



Guide de l'utilisateur de Cisco Unified Presence version 8.5

Première publication: 02 Juillet 2010

Dernière modification: 13 Décembre 2010

Americas Headquarters

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883

Référence texte: OL-14086-01

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, le logo Cisco, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband et Welcome to the Human Network sont des marques ; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card et One Million Acts of Green sont des marques de service ; Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, le logo Cisco Certified Internetwork Expert, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, le logo Cisco Systems, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, le logo IronPort, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx et le logo WebEx sont des marques déposées de Cisco ou de ses filiales aux États-Unis et dans certains autres pays.

Toutes les autres marques mentionnées dans ce document ou sur le site Web sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique nullement une relation de partenariat entre Cisco et toute autre entreprise. (1002R)



TABLE DES MATIÈRES

Utilisation de base de l'interface des options utilisateur de Cisco Unified Presence 1

Navigateurs pris en charge 1

Connexion aux options utilisateur de Cisco Unified Presence 1

Configuration des politiques de confidentialité 3

Définition de votre politique de confidentialité par défaut 3

Ajout d'utilisateurs internes aux listes d'exceptions autorisées et bloquées 5

Ajout d'utilisateurs externes aux listes d'exceptions autorisées et bloquées 6

Ajout de domaines externes aux listes d'exceptions autorisées et bloquées 7

Organisation de la liste de contacts 9

Ajout de contacts à la liste de contacts 9

Suppression de contacts de la liste de contacts 11

Affichage de la liste de contacts 12

Configuration du temporisateur d'actualisation de la liste de contacts 12

Configuration des paramètres des réunions 15

Configuration des notifications de réunion 15

Configuration des paramètres des messages 17

Authentification des utilisateurs pour afficher l'historique des messages 17

Configuration d'une alerte de message entrant 18

Envoi d'un message de diffusion 18

Création de messages de réponse personnels 18

Déconnexion de Cisco IP Phone Messenger 19

Dépannage de l'interface des options utilisateur de Cisco Unified Presence 21

Connexion impossible à l'interface des options utilisateur 21

Connexion établie mais options non disponibles 21

Déconnexion automatique de l'interface des options utilisateur 21

Options d'accessibilité 23

Accès aux icônes de la fenêtre 23

[Accès aux boutons de la fenêtre](#) 23



CHAPITRE 1

Utilisation de base de l'interface des options utilisateur de Cisco Unified Presence

- [Navigateurs pris en charge](#), page 1
- [Connexion aux options utilisateur de Cisco Unified Presence](#), page 1

Navigateurs pris en charge

L'interface **Options utilisateur** de Cisco Unified Presence prend en charge les navigateurs suivants :

- Microsoft Internet Explorer 7
- Microsoft Internet Explorer 8
- Firefox 3.x



Remarque

Actuellement, Cisco Unified Presence ne prend pas en charge Safari et Google Chrome.

Rubriques connexes

- [Connexion aux options utilisateur de Cisco Unified Presence](#), page 1

Connexion aux options utilisateur de Cisco Unified Presence

Avant de commencer

L'interface Options utilisateur de Cisco Unified Presence permet de personnaliser les paramètres, de créer des messages de réponse personnels, d'organiser les contacts et d'envoyer des messages de diffusion.

- Pour se connecter aux Options utilisateur de Cisco Unified Presence, l'administrateur doit affecter l'utilisateur au groupe de l'utilisateur final CCM standard.
- Demandez les informations suivantes à l'administrateur système :
 - une adresse URL pour les options utilisateur de Cisco Unified Presence ;

- votre nom d'utilisateur et votre mot de passe pour les options utilisateur de Cisco Unified Presence.
- Vérifiez que vous utilisez un navigateur pris en charge.

Procédure

- Étape 1** Ouvrez un navigateur Web compatible sur votre ordinateur.
- Étape 2** Entrez l'adresse URL des options utilisateur de Cisco Unified Presence. Elle doit ressembler à ceci :
`http://<serveur CUPS>/cupuser.`
- Étape 3** Entrez votre nom d'utilisateur pour les options utilisateur de Cisco Unified Presence.
- Étape 4** Entrez votre mot de passe pour les options utilisateur de Cisco Unified Presence fourni par l'administrateur système.
- Étape 5** Sélectionnez **Connex.**
Pour vous déconnecter de l'interface des options utilisateur, sélectionnez **Déconn.** dans le coin supérieur droit de la fenêtre Options utilisateur. Pour des raisons de sécurité, vous êtes automatiquement déconnecté des options utilisateur après trente minutes d'inactivité.
-

Rubriques connexes

- [Navigateurs pris en charge](#) , page 1



CHAPITRE 2

Configuration des politiques de confidentialité

- [Définition de votre politique de confidentialité par défaut, page 3](#)
- [Ajout d'utilisateurs internes aux listes d'exceptions autorisées et bloquées, page 5](#)
- [Ajout d'utilisateurs externes aux listes d'exceptions autorisées et bloquées, page 6](#)
- [Ajout de domaines externes aux listes d'exceptions autorisées et bloquées, page 7](#)

Définition de votre politique de confidentialité par défaut

Les politiques de confidentialité permettent de déterminer quels sont les utilisateurs autorisés à voir votre état de disponibilité et à vous envoyer des messages instantanés. Cette version de Cisco Unified Presence prend en charge la règle de liste de contacts qui stipule que toute personne figurant sur la liste (surveillée par vous) peut, par défaut, voir votre état de disponibilité, *sauf* si vous refusez explicitement d'accorder une telle autorisation à cette personne.

Ainsi, les politiques de confidentialité permettent d'autoriser et de bloquer des utilisateurs et des domaines. Les options suivantes vous permettent de configurer la politique de confidentialité soit en tant que paramètre par défaut au niveau de l'organisation, soit par l'envoi d'une requête spécifique à l'utilisateur.

- **Autoriser** : par défaut, les utilisateurs/domaines peuvent voir votre état de disponibilité et vous envoyer des messages instantanés, sauf si vous les ajoutez explicitement à votre liste bloquée. Vous pouvez définir la politique de confidentialité Autoriser uniquement pour les domaines et les utilisateurs internes. Cette option *n'est pas* disponible pour les domaines/utilisateurs (fédérés) externes.
- **Bloquer** : les utilisateurs/domaines que vous bloquez ne peuvent pas voir votre état de disponibilité ni vous envoyer des messages instantanés. Pour eux, vous présentez toujours l'état Non disponible. Vous pouvez définir la politique de confidentialité Bloquer pour les domaines et les utilisateurs (fédérés) internes et externes.
- **Me demander** : la politique de confidentialité Me demander invite les utilisateurs (par l'intermédiaire d'une requête) à bloquer ou à autoriser explicitement l'échange des états de disponibilité et des messages instantanés provenant de domaines ou d'utilisateurs spécifiques. L'application client invite l'utilisateur à autoriser ou à rejeter l'abonnement. Vous pouvez définir la politique de confidentialité Me demander uniquement pour les domaines et utilisateurs (fédérés) externes, et seulement si le domaine ou contact externe *ne figure pas* dans la liste autorisée ou la liste bloquée de l'utilisateur.

Procédure

Étape 1 Sélectionnez **Options utilisateur > Politiques de confidentialité**.

Étape 2 Sélectionnez l'une des options suivantes :

Pour...	Procédez comme suit
<p><i>Autoriser tous les utilisateurs internes</i> à voir votre disponibilité et à vous envoyer des messages instantanés (à l'exclusion des utilisateurs/domaines internes que vous ajoutez explicitement à votre liste d'exceptions bloquées).</p> <p>Remarque Consultez l'exception à ce paramètre de politique dans la section Conseils relatifs au dépannage de cette rubrique. Cette politique ne permet pas aux utilisateurs externes de voir votre disponibilité.</p>	<ol style="list-style-type: none"> 1 Sélectionnez Autoriser dans le menu déroulant Utilisateurs internes (de votre société/organisation). 2 (Facultatif) Ajoutez des utilisateurs internes à vos listes d'exceptions bloquées selon les procédures décrites dans ce module. Reportez-vous à la rubrique Que faire ensuite.
<p><i>Empêcher tous les utilisateurs internes</i> de voir votre disponibilité et de vous envoyer des messages instantanés (à l'exception de ceux que vous ajoutez à votre liste d'exceptions autorisées).</p> <p>Remarque Cette politique n'empêche pas les utilisateurs externes de voir votre disponibilité.</p>	<ol style="list-style-type: none"> 1 Sélectionnez Bloquer dans le menu déroulant Utilisateurs internes (de votre société/organisation). 2 (Facultatif) Ajoutez des utilisateurs internes à votre liste d'exceptions autorisées selon les procédures décrites dans ce module. Reportez-vous à la rubrique Que faire ensuite.
<p><i>Empêcher tous les utilisateurs externes</i> de voir votre disponibilité et de vous envoyer des messages instantanés (à l'exception de ceux que vous ajoutez explicitement à votre liste d'exceptions autorisées).</p> <p>Remarque Cette politique n'empêche pas les utilisateurs internes de voir votre disponibilité.</p>	<ol style="list-style-type: none"> 1 Sélectionnez Bloquer dans le menu déroulant Utilisateurs externes (tous les autres). 2 (Facultatif) Ajoutez des utilisateurs externes à votre liste d'exceptions autorisées selon les procédures décrites dans ce module. Reportez-vous à la rubrique Que faire ensuite.
<p><i>Inviter tous les utilisateurs</i> (à l'aide d'une requête Me demander) à définir leur propre politique Autoriser/Bloquer pour les utilisateurs externes (à l'exception de ceux que vous ajoutez à votre liste d'exceptions autorisées/bloquées).</p> <p>Remarque Cette politique n'empêche pas les utilisateurs internes de voir votre disponibilité.</p>	<ol style="list-style-type: none"> 1 Sélectionnez Me demander dans le menu déroulant Utilisateurs externes (tous les autres). 2 (Facultatif) Ajoutez des utilisateurs externes à votre liste d'exceptions autorisées/bloquées selon les procédures décrites dans ce module. Reportez-vous à la rubrique Que faire ensuite.

Étape 3 Sélectionnez **Enregistrer les valeurs par défaut**.

Conseils pour le dépannage

Le serveur Cisco Unified Presence autorise automatiquement un utilisateur figurant sur la liste de contacts d'un autre utilisateur à voir leur état de disponibilité. Notez cette exception à la politique *Autoriser tous les*

utilisateurs internes : si vous *désactivez* l'autorisation automatique sur le serveur Cisco Unified Presence et si les paramètres par défaut du domaine global et du domaine local sont tous les deux définis sur Autoriser, l'utilisateur est invité à approuver ou à rejeter la requête d'abonnement. Il s'agit du scénario Me demander pour le domaine local. Pour plus d'informations sur le paramètre d'autorisation automatique de Cisco Unified Presence, reportez-vous au *Guide de déploiement de Cisco Unified Presence*(sur Cisco.com).

Que faire ensuite

- Si vous souhaitez remplacer la politique de confidentialité Autoriser/Bloquer par défaut définie pour les utilisateurs internes/externes au niveau de l'organisation, reportez-vous aux rubriques suivantes qui décrivent la configuration des listes d'exceptions pour les utilisateurs.

Ajout d'utilisateurs internes aux listes d'exceptions autorisées et bloquées

Cette procédure permet de gérer les exceptions à la politique de confidentialité générale sous la forme d'une liste autorisée et d'une liste bloquée. Selon la politique de confidentialité par défaut définie au niveau de l'organisation, vous pouvez modifier soit la liste autorisée, soit la liste bloquée. Ainsi, vous pouvez remplacer le comportement de la politique par défaut qui consiste à ajouter des personnes spécifiques de votre organisation sur la liste autorisée ou la liste bloquée.

- La définition de la politique d'autorisation pour des utilisateurs spécifiques permet à ces derniers de voir votre état de disponibilité et de vous envoyer des messages instantanés, même si la politique générale les bloque.
- La définition de la politique de blocage pour des utilisateurs spécifiques empêche ces derniers de voir le statut et d'échanger des messages instantanés lorsqu'ils utilisent des clients Cisco (Cisco Unified Personal Communicator Version 7 et Cisco Unified Personal Communicator Version 8), même si la politique générale les y autorise. Les utilisateurs de la liste de contacts sont toujours autorisés, sauf s'ils sont explicitement bloqués dans la liste des exceptions. Notez que certains clients XMPP tiers envoient et reçoivent malgré tout des messages instantanés, quelle que soit la politique que vous ayez définie.

Avant de commencer

Définissez votre politique de confidentialité par défaut.

Procédure

Étape 1 Sélectionnez **Options utilisateur > Politiques de confidentialité**.

Étape 2 Dans la fenêtre Politique de confidentialité, dans le cadre Paramètres utilisateur, sélectionnez **Ajouter un utilisateur**.

Étape 3 Effectuez l'une des opérations suivantes :

- Sélectionnez **Autoriser** pour permettre à l'utilisateur de voir votre disponibilité.
- Sélectionnez **Bloquer** pour empêcher l'utilisateur de voir votre disponibilité.

- Étape 4** Entrez un ID utilisateur valide pour l'utilisateur interne. L'ID utilisateur doit exister sur votre réseau interne au format `<IDutilisateur@domaine>`.
- Étape 5** Sélectionnez **Domaine local**.
- Étape 6** Sélectionnez **Ajouter** pour ajouter l'utilisateur interne au domaine local.
-

Conseils pour le dépannage

- Les utilisateurs fédérés peuvent ajouter un utilisateur local à l'aide d'un ID d'e-mail ou d'un JID standard. Le choix varie selon que l'administrateur a activé ou désactivé l'ID d'e-mail pour le domaine.
- Une fois que vous avez **ajouté** un utilisateur à la liste autorisée/bloquée, les détails s'affichent dans le tableau de cette fenêtre. Pour supprimer un utilisateur dans la liste autorisée/bloquée, cochez la case correspondante et sélectionnez **Supprimer la sélection**.

Ajout d'utilisateurs externes aux listes d'exceptions autorisées et bloquées

Cette procédure permet de gérer les exceptions à la politique de confidentialité générale sous la forme d'une liste autorisée et d'une liste bloquée. Selon la politique de confidentialité par défaut définie au niveau de l'organisation, vous pouvez modifier soit la liste autorisée, soit la liste bloquée. Ainsi, vous pouvez remplacer le comportement de la politique par défaut qui consiste à ajouter des personnes spécifiques extérieures à votre organisation sur la liste autorisée ou la liste bloquée.

- La définition de la politique d'autorisation pour des utilisateurs spécifiques permet à ces derniers de voir votre état de disponibilité et de vous envoyer des messages instantanés, même si la politique générale les bloque.
- La définition de la politique de blocage pour des utilisateurs spécifiques empêche ces derniers de voir votre état de disponibilité et de vous envoyer des messages instantanés, même si la politique générale les y autorise (par l'intermédiaire d'une réponse positive à une requête Me demander).

Avant de commencer

Définissez votre politique de confidentialité par défaut.

Procédure

- Étape 1** Sélectionnez **Options utilisateur > Politiques de confidentialité**.
- Étape 2** Dans la fenêtre Politique de confidentialité, dans le cadre Paramètres utilisateur, sélectionnez **Ajouter un utilisateur**.
- Étape 3** Effectuez l'une des opérations suivantes :
- Sélectionnez **Autoriser** pour permettre à l'utilisateur de voir votre disponibilité.
 - Sélectionnez **Bloquer** pour empêcher l'utilisateur de voir votre disponibilité.

Étape 4 Entrez un ID utilisateur valide pour l'utilisateur interne. L'ID utilisateur doit exister sur votre réseau interne au format <IDutilisateur@domaine>.

Étape 5 Sélectionnez l'un des domaines dont l'utilisateur fait partie :

- **Domaine fédéré.**
- **Domaine personnalisé** : domaine externe qui ne figure pas sur la liste des domaines fédérés.

Étape 6 Effectuez l'une des opérations suivantes :

Si vous avez sélectionné...	Procédez comme suit :
Domaine fédéré	Dans la liste déroulante, sélectionnez le domaine avec lequel vous procédez à une fédération.
Domaine personnalisé	Indiquez le domaine pour l'utilisateur. Remarque Par exemple, « masociété.com ».

Étape 7 Cliquez sur **Ajouter**.

Conseils pour le dépannage

Une fois que vous avez **ajouté** un utilisateur à la liste autorisée/bloquée, les détails s'affichent dans le tableau de cette fenêtre. Pour supprimer un utilisateur dans la liste autorisée/bloquée, cochez la case correspondante et sélectionnez **Supprimer la sélection**.

Ajout de domaines externes aux listes d'exceptions autorisées et bloquées

Avant de commencer

Vous pouvez autoriser ou bloquer l'ensemble d'un domaine externe. Si vous bloquez un domaine externe, toute requête de ses utilisateurs visant à consulter votre disponibilité est refusée, pour autant que vous n'ayez pas ajouté ces utilisateurs externes à votre liste autorisée.

Procédure

Étape 1 Sélectionnez **Options utilisateur > Politiques de confidentialité**.

Étape 2 Dans la fenêtre Politique de confidentialité, dans le cadre Paramètres utilisateur, sélectionnez **Ajouter un domaine**.

Étape 3 Effectuez l'une des opérations suivantes :

- Sélectionnez **Autoriser** pour permettre à l'utilisateur de voir votre disponibilité.
- Sélectionnez **Bloquer** pour empêcher l'utilisateur de voir votre disponibilité.

Étape 4 Sélectionnez l'un de ces domaines à autoriser ou à bloquer :

- **Domaine fédéré**
- **Domaine personnalisé** : domaine externe qui ne figure pas sur la liste des domaines fédérés.

Étape 5 Effectuez l'une des opérations suivantes :

Si vous avez sélectionné...	Procédez comme suit :
Domaine fédéré	Dans la liste déroulante, sélectionnez le domaine avec lequel vous procédez à une fédération.
Domaine personnalisé	Indiquez le domaine pour l'utilisateur. Remarque Par exemple, « masociété.com ».

Étape 6 Cliquez sur **Ajouter**.

Conseils pour le dépannage

Une fois que vous avez **ajouté** un domaine à la liste autorisée/bloquée, les détails s'affichent dans le tableau de cette fenêtre. Pour supprimer un domaine dans la liste autorisée/bloquée, cochez la case correspondante et sélectionnez **Supprimer la sélection**.



CHAPITRE 3

Organisation de la liste de contacts

- [Ajout de contacts à la liste de contacts, page 9](#)
- [Suppression de contacts de la liste de contacts, page 11](#)
- [Affichage de la liste de contacts, page 12](#)
- [Configuration du temporisateur d'actualisation de la liste de contacts, page 12](#)

Ajout de contacts à la liste de contacts

Avant de commencer

- L'administrateur système définit le nombre de contacts que peut contenir la liste, avec un maximum de 100. Adressez-vous à lui pour connaître la valeur définie pour votre téléphone.
- Pour ajouter un contact externe, vous pouvez soit sélectionner un domaine externe, soit configurer un domaine personnalisé pour les utilisateurs qui sont en dehors de votre organisation.
- Les utilisateurs internes et externes de la liste de contacts sont des exceptions aux politiques internes et externes. Les utilisateurs de la liste de contacts sont toujours autorisés, sauf s'ils sont explicitement bloqués dans la liste des exceptions.
- Dans l'application de messagerie instantanée, vous pouvez ajouter des contacts dont vous ne voyez pas l'état de disponibilité. Par exemple, vous pouvez ajouter des personnes que vous souhaitez simplement pouvoir appeler depuis la liste de contacts de l'application. Ces types de contacts ne sont pas visibles dans la liste de contacts de l'interface **Options utilisateur**.
- Si vous apportez des modifications à la liste de contacts (ajout, suppression ou modification), ces changements sont automatiquement pris en compte au niveau des clients Cisco (pour tous les utilisateurs connectés).

Procédure

Étape 1 Sélectionnez **Options utilisateur > Contacts**.

Étape 2 Sélectionnez **Ajouter nouveau**.

Étape 3 Sélectionnez l'une des options suivantes :

Si le contact que vous souhaitez ajouter est...	Procédez comme suit :
Interne : utilisateur qui appartient à votre domaine local (en général, la société ou l'organisation).	<ol style="list-style-type: none"> 1 Dans le champ Contact, indiquez l'ID utilisateur du contact fédéré que vous souhaitez ajouter. 2 Choisissez Sélectionnez dans la liste de domaine. 3 Dans le menu Domaine, sélectionnez un domaine interne (local). 4 Vous pouvez également entrer un nom alternatif pour l'utilisateur si vous souhaitez afficher un surnom sur son ordinateur. <p>Remarque Vous ne pouvez pas ajouter des utilisateurs ou des domaines qui sont déjà bloqués par l'administrateur. La politique de confidentialité de l'organisation doit être définie de façon à autoriser le domaine interne ou des utilisateurs spécifiques de ce domaine à voir votre état de disponibilité et à vous envoyer des messages instantanés.</p>

Si le contact que vous souhaitez ajouter est...	Procédez comme suit :
Externe : utilisateur qui ne fait pas partie de votre domaine local (en général, la société ou l'organisation)	<p>Procédez comme suit :</p> <ol style="list-style-type: none"> 1 Dans le champ Contact, indiquez l'ID utilisateur du contact fédéré que vous souhaitez ajouter. 2 Sélectionnez Effectuer une sélection dans la liste de domaines. <ul style="list-style-type: none"> • Dans le menu Domaine, sélectionnez un domaine externe. 3 Sélectionnez Saisir un domaine personnalisé. <ul style="list-style-type: none"> • Indiquez le domaine personnalisé pour les contacts qui ne font pas partie de votre organisation. <p>Remarque Vous ne pouvez pas ajouter des utilisateurs ou des domaines qui sont déjà bloqués par l'administrateur. La politique de confidentialité de l'organisation doit être définie de façon à vous inviter (dans une fenêtre contextuelle) à autoriser le domaine externe ou des utilisateurs spécifiques de ce domaine à voir votre état de disponibilité et à vous envoyer des messages instantanés.</p>

Étape 4 (facultatif) Indiquez un nom alternatif (surnom) pour le contact.

Étape 5 Sélectionnez **Enregistrer**.

Conseils pour le dépannage

Vous ne pouvez avoir qu'un seul nom alternatif (surnom) par contact. Si vous entrez également un nom alternatif pour un contact, celui-ci s'affiche sur les clients Cisco, mais pas nécessairement sur les clients XMPP tiers. Si vous mettez à jour le nom d'un contact, cette modification se répercute dans la liste de contacts de Cisco Unified Personal Communicator, ainsi que dans tous vos groupes de contacts.

Suppression de contacts de la liste de contacts

Procédure

Étape 1 Sélectionnez **Options utilisateur > Contacts**.

Étape 2 Sélectionnez **Trouver**.

Étape 3 Effectuez l'une des opérations suivantes :

Pour...	Procédez comme suit :
Supprimer tous vos contacts	Sélectionnez Tout sélectionner .
Supprimer les contacts sélectionnés	Cochez la case en regard du nom du contact à supprimer.

Étape 4 Sélectionnez **Supprimer la sélection**.

Étape 5 Sélectionnez **OK**.

Conseils pour le dépannage

La suppression d'un contact peut prendre du temps, car cela implique des opérations au niveau de la base de données. Un message s'affiche dans l'interface utilisateur et indique : « Une récente mise à jour effectuée sur votre liste de contacts n'est pas encore entrée en vigueur. Elle sera traitée très prochainement. » Si vous actualisez la page, la liste de contacts mise à jour s'affiche.

Affichage de la liste de contacts

Procédure

Étape 1 Sélectionnez **Options utilisateur > Préférences**.

Étape 2 Sélectionnez une valeur dans le menu **Filtrage des contacts** :

- Pour afficher tous les contacts, sélectionnez **Afficher tous les contacts**.
- Pour afficher uniquement les contacts actuellement disponibles, sélectionnez **Afficher uniquement les contacts en ligne**.

Étape 3 Sélectionnez **Enregistrer**.

Étape 4 Sélectionnez **Options utilisateur > Contacts**.

Étape 5 Dans **Options de recherche**, sélectionnez **Contact « n'est pas vide »** pour afficher tous les contacts correspondant aux critères du filtre.

Étape 6 Sélectionnez **Trouver**.

Configuration du temporisateur d'actualisation de la liste de contacts

Vous pouvez modifier la fréquence d'actualisation de la liste de contacts sur votre téléphone.

Procédure

- Étape 1** Sélectionnez **Options utilisateur > Préférences**.
- Étape 2** Saisissez une valeur (en secondes) comprise entre 7 et 3600 dans le champ **Intervalle d'actualisation de l'écran du téléphone**. La valeur par défaut est 30 secondes.
- Étape 3** Sélectionnez **Enregistrer**.
-



CHAPITRE 4

Configuration des paramètres des réunions

- [Configuration des notifications de réunion, page 15](#)

Configuration des notifications de réunion

Si votre organisation utilise un serveur Microsoft Exchange, Cisco IP Phone Messenger vous permet de recevoir des notifications de réunion sur votre téléphone IP Cisco Unified et fait correspondre l'état des réunions dans votre agenda avec votre état de disponibilité dans Cisco IP Phone Messenger.

Si votre organisation utilise Cisco Unified MeetingPlace, vous pouvez configurer ce programme pour vous connecter directement à des réunions sélectionnées sans avoir à saisir leur ID. En consultant vos réunions quotidiennes et en vous y connectant directement depuis votre téléphone, vous n'avez plus besoin d'ouvrir l'application d'agenda du bureau de votre ordinateur.

Avant de commencer

Vous devez uniquement configurer des notifications de réunion pour une intégration Microsoft Exchange WebDAV avec Cisco Unified Presence. Si votre intégration Microsoft Exchange avec Cisco Unified Presence se fait via Exchange Web Services (EWS), les champs ID utilisateur de MeetingPlace et Mot de passe MeetingPlace de cette procédure ne peuvent pas être configurés et ne s'affichent pas.

Procédure

- Étape 1** Sélectionnez **Options utilisateur > Préférences**.
- Étape 2** Sélectionnez **Activer les notifications de réunion**.
- Étape 3** Effectuez les opérations ci-dessous pour configurer Cisco Unified MeetingPlace afin de vous connecter directement aux réunions sélectionnées :
 - a) Saisissez l'ID utilisateur dans le champ **ID utilisateur de MeetingPlace**.
 - b) Entrez le mot de passe dans le champ **Mot de passe MeetingPlace**, puis saisissez-le à nouveau dans le champ **Confirmer le mot de passe MeetingPlace**.
- Étape 4** Sélectionnez une valeur pour le menu **Ajouter des informations d'agenda à mon état de présence** :
 - Sélectionnez **Activé** pour intégrer vos informations d'agenda à votre état de disponibilité.
 - Sélectionnez **Désactivé** pour ne pas intégrer vos informations d'agenda à votre état de disponibilité.

Étape 5 Sélectionnez **Enregistrer**.

Conseils pour le dépannage

Si votre ID utilisateur inclut un espace, l'intégration au serveur Microsoft Exchange ne fonctionne pas et vous ne recevez pas de notifications de réunion sur votre téléphone IP Cisco Unified. Contactez l'administrateur système pour supprimer les espaces dans votre ID utilisateur.



CHAPITRE 5

Configuration des paramètres des messages

- [Authentification des utilisateurs pour afficher l'historique des messages, page 17](#)
- [Configuration d'une alerte de message entrant, page 18](#)
- [Envoi d'un message de diffusion, page 18](#)
- [Création de messages de réponse personnels, page 18](#)
- [Déconnexion de Cisco IP Phone Messenger, page 19](#)

Authentification des utilisateurs pour afficher l'historique des messages

Par défaut, les utilisateurs doivent entrer leur PIN pour accéder au service Cisco IP Phone Messenger sur leur téléphone IP Cisco. Vous pouvez contourner cette demande d'authentification, le cas échéant, et autoriser les utilisateurs à afficher automatiquement l'historique des messages et les paramètres.

Procédure

	Commande ou action	But
Étape 1	Sélectionnez Options utilisateur > Préférences .	
Étape 2	Sélectionnez une valeur dans le menu Protégé par PIN :	<ul style="list-style-type: none">• Sélectionnez ACT pour activer la demande d'authentification par PIN.• Sélectionnez INA pour désactiver la demande d'authentification par PIN.
Étape 3	Sélectionnez Enregistrer .	

Configuration d'une alerte de message entrant

Cisco IP Phone Messenger permet d'envoyer des messages instantanés et d'en recevoir d'utilisateurs disposant d'ID utilisateur ou de numéros de poste valides au sein de votre organisation. Vous pouvez configurer certains paramètres de message pour Cisco IP Phone Messenger à partir de l'interface **Options utilisateur** de Cisco Unified Presence.

Vous pouvez configurer votre téléphone pour qu'il sonne en cas de réception d'un appel entrant.

Procédure

Étape 1 Sélectionnez **Options utilisateur > Préférences**.

Étape 2 Sélectionnez une valeur dans le menu **Émettre une notification sonore** :

- Sélectionnez **Activé** pour activer l'alerte de message entrant.
- Sélectionnez **Désactivé** pour désactiver l'alerte de message entrant.

Étape 3 Sélectionnez **Enregistrer**.

Envoi d'un message de diffusion

Vous pouvez envoyer un message court (maximum 150 caractères) à certains contacts de votre liste ou à tous.

Procédure

Étape 1 Sélectionnez **Options utilisateur > Diffusion des messages IPPM**.

Étape 2 Sélectionnez **Trouver**.

Étape 3 Effectuez l'une des opérations suivantes :

- Cochez la case en regard des contacts auxquels vous souhaitez envoyer le message.
- Cliquez sur **Tout sélectionner** pour envoyer un message à tous les contacts.

Étape 4 Saisissez votre message dans le champ **Message**.

Étape 5 Sélectionnez **Diffuser**.

Étape 6 Sélectionnez **OK**.

Création de messages de réponse personnels

Vous pouvez créer des messages de réponse personnels. Ils vous permettent de gagner du temps en saisissant un texte personnalisé chaque fois que vous voulez envoyer un message. Vous pouvez créer jusqu'à 15 messages

de ce type et l'administrateur système peut en créer 10 autres. Vos messages de réponse personnels s'affichent toujours après ceux créés par l'administrateur système.

Vous pouvez créer jusqu'à 15 messages de réponse personnels, chacun pouvant contenir un maximum de 255 caractères.

Procédure

- Étape 1** Sélectionnez **Options utilisateur > Messages de réponse IPPM**.
 - Étape 2** Sélectionnez **Ajouter nouveau**.
 - Étape 3** Entrez votre message dans le champ **Texte du message de réponse**.
 - Étape 4** Sélectionnez **Enregistrer**.
 - Étape 5** Sélectionnez les flèches **Haut** et **Bas** pour réorganiser vos messages personnels.
 - Étape 6** Sélectionnez **Enregistrer**.
-

Conseils pour le dépannage

Pour supprimer un message de réponse personnel, sélectionnez-le et cliquez sur **Supprimer**.

Déconnexion de Cisco IP Phone Messenger

Vous pouvez vous déconnecter de Cisco IP Phone Messenger à partir de l'interface Options utilisateur de Cisco Unified Presence.

Si votre téléphone ne vous est pas affecté personnellement, par exemple si vous le partagez avec d'autres, il se peut que vous souhaitiez être automatiquement déconnecté du service Cisco IP Phone Messenger pour plus de sécurité. Pour ce faire, configurez la durée de session comme décrit ici, de sorte que le téléphone vous déconnectera de Cisco IP Phone Messenger une fois le délai de session écoulé.

Procédure

- Étape 1** Sélectionnez **Options utilisateur > Préférences**.
 - Étape 2** Sélectionnez **Déconnex.** dans le volet **Paramètres IPPM**.
Le bouton **Déconn.** n'apparaît que si vous êtes actuellement connecté à Cisco IP Phone Messenger.
 - Étape 3** Sélectionnez **OK**.
 - Étape 4** Pour définir la durée de session de Cisco IP Phone Messenger sur votre téléphone, entrez une valeur comprise entre 1 et 9999 (minutes) dans le champ **Délai de session**. La valeur par défaut est 480 minutes.
 - Étape 5** Sélectionnez **Enregistrer**.
-



CHAPITRE 6

Dépannage de l'interface des options utilisateur de Cisco Unified Presence

- [Connexion impossible à l'interface des options utilisateur, page 21](#)
- [Connexion établie mais options non disponibles, page 21](#)
- [Déconnexion automatique de l'interface des options utilisateur, page 21](#)

Connexion impossible à l'interface des options utilisateur

Problème J'accède à la bonne page Web **Options utilisateur**, mais je ne parviens pas à me connecter à l'aide de mon nom d'utilisateur et de mon mot de passe.

Solution Vérifiez auprès de l'administrateur système si vous utilisez le bon lien pour les pages Web **Options utilisateur** et si le nom d'utilisateur et le mot de passe que vous spécifiez sont corrects. Vérifiez également que vous êtes enregistré en tant que titulaire d'une licence d'utilisation et que vous disposez de l'accès affecté aux pages Web **Options utilisateur**.

Connexion établie mais options non disponibles

Problème Je suis connecté à la page Web **Options utilisateur**, mais je ne vois aucune des options Cisco IP Phone Messenger décrites ici.

Solution Vérifiez auprès de l'administrateur système que vous accédez aux pages Web **Options utilisateur** de Cisco IP Phone Messenger. Assurez-vous également que vous êtes configuré pour accéder aux fonctions de Cisco IP Phone Messenger. Si tel n'est pas le cas, ces fonctions n'apparaissent pas dans vos pages Web **Options utilisateur**.

Déconnexion automatique de l'interface des options utilisateur

Problème Je dois entrer à nouveau mes nom d'utilisateur et mot de passe pour accéder à l'interface des options utilisateur.

Solution Pour plus de sécurité, les pages Web Options utilisateur vous déconnectent automatiquement après trente minutes d'inactivité.



CHAPITRE 7

Options d'accessibilité

- [Accès aux icônes de la fenêtre , page 23](#)
- [Accès aux boutons de la fenêtre , page 23](#)

Accès aux icônes de la fenêtre

Les options utilisateur de Cisco Unified Presence permettent d'accéder aux icônes de la fenêtre sans utiliser la souris. Vous pouvez effectuer cette procédure depuis n'importe quel endroit de la fenêtre, ce qui vous évite de devoir faire défiler l'affichage ou de parcourir plusieurs champs.

De nombreuses fenêtres de Cisco Unified Presence comportent des icônes dans leur partie supérieure. Par exemple, une icône de disque pour la fonction Enregistrer, une icône de signe plus (+) pour Ajouter, etc.

Procédure

- Étape 1** Appuyez sur Alt, sur 1, puis sur Tab.
 - Étape 2** Le curseur affiche en surbrillance la première icône à gauche. Appuyez de nouveau sur Tab pour passer à l'icône suivante.
 - Étape 3** Appuyez sur Entrée pour exécuter la fonction de l'icône.
-

Accès aux boutons de la fenêtre

Les options utilisateur de Cisco Unified Presence permettent d'accéder aux icônes de la fenêtre sans utiliser la souris. Vous pouvez effectuer cette procédure depuis n'importe quel endroit de la fenêtre, ce qui vous évite de devoir faire défiler l'affichage ou de parcourir plusieurs champs.

De nombreuses fenêtres de Cisco Unified Presence comportent des boutons dans leur partie inférieure, notamment pour la fonction Enregistrer ou Ajouter.

Procédure

Étape 1 Appuyez sur Alt, sur 2, puis sur Tab.

Étape 2 Le curseur affiche en surbrillance le premier bouton à gauche. Appuyez de nouveau sur Tab pour passer au bouton suivant.

Étape 3 Appuyez sur Entrée pour exécuter la fonction du bouton.
