnez un périphérique sans fil dans la liste Nom de l'hôte.

Le rapport Utilisation sans fil affiche les données suivantes pour chaque client connecté.

- Adresse MAC
- Nom
- Adresse IP
- Numéro de VLAN
- SSID (secure site identifier)
- Type de gestion des clés
- Type de chiffrement
- Flux de données, en Mbits/s

- Puissance du signal en dBM pour les clients connectés à l'AP521 et aux points d'accès intégrés UC500
- RSSI (indication de la puissance du signal en réception) pour les points d'accès AP541N

  Le RSSI indique la puissance du signal radio pour les clients connectés aux points d'accès AP541N. La valeur affichée est comprise entre 1 et 100.
- Paquets en entrée/sortie
- Octets en entrée/sortie

État T1/E1/BRI

En présence d'une interface T1/E1 ou BRI, sélectionnez l'option **Superviser** > **Réseau** > **État T1/E1/BRI** dans la barre de fonctions pour afficher le résultat des commandes IOS telles que **show isdn status** et **show controller** pour bri, t1 ou e1 selon les interfaces disponibles.

DNS et hôtes

Sélectionnez l'option **DNS et hôtes** pour afficher le résultat de la commande **show hosts** pour le site du client. Le résultat comprend le nom d'hôte et le domaine de l'UC500 ou du SR500 ainsi que les adresses IP des serveurs DNS primaires et secondaires.

Sécurité

Pour accéder aux options de supervision, sélectionnez **Superviser** > **Sécurité** dans la barre de fonctions. Les rapports de sécurité en mode Expert sont décrits dans la liste ci-dessous.

Ces rapports sont au format texte et sont créés à partir des commandes Cisco IOS.

REMARQUE Ces rapports permettent d'aider le Small Business Support Center (SBSC) à résoudre les problèmes associés au déploiement de Cisco SBCS. Vous devrez maîtriser Cisco IOS et la ligne de commande pour interpréter correctement les données composant le rapport.

Rapport de sécurité	Description
Client et serveur EZVPN	Affiche le résultat de la commande **show crypto** qui permet d'obtenir des informations sur les associations de sécurité IKE, la configuration distante d'EasyVPN, les paramètres utilisés par les SA, les sessions VPN actives et les statistiques de l'accélérateur de chiffrement.
État du VPN site-à-site	Affiche le résultat de la commande **show crypto** qui permet d'obtenir des informations sur les associations de sécurité IKE, les sessions VPN actives, les paramètres utilisés par les SA, et les statistiques de l'accélérateur de chiffrement.
État du VPN SSL	Affiche le résultat des commandes **show tcp** et **show webvpn** qui permet d'obtenir des informations sur les terminaisons des connexions TCP, les sessions utilisateurs SSL VPN et les statistiques du tunnel SSL VPN. Pour afficher les données des sessions utilisateurs SSL VPN propres à un utilisateur donné, entrez le nom d'utilisateur et cliquez sur **Requête**.
Pare-feu	Affiche le résultat des commandes **show access-list** et **show ip inspect session**.
NAT	Affiche le résultat des commandes **show ip nat** et **show ip route** permettant d'obtenir des statistiques sur le NAT, les routages IP et les conversions NAT.
État du VPN	Voir la rubrique **État du VPN, page 595**.

État du VPN

La fenêtre État du VPN s'affiche lorsque vous sélectionnez **Superviser** > **Sécurité** > **État du VPN** dans la barre de fonctions.

EasyVPN

Cet onglet vous permet de contrôler l'état des tunnels EasyVPN.

Sélectionnez le périphérique faisant l'objet du rapport dans la liste Nom de l'hôte. Les données sont automatiquement ajoutées au rapport.

État du VPN	Description
UP-ACTIVE	Fonctionnel et actif.
UP-IDLE	Fonctionnel mais aucune activité n'est détectée.
UP-NO-IKE	Fonctionnel mais aucune activité IKE (Internet Key Exchange) n'est détectée.
DOWN-NEGOTIATING	Non opérationnelle, le périphérique négocie la liaison.
DOWN	En panne.

SSL VPN

Cet onglet vous permet d'assurer le suivi de l'état des tunnels VPN SSL (secure socket layer).

Téléphonie

Pour accéder aux options de supervision relatives aux fonctions de téléphonie, sélectionnez **Superviser** > **Téléphonie** dans la barre de fonctions. Les rapports de téléphonie en mode Expert sont décrits dans la liste ci-dessous.

Ces rapports sont au format texte et sont créés à partir des commandes Cisco IOS et CUE.

REMARQUE Ces rapports permettent d'aider le Small Business Support Center (SBSC) à résoudre les problèmes associés au déploiement de Cisco SBCS. Vous devrez maîtriser CUE, Cisco IOS et la ligne de commande pour interpréter correctement les données composant les rapports.

Rapport de téléphonie	Description
Téléphones et postes	**Téléphones**. Affiche les données de configuration interne et l'état en lecture seule des téléphones et des numéros de poste, dont les balises, l'adresse MAC, le type de téléphone, le nom d'utilisateur, l'affectation des boutons, le modèle utilisé, l'adresse IP, la charge utilisée et l'état. **Postes**. Pour chaque numéro de poste, ce rapport affiche la balise DN, le numéro de poste interne, le type de ligne, le libellé, le nom d'utilisateur, le type de trunk, le COR entrant et l'état du canal. Le cas échéant, le numéro d'interphone et son libellé s'affichent. Les numéros d'interphone commencent par une lettre (par exemple : A502).
Groupement de postes	Affiche les données de configuration interne des groupements de postes, dont la balise, le numéro pilote, le type, les membres, les paramètres relatifs au délai d'expiration et la cible de la fonction Transfert si pas de réponse vers. **Rechercher un membre du groupe**. Entrez un numéro de poste ou une série de numéros séparés par des virgules pour savoir à quels groupements de postes le numéro appartient.
Groupes d'appel	Affiche les données de configuration interne des groupements de postes, dont la balise, le numéro pilote, le type, les membres, les paramètres relatifs au délai d'expiration et la cible de la fonction Transfert si pas de réponse vers. **Rechercher un membre du groupe**. Entrez un numéro de poste ou une série de numéros séparés par des virgules pour savoir à quels groupes le numéro appartient. Cliquez sur **Afficher le récapitulatif de la configuration** pour afficher les données relatives à chaque groupe d'appel.

Rapport de téléphonie	Description
Fichiers du serveur TFTP	Affiche le nom des fichiers du serveur TFTP stockés sur la mémoire flash. Le cas échéant, le nom du périphérique propriétaire du fichier et son alias figurent également dans la liste.
Dial-peers	Affiche les données de configuration interne des dial-peers POTS et VoIP configurés sur le système. **POTS**. Pour les dial-peers POTS, les données comprennent le numéro de balise, le port, la description, le modèle cible, la cible entrante, le nom de profil de traduction, les codes de transfert et les préférences de trunk. **VoIP**. Pour les dial-peers VoIP, les données comprennent le numéro de balise, la description, le modèle cible, la catégorie vocale, la cible de la session, le relais DTMF et le codec.
Profils de traduction	Affiche les données de configuration interne pour les profils de traduction et les règles de traduction. Offre la possibilité de tester les règles de traduction.
État du trunk SIP	Affiche le résultat des commandes **show sip-ua** relatives à l'état de service SIP, l'inscription, les compteurs et les statistiques.
Modèle de téléphone	Affiche les propriétés du modèle interne pour les touches et les boutons des modèles de téléphone IP sélectionnés. Ces données sont en lecture seule. Les modèles ne peuvent pas être modifiés avec Configuration Assistant.

Rapport de téléphonie	Description
État de la messagerie	Lorsque vous sélectionnez un rapport d'état de la messagerie, Configuration Assistant affiche la fenêtre Progression tant que la connexion à la messagerie du module CUE est active et que les résultats de la commande sont rassemblés. Les rapports d'état de la messagerie sont accessibles au format texte : **Système**. Affiche le résultat des commandes d'affichage permettant d'obtenir des informations sur l'horloge et les fuseaux horaires, les privilèges affectés aux groupes configurés, les versions des logiciels et des applications, les licences achetées pour le système et les logiciels installés. **Messagerie**. Affiche le résultat des commandes d'affichage de la messagerie permettant d'obtenir des informations sur les messageries configurées et l'état de stockage, les valeurs par défaut pour toutes les messageries et les statistiques d'usage de la messagerie. **Calendrier**. Affiche les plannings et les vacances configurées pour le système au format texte. **Autres**. Affiche le résultat des commandes permettant d'obtenir des informations sur les applications configurées, les messages d'accueil du standard automatique, les noms de fichier de script et les types de déclencheurs actifs.
État DSP	Le rapport État DSP affiche les résultats détaillés des commandes d'affichage relatives au matériel DSP, à la ferme DSP, aux groupes, aux erreurs et au DSP de voix active/de signalement.

Rapport de téléphonie	Description
Paquet logiciel	Le rapport Paquet logiciel contient les données de version du paquet et des composants, l'utilisation de la mémoire flash, l'état CUE ainsi que les types de téléphone pris en charge pour le paquet logiciel de l'UC500 actuellement installé. Les données de version pour les paquets logiciels de l'UC500 antérieurs à la version 7.0.0 ne sont pas disponibles.
Etat Mobilité de poste	Le rapport Etat Mobilité de poste contient les téléphones concernés et l'état Mobilité de poste correspondant ainsi que le profil du téléphone et le profil de l'utilisateur. Ces données sont en lecture seule. Pour configurer ces paramètres, voir **Mobilité de poste, page 343**.

Inventaire

Pour afficher un rapport d'inventaire relatif à un site client ou un site isolé, sélectionnez l'option **Superviser** > **Inventaire**.

Le rapport d'inventaire d'un site client contient les types de périphériques, les numéros de série, les adresses IP et les versions des logiciels pour le site. Vous pouvez aussi sélectionner un seul périphérique pour lequel vous pourrez afficher les détails d'inventaire.

Les données de la fenêtre sont en lecture seule. Pour chaque périphérique du site client, l'inventaire contient les éléments suivants :

- Nom de l'hôte
- Type de périphérique
- Numéro de série
- Numéro de version matérielle (identifiant de version)
- Adresse MAC
- Adresse IP
- Version du logiciel installé

- Emplacement du système
- Temps de fonctionnement du système

Si vous n'avez pas affecté de nom d'hôte à un commutateur du site, le nom d'hôte **switch-***<numéro>* est affecté par défaut. Le numéro indique l'ordre dans lequel le commutateur a été ajouté au site.

Cliquez sur **Détails** pour afficher les détails propres au périphérique. Voir la rubrique **Détails de l'inventaire, page 601**.

Cliquez sur **Actualiser** pour mettre à jour la fenêtre.

Détails de l'inventaire

Cette fenêtre s'affiche lorsque vous sélectionnez un périphérique de routage et que vous cliquez sur **Détails** dans la fenêtre Inventaire.

La fenêtre affiche les données du périphérique en fonction de ses composants, de la description, des références des pièces, de la version du matériel, de la carte de circuit imprimé, du numéro de série et de produit. La description fournit des détails sur le composant. La référence des pièces correspond au numéro d'ordre du composant.

Si vous savez qu'une modification a eu lieu et souhaitez visualiser les modifications, cliquez sur **Actualiser**. Configuration Assistant contrôle les composants et affiche les informations lorsque des composants sont supprimés ou ajoutés.

Journal système

Le journal système affiche le résultat de la commande **show log**.

État multi-sites

Vous devez être directement connecté à un port LAN sur l'UC500 ou sur le routeur sécurisé SR520-T1 pour afficher l'état multi-sites.

Le rapport État multi-sites affiche le résultat de la commande Cisco IOS **show crypto session detail**. Cette commande dresse la liste de toutes les sessions VPN actives ainsi que des éléments IKE (Internet Key Exchange) et IPsec SA (associations de sécurité) pour chaque session VPN.

Voir la rubrique **Suivi de l'état multi-sites, page 511**.

État

Vous pouvez surveiller une série de valeurs relatives à l'état d'un périphérique afin d'éviter les temps d'arrêt et d'assurer l'efficacité du fonctionnement de votre réseau. Ces données vous fournissent des indications sur l'utilisation de la bande passante, l'alimentation électrique par câble Ethernet, le processeur et la mémoire ainsi que sur la température du périphérique et le pourcentage d'erreurs au niveau des paquets.

Pour accéder aux valeurs d'état, sélectionnez **Superviser** > **État** dans la barre de fonctions.

Configuration Assistant dispose également de fonctions se concentrant sur l'utilisation de ressources spécifiques :

- Pour plus d'informations sur l'utilisation de la fonction PoE, sélectionnez l'option **Configurer** > **Ports** > **Paramètres des ports**.
- Pour de plus amples informations sur l'utilisation de la bande passante au fil du temps, sélectionnez **Superviser** > **Réseau**>**Graphiques de bande passante**.
- Pour de plus amples informations sur l'utilisation de la liaison au fil du temps, sélectionnez **Superviser** > **Réseau** > **Graphiques de liaison**.
- Pour plus d'informations sur les erreurs de paquets, sélectionnez l'option **Superviser** > **Réseau** > **Statistiques des ports**.

Cette fenêtre vous permet d'afficher un maximum de cinq périphériques présentant les résultats les plus importants pour les catégories que vous avez choisi de surveiller. Cliquez sur les barres dans la fenêtre pour afficher des données supplémentaires.

Pour de plus amples informations, cliquez sur **Détails** afin d'ouvrir la fenêtre Détails de l'état. Voir la rubrique **Détails de l'état, page 603**.

Détails de l'état

Cette fenêtre s'affiche lorsque vous cliquez sur **Détails** dans la fenêtre État du système (**Superviser** > **État**). Pour un affichage graphique de ces données, sélectionnez l'option **Accueil** > **Tableau de bord**.

Lorsque vous avez terminé de travailler dans cette fenêtre, cliquez sur **OK**.

La fenêtre Détails de l'état présente les onglets suivants :

- **Vue d'ensemble**
- **Utilisation de la bande passante**
- **Erreurs de paquet**
- **Utilisation du PoE**
- **Température**
- **Utilisation du processeur**
- **Utilisation de la mémoire**

Vue d'ensemble

Cet onglet présente les mesures générales pour chacune des catégories surveillées et pour chaque périphérique du réseau concerné par ces catégories. Ce tableau explique les colonnes de l'onglet.

Colonne	Explication
Nom de l'hôte	Nom d'hôte d'un périphérique autonome ou noms d'hôte des périphériques composant votre communauté
Utilisation de la bande passante	Bande passante moyenne utilisée pour la réception et la transmission des paquets depuis le dernier intervalle de sondage.
Erreurs de paquet	Pourcentage global (entrée et sortie) des paquets erronés
Utilisation du PoE	Pourcentage de watts PoE utilisés
Température	Température en Celsius

Colonne	Explication
Utilisation du processeur	Pourcentage de l'utilisation du processeur au cours des 5 dernières secondes
Utilisation de la mémoire	Pourcentage de la mémoire utilisée

Utilisation de la bande passante

Cet onglet présente le pourcentage de bande passante utilisé pour la réception des paquets, le pourcentage pour l'envoi de paquets ainsi que la moyenne des deux.

Vous pouvez afficher la fenêtre Graphiques de bande passante pour visualiser l'utilisation de la bande passante d'un périphérique au fil du temps. La fenêtre Graphiques de liaison indique les ports présentant le trafic le plus important.

Erreurs de paquet

Cet onglet présente le pourcentage de paquets en entrée et en sortie présentant des erreurs ainsi qu'un pourcentage d'erreur global.

Utilisation du PoE

Pour les périphériques compatibles avec le PoE (alimentation par câble Ethernet), cet onglet présente le pourcentage de watts affectés à l'alimentation par câble Ethernet utilisé ainsi que le total, la valeur utilisée et le volume disponible. Si vous ajoutez des points d'accès et des téléphones IP à votre réseau, reliez-les à des périphériques présentant une faible utilisation de l'alimentation PoE.

Température

Pour les périphériques capables de mesurer précisément la température, cet onglet affiche la température actuelle, la limite de surchauffe et le seuil critique pour chaque périphérique. Ces valeurs sont exprimées en Celsius. Pour les autres périphériques, la température présente les états OK, Normal, Erreur ou N/A, ce dernier indiquant que la température actuelle, la limite de surchauffe ou le seuil critique n'ont pas pu être détectés.

Utilisation du processeur

Cet onglet affiche pour chaque périphérique le pourcentage de la capacité du processeur utilisée au cours des 5 dernières secondes, les 60 dernières secondes et les 5 dernières minutes.

Utilisation de la mémoire

Cet onglet présente le pourcentage de mémoire utilisé et le nombre total d'octets, le nombre d'octets utilisés et le nombre d'octets libres.

Notification d'événements

La fenêtre Notification d'événements s'affiche lorsque vous effectuez l'une des opérations suivantes :

- Lorsque vous cliquez sur une icône d'événement dans la barre d'état ou dans la fenêtre Topologie.
- Lorsque vous sélectionnez l'option **Superviser** > **Notification d'événements** dans la barre de fonctions.
- Lorsque vous cliquez sur l'icône Notification d'événements dans la barre d'outils.

Vue d'ensemble

Un événement est un état détecté par Configuration Assistant et que le programme souhaite vous signaler. Voici les exemples d'événements :

- Température du périphérique élevée
- Ventilateur en panne sur un périphérique
- Port désactivé pour l'administration
- Port présentant un problème de correspondance duplex
- Port pouvant être configuré avec Smartports
- Périphérique inconnu sur le réseau
- Conflits VLAN

Pour vous signaler un événement, Configuration Assistant affiche une fenêtre contextuelle. Il présente également une icône sur laquelle vous pouvez cliquer dans la barre d'état et dans la fenêtre Topologie sous l'événement concerné. Lorsque le pointeur survole l'icône de l'événement dans la fenêtre Topologie, un résumé de l'événement s'affiche.

L'aspect de l'icône dépend du type d'événement. Les types d'événement varient en fonction de leur numéro : plus le numéro est petit, plus la réaction est urgente.

Si Configuration Assistant détecte plusieurs événements, toutes les icônes s'affichent dans la fenêtre Topologie. Dans la barre d'état, seule l'icône de l'événement le plus urgent s'affiche.

La fenêtre Notification d'événements vous donne une description complète des événements détectés sur votre réseau. Utilisez cette fenêtre pour les opérations suivantes :

- Indiquer à Configuration Assistant que vous avez connaissance de l'événement.
- Demander à Configuration Assistant de réagir, dans la mesure du possible.
- Désactiver les voyants d'alerte sur les commutateurs.

Procédures

L'onglet Événements présente la description de tous les événements de votre réseau. Vous pouvez les consulter et utiliser Configuration Assistant pour les résoudre (si possible)

Afin d'afficher un sous-ensemble des informations, cliquez sur **Filtre** et utilisez la fenêtre Filtre des notifications. Voir la rubrique **Filtre des notifications, page 607**.

Lorsque vous avez terminé, cliquez sur **OK**.

Ce tableau explique le contenu de l'onglet.

Colonne	Explication
Type	Indique s'il est urgent ou non de résoudre l'événement. Plus le nombre est bas, plus l'événement est urgent.
Heure	Heure à laquelle l'événement s'est produit.
Description de l'événement	Courte description de ce qui s'est produit. Lorsque vous sélectionnez un événement, une description plus longue s'affiche sous la liste des événements.
Peut être résolu	**Oui** si Configuration Assistant peut résoudre l'événement, **Non** si c'est impossible. Pour demander à Configuration Assistant de résoudre un événement, mettez-le en surbrillance et cliquez sur **Résoudre**. Configuration Assistant affiche une fenêtre permettant de résoudre l'événement.

Colonne	Explication
Accepté	Les cases cochées indiquent que vous avez connaissance des événements. Si vous cliquez sur **Accepter tout**, vous acceptez tous les événements en une fois. Lorsque l'événement est accepté, l'icône est réduite.
Périphérique	Périphérique concerné par l'événement.

Filtre des notifications

Cette fenêtre s'affiche lorsque vous cliquez sur **Filtre** dans la fenêtre Notification d'événements. Elle vous permet de limiter les types d'événement s'affichant dans la fenêtre.

Suivez les étapes ci-dessous :

ETAPE 1 Sous **Types**, annulez la sélection des cases correspondant aux types d'événement à filtrer. Ces événements n'apparaîtront donc pas dans la fenêtre Notification d'événements.

ETAPE 2 Cliquez sur **Définir les valeurs par défaut** si vous souhaitez que toutes les cases soient à nouveau cochées.

Lorsque vous avez terminé, cliquez sur **OK**.

Messages système

La fenêtre Messages système vous permet d'afficher les messages en provenance des périphériques se trouvant sur le site du client.

Pour accéder à la fenêtre Messages système, sélectionnez **Superviser** > **Message système** dans la barre de fonctions.

Procédures

Suivez les étapes suivantes pour afficher et filtrer les messages système.

ETAPE 1 Dans la liste Nom de l'hôte, sélectionnez un périphérique pour lequel vous souhaitez afficher les messages ou sélectionnez **Tous les périphériques** pour afficher les messages envoyés par tous les périphériques de la communauté.

ETAPE 2 Cliquez sur un en-tête du tableau afin de classer les messages en fonction de vos besoins. Par défaut, les messages sont classés par importance.

ETAPE 3 Pour afficher les détails d'un message en particulier, mettez la ligne du tableau correspondante en surbrillance. Les détails du message s'affichent dans la zone sous le tableau.

ETAPE 4 *Facultatif* : cliquez sur **Filtre** pour ouvrir la fenêtre Filtre des messages système vous permettant de définir des critères permettant de limiter le nombre de messages affichés. Voir la rubrique **Filtre des messages système, page 608**.

ETAPE 5 *Facultatif* : Cliquez sur **Enregistrer le rapport** pour enregistrer le contenu de la fenêtre dans un fichier au format séparé par des virgules. Le nom par défaut se présente sous la forme d'un horodatage unique.

ETAPE 6 Lorsque vous avez terminé, cliquez sur **OK**.

Filtre des messages système

Cette fenêtre s'affiche lorsque vous cliquez sur **Filtre** dans la fenêtre Messages système. Elle vous permet de limiter les types d'événement s'affichant dans la fenêtre.

Pour filtrer les messages système, procédez comme suit :

ETAPE 1 Sous **Niveaux de gravité**, annulez la sélection des cases correspondant aux niveaux de gravité à ne pas prendre en compte. Les messages qui présentent ces niveaux de gravité n'apparaîtront pas dans la fenêtre Messages système.

ETAPE 2 Cliquez sur **Définir les valeurs par défaut** si vous souhaitez que toutes les cases soient à nouveau cochées.

Lorsque vous avez terminé, cliquez sur **OK**.

19

Dépannage

Configuration Assistant dispose de plusieurs outils permettant de dépanner votre système :

- **Diagnostic des circuits (boucle de rappel T1)**
- **Diagnostic du réseau**
- **Diagnostic de la téléphonie**
- **Diagnostic de connectivité CUE**
- **Diagnostic de la sécurité**
- **Débogages généraux**
- **Commandes IOS Exec**
- **Commandes CUE Exec**
- **Création d'un journal de dépannage système**
- **Liaisons et connectivité (commutateurs CE520)**

Diagnostic des circuits (boucle de rappel T1)

Pour accéder à l'outil de diagnostic de boucle de rappel T1 permettant de dépanner le circuit T1, sélectionnez l'option **Dépanner** > **Diagnostic du circuit** > **Boucle de rappel T1**.

Ce diagnostic n'est valable qu'en présence d'un UC500 doté d'une interface vocale T1 ou d'un routeur SR520-T1 avec une connexion WAN T1.

Vue d'ensemble

Utilisez l'outil de diagnostic Boucle de rappel T1 pour effectuer un test de boucle de rappel local ou à distance sur un circuit T1.

Pour les plateformes UC500 dotées d'une interface T1, vous pouvez aussi effectuer un test de taux d'erreur binaire (BERT). Pour lancer le test BERT, la connexion T1 doit être active et le circuit doit disposer d'une boucle d'extrémité. Si tel n'est pas le cas, les options BERT ne seront pas disponibles.

En fonctionnement normal, le champ réservé aux erreurs BERT doit toujours présenter la valeur 0. Si le taux d'erreur binaire est supérieur à 0, contactez votre fournisseur de services ou le responsable du circuit T1 (Telco).

Le diagnostic BERT n'est pas pris en charge sur les plateformes SR520-T1.

Procédures

Pour effectuer un diagnostic de boucle de rappel, procédez comme suit :

ETAPE 1 Sélectionnez un hôte dans la liste Nom de l'hôte.

ETAPE 2 Sélectionnez l'interface T1. Dans la plupart des cas, une seule interface figure dans la liste.

ETAPE 3 Sélectionnez un **Type de boucle de rappel** dans la liste déroulante.

Les types de boucle de rappel disponibles varient selon que le diagnostic concerne une plateforme UC500 ou un routeur sécurisé SR520-T1 et si vous avez paramétré ou non une boucle de rappel FDL (liaison de données d'infrastructure).

Les boucles de rappel suivantes sont disponibles sur l'UC500 :

- Diag
- Ligne locale
- Données utiles locales
- IBOC distant
- Ligne ESF distante (si le Type FDL est défini sur ansi, att ou les deux)
- Données utiles ESF distantes (si le Type FDL est défini sur ansi, att ou les deux)

Les boucles de rappel suivantes sont disponibles sur le SR520-T1 :

- Local.
- À distance
- Données utiles

ETAPE 4 Vous pouvez éventuellement choisir un type FDL. Les types disponibles sont **ansi (ANSI T1.403)**, **att (AT&T TR54016)**, **les deux** ou **non défini**.

Le type FDL est associé à des fonctions de test à distance supplémentaires, notamment l'envoi de données de signalement hors bande entre les différents sites reliés par un circuit T1.

ETAPE 5 Cliquez sur **Rechercher** pour créer une boucle de rappel sur le circuit.

Le message **Récapitulatif** affiché au-dessus de la fenêtre de résultats indique l'état de la boucle (boucle à l'extrémité locale, boucle à l'extrémité distante, aucune boucle détectée).

Vous pouvez cliquer sur **Effacer les compteurs** pour remettre les compteurs à zéro.

ETAPE 6 Pour lancer un test BERT lorsque la boucle est active, suivez les étapes suivantes :

a. Sélectionnez un modèle. Les options disponibles sont **Tous les 0**, **Tous les 1**, **2^11-1**, **0 et 1 en alternance**, **2^20 QRSS**, **0.151** et **2^15-1 QRW**.

b. Définissez un intervalle compris entre 1 et 14 400 minutes.

c. Cliquez sur **Démarrer le test BERT**

d. Cliquez sur **Annuler le test BERT en cours** pour interrompre le test.

Cliquez sur **Actualiser** pour actualiser l'interface et les données du test BERT.

Le cas échéant, les données BERT sont toujours affichées en haut de la fenêtre de résultats. Les données BERT restent dans la fenêtre de résultats jusqu'à ce que vous cliquiez sur le bouton **Effacer les compteurs**.

ETAPE 7 Cliquez sur **Boucle arrêtée** pour supprimer la boucle.

Si la boucle est toujours activée lorsque vous fermez cette fenêtre, vous êtes invité(e) à supprimer les boucles existantes. Vous devrez supprimer les boucles à moins de devoir la laisser active en vue d'un test prolongé.

Diagnostic du réseau

Configuration Assistant dispose de plusieurs outils de diagnostic :

- **Ping**
- **Tracé, page 613**
- **Liaisons DHCP**
- **État système**
- **Journal de débogage du WAN (SR520-T1)**

Ping

Pour accéder au test Ping, sélectionnez **Dépanner** > **Diagnostic réseau** > **Ping** dans la barre de fonctions.

L'outil de diagnostic de ping est une méthode très courante permettant de vérifier l'accessibilité des appareils.

Vue d'ensemble

Il exploite une série d'échos ICMP pour déterminer les éléments suivants :

- Si un hôte distant est actif ou inactif
- Le délai de la boucle de communication avec l'hôte
- La perte des paquets

Le diagnostic de ping envoie d'abord un paquet de demande d'écho vers une adresse et attend la réponse. Le ping a réussi uniquement si :

- La demande d'écho atteint la cible et si
- La cible est capable de renvoyer un écho à la source dans le délai défini (délai d'expiration). La valeur par défaut de ce délai d'expiration est de deux secondes sur les routeurs Cisco.

Procédures

Pour effectuer un test de ping, suivez les étapes suivantes :

ETAPE 1 Sélectionnez une interface source (soit l'interface WAN par défaut, soit une interface/adresse IP interne).

Pour effectuer un test de la liaison VPN de site à site, sélectionnez une interface interne (par exemple : VLAN1).

ETAPE 2 Entrez une adresse IP ou un nom d'hôte valable.

ETAPE 3 Cliquez sur **Aller**.

Le résultat de la commande ping indique si le test a réussi (> 50 % des paquets transmis) ainsi que les délais moyen, minimum et maximum pour les allers-retours.

Tracé

Pour accéder au test Tracé, sélectionnez **Dépanner** > **Diagnostic réseau** > **Tracé** dans la barre de fonctions.

Vue d'ensemble

Le test Tracé repose sur la commande IOS "traceroute". Il permet de connaître le chemin emprunté par un paquet pour arriver à destination à partir d'une source en indiquant la séquence de bonds du paquet.

Le tracé indique quand :

- La cible répond
- La valeur TTL maximum (durée de vie) est dépassée
- Le nombre maximum de bonds (30) est atteint
- Le tracé est annulé

Les résultats de chaque tracé sont repris dans un tableau. Le nombre de bonds est indiqué ainsi que l'adresse IP et le nom d'hôte associé à ce bond, sans oublier la latence exprimée en millisecondes.

Procédures

Pour exécuter le test Tracé, procédez comme suit :

ETAPE 1 Entrez le nom d'hôte ou l'adresse IP de la cible.

ETAPE 2 Cliquez sur **Aller**.

Liaisons DHCP

Pour accéder au test DHCP, sélectionnez **Dépanner** > **Diagnostic réseau** > **Liaisons DHCP** dans la barre de fonctions.

Le test Liaisons DHCP affiche les adresses IP affectées de manière dynamique sur le système.

Les liaisons manuelles ne peuvent pas être supprimées. Vous ne pouvez supprimer que les liaisons automatiques.

Les résultats comprennent l'adresse IP, l'adresse matérielle (adresse MAC) et la date/heure de la fin de la location.

Procédures

ETAPE 1 Faites un choix parmi les options suivantes :

- Cliquez sur **Annuler la liaison sélectionnée** pour annuler la liaison DHCP sélectionnée.
- Cliquez sur **Annuler toutes les liaisons** pour annuler la liaison DHCP sélectionnée.
- Cliquez sur **Lire les liaisons** pour actualiser la liste.

ETAPE 2 Cliquez sur **OK** pour fermer la fenêtre.

État système

Pour afficher l'état système, sélectionnez **Dépanner** > **Diagnostic réseau** > **État système** dans la barre de fonctions. Ces informations sont également affichées dans la fenêtre État système du Tableau de bord (**Accueil** > **Tableau de bord**).

La fenêtre État système affiche les informations suivantes pour les périphériques gérés au niveau du site client :

- Nom de l'hôte
- Type de périphérique
- Adresse IP WAN
- Masque de sous-réseau
- Passerelle
- Adresses IP du serveur DNS
- Version de Cisco IOS
- Temps de fonctionnement (temps écoulé depuis le dernier redémarrage du système)
- Date et heure de la dernière mise à jour

Journal de débogage du WAN (SR520-T1)

La fenêtre Journal de débogage du WAN s'affiche lorsqu'un routeur sécurisé SR520-T1 se trouve sur le site client et que vous sélectionnez l'option **Dépannage** > **Diagnostic réseau** > **Journal de débogage du WAN** dans la barre de fonctions.

Vue d'ensemble

La fonction Journal de débogage du WAN vous permet d'obtenir des informations de débogage IOS lors du dépannage d'une connexion WAN T1 sur un routeur sécurisé SR520-T1. Vous pouvez aussi utiliser cet outil pour obtenir les données de configuration et de connexion WAN du SR520-T1. Les informations sont rassemblées dans un fichier texte et compressées dans un fichier .zip. La fonction de débogage IOS et les commandes "show" permettent de rassembler les informations.

ATTENTION L'activation de la collecte des données de débogage du WAN nécessite l'utilisation de nombreuses ressources, ce qui peut contribuer à la baisse des performances. N'activez le débogage que pour un court laps de temps et évitez les périodes de pointe dans la mesure du possible.

C'est la raison pour laquelle toutes les options de débogage du WAN sont désactivées lorsque vous fermez la fenêtre Journal de débogage du WAN ou Configuration Assistant. Si Configuration Assistant est fermé de manière inopinée, le débogage du WAN est désactivé au démarrage suivant du programme.

Procédures

Pour obtenir un journal relatif uniquement à la commande **show**, procédez comme suit :

ETAPE 1 Dans la fenêtre Journal de débogage du WAN, cliquez sur **Parcourir** et sélectionnez un répertoire pour le fichier journal.

ETAPE 2 Cliquez sur **Générer journal de dépannage**.

Vous ne devez pas forcément choisir les options de débogage du WAN ou activer le débogage.

Un fichier texte est créé dans le dossier indiqué, mais aucun fichier .zip. Le fichier journal contient le résultat des commandes "show" relatives au débogage du WAN. Une barre de progression s'affiche lors de la création du fichier journal.

ETAPE 3 Cliquez sur **OK** pour fermer la fenêtre une fois le fichier journal créé.

Pour activer le débogage et collecter les données de la commande "show" et les données de débogage du WLAN, suivez les étapes suivantes :

ETAPE 1 Dans la fenêtre Journal de débogage du WAN, cliquez sur **Parcourir** et sélectionnez un répertoire pour le fichier journal.

ETAPE 2 Cochez la case **T1** pour rassembler les données de débogage du WAN relatives à la connexion T1.

ETAPE 3 Cliquez sur **Appliquer débogage** pour activer le débogage.

ETAPE 4 Reproduisez le scénario sur votre réseau.

ETAPE 5 Cliquez sur **Générer journal de dépannage**.

Un fichier .zip est créé dans le dossier choisi. Ce journal comprend le résultat des commandes "show" relatives au débogage du WAN ainsi que toutes les données de débogage du WAN. Une barre de progression s'affiche lors de la création du fichier journal.

ETAPE 6 Cliquez sur **OK** pour fermer la fenêtre une fois le fichier journal créé.

ETAPE 7 Désactivez toutes les options de débogage du WAN et cliquez sur **OK** pour fermer la fenêtre.

Le débogage du WAN est automatiquement désactivé lorsque vous fermez la fenêtre.

Diagnostic de la téléphonie

Configuration Assistant dispose de plusieurs outils de diagnostic pour la fonction Voix :

- **Test du plan de numérotation**
- **Enregistrement des trunks SIP**
- **Journal de dépannage de la voix**
- **Journal de débogage pour le téléphone**
- **Capture PCM**
- **Postes analogiques SCCP**

Test du plan de numérotation

Pour accéder au test du plan de numérotation, sélectionnez **Dépanner** > **Diagnostic téléphonie** > **Plan de numérotation** dans la barre de fonctions.

Utilisez le test du plan de numérotation pour savoir comment le plan de numérotation achemine les appels entrants et sortants à partir ou vers le port ou le numéro de poste défini sur le système. Vous pouvez effectuer deux types de test du plan de numérotation :

- **Test du plan de numérotation sortant**

- **Test du plan de numérotation entrant**

REMARQUE les tests du plan de numérotation ne concernent pas les appels actifs.

Test du plan de numérotation sortant

Le test du plan de numérotation sortant précise la manière dont les appels sortants sont pris en charge par le plan de numérotation sortant.

Le test vérifie les autorisations pour le numéro de poste source (ligne utilisateur ou partagée), les conversations du numéro de destination et les chemins possibles (interfaces sortantes sur le routeur) pour l'appel.

En présence d'un numéro de poste utilisateur et d'un numéro de destination, la configuration vocale du routeur est passée au crible et les données d'appel suivantes s'affichent :

- Si l'appel est autorisé
- Le nombre de transferts vers la cible
- Toutes les interfaces potentielles ainsi que leurs préférences
- Les trunks SIP figurent parmi les interfaces sortantes affichées (le cas échéant).
- L'adresse IP du serveur SIP est affichée pour les trunks SIP.

Pour effectuer le test du plan de numérotation sortant, suivez les étapes suivantes :

ETAPE 1 Cliquez sur l'onglet Sortant dans la fenêtre Test du plan de numérotation.

ETAPE 2 Sélectionnez un **Numéro de poste utilisateur/partagé** dans la liste déroulante.

ETAPE 3 Entrez le numéro pour l'appel sortant.

Le numéro de destination peut être un numéro de poste interne ou un numéro extérieur (local, longue distance ou international). Il peut contenir jusqu'à 20 chiffres.

Pour les numéros extérieurs, le numéro indiqué doit comprendre tous les codes d'accès nécessaires, à savoir : le code d'accès au SDA pour les appels externes, le préfixe pour les appels longue distance, le code du pays (par exemple : 011) ou le code international.

ETAPE 4 Cliquez sur **Obtenir le détail du plan de numérotation**.

Test du plan de numérotation entrant

Pour les appels entrants, en présence d'un port FXO analogique ou d'un numéro DID, le test du plan de numérotation interne précise le routage de l'appel et les données de base sur le numéro de poste cible.

Le résultat indique si la cible a été trouvée et affiche le numéro de poste cible ainsi que le type de numéro de poste (par exemple : utilisateur, téléphone analogique, etc.).

Pour effectuer le test du plan de numérotation entrant, suivez les étapes suivantes :

ETAPE 1 Cliquez sur l'onglet Entrant dans la fenêtre Test du plan de numérotation.

ETAPE 2 Sélectionnez l'option **Port FXO analogique** ou entrez le **Numéro DID** pour l'appel entrant. Le numéro DID est généralement au format E.164 (par exemple : 16905552222).

ETAPE 3 Cliquez sur **Trouver cible**.

Enregistrement des trunks SIP

La fenêtre Enregistrement de trunk SIP affiche les données d'enregistrement SIP et fournit les outils de diagnostic pour le dépannage des problèmes d'inscription des trunks SIP. En cas d'échec de l'enregistrement du trunk SIP, le système vocal est désactivé et les utilisateurs ne peuvent pas passer et/ou recevoir des appels par le trunk. Pour accéder à cette fenêtre, sélectionnez l'option **Dépanner** > **Diagnostic téléphonie** >**Enregistrement des trunks SIP**.

Pour de plus amples informations, consultez les rubriques suivantes :

- **Informations sur l'enregistrement SIP**
- **Diagnostic d'enregistrement SIP (Appel du serveur d'enregistrement, Appeler le proxy, Réinitialiser le serveur d'enregistrement)**

Informations sur l'enregistrement SIP

Les données d'enregistrement SIP suivantes s'affichent :

- Informations sur les trunks SIP actifs ou non
- Nom du fournisseur de trunk SIP configuré dans la fenêtre Trunk SIP. Il peut s'agir de l'un des fournisseurs pris en charge par CCA ou des fournisseurs génériques.
- Le modèle d'enregistrement SIP utilisé pour le fournisseur de trunk SIP sélectionné. Le modèle d'enregistrement peut être l'une des options suivantes :
  - Ce fournisseur de service définit le numéro principal comme identifiant de l'appelant sortant.
  - Ce fournisseur de services enregistre tous les DID à l'aide du même nom d'utilisateur et du même mot de passe.
  - Ce fournisseur de services enregistre tous les DID à l'aide de noms d'utilisateur et de mots de passe différents. Les codes d'accès pour chaque DID doivent être introduits sous **Configurer** > **Téléphonie** > **Trunks** > **Trunk SIP**.
  - Ce fournisseur de services n'enregistre pas les DID (enregistrement accessoire).
- Adresse IP ou nom d'hôte du serveur d'enregistrement SIP en cas de configuration dans la fenêtre Trunk SIP.
- Adresse IP ou nom d'hôte du serveur proxy SIP sortant, en cas de configuration dans la fenêtre Trunk SIP.

Diagnostic d'enregistrement SIP (Appel du serveur d'enregistrement, Appeler le proxy, Réinitialiser le serveur d'enregistrement)

Ces fonctions de diagnostic de l'enregistrement SIP sont fournies.

Diagnostic DIP	Description
Appel du serveur d'enregistrement	Cliquez sur **Appel du serveur d'enregistrement** pour vérifier la liaison avec le serveur d'enregistrement SIP configuré à partir de la fenêtre Trunk SIP. Le résultat obtenu au test peut indiquer une erreur de résolution du nom de l'hôte DNS, des problèmes au niveau des paramètres réseau, des problèmes au niveau du pare-feu ou de l'ACL empêchant l'accès du trafic au serveur ou un hôte inaccessible.
Appeler le proxy	Cliquez sur **Appeler le proxy** pour vérifier la liaison avec le serveur proxy sortant SIP configuré à partir de la fenêtre Trunk SIP.

Diagnostic DIP	Description
Réinitialiser le serveur d'enregistrement	Lorsque vous cliquez sur **Réinitialiser le serveur d'enregistrement**, les actions suivantes sont entreprises : ▪ CCA reconfigure et réinitialise le serveur d'enregistrement SIP. Une fois que le serveur d'enregistrement est réinitialisé, les décomptes sont également réinitialisés pour l'agent SIP sous Cisco Unified CME. Cela permet le redémarrage de l'enregistrement SIP sans redémarrage de l'UC500. ▪ Si un nom de domaine est défini pour le serveur d'enregistrement SIP, CCA reconfigure le groupe source interne pour la voix ainsi que les listes de contrôle d'accès du pare-feu CBAC de l'UC500. Cela permet de résoudre les problèmes qui apparaissent lorsque l'adresse IP du serveur d'enregistrement ajouté à l'ACL lors de la configuration diffère de l'adresse IP du serveur d'enregistrement définie lors de l'enregistrement. Après avoir réinitialisé le serveur d'enregistrement et laissé le temps nécessaire à l'enregistrement auprès du fournisseur de services, vous pouvez vérifier l'état d'enregistrement SIP à l'aide de la fenêtre Etat du trunk SIP (**Superviser** > **Téléphonie** > **État du trunk SIP**). L'état repris dans le volet Registre SIP de la fenêtre doit être "oui" si le trunk SIP a été correctement enregistré. Le trunk SIP tente un enregistrement immédiat. Cependant, selon le fournisseur, plusieurs heures peuvent s'avérer nécessaires pour que les appels puissent être effectués une fois que le trunk SIP a été correctement enregistré.

Journal de dépannage de la voix

La fonction Journal de dépannage de la voix vous permet d'obtenir des données de débogage IOS propres à une situation ou un problème spécifique. Vous pouvez aussi utiliser cet outil pour obtenir les données de configuration de la voix ainsi que des informations sur l'état du système vocal pour le périphérique. Les informations sont rassemblées dans un fichier texte et compressées dans un fichier .zip.

Vue d'ensemble

La fonction de débogage IOS et les commandes "show" permettent de rassembler les informations. Vous pouvez définir au moins un des types de données de débogage pour la voix suivants :

- Plan de numérotation
- Ports vocaux
- Téléphones IP (SCCP)
- VoIP (SIP)
- VoIP (H323)

ATTENTION L'activation de la collecte des données de débogage de la voix nécessite l'utilisation de nombreuses ressources, ce qui peut contribuer à la baisse des performances. N'activez le débogage que pour un court laps de temps et évitez les périodes de pointe dans la mesure du possible.

C'est la raison pour laquelle toutes les options de débogage de la voix sont désactivées lorsque vous fermez la fenêtre Journal de débogage de la voix. Si Configuration Assistant est fermé de manière inopinée, le débogage est désactivé au démarrage suivant du programme.

Procédures

Pour obtenir un journal relatif uniquement à la commande show, procédez comme suit :

ETAPE 1 Dans la fenêtre Journal de débogage de la voix, cliquez sur **Parcourir** et sélectionnez un répertoire pour le fichier journal.

ETAPE 2 Cliquez sur **Générer journal de dépannage**.

Vous ne devez pas forcément choisir les options de débogage de la voix ou activer le débogage.

Un fichier texte est créé dans le dossier indiqué, mais aucun fichier .zip. Le fichier journal contient le résultat des commandes "show" relatives au débogage de la fonction Voix. Une barre de progression s'affiche lors de la création du fichier journal.

ETAPE 3 Cliquez sur **OK** pour fermer la fenêtre une fois le fichier journal créé.

Pour activer le débogage et collecter les données de la commande "show" et les données de débogage de la voix, suivez les étapes suivantes :

ETAPE 1 Dans la fenêtre Journal de débogage de la voix, cliquez sur **Parcourir** et sélectionnez un dossier pour le fichier journal.

ETAPE 2 Sélectionnez au moins un des types de données de débogage pour la voix.

ETAPE 3 Cliquez sur **Appliquer débogage** pour commencer la collecte des données de débogage.

ETAPE 4 Reproduisez le scénario sur votre réseau.

ETAPE 5 Cliquez sur **Générer journal de dépannage**.

Un fichier .zip est créé dans le dossier choisi. Ce journal comprend le résultat des commandes "show" relatives au débogage de la voix ainsi que toutes les données de débogage de la voix. Une barre de progression s'affiche lors de la création du fichier journal.

ETAPE 6 Cliquez sur **OK** pour fermer la fenêtre une fois le fichier journal créé.

ETAPE 7 Désactivez toutes les options de débogage de la voix et cliquez sur **OK** pour fermer la fenêtre.

Le débogage de la voix est automatiquement désactivé lorsque vous fermez la fenêtre.

Journal de débogage pour le téléphone

La fenêtre Journal de débogage pour le téléphone s'affiche lorsque vous cliquez sur **Dépanner** > **Diagnostic téléphonie** > **Journal de débogage pour le téléphone**.

Vue d'ensemble

La fonction Journal de débogage pour le téléphone vous permet de rassembler les données de débogage IOS lors de la résolution des problèmes associés à un téléphone ou un groupe de téléphones.

Vous pouvez aussi utiliser cet outil pour obtenir les données de configuration de la voix ainsi que des informations sur l'état du système vocal propres aux téléphones sélectionnés. Les informations sont rassemblées dans un fichier texte et compressées dans un fichier .zip.

ATTENTION La fonction de débogage IOS et les commandes "show" permettent de rassembler les informations. L'activation de la collecte des données de débogage du téléphone nécessite l'utilisation de nombreuses ressources, ce qui peut contribuer à la baisse des performances. N'activez le débogage que pour un court laps de temps et évitez les périodes de pointe dans la mesure du possible.

C'est la raison pour laquelle toutes les options de débogage du téléphone sont désactivées lorsque vous fermez la fenêtre Journal de débogage pour le téléphone. Si Configuration Assistant est fermé de manière inopinée, le débogage est désactivé au démarrage suivant du programme.

Procédures

Pour obtenir un journal relatif uniquement à la commande show, procédez comme suit :

ETAPE 1 Dans la fenêtre Journal de débogage pour le téléphone, cliquez sur **Parcourir** et sélectionnez un dossier pour le fichier journal.

ETAPE 2 Cliquez sur **Générer journal de dépannage**.

Vous ne devez pas forcément choisir les téléphones ni activer le débogage.

Un fichier texte est créé dans le dossier indiqué, mais aucun fichier .zip. Le fichier journal contient le résultat des commandes "show" relatives au débogage de la fonction Voix. Une barre de progression s'affiche lors de la création du fichier journal.

ETAPE 3 Cliquez sur **OK** pour fermer la fenêtre une fois le fichier journal créé.

Pour activer le débogage et collecter les données de la commande "show" et les données de débogage de la voix, suivez les étapes suivantes :

ETAPE 1 Dans la fenêtre Journal de débogage pour le téléphone, cochez l'option **Activer** correspondant à chaque téléphone que vous souhaitez intégrer au journal de débogage. Cette

ETAPE 2 Cliquez sur **Parcourir** et sélectionnez un répertoire.

ETAPE 3 Sélectionnez au moins un des types de données de débogage pour la voix.

ETAPE 4 Cliquez sur **Appliquer débogage** pour commencer la collecte des données de débogage.

ETAPE 5 Reproduisez le scénario sur votre réseau.

ETAPE 6 Cliquez sur **Générer journal de dépannage**.

Un fichier .zip est créé dans le dossier choisi. Ce journal comprend le résultat des commandes "show" relatives au débogage de la voix ainsi que toutes les données de débogage de la voix. Une barre de progression s'affiche lors de la création du fichier journal.

ETAPE 7 Lorsque le journal est créé, désactivez le débogage pour tous les téléphones et cliquez sur **OK** pour fermer la fenêtre.

Le débogage des téléphones est automatiquement désactivé lorsque vous fermez la fenêtre.

Capture PCM

La fenêtre Capture PCM s'affiche lorsque vous sélectionnez **Dépanner** > **Diagnostic de téléphonie** > **Capture PCM** dans la barre de fonctions.

Cette fenêtre permet le dépannage des problèmes de qualité vocale ou de son en obtenant une capture PCM (modulation du code d'impulsion) sur un port vocal donné, conformément aux instructions de l'assistance Cisco.

Procédez comme suit pour reproduire le scénario :

ETAPE 1 Veillez à ce qu'il y ait suffisamment de place sur la mémoire flash de l'UC500 pour créer la capture PCM. Pour ce faire, sélectionnez l'option **Accueil** > **Tableau de bord** et consultez la fenêtre Utilisation de la mémoire flash.

ETAPE 2 Essayez de reproduire la situation.

ETAPE 3 Une fois l'appel configuré, examinez le résultat dans la **Table d'appels actifs** et le **Récapitulatif de l'état de l'appel du port vocal** pour définir le port vocal à capturer conformément aux instructions de l'assistance Cisco.

La Table d'appels actifs affiche le résultat de la commande d'affichage du résumé des appels vocaux actifs (**show call active voice brief**) alors que le Récapitulatif de l'état de l'appel du port vocal affiche le résultat de la commande d'affichage de la somme des appels vocaux (**show voice call sum**).

Par exemple, si la Table d'appels actifs affiche les résultats suivants pour la configuration d'appel entre le poste 201 et le poste 209 et que le poste 201 présente des problèmes, le port vocal 50/0/10 devra être utilisé pour la capture PCM.

```
26 1118849120ms.1 +2710 pid:20006 Answer 201 active
dur 00:00:06 tx:131/31280 rx:130/31200
Tele 50/0/10 (26) [50/0/10,0] tx:2620/2620/0ms g711ulaw
noise:0 acom:0 i/0:0/0 dBm

27 1118849600ms.1 +2220 pid:20034 Originate 209 active
dur 00:00:06 tx:131/31280 rx:130/31200
Tele 50/0/18 (27) [50/0/18.0] tx:2600/2600/0ms g711ulaw
noise:0 acom:0 i/0:0/0 dBm
```

ETAPE 4 Dans le champ **Port de voix**, introduisez l'identifiant du port auquel vous souhaitez associer la capture (par exemple, 50/0/10).

ETAPE 5 Cliquez sur **Commencer**.

Lorsque vous cliquez sur **Commencer** :

- CCA publie les commandes pour définir la mémoire tampon pour la capture. Le programme définit le fichier cible pour la capture (fichier pcm.dat sur la mémoire flash de l'UC500).

  ```
  voice hpi capture buffer 5000000
  voice hpi capture destination flash:pcm.dat
  ```

- Le système commence par écrire les données PCM dans le fichier pcm.dat qui se trouve dans la mémoire flash de l'UC500.

ETAPE 6 Lorsque vous êtes prêt à interrompre la capture, cliquez sur **Terminer et Enregistrer**.

ETAPE 7 Enregistrez le fichier de capture pcm.dat.

Une fois le fichier enregistré, il est supprimé de la mémoire flash. La taille du fichier de capture varie en fonction des actions effectuées.

Postes analogiques SCCP

La fenêtre Postes analogiques SCCP s'affiche lorsque vous cliquez sur **Dépanner** > **Diagnostic de téléphonie** > **Postes analogiques SCCP**.

Les codes d'accès permettent aux utilisateurs des téléphones analogiques SCCP d'accéder à certaines fonctions en composant les codes (par exemple, **1 pour transférer tous les appels sur le téléphone).

Lorsque la configuration par défaut est active sur l'UC500, le processus d'initialisation de la voix supprime la commande associée au code d'accès stcapp.

Cette fenêtre vous permet d'activer ou désactiver les codes d'accès stcapp.

- Lorsque la fonction **Activer les codes d'accès stcapp** est désactivée, les codes d'accès sont configurés à l'aide des commandes `fac` qui se trouvent sous `telephony-service`. Il s'agit de la valeur recommandée.
- Lorsque la fonction **Activer les codes d'accès stcapp** est activée, la commande relative aux codes d'accès de la fonction `stcapp` est configurée en plus des commandes `fac` sous telephony-service. Cependant, l'activation de ce paramètre donne lieu à un conflit au niveau des codes de fonction puisque les codes 5, 6, 7 et 8 sont configurés différemment par ces commandes. Le résultat des commandes "show" suivant illustre le conflit.

```
UC_540# show stcapp feature codes

stcapp feature access-code
  malicious call ID (MCID) ***
  prefix **
  call forward all **1
  call forward cancel **2
  pickup local group **3
  pickup different group **4
  meetme-conference **5
```

```
  pickup direct **6
  forward-to-voicemail **7
  cancel call waiting **8

UC540# sh telephony-service fac

  telephony-service fac standard
  callfwd all **1
  callfwd cancel **2
  pickup local **3
  pickup group **4
  pickup direct **5
  park **6
  dnd **7
  redial **8
```

Diagnostic de connectivité CUE

La fenêtre Diagnostic CUE s'affiche lorsque vous sélectionnez **Dépanner** > **Diagnostic CUE** >**Diagnostic de connectivité CUE**.

Avant de lancer le diagnostic CUE :

- Veillez à ce que Telnet soit activé sur l'UC500. Lorsque vous utilisez CCA, Telnet est toujours actif.
- Le pare-feu actif sur votre PC peut être amené à bloquer la liaison entre le module CUE sur l'UC 500 et Configuration Assistant. Mieux vaut donc désactiver le pare-feu ou le configurer pour laisser l'accès au module CUE lors du diagnostic CUE.

La fenêtre Diagnostic de connectivité CUE contient les outils nécessaires au dépannage et au diagnostic des problèmes associés au module CUE de l'UC500. La messagerie vocale Cisco Unity Express (CUE) et les applications de l'UC500 telles que TimecardView résident sur le module CUE de l'UC500.

Dans cette fenêtre, vous pouvez effectuer les opérations suivantes :

- Vérifiez la connectivité entre le PC exécutant CCA et le module CUE pour afficher le résultat des commandes CUE dans la fenêtre de la console.
- Exécutez une ou plusieurs tâches de récupération pour que le module puisse résoudre les problèmes du CUE (par exemple, problème de redémarrage continu ou de mise à niveau du logiciel) :

  - Recharger CUE
  - Modifier le mode Bootloader
  - Démarrer le CUE à partir de l'image sur la mémoire flash
- Génère un fichier journal CUE pour dépanner les problèmes de niveau inférieur au niveau du module CUE

Pour en savoir plus sur les options de diagnostic de CUE, consultez les rubriques suivantes :

- **Vérifier l'état, page 630**
- **Générer les fichiers journaux, page 630**
- **Exécution des tâches de récupération, page 631**

Vérifier l'état

Lorsque vous cliquez sur **Vérifier l'état**, CCA tente d'ouvrir une connexion Telnet vers le module CUE pour vérifier l'état général du module. Selon l'état du module CUE, plusieurs résultats s'affichent :

- Si CUE démarre au clic du bouton, la progression du démarrage s'affiche dans la console.
- Si CUE est actif et s'exécute, la commande **show tech-support** est activée et le résultat s'affiche dans la console.
- Si CUE est en mode Bootloader, la commande **show config** s'affiche et le résultat ainsi que les paramètres de configuration s'affichent dans la console.
- Si la session CUE ne peut pas être établie, le message d'erreur adéquat s'affiche dans la console.

Générer les fichiers journaux

La fonction **Générer les fichiers journaux** n'est disponible que si CUE est en mode Exec ou Config.

Lorsque vous cliquez sur **Générer les fichiers journaux**, CCA rassemble les données de débogage à partir du module CUE et crée un dossier .zip contenant tous les fichiers journaux ainsi créés. Les journaux suivants sont récupérés :

- install.log
- syslog.log

- atrace_save.log
- debug_server.log
- sshd.log
- postgres.log
- klog.log
- messages.log
- shutdown_installer.log

Vous êtes invité à définir le répertoire par défaut pour le fichier .zip.

Exécution des tâches de récupération

Sélectionnez les tâches de récupération et cliquez sur **OK**.

ATTENTION Vous ne devez effectuer les tâches de récupération sur le module CUE que si l'Assistance Cisco vous le demande et afin de résoudre un problème donné.

Le redémarrage CUE peut prendre de 10 à 15 minutes.

Au cours de cette période, la messagerie, le standard automatique et les applications de téléphonie telles que Cisco WebEx PhoneConnect et TimeCardView ne sont pas disponibles.

Tâches de récupération	Description
Recharger CUE	L'interface de CUE est réinitialisée et la progression du démarrage s'affiche dans la console.
Placer CUE en mode Bootloader	Cette option vise à placer CUE en mode Bootloader. Cela peut s'avérer particulièrement utile pour mettre CUE dans un état connu de sorte que vous puissiez examiner la configuration de démarrage et tenter ensuite de démarrer CUE à partir de l'image figurant dans la mémoire flash de CUE.

Tâches de récupération	Description
Démarrer le CUE à partir de l'image sur la mémoire flash	Cette fonction n'est disponible que si CUE est en mode Bootloader. L'image de la mémoire flash de CUE est utilisée pour démarrer CUE et la progression du démarrage s'affiche dans la console.

Diagnostic de la sécurité

Cisco Configuration Assistant dispose des outils de diagnostic de sécurité suivants :

- **Journal de débogage du pare-feu/NAT**
- **Journal de débogage pour le VPN**

Journal de débogage du pare-feu/NAT

La fenêtre Journal de débogage du pare-feu/NAT s'affiche lorsque vous cliquez sur **Dépanner** > **Diagnostic de la sécurité** > **Journal de débogage du pare-feu/NAT**.

Vue d'ensemble

La fonction Journal de débogage du pare-feu/NAT vous permet d'obtenir des informations de débogage IOS lors du dépannage d'un problème de sécurité sur une plateforme UC 500 et les routeurs sécurisés SR500. Vous pouvez aussi utiliser cet outil pour obtenir les données de configuration et d'état pour le pare-feu et la traduction d'adresse réseau. Les informations sont rassemblées dans un fichier texte et compressées dans un fichier .zip.

La fonction de débogage IOS et les commandes "show" permettent de rassembler les informations. Vous pouvez définir au moins un des types de données de débogage de la sécurité suivants :

- NAT
- Pare-feu
- Filtrage d'URL

ATTENTION L'activation de la collecte des données de débogage de la sécurité nécessite l'utilisation de nombreuses ressources, ce qui peut contribuer à la baisse des performances. N'activez le débogage que pour un court laps de temps et évitez les périodes de pointe dans la mesure du possible.

C'est la raison pour laquelle toutes les options de débogage de la sécurité sont désactivées lorsque vous fermez la fenêtre Journal de débogage du pare-feu/NAT ou Configuration Assistant. Si Configuration Assistant est fermé de manière inopinée, le débogage est désactivé au démarrage suivant du programme.

Procédures

Pour obtenir un journal relatif uniquement à la commande **show**, procédez comme suit :

ETAPE 1 Dans la fenêtre Journal de débogage du pare-feu/NAT, cliquez sur **Parcourir** et sélectionnez un répertoire pour le fichier journal.

ETAPE 2 Cliquez sur **Générer journal de dépannage**.

Vous ne devez pas forcément choisir les options de débogage du pare-feu/NAT ou activer le débogage.

Un fichier texte est créé dans le dossier indiqué, mais aucun fichier .zip. Le fichier journal contient le résultat des commandes "show" relatives au débogage du pare-feu/WAN. Une barre de progression s'affiche lors de la création du fichier journal.

ETAPE 3 Cliquez sur **OK** pour fermer la fenêtre une fois le fichier journal créé.

Pour activer le débogage et collecter les données de la commande "show" et les données de débogage de la sécurité, suivez les étapes suivantes :

ETAPE 1 Dans la fenêtre Journal de débogage du pare-feu/NAT, cliquez sur **Parcourir** et sélectionnez un répertoire pour le fichier journal.

ETAPE 2 Sélectionnez le type de données de débogage de la sécurité à rassembler.

ETAPE 3 Cliquez sur **Appliquer débogage** pour commencer la collecte des données de débogage.

ETAPE 4 Reproduisez le scénario sur votre réseau.

ETAPE 5 Cliquez sur **Générer journal de dépannage**.

Un fichier .zip est créé dans le dossier choisi. Ce journal comprend le résultat des commandes "show" relatives au débogage du pare-feu et du NAT ainsi que toutes les données de débogage de la sécurité. Une barre de progression s'affiche lors de la création du fichier journal.

ETAPE 6 Cliquez sur **OK** pour fermer la fenêtre une fois le fichier journal créé.

ETAPE 7 Désactivez toutes les options de débogage du NAT et cliquez sur **OK** pour fermer la fenêtre.

Le débogage du pare-feu et du NAT est automatiquement désactivé lorsque vous fermez la fenêtre.

Journal de débogage pour le VPN

La fenêtre Journal de débogage pour le VPN s'affiche lorsque vous cliquez sur **Dépanner** > **Diagnostic de la sécurité** > **Journal de débogage pour le VPN**.

Vue d'ensemble

La fonction Journal de débogage pour le VPN vous permet d'obtenir des informations de débogage IOS lors du dépannage d'un problème de VPN sur une plateforme UC 500 et les routeurs sécurisés SR500. Vous pouvez aussi utiliser cet outil pour obtenir les données de configuration et d'état du VPN. Les informations sont rassemblées dans un fichier texte et compressées dans un fichier .zip.

La fonction de débogage IOS et les commandes "show" permettent de rassembler les informations. Vous pouvez définir au moins un des types de données de débogage suivants pour le VPN :

- EZVPN
- VPN site-à-site (IPsec)
- SSL VPN (sans client)
- SSL VPN (Full Tunnel)

  Si vous avez sélectionné l'option SSL VPN (Full Tunnel), sélectionnez une ACL et introduisez le nom d'utilisateur pour le VPN. Les ACL figurant dans la liste sont celles qui ont été configurées sur le routeur.

ATTENTION L'activation de la collecte des données de débogage VPN nécessite l'utilisation de nombreuses ressources, ce qui peut contribuer à la baisse des performances. N'activez le débogage que pour un court laps de temps et évitez les périodes de pointe dans la mesure du possible.

C'est la raison pour laquelle toutes les options de débogage VPN sont désactivées lorsque vous fermez la fenêtre Journal de débogage pour le VPN ou Configuration Assistant. Si Configuration Assistant est fermé de manière inopinée, le débogage du VPN est désactivé au démarrage suivant du programme.

Procédures

Pour obtenir un journal relatif uniquement à la commande **show**, procédez comme suit :

ETAPE 1 Dans la fenêtre Journal de débogage pour le VPN, cliquez sur **Parcourir** et sélectionnez un répertoire pour le fichier journal.

ETAPE 2 Cliquez sur **Générer journal de dépannage**. Vous ne devez pas forcément choisir les options de débogage du VPN ou activer le débogage.

Un fichier texte est créé dans le dossier indiqué, mais aucun fichier .zip. Le fichier journal contient le résultat des commandes "show" relatives au débogage du pare-feu/WAN. Une barre de progression s'affiche lors de la création du fichier journal.

ETAPE 3 Cliquez sur **OK** pour fermer la fenêtre une fois le fichier journal créé.

Pour activer le débogage et collecter les données de la commande "show" et les données de débogage du VPN, suivez les étapes suivantes :

ETAPE 1 Dans la fenêtre Journal de débogage pour le VPN, cliquez sur **Parcourir** et sélectionnez le répertoire pour le fichier journal. Sélectionnez le type de données de débogage du VPN à rassembler.

- EZVPN
- VPN site-à-site (IPsec)
- SSL VPN (sans client)

- SSL VPN (Full Tunnel). Sélectionnez une ACL (liste d'accès) dans le menu déroulant ou entrez le nom d'utilisateur pour le WebVPN.

ETAPE 2 Cliquez sur **Appliquer débogage** pour commencer la collecte des données de débogage.

ETAPE 3 Reproduisez le scénario sur votre réseau.

ETAPE 4 Cliquez sur **Générer journal de dépannage**.

Un fichier .zip est créé dans le dossier choisi. Ce journal comprend le résultat des commandes "show" relatives au débogage du VPN ainsi que toutes les données de débogage de la sécurité. Une barre de progression s'affiche lors de la création du fichier journal.

ETAPE 5 Cliquez sur **OK** pour fermer la fenêtre une fois le fichier journal créé.

ETAPE 6 Désactivez toutes les options de débogage du VPN et cliquez sur **OK** pour fermer la fenêtre. Le débogage du VPN est automatiquement désactivé lorsque vous fermez la fenêtre.

Débogages généraux

La fenêtre Débogages généraux s'affiche lorsque vous sélectionnez **Dépanner** > **Débogages généraux** dans la barre de fonctions.

Consultez les rubriques **Commandes IOS Exec, page 637** et **Commandes CUE Exec, page 638** pour plus d'informations sur l'affichage des données de diagnostic supplémentaires.

Vue d'ensemble

Dans la fenêtre Mise à jour du logiciel, vous pouvez effectuer les opérations suivantes : entrer les commandes de débogage Cisco IOS. Une fois que les données de débogage ont été rassemblées, vous pouvez afficher le résultat du débogage dans votre éditeur de texte par défaut et l'enregistrer dans un fichier ou effectuer une recherche.

Certaines commandes de débogage exploitant de nombreuses ressources sont exclues de cette fenêtre. Configuration Assistant affiche un message si vous introduisez l'une de ces commandes ou si la commande n'est pas valable.

Les résultats de la commande sont stockés dans une mémoire tampon de 5 Mo. Lorsque le volume de données dépasse 5 Mo, les données les plus anciennes sont écrasées par les plus récentes.

Pour collecter des données de débogage générales, procédez comme suit :

ETAPE 1 Entrez les commandes de débogage IOS à exécuter sur le périphérique (une par ligne).

ETAPE 2 Cliquez sur **Commencer** pour lancer la collecte des données.

ETAPE 3 Reproduisez le scénario/problème dans votre réseau.

ETAPE 4 Cliquez sur **Fin** pour interrompre la collecte des données de débogage.

ETAPE 5 Une fois les données collectées, vous pouvez effectuer les opérations suivantes :

- Cliquez sur **Rechercher** pour rechercher les résultats du débogage dans le volet Résultats de la fenêtre. La fenêtre de commande n'affiche que le résultat de chaque commande. Elle ne reprend pas les commandes au fur et à mesure de leur exécution.
- Cliquez sur **Enregistrer et afficher les résultats du débogage** pour afficher les résultats du débogage dans votre éditeur de texte par défaut et les enregistrer dans un fichier.
- Cliquez sur **Effacer la liste** pour réinitialiser la liste des commandes de débogage et introduire différentes commandes ou dans un ordre différent.

ETAPE 6 Cliquez sur **OK** pour fermer la fenêtre. Le débogage est automatiquement désactivé lorsque vous fermez la fenêtre. Si Configuration Assistant est fermé de manière inopinée, le débogage est désactivé au démarrage suivant du programme.

Commandes IOS Exec

Pour afficher les résultats des commandes IOS Exec, sélectionnez l'option **Dépanner**> **Commandes IOS Exec**.

Dans la fenêtre Commandes IOS Exec, vous pouvez afficher simultanément le résultat de quatre commandes IOS Exec au maximum. Les commandes peuvent être sélectionnées dans une liste ou introduites manuellement.

- Pour afficher le résultat d'une seule commande, sélectionnez une commande IOS Exec dans la liste. Vous pouvez aussi introduire manuellement la commande et cliquer sur **Run**.
- Pour afficher le résultat de plusieurs commandes, sélectionnez le nombre de volets à afficher (1, 2 ou 4). Entrez ou sélectionnez chaque commande et cliquez sur **Exécuter** pour afficher le résultat dans un nouveau volet. Si tous les panneaux sont utilisés, le résultat de la commande la plus récente écrase celui de la commande la plus ancienne.
- Cliquez sur **Réinitialiser les volets** pour réinitialiser tous les volets affichés.
- Cliquez sur **Actualiser** pour mettre à jour les données affichées dans chaque panneau.

Commandes CUE Exec

Pour afficher les résultats des commandes CUE Exec, sélectionnez l'option **Dépanner**> **Commandes CUE Exec**.

Dans la fenêtre Commandes CUE Exec, vous pouvez afficher simultanément le résultat de quatre commandes CUE Exec au maximum. Les commandes peuvent être sélectionnées dans une liste ou introduites manuellement.

- Pour afficher le résultat d'une seule commande, introduisez-la manuellement et cliquez sur **Exécuter**.
- Pour afficher le résultat de plusieurs commandes CUE Exec, sélectionnez le nombre de volets à afficher (1, 2 ou 4). Entrez chaque commande et cliquez sur **Exécuter** pour afficher le résultat dans un nouveau volet. Si tous les panneaux sont utilisés, le résultat de la commande la plus récente écrase celui de la commande la plus ancienne.
- Cliquez sur **Réinitialiser les volets** pour réinitialiser tous les volets affichés.
- Cliquez sur **Actualiser** pour mettre à jour les données affichées dans chaque panneau.

Création d'un journal de dépannage système

Effectuez les opérations suivantes pour rassembler les données de dépannage dans Configuration Assistant afin de permettre à l'assistance technique Cisco de résoudre les problèmes.

Vous pouvez sélectionner un périphérique UC500 ou SR500 si un site client a été configuré.

ETAPE 1 Dans Configuration Assistant, sélectionnez **Aide** > **Support technique** dans le menu en haut de la fenêtre principale.

ETAPE 2 Dans le volet Support technique, cliquez sur **Journal de dépannage**.

ETAPE 3 Cliquez sur **Parcourir** et sélectionnez un dossier de votre PC où stocker le fichier journal.

ETAPE 4 Dans le champ Nom de l'hôte, sélectionnez le périphérique UC500 ou SR500 dans la communauté.

ETAPE 5 Cliquez sur **Créer un journal**.

Configuration Assistant rassemble les fichiers journaux et de configuration nécessaires au dépannage.

Cela peut durer jusqu'à 5 minutes. Le fichier journal est créé dans le dossier défini à l'étape 3.

ETAPE 6 Annexez ce fichier journal au dossier à envoyer à l'assistance technique Cisco.

Le nom et le format du fichier journal sont les suivants : UC5*x*0_*adresse MAC_Date_Heure*_tac_logs.zip.

Liaisons et connectivité (commutateurs CE520)

Pour tester les liaisons ou la connectivité en présence d'un commutateur CE520, sélectionnez l'option Liaisons et connectivité dans la barre de fonctions.

Vue d'ensemble

La fenêtre Liaisons et connectivité présente les types de problème suivants dans votre réseau :

- Aucune connectivité entre le périphérique source et le périphérique cible.
- Aucun câble ou problème au niveau du câble relié au port.
- Erreur de vitesse du port pour une liaison donnée.
- Problèmes de liaison entre deux périphériques du réseau (par exemple : un hôte et un serveur).

REMARQUE Les tests de connectivité ne sont réalisables que sur les ports cuivrés Ethernet 10/100/1000.

Procédures

Pour tester une liaison, procédez comme suit.

ETAPE 1 Sélectionnez **Liaison (hors service)** dans la liste **Type de test**.

ETAPE 2 Sélectionnez un nom d'hôte dans la liste Nom de l'hôte.

ETAPE 3 Sélectionnez une interface dans la liste Interface ou cliquez sur l'icône à côté du champ Interface.Vous pouvez alors sélectionner l'interface pour le périphérique affiché.

ETAPE 4 Cliquez sur **Démarrer** pour commencer le test.

En présence d'erreurs sur la liaison, la description du message d'erreur et les conseils s'affichent dans la zone Résultats. En l'absence d'erreurs, un message indiquant l'absence d'erreurs s'affiche.

Pour résoudre un problème de liaison, cliquez sur le bouton **Réparer**. Vous pouvez réparer uniquement un problème d'incohérence de vitesse à l'aide de Configuration Assistant.

Pour tester la connectivité réseau entre deux périphériques, vous devez entrer l'adresse IP source de l'un des périphériques et l'adresse IP cible de l'autre périphérique. Les résultats montrent si la connectivité existe entre ces périphériques.

Pour tester la connectivité réseau entre deux périphériques, procédez comme suit :

ETAPE 1 Sélectionnez **Connectivité** dans la liste Type de test.

ETAPE 2 Dans le champ **Adresse IP source**, entrez l'adresse IP source de l'un des périphériques.

ETAPE 3 Dans le champ **Adresse IP de destination**, entrez l'adresse IP cible de l'autre périphérique.

Cliquez sur **Démarrer** pour commencer le test. La description du message et les conseils s'affichent dans la zone Résultats.

A

Que faire ensuite ?

Cisco met à votre disposition un grand nombre de ressources afin de vous aider vous et vos clients et profiter au maximum de Cisco Configuration Assistant et de Cisco Smart Business Communications System (SBCS).

Cisco Configuration Assistant	
Cisco Configuration Assistant Page produit	www.cisco.com/go/configassist
Documents techniques pour Cisco Configuration Assistant	www.cisco.com/en/US/products/ps7287/tsd_products_support_series_home.html
Consignes de configuration hors bande pour Cisco Configuration Assistant	http://www.cisco.com/en/US/partner/products/ps7287/prod_installation_guides_list.html
Cisco Small Business	
Centrale des partenaires Cisco pour les petites entreprises (connexion requise)	www.cisco.com/web/partners/sell/smb
Page d'accueil de Cisco Small Business	www.cisco.com/smb
Assistance Cisco Small Business	
Communauté Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Assistance et ressources pour Cisco Small Business	www.cisco.com/go/smallbizhelp
Assistance téléphonique	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Téléchargement de microprogrammes pour Cisco Small Business	www.cisco.com/go/smallbizfirmware Sélectionnez un lien pour télécharger le microprogramme des produits Cisco Small Business. La connexion n'est pas nécessaire. Les téléchargements pour tous les autres produits Cisco Small Business, dont les systèmes de stockage réseau, sont disponibles dans la zone de téléchargement sur Cisco.com à l'adresse www.cisco.com/go/software (inscription ou connexion nécessaire).

Cisco Smart Business Communications System et composants	
Paquets logiciels et fichiers de localisation pour Cisco UC500 (connexion requise sur Cisco.com)	www.cisco.com/go/uc500swpk
Cisco Smart Business Communications System	www.cisco.com/go/sbcsresources
Cisco Unified Communications 500 Series	www.cisco.com/go/uc500resources
Téléphones IP Cisco SPA 500	www.cisco.com/go/spa500phones
Téléphones IP Cisco SPA 300	www.cisco.com/go/300phones
Téléphone IP Cisco Unified 7900	www.cisco.com/en/US/products/hw/phones/ps379/
Point d'accès Cisco AP541N	www.cisco.com/go/ap500resources
Système de sécurité Cisco SA500	www.cisco.com/go/sa500resources
Commutateurs Cisco ESW500	www.cisco.com/go/esw500resources
Caméras vidéo Cisco PVC2300 (audio/PoE) et WVC2300 (audio/wireless-G)	www.cisco.com/go/smallbizcameras
Routeurs sécurisés Cisco SR500	www.cisco.com/go/sr500
Guide de référence pour Cisco Smart Business Commications System	www.cisco.com/en/US/partner/prod/collateral/voicesw/ps6882/ps10585/partner_reference_c07-557625-00.html
Avis sur les licences	
Avis sur les licences Open source	www.cisco.com/go/osln La licence open source pour CCA 3.0 se trouve sur la page de téléchargement du logiciel CCA sur le site Cisco.com.

Glossaire

A

AAA	Authentification, autorisation et comptabilisation. Prononcé "triple A".
ABR	Area border router. Routeur disposé à la frontière de plusieurs zones OSPF et permettant de les relier à la dorsale. Les ABR sont à la fois membres de la dorsale OSPF et des zones limitrophes. Ils disposent dès lors de tables de routage décrivant à la fois la topologie de la dorsale et la topologie de ces zones.
point d'accès	Périphérique faisant office de point central dans un réseau sans fil ou de point de liaison entre les périphériques sans fil et un réseau câblé. Voir aussi point d'accès autonome et LAP (point d'accès léger).
port d'accès	Port prenant en charge le trafic d'un réseau local virtuel (VLAN). En opposition au port trunk.
VLAN d'accès	VLAN utilisé par un commutateur pour le trafic de données. Voir aussi VLAN natif et VLAN vocal.
agrégation d'adresses	Fonction du protocole de routage permettant de découper les longues adresses réseau en agrégats d'adresses contigus (super-réseaux). Cette fonction supprime automatiquement les annonces de réseaux précis sur une interface définie.
annonce	Processus mis en place par le routeur et permettant de notifier les mises à jour de routage et de service de sorte que les autres routeurs puissent disposer d'un tableau reprenant les routes utilisables.
masque d'adresse	Combinaison d'octets utilisée pour décrire la portion d'une adresse se rapportant au réseau ou au sous-réseau et celle se rapportant à l'hôte. Voir aussi Adresse IP et Masque de sous-réseau.
vitesse d'administration	Vitesse d'une liaison définie par l'administrateur. Si l'administrateur indique auto comme valeur pour la vitesse, la vitesse réelle est fixée par négociation automatique.

A

AES	Advanced Encryption Standard. Chiffrement par blocs permettant de crypter et de décrypter les données à l'aide de clés de 128, 192 ou 256 bits.
AES CCMP	Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol. Protocole de chiffrement exploitant la norme AES. L'algorithme CCMP produit un code garantissant l'intégrité du message et permettant l'identification de l'origine des données composant le paquet sans fil et leur intégrité.
interface du gestionnaire de PA	Interface utilisée pour toutes les communications de couche 3 entre un contrôleur de WLAN et les points d'accès légers (LAP) après que ceux-ci ont rejoint le contrôleur.
ARP	Address Resolution Protocol (Protocole de résolution d'adresse) Protocole Internet utilisé pour associer une adresse IP à une adresse MAC.
secteur	Groupe de routeurs contigus partageant les mises à jour de l'état de la liaison OSPF. Identifié par un numéro appelé Identifiant du secteur.
ATM	Mode de transfert autonome. Norme internationale pour le relais de cellule permettant la conversion de divers types de services (voix, vidéo, données) en cellules d'une longueur déterminée (53 octets). Les cellules fixes permettent un traitement sur le matériel, ce qui permet de réduire les retards de transit. L'ATM est conçu pour profiter des supports de transmission à haute vitesse comme l'E3, SONET et T3.
Négociation automatique	Capacité des ports liés à détecter les caractéristiques de chacun et de sélectionner la meilleure méthode de communication.
point d'accès autonome	Point d'accès autonome ne nécessitant pas le contrôleur WLAN pour fonctionner. Voir aussi LAP (point d'accès léger).
AWP	Alternatively wired ports. Deux ports physiques fonctionnant comme un seul port logique. Généralement, un port utilise un connecteur SFP en fibre optique et l'autre un connecteur RJ-45 en cuivre.

B

BOOTP	Protocole Bootstrap. Protocole utilisé par un nœud réseau pour déterminer l'adresse IP de ses interfaces Ethernet, dans le but d'affecter l'amorçage réseau.

C

CAC	Contrôle des admissions d'appel. Processus permettant de réguler la qualité de la voix en limitant le nombre d'appels actifs simultanément sur une liaison particulière. CAC ne garantit pas le niveau de qualité audio de la liaison mais vous permet de réguler le volume de bande passante utilisée par les appels actifs sur la liaison.
CAS	Channel-associated signaling (signalement associé au canal). Transmission des données de signalement sur le canal réservé à la voix. Le signalement CAS est souvent associé à un signalement RBS étant donné que la bande passante de l'utilisateur est utilisée par le réseau à d'autres fins.
CCKM	Cisco Centralized Key Management (gestion centralisée de clés Cisco). Protocole prenant en charge les applications temporelles telles que la VoIP sans fil. CCKM exploite les techniques de réintroduction de clés afin de permettre aux clients de passer d'un point d'accès à l'autre sans transiter par le contrôleur.
CDP	Cisco Discovery Protocol. Protocole utilisé par un périphérique pour annoncer son existence à d'autres périphériques et pour obtenir des informations sur les autres périphériques du même LAN ou le périphérique distant du WAN.
CEF	Cisco Express Forwarding. Technologie de commutation de couche 3 avancée pour IP. Le CEF permet d'optimiser les performances et l'évolutivité des réseaux dotés de modèles de trafic important et dynamique tels que ceux associés à Internet, aux applications Web et aux sessions interactives.
CGMP	Cisco Group Management Protocol. Protocole permettant de limiter les inondations de paquets IP multicast en limitant la transmission de ces paquets à des clients qui les demandent. Les stations finales deviennent les clients lorsqu'elles envoient des messages d'adhésion afin de rejoindre un groupe CGMP.De même, un message d'abandon est envoyé lorsqu'elles quittent le groupe.
mode sans client	Offre un accès sécurisé aux ressources Web privées et un accès au contenu Web.
site client	Groupe de périphériques gérés grâce aux adresses IP de ses membres. Les commutateurs, les routeurs, les contrôleurs de points d'accès et les points d'accès autonomes peuvent être membres.

D

passerelle par défaut	Nœud dans un réseau servant de point de sortie vers un autre réseau et de point d'entrée à partir d'un réseau donné.
appel différé	L'extrémité source utilise la ligne et attend 20 ms afin de vérifier si l'extrémité cible est accessible. Si tel est le cas, l'extrémité source émet des impulsions. Si la cible n'est pas en ligne, la source attend que celle-ci le soit avant d'émettre les impulsions.
transfert basé sur la cible	Transfert d'un paquet par un groupe de ports en fonction de l'adresse cible du paquet. Voir aussi transfert basé sur la source.
DHCP	Dynamic Host Configuration Protocol. Mécanisme permettant l'affectation dynamique d'adresses IP de sorte que les adresses puissent être réutilisées lorsque les hôtes n'en ont plus besoin.
DID	Direct Inward Dial (Appel entrant direct). Service offert par les opérateurs téléphoniques permettant aux appelants d'appeler directement un numéro de poste sur un autocommutateur privé ou sur un système vocal sans recourir à un opérateur ou un standard automatique. Ce service exploite le trunk DID, lequel assure la transmission de 3 des 5 chiffres d'un numéro de téléphone à l'autocommutateur privé, au routeur ou à la passerelle.
identification Digest	Processus réservé aux trunks SIP et aux téléphones permettant de vérifier l'identité de l'utilisateur SIP lorsque celui-ci envoie une requête. (L'utilisateur SIP représente un périphérique ou une application à l'origine du message SIP.)
DMZ	Zone démilitarisée. Zone tampon entre l'Internet et les réseaux privés. Il peut s'agir d'un réseau public généralement utilisé pour les serveurs Web, FTP ou de messagerie et accessibles par des clients externes depuis l'Internet. En plaçant ces serveurs d'accès public sur un réseau distinct et isolé, vous pourrez renforcer la sécurité de votre réseau interne.
DNS	Domain Name Service (service de nom de domaine). Service Internet assurant la traduction des noms de domaine composés de lettres en adresses IP composées de chiffres.
nom de domaine	Nom familier d'un hôte sur Internet correspondant à son adresse IP.
adresse dynamique	Adresse MAC obtenue par un port. Elle est stockée dans le tableau d'adresses et effacée au chargement du commutateur. La première adresse MAC détectée lors de l'activation de la sécurité du port devient une adresse dynamique sécurisée. Voir aussi adresse statique.

routage dynamique	Routage ajusté automatiquement en fonction du trafic réseau ou des changements de topologie. Aussi appelé routage adaptatif.

E

EANA	Equal Access North American. Une des quatre principales sources de signalement CAS. Les autres options sont Ground Start, Loop Start et E&M.
EAP	Extensible Authentication Protocol. Méthode d'authentification où un point d'accès aide un périphérique client sans fil et un serveur RADIUS à réaliser une authentification et à obtenir une clé WEP dynamique.
EIGRP	Enhanced Interior Gateway Routing Protocol. Version Cisco de l'IGRP offrant des fonctionnalités de convergence supérieures ainsi qu'un fonctionnement plus efficace tout en apportant les avantages des protocoles link-state et distance-vector.
E&M	Une des quatre principales sources de signalement CAS. Les autres options sont Ground Start, Loop Start et EANA.
terminaison	Terminal ou passerelle SIP. Une terminaison peut appeler et être appelée. Elle génère et/ou met fin au flux d'informations.
EtherChannel	Groupe de ports Fast Ethernet ou Gigabit Ethernet agissant comme un port logique isolé pour les liaisons à bande passante importante entre les commutateurs ou entre les commutateurs et les serveurs. En cas d'échec d'un port au sein d'un EtherChannel, le trafic transitant par le port est transféré vers les autres ports au sein de l'EtherChannel.
Port de gestion Ethernet	Le port de gestion Ethernet est un port hôte compatible avec la couche 3 et pouvant être relié à un PC. Vous pouvez utiliser le port de gestion Ethernet à la place du port de la console du commutateur lors de l'administration du réseau. Utilisez ce port uniquement pour assurer la gestion du commutateur. Le port de gestion Ethernet prend uniquement en charge les fonctions Paramètres du port, Adresse IP sous Configuration Assistant.
EZVPN	Easy VPN. Système de gestion de VPN centralisée basée sur Cisco Unified Client Framework. Le Cisco Easy VPN se compose de deux éléments : un client distant Cisco Easy VPN et un serveur Cisco Easy VPN.

F

basculement	Transfert des responsabilités vers un commutateur en attente.
Fast Leave	Fonction de routage multicast accélérant la suppression d'un groupe multicast d'un routeur. Lorsqu'un membre quitte un groupe, Fast Leave recherche les autres membres du groupe (périphériques réceptionnant les paquets multicast en provenance d'un port donné du commutateur). S'il n'y a aucun autre membre sur le port, le commutateur supprime le port du groupe. S'il n'y a aucun autre port dans le groupe, le commutateur avertit les routeurs reliés au VLAN afin de supprimer le groupe.
pare-feu	Routeur ou serveur d'accès, ou plusieurs routeurs ou serveurs d'accès, désignés comme tampons entre les réseaux publics connectés et un réseau privé. Un routeur pare-feu utilise des listes de contrôle d'accès ainsi que d'autres méthodes pour assurer la sécurité du réseau privé.
FTP	File Transfer Protocol. Élément du stack du protocole TCP/IP utilisé pour le transfert des fichiers entre les hôtes.

G

GBIC	Gigabit Interface Converter. Émetteur-récepteur capable de convertir les courants électriques (basses et hautes tensions numériques) en signaux optiques et les signaux optiques en courants électriques numériques. Le GBIC est généralement utilisé dans les systèmes à fibre optique ou Ethernet comme interface pour la mise en réseau rapide. Le débit de transfert des données est de 1 gigaoctet par seconde (1 Go/s) au minimum.
fréquence d'interrogation graphique	Fréquence à laquelle Configuration Assistant interroge les membres d'un site client afin d'obtenir des informations sur le périphérique ou la liaison au sein du groupe. Ces informations sont utilisées pour mettre à jour les graphiques de connexion et de bande passante. Voir aussi fréquence d'interrogation de l'état, fréquence d'interrogation LED et fréquence d'interrogation du réseau.

GRE Generic Routing Encapsulation. Protocole de tunnellisation encapsulant plusieurs types de paquets de protocoles dans les tunnels IP et créant une connexion virtuelle point par point vers les périphériques à distance sur le réseau IP. Grâce à cette technologie, le protocole GRE permet d'intégrer le paquet d'origine entre un en-tête IP standard et un en-tête GRE avant la procédure IPsec. Ensuite, IPsec considère le paquet GRE comme un paquet IP ne devant pas être remarqué et procède au chiffrement et à l'identification conformément aux paramètres IKE. Étant donné que le protocole GRE peut réaliser un trafic multicast et broadcast, il est possible de configurer un protocole de routage pour les tunnels GRE virtuels. Le protocole de routage détecte les pertes de connexion et redirige les paquets vers le tunnel de sauvegarde GRE, assurant ainsi une redondance parfaite.

groundstart L'une des quatre formes de signalement CAS T1 standard. Il s'agit essentiellement d'un signal analogique exploitable sur les ports FXS, FXO et analogiques. Les autres formes standard sont EANA et E&M.

H

fréquence d'interrogation de l'état Fréquence à laquelle Configuration Assistant sonde les ports d'un site client pour obtenir des données relatives à l'utilisation des ressources du périphérique ainsi que sa température. Voir aussi fréquence d'interrogation graphique, fréquence d'interrogation LED et fréquence d'interrogation du réseau.

réseau domestique Réseau situé côté serveur dans un tunnel VPN. Par exemple, un utilisateur pourra, à partir de l'hôtel où il est descendu, relier son PC au réseau de l'hôtel pour télécharger un fichier placé sur un serveur de son entreprise. La liaison entre le réseau de l'hôtel et le réseau de l'entreprise est établie par Internet à l'aide d'un tunnel VPN. Dans cet exemple, le réseau de l'hôtel représente le réseau distant alors que le réseau de l'entreprise constitue le réseau domestique.

groupement de postes Groupe de lignes téléphoniques associées par l'opérateur téléphonique ou un autocommutateur privé. Lorsqu'un appel atteint un groupement de postes, il passe d'une ligne à l'autre jusqu'à ce qu'il trouve un poste qui n'est pas occupé, puis fait sonner ce téléphone (ou le poste s'il s'agit d'un autocommutateur privé.

HSRP Hot Standby Routing Protocol. Protocole assurant la haute disponibilité du réseau et les modifications transparentes de la topologie du réseau. Il crée un groupe de périphériques composé d'un périphérique principal desservant tous les paquets envoyés à une adresse de secours. Le périphérique principal est surveillé par les autres du groupe.En cas de problème, d'autres périphériques récupèrent la fonction de leader et celle de secours.

HWIC High-Speed WAN Interface Card. Carte LAN sans fil au format HWIC offrant un point d'accès intégré pour les périphériques Cisco disposant d'une fonction de routage.

I

ICMP Internet Control Message Protocol. Protocole Internet de couche réseau signalant les erreurs et fournissant des informations importantes pour le traitement des paquets IP.

IGMP Internet Group Management Protocol. Protocole utilisé entre les hôtes et les routeurs du LAN afin de déterminer les groupes multicast auxquels les hôtes appartiennent.

IGMP Snooping Étude par un commutateur de couche 2 de certaines informations de couche 3 dans un paquet IGMP envoyé d'un hôte à un routeur. Le commutateur peut ainsi déterminer s'il convient d'ajouter ou de supprimer les ports membres.

IGRP Interior Gateway Routing Protocol. Routage IGP prenant en charge les problèmes de routage dans les réseaux hétérogènes de grandes dimensions.

IKE Internet Key Exchange. Protocole de gestion de clé utilisé en association avec les normes IPsec et autres. L'IPsec peut être configuré sans IKE mais IKE renforce l'IPsec en y apportant des fonctions supplémentaires, une flexibilité et une facilité de configuration. IKE permet l'identification des postes IPsec, la négociation des clés IPsec et des associations de sécurité IPsec.

Immediate Leave Fonction de routage multicast accélérant la suppression d'un groupe multicast d'un routeur. Lorsqu'un membre signale qu'il veut quitter le groupe, Immediate Leave supprime directement le port membre du groupe.

démarrage immédiat La terminaison source capture la ligne en décrochant et, sans attendre de réponse, commence à émettre des impulsions.

interface interne	Première interface connectant le périphérique à votre réseau interne fiable protégé par un système de sécurité.
Adresse IP	Adresse à 32 bits affectée aux hôtes utilisant le protocole TCP/IP. Cinq classes d'appartenance existent (A, B, C, D ou E). Elle se présente sous la forme de quatre octets séparés par des points (format décimal binaire). Chaque adresse se compose de la référence du réseau, éventuellement de celle du sous-réseau et de celle de l'hôte. Les références du réseau et du sous-réseau sont utilisées pour le routage et la référence de l'hôte est utilisée pour prendre en charge un hôte distinct au sein du réseau ou du sous-réseau. Le masque de sous-réseau est utilisé pour extraire les informations sur le réseau et le sous-réseau à partir de l'adresse IP.
Téléphone IP	Téléphone permettant la communication vocale sur un réseau IP.
IPsec	Ensemble de normes ouvertes assurant la confidentialité, l'intégrité et l'authentification des données entre les postes participants. L'IPsec offre ces protections au niveau de la couche IP. IPsec utilise IKE pour gérer la négociation des protocoles et des algorithmes en fonction d'une règle locale et pour générer les clés de cryptage et d'authentification utilisées par IPSec. L'IPsec peut être utilisé pour protéger un ou plusieurs flux de données entre un couple d'hôtes, de passerelles de sécurité ou entre une passerelle et un hôte.
ISL	Inter-Switch Link. Protocole détenu par Cisco assurant la maintenance des informations du VLAN alors que le trafic transite entre les commutateurs et les routeurs.

K

systèmes d'appareils à clé	Système téléphonique de faible envergure conçu pour les communications dans les bureaux composés de 1 à 25 utilisateurs. Les systèmes d'appareils à clé peuvent être analogiques ou numériques. Dans un système à clé, chaque téléphone peut répondre à tout appel destiné au standard. En présence de plusieurs appels simultanés, chaque appel est visible et peut être directement sélectionné par une pression sur le bouton correspondant sur un téléphone IP.

L

LACP	Link Aggregate Control Protocol. Protocole prenant en charge la norme IEEE 802.3AD pour l'agrégation des interfaces physiques afin de former une seule interface logique.
fréquence d'interrogation LED	Fréquence à laquelle Configuration Assistant sonde les ports d'un site client et affiche les modifications sous la forme des couleurs LED des ports. Voir aussi fréquence d'interrogation graphique, fréquence d'interrogation de l'état et fréquence d'interrogation du réseau.
point d'accès léger	Point d'accès ne pouvant fonctionner indépendamment du contrôleur WLAN. Le contrôleur WLAN assure la gestion des configurations et du logiciel du PA. Aucune configuration individuelle de ces points d'accès n'est nécessaire. Ils prennent uniquement en charge la fonction MAC en temps réel. Le contrôleur WLAN s'occupe de la fonction MAC en différé. Cette structure est aussi appelée *split MAC*. Voir aussi point d'accès autonome.
link state protocol	Type de protocole de routage proposant une carte de l'inter-réseau et permettant d'afficher les autres chemins ou les voies parallèles autorisant l'équilibrage des charges. L'OSPF est un exemple de ce type de protocole. Voir aussi distance-vector protocol.
LEAP	Lightweight Extensible Authentication Protocol. Type d'identification 802.1X pour les LAN sans fil permettant une identification mutuelle rigoureuse entre le client et le serveur RADIUS grâce à un mot de passe commun. Autorise les clés de chiffrement dynamiques par utilisateur et par session.
link-state protocol	Type de protocole de routage proposant une carte de l'inter-réseau et permettant d'afficher les autres chemins ou les voies parallèles autorisant l'équilibrage des charges. L'OSPF est un exemple de ce type de protocole. Voir aussi distance-vector protocol.
SPAN local	Session SPAN rassemblant tous les ports sources et de destination sur le même commutateur. Voir aussi SPAN distant.
loopstart	L'un des quatre types de signalement CAS T1. Il s'agit essentiellement d'un signal analogique exploitable sur les ports FXS, FXO et analogiques. Les autres formes standard sont groundstart, EANA et E&M.

M

MAC	Media Access Control. La plus basse des deux sous-couches de la couche liaison de données définie par l'IEEE. La sous-couche MAC régit l'accès aux supports partagés, notamment l'utilisation d'un passage de jeton ou d'une collision.
Adresse MAC	Adresse de la couche liaison de données normalisée requise par chaque port ou périphérique se connectant à un LAN. Les autres périphériques du réseau utilisent ces adresses pour localiser des ports spécifiques du réseau ainsi que pour créer et mettre à jour les tables de routage et les structures des données. Les adresses MAC font 6 octets et sont soumises au contrôle de l'IEEE.
interface de gestion	Interface par défaut pour la gestion d'un périphérique. Media Access Control. La plus basse des deux sous-couches de la couche liaison de données définie par l'IEEE. La sous-couche MAC régit l'accès aux supports partagés, notamment l'utilisation d'un passage de jeton ou d'une collision.
routage multicast	Technique de routage permettant aux copies d'un paquet isolé d'être transférées à un sous-réseau défini. Voir aussi routage unicast.
Serveur MWI	Le serveur SIP MWI (serveur de témoin de présence de messagerie) est un serveur proxy relayant les messages MWI SIP.

N

NAT	Traduction d'adresse réseau. Mécanisme permettant de limiter le besoin d'adresses IP uniques. Le NAT permet à une entreprise disposant d'adresses IP multiples de se connecter à Internet en traduisant ces adresses en des adresses IP acheminables.
VLAN natif	VLAN acheminant les paquets non balisés à partir d'un port trunk IEEE 802.1Q. Voir aussi VLAN d'accès et VLAN vocal.
EAP réseau	Méthode d'authentification où un point d'accès aide un périphérique client sans fil et un serveur RADIUS à réaliser une authentification et à obtenir une clé WEP dynamique.

fréquence d'interrogation du réseau	Fréquence à laquelle Configuration Assistant interroge les membres d'un site client afin d'obtenir des informations sur l'état d'un groupe de périphériques et la présence de nouveaux membres. Voir aussi fréquence d'interrogation graphique, fréquence d'interrogation de l'état et fréquence d'interrogation LED.
port réseau	Port auquel le commutateur transfère tout le trafic VLAN présentant des adresses de destination inconnues. Ce processus permet d'éviter l'inondation de tous les ports du VLAN.
nom de notification	Nom d'un ensemble d'informations définissant les types d'événements système et l'adresse e-mail à laquelle ces notifications sont envoyées.
NTP	Network Time Protocol. Protocole responsable de l'obtention d'une heure exacte sur la base des horloges radio et atomiques disponibles sur l'Internet.

O

authentification ouverte	Méthode d'authentification permettant à n'importe quel périphérique de s'identifier et de communiquer avec le point d'accès.
authentification ouverte avec EAP	Méthode d'authentification où le point d'accès force tous les périphériques client à effectuer une authentification EAP avant de pouvoir rejoindre le réseau.
OSPF	Open Shortest Path First. Protocole link-state n'imposant aucune limite au nombre de bonds et propageant instantanément les modifications de routage. Il prend en charge les masques de sous-réseau de taille variable et permet un équilibrage des charges en fonction de la liaison. Il permet également de compartimenter les réseaux en secteurs afin de limiter le trafic généré par les mises à jour de l'état de la liaison.
interface externe	Première interface, généralement le port 0, connectant le périphérique à d'autres réseaux non fiables au-delà du système de sécurité (WAN ou Internet).

P

PAT	Traduction d'adresse de port. Conserve les adresses dans la réserve globale en permettant la traduction des ports sources des liaisons TCP ou des échanges UDP. Des adresses locales différentes sont ensuite mappées vers la même adresse globale. La traduction fait en sorte que chacune d'elles soit unique. Les adresses de la réserve globale sont toujours utilisées avant les adresses PAT.
groupe d'interception	Cette fonction permet aux administrateurs d'associer des groupes d'interception à des téléphones IP isolés. Les utilisateurs peuvent donc répondre (décrocher) à un appel sur un autre poste ou numéro de téléphone.
PBX	Autocommutateur privé. Standard numérique ou analogique situé chez l'abonné et permettant de relier un réseau privé à un réseau public.
PKI	infrastructure à clé publique. Système d'organismes de certification (OC) et d'organismes d'enregistrement (OE) offrant l'aide nécessaire quant à l'utilisation d'un chiffrement à clé asymétrique dans les communications, grâce à la gestion des certificats, des archives, des clés et des jetons. Représente aussi toute norme relative à l'échange de clés asymétriques. Ce type d'échange permet au destinataire d'un message de se fier à la signature intégrée au message et à l'expéditeur du message de le crypter à l'intention du destinataire. Voir Gestion des clés.
PPPoE	Point-to-Point Protocol over Ethernet. Protocole PPP encapsulé dans les trames Ethernet. Le protocole PPPoE permet aux hôtes d'un réseau Ethernet de se connecter aux hôtes distants par un modem à haut débit.
PoE	Alimentation électrique par câble Ethernet. Technologie alimentant les périphériques connectés à l'aide de câbles de données au lieu de câbles d'alimentation.
fréquence d'interrogation	Voir aussi fréquence d'interrogation graphique, fréquence d'interrogation LED et fréquence d'interrogation du réseau.
clé partagée	Méthode d'authentification proposée en IPsec. Les clés partagées permettent à un ou plusieurs clients d'utiliser des codes secrets individuels pour assurer l'identification de tunnels chiffrés sur une passerelle à l'aide du protocole IKE (Internet Key Exchange). Les clés partagées sont couramment utilisées dans les petits réseaux composés de 10 clients maximum. Elles permettent d'éviter le recours à un organisme de certification à des fins de sécurité.

niveau de privilège	Valeur régissant l'accès à Configuration Assistant autorisé à un utilisateur. Le niveau 15 octroie l'accès en lecture et en écriture ; les niveaux 1 à 14 n'octroient que l'accès en lecture seule.
PSTN	Réseau téléphonique public commuté. Terme générique désignant une variété de réseaux et de services téléphoniques dans le monde.

Q

QoS	Quality of Service. Capacité d'un réseau ou d'un périphérique à fournir un service préférentiel au trafic sélectionné. L'objectif principal du service QoS consiste à affecter une bande passante dédiée, une gigue et une latence contrôlées (demandées par le trafic interactif ou en temps réel) afin d'éviter les pertes.

R

RADIUS	Remote Authentication Dial-In User Service. Base de données permettant l'authentification des modems et des liaisons ISDN ainsi que le suivi des durées de connexion.
réseau distant	Réseau situé côté serveur dans un tunnel VPN. Par exemple, un utilisateur pourra, à partir de l'hôtel où il est descendu, relier son PC au réseau de l'hôtel pour télécharger un fichier placé sur un serveur de son entreprise. La liaison entre le réseau de l'hôtel et le réseau de l'entreprise est établie par Internet à l'aide d'un tunnel VPN. Dans cet exemple, le réseau de l'hôtel représente le réseau distant alors que le réseau de l'entreprise constitue le réseau domestique.
SPAN distant	Session SPAN où les ports sources sont distants du commutateur hébergeant le port de destination. Voir aussi SPAN local.
RIP	Routing Information Protocol. Routage IGP le plus répandu sur l'Internet. Utilise le décompte des bonds comme mesure.
port racine	Port du commutateur présentant le meilleur chemin vers le commutateur racine.
commutateur racine	Commutateur se trouvant au centre d'une topologie spanning-tree. Tous les flux de données sur le réseau se font à partir de ce commutateur.
interface routable	Port routé ou SVI.

protocole de routage	Ensemble de règles et de conventions permettant de rassembler des informations sur les réseaux disponibles, notamment la distance et le coût pour les atteindre ainsi que la détermination du chemin de routage d'un paquet.

S

adresse sécurisée	Adresse MAC transférée vers un seul port par VLAN. Les adresses sécurisées sont conservées même quand le périphérique se recharge. Voir aussi Adresse dynamique et Adresse statique.
port sécurisé	Port pour lequel une action définie par l'utilisateur a lieu dès l'apparition d'une attaque.
SDP	1. Session Description Protocol. Protocole permettant la définition des informations nécessaires pour établir un transport multimédia par IP. Le protocole SDP assure la transmission des informations telles que l'annonce d'une session, l'invitation à une session, les adresses de transport et les types de support. Par exemple, dans un appel SIP, les messages SDP indiquent en cas d'utilisation de NTE les événements à envoyer à l'aide de NTE ainsi que la valeur du type de données utiles de NTE. 2. Secure Device Provisioning. Déploie l'infrastructure PKI de clé publique entre deux terminaux (client Cisco IOS et serveur de certificat Cisco IOS).
SFP	Small form-factor pluggable. Module émetteur-récepteur optique remplaçable en clientèle. Les modules SFP permettent les liaisons ascendantes Gigabit vers les autres commutateurs.
SFTP	Protocole de transfert de fichiers SSH. Le protocole SFTP fait partie du protocole SSH et est toujours actif sur le routeur. L'utilisateur disposant du niveau adéquat peut copier des fichiers vers ou à partir du routeur à l'aide du protocole SFTP.
authentification partagée	Méthode d'authentification où le point d'accès envoie une chaîne de texte non cryptée à n'importe quel périphérique tentant d'entrer en communication avec lui. Si le texte est correctement crypté, le point d'accès autorisera l'authentification.
SIP	Session Initiation Protocol. Active les sessions de gestion d'appels, notamment les conférences audio entre deux parties. SIP fonctionne conjointement avec le protocole SDP (Session Description Protocol) pour le signalement des appels. Avec le SIP, le routeur est compatible avec toutes les passerelles et serveurs proxy VoIP.

SMTP	Simple Mail Transfer Protocol. Protocole Internet chargé des services de messagerie électronique.
SNMP	Simple Network Management Protocol. Protocole des réseaux TCP/IP permettant de superviser et de contrôler les périphériques et de gérer les configurations, les statistiques, la performance et la sécurité.
transfert basé sur la source	Transfert d'un paquet par un groupe de ports en fonction de l'adresse source du paquet. Voir aussi transfert basé sur la cible.
aiguillage de trafic	L'aiguillage de trafic permet aux clients VPN de communiquer localement sans cryptage. Les utilisateurs envoient uniquement par le tunnel les données destinées au réseau domestique. Le reste du trafic (messagerie instantanée, courrier électronique ou navigation sur Internet) est envoyé vers Internet à l'aide du réseau local du client VPN.
SPAN	Switched Port Analyzer. Fonction utilisée pour définir un groupe de ports (ou de VLAN) à surveiller. Une copie du trafic sur ces ports sources est envoyée vers un port cible donné. Généralement, l'utilisateur connecte un analyseur de réseau au port cible afin d'afficher le trafic sur les ports sources. Voir aussi VLAN d'accès et VLAN vocal.
Spanning Tree Protocol	Voir STP.
adresse statique sécurisée	Adresse sécurisée configurée manuellement stockée dans la table d'adresses et ajoutée à la configuration en cours. Voir aussi Adresse dynamique et Adresse statique.
SSH	Secure Shell. Application exécutée par-dessus une couche de transport fiable (TCP/IP par exemple) offrant des fonctions d'authentification et de cryptage puissantes.
SSID	Service set identifier. Code associé aux paquets d'un réseau sans fil afin d'identifier chaque paquet faisant partie de ce réseau. Tous les périphériques sans fil qui tentent de communiquer doivent disposer du même SSID.
chemin statique	Chemin configuré et introduit dans une table de routage. Les chemins statiques sont prioritaires sur les chemins sélectionnés par les protocoles de routage dynamiques.
STP	Spanning Tree Protocol. Technique standard de maintenance d'un réseau composé de plusieurs ponts ou commutateurs. Lorsque la topologie du réseau change, le STP empêche la création de boucles en reconfigurant les ponts et les commutateurs et en plaçant des ports dans un état de transmission ou de blocage. Chaque VLAN est traité comme un pont séparé et une application séparée du STP est appliquée à chacun d'eux.

masque de sous-réseau	Masque d'adresse à 32 bits utilisé dans l'IP afin de présenter les bits d'une adresse IP identifiant le numéro de réseau, le numéro de sous-réseau ou le numéro de nœud.
port de commutation	Interface de couche 2 uniquement associée à un port physique. Il peut s'agir d'un port d'accès ou d'un port trunk.
SVI	Interface virtuelle commutée. VLAN disposant d'une adresse IP utilisée par les périphériques de couche 3 afin d'accéder au VLAN. Le SVI peut être configuré de sorte à router les paquets d'un VLAN à un autre.

T

TCP	Transmission Control Protocol. Protocole de couche transport offrant une transmission de données en full duplex fiable. TCP fait partie de la pile de protocoles TCP/IP.
TCP/IP	Nom commun pour une suite de protocoles prenant en charge la structure des inter-réseaux mondiaux.
Telnet	Protocole d'émulation de terminal pour les réseaux TCP/IP comme Internet. Telnet est très utilisé pour contrôler les serveurs Web à distance.
TFTP	Trivial File Transfer Protocol. Version simplifiée du FTP permettant le transfert de fichiers d'un ordinateur à un autre sur un réseau sans recours à l'authentification du client (par exemple par nom d'utilisateur et mot de passe).
TKIP	Temporal Key Integrity Protocol. Chiffrement assurant la défense en cas d'attaque du WEP où l'intrus utilise un segment non crypté (vecteur d'initialisation) dans les paquets cryptés afin de calculer la clé WEP.
port trunk	Port prenant en charge le trafic de plusieurs VLAN. Voir aussi port d'accès.
tunnel	Canal virtuel passant par un support partagé (Internet par exemple) et utilisé pour l'échange de paquets de données encapsulés.

U

UDP	User Datagram Protocol (protocole de datagramme utilisateur). Protocole de couche transport sans connexion du stack de protocole TCP/IP. UDP est un protocole simple assurant l'échange de datagrammes sans accusé de réception ni garantie de livraison. Le traitement des erreurs et la retransmission sont assurés par les autres protocoles.

routage unicast Technique de routage acheminant un paquet à une destination précise et utilisant un protocole de routage déterminant le chemin vers cette destination. Voir aussi routage multicast.

V

interface virtuelle Interface remplaçant le serveur DHCP pour les clients sans fil et obtenant leur adresse IP à partir d'un serveur DHCP.Celle-ci fait office d'adresse de redirection pour la fenêtre de connexion au Web.

VLAN LAN virtuel LAN logique composé de groupes de travail rassemblés à des fins déterminées ou pour un projet spécifique, quel que soit l'emplacement réel de chaque membre.

VPN réseau privé virtuel. Dispose des mêmes fonctions de sécurité et de confidentialité au sein d'une infrastructure de réseau publique qu'un réseau privé. Les VPN permettent le passage du trafic IP en toute sécurité sur un réseau TCP/IP public en assurant le chiffrement de tout le trafic d'un réseau à l'autre. Le VPN utilise la tunnellisation pour chiffrer toutes les informations au niveau de l'IP.

VTP VLAN Trunking Protocol. Protocole de messagerie de couche 2 respectant la configuration du VLAN en assurant la gestion de l'ajout, la suppression et les noms des VLAN sur la totalité du réseau.

élagage VTP Blocage d'une transmission broadcast, multicast ou d'un trafic unicast inconnu trop important vers les VLAN sur les ports trunk figurant dans la liste réservée à l'élagage.

VLAN vocal VLAN utilisé par un commutateur pour le trafic de données vocales en provenance des téléphones IP. Voir aussi VLAN d'accès et VLAN vocal.

W

WEP Wired Equivalent Privacy. Chiffrement brouillant les échanges entre les points d'accès et les périphériques clients afin d'assurer la confidentialité des communications. Le point d'accès et le périphérique utilisent la même clé WEP pour crypter et décrypter les signaux radio.

wink start	La terminaison source prend la ligne en décrochant. Elle attend la confirmation de l'autre terminaison avant d'émettre les impulsions. Cela permet de contrôler l'intégrité et d'isoler les trunks problématiques en permettant au réseau de renvoyer une nouvelle tonalité à la partie appelante.
WINS	Windows Internet Naming Service. Système Windows déterminant l'adresse IP associée à un ordinateur spécifique du réseau.
WMM	Multimédia sans fil. Amélioration QOS des LAN sans fil. WMM prend en charge les périphériques répondant à la norme 802.11E QoS Basic Service Set (QBSS). WMM active les services différenciés pour la voix, la vidéo et les données afin de permettre la gestion du trafic vocal avant tout autre type de trafic sur le réseau.
WPA	Wi-Fi Protected Access. Fonction de sécurité polyvalente et normalisée améliorant le niveau de protection des données et le contrôle d'accès sur les systèmes LAN sans fil. Grâce à l'identification par clé WPA, les clients et les serveurs d'authentification permettent de s'identifier à l'aide de la méthode EAP. Le client et le serveur génèrent également une clé PMK. WPA utilise le protocole TKIP pour la protection des données et IEEE 802.1X pour la gestion des clés.
WPA2	Wi-Fi Protected Access 2. Amélioration de la protection sur la base de normes exploitant le protocole AES CCMP pour la protection des données. WPA2 offre un niveau de sécurité supérieur à WPA car le chiffrement AES est supérieur au chiffrement TKIP.
WPA-PSK	Wi-Fi Protected Access-Pre-shared key. Méthode d'authentification prenant en charge WPA sur un réseau local sans fil dépourvu de l'authentification IEEE 802.1X. Une clé partagée est configurée sur le client et le point d'accès.
WPA2-PSK	Wi-Fi Protected Access 2-Preshared key. Méthode d'authentification prenant en charge WPA2 sur un réseau local sans fil dépourvu de l'authentification IEEE 802.1X. Une clé partagée est configurée sur le client et le point d'accès.

A