دليل المستخدم للإصدار 8.5 من Cisco Unified Presence

تاريخ أول نشر: July 02, 2010

تاريخ آخر تعديل: December 13, 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

رقم جزء النص: OL-14086-01

المحتويات

الفصل 1

بدء استخدام واجهة خيارات مستخدم Cisco Unified Presence

المستعرضات المدعمة

تدعم واجهة Cisco Unified Presence **خيارات المستخدم** المستعرضات التالية:

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

ملاحظة لا يدعم Cisco Unified Presence مستعرض Safari أو Google Chrome حاليًا.

موضوعات ذات صلة

- تسجيل الدخول إلى "خيارات مستخدم Cisco Unified Presence" , الصفحة 1

تسجيل الدخول إلى "خيارات مستخدم Cisco Unified Presence"

قبل البدء

يمكنك استخدام واجهة "خيارات مستخدم Cisco Unified Presence" لتخصيص الإعدادات وإنشاء رسائل رد شخصية وتنظيم جهات الاتصال وإرسال رسائل بث.

- لكي تتمكن من تسجيل الدخول إلى "خيارات مستخدم Cisco Unified Presence"، يجب على المسؤول تعيين المستخدم إلى مجموعة "مستخدم CCM القياسية".
- احصل على المعلومات التالية من مسؤول النظام لديك:

- عنوان URL الخاص "بخيارات مستخدم Cisco Unified Presence".
- اسم المستخدم وكلمة المرور الخاصين "بخيارات مستخدم Cisco Unified Presence".

- تأكد من أنك تستخدم مستعرض ويب مدعَم.

الإجراء

الخطوة 1 افتح مستعرض ويب مدعَم على الكمبيوتر.

الخطوة 2 أدخل عنوان URL الخاص "بخيارات مستخدم Cisco Unified Presence"، مثل: http://<*CUPS server*>/cupuser.

الخطوة 3 أدخل اسم المستخدم الخاص "بخيارات مستخدمCisco Unified Presence".

الخطوة 4 أدخل كلمة المرور الخاصة "بخيارات مستخدم Cisco Unified Presence" التي أعطاها لك مسؤول النظام لديك.

الخطوة 5 حدد **تسجيل الدخول**.

لتسجيل الخروج من واجهة "خيارات المستخدم"، حدد **تسجيل الخروج** الموجودة في الزاوية العليا اليمنى في نافذة "خيارات المستخدم". سيتم تسجيل خروجك تلقائيًا من "خيارات المستخدم" بعد ثلاثين دقيقة من حالة عدم النشاط، وذلك لأغراض أمنية.

موضوعات ذات صلة

- المستعرضات المدعمة , الصفحة 1

الفصل 2

إعداد نُهج الخصوصية

إعداد نهج الخصوصية الافتراضي

يسمح لك نُهج الخصوصية بتحديد المستخدمين الذين يمكنهم رؤية حالة التوفر الخاصة بك وإرسال رسائل فورية إليك. يدعم هذا الإصدار من Cisco Unified Presence القاعدة الخاصة بجهات الاتصال التي يمكن لأي شخص (تقوم بمشاهدته) رؤية حالة توفرك افتراضيًا من خلالها ما لم ترفض منحه الإذن صراحةً لعرض حالتك.

ولذلك، يمكنك استخدام نُهج خصوصية للسماح بالمستخدمين والمجالات أو حظرهم. تسمح لك الخيارات التالية تهيئة نهج خصوصية كإعداد افتراضي على مستوى المؤسسة أو من خلال طلب محدد للمستخدم.

- سماح - يُسمح للمستخدمين/المجالات رؤية حالة توفرك، بالإضافة إلى قدرتهم على إرسال رسائل فورية افتراضيًا إليك. ما لم تُضرف المستخدم/المجال بشكلٍ صريح إلى القائمة المحظورة الخاصة بك. يمكنك إعداد نهج الخصوصية "سماح" للمستخدمين الداخليين والمجالات الداخلية فقط. هذا الخيار غير متوفر للمستخدمين/المجالات (المجمعة) الخارجية.
- حظر- المستخدمون/المجالات التي تقوم بحظرها لا يمكنها رؤية حالة توفرك ولا إرسال رسائل فورية إليك. المستخدمون الذين تقوم بحظرهم يرون دائمًا حالتك "غير متاح". يمكنك إعداد نهج خصوصية "حظر" للمستخدمين/المجالات (المجمعة) الداخلية والخارجية.
- سؤال - يطالب نهج الخصوصية "سؤال" المستخدمين (من خلال طلب) بحظر تبادل حالة التوفر أو السماح بها بشكلٍ صريح، وكذلك حظر الرسائل الفورية من مستخدمين/مجالات محددة أو السماح بها. يطالب التطبيق العميل المستخدم باعتماد الاشتراك أو رفضه. يمكنك إعداد نهج الخصوصية "سؤال" للمستخدمين أو المجالات (المجمعة) الخارجية فقط، وكذلك إذا كانت جهة الاتصال أو المجال الخارجي غير موجود في القائمة "مسموح به" أو "محظور" للمستخدم.

الإجراء

الخطوة 1 حدد **خيارات المستخدم** > **نُهج الخصوصية**.

الخطوة 2 حدد أحد الخيارين التاليين:

الإجراء...	اتبع الآتي
سماح لكل المستخدمين الداخليين برؤية توفرك وإرسال رسائل فورية (ما عدا المستخدمين/المجالات الداخلية التي قمت بإضافتها بشكلٍ صريح إلى قائمة استثناءات المحظورة). **ملاحظة** راجع الاستثناء الخاص بإعداد النهج هذا في قسم "تلميحات خاصة باستكشاف الأخطاء وإصلاحها" في هذا الموضوع. مع العلم بأن هذا النهج لن يسمح للمستخدمين الخارجيين برؤية توفرك.	1 حدد **سماح** من المستخدمين الداخليين (داخل شركتك/مؤسستك): القائمة المنسدلة. 2 (اختياري) أضف المستخدمين الداخليين إلى قوائم الاستثناءات المحظورة مُتبعًا الإجراءات المذكورة في هذه الوحدة. راجع الإجراء التالي.
حظر كل المستخدمين الداخليين من رؤية توفرك وإرسال رسائل فورية إليك (ما عدا المستخدمين الداخليين الذين قمت بإضافتهم بشكلٍ صريح إلى قائمة الاستثناءات المسموح بها). **ملاحظة** لن يحظر هذا النهج المستخدمين الخارجيين من رؤية توفرك.	1 حدد **حظر** من المستخدمين الداخليين (داخل شركتك/مؤسستك): القائمة المنسدلة. 2 (اختياري) أضف المستخدمين الداخليين إلى قائمة الاستثناءات المسموح بها مُتبعًا الإجراءات المذكورة في هذه الوحدة. راجع الإجراء التالي.
حظر كل المستخدمين الخارجيين من رؤية توفرك وإرسال رسائل فورية إليك (ما عدا المستخدمين الخارجيين الذين قمت بإضافتهم بشكلٍ صريح إلى قائمة الاستثناءات المسموح بها). **ملاحظة** لن يحظر هذا النهج المستخدمين الداخليين من رؤية توفرك.	1 حدد **حظر** من "مستخدمون خارجيون (كل الآخرين)": القائمة المنسدلة. 2 (اختياري) قم بإضافة المستخدمين الخارجيين إلى قائمة الاستثناءات المسموح بها مُتبعًا الإجراءات المذكورة في هذه الوحدة. راجع الإجراء التالي.
مطالبة كل المستخدمين (بطلب سؤال) لإعداد النهج سماح/حظر الخاص بهم للمستخدمين الخارجيين (ما عدا المستخدمين الخارجيين الذين قمت بإضافتهم بشكلٍ صريح إلى قائمة الاستثناءات المسموح بها/المحظورة). **ملاحظة** لن يحظر هذا النهج المستخدمين الداخليين من رؤية توفرك.	1 حدد **سؤال** من "مستخدمون خارجيون (كل الآخرين)": القائمة المنسدلة. 2 (اختياري) قم بإضافة مستخدمين خارجيين إلى قائمة الاستثناءات المسموح بها/المحظورة مُتبعًا الإجراءات المذكورة في هذه الوحدة. راجع الإجراء التالي.

الخطوة 3 حدد **حفظ الافتراضي**.

تلميحات لاستكشاف الأخطاء وإصلاحها

يخول خادم Cisco Unified Presence تلقائيًا أحد المستخدمين بقائمة جهات اتصال مستخدم آخر لعرض حالة التوفر الخاصة به. يجب مراعاة هذا الاستثناء مع إعداد النهج سماح لكل المستخدمين الداخليين إذا قمت بالإجراء إيقاف تشغيل التخويل التلقائي على خادمCisco Unified Presence، كما يجب مراعاة أن الإعداد الافتراضي للمجالين العام والمحلي معيَّن على "سماح" - ستتم مطالبة المستخدم بالموافقة على طلب الاشتراك أو رفضه. وهو ما يُعد مخطط "سؤال" للمجال المحلي. لمزيدٍ من المعلومات حول إعداد التخويل التلقائي في Cisco Unified Presence، راجع دليل توزيع *Cisco Unified Presence*(على موقع الويب Cisco.com).

ما الذي يتم لاحقًا

- إذا أردت تجاوز نهج الخصوصية "سماح/حظر" الافتراضي الذي تم تعيينه للمستخدمين الداخليين/الخارجيين على مستوى المؤسسة، راجع الموضوعات التالية التي توضح كيفية تهيئة قوائم الاستثناءات للمستخدمين.

إضافة مستخدمين داخليين إلى قوائم الاستثناءات المسموح بها أو المحظورة

يسمح لك هذا الإجراء بإدارة استثناءات نهج الخصوصية العام في شكل القائمتين "سماح" و"حظر". وحسب نهج الخصوصية الافتراضي الذي تقوم بتعيينه على مستوى المؤسسة، تتوفر القائمة المسموح بها أو المحظورة للتحرير. وبهذه الطريقة، يمكنك تجاوز سلوك النهج الافتراضي لإضافة أشخاص محددين داخل مؤسستك إلى القائمة المسموح بها أو المحظورة.

- يتيح تعيين النهج "سماح" للمستخدمين المحددين إمكانية رؤية توفرك وإرسال رسائل فورية إليك، حتى إذا حظرهم النهج العام.
- يمنع تعيين النهج "حظر" مستخدمين محددين من عرض الحالة وتبادل إرسال الرسائل الفورية عند استخدامهم عملاء Cisco (الإصدار 7 من Cisco Unified Personal Communicator، والإصدار 8 من Cisco Unified Personal Communicator) - حتى في حالة سماح النهج العام لهم بذلك. ويُسمح دائمًا للمستخدمين الموجودين بالقائمة "جهة الاتصال" ما لم يتم حظرهم بشكل صريح في قائمة الاستثناءات. لاحظ أنه سيستمر بعض عملاء XMPP لجهة خارجية في إرسال رسائل فورية ويتلقونها بغض النظر عن النهج الذي قمت بتعيينه.

قبل البدء

قم بتعيين نهج الخصوصية الافتراضي الخاص بك.

الإجراء

الخطوة 1 حدد **خيارات المستخدم > نُهج الخصوصية**.

الخطوة 2 حدد **إضافة مستخدم** في إطار "إعدادات المستخدم" على النافذة "نهج الخصوصية".

الخطوة 3 قم بتنفيذ أحد هذه الإجراءات:

- حدد **سماح** للسماح للمستخدم برؤية توفرك.
- حدد **حظر** لحظر المستخدم من رؤية توفرك.

الخطوة 4 أدخل "معرف المستخدم" الصالح للمستخدم الداخلي. يجب أن يكون "معرف المستخدم" في الشبكة الداخلية الخاصة بك بالتنسيق *<userid@domain>*.

الخطوة 5 حدد **المجال المحلي**.

الخطوة 6 حدد **إضافة** لإضافة المستخدم الداخلي إلى المجال المحلي.

تلميحات لاستكشاف الأخطاء وإصلاحها

- يمكن للمستخدمين المجمعين إضافة مستخدم محلي باستخدام معرف البريد الإلكتروني أو JID قياسي. يعتمد هذا الاختيار على ما إذا كان "المسؤول" قد قام بتمكين معرف البريد الإلكتروني الخاص بالمجال أو تعطيله.
- بمجرد **إضافة** مستخدم إلى القائمة "مسموح به/محظور"، يتم عرض التفاصيل في الجدول الذي يظهر على هذه النافذة. لإزالة أي مستخدم من القائمة "مسموح به/محظور"، حدد مربع الاختيار الخاص بالمستخدم وحدد **حذف المحدد**.

إضافة مستخدمين خارجيين إلى قوائم الاستثناءات المسموح بها أو المحظورة

يسمح لك هذا الإجراء بإدارة استثناءات نهج الخصوصية العام في شكل القائمتين "سماح" و"حظر". وحسب نهج الخصوصية الافتراضي الذي تقوم بتعيينه على مستوى المؤسسة، تتوفر القائمة المسموح بها أو المحظورة للتحرير. وبهذه الطريقة، يمكنك تجاوز سلوك النهج الافتراضي لإضافة أشخاص محددين من خارج مؤسستك إلى القائمة المسوح بها أو المحظورة.

- يتيح تعيين النهج "سماح" للمستخدمين المحددين إمكانية رؤية توفرك وإرسال رسائل فورية إليك، حتى إذا حظرهم النهج العام.
- يمنع تعيين النهج "حظر" مستخدمين محددين من رؤية توفرك أو إرسال رسائل فورية إليك، حتى إذا كان النهج العام يسمح لهم بذلك (من خلال الرد الإيجابي على طلب "سؤال").

قبل البدء

قم بتعيين نهج الخصوصية الافتراضي الخاص بك.

الإجراء

الخطوة 1 حدد **خيارات المستخدم** > **نُهج الخصوصية**.

الخطوة 2 حدد **إضافة مستخدم** في إطار "إعدادات المستخدم" على النافذة "نهج الخصوصية".

الخطوة 3 قم بتنفيذ أحد هذه الإجراءات:

- حدد **سماح** للسماح للمستخدم برؤية توفرك.
- حدد **حظر** لحظر المستخدم من رؤية توفرك.

الخطوة 4 أدخل "معرف المستخدم" الصالح للمستخدم الداخلي. يجب أن يكون "معرف المستخدم" موجودًا على الشبكة الداخلية الخاصة بك بالتنسيق (*<userid@domain>*).

الخطوة 5 حدد المجال الذي ينتمي إليه المستخدم من المجالات التالية:

- **المجال المجمع**.
- **المجال المخصص** - المجال المخصص هو مجال خارجي غير موجود في قائمة المجال المجمع.

الخطوة 6 أكمل أحد هذه الإجراءات:

إذا قمت بتحديد...	اتبع الآتي:
المجال المجمع	حدد المجال الذي تقوم بالتجميع باستخدامه من القائمة المنسدلة.
المجال المخصص	أدخل المجال الخاص بالمستخدم. **ملاحظة** من الأمثلة على المجال المخصص؛ المجال "mycompany.com".

الخطوة 7 حدد **إضافة**.

تلميحات لاستكشاف الأخطاء وإصلاحها

بمجرد **إضافة** مستخدم إلى القائمة "مسموح به/محظور"، يتم عرض التفاصيل في الجدول الذي يظهر على هذه النافذة. لإزالة أي مستخدم من القائمة "مسموح به/محظور"، حدد مربع الاختيار الخاص بالمستخدم وحدد **حذف المحدد**.

إضافة المجالات الخارجية إلى قوائم الاستثناءات المسموح بها أو المحظورة

قبل البدء

يمكنك حظر مجال خارجي بأكمله أو السماح به. إذا قمت بحظر أي مجال خارجي، فسيتم حظر أية طلبات من المستخدمين برؤية توفرك في ذلك المجال، بشرط أنك لم تكن قد قمت بإضافة هؤلاء المستخدمين الخارجيين إلى قائمتك المسموح بها.

الإجراء

الخطوة 1 حدد **خيارات المستخدم** > **نُهج الخصوصية**.

الخطوة 2 حدد **إضافة مجال** في إطار "إعدادات المستخدم" على النافذة "نهج الخصوصية".

الخطوة 3 قم بتنفيذ أحد هذه الإجراءات:

- حدد **سماح** للسماح للمستخدم برؤية توفرك.
- حدد **حظر** لحظر المستخدم من رؤية توفرك.

الخطوة 4 حدد أحد هذه المجالات للسماح بها أو حظرها:

- **المجال المجمع**
- **المجال المخصص** - المجال المخصص هو مجال خارجي غير موجود في قائمة المجال المجمع.

الخطوة 5 أكمل أحد هذه الإجراءات:

إذا قمت بتحديد...	اتبع الآتي:
المجال المجمع	حدد المجال الذي تقوم بالتجميع باستخدامه من القائمة المنسدلة.
المجال المخصص	أدخل المجال الخاص بالمستخدم. **ملاحظة** من الأمثلة على المجال المخصص؛ المجال "mycompany.com".

الخطوة 6 حدد **إضافة**.

تلميحات لاستكشاف الأخطاء وإصلاحها

بمجرد **إضافة** مجال إلى القائمة "مسموح به/محظور"، سيتم عرض التفاصيل في الجدول الذي يظهر على هذه النافذة. لإزالة أي مستخدم من القائمة "مسموح به/محظور"، حدد مربع الاختيار الخاص بالمستخدم وحدد **حذف المحدد**.

الفصل 3

تنظيم قائمة جهات الاتصال

إضافة جهات اتصال إلى قائمة جهات الاتصال

قبل البدء

- يحدد مسؤول النظام لديك عدد جهات الاتصال التي يمكنك إدراجها بالقائمة، بحد أقصى 100 جهة اتصال. اتصل بمسؤول النظام لديك للتحقق من حد جهات الاتصال على هاتفك.
- يمكنك إضافة جهة اتصال خارجية إما بتحديد مجال خارجي أو بتهيئة مجال مخصص للمستخدمين من خارج مؤسستك.
- يُعد المستخدمون الداخليون والخارجيون بالقائمة "جهة الاتصال" استثناءات للنُهج الداخلية والخارجية. ويُسمح دائمًا للمستخدمين الموجودين بالقائمة "جهة الاتصال" ما لم يتم حظرهم بشكل صريح في قائمة الاستثناءات.
- في تطبيق إرسال الرسائل الفورية الخاص بك، يمكنك إضافة جهات الاتصال الذين لديهم حالة التوفر غير مرئي، فعلى سبيل المثال، قد ترغب في إضافة أشخاص تفضل الاتصال بهم من قائمة جهات الاتصال في التطبيق. هذه الأنواع من جهات الاتصال غير مرئية في قائمة جهات الاتصال بواجهة **خيارات المستخدم**.
- إذا قمت بإجراء تغييرات (إضافة/حذف/تعديل) على قائمة جهات الاتصال لديك، فإن هذه التغييرات تنعكس تلقائيًا على عملاء Cisco (بالنسبة للمستخدمين الذين قاموا بتسجيل الدخول).

الإجراء

الخطوة 1 حدد **خيارات المستخدم** > **جهات الاتصال**.

الخطوة 2 حدد **إضافة جديد**.

الخطوة 3 حدد أحد الخيارين التاليين:

إذا كانت جهة الاتصال التي ترغب في إضافتها هي...	اتبع الآتي:
داخلي - مستخدم ينتمي إلى المجال المحلي الخاص بك (شركتك أو مؤسستك عادةً)	**1** إضافة معرف المستخدم لجهة الاتصال المجمعة التي ترغب في إضافتها، في الحقل "جهة اتصال". **2** تحديد **تحديد من قائمة المجالات** **3** تحديد مجال (محلي) داخلي من القائمة "مجال". **4** يمكنك إدخال "الاسم البديل" للمستخدم إذا كنت ترغب في عرض كنية على الكمبيوتر. **ملاحظة** لقد تم منعك من إضافة مستخدمين محظورين/مجالات محظورة بالفعل من قبل المسؤول. يجب تعيين نهج الخصوصية للمؤسسة للسماح بالمجال الداخلي أو مستخدمين محددين في هذا المجال بعرض حالة التوفر الخاصة بك وإرسال رسائل فورية إليك.
خارجي - مستخدم ينتمي إلى خارج المجال المحلي الخاص بك (شركتك أو مؤسستك عادة).	قم بتنفيذ أحد الإجراءين التاليين: **1** إضافة معرف المستخدم لجهة الاتصال المجمعة التي ترغب في إضافتها، في الحقل "جهة اتصال". **2** تحديد **تحديد من قائمة المجالات.** • حدد مجالاً خارجيًا من القائمة "مجال". **3** تحديد **إدخال مجال مخصص.** • أدخل مجالاً مخصصًا لجهات الاتصال الموجودة خارج مؤسستك. **ملاحظة** لقد تم منعك من إضافة مستخدمين محظورين/مجالات محظورة بالفعل من قبل المسؤول. يجب تعيين نهج الخصوصية للمؤسسة ليطلب منك (في نافذة منبثقة) السماح للمجال الخارجي أو مستخدمين محددين في هذا المجال بعرض حالة التوفر الخاصة بك وإرسال رسائل فورية إليك.

الخطوة 4 إدخال اسم بديل (كنية) لجهة الاتصال.

الخطوة 5 حدد **حفظ**.

تلميحات لاستكشاف الأخطاء وإصلاحها

يمكنك تخصيص اسم بديل واحد فقط (كنية) لكل جهة اتصال. إذا قمت بإدخال اسم بديل لجهة اتصال اختياريًا، فسيتم عرضه على عملاء Cisco، وليس بالضرورة على عملاء XMPP لجهة خارجية. إذا قمت بتحديث اسم إحدى جهات الاتصال، فسيتم تحديث تغيير الاسم هذا في قائمة جهات الاتصال الخاصة بك في Cisco Unified Personal Communicator، وسيتم تحديثه في جميع مجموعات جهات الاتصال الخاصة بك.

حذف جهات اتصال من قائمة جهات الاتصال

الإجراء

الخطوة 1 حدد **خيارات المستخدم** > **جهات الاتصال**.

الخطوة 2 حدد "بحث".

الخطوة 3 قم بتنفيذ أحد هذه الإجراءات:

الإجراء...	اتبع الآتي:
حذف كل جهات الاتصال لديك	حدد **تحديد الكل.**
حذف جهات الاتصال المحددة	حدد جهات الاتصال الموجودة بجوار اسم جهة الاتصال التي تريد حذفها.

الخطوة 4 حدد **حذف المحدد**.

الخطوة 5 حدد **موافق**.

تلميحات لاستكشاف الأخطاء وإصلاحها

قد يستغرق حذف إحدى جهات الاتصال بعض الوقت لأن هذا الإجراء يتضمن معالجة قاعدة البيانات. يتم عرض رسالة على "UI" تشير إلى أنه "لم يتم بعد تفعيل عملية التحديث الأخيرة لقائمة جهات الاتصال لديك. وهي قيد انتظار المعالجة قريبًا". إذا قمت بتحديث الصفحة، فسيتم عرض قائمة جهات الاتصال المحدّثة.

عرض قائمة جهات الاتصال

الإجراء

الخطوة 1 حدد **خيارات المستخدم** > **تفضيلات**.

الخطوة 2 حدد قيمة من القائمة **تصفية جهات الاتصال**.

- لعرض كل جهات الاتصال، حدد **عرض كل جهات الاتصال**.
- لعرض جهات الاتصال المتوفرين حاليًا فقط، حدد **عرض جهات الاتصال المباشرة فقط**.

الخطوة 3 حدد **حفظ**.

الخطوة 4 حدد **خيارات المستخدم** > **جهات الاتصال**.

الخطوة 5 من **خيارات البحث**، حدد **جهة اتصال "ليس فارغًا"** لعرض كل جهات الاتصال المتطابقة مع معايير التصفية.

الخطوة 6 حدد **بحث**.

تهيئة مؤقت تحديث قائمة جهات الاتصال

يمكنك تعديل عدد مرات تحديث قائمة جهات الاتصال على هاتفك.

الإجراء

الخطوة 1 حدد **خيارات المستخدم** > **تفضيلات**.

الخطوة 2 أدخل قيمة (بالثواني) من 7 إلى 3600 ثانية في الحقل **فاصل تحديث شاشة الهاتف**. القيمة الافتراضية هي 30 ثانية.

الخطوة 3 حدد **حفظ**.

الفصل 4

تهيئة إعدادات الاجتماع

إعداد رسائل الإعلام باجتماع

إذا كانت المؤسسة التي تعمل بها تستخدم خادم Microsoft Exchange، فسيمكّنك Cisco IP Phone Messenger من تلقي رسائل إعلام بالاجتماع على هاتف Cisco Unified IP الخاص بك، كما يربط بين حالة الاجتماعات الموجودة في التقويم الخاص بك وحالة التوفر الخاص بك في Cisco IP Phone Messenger.

فإذا كانت المؤسسة التي تعمل بها تستخدم Cisco Unified MeetingPlace، فيمكنك تهيئته لتوصيلك مباشرةً بالاجتماعات المحددة ولن تحتاج إلى إدخال أية معرفات للاجتماعات. ومع استعراض الاجتماعات اليومية مباشرة من الهاتف الخاص بك والانضمام إليها، فإنك لن تحتاج إلى فتح برنامج التقويم الموجود على سطح مكتب الكمبيوتر.

قبل البدء

لا تحتاج سوى تهيئة رسائل إعلام بالاجتماعات لتكامل Microsoft Exchange WebDAV مع Cisco Unified Presence. إذا كان تكامل Microsoft Exchange مع Cisco Unified Presence يتم عبر Exchange Web Services (EWS)، فلا يمكن تهيئة حقلي معرف المستخدم وكلمة المرور لمكان الاجتماع، مما يعني أنه لا يتم عرضهما.

الإجراء

الخطوة 1 حدد **خيارات المستخدم** > **تفضيلات**.

الخطوة 2 حدد **تمكين رسائل إعلام باجتماع**.

الخطوة 3 قم بتنفيذ هذه الإجراءات لتهيئة Cisco Unified MeetingPlace لتوصيلك مباشرة بالاجتماعات المحددة:

a) أدخل معرف المستخدم في الحقل **معرف مستخدم مكان الاجتماع**.

b) أدخل كلمة المرور في الحقل **كلمة مرور مكان الاجتماع**، ثم قم بإدخالها مرة أخرى في الحقل **تأكيد كلمة مرور مكان الاجتماع**.

الخطوة 4 حدد قيمة للقائمة **تضمين معلومات التقويم في حالة التواجد الخاصة بي**:

- حدد **تشغيل** لدمج معلومات التقويم الخاص بك في حالة التوفر الخاصة بك.
- حدد **إيقاف** لعدم دمج معلومات التقويم الخاص بك في حالة التوفر الخاصة بك.

الخطوة 5 حدد **حفظ**.

تلميحات لاستكشاف الأخطاء وإصلاحها

إذا كان معرف المستخدم الخاص بك يحتوي على حرف مسافة، فلن يتم التكامل مع خادم Microsoft Exchange، ولن تتلقى رسائل إعلام بالاجتماعات على هاتفCisco Unified IP الخاص بك. اتصل بمسؤول النظام لديك لإزالة المسافات من معرف المستخدم الخاص بك.

الفصل 5

تهيئة إعدادات الرسائل

مصادقة المستخدمين لعرض تاريخ الرسالة

يُطلب من المستخدمين - بشكل افتراضي - إدخال PIN عند الوصول إلى خدمة Cisco IP Phone Messenger على هاتف Cisco IP الخاص بهم. يمكنك تجاوز طلب المصادقة - إذا لزم الأمر - والسماح للمستخدمين بعرض تاريخ الرسالة وإعدادتها تلقائيًا.

الإجراء

	الأمر أو الإجراء	الغرض
الخطوة 1	حدد **خيارات المستخدم** > **تفضيلات**.	
الخطوة 2	حدد قيمة من القائمة **الحماية برقم PIN**:	• حدد **تشغيل** - لتشغيل طلب مصادقة PIN • حدد **إيقاف** - لإيقاف تشغيل طلب مصادقة PIN
الخطوة 3	حدد **حفظ**.	

تهيئة تنبيه الرسائل الواردة

يتيح لك Cisco IP Phone Messenger إمكانية إرسال رسائل فورية وتلقيها من المستخدمين الذين لديهم معرفات مستخدمين صالحة أو أرقام داخلية في مؤسستك. يمكنك تهيئة إعدادات رسائل معينة لـ Cisco IP Phone Messenger من واجهة **خيارات المستخدم** في Cisco Unified Presence.

يمكنك تهيئة الهاتف للتنبيه بالرنين عند تلقي رسالة واردة.

الإجراء

الخطوة 1 حدد **خيارات المستخدم** > **تفضيلات**.
الخطوة 2 حدد قيمة من القائمة **تشغيل إشعار صوتي**:

- **حدد تشغيل** - لتشغيل تنبيه الرسائل الواردة
- **حدد إيقاف** - لإيقاف تنبيه الرسائل الواردة

الخطوة 3 حدد **حفظ**.

إرسال رسالة بث

يمكنك إرسال رسالة قصيرة (بحد أقصى 150 حرفًا) إلى بعض أو كل جهات الاتصال المدرجة بقائمة جهات الاتصال لديك.

الإجراء

الخطوة 1 حدد **خيارات المستخدم** > **رسائل بث IPPM.**
الخطوة 2 حدد **بحث**.
الخطوة 3 قم بتنفيذ أحد هذه الإجراءات:

- حدد جهات الاتصال الذين تريد إرسال الرسالة إليهم.
- حدد **تحديد الكل** لإرسال رسالة إلى كل جهات الاتصال.

الخطوة 4 أدخل الرسالة في حقل **الرسالة**.
الخطوة 5 حدد **بث**.
الخطوة 6 حدد **موافق**.

إنشاء رسائل الرد الشخصية

يمكنك إنشاء رسائل رد شخصية. يوفر هذا النوع من الرسائل الوقت في كتابة رسالة نصية مخصصة في كل مرة تقوم فيها بإرسال رسالة. يمكنك إنشاء عدد من الرسائل يصل إلى 15 رسالة، ويمكن لمسؤول النظام لديك إنشاء 10 رسائل إضافية. تظهر دائمًا رسائل الرد الشخصية التي تقوم بإنشائها بعد الرسائل التي يقوم مسؤول النظام بإنشائها.

يمكنك إنشاء عدد من رسائل الرد الشخصية الجديدة يصل إلى 15 رسالة بحد أقصى 255 حرفًا لكل رسالة.

الإجراء

الخطوة 1 حدد **خيارات المستخدم** > **رسائل استجابة IPPM**.
الخطوة 2 حدد **إضافة جديد**.
الخطوة 3 أدخل رسالتك في الحقل **نص رسالة الرد**.
الخطوة 4 حدد **حفظ**.
الخطوة 5 حدد السهمين **أعلى** و**أسفل** لإعادة ترتيب رسائلك الشخصية.
الخطوة 6 حدد **حفظ**.

تلميحات لاستكشاف الأخطاء وإصلاحها

لحذف رسالة رد شخصية، حدد الرسالة، ثم حدد **حذف**.

تسجيل الخروج من Cisco IP Phone Messenger

يمكنك تسجيل الخروج من Cisco IP Phone Messenger من خلال واجهة "خيارات مستخدم Cisco Unified Presence".

إذا كان الهاتف الخاص بك غير معين لك، على سبيل المثال إذا كنت تتشارك الهاتف مع الآخرين، فإنك قد تريد أن يقوم الهاتف بتسجيل خروجك تلقائيًا من خدمة Cisco IP Phone Messenger لتوفير مزيد من الأمان. قم بتهيئة مؤقت الجلسة كما هو مذكور هنا وسيقوم الهاتف بتسجيل خروجك من Cisco IP Phone Messenger حينما ينتهي مؤقت الجلسة.

الإجراء

الخطوة 1 حدد **خيارات المستخدم** > **تفضيلات**.
الخطوة 2 حدد **تسجيل الخروج في جزء إعدادات IPPM**.
يتم عرض زر تسجيل الخروج فقط إذا كنت مسجلاً حاليًا في Cisco IP Phone Messenger.
الخطوة 3 حدد **موافق**.
الخطوة 4 لإعداد مؤقت الجلسة بخصوص Cisco IP Phone Messenger في هاتفك، أدخل قيمة من 1 إلى 9999 (بالدقائق) في الحقل **مؤقت الجلسة**.
القيمة الافتراضية هي 480 دقيقة.
الخطوة 5 حدد **حفظ**.

الفصل 6

استكشاف الأخطاء وإصلاحها في واجهة خيارات مستخدم Cisco Unified Presence

لا يمكن تسجيل الدخول إلى واجهة خيارات المستخدم

المشكلة أحاول الوصول إلى صفحة ويب **خيارات المستخدم** الصحيحة، ولكن لا يمكنني تسجيل الدخول باستخدام اسم المستخدم وكلمة المرور الخاصين بي.

الحل اتصل بمسؤول النظام لديك للتحقق من أنك تستخدم الارتباط الصحيح لصفحات ويب **خيارات المستخدم**، وأنك تقوم بإدخال اسم المستخدم وكلمة المرور الصحيحين. وللتحقق أيضًا من أنك مسجل كمستخدم مرخص وأن لديك إمكانية الوصول المعين إلى صفحات ويب **خيارات المستخدم**.

تم تسجيل الدخول ولكن الخيارات غير متاحة

المشكلة لقد قمت بتسجيل الدخول إلى صفحة ويب **خيارات المستخدم**، ولكنني لا أجد أيًا من خيارات Cisco IP Phone Messenger المذكورة هنا.

الحل اتصل بمسؤول النظام لديك للتحقق من وصولك إلى صفحات ويب **خيارات المستخدم** بخصوص Cisco IP Phone Messenger. وللتحقق أيضًا من أنه تمت تهيئة بياناتك لتتمكن من الوصول إلى ميزات Cisco IP Phone Messenger. إذا لم يتم إعداد بياناتك لتتمكن من الوصول إلى هذه الميزات، فلن تظهر تلك الميزات على صفحات ويب **خيارات المستخدم**.

تم تسجيل الخروج تلقائيًا من واجهة خيارات المستخدم

المشكلة يجب إعادة إدخال اسم مستخدم وكلمة مرور "خيارات المستخدم" للوصول إلى واجهة "خيارات المستخدم".

الحل لمزيد من الأمان، تقوم صفحات ويب "خيارات المستخدم" بتسجيل خروجك تلقائيًا بعد ثلاثين دقيقة من الخمول.

تم تسجيل الخروج تلقائيًا من واجهة خيارات المستخدم

الفصل 7

كيفية الوصول إلى خيارات إمكانية الوصول

الوصول إلى الرموز في النافذة

توفر خيارات مستخدم Cisco Unified Presence الوظائف التي تسمح لك بالوصول إلى الرموز في النافذة دون استخدام الماوس. يمكنك تنفيذ هذا الإجراء من أي مكان على النافذة، فلا تحتاج إلى التمرير أو التنقل بين حقول متعددة.

هناك العديد من النوافذ في Cisco Unified Presence تحتوي على رموز يتم عرضها أعلى النافذة، فعلى سبيل المثال، يوجد رمز على شكل قرص للخيار "حفظ"، ورمز على شكل علامة الجمع (+) للخيار "إضافة"، وهكذا.

الإجراء

الخطوة 1 اضغط على المفتاح Alt، ثم اضغط على المفتاح 1، ثم اضغط على المفتاح Tab.

الخطوة 2 يقوم المؤشر بتمييز أول رمز من اليمين. اضغط Tab مرة أخرى للانتقال إلى الرمز التالي.

الخطوة 3 اضغط Enter لتنفيذ وظيفة الرمز.

الوصول إلى الأزرار في النافذة

توفر خيارات مستخدم Cisco Unified Presence الوظائف التي تسمح لك بالوصول إلى الرموز في النافذة دون استخدام الماوس. يمكنك تنفيذ هذا الإجراء من أي مكان على النافذة، فلا تحتاج إلى التمرير أو التنقل بين حقول متعددة.

هناك العديد من النوافذ في Cisco Unified Presence تحتوي على أزرار معروضة أسفل النافذة، على سبيل المثال، الزر "حفظ" والزر "إضافة" وهكذا.

الإجراء

الخطوة 1 اضغط على المفتاح Alt، ثم اضغط على المفتاح 2، ثم اضغط على المفتاح Tab.
الخطوة 2 يقوم المؤشر بتمييز أول زر من اليمين. اضغط على المفتاح Tab مرة أخرى للانتقال إلى المفتاح التالي.
الخطوة 3 اضغط على المفتاح Enter لتنفيذ وظيفة المفتاح.