دليل إدارة هاتف مؤتمر Cisco IP 8832 لـ Cisco Unified Communications Manager

تاريخ أول نشر: 15-09-2017

تاريخ آخر تعديل: 16-06-2023

Americas Headquarters
.Cisco Systems, Inc
West Tasman Drive 170
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
(NETS (6387-553 800
Fax: 408 527-0883

تخضع المواصفات والمعلومات المتعلقة بالمنتجات الواردة في هذا الدليل للتغيير دون إشعار. يُعتقد أن جميع البيانات والمعلومات والتوصيات الواردة في هذا الدليل دقيقة ولكنها مقدمة دون أي ضمان من أي نوع، صريحًا كان أم ضمنيًا. يجب أن يتحمل المستخدمون المسؤولية الكاملة عن استخدامهم لأي من المنتجات.

تم وضع ترخيص البرنامج والضمان المحدود للمنتج المرافق في حزمة المعلومات التي يتم شحنها مع المنتج والتي تم تضمينها هنا من خلال هذه الإشارة. إذا لم تتمكن من تحديد موقع ترخيص البرنامج أو الضمان المحدود، فاتصل بممثل CISCO لديك للحصول على نسخة.

المعلومات التالية خاصة بالامتثال لقواعد لجنة الاتصالات الفيدرالية (FCC) للأجهزة من الفئة أ: تم اختبار هذا الجهاز ووجد أنه يمتثل للحدود المطبقة على الأجهزة الرقمية من الفئة أ، وفقًا للجزء 15 من قواعد لجنة الاتصالات الفيدرالية. تم تصميم هذه الحدود لتوفير حماية معقولة ضد التداخل الضار عند تشغيل الجهاز في بيئة تجارية. يصدر هذا الجهاز طاقة التردد اللاسلكي ويستخدمها ويطلقها، وإذا لم يتم تركيبه واستخدامه وفقًا لدليل الإرشادات، فقد يتسبب ذلك في حدوث تداخل ضار مع الاتصالات اللاسلكية. من المحتمل أن يتسبب تشغيل هذا الجهاز في منطقة سكنية في حدوث تداخل ضار، وفي هذه الحالة سيُطلب من المستخدمين تصحيح التداخل على نفقتهم الخاصة.

المعلومات التالية خاصة بالامتثال لقواعد لجنة الاتصالات الفيدرالية (FCC) للأجهزة من الفئة ب: تم اختبار هذا الجهاز ووجد أنه يمتثل للحدود المطبقة على الأجهزة الرقمية من الفئة ب، وفقًا للجزء 15 من قواعد لجنة الاتصالات الفيدرالية. وتم وضع هذه الحدود لتوفير حماية معقولة تجاه التداخل الضار عند التركيب في منطقة سكنية. يصدر هذا الجهاز طاقة التردد اللاسلكي ويستخدمها ويطلقها، وإذا لم يتم تركيبه واستخدامه وفقًا للإرشادات، فقد يتسبب ذلك في حدوث تداخل ضار مع الاتصالات اللاسلكية. وبالرغم من ذلك، ليس هناك ضمان لعدم حدوث هذا التداخل في تثبيت معين. إذا تسبب الجهاز في حدوث تداخل في استقبال الراديو أو التلفزيون، والذي يمكن تحديده عن طريق إيقاف تشغيل الجهاز وتشغيله، فيوصى بأن يحاول المستخدمين تصحيح التداخل باتباع إجراء واحد أو أكثر من الإجراءات التالية:

- أعد توجيه هوائي الاستقبال أو غير موقعه.
- قم بزيادة المساحة الفاصلة بين الجهاز وجهاز الاستقبال.
- قم بتوصيل الجهاز بمأخذ في دائرة مختلفة عن تلك التي يتصل بها جهاز الاستقبال.
- استشر الموزع أو فني راديو أو تلفزيون خبير للحصول على المساعدة.

قد يؤدي إجراء تعديلات على هذا المنتج من دون تصريح من شركة Cisco إلى إبطال موافقة لجنة الاتصالات الفيدرالية (FCC) وإلغاء حقك في تشغيل المنتج.

يعد تنفيذ Cisco لضغط عنوان TCP عبارة عن مواءمة لبرنامج تم تطويره بواسطة جامعة كاليفورنيا، في بيركلي (UCB) كجزء من نسخة المجال العام الخاص بجامعة UCB لنظام التشغيل UNIX. جميع الحقوق محفوظة. حقوق الطبع والنشر © لعام 1981، أعضاء مجلس جامعة كاليفورنيا.

بصرف النظر عن أي ضمان آخر وارد هنا، يتم توفير جميع ملفات المستندات والبرامج الخاصة بهؤلاء الموردين "كما هي" مع جميع الأخطاء. تخلي شركة CISCO والموردون المذكورون أعلاه مسؤوليتهم عن جميع الضمانات، الصريحة أو الضمنية، بما في ذلك، على سبيل المثال لا الحصر، الضمانات المتعلقة بالقابلية للتسويق، والملاءمة لغرض معين، وعدم الانتهاك أو الناشئة عن سير التعاملات أو الاستخدام أو الممارسة التجارية.

لا تتحمل شركة CISCO أو موردوها بأي حال من الأحوال المسؤولية عن أي أضرار غير مباشرة أو خاصة أو تبعية أو عرضية، بما في ذلك، على سبيل المثال لا الحصر، الأرباح المفقودة أو الخسائر أو الأضرار التي تلحق بالبيانات الناشئة عن الاستخدام أو عدم القدرة على استخدام هذا الدليل، حتى إذا تم إخطار شركة CISCO أو موردييها بإمكانية حدوث مثل هذه الأضرار.

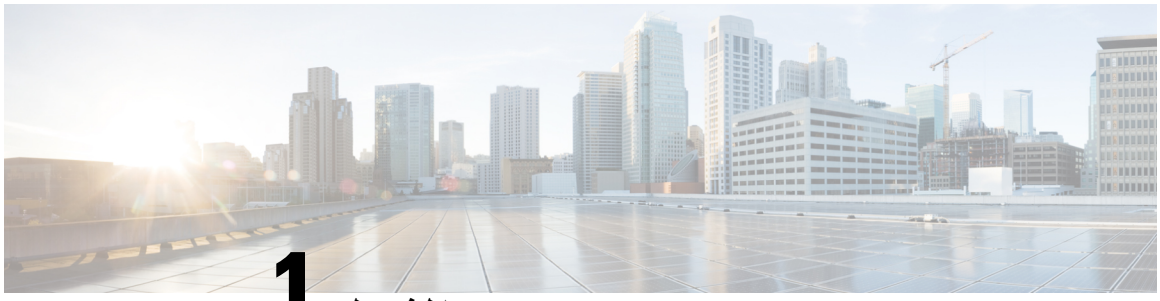
لا يُقصد من عناوين بروتوكول الإنترنت (IP) وأرقام الهواتف المستخدمة في هذا المستند أن تكون عناوين وأرقام هواتف فعلية. يتم عرض أي أمثلة ومخرجات عرض الأمر ومخططات تصميم الشبكة والأشكال الأخرى المضمنة في المستند لأغراض توضيحية فقط. أي استخدام لعناوين IP فعلية أو أرقام الهواتف في المحتوى التوضيحي هو غير مقصود ومن قبيل الصدفة.

تعتبر جميع النسخ المطبوعة والنسخ الإلكترونية المكررة من هذا المستند غير خاضعة للرقابة. اطلع على النسخة الحالية عبر الإنترنت للحصول على أحدث نسخة.

يوجد لدى Cisco أكثر من 200 مكتب في جميع أنحاء العالم. توجد قائمة بالعناوين وأرقام الهواتف على موقع الويب الخاص بشركة Cisco على الارتباط www.cisco.com/go/offices.

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

المحتويات



الفصل 1

المعلومات الجديدة والمتغيرة

معلومات جديدة ومتغيرة عن الإصدار 14.2(1) الخاص بالبرامج الثابتة

المعلومات التالية هي جديدة أو متغيرة عن الإصدار 14.2(1) الخاص بالبرامج الثابتة.

الميزة	الجديدة أو المتغيرة
دعم لـ SIP OAuth على SRST	تحسينات أمان شبكة هاتفك, في الصفحة 70

معلومات جديدة ومتغيرة عن الإصدار 14.1(1) الخاص بالبرامج الثابتة

المعلومات التالية هي جديدة أو متغيرة عن الإصدار 14.1(1) الخاص بالبرامج الثابتة.

الميزة	الجديدة أو المتغيرة
SIP OAuth لدعم TFTP الخاص بالوكيل	تحسينات أمان شبكة هاتفك, في الصفحة 70
ترحيل الهاتف بدون تحميل انتقالي	ترحيل هاتفك إلى هاتف ذو أنظمة متعددة, في الصفحة 89

معلومات جديدة ومتغيرة للإصدار 14.0(1) الخاص بالبرنامج الثابت

الجدول *1*: معلومات جديدة ومتغيرة

الميزة	الجديدة أو المتغيرة
تحسين مراقبة تعليق المكالمات	التكوين الخاص بالمنتج, في الصفحة 93
تحسينات SIP OAuth	تحسينات أمان شبكة هاتفك, في الصفحة 70
تحسينات OAuth لـ MRA	تقنية الوصول عن بعد ومن الأجهزة المتنقلة من خلال الخادم Expressway, في الصفحة 112
تحسينات واجهة المستخدم	هتفية الموقع البعيد المتين, في الصفحة 61

اعتبارًا من إصدار البرنامج الثابت 14.0، تدعم الهواتف DTLS 1.2. يتطلب DTLS 1.2 الإصدار Cisco Adaptive Security Appliance (ASA) 9.10 أو الأحدث. يمكنك تكوين الحد الأدنى من إصدار DTLS لاتصال VPN في ASA. للحصول على مزيد من المعلومات، راجع دليل تكوين كتاب *SDM B: Cisco ASA Series VPN ASDM* في https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

معلومات جديدة ومتغيرة للإصدار 12.8(1) الخاص بالبرنامج الثابت

المعلومات التالية جديدة أو تم تغييرها للإصدار 12.8(1) الخاص بالبرنامج الثابت.

الميزة	المحتوي الجديد أو المتغير
ترحيل بيانات الهاتف	تغيير طراز الهاتف الخاص بالمستخدم, في الصفحة 51
إضافة معلومات إضافية عن حقل الوصول إلى الويب	التكوين الخاص بالمنتج, في الصفحة 93

المعلومات الجديدة والمتغيرة للإصدار 12.7(1) الخاص بالبرنامج الثابت

لا توجد تحديثات أدلة إدارية مطلوبة لإصدار البرنامج الثابت 12.7(1).

معلومات جديدة ومتغيرة للإصدار 12.6(1) الخاص بالبرنامج الثابت

لا توجد تحديثات أدلة إدارية مطلوبة لإصدار البرنامج الثابت 12.6(1).

معلومات جديدة ومتغيرة عن الإصدار SR3(1)12.5 الخاص بالبرنامج الثابت

تم تحديث جميع المراجع الواردة في وثائق Cisco Unified Communications Manager لتدعم جميع إصدارات Cisco Unified Communications Manager.

الجدول 2: مراجعات دليل إدارة *Cisco IP Phone 8832* للإصدار *SR3(1)12.5* الخاص بالبرنامج الثابت

مراجعة	قسم تم تحديثه
الدعم لميزات إلحاق رمز التنشيط والوصول البعيد وRemote Access	إعداد رمز التنشيط والوصول عبر الأجهزة المحمولة وعن بُعد, في الصفحة 28
دعم استخدام أداة الإبلاغ عن المشكلات من Cisco Unified Communications Manager.	إنشاء تقرير بمشكلات الهاتف من Cisco Unified Communications Manager, في الصفحة 156

معلومات جديدة ومتغيرة عن الإصدار SR2(1)12.5 الخاص بالبرنامج الثابت

لا توجد تحديثات أدلة إدارية مطلوبة لإصدار البرنامج الثابت SR2(1)12.5.

يحل إصدار البرنامج الثابت SR2(1)12.5 محل إصدار البرنامج الثابت 12.5(1) والبرنامج الثابت SR1(1)12.5. تم تأجيل إصدار البرنامج الثابت 12.5(1) وإصدار البرنامج الثابت SR1(1)12.5 لصالح إصدار البرنامج الثابت SR2(1)12.5.

معلومات جديدة ومتغيرة عن الإصدار SR1(1)12.5 الخاص بالبرامج الثابتة

يدرج الجدول التالي التغييرات في دليل إدارة هاتف مؤتمر *Cisco IP 8832* لـ *Cisco Unified Communications Manager* لدعم إصدار البرنامج الثابت SR1(1)12.5.

الجدول 3: مراجعات دليل "إدارة *Cisco IP 8832*" للإصدار *SR1(1)12.5* للبرامج الثابتة.

مراجعة	القسم الجديد أو المحدّث
الدعم للحصول على منحنى إهليلجي	ميزات الأمان المدعومة, في الصفحة 71

معلومات جديدة ومتغيرة عن الإصدار 12.5(1) الخاص بالبرامج الثابتة

يدرج الجدول التالي التغييرات في دليل إدارة هاتف مؤتمر *Cisco IP 8832* لـ *Cisco Unified Communications Manager* لدعم إصدار البرنامج الثابت 12.5(1).

الجدول 4: مراجعات دليل "إدارة *Cisco IP 8832*" لإصدار البرنامج الثابت *12.5(1)*.

مراجعة	القسم الجديد أو المحدّث
الدعم لصفحة الهمس على Cisco Unified Communications Manager Express	تفاعل Cisco Unified Communications Manager Express, في الصفحة 22
الدعم لتشفيرات تعطيل TLS	التكوين الخاص بالمنتج, في الصفحة 93
دعم طلب Enbloc لتحسين T.302 لمؤقت الأرقام البينية.	التكوين الخاص بالمنتج, في الصفحة 93

معلومات جديدة ومتغيرة عن الإصدار 12.1(1) الخاص بالبرامج الثابتة

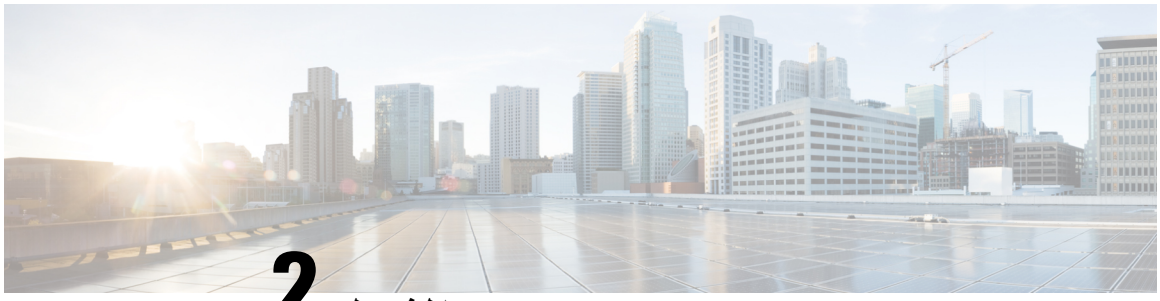
يصف الجدول التالي التغييرات في دليل إدارة هاتف مؤتمر *Cisco IP 8832* لـ *Cisco Unified Communications Manager* لدعم إصدار البرنامج الثابت 12.1(1).

مراجعة	القسم الجديد أو المحدّث
دعم حاقن PoE لهاتف مؤتمر Cisco IP 8832	• متطلبات الطاقة في الهاتف, في الصفحة 18 • طرق توفير هاتف المؤتمر بالطاقة, في الصفحة 32 • تثبيت هاتف المؤتمر, في الصفحة 31
دعم الميكروفونات اللاسلكية	• هاتف مؤتمر Cisco IP 8832, في الصفحة 9 • ميكروفون التوسيع اللاسلكي (8832 فقط), في الصفحة 12 • تثبيت ميكروفونات التوسيع اللاسلكية, في الصفحة 35 • تثبيت حامل شحن الميكروفون اللاسلكي, في الصفحة 36
دعم السلسلة الخطية	• هاتف مؤتمر Cisco IP 8832, في الصفحة 9 • وضع سلسلتين, في الصفحة 30 • تثبيت هاتف المؤتمر في وضع Daisy Chain, في الصفحة 36 • لا يعمل الهاتف الأول في وضع Daisy Chain, في الصفحة 155
دعم حاقن إيثرنت غير PoE لهاتف مؤتمر Cisco IP 8832	• تثبيت هاتف المؤتمر, في الصفحة 31 • طرق توفير هاتف المؤتمر بالطاقة, في الصفحة 32
دعم لشبكة Wi-Fi	• تثبيت هاتف المؤتمر, في الصفحة 31 • طرق توفير هاتف المؤتمر بالطاقة, في الصفحة 32 • تعيين حقل اسم المجال, في الصفحة 44 • تمكين شبكة LAN اللاسلكية من الهاتف, في الصفحة 45 • إعداد شبكة LAN اللاسلكية باستخدام Cisco Unified Communications Manager, في الصفحة 45 • إعداد الشبكة المحلية اللاسلكية من الهاتف, في الصفحة 46 • تعيين عدد محاولات مصادقة WLAN, في الصفحة 47 • تمكين وضع مطالبة الشبكة المحلية اللاسلكية, في الصفحة 48 • إعداد ملف تعريف Wi-Fi باستخدام Cisco Unified Communications Manager, في الصفحة 48 • إعداد مجموعة Wi-Fi باستخدام Cisco Unified Communications Manager, في الصفحة 50

مراجعة	القسم الجديد أو المحدّث
دعم Remote Access ومن الأجهزة المتنقلة من خلال Expressway	• تقنية الوصول عن بعد ومن الأجهزة المتنقلة من خلال الخادم Expressway, في الصفحة 112 • سيناريوهات النشر, في الصفحة 113 • استمرار تسجيل الدخول إلى Expressway ببيانات اعتماد المستخدم, في الصفحة 113
دعم لتمكين أو تعطيل TLS 1.2 للوصول إلى خادم الويب.	التكوين الخاص بالمنتج, في الصفحة 93
دعم لبرنامج الترميز الصوتي G722.2 AMR-WB	• هاتف مؤتمر Cisco IP 8832, في الصفحة 9 • حقول إحصاءات المكالمات, في الصفحة 130

الجزء I

نبذة عن هاتف مؤتمر Cisco IP



الفصل 2

أجهزة هاتف مؤتمر Cisco IP

هاتف مؤتمر Cisco IP 8832

يقوم هاتف Cisco IP Phone Conference Phone 8832 وNR8832 بتحسين الاتصالات التي تركز على الأشخاص. إنه يجمع بين الأداء الصوتي عالي الدقة وتغطية 360 درجة لغرف المؤتمرات المتوسطة إلى الكبيرة والمكاتب التنفيذية. ويوفر تجربة صوت audiophile مع مكبر صوت لاسلكي ثنائي الاتجاهات وذي ازدواج كامل وفائق السرعة (G.722). هذا الهاتف هو حل بسيط يفي بالتحديات الغرف الأكثر تنوعًا.

الشكل 1: هاتف مؤتمر *Cisco IP 8832*

يشتمل هاتف المؤتمر على ميكروفونات حساسة بتغطية 360 درجة. تتيح هذه التغطية للمستخدمين إمكانية التحدث بصوت عادي والاستماع إليك بوضوح من على مسافة تصل إلى 10 أقدام (3 م). كما يشتمل الهاتف على تقنية تقاوم التدخل من الهواتف المحمولة والأجهزة اللاسلكية الأخرى، مما يضمن تقديم اتصالات واضحة دون انحرافات. يشتمل الهاتف على شاشة ملونة وأزرار المفاتيح المرنة للوصول إلى وظائف المستخدم. مع الوحدة الأساسية وحدها، يوفر الهاتف تغطية لغرفة مساحتها 20 × 20 قدمًا (6.1 × 6.1 م) وما يصل إلى 10 أشخاص.

ميكروفونا التوسيع السلكيان متوفران للاستخدام في الهاتف. يوفر وضع ميكروفونات التوسيع بعيدًا عن الوحدة الأساسية تغطية أكبر في غرف الاجتماعات الكبيرة. مع الوحدة الأساسية وميكروفونات التوسيع السلكية، يوفر هاتف المؤتمر تغطية لغرفة مساحتها 20 × 34 قدمًا (6.1 × 10 م) وما يصل إلى 22 أشخاص.

كما يدعم الهاتف مجموعة اختيارية من ميكروفوني توسيع لاسلكيين. مع الوحدة الأساسية وميكروفونات التوسيع اللاسلكية، يوفر هاتف المؤتمر تغطية لغرفة مساحتها 20 40 x قدمًا (6.1 12.2 x م) وما يصل إلى 26 شخصًا. لتغطية غرفة مسساحتها 20 40 x قدمًا، ننصحك بوضع كل ميكروفون في مسافة أقصاها 10 أقدام من القاعدة.

يمكنك توصيل وحدتين أساسيتين لزيادة تغطية الخاصة بغرفة. يتطلب هذا التكوين مجموعة السلاسل الخطية الاختيارية ويمكنه أن يدعم اثنين من ميكروفونات التوسيع (سلكية أو لاسلكية، ولكن ليس مجموعة مختلطة منهما). إذا كنت تستخدم ميكروفونات سلكية مع مجموعة السلاسل الخطية، يوفر التكوين تغطية لغرفة تصل مساحتها إلى 20 × 50 قدمًا (6.1 × 15.2 م) وتستوعب ما يصل إلى 38 شخصًا. إذا كنت تستخدم ميكروفونات لاسلكية مع مجموعة السلاسل الخطية، يوفر التكوين تغطية لغرفة تصل مساحتها إلى 20 × 57 قدمًا (6.1 × 17.4 م) وتستوعب ما يصل إلى 42 شخصًا.

لا يدعم هاتف مؤتمر Cisco IP 8832NR الإصدار (اللاسلكي) Wi-Fi أو ميكروفونات التوسيع اللاسلكية أو Bluetooth.

مثل الأجهزة الأخرى، يجب تكوين هاتف Cisco IP وإدارته. تُرمِّز هذه الهواتف وتفك الرموز التالية:

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

تنبيه قد يتسبب استخدام هاتف خلوي أو جوال أو هاتف GSM، أو جهاز لاسلكي يعمل باتجاهين بالقرب من هاتف Cisco IP في حدوث تداخل. للحصول على مزيد من المعلومات، راجع وثائق الجهة المصنعة للجهاز المتداخل.

توفر هواتف Cisco IP وظائف الهاتفية التقليدية، مثل إعادة توجيه المكالمات والنقل وإعادة الطلب والطلب السريع ومكالمات المؤتمر والوصول إلى نظام المراسلة الصوتية. كما توفر هواتف Cisco IP مجموعة متنوعة من الميزات الأخرى.

وفيما يتعلق بأجهزة الشبكة الأخرى، يجب تكوين هواتف Cisco IP لإعدادها للوصول إلى Cisco Unified Communications Manager وبقية شبكة IP. باستخدام DHCP، تتوفر لديك إعدادات أقل للتكوين على الهاتف. ولكن إذا كانت شبكتك تحتاج إليه، فإنه يمكنك تكوين المعلومات يدويًا مثل: عنوان IP، وخادم TFTP، ومعلومات الشبكة الفرعية.

يمكن أن تتفاعل هواتف Cisco IP مع الخدمات والأجهزة الأخرى على شبكة IP لتوفير وظائف محسنة. على سبيل المثال، يمكنك دمج Cisco Unified Communications Manager مع الدليل القياسي للبروتوكول الخفيف لتغيير بيانات الدليل 3 (LDAP3) الخاص بالشركة لتمكين المستخدمين من البحث عن معلومات اتصال زميل العمل مباشرة من هواتف IP الخاصة بهم. يمكنك أيضًا استخدام XML لتمكين المستخدمين من الوصول إلى معلومات مثل الطقس والأسهم وحكمة اليوم والمعلومات الأخرى المستندة إلى الويب.

وأخيرًا، ونظرًا لأن هاتف Cisco IP يعد جهاز شبكة، فإنه يمكنك الحصول على معلومات تفصيلية عن الحالة منه مباشرة. يمكن أن تساعدك هذه المعلومات في استكشاف وإصلاح أي مشكلات قد تواجه المستخدم أثناء استخدام هواتف IP. يمكنك أيضًا الحصول على إحصائيات حول مكالمة نشطة أو إصدارات البرامج الثابتة على الهاتف.

للتشغيل في شبكة هاتفية IP، يجب أن يتصل هاتف Cisco IP بجهاز شبكة، مثل مفتاح تحويل Cisco Catalyst. يجب أيضًا أن تسجّل هاتف Cisco IP من خلال نظام Cisco Unified Communications Manager قبل إرسال المكالمات واستقبالها.

أزرار هاتف مؤتمر Cisco IP 8832 والأجهزة التابعة له

يعرض الشكل التالي هاتف مؤتمر Cisco IP 8832.

الشكل *2*: أزرار هاتف مؤتمر *Cisco IP 8832* والميزات التابعة له

يصف الجدول التالي الأزرار الموجودة على هاتف مؤتمر Cisco IP 8832.

الجدول *5*: أزرار هاتف مؤتمر *Cisco IP 8832*

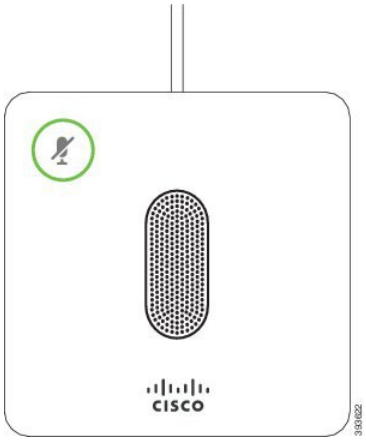
1	شريط LED	يشير إلى حالات المكالمات: • أخضر، ثابت - مكالمة نشطة • أخضر، يومض - مكالمة واردة • أخضر، نابض - مكالمة قيد الانتظار • أحمر، ثابت - مكالمة تم تجاهلها
2	منفذ ميكروفون التوسيع	يتم توصيل كبل ميكروفون التوسيع السلكي بالمنفذ.
3	شريط **كتم الصوت**	للتبديل بين تشغيل الميكروفون أو إيقاف تشغيله. عند قيامك بكتم صوت الميكروفون، يضيء شريط المؤشر الضوئي باللون الأحمر.
4	الأزرار الوظيفية	الوصول إلى المهام والخدمات.
5	شريط التنقل وزر **التحديد**	للتمرير عبر القوائم وتمييز العناصر وتحديد العنصر المميز.

6	زر **مستوى الصوت**	لضبط مستوى صوت مكبر صوت الهاتف (في وذع السماعة المرفوعة) ومستوى صوت الرنين (في وذع السماعة المغلقة). عند تغيير مستوى الصوت، يضيء شريط LED باللون الأبيض لإظهار تغيير مستوى الصوت.

ميكروفون التوسيع السلكي (8832 فقط)

تدعم هاتف Cisco IP Phone Conference Phone 8832 ميكروفوني توسيع سلكيين متوفرين في مجموعة مواد اختيارية. استخدم ميكروفونات التوسيع في غرف أكبر أو غرفة مزدحمة. للحصول على أفضل النتائج، نُوصي بوضع الميكروفونات بعيدًا عن الهاتف بمسافة تتراوح بين 3 أقدام (0.91 م) و7 أقدام (2.1 م).

الشكل 3: ميكروفون التوسيع السلكي



عند إجراء مكالمة، يُضيء شريط LED الخاص بميكروفون التوسيع والموجود حول زر **كتم الصوت** باللون الأخضر.

عند قيامك بكتم صوت الميكروفون، يضيء مصباح LED باللون الأحمر. عند الضغط على الزر **كتم الصوت**، يتم كتم صوت الهاتف وميكروفونات التوسيع.

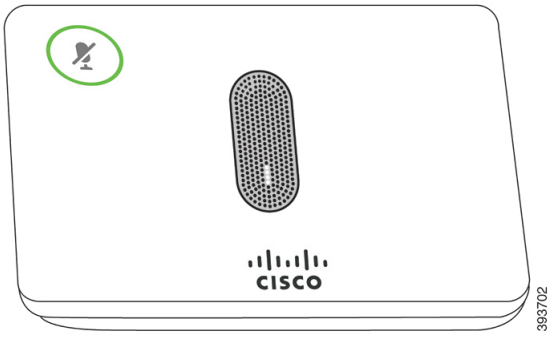
موضوعات ذات صلة

تثبيت ميكروفونات التوسيع السلكية, في الصفحة 34

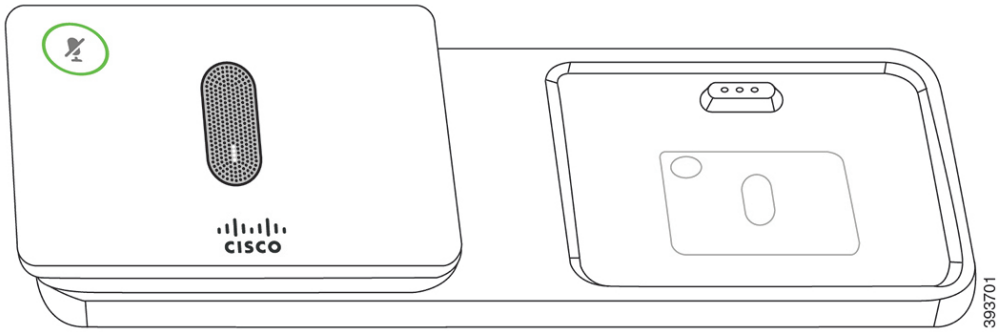
ميكروفون التوسيع اللاسلكي (8832 فقط)

تدعم هاتف Cisco IP Phone Conference Phone 8832 ميكروفوني توسيع سلكيين متوفرين بحامل شاحن في مجموعة مواد اختيارية. عندما يتم وضع الميكروفون اللاسلكي في الحامل الخاص به للشحن، يضيء مصباح LED الموجود بالحامل باللون الأبيض.

الشكل *4*: الميكروفون اللاسلكي



الشكل *5*: تم تثبيت الميكروفون اللاسلكي على حامل الشحن



عند إجراء مكالمة في هاتف المؤتمر، يُضيء شريط LED الخاص بميكروفون التوسيع والموجود حول زر **كتم الصوت** باللون الأخضر.

عندما يكون الميكروفون في وضع كتم الصوت، يضيء شريط LED باللون الأحمر. عند الضغط على الزر **كتم الصوت**، يتم كتم صوت الهاتف وميكروفونات التوسيع.

إذا تم توصيل الهاتف بهاتف ميكروفون لاسلكي (على سبيل المثال، الميكروفون اللاسلكي 1) وقمت بتوصيل الميكروفون اللاسلكي بشاحن، فإن الضغط على الزر الوظيفي **إظهار التفاصيل** يشير إلى مستوى الشحن لذلك الميكروفون.

عندما يتم توصيل الهاتف باستخدام ميكروفون لاسلكي وتقوم بتوصيل ميكروفون سلكي، فإنه يتم فصل الميكروفون اللاسلكي ويتم توصيل الهاتف باستخدام الميكروفون السلكي. يظهر إعلام على شاشة الهاتف يشير إلى أنه تم توصيل الميكروفون السلكي.

موضوعات ذات صلة

تثبيت ميكروفونات التوسيع اللاسلكية, في الصفحة 35
تثبيت حامل شحن الميكروفون اللاسلكي, في الصفحة 36

وثائق مرتبطة

استخدم الأقسام التالية للحصول على المعلومات المرتبطة.

وثائق هاتف مؤتمر Cisco IP 8832

ابحث عن الوثائق الخاصة بلغتك وطراز الهاتف ونظام التحكم في المكالمات في صفحة دعم المنتجات لـ Cisco IP Phone 7800 Series.

وثائق Cisco Unified Communications Manager

راجع *Cisco Unified Communications Manager* دليل الوثائق والمنشورات الأخرى الخاصة بإصدار Cisco Unified Communications Manager الذي لديك. انتقل من URL الوثائق التالي:

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

وثائق Cisco Unified Communications Manager Express

راجع المنشورات الخاصة بلغتك، وطراز الهاتف وإصدار Cisco Unified Communications Manager Express. انتقل من URL الوثائق التالي:

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

وثائق خدمة التعاون المستضافة من Cisco

راجع *Cisco Hosted Collaboration Solution* دليل الوثائق والمنشورات الأخرى الخاصة بإصدار Cisco Hosted Collaboration Solution الذي لديك. انتقل من عنوان URL التالي:

https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html

وثائق Cisco Business Edition 4000

راجع *Cisco Business Edition 4000* دليل الوثائق والمنشورات الأخرى الخاصة بإصدار Cisco Business Edition 4000 الذي لديك. انتقل من عنوان URL التالي:

https://www.cisco.com/c/en/us/support/unified-communications/business-edition-4000/tsd-products-support-series-home.html

الوثائق والدعم وإرشادات الأمان

للاطلاع على معلومات حول كيفية الحصول على الوثائق والدعم، وتوفير ملاحظات خاصة بالوثائق، ومراجعة إرشادات الأمان، والأسماء المستعارة الموصى بها، ووثائق Cisco العامة، راجع إصدار ما الجديد في وثائق منتجات *Cisco* الشهري، والذي يقدم أيضًا قائمة بكل وثائق Cisco الفنية الجديدة والتي تمت مراجعتها، من خلال:

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

اشترك في ما الجديد في وثائق منتجات *Cisco* باعتباره موجز Really Simple Syndication (RSS) وقم بتعيين المحتوى لكي يتم تسليمه مباشرة إلى سطح المكتب الخاص بك باستخدام أحد تطبيقات القراءة. تعتبر مواجز RSS خدمة مجانية وتوفر Cisco الدعم حاليًا للإصدار 2.0 من RSS.

نظرة عامة على أمان منتج Cisco

يحتوي هذا المنتج على ميزات تشفير ويخضع لقوانين الولايات المتحدة وقوانين البلد المحلية التي تحكم عمليات الاستيراد والتصدير والنقل والاستخدام. توصيل منتجات Cisco المشفرة لا يتضمن سلطة الطرف الآخر لاستيراد التشفير أو تصديره أو توزيعه أو استخدامه. يجب أن يمتثل المستوردون والمصدرون والموزعون والمستخدمون إلى قوانين الولايات المتحدة وقوانين البلد المحلية. استخدام هذا المنتج يعني موافقتك على الالتزام بالقوانين واللوائح السارية. في حالة عدم تمكنك من الالتزام بقوانين الولايات المتحدة والقوانين المحلية، أعد هذا المنتج فورًا.

يمكن العثور على معلومات إضافية بشأن لوائح الولايات المتحدة الخاصة بالتصدير على https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear.

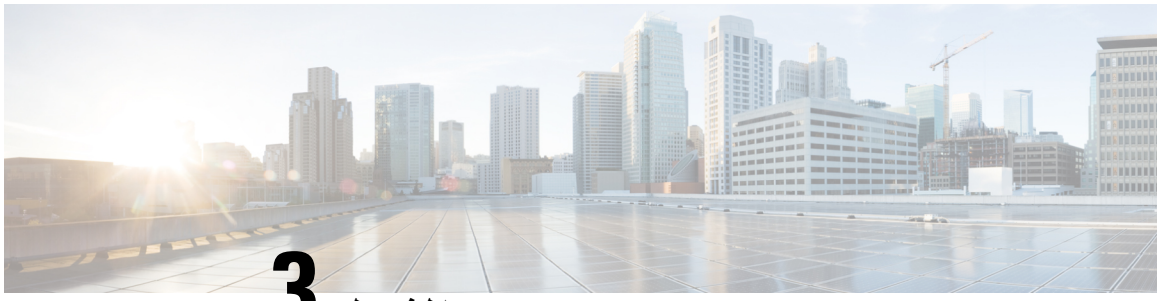
اختلافات المصطلحات

في هذا المستند، يشمل المصطلح هاتف *Cisco IP* هاتف مؤتمر Cisco IP 8832.

يُبرز الجدول التالي بعض اختلافات المصطلحات في دليل مستخدم سلسلة هواتف مؤتمر *Cisco IP 8832*، ودليل إدارة هاتف مؤتمر *Cisco IP 8832* لـ *Cisco Unified Communications Manager*، ووثائق Cisco Unified Communications Manager.

الجدول *6*: اختلافات المصطلحات

دليل المستخدم	دليل الإدارة
مؤشرات الرسائل	مؤشر انتظار الرسائل (MWI)
نظام البريد الصوتي	نظام المراسلة الصوتية



الفصل 3

التفاصيل الفنية

مواصفات البيئة التشغيلية والمادية

يعرض الجدول التالي مواصفات البيئة التشغيلية والمادية لهاتف المؤتمر.

الجدول 7: المواصفات التشغيلية والمادية

المواصفات	القيمة أو النطاق
درجة حرارة التشغيل	32 إلى 104 درجة فهرنهايت (0 إلى 40 درجة مئوية)
رطوبة التشغيل النسبية	10% إلى 90% (بدون تكاثف)
درجة حرارة التخزين	14 إلى 140 درجة فهرنهايت (–10 إلى 60 درجة مئوية)
الارتفاع	10.9 بوصة (278 مم)
العرض	10.9 بوصة (278 مم)
العمق	2.4 بوصة (61.3 مم)
الوزن	4.07 رطل (1852 جم)
الطاقة	الفئة 3 من IEEE PoE عبر حاقن PoE. الهاتف متوافق مع كلّ من شفرات مفتاح 802.3af عبر إيثرنت (LLDP-PoE). تشمل الخيارات الأخرى حاقن غير PoE Ethernet إذا لم تدعم مفاتيح LAN حاقن PoE.

المواصفات	القيمة أو النطاق
ميزات الحماية	التمهيد الآمن
كابلات	USB-C
متطلبات المسافة	تفترض مواصفات إيثرنت أن يبلغ الحد الأقصى لطول الكابل بين كل هاتف مؤتمر والم

لمزيد من المعلومات، راجع صفحة بيانات هاتف مؤتمر *Cisco IP 8832*: https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/datasheet-listing.html

متطلبات الطاقة في الهاتف

يمكن لـ هاتف Cisco IP Phone Conference Phone 8832 استخدام مصادر الطاقة التالية:

- نشر الطاقة عبر Ethernet (PoE) باستخدام حاقن PoE لهاتف مؤتمر Cisco IP 8832
- نشر غير PoE Ethernet باستخدام حاقن إيثرنت غير PoE لهاتف مؤتمر Cisco IP 8832
- نشر Wi-Fi باستخدام محول الطاقة 8832 لهاتف مؤتمر Cisco IP

الجدول 8: إرشادات خاصة بطاقة هاتف مؤتمر *Cisco IP*

نوع الطاقة	إرشادات
طاقة PoE — يتم توفيرها إما من خلال حاقن PoE لهاتف مؤتمر Cisco IP 8832 أو حاقن Ethernet لهاتف مؤتمر Cisco IP 8832 عبر كابل USB-C المقترن بالهاتف.	إذا كنت تستخدم إما حاقن PoE لهاتف مؤتمر Cisco IP 8832 أو حاقن Ethernet لهاتف مؤتمر Cisco IP 8832، فتأكد أن المفتاح يحتوي على موفر طاقة كنسخة احتياطية لضمان تشغيل الهاتف دون انقطاع. تأكد أن إصدار CatOS أو IOS الذي يعمل على مفتاح التحويل لديك يدعم نشر الهاتف المقصود. راجع وثائق مفتاح التحويل للتعرف على معلومات حول إصدار نظام التشغيل. عند تركيب هاتف يعمل بواسطة PoE، فقم بتوصيل الحاقن بشبكة LAN قبل قيامك بتوصيل كابل USB-C بالهاتف. عندما تقوم بإزالة هاتف يستخدم PoE، افصل كبل USB-C من الهاتف قبل إزالة الطاقة من المحول.
مصدر طاقة خارجي • نشر غير PoE Ethernet باستخدام حاقن إيثرنت غير PoE لهاتف مؤتمر Cisco IP 8832 • نشر Wi-Fi باستخدام محول الطاقة 8832 لهاتف مؤتمر Cisco IP • نشر غير PoE Ethernet باستخدام حاقن Ethernet لهاتف مؤتمر Cisco IP 8832 محول الطاقة 8832 لهواتف مؤتمر Cisco IP	عند تركيب هاتف يعمل بطاقة خارجية، قم بتوصيل الحاقن بمصدر الطاقة وإيثرنت قبل توصيل كابل USB-C بالهاتف. عندما تقوم بإزالة هاتف يستخدم طاقة خارجية، افصل كبل USB-C من الهاتف قبل إزالة الطاقة من المحول.

انقطاع التيار الكهربائي

يتطلب وصولك إلى خدمة الطوارئ عبر الهاتف أن يتصل الهاتف بالتيار الكهربائي. في حالة انقطاع التيار الكهربائي، تتوقف الخدمة أو طلب خدمة مكالمات الطوارئ عن العمل لحين وصول التيار الكهربائي. في حالة حدوث انقطاع أو عطل في التيار الكهربائي، قد تضطر إلى إعادة ضبط الجهاز أو إعادة تهيئته قبل أن تتمكن من استخدام الخدمة أو طلب خدمة مكالمات الطوارئ.

خفض الطاقة

يمكنك تقليل كمية الطاقة التي يستهلكها هاتف Cisco IP باستخدام وضع توفير الطاقة أو EnergyWise (توفير الطاقة الإضافي).

توفير الطاقة

في وضع توفير الطاقة، لا تعمل الإضاءة الخلفية الموجودة بالشاشة عند عدم استخدام الهاتف. يظل الهاتف في وضع توفير الطاقة للمدة المجدولة أو يضغط المستخدم على أي زر.

توفير الطاقة الإضافي (EnergyWise)

يدعم هاتف Cisco IP وضع Cisco EnergyWise (توفير الطاقة الإضافي). عند احتواء شبكتك على عنصر تحكم EnergyWise (EW) (على سبيل المثال، مفتاح تحويل Cisco ممكنًا عليه ميزة EnergyWise)، فإنه يمكنك تكوين هذه الهواتف لتسكن (تتوقف عن التشغيل) وتنتبه (تعمل) بناءً على جدول محدد لتقليل استهلاك الطاقة.

قم بإعداد كل هاتف لتمكين إعدادات EnergyWise أو تعطيلها. إذا كان EnergyWise ممكنًا، فقم بتكوين وقت محدد للسكون والانتباه، بالإضافة إلى معلمات أخرى. يتم إرسال هذه المعلمات إلى الهاتف كجزء من ملف XML الخاص بتكوين الهاتف.

موضوعات ذات صلة

جدول توفير الطاقة لهاتف Cisco IP, في الصفحة 103
جدولة EnergyWise على هاتف Cisco IP, في الصفحة 105

بروتوكولات الشبكة

تدعم هاتف Cisco IP Phone Conference Phone 8832 العديد من بروتوكولات شبكة Cisco القياسية على مستوى الصناعة والتي تعد ضرورية للاتصالات الصوتية. ويقدم الجدول التالي نظرة عامة عن بروتوكولات الشبكة التي تدعمها الهواتف.

الجدول *9*: بروتوكولات الشبكة المدعومة على هاتف مؤتمر *Cisco IP*

بروتوكول الشبكة	الغرض	ملاحظات الاستخدام
بروتوكول تمهيد تشغيل الجهاز (BootP)	يعمل بروتوكول BootP على تمكين أحد أجهزة الشبكة، مثل الهاتف، من اكتشاف معلومات بدء التشغيل المحددة، مثل عنوان IP.	—
بروتوكول استكشاف Cisco (واختصاره CDP)	يعد CDP بروتوكولاً يختص باكتشاف الأجهزة التي تعمل على جميع المعدات المصنعة بواسطة Cisco. يمكن أن يستخدم الجهاز بروتوكول CDP ليعلن عن وجوده للأجهزة الأخرى وليتلقى معلومات حول الأجهزة الأخرى في الشبكة.	يستخدم الهاتف بروتوكول CDP لنقل المعلومات مثل معرف LAN تحويل Cisco Catalyst.
بروتوكول تهيئة الاستضافة الديناميكية (DHCP)	يخصص بروتوكول DHCP عنوان IP ويعينه بشكل ديناميكي إلى أجهزة الشبكة. يتيح لك بروتوكول DHCP إمكانية توصيل هاتف IP بالشبكة وتشغيل الهاتف دون الحاجة إلى تعيين عنوان IP يدويًا أو تكوين معلمات الشبكة الإضافية.	يتم تمكين بروتوكول DHCP افتراضيًا. في حالة تعطيله، يجب أن نوصي باستخدام خيار بروتوكول DHCP 150 المخصص. بهذه ال الإضافية المدعومة، راجع الوثائق الخاصة بإصدار ns Manager **ملاحظة** إذا تعذر عليك استخدام الخيار 150، فاستخدم خيار

بروتوكول الشبكة	الغرض	ملاحظات الاستخدام
بروتوكول نقل النص التشعبي (HTTP)	يعد HTTP البروتوكول القياسي لنقل المعلومات والمستندات عبر الإنترنت والويب.	تستخدم الهواتف HTTP لخدمات XML والتوفير والترقية و
بروتوكول نقل النص التشعبي الآمن (HTTPS)	يعد بروتوكول نقل النص التشعبي الآمن (HTTPS) مزيجًا من بروتوكول نقل النص التشعبي وبروتوكول SSL/TLS لتوفير التشفير والتعريف الآمن للخوادم.	تشتمل تطبيقات الويب المتوفر لها دعم كلٍّ HTTP وHTTPS يتم عرض أيقونة قفل للمستخدم إذا كان الاتصال بالخدمة يتم ع
IEEE 802.1X	يحدد معيار IEEE 802.1X التحكم في الوصول القائم على خادم—العميل وبروتوكول المصادقة الذي يقيد اتصال العملاء غير المصادقين بشبكة LAN من خلال منافذ يمكن الوصول إليها بشكل عام. وحتى تتم مصادقة العميل، يسمح التحكم في وصول X802.1 فقط بحركة بروتوكول المصادقة القابل للتوسعة عبر شبكة LAN (EAPOL) من خلال المنفذ الذي يتصل به العميل. بعد نجاح المصادقة، يمكن أن تمر الحركة العادية عبر المنفذ.	يُنفذ الهاتف معيار IEEE 802.1X من خلال دعم طرق المص عند تمكين مصادقة X802.1 على الهاتف، يجب أن تعطل AN
بروتوكول الإنترنت (IP)	يعد IP بروتوكول مراسلة يعالج الحزم ويرسلها عبر الشبكة.	للاتصال بـ IP، يجب أن تمتلك أجهزة الشبكة عنوان IP معينًا و يتم تعيين تعريفات عناوين IP والشبكات الفرعية والبوابات تلقا بروتوكول DHCP، فيجب أن تعين هذه الخصائص يدويًا إلى تدعم الهواتف عنوان IPv6. للحصول على مزيد من المعلوم
بروتوكول استكشاف طبقة الارتباط (LLDP)	يعد LLDP بروتوكولاً موحدًا لاستكشاف الشبكة (على غرار CDP) وهو معتمد على بعض أجهزة Cisco والجهات الخارجية.	يدعم الهاتف بروتوكول LLDP على منفذ PC.
بروتوكول استكشاف طبقة الارتباط — أجهزة نقطة نهاية الوسائط (LLDP—MED)	يعد LLDP—MED امتدادًا لمعيار LLDP—MED تم تطويره للمنتجات الصوتية	يدعم الهاتف LLDP—MED على منفذ SW لنقل معلومات • تكوين VLAN للصوت • اكتشاف الجهاز • إدارة الطاقة • إدارة المخزون لمزيد من المعلومات حول دعم LLDP—MED، راجع المس nologies_white_paper0900aecd804cd46d.shtml
بروتوكول النقل في الوقت الحقيقي (RTP)	يعد RTP بروتوكولاً قياسيًا لنقل البيانات في الوقت الحقيقي، مثل الصوت والفيديو التفاعليين، عبر شبكات البيانات.	تستخدم الهواتف بروتوكول RTP لإرسال حركة مرور الصو
بروتوكول التحكم في الوقت الحقيقي (RTCP)	يعمل بروتوكول RTCP بالتزامن مع RTP لتوفير بيانات QoS (مثل التشويش وزمن الوصول وتأخر وقت الجولة) على عمليات دفق RTP.	يتم تمكين بروتوكول RTCP افتراضيًا.
بروتوكول وصف جلسة العمل (SDP)	بروتوكول SDP هو جزء من بروتوكول SIP الذي يحدد المعلمات المتاحة أثناء الاتصال بين نقطتي نهاية. يتم إنشاء المؤتمرات مع الاقتصار على استخدام إمكانيات SDP التي تدعم جميع نقاط النهاية في المؤتمر.	يتم تهيئة إمكانيات SDP، مثل أنواع الترميز والكشف عن MF Communications Manager أو بتشغيل بوابة الوسائط. ق
بروتوكول بدء جلسة العمل (SIP)	يعد SIP معيار قوة واجب الهندسة بالإنترنت (IETF) للمؤتمرات متعددة الوسائط عبر IP. يعد SIP بروتوكول التحكم في طبقات التطبيق المستندة إلى ASCII (معرف في الجزء RFC 3261) يمكن استخدامه لتأسيس المكالمات، بين طرفي نهاية أو أكثر، والحفاظ عليها وإنهاؤها.	تم تصميم بروتوكول SIP، مثل بروتوكولات VoIP الأخرى، معلومات المكالمة عبر حدود الشبكة. توفر إدارة الجلسة القدرة

بروتوكول الشبكة	الغرض	ملاحظات الاستخدام
بروتوكول النقل الآمن في الوقت الحقيقي (SRTP)	يعد بروتوكول SRTP امتدادًا لملف تعريف الصوت/الفيديو في بروتوكول الوقت الحقيقي (RTP)، ويضمن تكامل حزم RTP وبروتوكول التحكم في الوقت الحقيقي (RTCP) التي توفر المصادقة والتكامل والتشفير لحزم الوسائط بين نقطتي نهاية.	تستخدم الهواتف بروتوكول SRTP لتشفير الوسائط.
بروتوكول التحكم في الإرسال (TCP)	يُعد TCP بروتوكول نقل مهيأ للاتصال.	تستخدم الهواتف بروتوكول TCP للاتصال بـ cations Manager
أمان طبقة النقل (TLS)	يعد TLS بروتوكولاً قياسيًا لتأمين الاتصالات ومصادقتها.	عند تطبيق الأمان، تستخدم الهواتف بروتوكول TLS عند التسجيل المعلومات، راجع الوثائق الخاصة بإصدار nications Manager
بروتوكول نقل الملفات المبسط (TFTP)	يسمح بروتوكول TFTP بنقل الملفات عبر الشبكة. على الهاتف، يتيح بروتوكول TFTP لك إمكانية الحصول على ملف تكوين خاص بنوع الهاتف.	يتطلب بروتوكول TFTP وجود خادم TFTP في شبكتك، يمكن تح قبل خادم DHCP، فيجب أن تُعين عنوان IP الخاص بخادم IP يدو للحصول على مزيد من المعلومات، راجع الوثائق الخاصة بإصدا
بروتوكول مخطط بيانات المستخدم (UDP)	يعد UDP بروتوكول مراسلة بدون اتصال لتوصيل حزم البيانات.	يتم استخدام UDP فقط لعمليات دفق RTP. لا تدعم عملية إرسال إ

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14

تفاعل Cisco Unified Communications Manager

يُعد Cisco Unified Communications Manager نظام معالجة مكالمات مفتوحًا قياسيًا في الصناعة. يقوم برنامج Cisco Unified Communications Manager بإعداد المكالمات وتقسيمها بين الهواتف، مما يعمل على دمج وظائف PBX التقليدية بشبكة IP للشركة. يدير Cisco Unified Communications Manager مكونات نظام الاتصالات الهاتفية، مثل الهواتف وبوابات الوصول والموارد اللازمة لميزات، مثل مؤتمرات المكالمات وتخطيط المسار. كما توفر إدارة Cisco Unified Communications Manager:

- البرامج الثابتة للهواتف
- قائمة الثقة بالشهادات (CTL) وملفات "قائمة الثقة لتحديد الهويات" (ITL) باستخدام خدمات TFTP وHTTP
- تسجيل الهاتف
- الحجز الهاتفي، وذلك لكي تستمر الجلسة الوسائطية إذا تم فقدان التأشير بين "مدير الاتصالات" وأحد الهواتف.

للحصول على معلومات حول تكوين Cisco Unified Communications Manager للعمل مع الهواتف الموضحة في هذا الفصل، راجع وثائق إصدار Cisco Unified Communications Manager الخاص بك.

ملاحظة إذا لم يظهر طراز الهاتف الذي تريد تكوينه في القائمة المنسدلة "نوع الهاتف" في إدارة Cisco Unified Communications Manager، فقم بتثبيت أحدث حزمة جهاز لإصدارك من Cisco Unified Communications Manager من Cisco.com.

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14

تفاعل Cisco Unified Communications Manager Express

عندما يعمل هاتفك مع Cisco Unified Communications Manager Express (Unified CME)، يجب أن ينتقل إلى وضع CME.

عند استدعاء المستخدم لميزة المؤتمر، تتيح العلامة للهاتف استخدام جسر مؤتمر أجهزة شبكة أو محلية.

لا تدعم الهواتف الإجراءات التالية:

- النقل — مدعوم في سيناريو تحويل المكالمات المتصلة.
- المؤتمر — مدعوم فقط في سيناريو تحويل المكالمات المتصلة.
- الانضمام — مدعوم باستخدام زر المؤتمر أو وصول hookflash.
- التعليق — مدعوم باستخدام زر الانتظار.
- المداخلة والدمج — غير مدعوم.
- تحويل مباشر — غير مدعوم.
- التحديد — غير مدعوم.

لا يمكن للمستخدمين إنشاء مكالمات المؤتمر وتحويلها عبر الخطوط المختلفة.

يدعم CME الموحد مكالمات الاتصال الداخلي، والمعروفة أيضًا باسم صفحة الهمس. ولكن تم رفض الصفحة عبر الهاتف أثناء المكالمات.

تفاعل نظام المراسلة الصوتية

يتيح Cisco Unified Communications Manager الذي يتكامل مع أنظمة الرسائل الصوتية المختلفة، بما في ذلك نظام الرسائل الصوتية Cisco Unity Connection. لأنه يمكن أن يتكامل مع مجموعة متنوعة من الأنظمة، يجب أن تمد المستخدمين بمزيد من المعلومات حول كيفية استخدام النظام الخاص بك.

لتمكين قدرة المستخدم على التحويل إلى البريد الصوتي، قم بإعداد نمط طلب *xxxxx وتهيئته كخيار "إعادة توجيه الكل إلى البريد الصوتي". للحصول على مزيد من المعلومات، راجع وثائق Cisco Unified Communications Manager.

قدم المعلومات التالية لكل مستخدم:

- كيفية الوصول إلى حساب نظام الرسائل الصوتية.

  تأكد من استخدامك Cisco Unified Communications Manager لتهيئة زر الرسائل على هواتف Cisco IP .

- كلمة المرور الأولية للوصول إلى نظام الرسائل الصوتية.

  قم بتهيئة كلمة مرور نظام الرسائل الصوتية الافتراضية لجميع المستخدمين.

- كيف يشير الهاتف إلى أن يتم انتظار الرسائل الصوتية.

  استخدم Cisco Unified Communications Manager لإعداد طريقة مؤشر انتظار الرسائل (MWI).

ملفات تكوين الهاتف

يتم تخزين ملفات التهيئة للهاتف على خادم TFTP وتحديد معلمات للاتصال بـ Cisco Unified Communications Manager. بوجه عام، في أي وقت تجري فيه أي تغيير في Cisco Unified Communications Manager يحتاج فيه الهاتف لإعادة تعيين، يتم إجراء تغيير تلقائياً في ملف تهيئة الهاتف.

تحتوي ملفات التهيئة أيضًا على معلومات حول الصورة التي يجب تحميلها عند تشغيل الهاتف. إذا كانت هذه الصورة مختلفة عن تلك المحملة حاليًا على الهاتف، فيتصل الهاتف بخادم TFTP لطلب ملفات التحميل المطلوبة.

إذا قمت بتهيئة إعدادات متعلقة بالأمان في Cisco Unified Communications Manager Administration، سيحتوي ملف تهيئة الهاتف معلومات هامة. للتأكد من خصوصية ملف التكوين، يجب عليك تكوينه للتشفير. للحصول على مزيد من المعلومات، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك. يطلب هاتف ملف تهيئة عندما تتم إعادة التعيين والتسجيل في Cisco Unified Communications Manager.

يقوم هاتف بالوصول إلى ملف التهيئة بمسمى XmlDefault.cnf.xml من خادم TFTP وفي حال استيفاء الشروط التالية:

- لقد قمت بتمكين خاصية التسجيل التلقائي في Cisco Unified Communications Manager
- لم تتم إضافة الهاتف إلى قاعدة البيانات Cisco Unified Communications Manager
- يتم تسجيل الهاتف للمرة الأولى

سلوك الهاتف خلال أوقات الذروة على الشبكة

أي شيء يقلل من أداء الشبكة يمكن أن يؤثر على صوت الهاتف، وفي بعض الحالات، يمكن أن يتسبب في انقطاع المكالمة. يمكن أن تشمل المصادر المؤدية لسوء جودة الشبكة، على سبيل المثال لا الحصر، الأنشطة التالية:

- المهام الإدارية، مثل إجراء فحص على منفذ داخلي أو فحص أمان.
- الهجمات التي تحدث على شبكتك، مثل هجمة "رفض الخدمة".

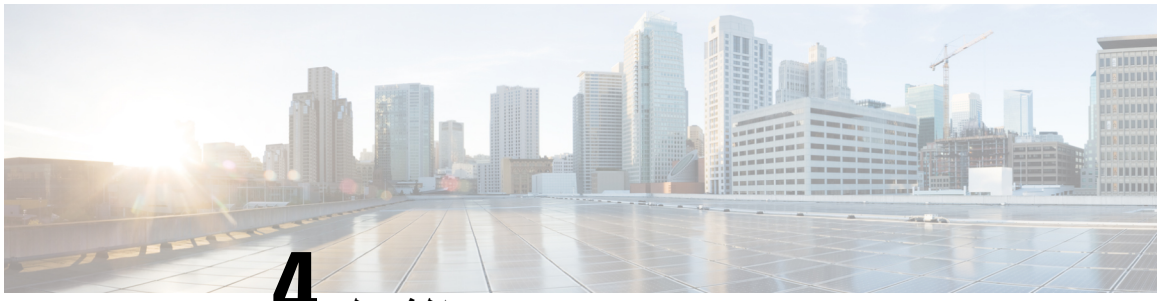
واجهة برمجة التطبيقات

تدعم Cisco استخدام واجهة API للهاتف بواسطة تطبيقات الجهات الخارجية التي تم اختبارها واعتمادها من خلال Cisco بواسطة مطور تطبيقات الطرف الخارجي. يجب معالجة أية مشكلات هاتفية تتعلق بالتفاعل مع التطبيق غير المعتمد من قبل الطرف الخارجي ولن تعالجها Cisco.

للحصول على نموذج دعم لتطبيقات / حلول الجهات الخارجية المعتمدة من Cisco، يرجى الرجوع إلى موقع الويب الخاص بـ Cisco Solution Partner Program للحصول على التفاصيل.

الجزء II

تثبيت هاتف مؤتمر Cisco IP



الفصل 4

تثبيت الهاتف

التحقق من إعداد الشبكة

عند نشر نظام هاتفية IP جديد، يجب أن يكمل مسؤولو الأنظمة والشبكات العديد من مهام التهيئة الأولية لإعداد الشبكة لخدمة هاتفية IP. للحصول على معلومات وقائمة اختيار خاصة بإعداد وتكوين شبكة هاتفية IP من Cisco، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.

لكي يتم تشغيل الهاتف بشكل ناجح كنقطة نهاية في شبكتك، يجب أن تفي شبكتك بمتطلبات محددة. أحد المتطلبات هو النطاق الترددي المناسب. تتطلب الهواتف عرض نطاق ترددي أكبر من الـ 32 كيلو بت في الثانية الموصى بها عند تسجيلها في Cisco Unified Communications Manager. خذ بعين الاعتبار متطلبات هذا النطاق الترددي العالي عند تكوين نطاق ترددي QoS. لمزيد من المعلومات، راجع تصاميم شبكة مرجع حل *Cisco Collaboration System 12.x (SRND)* أو أحدث (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.html).

ملاحظة يعرض الهاتف التاريخ والوقت من Cisco Unified Communications Manager. قد يختلف الوقت المعروض على الهاتف عن وقت Cisco Unified Communications Manager بمدة تصل إلى 10 ثوان.

اجراء

الخطوة 1 قم بتكوين شبكة VoIP للوفاء بالمتطلبات التالية:

- يتم تكوين VoIP على الموجهات والبوابات.

• Cisco Unified Communications Manager مثبت في شبكتك ومكون لمعالجة المكالمة.

الخطوة 2 قم بإعداد الشبكة لدعم أحد الخيارات التالية:

• دعم DHCP

• التعيين اليدوي لعنوان IP والبوابة وقناع الشبكة الفرعية

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14

إعداد رمز التنشيط للهواتف في الموقع

يمكنك استخدام "إعداد رمز التنشيط" لإعداد هواتف جديدة دون خاصية التسجيل التلقائي بسرعة. وبهذه الطريقة، يمكنك التحكم في عملية إعداد الهاتف باستخدام أي مما يلي:

• أداة الإدارة المجمعة للاتصالات الموحدة من Cisco (BAT)

• واجهة Cisco Unified Communications Manager

• خدمة ويب XML الإدارية (AXL)

قم بتمكين هذه الميزة من قسم **معلومات الجهاز** من صفحة "تهيئة الهاتف". حدد **المطالبة برمز التنشيط للإعداد** إذا كنت ترغب في تطبيق هذه الميزة على هاتف واحد في الموقع.

يجب على المستخدمين إدخال رمز تنشيط قبل تسجيل الهواتف الخاصة بهم. يمكن تطبيق "إعداد رمز" التنشيط الهواتف الفردية أو مجموعة من الهواتف، أو عبر شبكة بأكملها.

هذه طريقة سهلة ليقوم المستخدمون بتأهيل هواتفهم نظرًا لأنها تقوم بإدخال رمز تنشيط مكون من 16 رقمًا. يتم إدخال الرموز إما يدويًا أو باستخدام رمز QR إذا كان الهاتف يحتوي على كاميرا فيديو. نوصي باستخدام أسلوب اتصال آمن لتوفير هذه المعلومات للمستخدمين. ولكن إذا تم تعيين مستخدم إلى هاتف ما، فمن ثم تتوفر هذه المعلومات على "مدخل Self Care". يبدأ سجل التدقيق عند وصول المستخدم إلى الرمز من المدخل.

يمكن فقط استخدام رموز التنشيط مرة واحدة، والتي تنتهي صلاحيتها بعد أسبوع واحد بشكل افتراضي. إذا انتهت صلاحية أحد الرموز، فيجب عليك توفير رمز جديد للمستخدم.

ستجد أن هذا النهج يمثل طريقة سهلة للمحافظة على أمان شبكتك لأن أي هاتف لا يمكنه التسجيل حتى يتم التحقق من صحة "الشهادة المثبتة للتصنيع" (MIC) ورمز التنشيط. يمثل هذا الأسلوب طريقة ملائمة لتجميع هواتف اللوحة نظرًا لعدم استخدامه الأداة لدعم الهواتف المسجلة تلقائيًا (TAPS) أو خاصية التسجيل التلقائي. يعد معدل الإعداد هاتفًا واحدًا لكل ثانية أو نحو 3600 هاتف لكل ساعة. يمكن إضافة الهواتف باستخدام Cisco Unified Communications Manager، أو باستخدام خدمة ويب AXL) "XML") أو باستخدام BAT.

الهواتف الموجودة بإعادة تعيين بعد تكوينها لـ "إعداد رمز التنشيط". ولا يتم تسجيلها حتى يتم إدخال رمز التنشيط ويتم التحقق من خاصية MIC بالهاتف. إعلام المستخدمين الحاليين بأنك تنتقل إلى "إعداد رمز التنشيط" قبل تنفيذه.

للحصول على مزيد من المعلومات، راجع دليل إدارة *Cisco Unified Communications Manager* و*IM* و*Presence Service* والإصدار *12.0(1)* أو إصدار أحدث.

إعداد رمز التنشيط والوصول عبر الأجهزة المحمولة وعن بُعد

يمكنك استخدام إعداد رمز التنشيط باستخدام الوصول عبر الأجهزة المحمولة وعن بُعد عند توزيع هواتف Cisco IP للمستخدمين عن بُعد. تعد هذه الميزة طريقه أمنه لنشر الهواتف الداخلية عندما يكون خاصيه غير مطلوب. ولكن يمكنك تهيئه هاتف لخاصيه عندما يكون محليا ،

ورموز التنشيط عندما تكون محليا. تشبه هذه الميزة ميزه إلغاء إلحاق رمز التنشيط للهواتف الداخلية ، ولكنها تجعل رمز التنشيط متوفرا للهواتف الداخلية أيضا.

يتطلب إعداد رمز التنشيط للوصول عبر الأجهزة المحمولة وعن بُعد وجود الإصدار SU1(1)12.5 من Cisco Unified Communications Manager أو إصدار أحدث، والإصدار X12.5 من Cisco Expressway أو إصدار أحدث. يجب أن يتم تمكين الترخيص الذكي أيضًا.

يمكنك تمكين هذه الميزة من إدارة Cisco Unified Communications Manager، ولكن لاحظ ما يلي:

- قم بتمكين هذه الميزة من قسم **معلومات الجهاز** من صفحة "تهيئة الهاتف".
- حدد **المطالبة برمز التنشيط للإعداد** إذا كنت ترغب في تطبيق هذه الميزة على هاتف واحد في الموقع.
- حدد **السماح برمز التنشيط عبر MRA** و**المطالبة برمز تنشيط للإعداد** إذا كنت ترغب في استخدام "إعداد التنشيط" لهاتف واحد خارج الموقع. إذا كان الهاتف موجودًا في الموقع، فإنه يقوم بالتغيير إلى وضع الوصول عبر الأجهزة المحمولة وعن بُعد ويستخدم Expressway. إذا لم يتمكن الهاتف من الوصول إلى Expressway، فإنه لا يسجل حتى يوجد خارج الموقع.

للحصول علي مزيد من المعلومات ، راجع المستندات التالية:

- دليل الإدارة لـ *Cisco Unified Communications Manager و IM و Presence Service*، الإصدار *12.0(1)*.
- الوصول عبر الأجهزة المحمولة وعن بُعد من خلال *Cisco Expressway* لـ Cisco Expressway X12.5 أو إصدار أحدث

تمكين التسجيل التلقائي للهواتف

يحتاج هاتف Cisco IP أن يتولى Cisco Unified Communications Manager معالجة المكالمات. راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك أو التعليمات المتأثرة بالسياق في إدارة Cisco Unified Communications Manager لضمان أنه قد تم إعداد Cisco Unified Communications Manager بطريقة صحيحة لإدارة الهاتف ولتوجيه المكالمات ومعالجتها على نحو سليم.

قبل تثبيت هاتف Cisco IP ، يجب أن تختار طريقة لإضافة الهواتف إلى قاعدة بيانات Cisco Unified Communications Manager.

من خلال تمكين التسجيل التلقائي قبل تثبيت الهواتف، يمكنك إجراء ما يلي:

- إضافة الهواتف دون جمع عناوين MAC من الهواتف أولاً.
- إضافة هاتف Cisco IP تلقائيًا إلى قاعدة بيانات Cisco Unified Communications Manager بعد توصيل الهاتف فعليًا بشبكة هاتفية IP. أثناء التسجيل التلقائي، يُعيّن Cisco Unified Communications Manager رقم الدليل التسلسلي التالي إلى الهاتف.
- إدخال الهواتف بشكل سريع إلى قاعدة بيانات Cisco Unified Communications Manager وتعديل أي إعدادات، مثل أرقام الدليل، من Cisco Unified Communications Manager.
- نقل الهواتف المسجلة تلقائيًا إلى مواقع جديدة وتعيينها إلى مجمّعات أجهزة مختلفة دون التأثير على أرقام الدليل الخاصة بها.

يتم تعطيل خاصية التسجيل التلقائي بشكل افتراضي. في بعض الحالات، قد لا ترغب في استخدام خاصية التسجيل التلقائي؛ على سبيل المثال، إذا كنت ترغب في تعيين رقم دليل إلى الهاتف، أو إذا كنت ترغب في استخدام اتصال آمن من خلال Cisco Unified Communications Manager. للحصول على معلومات حول تمكين خاصية التسجيل التلقائي، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك. عندما تقوم بتكوين المجموعة للوضع المختلط من خلال عميل Cisco CTL، يتم تعطيل خاصية التسجيل التلقائي تلقائيًا، إلا أنه يمكنك تمكينها. عندما تقوم بتكوين المجموعة لوضع غير آمن من خلال عميل Cisco CTL، لا يتم تمكين خاصية التسجيل التلقائي تلقائيًا.

يمكنك إضافة الهواتف من خلال التسجيل التلقائي وTAPS، وهي أداة دعم الهواتف المسجلة تلقائيًا، دون جمع عناوين MAC من الهواتف أولاً.

تعمل TAPS مع أداة الإدارة المجمّعة (BAT) لتحديث مجموعة من الهواتف التي تمت إضافتها بالفعل إلى قاعدة بيانات Cisco Unified Communications Manager من خلال عناوين MAC وهمية. استخدم TAPS لتحديث عناوين MAC ولتنزيل التكوينات المحددة مسبقًا للهواتف.

توصي Cisco بأن تستخدم خاصية التسجيل التلقائي وTAPS لإضافة أقل من 100 هاتف إلى شبكتك. لإضافة أكثر من 100 هاتف إلى شبكتك، استخدام أداة الإدارة المجمّعة (BAT).

لتنفيذ TAPS، اطلب أنت أو المستخدم الآخر رقم دليل TAPS واتبع المطالبات الصوتية. بعد اكتمال العملية، يحتوي الهاتف على رقم الدليل وإعدادات أخرى، ويتم تحديث الهاتف في إدارة Cisco Unified Communications Manager بعناوين MAC الصحيحة.

تأكد من أنه قد تم تمكين خاصية التسجيل التلقائي بشكل صحيح في إدارة Cisco Unified Communications Manager قبل توصيل أي هاتف Cisco IP بالشبكة. للحصول على معلومات حول تمكين خاصية التسجيل التلقائي وتكوينها، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.

يجب تمكين خاصية التسجيل التلقائي في إدارة Cisco Unified Communications Manager لكي تعمل TAPS.

اجراء

الخطوة 1 في إدارة Cisco Unified Communications Manager، انقر فوق **النظام** > **Cisco Unified CM**.

الخطوة 2 انقر فوق **بحث** وحدد الخادم المطلوب.

الخطوة 3 في **معلومات التسجيل التلقائي**، قم بتكوين هذه الحقول.

- **قالب الجهاز العمومي**
- **قالب الخط العمومي**
- **رقم دليل بدء التشغيل**
- **رقم دليل الإنهاء**

الخطوة 4 قم بإلغاء تحديد خانة الاختيار **تم تعطيل التسجيل التلقائي على Cisco Unified Communications Manager هذا**.

الخطوة 5 انقر فوق **حفظ**.

الخطوة 6 انقر فوق **تطبيق التكوين**.

وضع سلسلتين

يمكنك توصيل هاتفي مؤتمر باستخدام محول ذكي وكبلات USB-C التي يتم توفيرها في مجموعة السلاسل الخطية لتوسيع منطقة تغطية الصوت في غرفة.

في وضع السلسلة الخطية، تستقبل كلتا الوحدتين الطاقة من خلال المحول الذكي المتصل بمحول طاقة. يمكنك استخدام ميكروفون خارجي واحد فقط لكل وحدة. يمكنك استخدام زوج من الميكروفونات السلكية مع الوحدات أو زوج من الميكروفونات اللاسلكية مع الوحدات، ولكن ليس مجموعة مختلط من الميكروفونات. عند توصيل ميكروفون سلكي بإحدى الوحدات، فإنه يتم إلغاء إقران أي ميكروفونات لاسلكية متصلة بنفس الوحدة. عندما تكون هناك مكالمة نشطة، تتم مزامنة مصابيح LED وخيارات القائمة على شاشة الهاتف لكلٍ من الوحدتين.

موضوعات ذات صلة

تثبيت هاتف المؤتمر في وضع Daisy Chain, في الصفحة 36
لا يعمل الهاتف الأول في وضع Daisy Chain, في الصفحة 155

تثبيت هاتف المؤتمر

بعد اتصال الهاتف بالشبكة، يبدأ تشغيل الهاتف ويتم تسجيل الهاتف باستخدام Cisco Unified Communications Manager. إذا قمت بتعطيل خدمة DHCP، فيجب عليك تكوين إعدادات الشبكة على الهاتف.

إذا استخدمت التسجيل التلقائي، فيلزمك تحديث معلومات التكوين الخاصة بالهاتف مثل إقران الهاتف بمستخدم، مما يؤدي إلى تغيير جدول الأزرار أو رقم الدليل.

بعد اتصال الهاتف، يحدد ما إذا كان يجب تثبيت برنامج ثابت جديد على الهاتف أو لا.

إذا كنت تستخدم هاتف المؤتمر في وضع سلسلة خطية، فراجع تثبيت هاتف المؤتمر في وضع Daisy Chain, في الصفحة 36.

قبل البدء

تأكد من أنه تم تثبيت أحدث إصدار برنامج مثبت على Cisco Unified Communications Manager. قم بالتحقق بحثًا عن حزم الأجهزة المحدثة هنا:

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

اجراء

الخطوة 1 اختر مصدر الطاقة الخاص بالهاتف:

- نشر الطاقة عبر Ethernet (PoE) باستخدام حاقن PoE لهاتف مؤتمر Cisco IP 8832
- نشر غير PoE Ethernet باستخدام حاقن إيثرنت غير PoE لهاتف مؤتمر Cisco IP 8832
- نشر Wi-Fi باستخدام محول الطاقة 8832 لهاتف مؤتمر Cisco IP

للحصول على مزيد من المعلومات، ارجع إلى طرق توفير هاتف المؤتمر بالطاقة, في الصفحة 32.

الخطوة 2 قم بتوصيل الهاتف بالمحول.

- إذا كنت تستخدم PoE:

1. قم بتركيب كابل Ethernet بمنفذ LAN.
2. صل الطرف الآخر من كبل Ethernet إما في حاقن PoE لهاتف مؤتمر Cisco IP 8832 أو حاقن Ethernet لهاتف مؤتمر Cisco IP 8832.
3. قم بتوصيل الحاقن بهاتف المؤتمر باستخدام كابل USB-C.

- إذا كنت لا تستخدم PoE:

1. إذا كنت تستخدم حاقن Ethernet لهاتف مؤتمر Cisco IP 8832، فقم بتوصيل محول الطاقة بمأخذ التيار الكهربائي.
2. قم بتوصيل محول الطاقة بحاقن Ethernet باستخدام كابل USB-C.

أو

إذا كنت تستخدم حاقن إيثرنت غير PoE لهاتف مؤتمر Cisco IP 8832، فقم بتوصيله بمأخذ التيار الكهربائي.

3. قم بتوصيل كابل Ethernet في حاقن Ethernet غير PoE أو حاقن Ethernet.
4. قم بتركيب كابل Ethernet بمنفذ LAN.

5. قم بتوصيل حاقن Ethernet غير PoE أو حاقن Ethernet بهاتف المؤتمر باستخدام كابل USB-C.

- إذا كنت تستخدم Wi-Fi:

1. قم بتوصيل محول الطاقة 8832 بهاتف مؤتمر Cisco IP بمأخذ التيار الكهربائي.
2. قم بتوصيل محول الطاقة بهاتف المؤتمر باستخدام كابل USB-C.

ملاحظة بدلاً من محول الطاقة، يمكنك استخدام حاقن إيثرنت غير PoE لتوصيل الطاقة إلى الهاتف. ورغم ذلك، يجب أن تقوم بفصل كبل LAN. يتصل الهاتف بشبكة Wi-Fi فقط عندما لا يكون اتصال إيثرنت متاحًا.

الخطوة 3 راقب عملية بدء تشغيل الهاتف. تعمل هذه الخطوة على التحقق من تكوين الهاتف بشكل صحيح.

الخطوة 4 إذا كنت لا تستخدم التسجيل التلقائي، فقم يدويًا بتكوين إعدادات الأمان على الهاتف.

الخطوة 5 يمكنك السماح للهاتف بالترقية إلى صورة البرنامج الثابت الحالي المخزنة على Cisco Unified Communications Manager.

الخطوة 6 اعمد إلى إجراء المكالمات باستخدام الهاتف للتحقق من أن الهاتف والميزات تعمل بشكل صحيح.

الخطوة 7 قدِّم المعلومات اللازمة للمستخدمين حول كيفية استخدام هواتفهم وكيفية تكوين خيارات الهاتف. تضمن هذه الخطوة أن توفر معلومات كافية لدى المستخدمين تتيح لهم استخدام هواتف Cisco بنجاح.

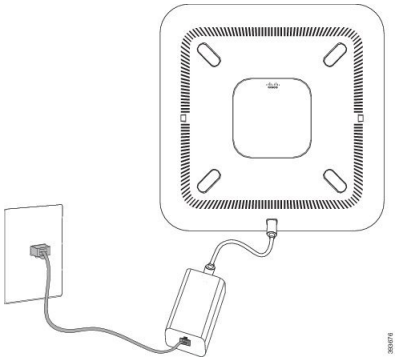
طرق توفير هاتف المؤتمر بالطاقة

يحتاج هاتف المؤتمر إلى الطاقة من أحد المصادر التالية:

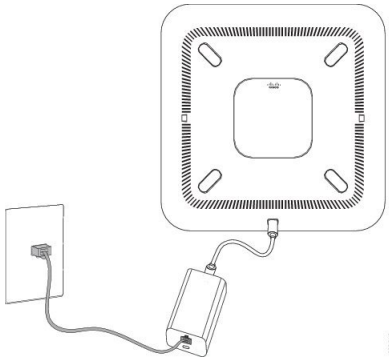
- الطاقة عبر PoE) Ethernet)
  - أمريكا الشمالية
    - حاقن PoE لهاتف مؤتمر Cisco IP 8832
    - حاقن Ethernet لهاتف مؤتمر Cisco IP 8832
  - خارج أمريكا الشمالية —حاقن PoE لهاتف مؤتمر Cisco IP 8832
- غير PoE Ethernet
  - أمريكا الشمالية
    - حاقن إيثرنت غير PoE لهاتف مؤتمر Cisco IP 8832
    - حاقن Ethernet لهاتف مؤتمر Cisco IP 8832 مع توصيل محول طاقة هاتف مؤتمر Cisco IP 8832 بمأخذ تيار كهربائي.
  - خارج أمريكا الشمالية —حاقن إيثرنت غير PoE لهاتف مؤتمر Cisco IP 8832
- شبكة WiFi — استخدم محول طاقة هاتف مؤتمر Cisco IP 8832 بمأخذ تيار كهربائي.

الشكل *6*: خيارات طاقة *PoE* لهاتف المؤتمر

يعرض الشكل التالي خيارين من خيارات طاقة PoE.



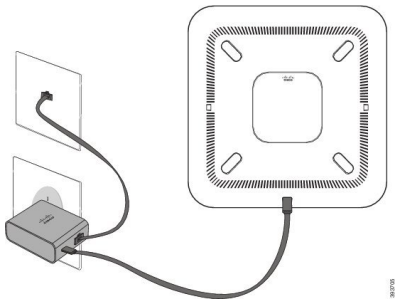
حاقن PoE لهاتف مؤتمر Cisco IP 8832 باستخدام خيار طاقة PoE



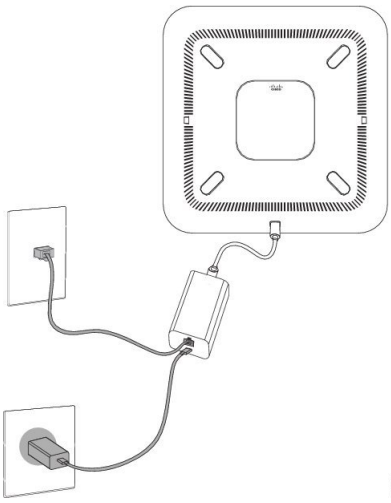
حاقن Ethernet لهاتف مؤتمر Cisco IP 8832 باستخدام خيار طاقة PoE

الشكل 7: خيارات طاقة *Ethernet* لهاتف المؤتمر

يعرض الشكل التالي خيارين من خيارات طاقة Ethernet.

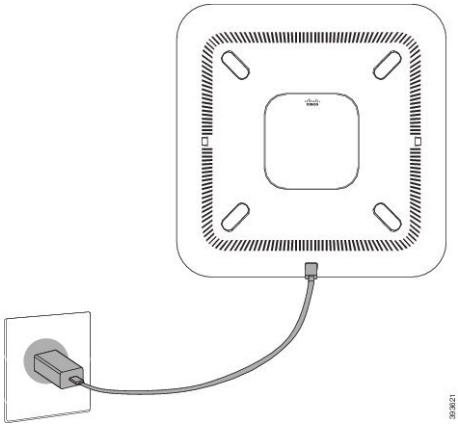


حاقن إيثرنت غير PoE لهاتف مؤتمر Cisco IP 8832 باستخدام خيار طاقة Ethernet



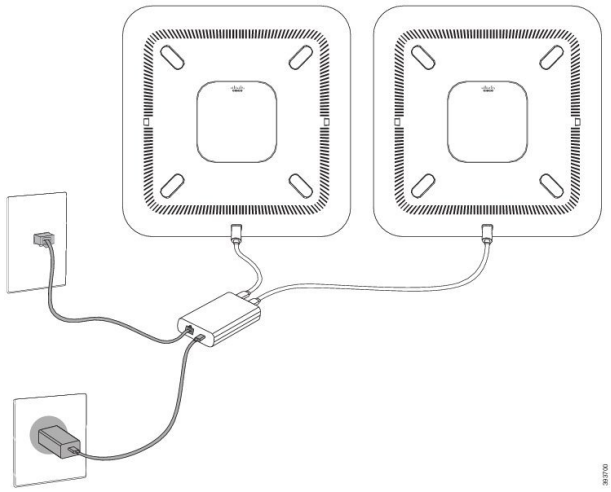
حاقن Ethernet لهاتف مؤتمر Cisco IP 8832 باستخدام خيار طاقة Ethernet

الشكل *8*: خيار طاقة هاتف المؤتمر عندما يكون متصلاً بشبكة *Wi-Fi*



الشكل *9*: خيار طاقة هاتف المؤتمر في وضع السلسلة الخطية

يعرض الشكل التالي خيار الطاقة عند توصيل الهاتف بوضع السلسلة الخطية.



تثبيت ميكروفونات التوسيع السلكية

يدعم الهاتف مجموعة اختيارية مزودة بميكروفوني توسيع سلكيين. يمكنك توسيع الميكروفونات حتى 7 أقدام (2.13 م) من الهاتف. للحصول على أفضل النتائج، ضع الميكروفونات بعيدًا عن الهاتف بمسافة تتراوح بين 3 أقدام (0.91 م) و7 أقدام (2.1 م).

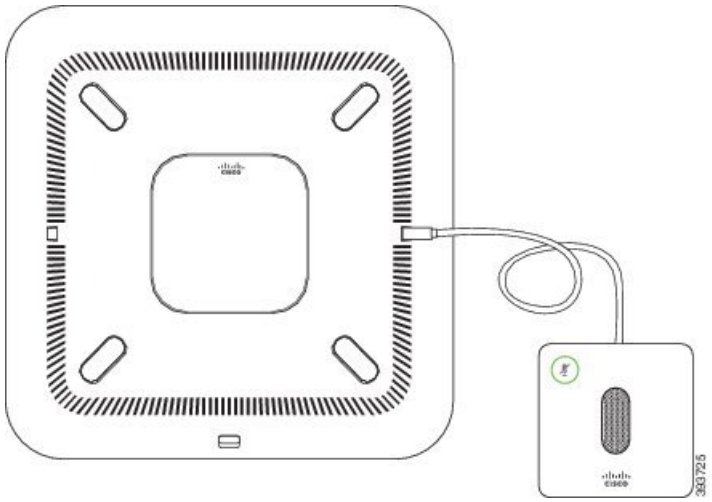
اجراء

الخطوة 1 قم بتوصيل نهاية كبل الميكروفون بالمنفذ الموجود على جانب الهاتف.

الخطوة 2 قم بتوسيع كبل الميكروفون إلى الموضع المطلوب.

يعرض الشكل التالي تثبيت ميكروفون توسيع سلكي.

الشكل *10*: تثبيت ميكروفونات التوسيع السلكية



تثبيت ميكروفونات التوسيع اللاسلكية

يوفر هاتف المؤتمر خيار توصيل ميكروفوني توسيع لاسلكيين.

ملاحظة يجب عليك استخدام إما ميكروفونين سلكيين أو ميكروفونين لاسلكيين بالهاتف، ولكن ليس مجموعة مختلطة منهما.

عند إجراء مكالمة في هاتف المؤتمر، يُضيء مصباح LED الموجود على ميكروفون التوسيع باللون الأخضر. لكتم صوت ميكروفون التوسيع، اضغط على مفتاح **كتم الصوت**. عندما يكون الميكروفون في وضع كتم الصوت، يضيء شريط LED باللون الأحمر. عندما يكون شحن البطارية في الميكروفون منخفضًا، يومض مصباح LED الموجود على البطارية سريعًا.

قبل البدء

قم بفصل ميكروفونات التوسيع السلكية قبل تثبيت ميكروفونات توسيع لاسلكية. لا يمكنك استخدام كلٍّ من ميكروفونات التوسيع السلكية واللاسلكية في نفس الوقت.

اجراء

الخطوة 1 ضع لوحة تثبيت الجدول على موقع سطح الجدول حيث تريد وضع الميكروفون.

الخطوة 2 قم بإزالة المادة اللاصقة لشريط العصا المزدوج أسفل لوحة تثبيت الجدول. ضع لوحة تثبيت الجدول لالصاقه بسطح الجدول.

الخطوة 3 قم بتوصيل الميكروفون بلوحة تثبيت المنضدة. تم تضمين مغناطيس في الميكروفون لتثبيت الوحدة في مكانها.

يمكنك نقل الميكروفون ولوحة تثبيت الجدول المثبتة إلى موقع آخر على سطح الجدول. توخ العناية عند النقل لحماية الوحدة.

موضوعات ذات صلة

ميكروفون التوسيع اللاسلكي (8832 فقط), في الصفحة 12
تثبيت حامل شحن الميكروفون اللاسلكي, في الصفحة 36

تثبيت حامل شحن الميكروفون اللاسلكي

يمكنك استخدام حامل الشحن لشحن بطارية الميكروفون اللاسلكي.

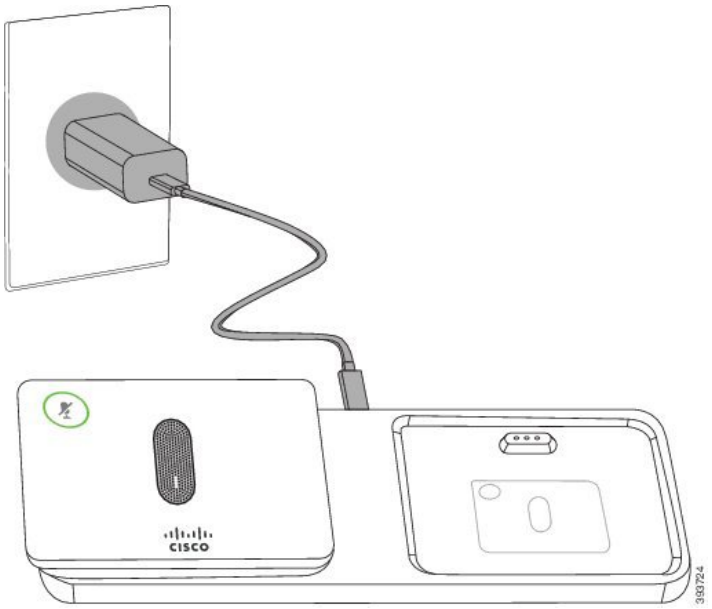
اجراء

الخطوة 1 قم بتوصيل محول طاقة حامل الشحن في مأخذ تيار كهربائي.

الخطوة 2 قم بتوصيل أحد طرفي كبل USB-C بحامل الشحن والطرف الآخر بمحول الطاقة.

يعرض الشكل التالي تثبيت حامل شحن الميكروفون اللاسلكي.

الشكل *11*: تثبيت حامل شحن الميكروفون اللاسلكي



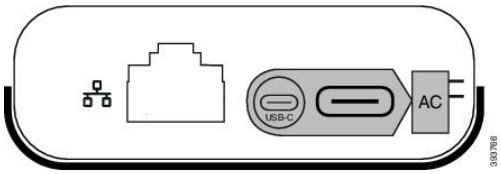
موضوعات ذات صلة

ميكروفون التوسيع اللاسلكي (8832 فقط), في الصفحة 12
تثبيت ميكروفونات التوسيع اللاسلكية, في الصفحة 35

تثبيت هاتف المؤتمر في وضع Daisy Chain

تحتوي مجموعة السلاسل الخطية على محول ذكي، وكبل LAN قصير وكبلا USB-C أطول وأكبر سمكًا وكبل USB-C أكثر نحافة. في وضع السلسلة الخطية، تتطلب هواتف المؤتمر مصدر طاقة خارجي من مأخذ التيار الكهربائي. يجب أن تستخدم محول ذكي لتوصيل الهواتف معًا. تنتقل كبلات USB-C الطويلة إلى الهاتف وينتقل الكبل القصير إلى محول الطاقة. أرجع إلى الشكل التالي عندما تقوم بتوصيل محول الطاقة ومنفذ LAN محول ذكي.

الشكل *12*: منفذ طاقة محول ذكي ومنفذ *LAN*



يمكنك استخدام ميكروفونًا واحدًا فقط لكل وحدة.

ملاحظة يجب عليك استخدام إما ميكروفونين سلكيين أو ميكروفونين لاسلكيين بالهاتف، ولكن ليس مجموعة مختلطة منهما.

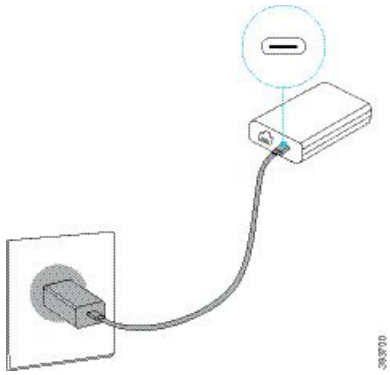
يعتبر كبل USB-C لمحول الطاقة أكثر نحافة من كبلات USB-C التي تتصل بالهاتف.

اجراء

الخطوة 1 قم بتوصيل محول الطاقة في مأخذ التيار الكهربائي.

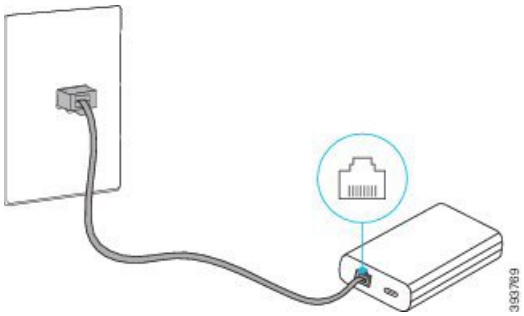
الخطوة 2 قم بتوصيل كبل USB-C القصير والأنحف من محول الطاقة إلى محول ذكي.

الشكل *13*: منفذ *USB* للمحول الذكي المتصل بمنفذ الطاقة



الخطوة 3 مطلوب: قم بتوصيل كبل Ethernet بـ محول ذكي ومنفذ LAN.

الشكل *14*: منفذ *LAN* للمحول الذكي المتصل بمنفذ *LAN* على مقبس الحائط

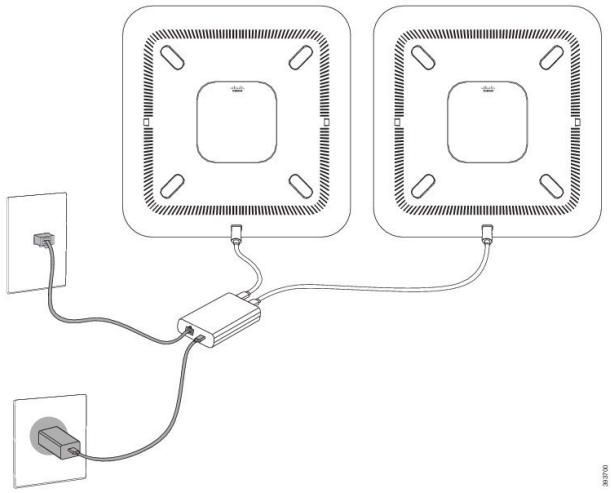


الخطوة 4 قم بتوصيل الهاتف الأول بـ محول ذكي باستخدام كبل أطول، وكبل USB-C أكثر سمكًا.

الخطوة 5 قم بتوصيل الهاتف الثاني بـ محول ذكي باستخدام كابل USB-C.

يعرض الشكل التالي تثبيت هاتف المؤتمر في وضع سلسلتين.

الشكل 15: تثبيت هاتف المؤتمر في وضع Daisy Chain



موضوعات ذات صلة

وضع سلسلتين, في الصفحة 30
لا يعمل الهاتف الأول في وضع Daisy Chain, في الصفحة 155

إعادة تشغيل هاتف المؤتمر من صورة النسخة الاحتياطية

يحتوي هاتف مؤتمر Cisco IP 8832 على نسخة احتياطية بصورة ثانية تسمح لك باسترداد الهاتف عندما اختراق الصورة الافتراضية.

لإعادة تشغيل هاتفك من صورة النسخة الاحتياطية، قم بتنفيذ الإجراء التالي.

اجراء

الخطوة 1 اضغط مفتاح * أثناء توصيل الطاقة بهاتف المؤتمر.

الخطوة 2 بعد تحول ضوء شريط LED إلى "تشغيل" ثم "إيقاف"، يمكنك تحرير مفتاح *.

الخطوة 3 تتم إعادة تشغيل هاتف المؤتمر من صورة النسخة الاحتياطية.

إعداد الهاتف من قوائم الإعداد

يشتمل الهاتف على العديد من إعدادات الشبكة القابلة للتكوين التي قد تحتاج إلى تعديلها قبل أن يكون الهاتف صالحًا للتشغيل لدى المستخدمين. يمكنك الوصول إلى هذه الإعدادات وتغيير بعض منها، وذلك من خلال القوائم الموجودة على الهاتف.

يشتمل الهاتف على قوائم الإعداد التالية:

- إعداد الشبكة: يوفر خيارات عرض وتكوين مجموعة متنوعة من إعدادات الشبكة.

- إعداد IPv4: توفر هذه القائمة الفرعية خيارات إضافية للشبكة.
- إعداد IPv6: توفر هذه القائمة الفرعية خيارات إضافية للشبكة.
- إعداد الأمان: يوفر خيارات عرض وتكوين مجموعة متنوعة من إعدادات الأمان.

ملاحظة يمكنك التحكم في ما إذا كان الهاتف لديه حق الوصول إلى قائمة الإعدادات أو إلى الخيارات الموجودة على هذه القائمة. استخدم حقل **الوصول إلى الإعدادات** في نافذة تكوين هاتف Cisco Unified Communications Manager Administration للتحكم في الوصول. يقبل حقل **الوصول إلى الإعدادات** القيم التالية:

- ممكّن: تتيح إمكانية الوصول إلى قائمة "إعدادات".
- مُعطّل: يمنع الوصول إلى معظم الإدخالات في قائمة الإعدادات. ما زال بإمكان المستخدم الوصول إلى **الإعدادات** > **الحالة**.
- مقيّد: تتيح إمكانية الوصول إلى قائمة "تفضيلات المستخدم" وعناصر قائمة الحالة وتسمح بحفظ تغييرات مستوى الصوت. تحول دون الوصول إلى خيارات أخرى في قائمة "إعدادات".

إذا تعذر عليك الوصول إلى أحد الخيارات في قائمة "إعدادات المسؤول"، فحدد حقل **الوصول إلى الإعدادات**.

يمكنك تكوين الإعدادات المخصصة للعرض فقط على الهاتف في Cisco Unified Communications Manager Administration.

اجراء

الخطوة 1 اضغط على **إعدادات**.

الخطوة 2 حدد **إعدادات المسؤول**.

الخطوة 3 أدخل كلمة المرور إذا لزم إدخالها، ثم انقر فوق **تسجيل الدخول**.

الخطوة 4 حدد **إعداد الشبكة** أو **إعداد الأمان**.

الخطوة 5 نفّذ أحد هذه الإجراءات لعرض القائمة المطلوبة:

- استخدم أسهم التنقل لتحديد القائمة المطلوبة، ثم اضغط على **تحديد**.
- استخدم لوحة المفاتيح الموجودة في الهاتف لإدخال الرقم المتوافق مع القائمة.

الخطوة 6 لعرض قائمة فرعية، كرّر الخطوة 5.

الخطوة 7 للخروج من القائمة، اضغط على **عودة**.

موضوعات ذات صلة

إعادة تشغيل أو إعادة تعيين هاتف المؤتمر, في الصفحة 161
تكوين إعدادات الشبكة, في الصفحة 40
تكوين إعدادات الأمان

تطبيق كلمة مرور الهاتف

اجراء

الخطوة 1 في إدارة Cisco Unified Communications Manager، انتقل إلى نافذة تكوين ملف تعريف الهاتف العام (**الجهاز** > **إعدادات الجهاز** > **ملف تعريف الهاتف العام**).

الخطوة 2 أدخل كلمة مرور في خيار "كلمة مرور إلغاء قفل الهاتف المحلي".

الخطوة 3 طبّق كلمة المرور على ملف تعريف الهاتف العام الذي يستخدمه الهاتف.

إدخال النصوص والدخول إلى القوائم من الهاتف

عند تحرير قيمة أحد إعدادات الخيارات، اتبع هذه الإرشادات:

- استخدم الأسهم الموجودة على لوحة التنقل لتمييز الحقل الذي تريد تحريره. اضغط على **تحديد** في لوحة التنقل لتنشيط الحقل. بعد تنشيط الحقل، يمكنك إدخال القيم.
- استخدم المفاتيح الموجودة على لوحة المفاتيح لإدخال الأرقام والأحرف.
- لإدخال الأحرف باستخدام لوحة المفاتيح، استخدم مفتاح الرقم المقابل. اضغط على المفتاح مرة واحدة أو أكثر من مرة لعرض حرف معين. على سبيل المثال، اضغط على المفتاح 2 مرة واحدة للحرف "a"، ومرتين سريعًا للحرف "b"، وثلاث مرات سريعًا للحرف "c." بعد أن تتوقف مؤقتًا، يتقدم المؤشر تلقائيًا للسماح لك بإدخال الحرف التالي.
- اضغط على المفتاح الوظيفي إذا أخطأت. يعمل هذا المفتاح الوظيفي على حذف الحرف الموجود على يسار المؤشر.
- اضغط على **سحب** قبل الضغط على **تطبيق** لتجاهل أي تغييرات قمت أجريتها.
- لإدخال نقطة (على سبيل المثال، في عنوان IP)، اضغط على * في لوحة المفاتيح.
- لإدخال فصلة لعنوان IPv6، اضغط على * على لوحة المفاتيح.

ملاحظة يوفر هاتف Cisco IP العديد من الأساليب لإعادة تعيين إعدادات الخيارات أو استعادتها، إذا لزم الأمر.

تكوين إعدادات الشبكة

اجراء

الخطوة 1 اضغط على **إعدادات**.

الخطوة 2 حدد **إعدادات المسؤول** > **إعداد الشبكة** > **إعداد إيثرنت**.

الخطوة 3 قم بتعيين الحقول كما هو موضح في حقول إعداد الشبكة, في الصفحة 41.
بعد تعيين الحقول، قد تحتاج إلى إعادة تشغيل الهاتف.

حقول إعداد الشبكة

تحتوي قائمة إعداد الشبكة على الحقول والقوائم الفرعية لـ IPv4 وIPv6.

لتغيير بعض الحقول، تحتاج إلى إيقاف تشغيل DHCP.

الجدول *10*: قائمة إعداد الشبكة

مبتدئ	النوع	الإعداد الافتراضي	الوصف
إعداد IPv4	القائمة		راجع جدول "القائمة الفرعية لإعداد IPv4". يتم عرض هذا الخيار فقط عند الوضع أو في وضع الكدس المزدوج.
إعداد IPv6	القائمة		راجع جدول "القائمة الفرعية لإعداد IPv4".
اسم المضيف	السلسلة		اسم المضيف الخاص بالهاتف. في حالة استخدام DHCP، فإنه يتم تعيين هذا الاسم تلقائيًا.
اسم المجال	السلسلة		اسم مجال نظام اسم المجال (DNS) الذي يوجد به الهاتف. لتغيير هذا الحقل، أوقف تشغيل DHCP.
VLAN ID للتشغيل			شبكة المنطقة المحلية الظاهرية (VLAN) القابلة للتشغيل المكونة على مفتاح تحويل Cisco Catalyst التي يوجد بها الهاتف كعضو.
معرف VLAN للإدارة			شبكة VLAN الإضافية التي يوجد بها الهاتف كعضو.
إعداد منفذ SW	تفاوض تلقائي 10 نصف 10 كامل 100 نصف 100 كامل	تفاوض تلقائي	السرعة والإرسال المزدوج في منفذ مفتاح التحويل، حيث: • 10 Half = 10—BaseT/أحادي الاتجاه • 10 ملء = 10—BaseT/ازدواج كامل • 100 Half = 100—BaseT/أحادي الاتجاه • 100 ملء = 100—BaseT/ازدواج كامل
LLDP—MED: منفذ SW	معطل ممكن	ممكن	يشير إلى ما إذا كان استكشاف نقطة نهاية وسائط بروتوكول استكشاف طبقة الارتباط (LLDP—MED) ممكنًا على منفذ مفتاح التحويل.

الجدول *11*: القائمة الفرعية لإعداد *IPv4*

مبتدئ	النوع	الإعداد الافتراضي	الوصف
DHCP	معطل ممكن	ممكن	تمكين أو تعطيل استخدام DHCP.

مبتدئ	النوع	الإعداد الافتراضي	الوصف
عنوان IP			عنوان الإصدار 4 من بروتوكول الإنترنت (IPv4) للهاتف. لتغيير هذا الحقل، أوقف تشغيل DHCP.
قناع الشبكة الفرعية			قناع الشبكة الفرعية الذي يستخدمه الهاتف. لتغيير هذا الحقل، أوقف تشغيل DHCP.
موجه افتراضي 1			الموجه الافتراضي الذي يستخدمه الهاتف. لتغيير هذا الحقل، أوقف تشغيل DHCP.
ملقم DNS 1			خادم نظام اسم المجال الأساسي (DNS) (خادم DNS 1) الذي يستخدمه الهاتف. لتغيير هذا الحقل، أوقف تشغيل DHCP.
ملقم DNS 2			خادم نظام اسم المجال الأساسي (DNS) (خادم DNS 2) الذي يستخدمه الهاتف.
ملقم DNS 3			خادم نظام اسم المجال الأساسي (DNS) (خادم DNS 3) الذي يستخدمه الهاتف.
TFTP بديل	لا نعم	لا	يشير إلى ما إذا كان الهاتف يستخدم خادم TFTP بديلاً.
خادم TFTP 1			خادم □بروتوكول نقل الملفات المبسط الأساسي (TFTP) الذي يستخدمه الهاتف. إذا قمت بتعيين خيار TFTP البديل على تشغيل، فيجب إدخال قيمة غير صفر لخيار "خادم TFTP الأول". إذا لم يتم إدراج خادم TFTP الأساسي وخادم TFTP الاحتياطي في ملف CTL أو ITL على الهاتف، فيجب عليك إلغاء تأمين الملف قبل حفظ التغييرات إلى خيار "خادم TFTP الأول". في هذه الحالة، يحذف الهاتف الملف عندما تقوم بحفظ تغييرات إلى خيار "خادم TFTP الأول". تنزيل ملف CTL أو ITL جديد من عنوان "خادم TFTP الأول" الجديد. راجع ملاحظات TFTP بعد الجدول النهائي.

مبتدئ	النوع	الإعداد الافتراضي	الوصف
ملقم TFTP 2			خادم TFTP الثانوي الذي يستخدمه الهاتف. إذا لم يتم إدراج خادم TFTP الأساسي وخادم TFTP الاحتياطي في ملف CTL أو ITL على الهاتف، فيجب عليك إلغاء تأمين الملف قبل حفظ التغييرات إلى خيار "خادم TFTP الأول". في هذه الحالة، يحذف الهاتف الملف عندما تقوم بحفظ تغييرات إلى خيار "خادم TFTP الأول". تنزيل ملف CTL أو ITL جديد من عنوان "خادم TFTP الثاني" الجديد. راجع قسم ملاحظات TFTP بعد الجدول النهائي.
تم تحرير عنوان DHCP	لا نعم	لا	

الجدول *12*: القائمة الفرعية لإعداد *IPv6*

مبتدئ	النوع	الإعداد الافتراضي	الوصف
تم تمكين DHCP	معطل ممكن	ممكن	تمكين أو تعطيل استخدام IPv6 DHCP.
عنوان IPv6			عنوان IPv6 الخاص بالهاتف. لتغيير هذا الحقل، أوقف تشغيل DHCP.
طول بادئة IPv6			طول عنوان IPv6. لتغيير هذا الحقل، أوقف تشغيل DHCP.
موجه افتراضي IPv6 1			موجه IPv6 الافتراضي. لتغيير هذا الحقل، أوقف تشغيل DHCP.
ملقم IPv6 DNS 1			خادم IPv6 DNS الأساسي لتغيير هذا الحقل، أوقف تشغيل DHCP.
TFTP بديل IPv6	لا نعم	لا	يشير إلى ما إذا كان الهاتف يستخدم خادم IPv6 TFTP بديلاً.
ملقم IPv6 TFTP 1			خادم IPv6 TFTP الأساسي المستخدم الذي يستخدمه الهاتف. راجع قسم ملاحظات TFTP بعد هذا الجدول.
ملقم IPv6 TFTP 2			خادم IPv6 TFTP الثانوي المستخدم الذي يستخدمه الهاتف. راجع قسم ملاحظات TFTP بعد هذا الجدول.

مبتدئ	النوع	الإعداد الافتراضي	الوصف
تم تحرير عنوان IPv6	لا نعم	لا	

قبل تكوين خيارات إعداد IPv6 على الجهاز الخاص بك، يجب تمكين IPv6 وتكوينه في إدارة Cisco Unified Communication. تنطبق حقول تكوين الجهاز التالية لتكوين IPv6:

- وضع عنونة IP
- تفضيل وضع عنونة IP لإرسال الإشارة

إذا تم تمكين IPv6 في مجموعة Unified، فسيكون الإعداد الافتراضي لوضع عنونة IP IPv4 وIPv6. في وضع العنونة هذا، سيتم الحصول على الهاتف واستخدامه عنوان IPv4 واحد وعنوان IPv6 واحد. وقد يستخدم عنوان IPv4 وعنوان IPv6 كما هو مطلوب للوسائط. يستخدم الهاتف إما عنوان IPv4 أو IPv6 لإرسال إشارة التحكم في المكالمات.

لمزيد من المعلومات حول IPv6، راجع:

- "تكوين الجهاز الشائع" في دليل خدمات وميزة *Cisco Unified Communications Manager*، فصل "دعم IPv6 في أجهزة Cisco Unified Communications".
- دليل نشر *IPv6* للإصدار *12.0* من *Cisco Collaboration Systems*، الموجود هنا: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html

ملاحظات TFTP

عندما يبحث الهاتف عن خادم TFTP، يمنح الهاتف الأسبقية لخوادم TFTP المعينة يدوياً، بغض النظر عن البروتوكول. إذا كان التكوين لديك يتضمن خوادم IPv4 TFTP وIPv6، فيحدد الهاتف أولويات الترتيب الذي يقوم بالبحث عن خادم TFTP بمنح الأولوية لخوادم IPv6 TFTP المعينة يدوياً وخوادم IPv4 TFTP. يبحث الهاتف عن خادم TFTP بالترتيب التالي:

1. أي خوادم IPv4 TFTP معينة يدوياً
2. أي خوادم IPv6 TFTP معينة يدوياً
3. خوادم TFTP مخصص لها DHCP
4. خوادم TFTP معيّن لها DHCPv6

لمزيد من المعلومات حول ملفات CTL وITL، راجع دليل أمان *Cisco Unified Communications Manager*.

تعيين حقل اسم المجال

اجراء

الخطوة 1 عيّن خيار "تمكين DHCP" إلى **لا**.

الخطوة 2 مرّر إلى خيار "اسم المجال"، واضغط على **تحديد**، وأدخل اسم مجال جديدًا.

الخطوة 3 اضغط على **تطبيق**.

تمكين شبكة LAN اللاسلكية من الهاتف

تأكد من وجود تغطية Wi-fi في الموقع حيث يتم نشر شبكة LAN اللاسلكية بطريقة ملائمة لإرسال الحزم الصوتية.

ينصح مستخدمي شبكة Wi-fi بطريقة تجوال سريعة وآمنة. نوصي باستخدام r (FT802.11).

لمعلومات التكوين الكاملة، راجع "دليل نشر شبكة *LAN* اللاسلكية لهاتف *Cisco IP 8832*" في هذا الموقع:

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

يحتوي "دليل نشر شبكة *LAN* اللاسلكية لهاتف *Cisco IP 8832*" على معلومات التكوين التالية:

- تكوين الشبكة اللاسلكية
- تهيئة الشبكة اللاسلكية في إدارة Cisco Unified Communications Manager
- تكوين الشبكة اللاسلكية على هاتف Cisco IP

قبل البدء

تأكد من أنه تم تمكين شبكة Wi-Fi على الهاتف، وتم قطع اتصال كبل إيثرنت.

اجراء

الخطوة 1 لتمكين التطبيق، اضغط على **الإعدادات**.

الخطوة 2 انتقل إلى **إعدادات المسؤول** > **إعداد الشبكة** > **إعداد عميل Wi-Fi** > **لاسلكي**.

الخطوة 3 اضغط **تشغيل**.

إعداد شبكة LAN اللاسلكية باستخدام Cisco Unified Communications Manager

في إدارة Cisco Unified Communications Manager، يجب تمكين معلمة يطلق عليها "Wi-Fi" لهاتف المؤتمر.

ملاحظة في نافذة "تكوين الهاتف" في إدارة Cisco Unified Communications Manager (**الجهاز** > **الهاتف**)، استخدم عنوان MAC بخط سلكي عندما تقوم بتكوين عنوان MAC. لا يستخدم تسجيل Cisco Unified Communications Manager عنوان MAC اللاسلكي.

نفذ الإجراء التالي في إدارة Cisco Unified Communications Manager.

اجراء

الخطوة 1 لتمكين شبكة LAN اللاسلكية على هاتف معين، قم بتنفيذ الخطوات التالية:

a) حدد **الجهاز** > **الهاتف**.

b) حدد موقع الهاتف المطلوب.

c) حدد الإعداد **ممكّن** الخاص بمعلمة شبكة Wi-Fi في قسم "مخطط التكوين الخاص بالمنتج".

d) حدد خانة الاختيار **تجاوز الإعدادات العامة**.

الخطوة 2 لتمكين شبكة LAN اللاسلكية لمجموعة من الهواتف،

a) حدد **الجهاز** > **إعدادات الجهاز** > **ملف تعريف الهاتف العام**
b) حدد الإعداد **ممكّن** الخاص بمعلمة شبكة Wi-Fi.

ملاحظة ولضمان عمل التكوين في هذه الخطوة، قم بإلغاء تحديد خانة الاختيار **تجاوز الإعدادات العامة** المذكورة في الخطوة 1د.

c) حدد خانة الاختيار **تجاوز الإعدادات العامة**.
d) إقران الهواتف بملف تعريف الهاتف العام ذلك باستخدام **الجهاز** > **الهاتف**.

الخطوة 3 لتمكين شبكة LAN اللاسلكية لجميع الهواتف الممكنة للشبكة المحلية اللاسلكية في شبكتك،

a) حدد **النظام** > **تكوين هاتف المؤسسة**
b) حدد الإعداد **ممكّن** الخاص بمعلمة شبكة Wi-Fi.

ملاحظة ولضمان عمل التكوين في هذه الخطوة، قم بإلغاء تحديد خانة الاختيار **تجاوز الإعدادات العامة** المذكورة في الخطوة 1د والخطوة 2ج.

c) حدد خانة الاختيار **تجاوز الإعدادات العامة**.

إعداد الشبكة المحلية اللاسلكية من الهاتف

قبل توصيل هاتف Cisco IP بالشبكة المحلية اللاسلكية، يجب عليك تكوين ملف تعريف الشبكة للهاتف باستخدام إعدادات الشبكة المحلية اللاسلكية المناسبة. يمكنك استخدام قائمة **إعداد الشبكة** الموجودة بالهاتف للوصول إلى القائمة الفرعية **إعداد عميل شبكة Wi-fi** وقم بإعداد تكوين الشبكة المحلية اللاسلكية.

ملاحظة لا يظهر خيار **إعداد عميل شبكة Wi-fi** في قائمة **إعداد الشبكة** عندما تكون شبكة Wi-fi معطلة في Cisco Unified Communications Manager.

للحصول على مزيد من المعلومات، راجع دليل نشر الشبكة المحلية اللاسلكية لهاتف مؤتمر *Cisco IP 8832*، الموجود هنا: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html.

قبل البدء

قم بإعداد الشبكة المحلية اللاسلكية باستخدام Cisco Unified Communications Manager

اجراء

الخطوة 1 اضغط على **إعدادات**.
الخطوة 2 حدد **إعدادات المسؤول** > **إعداد الشبكة** > **إعداد عميل شبكة Wi-fi**.
الخطوة 3 قم بإعداد التكوين اللاسلكي كما هو موضح في الجدول التالي.

الجدول *13*: خيارات قائمة إعداد عميل شبكة *Wi-Fi*

الخيار	الوصف	للتغيير
لاسلكي	يتم تشغيل الراديو اللاسلكي على هاتف Cisco IP أو إيقاف تشغيله.	قم بالتمرير إلى خيار **الوصول إلى الشبكة اللاسلك** مفتاح التحويل لتغيير الإعداد بين التشغيل والإيقاف
اسم الشبكة	تمكّنك من الاتصال بشبكة لاسلكية باستخدام النافذة **اختر شبكة**. تحتوي هذه النافذة على زرين وظيفيين - **عودة** و**أخرى**.	في **اختر شبكة اتصال** النافذة، حدد الشبكة التي تر الاتصال.
وصول تسجيل دخول WLAN	يتيح عرض سجل شبكة Wi-fi في نافذة.	قم بالتمرير إلى خيار **الوصول إلى تسجيل الدخول Wi-Fi**، واستخدم مفتاح التحويل لتغيير الإعداد ب والإيقاف.
إعداد IPv4	في القائمة الفرعية تكوين إعداد IPv4، يمكنك القيام بما يلي: • تمكين الهاتف أو تعطيله باستخدام عنوان IP الذي يقوم بتعيين خادم DHCP. • تعيين عنوان IP وقناع الشبكة الفرعية وأجهزة التوجيه الافتراضي وخادم DNS وخوادم TFTP البديلة يدويًا. للحصول على مزيد من المعلومات حول حقول عنوان IPv4، راجع الجدول "القائمة الفرعية لإعداد IPv4".	قم بالتمرير إلى **إعداد IPv4** واضغط على **حدد**.
إعداد IPv6	في القائمة الفرعية تكوين إعداد IPv6، يمكنك القيام بما يلي: • تمكين الهاتف أو تعطيله باستخدام عنوان IPv6 المخصص إما من قِبل خادم DHCPv6 أو الحصول عليه من خلال SLAAC باستخدام جهاز توجيه ممكّن عليه IPv6. • تعيين عنوان IPv6 وطول البادئة وأجهزة التوجيه الافتراضية وخادم DNS وخوادم TFTP البديلة يدويًا. للحصول على مزيد من المعلومات حول حقول عنوان IPv6، راجع الجدول "القائمة الفرعية لإعداد IPv6".	قم بالتمرير إلى **إعداد IPv6** واضغط على **حدد**.
عنوان MAC	عنوان التحكم في الوصول الفريد إلى الوسائط (MAC) الخاص بالهاتف.	العرض فقط. يتعذّر التكوين.
اسم المجال	اسم مجال نظام اسم المجال (DNS) الذي يوجد به الهاتف.	ارجع إلى تعيين حقل اسم المجال, في الصفحة 44

الخطوة 4 اضغط على **حفظ** لإجراء التغييرات أو اضغط على **رجوع** لتجاهل الاتصال.

تعيين عدد محاولات مصادقة WLAN

طلب المصادقة هو تأكيد لبيانات اعتماد تسجيل الدخول الخاصة بالمستخدم. يحدث هذا عند محاولة الهاتف المنضم بالفعل لشبكة Wi-Fi لإعادة الاتصال بخادم شبكة Wi-Fi. تشتمل أمثلة عندما تنتهي مهلة جلسة شبكة Wi-Fi أو فقدان اتصال شبكة Wi-Fi ثم إعادة الاتصال.

يمكنك تكوين عدد مرات إرسال هاتف شبكة Wi-Fi طلبات مصادقة إلى خادم Wi-Fi. العدد الافتراضي للمحاولات هو 2، ولكن يمكنك تعيين هذه المعلمة من 1 إلى 3. إذا فشل الهاتف في المصادقة، فستتم مطالبة المستخدم بتسجيل الدخول مرة أخرى.

يمكنك تطبيق "محاولات مصادقة الشبكة المحلية اللاسلكية" على هواتف فردية، أو مجموعة هواتف، أو جميع الهواتف التي على اتصال بشبكة Wi-Fi في شبكتك.

اجراء

الخطوة 1 في "إدارة Cisco Unified Communications Manager"، حدد **الجهاز** > **الهاتف** وحدد موقع الهاتف.
الخطوة 2 انتقل إلى منطقة "التكوين الخاص بالمنتج" وقم بتعيين الحقل **"محاولات مصادقة الشبكة المحلية اللاسلكية"**.
الخطوة 3 حدد **حفظ**.
الخطوة 4 حدد **تطبيق التكوين**.
الخطوة 5 أعِد تشغيل الهاتف.

تمكين وضع مطالبة الشبكة المحلية اللاسلكية

تمكين وضع المطالبة 1 لملف تعريف الشبكة اللاسلكية WLAN إذا كنت تريد من المستخدم تسجيل الدخول إلى شبكة Wi-fi عند تشغيل الهاتف أو إعادة التعيين.

اجراء

الخطوة 1 في إدارة Cisco Unified Communications Manager، حدد **الجهاز** > **الهاتف**.
الخطوة 2 حدد موقع الهاتف الذي تريد إعداده.
الخطوة 3 انتقل إلى منطقة "التكوين الخاص بالمنتج" واضبط حقل **"وضع المطالبة 1 لملف تعريف الشبكة اللاسلكية WLAN"** على **"تمكين"**.
الخطوة 4 حدد **حفظ**.
الخطوة 5 حدد **تطبيق التكوين**.
الخطوة 6 أعِد تشغيل الهاتف.

إعداد ملف تعريف Wi-Fi باستخدام Cisco Unified Communications Manager

يمكنك تهيئة ملف تعريف شبكة Wi-fi وقم بتعيين ملف تعريف على الهواتف التي تدعم Wi-fi. يحتوي على ملف تعريف المعلمات المطلوبة للهواتف للاتصال ب Cisco Unified Communications Manager بشبكة Wi-fi. عند إنشاء واستخدام ملف تعريف شبكة Wi-fi، أنت أو مستخدموك لا تحتاج لتهيئة الشبكة اللاسلكية لهواتف فردية.

يتم تخصيص ملفات تعريف شبكة Wi-fi المدعومة على إصدار 2) 10.5 Cisco Unified Communications Manager) أو الإصدار الأحدث منه. إن EAP-FAST، وPEAP-GTC، وPEAP-MSCHAPv2 مدعوم في Cisco Unified Communications Manager، إصدار 10.0 والإصدار الأحدث. إن EAP-TLS مدعوم في Cisco Unified Communications Manager، الإصدار 11.0 والإصدار الأحدث

ملف تعريف شبكة Wi-fi يتيح لك إمكانية منع أو تحديد التغييرات في تهيئة شبكة Wi-fi على الهاتف بالمستخدم.

نوصي باستخدام ملف تعريف الأمان مع التشفير TFTP ممكن لحماية المفاتيح وكلمات المرور عند استخدام ملف تعريف شبكة Wi-fi.

عند إعداد الهواتف لاستخدام مصادقة EAP-FAST أو PEAP-MSCHAPv2 أو PEAP-GTC، يحتاج المستخدمون إلى معرفات مستخدمين فردية وكلمات مرور لتسجيل الدخول إلى الهاتف.

تدعم الهواتف فقط شهادة خادم واحدة يمكن تثبيتها إما باستخدام SCEP أو طريقة التثبيت اليدوي لكن ليس بكلتا الطريقتين. لا تدعم الهواتف طريقة TFTP لتثبيت الشهادة.

اجراء

الخطوة 1 في "إدارة Cisco Unified Communications Manager"، حدد **الجهاز** > **إعدادات الجهاز** > **مجموعة ملف تعريف الشبكة المحلية اللاسلكية**.

الخطوة 2 انقر فوق **ضف جديد**.

الخطوة 3 في **"معلومات ملف التعريف الشبكة المحلية اللاسلكية"** ، قم بتعيين المعلمات:

- **اسم**-أدخل اسماً فريداً لملف تعريف شبكة Wi-fi. يتم عرض هذا الاسم على الهاتف.
- **وصف**-أدخل وصفاً لملف التعريف شبكة Wi-fi لمساعدتك في التمييز ملف التعريف هذا من ملفات تعريف شبكة Wi-fi أخرى.
- **التعديل المستخدم**— حدد أحد الخيارات:
  - **مسموح به**— تشير إلى أنه يمكن للمستخدم إجراء تغييرات في إعدادات شبكة Wi-fi من هواتفهم. يتم تحديد هذا الخيار افتراضيًا.
  - **غير مسموح به**— تشير إلى أنه لا يمكن للمستخدم إجراء تغييرات في إعدادات شبكة Wi-fi من هواتفهم.
  - **مقيد**— تشير إلى أنه يمكن للمستخدم تغيير شبكة Wi-fi اسم المستخدم وكلمة المرور على هواتفهم. ولكن لا يسمح للمستخدمين بإجراء تغييرات على إعدادات شبكة Wi-fi أخرى على الهاتف.

الخطوة 4 في **إعدادات الشبكة اللاسلكية"** ، قم بتعيين المعلمات:

- **SSID (اسم الشبكة)**-أدخل اسم الشبكة المتوفرة في بيئة المستخدم الذي يمكن توصيل الهاتف به. يتم عرض هذا الاسم ضمن قائمة الشبكات المتوفرة على الهاتف وتوصيل الهاتف بشبكة الاتصال اللاسلكية.
- **تردد**— الخيارات المتوفرة هي التلقائي و2.4 جيجاهيرتز 5 جيجاهيرتز. يحدد هذا الحقل تردد التي تستخدم الاتصال اللاسلكي. إذا قمت بتحديد تلقائي، يحاول استخدام النطاق 5 جيجاهرتز أولاً الهاتف ويستخدم النطاق 2.4 جيجاهيرتز فقط عندما 5 جيجاهرتز غير متوفر.

الخطوة 5 في **"إعدادات المصادقة"** القسم، قم بتعيين **"طريقة مصادقة"** لإحدى هذه الطرق مصادقة: EAP-FAST، EAP TLS، PEAP MSCHAPv2، جتك PEAP، PSK، WEP وبلا.

بعد تعيين هذا الحقل، فقد ترى الحقول الإضافية التي تحتاج إلى تعيين.

- **شهادة المستخدم**— اللازمة لمصادقة EAP TLS. حدد **تصنيع مثبتة** أو **المستخدم تثبيت**. يتطلب الهاتف تثبيت شهادة إما تلقائيًا من SCEP أو يدويًا من صفحة الإدارة على الهاتف.
- **عبارة المرور PSK**— اللازمة لمصادقة PSK. أدخل الحرف 8-63 ASCII أو 64 عبارة المرور الحرف HEX.
- **عبارة المرور WEP**— اللازمة لمصادقة WEP. أدخل مفتاح 40/102 أو 64/128 ASCII أو Hex WEP.
  - طول 40/104 ASCII يبلغ 5 أحرف.
  - طول 64/128 ASCII يبلغ 13 حرفًا.
  - طول 40/104 HEX يبلغ 10 أحرف.
  - طول 64/128 HEX يبلغ 26 أحرف.
- **توفير بيانات اعتماد مشتركة**: يكون مطلوباً لمصادقة EAP-FAST وPEAP-MSCHAPv2 وPEAP-GTC.
  - إذا كان المستخدم يدير اسم المستخدم وكلمة المرور، اترك حقلي **اسم المستخدم** و**كلمة المرور** فارغين.

- إذا كان جميع المستخدمين بمشاركة نفس اسم المستخدم وكلمة المرور، يمكنك إدخال المعلومات الموجودة في **اسم المستخدم** و**كلمة المرور** الحقول.
- أدخل وصفاً في الحقل **"وصف كلمة المرور"**.

ملاحظة إذا كنت تحتاج إلى تعيين كل مستخدم فريداً اسم مستخدم وكلمة المرور، تحتاج إلى إنشاء ملف تعريف لكل مستخدم.

الخطوة 6 انقر فوق **حفظ**.

ما تريد القيام به بعد الآن

تطبيق مجموعة ملف التعريف الشبكة المحلية اللاسلكية لمجمع الأجهزة (**النظام** > **"مجمع الأجهزة"**) أو مباشرة إلى الهاتف (**الجهاز** > **الهاتف**).

إعداد مجموعة Wi-Fi باستخدام Cisco Unified Communications Manager

يمكنك إنشاء مجموعة ملف تعريف الشبكة المحلية اللاسلكية وإضافة أي ملف تعريف الشبكة المحلية اللاسلكية لهذه المجموعة. ثم يمكن تعيين مجموعة ملف التعريف على الهاتف عندما تقوم بإعداد الهاتف.

اجراء

الخطوة 1 في "إدارة Cisco Unified Communications Manager"، حدد **الجهاز** > **إعدادات الجهاز** > **مجموعة ملف تعريف الشبكة المحلية اللاسلكية**.

يمكنك أيضًا تحديد مجموعة ملفات تعريف الشبكة المحلية اللاسلكية من خلال **النظام** > **"مجمع الأجهزة"**.

الخطوة 2 انقر فوق **ضف جديد**.

الخطوة 3 في قسم **"معلومات مجموعة ملف تعريف الشبكة المحلية اللاسلكية"** ، أدخل اسم المجموعة والوصف.

الخطوة 4 في قسم **ملفات تعريف لمجموعة ملف تعريف الشبكة المحلية اللاسلكية هذه**، حدد ملف تعريف متوفر من قائمة **"ملفات التعريف المتوفرة"** ونقل ملف التعريف المحدد إلى قائمة **"ملفات التعريف المحددة"**.

عند تحديد أكثر من ملف تعريف واحد من الشبكة المحلية اللاسلكية، يستخدم الهاتف فقط أول ملف تعريف شبكة محلية لاسلكية.

الخطوة 5 انقر فوق **حفظ**.

التحقق من بدء تشغيل الهاتف

بعد توصيل الهاتف بالطاقة، يتم تدويره تلقائيًا من خلال عملية تشخيصية لبدء التشغيل.

اجراء

قم بتشغيل الهاتف.

عندما يتم عرض الشاشة الرئيسية، فإنها تكون قد بدأت بشكل صحيح.

تغيير طراز الهاتف الخاص بالمستخدم

يمكنك أنت أو المستخدم تغيير طراز الهاتف الخاص بالمستخدم. قد يكون التغيير مطلوبًا لعدة أسباب، على سبيل المثال:

- لقد قمت بتحديث Cisco Unified Communications Manager (Unified CM) إلى إصدار برنامج لا يدعم طراز الهاتف.
- يريد المستخدم طراز هاتف مختلف عن الطراز الحالي.
- يتطلب الهاتف إصلاح أو استبدال.

يقوم Unified CM بتحديد الهاتف القديم ويستخدم عنوان MAC الخاص بالهاتف القديم لتحديد تكوين الهاتف القديم. ينسخ الرقم الموحد الخاص بتهيئة الهاتف القديمة إلى الإدخال الخاص بالهاتف الجديد. عندئذ يكون للهاتف الجديد نفس التكوين الخاص بالهاتف القديم.

التقييد: إذا كان الهاتف القديم يحتوي على خطوط أو أزرار خطوط أكثر من الهاتف الجديد، فإن الهاتف الجديد لا يحتوي على خطوط أو أزرار خطوط إضافية مكونة.

تتم أعاده تشغيل الهاتف عند اكتمال التهيئة.

قبل البدء

قم بإعداد Cisco Unified Communications Manager الخاص بك وفقًا للإرشادات الواردة في دليل تكوين ميزة لـ *Cisco Unified Communications Manager*.

أنت بحاجه إلى هاتف جديد غير مستخدم وتم تثبيته مسبقا باستخدام إصدار البرامج الثابتة 12.8 (1) أو إصدار أحدث.

اجراء

الخطوة 1 أوقف تشغيل الهاتف القديم.

الخطوة 2 الطاقة الخاصة بالهاتف الجديد.

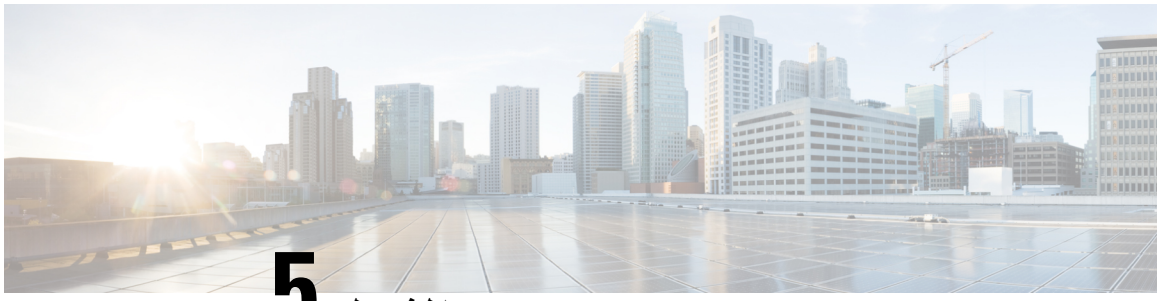
الخطوة 3 في الهاتف الجديد، حدد **استبدال هاتف موجود**.

الخطوة 4 ادخل الرقم الداخلي الأساسي الخاص بالهاتف القديم.

الخطوة 5 إذا كان الهاتف القديم به رقم تعريف شخصي معين، فأدخل رقم التعريف الشخصي.

الخطوة 6 اضغط **إرسال**.

الخطوة 7 في حالة وجود أكثر من جهاز للمستخدم، فحدد الجهاز لاستبداله واضغط **متابعة**.



الفصل 5

تثبيت الهاتف في Cisco Unified Communications Manager

إعداد هاتف مؤتمر Cisco IP

إذا كان التسجيل التلقائي غير ممكّن ولا يظهر الهاتف في قاعدة بيانات Cisco Unified Communications Manager، فيجب عليك تكوين هاتف Cisco IP يدويًا في إدارة Cisco Unified Communications Manager. تُعد بعض المهام الموجودة في هذا الإجراء اختيارية، وذلك بناءً على احتياجات النظام والمستخدمين لديك.

للحصول على مزيد من المعلومات حول أي من الخطوات، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.

نفّذ خطوات التكوين الواردة في الإجراء التالي باستخدام "إدارة Cisco Unified Communications Manager".

اجراء

الخطوة 1 اجمع المعلومات التالية حول الهاتف:

- طراز الهاتف
- عنوان MAC: راجع تحديد عنوان MAC للهاتف, في الصفحة 57
- الموقع المادي للهاتف
- اسم معرف المستخدم الخاص بمستخدم الهاتف
- مجمّع الأجهزة
- القسم ومساحة بحث الاتصال ومعلومات الموقع

- رقم الدليل (DN) المراد تعيينه إلى الهاتف
- مستخدم Cisco Unified Communications Manager المراد إقرانه بالهاتف
- معلومات استخدام الهاتف التي تؤثر على قالب المفتاح المرن أو ميزات الهاتف أو خدمات هاتف IP أو تطبيقات الهاتف.

للحصول على مزيد من المعلومات، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك، وراجع الارتباطات ذات الصلة.

الخطوة 2 تحقق من أن لديك تراخيص وحدات كافية لهاتفك.

للحصول على مزيد من المعلومات، راجع وثائق التراخيص الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.

الخطوة 3 تعريف مجمّعات الأجهزة حدد **النظام** > **مجمّع الأجهزة**.

تحدد مجمّعات الأجهزة السمات الشائعة للأجهزة، مثل المنطقة ومجموعة الوقت/التاريخ وقالب المفتاح المرن.

الخطوة 4 حدد ملف تعريف الهاتف العام. حدد **الجهاز** > **إعدادات الجهاز** > **ملف تعريف الهاتف العام**

توفر ملفات تعريف الهاتف العامة البيانات التي يحتاج إليها خادم TFTP، فضلاً عن إعدادات الهاتف العامة، مثل خياري "عدم الإزعاج" و"التحكم في الميزة".

الخطوة 5 حدد مساحة بحث الاتصال. في إدارة Cisco Unified Communications Manager، انقر فوق **توجيه مسار المكالمة** > **فئة التحكم** > **مساحة بحث الاتصال**.

تُعد "مساحة بحث الاتصال" مجموعة من الأقسام التي يتم فيها لتحديد كيفية توجيه مسار رقم مطلوب. تُستخدم مساحة بحث الاتصال للجهاز ولرقم الدليل معًا. تتفوق ميزة CSS لرقم الدليل في أولويتها على ميزة CSS في الجهاز.

الخطوة 6 قم بتكوين ملف تعريف الأمان لنوع الجهاز وبروتوكوله. حدد **النظام** > **الأمان** > **ملف تعريف أمان الهاتف**.

الخطوة 7 قم بإعداد الهاتف. حدد **الجهاز** > **الهاتف**.

a) حدد موقع الهاتف الذي تريد تعديله أو أضف هاتفًا جديدًا.

b) قم بتكوين الهاتف من خلال إكمال الحقول المطلوبة في جزء "معلومات الجهاز" داخل نافذة "تكوين الهاتف".

- عنوان MAC (مطلوب): تأكد من أن القيمة تشتمل على 12 حرفًا سداسيًا عشريًا.
- الوصف: أدخل وصفًا مفيدًا لمساعدتك في حالة الحاجة إلى البحث عن معلومات متعلقة بهذا المستخدم.
- مجمّع الأجهزة (مطلوب)
- ملف تعريف الهاتف العام
- مساحة بحث الاتصال
- تحديد الموقع
- المالك (مستخدم أو مجهول)، وإذا تم تحديد المستخدم، معرف المستخدم المالك

تتم إضافة الجهاز المقترن بإعداداته الافتراضية إلى قاعدة بيانات Cisco Unified Communications Manager.

للحصول على معلومات حول حقول "التكوين الخاص بالمنتج"، راجع "؟" الزر تعليمات في نافذة "تكوين الهاتف" والارتباط ذي الصلة.

ملاحظة إذا كنت تريد إضافة الهاتف والمستخدم إلى قاعدة بيانات Cisco Unifie Communications Manager في الوقت نفسه، فراجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.

c) في منطقة "المعلومات الخاصة بالبروتوكول" بهذه النافذة، اختر "ملف أمان الجهاز" وقم بتعيين وضع الأمان.

ملاحظة اختر ملف تعريف الأمان استنادًا إلى إستراتيجية الأمان الشاملة لدى الشركة. إذا كان الهاتف لا يدعم الأمان، فاختر ملف تعريف غير آمن.

d) في منطقة "معلومات الرقم الداخلي"، حدد خانة الاختيار "تمكين الاستضافة برقم داخلي" إذا كان هذا الهاتف يدعم "الاستضافة برقم داخلي من Cisco".

e) انقر فوق **حفظ**.

الخطوة 8 حدد **الجهاز** > **إعدادات الجهاز** > **ملف تعريف SIP** لإعداد معلمات SIP.

الخطوة 9 حدد **الجهاز** > **الهاتف** لتكوين أرقام (خطوط) الأدلة على الهاتف من خلال إكمال الحقول المطلوبة في نافذة "تكوين رقم الدليل".

a) ابحث في الهاتف.

b) في نافذة "تكوين الهاتف"، انقر فوق "الخط 1" في الجزء الأيسر من النافذة.

تحتوي هواتف المؤتمر على خط واحد فقط.

c) في حقل "رقم الدليل"، أدخل رقمًا صالحًا يمكن طلبه.

ملاحظة يجب أن يحتوي هذا الحقل على الرقم نفسه الذي يظهر في حقل "رقم الهاتف" داخل نافذة "تكوين المستخدم النهائي".

d) من قائمة "قسم المسار" المنسدلة، اختر القسم الذي ينتمي إليه رقم الدليل. إذا كنت لا تريد تقييد الوصول إلى رقم الدليل، فاختر <None> للقسم.

e) من قائمة "مساحة بحث الاتصال" المنسدلة، اختر مساحة بحث الاتصال الملائمة. يتم تطبيق القيمة التي تختارها على جميع الأجهزة التي تستخدم رقم الدليل هذا.

f) في منطقة "إعدادات إعادة توجيه المكالمة والرد على المكالمة"، اختر العناصر (على سبيل المثال، "توجيه الكل" و"توجيه المكالمة الداخلية المشغولة") والوجهات المتوافقة التي يجب إرسال المكالمات إليها.

أمثلة:

إذا كنت تريد توجيه المكالمات الداخلية والخارجية الواردة التي تتلقى إشارة مشغولة إلى البريد الصوتي لهذا الخط، فحدد خانة اختيار "البريد الصوتي" بجوار العنصرين "توجيه المكالمة الداخلية المشغولة" و"توجيه المكالمة الخارجية المشغولة" في العمود الأيسر من منطقة "إعدادات الرد على المكالمة وتوجيه المكالمة".

g) في جزء "الخط 1 في الجهاز"، قم بتكوين الحقول التالية:

- عرض (حقل "معرف المتصل الداخلي"): يمكنك إدخال الاسم الأول والاسم الأخير لمستخدم هذا الجهاز لكي يتم عرض هذا الاسم لجميع المكالمات الداخلية. اترك هذا الحقل فارغًا لكي يؤدي بالنظام إلى عرض الرقم الداخلي للهاتف.
- قناع رقم الهاتف الخارجي: وضّح رقم (أو قناع) الهاتف المستخدم لإرسال معلومات "معرف المتصل" عند إصدار مكالمة من هذا الخط. يمكنك إدخال عدد من الأرقام وأحرف "X" قوامه 24 كحد أقصى. تمثل أحرف X رقم الدليل ويجب أن تظهر في نهاية النمط.

أمثلة:

إذا قمت بتحديد قناع ممثل في XXXX408902، فتعرض المكالمة الخارجية الواردة من الرقم الداخلي الممثل في 6640 رقم معرف المتصل الممثل في 4089026640.

ويتم تطبيق هذا الإعداد على الجهاز الحالي فقط، وذلك ما لم تحدد خانة الاختيار على الجانب الأيمن (تحديث إعدادات الجهاز المشترك) وتنقر فوق **نشر ما تم تحديده**. لا يتم عرض خانة الاختيار الموجودة في الجانب الأيمن إلا فقط في حالة مشاركة أجهزة أخرى رقم الدليل هذا.

h) حدد **حفظ**.

للحصول على مزيد من المعلومات حول أرقام الأدلة، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager والارتباطات ذات الصلة.

الخطوة 10 (اختياري) أقرن المستخدم بهاتف. انقر فوق **إقران المستخدمين النهائيين** في الجزء السفلي من نافذة "تكوين الهاتف" لإقران مستخدم بالخط قيد التكوين.

a) استخدم **بحث** إلى جانب حقول "بحث" لتحديد موقع المستخدم.
b) حدد الخانة الموجودة بجوار اسم المستخدم، وانقر فوق **إضافة ما تم تحديده**.

يظهر اسم المستخدم ومعرف المستخدم في جزء "المستخدمين المقترنين بالخط" داخل نافذة "تكوين رقم الدليل".

c) حدد **حفظ**.

يقترن الآن المستخدم بالخط 1 في الهاتف.

الخطوة 11 (اختياري) أقرن المستخدم بالجهاز.

a) اختر **إدارة المستخدم** > **المستخدم النهائي**.
b) استخدم مربعات البحث وكذلك **بحث** لتحديد موقع المستخدم الذي أضفته.
c) انقر فوق معرف المستخدم.
d) في منطقة "عمليات إقران رقم الدليل" داخل الشاشة، عيّن "الرقم الداخلي الأساسي" من القائمة المنسدلة.
e) (اختياري) في منطقة "معلومات التنقل"، حدد خانة "تمكين التنقل".
f) في منطقة "معلومات الأذونات"، استخدم أزرار **إضافة إلى مجموعة التحكم في الوصول** لإضافة هذا المستخدم إلى أي من مجموعات المستخدمين.

على سبيل المثال، ربما تريد إضافة المستخدم إلى "مجموعة مستخدمين نهائيين قياسية لـ CCM".

g) لعرض تفاصيل إحدى المجموعات، حدد المجموعة وانقر فوق **عرض التفاصيل**.
h) في منطقة "تنقل الرقم الداخلي"، حدد خانة "تمكين تنقل الرقم الداخلي عبر المجموعة" إذا كان المستخدم بإمكانه الاستفادة من خدمة "تنقل الرقم الداخلي عبر المجموعة".
i) في منطقة "معلومات الجهاز"، انقر فوق **عمليات إقران الجهاز**.
j) استخدم حقول"بحث" وكذلك **بحث** لتحديد موقع الجهاز الذي تريد إقرانه بالمستخدم.
k) حدد الجهاز، وانقر فوق **حفظ ما تم تحديده/التغييرات**.
l) انقر فوق **انتقال** بجوار الارتباط ذي الصلة بـ "العودة إلى المستخدم" في الزاوية العلوية اليمنى من الشاشة.
m) حدد **حفظ**.

الخطوة 12 خصِّص قوالب المفاتيح المرنة حدد **الجهاز** > **إعدادات الجهاز** > **قالب المفتاح المرن**

استخدم الصفحة لإضافة ميزات المفتاح المرن أو حذفها أو تغيير ترتيبها، حيث يتم عرض هذه الميزات على هاتف المستخدم للوفاء باحتياجات استخدام الميزات.

يشتمل هاتف المؤتمر على متطلبات المفتاح المرن الخاصة. راجع الارتباطات ذات الصلة لمزيد من المعلومات.

الخطوة 13 قم بتكوين خدمات Cisco IP وتعيين الخدمات. حدد **الجهاز** > **إعدادات الجهاز** > **خدمات الهاتف**.

لتوفير خدمات "هاتف IP" للهاتف.

ملاحظة يمكن للمستخدمين إضافة خدمات أو تغييرها على هواتفهم باستخدام مدخل Cisco Unified Communications Self Care.

الخطوة 14 (اختياري) أضف معلومات المستخدم إلى الدليل العام الخاص بـ Cisco UnifiedCommunications Manager. حدد **مدير المستخدم** > **المستخدم النهائي**، ثم انقر فوق **إضافة جديد** وقم بتكوين الحقول المطلوبة. يُشار إلى الحقول المطلوبة بعلامة النجمة (*).

ملاحظة إذا كانت شركتك تستخدم دليل البروتوكول الخفيف لتغيير بيانات الدليل (LDAP) لتخزين معلومات عن المستخدمين، فيمكنك تثبيت Cisco Unified Communications وتكوينه لاستخدام دليل LDAP الحالي لديك، وراجع إعداد دليل الشركة, في الصفحة 117. بعد تمكين حقل "تمكين المزامنة من خادم LDAP"، لن تتمكن من إضافة مزيد من المستخدمين من "إدارة Cisco Unified Communications Manager".

a) قم بتعيين حقلي "معرف المستخدم" و"الاسم الأخير".
b) قم بتعيين كلمة مرور (لمدخل Self Care).
c) قم بتعيين رمز تعريف شخصي (PIN) (لـ Cisco Extension Mobility و"الدليل الشخصي").

d) أقرن المستخدم بهاتف.

لإمداد المستخدمين بالتحكم في هاتفهم مثل توجيه المكالمات أو إضافة أرقام طلب سريع أو خدمات.

ملاحظة لا تشتمل بعض الهواتف، مثل تلك الموجودة في غرف المؤتمرات، على مستخدم مقترن.

الخطوة 15 (اختياري) أقرن مستخدمًا بمجموعة مستخدمين. حدد **إدارة المستخدم** > **إعدادات المستخدم** > **مجموعة التحكم في الوصول**.

لتعيين قائمة بأدوار المستخدمين وأذونهم يتم تطبيقها على جميع المستخدمين في إحدى مجموعات المستخدمين. يمكن للمسؤولين إدارة مجموعات المستخدمين وأدوارهم وأذونهم للتحكم في مستوى وصول (وبالتالي، مستوى أمان) مستخدمي النظام.

ولكي يتمكن المستخدمون النهائيون من الوصول إلى مدخل Cisco Unified Communications Self Care، يجب أن تضيف مستخدمين إلى مجموعة "المستخدمين النهائيين" القياسية لـ Cisco Unified Communications Manager.

موضوعات ذات صلة

التكوين الخاص بالمنتج, في الصفحة 93
ميزات وإعداد هاتف مؤتمر Cisco IP, في الصفحة 89
وثائق Cisco Unified Communications Manager, في الصفحة 14
إعداد قالب مفتاح مرن جديد, في الصفحة 90

تحديد عنوان MAC للهاتف

لإضافة هواتف إلى Cisco Unified Communications Manager، يجب أن تحدد عنوان MAC الخاص بهاتف.

اجراء

قم بتنفيذ أحد الإجراءات التالية:

- على الهاتف، حدد **إعدادات** > **معلومات الهاتف** وابحث عن حقل عنوان MAC.
- انظر إلى ملصق MAC الموجود على ظهر الهاتف.
- اعرض صفحة ويب الهاتف، وانقر فوق **معلومات الجهاز**.

أساليب إضافة الهاتف

بعد تثبيت هاتف Cisco IP ، يمكنك اختيار أحد الخيارات التالية لإضافة هواتف إلى قاعدة بيانات Cisco Unified Communications Manager.

- إضافة الهواتف كل على حدة باستخدام إدارة Cisco Unified Communications Manager
- إضافة هواتف متعددة باستخدام أداة الإدارة المجمّعة (BAT)
- التسجيل التلقائي
- أداة الإدارة المجمّعة (BAT) وأداة دعم الهواتف المسجلة تلقائيًا (TAPS)

قبل إضافة الهواتف كلٌ على حدة أو باستخدام BAT، تحتاج إلى عنوان MAC للهاتف. للحصول على مزيد من المعلومات، ارجع إلى تحديد عنوان MAC للهاتف, في الصفحة 57.

للحصول على مزيد من المعلومات حول أداة الإدارة المجمّعة، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14

إضافة هواتف بشكل فردي

قم بتجميع عنوان MAC ومعلومات الهاتف الخاصة بالهاتف الذي ستضيفه إلى Cisco Unified Communications Manager.

اجراء

الخطوة 1	في إدارة Cisco Unified Communications Manager، اختر **الجهاز** > **الهاتف**.
الخطوة 2	انقر فوق **ضف جديد**.
الخطوة 3	حدد نوع الهاتف.
الخطوة 4	حدد **Next (التالي)**.
الخطوة 5	أكمل المعلومات الخاصة بالهاتف والتي تشمل عنوان MAC. للحصول على تعليمات كاملة ومعلومات مفاهيمية حول Cisco Unified Communications Manager، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.
الخطوة 6	حدد **حفظ**.

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14

إضافة الهواتف باستخدام قالب هاتف BAT

تتيح لك أداة الإدارة المجمّعة (BAT) في Cisco Unified Communications إجراء عمليات تصحيح، بما في ذلك تسجيل هواتف متعددة.

لإضافة هواتف باستخدام BAT فقط (دون الاقتران بـ TAPS)، يجب الحصول على عنوان MAC المناسب لكل هاتف.

للحصول على مزيد من المعلومات حول استخدام BAT، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.

اجراء

الخطوة 1	من "إدارة Cisco Unified Communications Manager"، اختر **إدارة مجمّعة** > **الهواتف** > **قالب الهاتف**.
الخطوة 2	انقر فوق **ضف جديد**.
الخطوة 3	اختر "نوع هاتف" وانقر فوق **التالي**.
الخطوة 4	أدخل تفاصيل المعلمات الخاصة بالهاتف، مثل "مجمّع الأجهزة" و"قالب زر الهاتف" و"ملف تعريف أمان الجهاز".
الخطوة 5	انقر فوق **حفظ**.

الخطوة 6 حدد **جهاز** > **الهاتف** > **إضافة جديد** لإضافة هاتف باستخدام قالب هاتف BAT.

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14

إضافة مستخدمين إلى Cisco Unified Communications Manager

يمكنك عرض معلومات عن المستخدمين المسجلين في Cisco Unified Communications Manager والاحتفاظ بها. كما يسمح Cisco Unified Communications Manager أيضًا للمستخدمين بإجراء المهام التالية:

- الوصول إلى دليل الشركة والأدلة الأخرى المخصصة من هاتف Cisco IP .
- إنشاء دليل شخصي.
- إعداد أرقام الطلب السريع وإعادة توجيه المكالمات.
- الاشتراك في الخدمات التي يمكن الوصول إليها من هاتف Cisco IP .

اجراء

الخطوة 1 لإضافة المستخدمين بشكل فردي، راجع إضافة مستخدم مباشرةً إلى Cisco Unified Communications Manager, في الصفحة 60.

الخطوة 2 لإضافة المستخدمين في دفعات، استخدم أداة الإدارة المجمّعة. تتيح لك هذه الطريقة إمكانية تعيين كلمة مرور افتراضية متطابقة لجميع المستخدمين.

للحصول على مزيد من المعلومات، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14

إضافة مستخدم من "دليل LDAP خارجي"

إذا أضفت مستخدمًا إلى دليل LDAP (دليل غير تابع لخادم Cisco Unified Communications)، فيمكنك مزامنة دليل LDAP فورًا مع Cisco Unified Communications Manager الذي تضيف فيه المستخدم وهاتفه.

ملاحظة إذا لم تقم بمزامنة دليل LDAP مع Cisco Unified Communications Manager فورًا، فيحدد "جدول مزامنة دليل LDAP" الموجود في نافذة "دليل LDAP" وقت جدولة المزامنة التالية. يجب أن تحدث المزامنة قبل أن تتمكن من إقران مستخدم جديد بأحد الأجهزة.

اجراء

الخطوة 1 سجّل الدخول إلى إدارة Cisco Unified Communications Manager

الخطوة 2 حدد **النظام** > **LDAP** > **دليل LDAP**.

الخطوة 3 استخدم **بحث** لتحديد موقع دليل LDAP.

الخطوة 4 انقر فوق اسم دليل LDAP.

الخطوة 5 انقر فوق **إجراء مزامنة كاملة الآن**.

إضافة مستخدم مباشرةً إلى Cisco Unified Communications Manager

إذا كنت لا تستخدم دليل البروتوكول الخفيف لتغيير بيانات الدليل (LDAP)، فيمكنك إضافة مستخدم مباشرةً باستخدام إدارة Cisco Unified Communications Manager من خلال الخطوات التالية.

ملاحظة إذا تمت مزامنة LDAP، فتتعذر عليك إضافة مستخدم باستخدام إدارة Cisco Unified Communications Manager.

اجراء

الخطوة 1 من إدارة Cisco Unified Communications Manager، اختر **إدارة المستخدم** > **المستخدم النهائي**.

الخطوة 2 انقر فوق **ضف جديد**.

الخطوة 3 في جزء "معلومات المستخدم"، أدخل ما يلي:

- معرف المستخدم: أدخل اسم تعريف المستخدم النهائي. لا يسمح Cisco Unified Communications Manager بتعديل معرف المستخدم بعد إنشائه. يمكنك استخدام الأحرف الخاصة التالية: =, +, <, >, #,;, \,, "والمسافات الفارغة. **على سبيل المثال**: johndoe
- كلمة المرور وتأكيدها: أدخل خمسة أحرف أبجدية أو خاصة أو أكثر لكلمة مرور المستخدم النهائي. يمكنك استخدام الأحرف الخاصة التالية: =, +, <, >, #,;, \,, "والمسافات الفارغة.
- الاسم الأخير: ادخل الاسم الأخير للمستخدم النهائي. يمكنك استخدام الأحرف الخاصة التالية: =، +، <, >، #، ;, \، , "والمسافات الفارغة. **على سبيل المثال**: doe
- رقم الهاتف: أدخل رقم الدليل الأساسي للمستخدم النهائي. يمكن أن تتوفر لدى المستخدمين النهائيين خطوط متعددة على هواتفهم. **على سبيل المثال**: 26640 (رقم هاتف الشركة الداخلي لـ John Doe)

الخطوة 4 انقر فوق **حفظ**.

إضافة مستخدم إلى مجموعة مستخدمين نهائيين

لإضافة مستخدم إلى مجموعة المستخدم النهائي القياسي لـ Cisco Unified Communications Manager، قم بتنفيذ الخطوات التالية:

اجراء

الخطوة 1 من إدارة Cisco Unified Communications Manager، اختر **إدارة المستخدم** > **إعدادات المستخدم** > **مجموعة التحكم في الوصول**.

يتم عرض نافذة "بحث عن المستخدمين وسردهم".

الخطوة 2 أدخل معايير البحث المناسبة، ثم انقر فوق **بحث**.

الخطوة 3 حدد ارتباط **المستخدمين النهائيين لـ CCM القياسي**. تظهر نافذة "تكوين مجموعة المستخدمين" الخاصة بـ "المستخدمين النهائيين لـ CCM القياسي".

الخطوة 4 حدد **إضافة مستخدمين نهائيين إلى مجموعة**. تظهر نافذة "بحث عن المستخدمين وسردهم".

الخطوة 5 استخدم مربعات قائمة "البحث عن مستخدم" المنسدلة للبحث عن المستخدمين الذين تريد إضافتهم، وانقر فوق **بحث**.

تظهر قائمة بالمستخدمين مطابقة لمعايير البحث لديك.

الخطوة 6 في قائمة السجلات الظاهرة، انقر فوق خانة الاختيار بجوار المستخدمين الذين تريد إضافتهم إلى مجموعة المستخدمين هذه. إذا كانت القائمة طويلة، فاستخدم الارتباطات الموجودة في الجزء السفلي لإظهار المزيد من النتائج.

ملاحظة لا تعرض قائمة نتائج البحث المستخدمين الذين ينتمون بالفعل إلى مجموعة المستخدمين.

الخطوة 7 اختر **إضافة ما تم تحديده**.

إقران الهواتف بالمستخدمين

يمكنك إقران الهواتف بالمستخدمين من خلال نافذة المستخدم النهائي لـ Cisco Unified Communications Manager.

اجراء

الخطوة 1 من إدارة Cisco Unified Communications Manager، اختر **إدارة المستخدم** > **المستخدم النهائي**.

تظهر نافذة "بحث عن المستخدمين وسردهم".

الخطوة 2 أدخل معايير البحث المناسبة، ثم انقر فوق **بحث**.

الخطوة 3 في قائمة السجلات التي تظهر، حدد الارتباط للمستخدم.

الخطوة 4 حدد **إقران جهاز**.

تظهر نافذة "إقران جهاز المستخدم".

الخطوة 5 أدخل معايير البحث المناسبة، ثم انقر فوق **بحث**.

الخطوة 6 اختر الجهاز الذي تريد إقرانه بالمستخدم عن طريق تحديد خانة الاختيار الموجودة على يسار الجهاز.

الخطوة 7 اختر **حفظ المحدد/التغييرات** لإقران الجهاز بالمستخدم.

الخطوة 8 من القائمة المنسدلة للارتباطات ذات الصلة في الزاوية اليمنى العلوية من النافذة، حدد **رجوع إلى المستخدم**، ثم انقر فوق **انتقال**.

تظهر نافذة تكوين المستخدم النهائي ويتم عرض الأجهزة المقترنة التي اخترتها في جزء الأجهزة المتحكم بها.

الخطوة 9 اختر **حفظ المحدد/التغييرات**.

هتفية الموقع البعيد المتين

تضمن هاتفية الموقع البعيد المتين (SRST) استمرار قابلية الوصول إلى وظائف الهاتف الرئيسية عند انقطاع الاتصالات باستخدام Cisco Unified Communications Manager المتحكم. في هذا السيناريو، يمكن للهاتف إبقاء المكالمة قيد التقدم نشطة، ويمكن للمستخدم الوصول إلى مجموعة فرعية من الميزات المتوفرة. عند تجاوز الفشل، يتلقى المستخدم رسالة تنبيه على الهاتف.

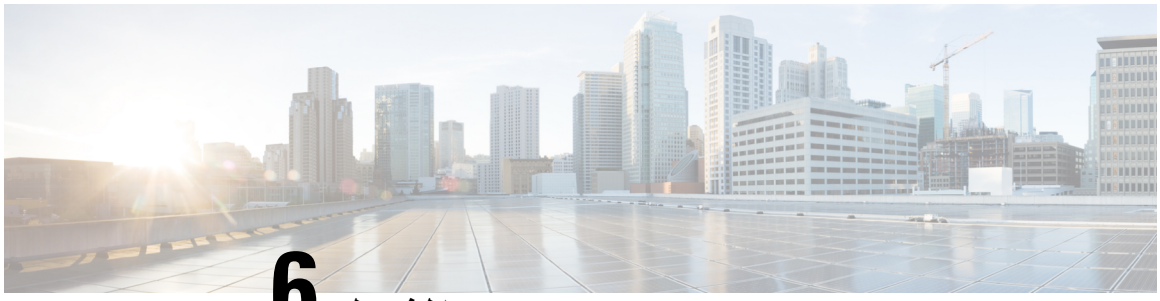
للحصول على معلومات حول SRST، راجع https://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/tsd-products-support-series-home.html

يصف الجدول التالي توفر الميزات أثناء تجاوز الفشل.

الجدول *14*: دعم ميزة *SRST*

الميزة	مدعوم	ملاحظات
مكالمة جديدة	نعم	
إنهاء المكالمة	نعم	
إعادة الطلب	نعم	
رد	نعم	
انتظار	نعم	
متابعة	نعم	
اتصال جماعي	نعم	3 أطراف فقط وخلط محلي فقط.
قائمة المؤتمر	لا	
التحويل	نعم	التشاور فقط.
التحويل إلى المكالمات النشطة (تحويل مباشر)	لا	
الرد الآلي	نعم	
انتظار المكالمات	نعم	
معرف المتصل	نعم	
عرض جلسة موحدة	نعم	المؤتمر هو الميزة الوحيدة المدعومة بسبب القيود على الميزات الأخرى.
البريد الصوتي	نعم	لن تتم مزامنة البريد الصوتي مع المستخدمين الآخرين في نظام مجموعة Cisco Unified Communications Manager.
إعادة توجيه كل المكالمات	نعم	لا تتوفر حالة إعادة التوجيه إلا على الهاتف الذي يعين إعادة التوجيه نظرًا لعدم ظهور الخط المشترك في وضع SRST. لا يتم حفظ جميع إعدادات إعادة توجيه مكالمة عند تجاوز الفشل إلى SRST من Cisco Unified Communications Manager أو من إرجاع موارد SRST إلى مدير الاتصالات. يجب الإشارة إلى أي عملية إعادة توجيه مكالمة أصلية لا تزال نشطة على مدير الاتصالات عندما يعيد الجهاز الاتصال بمدير الاتصالات بعد تجاوز الفشل.
الطلب السريع	نعم	
إلى البريد الصوتي (iDivert)	لا	لم يتم عرض مفتاح iDivert المرن.
عوامل تصفية الخط	متوسطة	يتم دعم الخطوط لكن لا يمكن مشاركتها.

الميزة	مدعوم	ملاحظات
رصد التعليق	لا	لم يتم عرض المفتاح المرن للتعليق.
إشارة انتظار الرسالة المعززة	نعم	تظهر شارات عدد الرسائل على شاشة الهاتف.
تعليق مكالمة موجهة	لا	لم يتم عرض المفتاح المرن.
سحب بعد الانتظار	نعم	
الانتظار البعيد	لا	تظهر المكالمات كمكالمات انتظار محلية.
مباشر	لا	لم يتم عرض المفتاح المرن لميزة الاتصال المباشر.
التقاط	نعم	
التقاط مكالمة مجموعة	لا	لم يتم عرض المفتاح المرن.
التقاط آخر	لا	لم يتم عرض المفتاح المرن.
معرف مكالمة ضارة	نعم	
تبليغ	نعم	
مجموعة بحث	لا	لم يتم عرض المفتاح المرن.
إمكانية التنقل بالأجهزة	لا	لم يتم عرض المفتاح المرن.
خصوصية	لا	لم يتم عرض المفتاح المرن.
معاودة الاتصال	لا	لم يتم عرض المفتاح المرن لمعاودة الاتصال.
URL للخدمة	نعم	لا يتم عرض مفتاح الخط القابل للبرمجة مع عنوان URL معين للخدمة.



الفصل 6

إدارة مدخل Self Care

نظرة عامة على مدخل Self Care

من مدخل Cisco Unified Communications Self Care، يمكن للمستخدمين تخصيص ميزات الهاتف وإعداداته والتحكم فيها.

وبصفتك المسؤول، تتحكم في إمكانية الوصول إلى "مدخل Self Care". يجب أيضًا أن توفر المعلومات للمستخدمين، وذلك لكي يتسنى لهم الوصول إلى "مدخل Self Care".

قبل أن يتمكن المستخدم من الوصول إلى مدخل العناية الذاتية، يجب عليك استخدام إدارة Cisco Unified Communications Manager لإضافة المستخدم إلى مجموعة Cisco Unified Communications Managerالمستخدم النهائي القياسية.

يجب أن تمد المستخدمين النهائيين بالمعلومات التالية حول "مدخل Self Care":

- عنوان URL اللازم للوصول إلى التطبيق. URL هذا هو:

  `https://<server_name:portnumber>/ucmuser/`، حيث يشير server_name إلى المضيف الذي يتم تثبيت خادم الويب عليه، كما يشير portnumber إلى رقم المنفذ على هذا المضيف.

- معرف المستخدم وكلمة مروره الافتراضية للوصول إلى التطبيق.
- نظرة عامة على المهام التي يمكن للمستخدمين إنجازها بهذا المدخل.

تتوافق هذه الإعدادات مع القيم التي أدخلتها عند إضافة المستخدم إلى Cisco Unified Communications Manager.

للحصول على مزيد من المعلومات، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.S

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14

إعداد وصول المستخدم إلى مدخل Self Care

قبل أن يتمكن المستخدم من الوصول إلى مدخل Self Care، يجب أن تمنحه تفويضًا بالوصول.

اجراء

الخطوة 1	في Cisco Unified Communications Manager الإدارة، حدد **إدارة المستخدم** > **المستخدم النهائي**.
الخطوة 2	ابحث عن المستخدم.
الخطوة 3	انقر فوق ارتباط معرف المستخدم.
الخطوة 4	تأكد من أن المستخدم لديه كلمة مرور ورمز تعريف شخصي مكونان.
الخطوة 5	في قسم معلومات الإذن، تأكد من أن قائمة المجموعات تتضمن **المستخدمين النهائيين لـ CCM القياسي**.
الخطوة 6	حدد **حفظ**.

تخصيص "شاشة بوابة مدخل Self Care"

يتم عرض معظم الخيارات على "مدخل Self Care". ومع ذلك، يجب أن تعين الخيارات التالية باستخدام إعدادات "تهيئة معلمات المؤسسة" في إدارة Cisco Unified Communications Manager:

- إظهار إعدادات الرنين
- إظهار إعدادات تسمية الخط

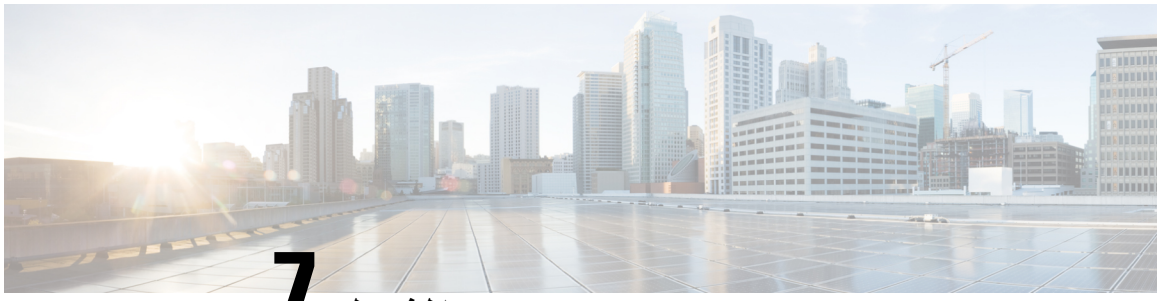
ملاحظة تنطبق الإعدادات على جميع صفحات "مدخل Self Care" في موقعك.

اجراء

الخطوة 1	في إدارة Cisco Unified Communications Manager، حدد **النظام** > **معلمات المؤسسة**.
الخطوة 2	في منطقة "مدخل Self Care"، قم بتعيين **الخادم الافتراضي لمدخل Self Care** في الحقل المحدد له.
الخطوة 3	قم بتمكين أو تعطيل المعلمات التي يمكن للمستخدمين الوصول إليها في المدخل.
الخطوة 4	حدد **حفظ**.

الجزء III

إدارة هاتف مؤتمر Cisco IP



الفصل 7

تخصيص أمان هاتف مؤتمر Cisco IP

نظرة عامة على أمان هاتف Cisco IP

تعمل ميزات الأمان على الحماية من العديد من التهديدات، بما في ذلك التهديدات التي تستهدف هوية الهاتف والبيانات. وتنشئ هذه الميزات تدفقات اتصال مصادقة وتحافظ على وجودها بين الهاتف وخادم Cisco Unified Communications Manager، كما تضمن أن الهاتف لا يستخدم سوى الملفات الموقعة توقيعًا رقميًا فقط.

يشتمل الإصدار 8.5(1) والإصدارات الأحدث لـ Cisco Unified Communications Manager على "الأمان بشكل افتراضي"، مما يوفر ميزات الأمان التالية لهواتف Cisco IP دون تشغيل عميل CTL:

- توقيع ملفات تكوين الهاتف
- تشفير ملف تكوين الهاتف
- بروتوكول HTTPS المزود بخدمة Tomcat وغيرها من الخدمات

ملاحظة لا تزال ميزات إرسال الإشارات والوسائط الآمنة تتطلب منك تشغيل عميل CTL واستخدام رموز eTokens للأجهزة.

للحصول على مزيد من المعلومات حول ميزات الأمان، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.

يتم تثبيت الشهادة المهمة محليًا (LSC) على الهواتف بعد تنفيذ المهام الضرورية المقترنة بوظيفة وكيل جهة منح الشهادات (CAPF). يمكنك استخدام "إدارة Cisco Unified Communications Manager لتكوين LSC. للحصول على مزيد من المعلومات، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.

لا يمكن استخدام LSC كشهادة المستخدم لـ EAP-TLS مع مصادقة الشبكة المحلية اللاسلكية.

أو يمكنك تكوين تثبيت شهادة هامة محليًا (LSC) من قائمة الأمان/إعداد على الهاتف. تتيح لك هذه القائمة أيضًا تحديث LCS أو إزالتها.

تتوافق سلسلة هاتف مؤتمر Cisco IP 8832 مع المقياس الفيدرالي لمعالجة المعلومات (FIPS). وليعمل وضع FIPS على نحوٍ صحيح، يتطلب وجود مفتاح RSA بحجم مقداره 2048 بت أو أكبر. إذا كان حجم شهادة خادم RSA دون 2048 بت أو أكبر، فلن يتم تسجيل الهاتف باستخدام Cisco Unified Communications Manager و يفشل تسجيل الهاتف. حجم المفتاح في الشهادة غير متوافق مع FIPS ويُعرض في رسائل حالة الهاتف.

لا يمكنك استخدام مفاتيح خاصة (LSC أو MIC) في وضع FIPS

إذا كان الهاتف يحتوي على شهادة LSC أصغر من 2048 بت، فإنك تحتاج إلى تحديث حجم مفتاح LSC إلى 2048 بت أو أكثر قبل تمكين FIPS.

موضوعات ذات صلة

إعداد شهادة هامة محليًا, في الصفحة 73
وثائق Cisco Unified Communications Manager, في الصفحة 14

تحسينات أمان شبكة هاتفك

يمكنك تمكين الإصدارين 11.5(1) و12.0(1) من Cisco Unified Communications Manager للعمل في بيئة أمان محسّنة. ومن خلال هذه التحسينات، تعمل شبكة الهاتف لديك بموجب مجموعة من الضوابط الصارمة لإدارة الأمان والمخاطر لحمايتك وحماية المستخدمين لديك.

لا يدعم الإصدار 12.5(1) من Cisco Unified Communications Manager بيئة أمان متقدمة. قم بتعطيل FIPS قبل الترقية إلى الإصدار 12.5(1) من Cisco Unified Communications Manager أو TFTP ولن تعمل الخدمات الأخرى بشكل مناسب.

تتضمن بيئة الأمان المحسنة الميزات التالية:

- مصادقة البحث عن جهة اتصال.
- استخدام TCP كبروتوكول افتراضي لإنشاء سجلات التدقيق عن بُعد.
- وضع FIPS.
- سياسة بيانات اعتماد محسّنة.
- دعم مجموعة تجزئات "خوارزمية التجزئة الآمنة 2" للتوقيعات الرقمية.
- دعم مفتاح RSA بحجمي 512 و4096 بت.

باستخدام 14.0 إصدار Cisco لمدير الاتصالات الموحدة من Cisco وإصدار البرامج الثابتة لهاتف Cisco IP 14.0 والإصدارات الأحدث، تدعم الهواتف مصادقة SIP OAuth.

تم دعم OAuth لـ "بروتوكول نقل الملفات المبسط" (TFTP) باستخدام Cisco Unified Communications Manager الإصدار 14.0(1)SU1 أو إصدار أحدث، و"إصدار البرنامج الثابت لهاتف 14.1(1) "Cisco IP). لا يتم دعم TFTP الخاص بالوكيل وOAuth لـ TFTP الخاص بالوكيل في "الوصول المتنقل عن بُعد" (MRA).

للحصول على مزيد من المعلومات حول الأمان، راجع ما يلي:

- دليل تكوين النظام لإدارة الاتصالات الموحدة من *Cisco*، والإصدار 14.0(1) أو إصدار أحدث (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html).
- دليل أمان *Cisco Unified Communications Manager* (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html)
- SIP OAuth: دليل تهيئة الميزات لبرنامج *Cisco Unified Communications Manager* (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html)

ملاحظة يمكن لهاتف Cisco IP تخزين عدد محدود فقط من ملفات قائمة الثقة لتحديد الهويات (ITL). يلزمك تحدلا يمكن أن تتجاوز ملفات ITL حد K46 على الهاتف لذا قم بتحديد عدد الملفات التي يقوم Cisco Unified Communications Manager بإرسالها إلى الهاتف.

ميزات الأمان المدعومة

تعمل ميزات الأمان على الحماية من العديد من التهديدات، بما في ذلك التهديدات التي تستهدف هوية الهاتف والبيانات. وتنشئ هذه الميزات تدفقات اتصال مصادقة وتحافظ على وجودها بين الهاتف وخادم Cisco Unified Communications Manager، كما تضمن أن الهاتف لا يستخدم سوى الملفات الموقعة توقيعًا رقميًا فقط.

يشتمل الإصدار 8.5(1) والإصدارات الأحدث لـ Cisco Unified Communications Manager على "الأمان بشكل افتراضي"، مما يوفر ميزات الأمان التالية لهواتف Cisco IP دون تشغيل عميل CTL:

- توقيع ملفات تكوين الهاتف
- تشفير ملف تكوين الهاتف
- بروتوكول HTTPS المزود بخدمة Tomcat وغيرها من الخدمات

ملاحظة لا تزال ميزات إرسال الإشارات والوسائط الآمنة تتطلب منك تشغيل عميل CTL واستخدام رموز eTokens للأجهزة.

تطبيق الأمان في نظام Cisco Unified Communications Manager يمنع سرقة الهوية من الهاتف وخادم Cisco Unified Communications Manager ويمنع التلاعب في البيانات ومنع إشارات المكالمة والتلاعب بدفق الوسائط.

للحد من هذه التهديدات، بشبكة هاتفية IP من Cisco يقوم بتحديد والحفاظ عليه تدفقات الاتصال (مشفرة) أمن بين هاتف والخادم رقمياً توقيع ملفات قبل تحويلها إلى هاتف وتشفير المكالمة إرسال الإشارات بين "هواتف Cisco IP " وعمليات دفق الوسائط.

يتم تثبيت الشهادة المهمة محليًا (LSC) على الهواتف بعد تنفيذ المهام الضرورية المقترنة بوظيفة وكيل جهة منح الشهادات (CAPF). يمكنك استخدام إدارة Cisco Unified Communications Manager لتكوين LSC، كما هو موضح في دليل أمان Cisco Unified Communication Manager. أو يمكنك تكوين تثبيت شهادة هامة محليًا (LSC) من قائمة الأمان/إعداد على الهاتف. تتيح لك هذه القائمة أيضًا تحديث LCS أو إزالتها.

لا يمكن استخدام LSC كشهادة المستخدم لـ EAP-TLS مع مصادقة الشبكة المحلية اللاسلكية.

يستخدم الهاتف ملف تعريف أمان الهاتف الذي يحدد ما إذا كان الجهاز آمنًا أم لا. للحصول على معلومات حول تكوين ملف تعريف الأمان وتطبيق ملف التعريف على الهاتف، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.

إذا قمت بتكوين إعدادات متعلقة بالأمان في إدارة Cisco Unified Communications Manager، فيحتوي ملف تكوين الهاتف على معلومات مهمة. للتأكد من خصوصية ملف التكوين، يجب عليك تكوينه للتشفير. للحصول على مزيد من المعلومات، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.

تطبيق الأمان في نظام Cisco Unified Communications Manager يمنع سرقة الهوية من الهاتف وخادم Cisco Unified Communications Manager ويمنع التلاعب في البيانات ومنع إشارات المكالمة والتلاعب بدفق الوسائط.

يقدم الجدول التالي نظرة عامة على ميزات الأمان التي يدعمها هاتف مؤتمر Cisco IP 8832. للحصول على مزيد من المعلومات هذه الميزات، وCisco Unified Communications Manager وأمان هاتف Cisco IP ، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.

الجدول *15*: نظرة عامة على ميزات الأمان

الميزة	الوصف
مصادقة الصور	تمنع الملفات الثنائية الموقعة (التي تحمل الامتداد .sbn) العبث بنسخة البرامج الجديدة.
تثبيت شهادة موقع العميل	يحتاج كل هاتف إلى شهادة فريدة لمصادقة الجهاز. تشتمل الهواتف على شهاد Unified Communications Manager أن يتم تثبيت الشهادة باستخدام و تكوين الأمان على الهاتف.
مصادقة الجهاز	تحدث بين خادم Cisco Unified Communications Manager والهات وCisco Unified Communications Manager؛ وإذا لزم الأمر، تُنشئ م Manager الهواتف إلا إذا كان يمكن مصادقتها من خلال tions Manager
مصادقة الملف	تتحقق من صحة الملفات الموقعة رقميًا التي ينزلها الهاتف. يتحقق الهاتف من ذاكرة Flash على الهاتف. يرفض الهاتف هذه الملفات دون إجراء معالجة إ
مصادقة إرسال الإشارات	تستخدم بروتوكول TLS للتحقق من عدم حدوث عبث بحزم إرسال الإشارات
شهادة التصنيع المثبتة	يشتمل كل هاتف على شهادة تصنيع مثبتة (MIC)، يتم استخدامها لمصادقة الج Manager بمصادقة الهاتف.
مرجع SRST آمن	بعد تكوين مرجع SRST للأمان، ثم إعادة تعيين الأجهزة التابعة في إدارة er cnf.xml بالهاتف ويرسل الملف إلى الهاتف. ثم يستخدم الهاتف الآمن بعد ذل
تشفير الوسائط	يستخدم SRTP للتأكد من أن عمليات دفق الوسائط بين الأجهزة المعتمدة تُثبت رئيسية للأجهزة، وتسليم المفاتيح للأجهزة، وتأمين عملية تسليم المفاتيح أثناء
CAPF (وظيفة وكيل جهة منح الشهادات)	تنفذ أجزاء من إجراء إنشاء الشهادات التي تتسم بكثافة المعالجة إلى حد كبير منح الشهادات الخاصة بالعميل بالنيابة عن الهاتف، أو يمكن تكوينها لإنشاء ال
ملفات تعريف الأمان	تحدد ما إذا كان الهاتف غير آمن أو مصادقًا أو مشفرًا.
ملفات التكوين المشفرة	تتيح لك التأكد من خصوصية ملفات تكوين الهاتف.
التعطيل الاختياري لوظائف خادم الويب بالهاتف	يمكنك منع الوصول إلى صفحة ويب الهاتف، التي تعرض مجموعة متنوعة
زيادة حماية الهاتف	خيارات الأمان الإضافية التي يمكنك التحكم بها من خلال إدارة s Manager • تعطيل الوصول إلى صفحات الويب للهاتف **ملاحظة** يمكنك عرض الإعدادات الحالية لـ GARP الممكن، وخيار
مصادقة X802.1	يمكن للهاتف استخدام مصادقة X802.1 لطلب الوصول إلى الشبكة والحصو

الميزة	الوصف
تشفير AES 256	عند الاتصال بإصدار Cisco Unified Communications Manager رقم 5 وتشفير الوسائط. وهذا يتيح للهواتف إمكانية بدء اتصالات TLS 1.2 ودعمها باست والمطابقة للمقاييس الفيدرالية لمعالجة المعلومات (FIPS). التشفيرات الجديدة هي • بالنسبة لاتصالات TLS: • S_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • S_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • بالنسبة لـ sRTP: • AEAD_AES_256_GCM • AEAD_AES_128_GCM للحصول على مزيد من المعلومات، راجع وثائق mmunications Manager
شهادات خوارزمية التوقيع الرقمي لمنحنى إهليلجي (ECDSA)	كجزء من شهادة "المعيار العام" (CC)، قام d Communications Manager من الإصدار 11.5 من nications Manager (Operating System (VOS

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14

إعداد شهادة هامة محليًا

تنطبق هذه المهمة على إعداد LSC بأسلوب سلسلة مصادقة.

قبل البدء

تأكد من اكتمال تكوينات الأمان المناسبة في Cisco Unified Communications Manager ووظيفة وكيل جهة منح الشهادات (CAPF):

- يشتمل ملف CTL أو ITL على شهادة CAPF.
- في إدارة تشغيل Cisco Unified Communications، تحقق من تثبيت شهادة CAPF.
- وظيفة وكيل جهة منح الشهادات (CAPF) قيد التشغيل وتم تكوينها.

للحصول على مزيد من المعلومات حول هذه الإعدادات، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.

اجراء

الخطوة 1 احصل على رمز مصادقة CAPF الذي تم تعيينه عند تكوين CAPF.

الخطوة 2 من الهاتف، اختر **الإعدادات**.

الخطوة 3 اختر **إعدادات المسؤول** > **إعداد الأمان**.

ملاحظة يمكنك التحكم في الوصول إلى قائمة "إعدادات" باستخدام حقل "الوصول إلى الإعدادات" في نافذة تكوين الهاتف عبر إدارة Cisco Unified Communications Manager.

الخطوة 4 اختر LSC واضغط على **تحديد** أو **تحديث**.

يطالب الهاتف بسلسلة مصادقة.

الخطوة 5 أدخل رمز المصادقة واضغط على **إرسال**.

يبدأ الهاتف في تثبيت LSC أو تحديثها أو إزالتها، وذلك بناءً على الكيفية التي تم بها تكوين CAPF. أثناء الإجراء، تظهر سلسلة من الرسائل في حقل خيار LSC داخل قائمة "تكوين الأمان"، حيث يمكنك مراقبة التقدم. عند اكتمال الإجراء، يتم عرض "تم التثبيت" أو "لم يتم التثبيت" على شاشة الهاتف.

قد يستغرق اكتمال عملية تثبيت LSC أو تحديثها أو إزالتها وقتًا طويلاً.

عند نجاح إجراء التثبيت على الهاتف، يتم عرض رسالة تم التثبيت على شاشة الهاتف. إذا ظهرت على شاشة الهاتف رسالة لم يتم التثبيت، فقد تكون سلسلة التفويض غير صحيحة أو قد يكون الهاتف غير ممكّن للترقية. إذا أدى تشغيل CAPF إلى حذف LSC، فتعرض شاشة الهاتف رسالة لم يتم التثبيت للإشارة إلى نجاح عملية التشغيل. يسجل خادم CAPF رسائل الأخطاء. راجع وثائق خادم CAPF لتحديد موقع السجلات ولفهم معنى رسائل الأخطاء.

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14

تمكين وضع FIPS

اجراء

الخطوة 1 في "إدارة Cisco Unified Communications Manager"، حدد **الجهاز** > **الهاتف** وحدد موقع الهاتف.

الخطوة 2 انتقل إلى منطقة "التكوين الخاص بالمنتج".

الخطوة 3 قم بتعيين حقل **وضع FIPS** إلى "ممكّن".

الخطوة 4 حدد **تطبيق التكوين**.

الخطوة 5 حدد **حفظ**.

الخطوة 6 أعِد تشغيل الهاتف.

أمان المكالمات الهاتفية

عندما يتم تطبيق الأمان على الهاتف، يمكنك تحديد المكالمات الهاتفية الآمنة عن طريق الأيقونات التي تظهر على شاشة الهاتف. يمكنك أيضًا تحديد ما إذا كان الهاتف المتصل آمنًا ومحميًا أم لا إذا تم إصدار نغمة أمان في بداية المكالمة.

في المكالمة الآمنة، يتم تشفير جميع إشارات المكالمة وعمليات دفق الوسائط. تقدم المكالمة الآمنة مستوى عاليًا من الأمان، وتوفر السلامة والخصوصية للمكالمة. عندما تكون المكالمة الجارية مشفرة، تتغير أيقونة تقدم المكالمة الموجودة على يمين مؤقت مدة المكالمة على شاشة الهاتف إلى الأيقونة التالية: .

ملاحظة إذا تم توجيه المكالمة من خلال اتجاهات المكالمة غير IP، على سبيل المثال، PSTN، فقد تصبح المكالمة غير آمنة حتى وإن كانت مشفرة داخل شبكة IP ولها أيقونة قفل مقترنة بها.

في المكالمة الآمنة، يتم إصدار نغمة أمان في بداية المكالمة للإشارة إلى أن الهاتف الآخر المتصل يتلقى ويستقبل صوت الأمان. وعند اتصال مكالمتك بهاتف غير آمن، لا يتم تشغيل نغمة الأمان.

ملاحظة المكالمات الآمنة مدعومة بين هاتفين. يمكن تكوين المؤتمر الآمن وCisco Extension Mobility والخطوط المشتركة من خلال جسر المؤتمر الآمن.

عندما يتم تكوين الهاتف في حالة الأمان (مشفر وموثوق) في Cisco Unified Communications Manager، يمكن منحه حالة "محمي". بعد ذلك، يمكن تكوين الهاتف المحمي لتشغيل نغمة الإيضاح في بداية المكالمة إذا كنت ترغب في ذلك:

- الجهاز المحمي: لتغيير حالة الهاتف الآمن إلى محمي، حدد خانة الاختيار "جهاز محمي" في نافذة تكوين الهاتف في إدارة Cisco Unified Communications Manager (**الجهاز** > **الهاتف**).
- تشغيل نغمة إيضاح الأمان: لتمكين الهاتف المحمي لتشغيل نغمة إيضاح الأمان أو عدم الأمان، قم بتعيين إعداد تشغيل نغمة إيضاح الأمان على "صواب". بشكل افتراضي، يتم تعيين إعداد تشغيل نغمة إيضاح الأمان على "خطأ". يمكنك تعيين هذا الخيار في إدارة Cisco Unified Communications Manager (**النظام** > **معلمات الخدمة**). حدد الخادم ثم خدمة Cisco Unified Communications Manager. في نافذة تكوين معلمة الخدمة، حدد الخيار الموجود في منطقة ميزة - نغمة الأمان. الوضع الافتراضي هو "خطأ".

تعريف مكالمة المؤتمر الآمنة

يمكنك بدء مكالمة مؤتمر آمنة ومراقبة مستوى أمان المشاركين. يتم تأسيس مكالمة مؤتمر آمنة باستخدم هذه العملية:

1. يبدأ المستخدم في إجراء مكالمة مؤتمر من هاتف آمن.
2. يُعيّن Cisco Unified Communications Manager جسر مؤتمر آمنًا للمكالمة.
3. بعد إضافة المشاركين، يتحقق Cisco Unified Communications Manager من وضع الأمان لكل هاتف ويحافظ على مستوى أمان المؤتمر.
4. يعرض الهاتف مستوى أمان مكالمة المؤتمر. يعرض المؤتمر الآمن أيقونة الأمان على يمين **المؤتمر** على شاشة الهاتف.

ملاحظة المكالمات الآمنة مدعومة بين هاتفين. في الهواتف المحمية، لا تتوفر بعض الميزات، مثل مكالمات المؤتمر والخطوط المشتركة وExtension Mobility، عندما يكون الاتصال الآمن مكونًا.

يقدم الجدول التالي معلومات حول التغييرات التي تطرأ على مستويات أمان المؤتمر تبعًا لمستوى أمان الهاتف المُنشئ، ومستويات أمان المشاركين، وتوفر جسور مؤتمر آمنة.

الجدول *16*: قيود الأمان مع مكالمات المؤتمر

مستوى أمان هاتف المنشئ	الميزة المستخدمة	مستوى أمان المشاركين	نتائج الإجراء
غير آمن	اتصال جماعي	اتصال	جسر مؤتمر غير آمن مؤتمر غير آمن
اتصال	اتصال جماعي	عضو واحد على الأقل غير آمن.	جسر مؤتمر آمن مؤتمر غير آمن

مستوى أمان هاتف المنشئ	الميزة المستخدمة	مستوى أمان المشاركين	نتائج الإجراء
اتصال	اتصال جماعي	اتصال	جسر مؤتمر آمن مؤتمر بمستوى تشفير آمن
غير آمن	مباشر	مستوى الأمان الأدنى مشفّر.	يتلقى المنشئ رسالة لا تفي بمستوى الأمان، تم رف
اتصال	مباشر	مستوى الأمان الأدنى غير آمن.	جسر مؤتمر آمن مؤتمر يقبل جميع المكالمات.

تعريف المكالمة الهاتفية الآمنة

يتم تأسيس مكالمة آمنة عند تكوين هاتفك وهاتف الطرف الآخر لإجراء مكالمة آمنة. قد يكون هاتف الطرف الآخر على شبكة Cisco IP نفسها أو على شبكة خارج شبكة IP. يمكن إجراء المكالمات المؤمنة بين هاتفين فقط. من المفترض أن تدعم مكالمات المؤتمر ميزة المكالمة الآمنة بعد إعداد جسر المؤتمر الآمن.

يتم تأسيس المكالمة المؤمنة باستخدام هذه العملية:

1. يشرع المستخدم في إجراء مكالمة من هاتف مؤمن (وضع الأمان الآمن).
2. يعرض الهاتف أيقونة الأمان على شاشة الهاتف. تشير هذه الأيقونة إلى أنه قد تم تكوين الهاتف لإجراء مكالمات آمنة، ولكن هذا لا يعني أن الهاتف الآخر المتصل مؤمن أيضًا.
3. يسمع المستخدم نغمة أمان عند اتصال المكالمة بهاتف آخر مؤمن، مشيرًا إلى أن هاتفي كلا طرفي المحادثة مشفّران ومؤمّنان. وعند اتصال المكالمة بهاتف غير آمن، فإن المستخدم لا يسمع نغمة الأمان.

ملاحظة المكالمات الآمنة مدعومة بين هاتفين. في الهواتف المحمية، لا تتوفر بعض الميزات، مثل مكالمات المؤتمر والخطوط المشتركة وExtension Mobility، عندما يكون الاتصال الآمن مكونًا.

الهواتف المحمية فقط هي التي تُصدر نغمات إيضاح الأمان أو عدم الأمان. ولا تُصدر الهواتف غير المحمية هذه النغمات مطلقًا. إذا تغيرت حالة المكالمة العامة أثناء المكالمة، تتغير نغمة الإيضاح ويُصدر الهاتف النغمة الملائمة.

يُصدر الهاتف المحمي نغمة أم لا في هذه الحالات:

- عند تمكين خيار نغمة إيضاح التشغيل الآمن:
- عندما يتم تأسيس وسائط أمان طرف إلى طرف وكانت حالة المكالمة آمنة، يُصدر الهاتف نغمة إيضاح الأمان (ثلاث صافرات طويلة يتخللها إيقاف مؤقت).
- عندما يتم تأسيس وسائط غير آمنة من طرف إلى طرف وكانت حالة المكالمة غير آمنة، يُصدر الهاتف نغمة إيضاح عدم الأمان (ست صافرات قصيرة يتخللها إيقاف مؤقت قصير).

عند تعطيل خيار نغمة إيضاح التشغيل الآمن، لا يتم إصدار أي نغمة.

توفير التشفير للمداخلة

يتحقق Cisco Unified Communications Manager من حالة أمان الهاتف عندما يتم إنشاء المؤتمرات وتغيير إيضاح الأمان للمؤتمر أو يحظر إتمام المكالمة للحفاظ على تكامل والأمان في النظام.

لا يمكن لمستخدم إجراء مداخلة في مكالمة مشفرة إذا لم يتم تكوين الهاتف الذي يتم استخدامه للمداخلة أثناء التشفير. عند فشل المداخلة في هذه الحالة، يتم طلب (انشغال سريعة) تشغيل نغمة على الهاتف الذي بدأ فيه دخول المداخلة.

إذا تم تكوين الهاتف المنشئ للتشفير، فيمكن إدخال منشئ المداخلة في مكالمة غير آمنة من الهاتف المشفر. بعد حدوث المداخلة، يصنف Cisco Unified Communications Manager الاتصال بأنه غير آمن.

إذا تم تكوين الهاتف المنشئ للتشفير، فيمكنك إدخال منشئ المداهلة في مكالمة مشفرة، ويشير الهاتف إلى أن المكالمة مشفرة.

أمان WLAN

نظرًا لإمكانية تلقي جميع أجهزة الشبكة المحلية اللاسلكية الواقعة ضمن النطاق كل حركة مرور الشبكة المحلية اللاسلكية الأخرى، فإن تأمين الاتصالات الصوتية أصبح يمثل عنصرًا مهمًا في الشبكات المحلية اللاسلكية. للتأكد من عدم اعتراض المقتحمين لحركة مرور الصوت، تدعم بنية أمان Cisco SAF هاتف Cisco IP ونقاط الاتصال Cisco Aironet الموجودة. للحصول على مزيد من المعلومات حول الأمان في الشبكات، راجع http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html.

يوفر حل الاتصال الهاتفي اللاسلكي Cisco Wireless IP أمان الشبكة اللاسلكية التي تمنع حالات تسجيل الدخول غير المصرح بها واختراق الاتصالات باستخدام طرق المصادقة التالية التي تدعم هاتف Cisco IP اللاسلكي:

- المصادقة المفتوحة: يمكن لأي جهاز لاسلكي طلب المصادقة في نظام مفتوح. يمنح AP الذي يتلقى الطلب المصادقة لأي طالب أو للطالبين الموجودين في قائمة المستخدمين. قد يكون الاتصال بين الأجهزة اللاسلكية ونقطة الوصول غير مشفر أو يمكن أن تستخدم الأجهزة مفاتيح خصوصية مكافئة سلكية (WEP) لتوفير الأمان. لا تحاول الأجهزة التي تستخدم WEP سوى المصادقة بواسطة AP الذي يستخدم WEP.
- المصادقة المرنة لبروتوكول المصادقة القابل للتوسعة عبر مصادقة "تفريعة آمنة" (EAP-FAST): تعمل بنية الأمان لخادم العميل هذه على تشفير معاملات EAP داخل نفق أمان مستوى نقل (TLS) بين AP وخادم RADIUS، مثل خادم التحكم في الوصول من Cisco (ACS).

  يستخدم نفق TLS بيانات اعتماد الوصول المحمية (PACs) للمصادقة بين العميل (هاتف) وخادم RADIUS. يرسل الخادم معرف المرجع (AID) إلى العميل (هاتف)، الذي بدوره يحدد PAC الملائم. يعيد العميل (هاتف) PAC-Opaque إلى خادم RADIUS. يلغي الخادم تشفير PAC باستخدام المفتاح الرئيسي. تحتوي نقطتا النهاية الآن على مفتاح PAC ويتم إنشاء نفق TLS. يدعم EAP-FAST توفير PAC تلقائي، ولكن يجب عليك تمكينه على خادم RADIUS.

ملاحظة في Cisco ACS، ووفقًا للإعدادات الافتراضية، تنتهي صلاحية PAC في غضون أسبوع واحد. إذا كان الهاتف يشتمل على PAC منتهية الصلاحية، فتستغرق عملية المصادقة على خادم RADIUS وقتًا أطول مقارنة بوجود PAC جديدة في الهاتف. لتجنب التأخير في توفير PAC، قم بتعيين مدة انتهاء الصلاحية لـ PAC حتى 90 يومًا أو أكثر على ACS أو خادم RADIUS.

- "بروتوكول المصادقة" القابل للتوسعة عبر "أمان طبقة النقل" (EAP-TLS): يتطلب EAP TLS شهادة عميل للمصادقة والوصول إلى الشبكة. بالنسبة لبروتوكول EAP-TLS السلكي، يمكن أن تكون شهادة العميل إما MIC أو LSC للهاتف. LSC هي شهادة مصادقة العميل المفضلة لبروتوكول EAP-TLS السلكي.
- بروتوكول المصادقة القابل للتوسعة المحمي (PEAP): نظام مصادقة متبادل يستند إلى كلمة مرور ملك Cisco بين العميل (هاتف) وخادم RADIUS. يمكن لهاتف Cisco IP استخدام PEAP للمصادقة في الشبكة اللاسلكية. يقتصر الدعم على PEAP-MSCHAPV2 فقط. PEAP-GTC غير مدعوم.

تستخدم أنظمة المصادقة التالية خادم RADIUS لإدارة مفاتيح المصادقة:

- WPA/WPA2: تستخدم معلومات الخادم RADIUS لإنشاء مفاتيح فريدة للمصادقة. ونظرًا لإنشاء تلك المفاتيح على الخادم RADIUS المركزي، يوفر WPA/WPA2 أماناً أكبر من مفاتيح WPA المشتركة مسبقًا والمخزنة في AP والهاتف.
- تجوال الأمان السريع: يستخدم خادم RADIUS ومعلومات خادم المجال اللاسلكي (WDS) لإدارة ومصادقة المفاتيح. ينشئ WDS ذاكرة تخزين مؤقتة لبيانات اعتماد "الأمان" بالنسبة لأجهزة العميل الممكن بها CCKM لإعادة المصادقة السريعة والآمنة. يدعم هاتف

Cisco IP الطراز 8800 (FT Series 802.11r). يعتبر كل من r (FT11) وCCKM مدعومًا للسماح بتجوال الأمان السريع. لكن توصي Cisco بشدة بالاستفادة من r (FT802.11) عبر الطريقة الهوائية.

باستخدام WPA/WPA2 وCCKM، لا يتم إدخال مفاتيح التشفير على الهاتف، ولكن يتم تناقلها تلقائياً بين AP والهاتف. ولكن يجب إدخال اسم المستخدم وكلمة المرور لـ EAP التي يتم استخدامها للمصادقة على كل هاتف.

للتأكد من أمان حركة مرور الصوت، يدعم هاتف Cisco IP WEP وTKIP ومعايير التشفير المتقدم (AES) للتشفير. عند استخدام هذه الآليات لتشفير، يتم تشفير كل من حزم SIP المخصصة للإشارة وبروتوكول نقل الصوت في الوقت الحقيقي (RTP) بين AP وهاتف Cisco IP .

WEP

باستخدام WEP في الشبكة اللاسلكية، تحدث المصادقة على AP باستخدام مصادقة مفتوحة أو عبر مفتاح مشترك. يجب أن يطابق مفتاح WEP الذي تم إعداده على الهاتف مفتاح WEP الذي تم تكوينه في AP الخاصة بالاتصالات الناجحة. يدعم هاتف Cisco IP مفاتيح WEP التي تستخدم تشفير 40 بت أو تشفير 128 بت ويظل على الهاتف وAP.

يمكن أن تستخدم مصادقة EAP وCCKM مفاتيح WEP للتشفير. يدير خادم RADIUS مفتاح WEP ويمرر مفتاحًا فريدًا إلى AP بعد المصادقة لتشفير جميع حزم الصوت؛ وبناء على ذلك، يمكنك تغيير مفاتيح WEP هذه مع كل مصادقة.

TKIP

تستخدم WPA وCCKM تشفير TKIP الذي يحتوي على العديد من التحسينات عبر WEP. يوفر TKIP التشفير باستخدام المفاتيح لكل حزمة وموجهات تهيئة أطول (IVs) تعزز من التشفير. بالإضافة إلى ذلك، يضمن التحقق من تكامل الرسائل (MIC) عدم تغيير الحزم المشفرة. يزيل TKIP التنبؤ بـ WEP الذي يساعد المقتحمين على فك تشفير مفتاح WEP.

AES

طريقة تشفير تُستخدم لمصادقة WPA2. يستخدم هذا المعيار الوطني للتشفير خوارزمية متناظرة تحتوي على نفس المفتاح للتشفير وفك التشفير. يستخدم AES التشفير سلسلة حظر التشفير (CBC) بحجم 128 بت، وهي التي تدعم حجم 128 و192 و256 بت، كحد أدنى. يدعم هاتف Cisco IP حجم مفتاح 256 بت.

ملاحظة لا يدعم هاتف Cisco IP "بروتوكول تكامل المفتاح من CKIP) "Cisco) مع CMIC.

يتم إعداد أنظمة المصادقة والتشفير داخل الشبكة المحلية اللاسلكية. يتم تهيئة شبكات VLAN في الشبكة ونقاط الاتصال الموجودة وتحدد مجموعات مختلفة من المصادقة والتشفير. يرتبط SSID بشبكة VLAN ونظام المصادقة والتشفير المعين. من أجل مصادقة أجهزة العميل اللاسلكية بنجاح، يجب عليك تكوين SSID نفسها مع مخططات المصادقة والتشفير على AP وعلى هواتف Cisco IP .

تتطلب بعض مخططات المصادقة أنواعًا معينة من التشفير. مع المصادقة المفتوحة، يمكنك استخدام WEP ثابت للتشفير لمزيد من الأمان. ولكن إذا كنت تستخدم مصادقة "المفتاح المشترك"، فيجب تعيين WEP ثابت للتشفير، ويجب عليك تكوين مفتاح WEP على الهاتف.

ملاحظة

- عند استخدام مفتاح WPA مشترك مسبقاً أو مفتاح WPA2 مشترك مسبقاً، يجب تعيين المفتاح المشترك مسبقاً بشكل ثابت على الهاتف. يجب أن تطابق هذه المفاتيح المفاتيح الموجودة على AP.
- لا يدعم هاتف Cisco IP اجتياز EAP التلقائي؛ ولاستخدام وضع EAP-FAST، يجب عليك تحديده.

يعرض الجدول التالي قائمة بأنظمة المصادقة والتشفير التي تم تكوينها في نقاط وصول Cisco Aironet التي تدعم هواتف Cisco IP . يعرض الجدول خيار تكوين الشبكة الخاصة بالهاتف الذي يتطابق مع تكوين AP.

الجدول 17: مخططات المصادقة والتشفير

تكوين هاتف Cisco IP	تكوين AP			
وضع الأمان	الأمان	إدارة المفاتيح	التشفير	التجوال السريع
بلا	بلا	بلا	بلا	لا يوجد
WEP	WEP ثابت	ثابت	WEP	لا يوجد
PSK	PSK	WPA	TKIP	بلا
		WPA2	AES	FT
EAP-FAST	EAP-FAST	x802.1	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
EAP-TLS	EAP-TLS	x802.1	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
PEAP-MSCHAPV2	PEAP-MSCHAPV2	x802.1	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM

للحصول على مزيد من المعلومات حول تكوين مخططات المصادقة والتشفير على AP، راجع دليل تكوين *Cisco Aironet* للطراز لديك على عنوان URL التالي:

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

أمان شبكة LAN اللاسلكية

هواتف cisco التي تدعم Wi-fi لديك أكثر من متطلبات الأمان وتتطلب إعدادات تهيئة إضافية. تتضمن هذه الخطوات الإضافية تثبيت شهادات وإعداد الأمان على الهواتف وفي Cisco Unified Communications Manager.

للحصول على مزيد من المعلومات، ارجع إلى دليل أمان *Cisco Unified Communications Manager*.

صفحة إدارة هاتف Cisco IP

هواتف Cisco التي تدعم Wi-Fi يكون لها صفحات خاصة على الويب مختلفة عن صفحات الهواتف الأخرى. يمكنك استخدام صفحات الويب الخاصة لتهيئة أمان الهاتف في حالة عدم توفر بروتوكول تسجيل الشهادات البسيطة (SCEP). استخدم هذه الصفحات لتثبيت شهادات الأمان يدويًا على الهاتف، أو لتنزيل شهادة أمان، أو لتهيئة تاريخ ووقت الهاتف يدويًا.

تعرض صفحات الويب هذه أيضًا المعلومات نفسها التي تراها على صفحات الويب الأخرى الخاصة بالهاتف، والتي تشمل معلومات عن الجهاز وإعداد الشبكة والسجلات والمعلومات الإحصائية.

تهيئة صفحة الإدارة للهاتف

يتم تمكين صفحة الإدارة على الويب عند شحن الهاتف من المصنع وتم تعيين كلمة المرور على Cisco. ولكن في حالة تسجيل هاتف باستخدام Cisco Unified Communications Manager، يجب تمكين صفحة الإدارة على الويب وتهيئة كلمة مرور جديدة.

قم بتمكين هذه الصفحة الويب وتعيين بيانات اعتماد تسجيل الدخول قبل أن يمكنك استخدام صفحة الويب لأول مرة بعد تسجيل الهاتف.

عند تمكين، تكون صفحة الإدارة على الويب يمكن الوصول إليها على منفذ 8443 HTTPS (**https://x.x.x.x:8443**، حيث x.x.x.x عنوان IP هاتف).

قبل البدء

حدد كلمة مرور قبل تمكين صفحة الإدارة على الويب. يمكن أن تكون كلمة المرور أي مجموعة من الأحرف أو الأرقام، ولكن يجب أن تكون بين 8 و127 حرفاً.

اسم المستخدم الخاص بك بشكل دائم معيناً إلى خيار admin.

اجراء

الخطوة 1 من إدارة Cisco Unified Communications Manager، حدد **الجهاز** > **الهاتف**.

الخطوة 2 حدد موقع الهاتف الخاص بك.

الخطوة 3 في قسم **مخطط التكوين الخاص بالمنتج**، عيّن **مسؤول الويب** على **ممكّن**.

الخطوة 4 أدخل كلمة مرور في حقل **كلمة مرور المسؤول**.

الخطوة 5 حدد **حفظ** ، ثم انقر فوق **موافق**.

الخطوة 6 حدد **"تطبيق التكوين"** ، ثم انقر فوق **موافق**.

الخطوة 7 أعِد تشغيل الهاتف.

يمكنك الوصول إلى صفحة ويب إدارة الهاتف

إذا كنت ترغب في الوصول إلى صفحات ويب الإدارة، فتحتاج إلى تحديد منفذ الإدارة.

اجراء

الخطوة 1 احصل على عنوان IP الخاص بالهاتف:

- في إدارة Cisco Unified Communications Manager Administration، حدد **الجهاز** > **الهاتف**، وحدد موقع الهاتف. تعرض الهواتف التي يتم تسجيلها باستخدام Cisco Unified Communications Manager عنوان IP في نافذة **"بحث في الهواتف وسردها"** وفي أعلى نافذة **"تكوين الهاتف"**.

الخطوة 2 افتح مستعرض ويب وأدخل عنوان URL التالي، حيث يكون *IP_address* هو عنوان IP الخاص بهاتف Cisco IP :

https://<IP_address>:8443

الخطوة 3 أدخل كلمة المرور في حقل كلمة المرور.

الخطوة 4 انقر فوق **إرسال**.

تثبيت شهادة مستخدم من صفحة إدارة الهاتف على الويب

يمكن تثبيت شهادة المستخدم يدوياً على الهاتف إذا لم يتوفر بروتوكول تسجيل الشهادات البسيطة (SCEP).

يمكن استخدام المثبت مسبقاً التصنيع تثبيت الشهادة (MIC) "شهادة المستخدم" ل EAP-TLS.

بعد تثبيت "شهادة المستخدم"، تحتاج لإضافته إلى قائمة الثقة "الخادم" RADIUS.

قبل البدء

قبل تثبيت "شهادة المستخدم" لهاتف، يجب أن لديك:

- شهادة المستخدم وفر من جهاز الكمبيوتر الخاص بك. يجب أن يكون الشهادة بتنسيق PKCS #12.
- الشهادة استخراج كلمة المرور.

اجراء

الخطوة 1 من صفحة ويب إدارة الهاتف، حدد **الشهادات**.

الخطوة 2 قم بالاستعراض للشهادة الموجودة على جهاز الكمبيوتر الخاص بك.

الخطوة 3 في **كلمة المرور استخراج** الحقل، أدخل كلمة المرور استخراج الشهادة.

الخطوة 4 انقر فوق **تحميل**.

الخطوة 5 قم بإعادة تشغيل الهاتف بعد انتهاء التحميل.

تثبيت شهادة خادم مصادقة من صفحة إدارة الهاتف على الويب

يمكن تثبيت شهادة "خادم المصادقة" يدوياً على الهاتف إذا لم يتوفر بروتوكول تسجيل الشهادات البسيطة (SCEP).

يجب تثبيت شهادة CA الجذر التي تصدر شهادة خادم RADIUS لـ EAP-TLS.

قبل البدء

قبل تثبيت شهادة على هاتف، يجب أن يكون لديك "شهادة خادم المصادقة" محفوظة على جهاز الكمبيوتر الخاص بك. يجب ترميز الشهادة في PEM (أساس 64) أو DER.

اجراء

الخطوة 1 من صفحة ويب إدارة الهاتف، حدد **الشهادات**.

الخطوة 2 حدد حقل **خادم المصادقة CA (صفحة ويب المسؤول)**، وانقر فوق **تثبيت**.

الخطوة 3 قم بالاستعراض للشهادة الموجودة على جهاز الكمبيوتر الخاص بك.

الخطوة 4 انقر فوق **تحميل**.

الخطوة 5 قم بإعادة تشغيل الهاتف بعد انتهاء التحميل.

إذا كنت تقوم بتثبيت شهادة واحد أو أكثر، فقم بتثبيت كافة الشهادات قبل إعادة تشغيل الهاتف.

إزالة شهادة أمان يدويًا من صفحة إدارة الهاتف على صفحة الويب

يمكنك إزالة شهادات أمان يدوياً من خلال هاتف في حالة عدم توفر بروتوكول تسجيل الشهادات البسيطة (SCEP).

اجراء

الخطوة 1 من صفحة ويب إدارة الهاتف، حدد **الشهادات**.
الخطوة 2 حدد موقع الشهادة على صفحة **شهادات**.
الخطوة 3 انقر فوق **حذف**.
الخطوة 4 قم بإعادة تشغيل الهاتف بعد إكمال عملية الحذف.

ضبط تاريخ ووقت الهاتف يدويًا

باستخدام مصادقة قائمة على شهادة، يجب أن يعرض الهاتف التاريخ والوقت الصحيحين. يتحقق خادم مصادقة من التاريخ والوقت في الهاتف في مقابل تاريخ انتهاء صلاحية الشهادة. إذا لم تتطابق التواريخ والأوقات بين الهاتف والخادم، فيتوقف الهاتف عن العمل.

استخدم هذا الإجراء لتعيين التاريخ والوقت يدويًا على الهاتف إذا كان الهاتف لا يتلقى المعلومات الصحيحة من الشبكة.

اجراء

الخطوة 1 من صفحة ويب إدارة الهاتف، قم بالتمرير إلى **التاريخ والوقت**.
الخطوة 2 قم بتنفيذ أحد الخيارات التالية:

- انقر فوق **تعيين التاريخ والوقت المحليين للهاتف** لمزامنة الهاتف مع خادم محلي.
- في حقول **Specify Date & Time** (تحديد التاريخ والوقت)، حدد الشهر، واليوم، والسنة، والساعة، والدقيقة، والثانية باستخدام القوائم وانقر فوق **تعيين التاريخ والوقت المحليين للهاتف**.

إعداد SCEP

بروتوكول تسجيل الشهادات البسيطة (SCEP) هو المعيار الخاص بتوفير وتجديد الشهادات تلقائيًا. وهو يتجنب التثبيت اليدوي للشهادات على هاتفك.

قم بتهيئة معلمات التهيئة الخاصة بالمنتج SCEP

يجب عليك تهيئة معلمات SCEP التالية على صفحة ويب الهاتف لديك

- عنوان IP لـ RA
- بصمة الإصبع SHA-1 أو SHA-256 لشهادة CA الجذر الخاصة بخادم SCEP

تعمل هيئة التسجيل RA) Cisco IOS) كوكيل لخادم SCEP. يستخدم العميل SCEP على الهاتف المعلمات التي يتم تنزيلها من Cisco Unified Communication Manager. بعد تهيئة المعلمات، يرسل الهاتف طلب `SCEP getcs` إلى RA ويتم التحقق من صحة شهادة CA الجذر باستخدام بصمة الإصبع المحددة.

اجراء

الخطوة 1	من إدارة Cisco Unified Communications Manager، حدد **الجهاز** > **الهاتف**.
الخطوة 2	حدد موقع الهاتف.
الخطوة 3	قم بالتمرير إلى منطقة **مخطط التكوين الخاص بالمنتج**.
الخطوة 4	حدد خانة الاختيار **خادم SCEP للشبكة المحلية اللاسلكية** لتنشيط المعلمة SCEP.
الخطوة 5	حدد خانة الاختيار **بصمة إصبع CA الجذر للشبكة المحلية اللاسلكية (SHA256 أو SHA1)** لتنشيط المعلمة SCEP QED.

دعم خادم بروتوكول تسجيل الشهادات البسيطة

إذا كنت تستخدم خادم بروتوكول تسجيل شهادات بسيطة (SCEP)، فيمكن للخادم تلقائياً الحفاظ على المستخدم وشهادات الخادم الخاصة بك. في خادم SCEP، قم بتهيئة عامل تسجيل SCEP (RA) لكي:

- يعمل كنقطة ثقة لـ PKI
- ليعمل كـ PKI RA
- قم بتنفيذ مصادقة الجهاز باستخدام خادم RADIUS

لمزيد من المعلومات، راجع وثائق خادم SCEP.

مصادقة x802.1

تدعم هواتف Cisco IP مصادقة X802.1.

عادةً ما تستخدم هواتف Cisco IP ومحولات Cisco IP بروتوكول اكتشاف Cisco (يُعرف اختصارًا بـ CDP) للتعرف على هوية بعضها البعض وتحديد معلمات مثل متطلبات تخصيص VLAN وطاقة الكبلات الداخلية.

يتطلب دعم مصادقة X802.1 العديد من المكونات:

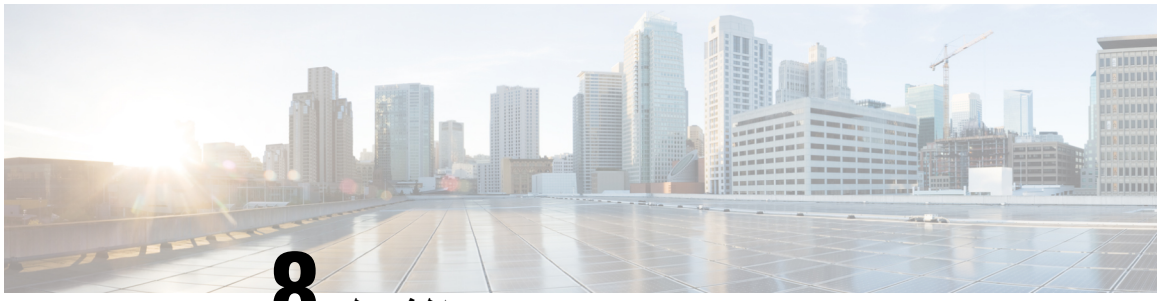
- هاتف Cisco IP : يعمل الهاتف على تكوين الطلب للوصول إلى الشبكة. تشتمل الهواتف على عميل X802.1. يتيح هذا العميل لمسؤولي الشبكة التحكم في اتصال هواتف IP بمنافذ محول LAN. يستخدم الإصدار الحالي من عميل X802.1 للهواتف الخيارين EAP—FAST وEAP—TLS لمصادقة الشبكة.
- محول Cisco Catalyst (أو محول آخر تابع لجهة خارجية): يجب أن يدعم المحول X802.1، بحيث يمكنه أن يؤدي وظيفة المصادقة ويمرر الرسائل بين الهاتف وخادم المصادقة. بعد اكتمال عملية التبادل، يمنح المحول أو يرفض إمكانية وصول الهاتف إلى الشبكة.

ويجب أن تنفذ الإجراءات التالية لتكوين X802.1.

- كوّن المكونات الأخرى قبل تمكين "مصادقة X802.1" على الهاتف.
- تكوين VLAN للصوت — لأن معيار X802.1 لا يعتد بوجود شبكات VLAN، يجب أن تعمد إلى تكوين هذا الإعداد بناءً على دعم المحول.
  - ممكّن — إذا كنت تستخدم محولاً يدعم المصادقة متعددة المجالات، فيمكنك الاستمرار في استخدام VLAN للصوت.
  - معطّل — إذا كان المحول لا يدعم المصادقة متعددة المجالات، فقم بتعطيل "VLAN للصوت" وضع في اعتبارك تعيين المنفذ إلى شبكة VLAN الأصلية.

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14



الفصل 8

تخصيص هاتف مؤتمر Cisco IP

نغمات رنين الهاتف المخصصة

يتم شحن هاتف Cisco IP بنوعين من نغمات الرنين الافتراضية المطبقة في الأجهزة: Chirp1 وChirp2. كما يوفر Cisco Unified Communications Manager مجموعة افتراضية من أصوات نغمات رنين الهاتف الإضافية التي يتم تطبيقها في البرنامج في صورة ملفات تضمين نبضي مشفر (PCM). يوجد ملف PCM بالإضافة إلى ملف XML الذي يصف خيارات قائمة الرنات المتوفرة في موقعك، في دليل TFTP على كل خادم من خوادم Cisco Unified Communications Manager.

انتبه جميع أسماء الملفات حساسة لحالة الأحرف. إذا استخدمت الحالة الخطأ لاسم الملف، فلن يطبق الهاتف التغييرات.

لمزيد من المعلومات، انظر الفصل "رنات وخلفيات الهواتف المخصصة"، دليل تكوين الميزات لـ Cisco Unified Communications Manager.

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14

إعداد رنين هاتف مخصص

اجراء

الخطوة 1 أنشئ ملف PCM لكل رنين مخصص (رنين واحد لكل ملف).

تأكد من أن ملفات PCM تتوافق مع إرشادات التنسيق الواردة في قسم تنسيقات ملفات الرنين المخصص.

الخطوة 2 قم بتحميل ملفات PCM الجديدة التي أنشأتها إلى خادم Cisco TFTP لكل Cisco Unified Communications Manager في المجموعة الخاصة بك.

للحصول على مزيد من المعلومات، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.

الخطوة 3 احفظ التعديلات وأغلق ملف Ringlist-wb.

الخطوة 4 لتخزين ملف Ringlist-wb الجديد في الذاكرة المؤقتة:

- أوقف وابدأ تشغيل خدمة TFTP باستخدام Cisco Unified Serviceability
- قم بتعطيل وإعادة تمكين معلمة خدمة TFTP "تمكين التخزين المؤقت لملفات Constant وBin عند بدء التشغيل"، الموجودة في منطقة معلمات الخدمة المتقدمة.

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14

تنسيقات ملف الرنين المخصص

يحدد ملف Ringlist—wb.xml كائن XML الذي يحتوي على قائمة بأنواع رنين الهاتف. يشتمل هذا الملف على ما يصل إلى 50 نوعًا من الرنين. ويحتوي كل نوع من الرنين على مؤشر إلى ملف PCM المستخدم لذلك النوع من الرنين والنص الذي يظهر في قائمة "نوع الرنين" على هاتف Cisco IP خصيصًا لذلك الرنين. يشتمل خادم Cisco TFTP لكل Cisco Unified Communications Manager على هذا الملف.

يستخدم كائن CiscoIPRinglist XML العلامة النموذجية التالية المعينة لوصف المعلومات:

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

تنطبق السمات التالية على أسماء التعريفات. يجب أن تقوم بتضمين DisplayName وFileName اللازمين لكل نوع رنين في الهاتف.

- يحدد DisplayName اسم الرنين المخصص لملف PCM المقترن الذي يتم عرضه في قائمة "نوع الرنين" على هاتف Cisco IP .
- يحدد FileName اسم ملف PCM للرنين المخصص لإقرانه بـ DisplayName.

ملاحظة يجب ألا يزيد طول الحقلين DisplayName وFileName عن 25 حرفًا.

يعرض هذا المثال ملف Ringlist—wb.xml الذي يحدد نوعين من رنين الهاتف:

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

يجب أن تفي ملفات PCM الخاصة بنغمات الرنين بالمتطلبات التالية لتشغيلها على هواتف Cisco IP بشكل سليم:

- ملف PCM بسيط (بدون عنوان)
- 800 نموذج في الثانية
- 8 بت لكل نموذج
- ضغط Mu—law
- أقصى حجم للرنين = 16080 نموذجًا

- أدنى حجم للرنين = 240 نموذجًا
- عدد النماذج في الرنين = عدد مضاعف قوامه 240 نموذجًا.
- يبدأ الرنين وينتهي عند نقاطع نقطة الانعدام.

لإنشاء ملفات PCM لنغمات رنين مخصصة في الهاتف، استخدم أيًا من حزم تحرير الصوت القياسية التي تدعم هذه المتطلبات الخاصة بتنسيق الملف.

تخصيص نغمة الطلب

يمكنك إعداد هواتفك بحيث تتيح للمستخدمين سماع نغمات اتصال مختلفة للمكالمات الداخلية والخارجية. بناءً على احتياجاتك، يمكنك اختيار ثلاثة خيارات لنغمة الطلب:

- افتراضي: نغمة طلب مختلفة للمكالمات الداخلية والخارجية.
- داخلي: تُستخدم نغمة الطلب الداخلي لجميع المكالمات.
- خارجي: تُستخدم نغمة الطلب الخارجي لجميع المكالمات.

يعد "□|□استخدام نغمة الطلب دائمًا□|□" حقلاً مطلوبًا في Cisco Unified Communications Manager.

اجراء

الخطوة 1 في إدارة Cisco Unified Communications Manager، حدد **النظام** > **معلمات الخدمة**.

الخطوة 2 حدد الخادم المناسب.

الخطوة 3 حدد **Cisco CallManager** باعتبارها "الخدمة".

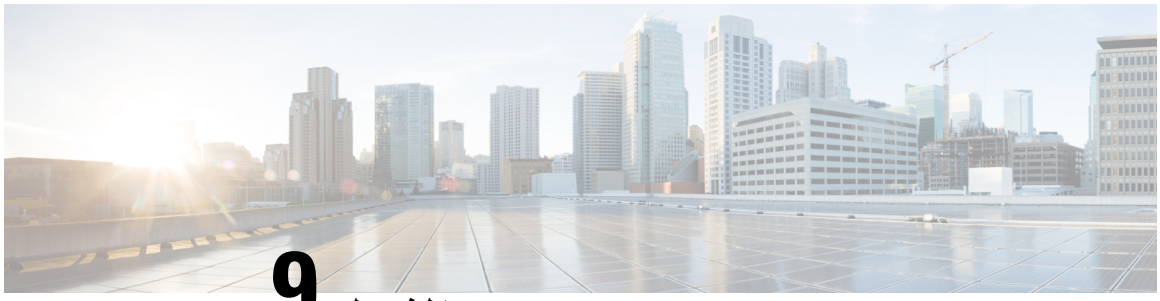
الخطوة 4 مرّر إلى جزء "معلمات على مستوى مجموعة النظام".

الخطوة 5 عيّن **استخدام نغمة الطلب دائمًا** إلى أحد الخيارات التالية:

- خارجي
- داخلي
- افتراضي

الخطوة 6 حدد **حفظ**.

الخطوة 7 أعِد تشغيل الهواتف.



الفصل 9

ميزات وإعداد هاتف مؤتمر Cisco IP

دعم مستخدم هاتف Cisco IP

إذا كنت مسؤول نظام، فمن الأرجح أن تكون المصدر الأساسي للمعلومات المتعلقة بمستخدمي هاتف Cisco IP في شبكتك أو شركتك. ومن المهم أن تزود المستخدمين النهائيين بمعلومات حديثة وشاملة.

لاستخدام بعض الميزات بنجاح على هاتف Cisco IP (بما في ذلك الخدمات وخيارات نظام الرسائل الصوتية)، يجب أن يتلقى المستخدمون معلومات منك أو من فريق شبكتك أو تكون لديهم القدرة على الاتصال بك للحصول على المساعدة. تأكد من إمداد المستخدمين بأسماء الأشخاص المراد الاتصال بهم للحصول على المساعدة وبالتعليمات الخاصة بالاتصال بهؤلاء الأشخاص.

ونوصي بأن تقوم بإنشاء صفحة ويب على موقع الدعم الخاص بك لإمداد المستخدمين النهائيين بالمعلومات المهمة حول هواتف Cisco IP .

ضع في اعتبارك تضمين الأنواع التالية من المعلومات في هذا الموقع:

- أدلة المستخدم الخاصة بجميع طرز هاتف Cisco IP التي تدعمها
- معلومات حول كيفية الوصول إلى مدخل Cisco Unified Communications Self Care.
- قائمة الميزات المدعومة
- دليل المستخدم أو مرجع سريع لنظام البريد الصوتي

ترحيل هاتفك إلى هاتف ذو أنظمة متعددة

يمكنك ترحيل هاتف مؤسستك إلى هاتف متعدد الأنظمة الأساسية بسهولة بخطوة واحدة دون استخدام تحميل البرامج الثابتة الخاصة بالنقل. كل ما تحتاجه هو الحصول على ترخيص الترحيل من الخادم والموافقة عليه.

للحصول على مزيد من المعلومات، راجع https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/MPP/MPP-conversion/enterprise-to-mpp/cuip_b_conversion-guide-ipphone.html

إعداد قالب مفتاح مرن جديد

تحتاج إلى إضافة مفاتيح مرنة إلى قالب مفتاح مرن لمنح المستخدمين حق الوصول إلى بعض الميزات. على سبيل المثال، إذا أردت أن يكون المستخدمون قادرين على استخدام ميزة عدم الإزعاج، فيجب عليك تمكين المفتاح المرن. للحصول على مزيد من المعلومات، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.

قد تحتاج إلى إنشاء عدة قوالب. على سبيل المثال، قد تحتاج إلى قالب للهاتف في غرفة المؤتمر، وقالب آخر بالنسبة لهاتف في المكتب التنفيذي.

يستغرق هذا الإجراء خطوات لإنشاء قالب مفتاح مرن جديد وتعيينه إلى هاتف معين. وبالمثل لميزات الهاتف الأخرى، يمكنك أيضًا استخدام القالب لجميع هواتف المؤتمر أو مجموعة من الهواتف.

اجراء

الخطوة 1 سجّل الدخول إلى إدارة Cisco Unified Communications Manager كمسؤول.

الخطوة 2 حدد **الجهاز** > **إعدادات الجهاز** > **قالب المفتاح المرن**

الخطوة 3 انقر فوق **بحث**.

الخطوة 4 حدد أحد الخيارات التالية:

- إصدار 11.5 من Cisco Unified Communications Manager والإصدارات السابقة - **المستخدم القياسي**
- الإصدار 12.0 من Cisco Unified Communications Manager والإصدارات الأحدث - **مستخدم المؤتمر الشخصي** أو **مستخدم المؤتمر العام**.

الخطوة 5 انقر فوق **نسخ**.

الخطوة 6 قم بتغيير اسم القالب.

على سبيل المثال، قالب غرفة مؤتمر 8832.

الخطوة 7 انقر فوق **حفظ**.

الخطوة 8 انتقل إلى صفحة **تكوين تخطيط المفتاح المرن** من القائمة العلوية اليمنى.

الخطوة 9 بالنسبة لكل حالة مكالمة، قم بتعيين الميزات لعرضها.

الخطوة 10 انقر فوق **حفظ**.

الخطوة 11 عُد إلى **شاشة البحث/القائمة** من القائمة العلوية اليمنى.

سترى القالب الجديد الخاص بك في قائمة القوالب.

الخطوة 12 حدد **الجهاز** > **الهاتف**.

الخطوة 13 اعثر على الهاتف للحصول على قالب جديد وتحديده.

الخطوة 14 في حقل **قالب المفتاح المرن**، حدد قالب المفتاح المرن الجديد.

الخطوة 15 انقر فوق **حفظ** و**تطبيق التكوين** .

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14

تكوين خدمات الهاتف للمستخدمين

يمكنك منح المستخدمين إمكانية الوصول إلى خدمات هاتف Cisco IP على هاتف IP. يمكنك أيضًا تعيين زر إلى خدمات الهاتف المختلفة. ويدير هاتف IP كل خدمة كتطبيق منفصل.

قبل أن يتمكن المستخدم من الوصول إلى أي من الخدمات:

- استخدم Cisco Unified Communications Manager Administration لتكوين الخدمات غير الموجودة افتراضيًا.
- يجب أن يشترك المستخدم في الخدمات باستخدام مدخل Cisco Unified Communications Self Care. يوفر التطبيق المستند إلى الويب واجهة مستخدم رسومية (GUI) لتكوين محدود لدى المستخدم النهائي لتطبيقات هاتف IP. ومع ذلك، يتعذر على المستخدم تسجيل اشتراك مؤسسي في أي من الخدمات التي تقوم بتكوينها.

للحصول على مزيد من المعلومات، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.

قبل إعداد الخدمات، اجمع عناوين URL الخاصة بالمواقع التي تريد إعدادها وتحقق من إمكانية وصول المستخدمين إلى تلك المواقع من شبكة هاتفية IP لدى الشركة. لا ينطبق هذا النشاط على الخدمات الافتراضية التي توفرها Cisco.

اجراء

الخطوة 1 في Cisco Unified Communications Manager Administration، اختر **الجهاز** > **إعدادات الجهاز** > **خدمات الهاتف**.

الخطوة 2 تحقق من إمكانية وصول مستخدميك إلى مدخل Cisco Unified Communications Self Care، والتي يمكنهم من خلالها تحديد الخدمات التي تم تكوينها والاشتراك فيها.

راجع نظرة عامة على مدخل Self Care, في الصفحة 65 للاطلاع على ملخص للمعلومات التي يجب أن توفرها للمستخدمين النهائيين.

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14

تكوين ميزات الهاتف

يمكنك إعداد الهواتف لتوفر مجموعة متنوعة من الميزات، وذلك بناءً على احتياجات مستخدميك. يمكنك تطبيق ميزات على جميع الهواتف أو مجموعة من الهواتف أو هواتف فردية.

عند إعداد الميزات، تعرض نافذة Cisco Unified Communications Manager Administration المعلومات القابلة للتطبيق على جميع الهواتف والمعلومات القابلة للتطبيق على طراز الهاتف. توجد المعلومات الخاصة بطراز الهاتف في منطقة "مخطط التهيئة الخاص بالمنتج" بالنافذة.

للحصول على معلومات حول الحقول القابلة للتطبيق على جميع طرز الهواتف، راجع وثائق Cisco Unified Communications Manager.

عند تعيين حقل، تُعد النافذة التي تقوم بتعيين الحقل فيها مهمة نظرًا لوجود أولوية للنوافذ. وترتيب الأولوية كالتالي:

1. الهواتف الفردية (أعلى أولوية)
2. مجموعة الهواتف
3. جميع الهواتف (أقل أولوية)

على سبيل المثال، إذا كنت تريد وصول مجموعة محددة من المستخدمين إلى صفحات الهاتف على الويب، مع منح إمكانية وصول باقي المستخدمين إلى الصفحات، فاعمد إلى:

1. تمكين الوصول إلى صفحات الهاتف على الويب لجميع المستخدمين.
2. تعطيل الوصول إلى صفحات الهاتف على الويب لكل مستخدم على حدة أو إعداد وصول مجموعة من المستخدمين أو تعطيل الوصول إلى صفحات الهاتف على الويب لمجموعة المستخدمين.
3. إذا احتاج مستخدم محدد في مجموعة المستخدمين إلى الوصول إلى صفحات الهاتف على الويب، فيمكنك تفعيل الوصول فقط لذلك المستخدم تحديدًا.

موضوعات ذات صلة

استمرار تسجيل الدخول إلى Expressway ببيانات اعتماد المستخدم, في الصفحة 113

إعداد الميزات الهاتفية لجميع الهواتف

اجراء

الخطوة 1	سجّل الدخول إلى Cisco Unified Communications Manager الإدارة كمسؤول.
الخطوة 2	حدد **النظام** > **تكوين هاتف المؤسسة**.
الخطوة 3	قم بتعيين الحقول التي تريد تغييرها.
الخطوة 4	حدد خانة اختيار **تجاوز إعدادات المؤسسة** للتحقق من وجود أي حقول متغيرة.
الخطوة 5	انقر فوق **حفظ**.
الخطوة 6	انقر فوق **تطبيق التكوين**.
الخطوة 7	أعِد تشغيل الهواتف.
ملاحظة	سيؤثر هذا على جميع الهواتف الموجودة في مؤسستك.

موضوعات ذات صلة

التكوين الخاص بالمنتج, في الصفحة 93

إعداد الميزات الهاتفية لمجموعة من الهواتف

اجراء

الخطوة 1	سجّل الدخول إلى Cisco Unified Communications Manager الإدارة كمسؤول.
الخطوة 2	حدد **الجهاز** > **إعدادات الجهاز** > **ملف تعريف الهاتف العام**
الخطوة 3	حدد موقع ملف التعريف.
الخطوة 4	انتقل إلى جزء "مخطط التهيئة الخاص بالمنتج" وقم بتعيين الحقول.
الخطوة 5	حدد خانة اختيار **تجاوز إعدادات المؤسسة** للتحقق من وجود أي حقول متغيرة.
الخطوة 6	انقر فوق **حفظ**.
الخطوة 7	انقر فوق **تطبيق التكوين**.

الخطوة 8 أعِد تشغيل الهواتف.

موضوعات ذات صلة

التكوين الخاص بالمنتج, في الصفحة 93

إعداد الميزات الهاتفية لهاتف واحد

اجراء

الخطوة 1 سجّل الدخول إلى Cisco Unified Communications Manager الإدارة كمسؤول.
الخطوة 2 حدد **الجهاز** > **الهاتف**
الخطوة 3 حدد موقع الهاتف المقترن بالمستخدم.
الخطوة 4 انتقل إلى جزء "مخطط التهيئة الخاص بالمنتج" وقم بتعيين الحقول.
الخطوة 5 حدد خانة اختيار **تجاوز الإعدادات العامة** للتحقق من وجود أي حقول متغيرة.
الخطوة 6 انقر فوق **حفظ**.
الخطوة 7 انقر فوق **تطبيق التكوين**.
الخطوة 8 أعِد تشغيل الهاتف.

موضوعات ذات صلة

التكوين الخاص بالمنتج, في الصفحة 93

التكوين الخاص بالمنتج

يصف الجدول التالي الحقول الموجودة في جزء "مخطط التهيئة الخاص بالمنتج". يتم عرض بعض الحقول الموجودة في هذا الجدول فقط في صفحة **الجهاز** > **الهاتف**.

الجدول *18*: حقول التهيئة الخاص بالمنتج

اسم الحقل	نوع الحقل أو الاختيارات	افتراضي	الوصف
الوصول إلى الإعدادات	معطل ممكن مقيد	ممكن	لتمكين أو تعطيل أو تقييد الوصول إلى إعدادات التهيئة المحلية في تطبيق "الإعدادات". من خلال الوصول المقيد، يمكن الوصول إلى قوائم التفضيلات ومعلومات النظام. كما يمكن الوصول إلى بعض الإعدادات في قائمة Wi-Fi. مع الوصول المعطل، لا تعرض قائمة "الإعدادات" أي خيارات.
Gratuitous ARP	معطل ممكن	معطل	لتمكين أو تعطيل قدرة الهاتف على معرفة عناوين MAC من Gratuitous ARP. يلزم وجود هذه الإمكانية لمراقبة عمليات دفق الصوت أو تسجيلها.

اسم الحقل	نوع الحقل أو الاختيارات	افتراضي	الوصف
الوصول إلى الويب	معطل ممكن	معطل	لتمكين أو تعطيل الوصول إلى صفحات الهاتف على الويب عبر مستعرض ويب. **تنبيه** إذا قمت بتمكين هذا الحقل، فقد تكشف عن معلومات حساسة حول الهاتف.
تعطيل TLS 1.0 وTLS 1.1 للوصول إلى الويب	معطل ممكن	ممكن	التحكم في استخدام TLS 1.2 لاتصال خادم ويب. • معطل — يمكن لهاتف مكوّن لـ TLS1.0 أو TLS 1.1 أو TLS1.2 العمل كخادم HTTPs. • ممكّن — يمكن فقط لهاتف مكوّن لـ TLS1.2 العمل كخادم HTTPs.
طلب Enbloc	معطل ممكن	معطل	للتحكم في أسلوب الطلب. • معطل — ينتظر Cisco Unified Communications Manager انتهاء صلاحية المؤقت الرقمي عندما تتداخل خطة الطلب أو نمط إعادة التوجيه. • ممكّن — يتم إرسال السلسلة التي تم الاتصال بها بالكامل إلى Cisco Unified Communications Manager بمجرد اكتمال الطلب. لتجنب انتهاء مهلة مؤقت T.302، نوصي بتمكين ميزة طلب Enbloc عندما تتداخل خطة اتصال أو نمط توجيه. لا تدعم "رموز التفويض المفروضة" (FAC) أو "رموز حالة العميل" (CMC) طلب Enbloc. إذا كنت تستخدم FAC أو CMC لإدارة الوصول إلى المكالمة والمحاسبة، فلا يمكنك استخدام هذه الميزة.
الضوء الخلفي للأيام غير نشط	أيام الأسبوع		لتحديد الأيام التي لا يتم خلالها تشغيل الضوء الخلفي تلقائيًا في الوقت المحدد داخل حقل "وقت تشغيل الضوء الخلفي". اختر اليوم أو الأيام من القائمة المنسدلة. لاختيار أكثر من يوم، اضغط على زر **Ctrl مع النقر فوق** كل يوم تريده. ارجع إلى جدول توفير الطاقة لهاتف Cisco IP, في الصفحة 103.
وقت تشغيل الضوء الخلفي	hh:mm		لتحديد الوقت الذي يتم خلاله يوميًا تشغيل الضوء الخلفي تلقائيًا (باستثناء الأيام المحددة في حقل "شاشة الضوء الخلفي غير نشطة"). أدخل الوقت في هذا الحقل بتنسيق 24 ساعة، حيث يشير التنسيق 0:00 إلى منتصف الليل. على سبيل المثال، لتشغيل الإضاءة الخلفية تلقائيًا في الساعة 07:00 صباحًا (0700)، أدخل 07:00. لتشغيل الإضاءة الخلفية الساعة 02:00 ظهرًا (1400)، أدخل 14:00. إذا كان هذا الحقل فارغًا، فيتم تشغيل الضوء الخلفي تلقائيًا الساعة 0:00. ارجع إلى جدول توفير الطاقة لهاتف Cisco IP, في الصفحة 103.

اسم الحقل	نوع الحقل أو الاختيارات	افتراضي	الوصف
مدة تشغيل الضوء الخلفي	hh:mm		لتحديد طول الفترة الزمنية التي يظل خلالها الضوء الخلفي مضاءً بعد تشغيله في الوقت المحدد داخل حقل "وقت تشغيل الضوء الخلفي". على سبيل المثال، للاحتفاظ بالضوء الخلفي مضاءً لمدة 4 ساعات و30 دقيقة بعد تشغيله تلقائيًا، أدخل 04:30. إذا كان هذا الحقل فارغًا، فيتم إيقاف تشغيل الهاتف في نهاية اليوم (0:00). إذا كان "وقت تشغيل الضوء الخلفي" الساعة 0:00 والحقل الخاص بمدة تشغيل الضوء الخلفي فارغًا (أو 24:00)، فلا يتم إيقاف تشغيل الضوء الخلفي. ارجع إلى جدول توفير الطاقة لهاتف Cisco IP, في الصفحة 103.
مهلة خمول الضوء الخلفي	hh:mm		لتحديد طول الفترة الزمنية التي يكون الهاتف خلالها في حالة خمول قبل إيقاف تشغيل الضوء الخلفي. يتم تطبيقه فقط عند إيقاف تشغيل الضوء الخلفي وفقًا للجدول الزمني وعند تشغيله بواسطة المستخدم (بالضغط على زر في الهاتف أو رفع سماعة الهاتف). على سبيل المثال، لإيقاف تشغيل الضوء الخلفي عندما يكون الهاتف في وضع الخمول لمدة ساعة و30 دقيقة بعد أن يقوم المستخدم بتشغيل الضوء الخلفي، أدخل 01:30. ارجع إلى جدول توفير الطاقة لهاتف Cisco IP, في الصفحة 103.
تشغيل الضوء الخلفي عند تلقي مكالمة واردة	معطل ممكن	ممكن	لتشغيل الضوء الخلفي عند وجود مكالمة واردة.

اسم الحقل	نوع الحقل أو الاختيارات	افتراضي	الوصف
تمكين توفير الطاقة الإضافي	أيام الأسبوع		لتحديد الجدول الزمني للأيام التي يتم إيقاف تشغيل الهاتف خلالها. اختر اليوم أو الأيام من القائمة المنسدلة. لاختيار أكثر من يوم، اضغط على زر **Ctrl مع النقر فوق** كل يوم تريده. عند تشغيل "تمكين توفير الطاقة الإضافي"، تتلقى رسالة تحذر من وجود مشكلات طارئة (e911). **تنبيه** أثناء نفاذ مفعول "وضع توفير الطاقة الإضافي" (يشار إليه باسم "الوضع")، يتم تعطيل نقاط النهاية المكونة للوضع عند المكالمات الطارئة ومنعها من تلقي المكالمات الواردة. بتحديد هذا الوضع، تقر بموافقتك على ما يلي: (1) أن تتحمل المسؤولية كاملة عن توفير طرق بديلة لمكالمات الطوارئ وتلقي المكالمات أثناء نفاذ مفعول الوضع، و(2) ألا تتحمل Cisco أية مسؤولية بشأن تحديدك للوضع وتخلي مسؤوليتها الكاملة بشأن تمكين الوضع الذي يُعد مسؤوليتك، و(3) أن تُعلم المستخدمين بالآثار المترتبة على المكالمات أثناء تشغيل الوضع والاتصال وغير ذلك. لتعطيل "توفير الطاقة الإضافي"، يجب إلغاء تحديد خانة اختيار "السماح بتجاوز EnergyWise". إذا ظل اختيار "السماح بتجاوز EnergyWise" محددًا دون تحديد أيام في حقل "توفير الطاقة الإضافي"، فلا يتم تعطيل "توفير الطاقة الإضافي". ارجع إلى جدولة EnergyWise على هاتف Cisco IP, في الصفحة 105.
وقت تشغيل الهاتف	hh:mm		لتحديد الوقت الذي يتم خلاله تشغيل الهاتف تلقائيًا وفقًا للأيام الموجودة في حقل "تمكين توفير الطاقة الإضافي". أدخل الوقت في هذا الحقل بتنسيق 24 ساعة، حيث يشير التنسيق 00:00 إلى منتصف الليل. على سبيل المثال، لتشغيل الهاتف تلقائيًا في الساعة 07:00 صباحًا (0700)، أدخل 07:00. لتشغيل الهاتف الساعة 02:00 ظهرًا (1400)، أدخل 14:00. القيمة الافتراضية فارغة، مما يعني أنها 00:00. يجب أن يكون "وقت تشغيل الهاتف" بعد "وقت إيقاف تشغيل الهاتف" بمدة مقدارها 20 دقيقة على الأقل. على سبيل المثال، إذا كان "وقت إيقاف تشغيل الهاتف" الساعة 07:00، فيجب ألا يكون "وقت تشغيل الهاتف" قبل الساعة 07:20. ارجع إلى جدولة EnergyWise على هاتف Cisco IP, في الصفحة 105.

اسم الحقل	نوع الحقل أو الاختيارات	افتراضي	الوصف
وقت إيقاف تشغيل الهاتف	hh:mm		لتحديد الوقت الذي يتم خلاله إيطال تشغيل الهاتف تلقائيًا في اليوم وفقًا لما هو محدد في حقل "تمكين توفير الطاقة الإضافي". إذا كان حقلا "وقت تشغيل الهاتف" و"وقت إيقاف تشغيل الهاتف" يحتويان على القيمة نفسها، فلا يتم إيطال تشغيل الهاتف. أدخل الوقت في هذا الحقل بتنسيق 24 ساعة، حيث يشير التنسيق 00:00 إلى منتصف الليل. على سبيل المثال، لإيقاف تشغيل الهاتف تلقائيًا في الساعة 7:00 صباحًا (0700)، أدخل 7:00. لإيقاف تشغيل الهاتف الساعة 2:00 ظهرًا (1400)، أدخل 14:00. القيمة الافتراضية فارغة، مما يعني أنها 00:00. يجب أن يكون "وقت تشغيل الهاتف" بعد "وقت إيقاف تشغيل الهاتف" بمدة مقدارها 20 دقيقة على الأقل. على سبيل المثال، إذا كان "وقت إيقاف تشغيل الهاتف" الساعة 7:00، فيجب ألا يكون "وقت تشغيل الهاتف" قبل الساعة 7:20. ارجع إلى جدولة EnergyWise على هاتف Cisco IP, في الصفحة 105.
انتهاء مهلة خمول إيقاف تشغيل الهاتف	hh:mm		للإشارة إلى طول الفترة الزمنية التي يجب أن يكون الهاتف خلالها في حالة خمول قبل إيطال تشغيل الهاتف. تنتهي المهلة بموجب الشروط التالية: • إذا كان الهاتف في وضع "توفير الطاقة الإضافي" وفقًا للجدول الزمني، وتم إخراجه من وضع "توفير الطاقة الإضافي" نظرًا لضغط مستخدم الهاتف على مفتاح "تحديد". • عند إعادة تشغيل الهاتف من خلال جهاز التبديل المتصل. • عند الوصول إلى "وقت إيقاف تشغيل الهاتف"، ولكن الهاتف قيد الاستخدام. ارجع إلى جدولة EnergyWise على هاتف Cisco IP, في الصفحة 105.
تمكين التنبيه المسموع	خانة اختيار	غير مختار	عند تمكينه، يتم توجيه الهاتف إلى تشغيل تنبيه مسموع يبدأ قبل 10 دقائق من الوقت المحدد في حقل "وقت إيقاف تشغيل الهاتف". يتم تطبيق خانة الاختيار هذه فقط إذا كانت خانة قائمة "توفير الطاقة الإضافي" تحتوي على يوم واحد أو أكثر من يوم مختار. ارجع إلى جدولة EnergyWise على هاتف Cisco IP, في الصفحة 105.
مجال EnergyWise	حتى 127 حرفًا		لتحديد مجال EnergyWise الذي يوجد به الهاتف. ارجع إلى جدولة EnergyWise على هاتف Cisco IP, في الصفحة 105.

اسم الحقل	نوع الحقل أو الاختيارات	افتراضي	الوصف
كلمة سر EnergyWise	حتى 127 حرفًا		لتحديد كلمة مرور الأمان السرية المستخدمة للاتصال بنقاط النهاية الموجودة بنطاق EnergyWise. ارجع إلى جدولة EnergyWise على هاتف Cisco IP, في الصفحة 105.
السماح بتجاوز EnergyWise.	خانة اختيار	غير مختار	لتحديد ما إذا كنت تسمح لسياسة وحدة التحكم في نطاق EnergyWise بإرسال تحديثات مستوى الطاقة إلى الهواتف أم لا. تنطبق الشروط التالية: • يجب تحديد يوم واحد أو أكثر من يوم في حقل "تمكين توفير الطاقة الإضافي". • تسري الإعدادات الموجودة في إدارة Cisco Unified Communications Manager وفقًا للجدول الزمني حتى إذا أرسل EnergyWise تجاوزًا. على سبيل المثال، بافتراض تعيين "وقت إيقاف تشغيل الهاتف" إلى 22:00 (الساعة 10:00 مساءً)، فإن القيمة الموجودة داخل حقل "وقت تشغيل الهاتف" تكون 06:00 (الساعة 6:00 صباحًا) ويحتوي وضع "تمكين توفير الطاقة الإضافي" على يوم واحد أو أكثر من يوم محدد. • إذا وجه EnergyWise الهاتف إلى إيقاف التشغيل عند 20:00 (الساعة 8:00 مساءً)، فيظل هذا التوجيه ساريًا (بافتراض عدم حدوث تدخل من مستخدم الهاتف) إلى أن يحين "وقت تشغيل الهاتف" المكون الساعة 6:00 صباحًا. • يتم تشغيل الهاتف الساعة 6:00 صباحًا ويستأنف الهاتف تلقي تغييرات مستوى الطاقة من إدارة Cisco Unified Communications Manager. • لتغيير مستوى الطاقة في الهاتف مرة أخرى، يجب أن يعيد EnergyWise إصدار أمر جديد لتغيير مستوى الطاقة. لتعطيل "توفير الطاقة الإضافي"، يجب إلغاء تحديد خانة اختيار "السماح بتجاوز EnergyWise". إذا ظل اختيار "السماح بتجاوز EnergyWise" محددًا دون تحديد أيام في حقل "توفير الطاقة الإضافي"، فلا يتم تعطيل "توفير الطاقة الإضافي". ارجع إلى جدولة EnergyWise على هاتف Cisco IP, في الصفحة 105.
سياسة الربط والتحويل المباشر	تمكين الخط نفسه تعطيل الخط نفسه	تمكين الخط نفسه والربط بين الخطوط	للتحكم في قدرة المستخدم على ربط المكالمات ونقلها. • تمكين الخط نفسه - يمكن للمستخدمين نقل مكالمة أو ربطها على الخط الحالي مباشرةً بمكالمة أخرى على الخط نفسه. • تعطيل الخط نفسه - يتعذر على المستخدمين نقل مكالمات أو الانضمام إليها على الخط نفسه. يتم تعطيل ميزتي الربط والنقل ويتعذر على المستخدمين إجراء النقل المباشر أو تنفيذ وظيفة الربط.

اسم الحقل	نوع الحقل أو الاختيارات	افتراضي	الوصف
نغمة التسجيل	معطل ممكن	معطل	للتحكم في تشغيل النغمة عندما يسجل المستخدم مكالمة
الصوت المحلي لنغمة التسجيل	عدد صحيح من 0 إلى 100	100	للتحكم في مستوى صوت تسجيل النغمة إلى المستخدم المحلي.
صوت نغمة التسجيل عن بُعد	عدد صحيح من 0 إلى 100	50	للتحكم في مستوى صوت تسجيل النغمة إلى المستخدم البعيد.
مدة نغمة التسجيل	مللي ثانية ممثلة في عدد صحيح من 1 إلى 3000		للتحكم في مدة نغمة التسجيل.
خادم التسجيل	سلسلة تضم ما يصل إلى 256 حرفًا		تحديد خادم سجل نظام IPv4 لإخراج تصحيح أخطاء الهاتف. تنسيق العنوان هو: **العنوان:<0-1>;pfs=<0-7>@@base=<port>**
السجل البعيد	معطل ممكن	معطل	التحكم في القدرة على إرسال السجلات إلى خادم سجل النظام.
ملف تعريف السجل	افتراضي معين مسبقًا المهاتفة SIP UI طبقة الشبكة الوسائط ترقية ملحق الأمان Energywise MobileRemoteAccess	معين مسبقًا	لتحديد ملف تعريف التسجيل المعرّف مسبقًا. • افتراضي - مستوى تسجيل تصحيح الأخطاء الافتراضي • معين مسبقًا - لعدم تعديل إعداد تسجيل تصحيح الأخطاء المحلي للهاتف • الهاتفية - لتسجيل معلومات حول ميزات الهاتفية أو المكالمات • SIP - لتسجيل معلومات حول تأشير SIP • واجهة المستخدم - لتسجيل معلومات عن واجهة مستخدم الهاتف • الشبكة - لتسجيل معلومات الشبكة • الوسائط - لتسجيل معلومات الوسائط • الترقية - لتسجيل معلومات الترقية • الملحقات - لتسجيل معلومات الملحقات • الأمان - لتسجيل معلومات الأمان • Energywise - لتسجيل معلومات توفير الطاقة • MobileRemoteAccess — لتسجيل الوصول إلى الأجهزة المتنقلة وRemote Access من خلال معلومات خادم Expressway
خادم تسجيل IPv6	سلسلة تضم ما يصل إلى 256 حرفًا		تحديد خادم سجل نظام IPv6 لإخراج تصحيح أخطاء الهاتف.

اسم الحقل	نوع الحقل أو الاختيارات	افتراضي	الوصف
بروتوكول اكتشاف Cisco (واختصاره CDP): منفذ جهاز تبديل	معطل ممكن	ممكن	التحكم في بروتوكول اكتشاف Cisco على الهاتف.
بروتوكول اكتشاف طبقة الارتباط - اكتشاف نقطة نهاية الوسائط (LLDP-MED): منفذ جهاز تبديل	معطل ممكن	ممكن	لتمكين LLDP-MED في منفذ SW.
LLDP Asset ID	سلسلة تضم ما يصل إلى 32 حرفًا		يحدد معرف الأصل المعين للهاتف لإدارة المخزون.
شبكة إيثرنت موفرة للطاقة (EEE): منفذ جهاز التبديل	معطل ممكن	معطل	للتحكم بـ EEE في منفذ جهاز التبديل.
LLDP Power Priority	غير معروف منخفضة مرتفعة حرج	غير معروف	لتعيين أولوية طاقة الهاتف إلى مفتاح التحويل، مما يتيح بالتالي لجهاز التبديل إمكانية توفير الطاقة بقدر مناسب للهواتف.
مصادقة 802.1x	تحكم مستخدم معطل ممكن	تحكم مستخدم	لتحديد حالة ميزة المصادقة وفقًا لمعيار 802.1x. • متحكم به من قِبل المستخدم - يمكن للمستخدم تكوين معيار 802.1x على الهاتف. • معطل - المصادقة وفقًا لمعيار 802.1x غير مستخدمة. • ممكّن - المصادقة وفقًا لمعيار X802.1 مستخدمة، ويمكنك تكوين مصادقة الهاتف.
تهيئة منفذ مفتاح التبديل عن بُعد	معطل تفاوض تلقائي 10 نصف 10 كامل 100 نصف 100 كامل	معطل	للسماح لك بتكوين السرعة ووظيفة الاتصال المزدوج لمنفذ SW في الهاتف عن بُعد. يعمل ذلك على تحسين أداء عمليات النشر الكبيرة باستخدام إعدادات محددة للمنفذ. إذا كانت منافذ SW مكونة وفقًا لتكوين المنفذ عن بُعد في Cisco Unified Communications Manager، فيتعذر تغيير البيانات على الهاتف.
الوصول إلى SSH	معطل ممكن	معطل	للتحكم في الوصول إلى البرنامج الخفي لـ SSH عبر المنفذ 22. يؤدي ترك المنفذ 22 مفتوحًا إلى جعل الهاتف معرضًا لهجمات قطع الخدمة (DoS).
الإعداد المحلي للرنين	افتراضي اليابان	افتراضي	للتحكم في نمط الرنين.

اسم الحقل	نوع الحقل أو الاختيارات	افتراضي	الوصف
مؤقت متابعة TLS	ثوان ممثلة بالعدد الصحيح من 0 إلى 3600	3600	للتحكم في القدرة على متابعة جلسة عمل TLS دون تكرار عملية مصادقة TLS بالكامل. إذا تم تعيين الحقل إلى 0، فيتم تعطيل متابعة جلسة عمل TLS.
وضع FIPS	معطل ممكن	معطل	لتمكين وضع "مقاييس معالجة المعلومات الفيدرالية (FIPS)" أو تعطيله على الهاتف.
التسجيل في سجل المكالمات من الخط المشترك	معطل ممكن	معطل	لتحديد ما إذا كان سيتم تسجيل مكالمة من خط مشترك.
أدنى مستوى لصوت الرنين	0 - صامت 15–1	0 - صامت	للتحكم في أدنى مستوى لصوت رنين الهاتف
تمكين البرامج الثابتة بين النظراء	معطل ممكن	ممكن	للسماح للهاتف بالبحث عن هواتف أخرى من الطراز نفسه على الشبكة الفرعية ومشاركة ملفات البرامج الثابتة التي تم تحديثها. إذا كان الهاتف يشتمل على تحميل جديد للبرامج الثابتة، فيمكنه مشاركة ذلك التحميل مع الهواتف الأخرى. إذا كان أحد الهواتف الأخرى يشتمل على تحميل جديد للبرامج الثابتة، فيمكن للهاتف تنزيل البرامج الثابتة من هاتف آخر، وذلك بدلاً من خادم TFTP. مشاركة البرامج الثابتة للنظراء: • لتحديد أوقات الذروة في عمليات النقل عبر TFTP لإزالة خوادم TFTP بشكل مكثف. • التخلص من الحاجة إلى التحكم يدويًا في ترقيات البرامج الثابتة. • التقليل من وقت تعطل الهاتف أثناء الترقيات عند إعادة تعيين عدد كبير من الهواتف في وقت واحد. • للمساعدة في ترقيات البرامج الثابتة خلال سيناريوهات النشر بمكتب فرعي أو عن بُعد، حيث تعمل هذه السيناريوهات عبر ارتباطات WAN ذات نطاق ترددي محدود.
خادم التحميل	سلسلة تضم ما يصل إلى 256 حرفًا		لتحديد خادم IPv4 البديل الذي يستخدمه الهاتف للحصول على عمليات تحميل البرامج الثابتة وترقياتها.
خادم تحميل IPv6	سلسلة تضم ما يصل إلى 256 حرفًا		لتحديد خادم IPv6 البديل الذي يستخدمه الهاتف للحصول على عمليات تحميل البرامج الثابتة وترقياتها.

اسم الحقل	نوع الحقل أو الاختيارات	افتراضي	الوصف
اكتشاف فشل اتصال Unified CM	عادي متأخر	عادي	لتحديد مدى حساسية الهاتف لاكتشاف فشل الاتصال بـ Cisco Unified Communications Manager (Unified CM)، والذي يمثل الخطوة الأولى قبل تجاوز فشل الجهاز في تشغيل Unified CM/SRST احتياطي. تحدد القيم الصالحة "عادي" (اكتشاف فشل اتصال Unified CM يحدث بمعدل النظام القياسي) أو "متأخر" (اكتشاف تجاوز فشل اتصال Unified CM يحدث تقريبًا أبطأ من "العادي" أربعة أضعاف). للتعرف بشكل أسرع على فشل اتصال Unified CM، اختر "عادي". إذا كنت تفضل تأخير تجاوز الفشل قليلاً لإتاحة الفرصة لإعادة إنشاء الاتصال، اختر "متأخر". يتوقف الفرق الدقيق بين توقيت اكتشاف فشل الاتصال "العادي" و"المتأخر" على العديد من المتغيرات التي تتغير بشكل مستمر.
معرف المتطلب الخاص	السلسلة		للتحكم في الميزات المخصصة من عمليات تحميل Engineering Special (ES)
خادم HTTPS	http وhttps ممكّنان https فقط	http وhttps ممكّنان	للتحكم في نوع الاتصال بالهاتف. إذا قمت بتحديد HTTPS فقط، يصبح اتصال الهاتف أكثر أمانًا.
استمرار تسجيل الدخول إلى Expressway ببيانات اعتماد المستخدم	معطل ممكن	معطل	للتحكم فيما إذا كان الهاتف سيخزن بيانات اعتماد تسجيل دخول المستخدم أم لا. عند تعطيلها، دائمًا ما يظهر للمستخدم موجه لتسجيل الدخول إلى خادم Expressway للوصول من الأجهزة المتنقلة وعن بُعد (MRA). إذا كنت ترغب في تسهيل تسجيل دخول المستخدمين، فقم بتمكين هذا الحقل لكي يتم الاحتفاظ ببيانات اعتماد تسجيل الدخول إلى Expressway. وعلى المستخدم عندئذٍ إدخال بيانات الاعتماد الخاصة به لتسجيل الدخول في المرة الأولى. حيث يتم نشر معلومات تسجيل الدخول على شاشة "تسجيل الدخول" في أي وقت بعد هذه المرة (عند تشغيل الهاتف خارج الموقع). للحصول على مزيد من المعلومات، ارجع إلى استمرار تسجيل الدخول إلى Expressway ببيانات اعتماد المستخدم, في الصفحة 113.
عنوان URL لتحميل دعم العملاء	سلسلة تضم ما يصل إلى 256 حرفًا		لتوفير عنوان URL الخاص بأداة الإبلاغ عن المشكلات (PRT). إذا قمت بنشر أجهزة مزودة بإمكانية "الوصول من الأجهزة المتنقلة وعن بُعد" من خلال Expressway، فيجب أيضًا أن تضيف عنوان خادم PRT إلى قائمة "السماح لخادم HTTP" على خادم Expressway. للحصول على مزيد من المعلومات، ارجع إلى استمرار تسجيل الدخول إلى Expressway ببيانات اعتماد المستخدم, في الصفحة 113.
تعطيل تشفيرات TLS	ارجع إلى تعطيل تشفيرات أمان طبقة النقل, في الصفحة 103.	بلا	تعطيل تشفير TLS المحدد. تعطيل واحد أو أكثر من مجموعة التشفير عن طريق تحديد والضغط باستمرار على مفتاح **Ctrl** على لوحة المفاتيح بالكمبيوتر.

اسم الحقل	نوع الحقل أو الاختيارات	افتراضي	الوصف
خط واحد لتخصيص ميزة تعليق المكالمة	معطل ممكن	ممكن	للتحكم فيما إذا كانت مكالمة معلقة تحتل خطًا واحدًا أم لا. للحصول على مزيد من المعلومات، راجع وثائق Cisco Unified Communications Manager.

موضوعات ذات صلة

استمرار تسجيل الدخول إلى Expressway ببيانات اعتماد المستخدم, في الصفحة 113

تعطيل تشفيرات أمان طبقة النقل

يمكنك تعطيل تشفيرات أمان طبقة النقل (TLS) باستخدام المعلمة **Disable TLS Ciphers**. يسمح لك هذا بتكييف الأمان للثغرات الأمنية المعروفة، وبمحاذاة شبكتك باستخدام نُهج الشركة للتشفيرات.

"بلا" هو الإعداد الافتراضي.

تعطيل واحد أو أكثر من مجموعة التشفير عن طريق تحديد والضغط باستمرار على مفتاح **Ctrl** على لوحة المفاتيح بالكمبيوتر. إذا قمت بتحديد جميع تشفيرات الهاتف، تتأثر خدمة TLS بالهاتف. خياراتك هي:

- بلا
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

لمزيد من المعلومات حول أمان الهاتف، راجع المستند التقني حول هواتف *Cisco IP 7800* ونظرة عامة حول أمان سلسلة *8800* (https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html).

جدول توفير الطاقة لهاتف Cisco IP

للحفاظ على الطاقة وضمان طول عمر عرض شاشة الهاتف، يمكنك تعيين العرض على وضع إيقاف التشغيل عند عدم الحاجة إليه.

يمكنك تكوين الإعدادات في إدارة Cisco Unified Communications Manager لإيقاف تشغيل العرض في وقت محدد في بعض الأيام وطوال اليوم في الأيام الأخرى. على سبيل المثال، يمكنك اختيار إيقاف عرض الشاشة بعد ساعات العمل خلال أيام الأسبوع وطوال أيام السبت والأحد.

يمكنك تنفيذ أي من هذه الإجراءات لتشغيل الشاشة في أي وقت تكون فيه قيد إيقاف التشغيل:

- اضغط على أي زر في الهاتف.

  يتخذ الهاتف الإجراء المحدد بواسطة هذا الزر بالإضافة إلى تشغيل الشاشة.

- ارفع سماعة الهاتف.

عند تشغيل الشاشة، تظل قيد التشغيل حتى يكون الهاتف في وضع السكون لفترة معينة من الوقت، ثم يتم إيقاف تشغيله تلقائيًا.

اجراء

الخطوة 1 في إدارة Cisco Unified Communications Manager، حدد **الجهاز** > **الهاتف**.

الخطوة 2 حدد موقع الهاتف الذي تريد إعداده.

الخطوة 3 انتقل إلى منطقة "التكوين الخاص بالمنتج" وعيّن الحقول التالية:

- أيام عدم نشاط الشاشة
- وقت تشغيل الشاشة
- مدة تشغيل الشاشة
- مهلة خمول الشاشة

الجدول *19*: حقول تكوين توفير الطاقة

الحقل	الوصف
أيام عدم نشاط الشاشة	الأيام التي لا يتم خلالها تشغيل الشاشة تلقائيًا في الوقت المحدد داخل حقل "وقت تشغيل الشاشة". اختر اليوم أو الأيام من القائمة المنسدلة. لاختيار أكثر من يوم، انقر فوق زر Ctrl لكل يوم تريده.
وقت تشغيل الشاشة	الوقت الذي يتم خلاله يوميًا تشغيل الشاشة تلقائيًا (باستثناء الأيام المحددة في حقل "شاشة الأيام غير نشطة"). أدخل الوقت في هذا الحقل بتنسيق 24 ساعة، حيث يشير التنسيق 00:00 ص إلى منتصف الليل. على سبيل المثال، لتشغيل الشاشة تلقائيًا في الساعة 07:00 صباحًا، (0700)، أدخل **07:00**. لتشغيل الشاشة تلقائيًا الساعة 02:00 مساءً. (1400)، أدخل **14:00**. إذا كان هذا الحقل فارغًا، فسيتم تشغيل الشاسة تلقائيًا عند الساعة 0:00.
مدة تشغيل الشاشة	طول الفترة الزمنية التي تبقى الشاشة خلالها قيد التشغيل بعد التشغيل عند الوقت المحدد داخل حقل "وقت تشغيل الشاشة". أدخِل القيمة في هذا الحقل بتنسيق ساعة:دقائق. على سبيل المثال، للاحتفاظ بتشغيل الشاشة لمدة 4 ساعات و30 دقيقة بعد تشغيلها تلقائيًا، أدخِل **04:30**. إذا كان هذا الحقل فارغًا، فسيتم إيقاف تشغيل الهاتف في نهاية اليوم (0:00). **ملاحظة** إذا كان "وقت تشغيل الشاشة" 0:00 ومدة تشغيل الشاشة فارغة (أو 24:00)، فستبقى الشاشة قيد التشغيل باستمرار.
مهلة خمول الشاشة	طول الفترة الزمنية التي يكون الهاتف خلالها في حالة سكون قبل إيقاف تشغيل الشاشة. يتم تطبيقه فقط عند إيقاف تشغيل الشاشة وفقًا للجدول الزمني وعند تشغيله بواسطة المستخدم (بالضغط على زر في الهاتف أو رفع سماعة الهاتف). أدخِل القيمة في هذا الحقل بتنسيق ساعة:دقائق. على سبيل المثال، لإيقاف تشغيل الشاشة عندما يكون الهاتف في وضع السكون لمدة ساعة و30 دقيقة بعد أن يقوم المستخدم بتشغيل الشاشة، أدخِل **01:30**. والقيمة الافتراضية هي 01:00.

الخطوة 4 حدد **حفظ**.

الخطوة 5 حدد **تطبيق التكوين**.

الخطوة 6 أعِد تشغيل الهاتف.

جدولة EnergyWise على هاتف Cisco IP

لتقليل استهلاك الطاقة، قم بتهيئة الهاتف لتعيينه في وضع السكون (إبطال التشغيل) والتنبيه (التشغيل) إذا كان النظام لديك يشتمل على وحدة تحكم EnergyWise.

قم بتكوين الإعدادات في "إدارة Cisco Unified Communications Manager" لتمكين EnergyWise وتكوين وضع السكون وأوقات التنبيه. ترتبط هذه المعلمات ارتباطًا وثيقًا بمعلمات تكوين شاشة الهاتف.

عند تمكين EnergyWise وتعيين وقت السكون، يرسل الهاتف طلبًا إلى جهاز التبديل لتنبيهه في الوقت الذي تم تكوينه. ويرد جهاز التبديل إما بقبول الطلب أو رفضه. إذا رفض جهاز التبديل الطلب أو إذا لم يرد، فلا يتم إبطال تشغيل الهاتف. إذا قبل جهاز التبديل الطلب، ينتقل الهاتف من وضع الخمول إلى وضع السكون، وبالتالي يقل استهلاك الطاقة إلى مستوى محدد مسبقًا. يعين الهاتف الذي خارج وضع الخمول مؤقتًا للخمول وينتقل إلى وضع السكون بعد انتهاء زمن مؤقت وضع الخمول.

لتنشيط الهاتف، اضغط تحديد. عند الوقت المجدول للتنبيه، يستعيد النظام توصيل الطاقة بالهاتف للتنبيه.

اجراء

الخطوة 1 من إدارة Cisco Unified Communications Manager، حدد **الجهاز** > **الهاتف**.

الخطوة 2 حدد موقع الهاتف الذي تريد إعداده.

الخطوة 3 انتقل إلى منطقة "التكوين الخاص بالمنتج" وقم بتعيين الحقول التالية.

- تمكين توفير الطاقة الإضافي
- وقت تشغيل الهاتف
- وقت إيقاف تشغيل الهاتف
- انتهاء مهلة خمول إيقاف تشغيل الهاتف
- تمكين التنبيه المسموع
- مجال EnergyWise
- كلمة سر EnergyWise
- السماح بتجاوز EnergyWise.

الجدول *20*: حقول تكوين *energyWise*

الحقل	الوصف
تمكين توفير الطاقة الإضافي	لتحديد الجدول الزمني للأيام التي يتم إيقاف تشغيل الهاتف خلالها. حدد عدة أيام بالضغط مع الاستمرار على المفتاح Control فوق أيام الجدول. بشكل افتراضي، لا يتم تحديد أي أيام. عند تحديد "تمكين توفير الطاقة الإضافي"، تتلقى رسالة تحذر من وجود مشكلات طارئة (e911). **تنبيه** أثناء نفاذ مفعول "وضع توفير الطاقة الإضافي" (يشار إليه باسم "الوضع")، يتم تعطيل نقاط النهاية المكونة للوضع عند المكالمات الطارئة ومنعها من تلقي المكالمات الواردة. بتحديد هذا الوضع، تقر بموافقتك على ما يلي: (1) أن تتحمل المسؤولية كاملة عن توفير طرق بديلة لمكالمات الطوارئ وتلقي المكالمات أثناء نفاذ مفعول الوضع، و(2) ألا تتحمل Cisco أية مسؤولية بشأن تحديدك للوضع وتخلي مسؤوليتها الكاملة بشأن تمكين الوضع الذي يُعد مسؤوليتك، و(3) أن تُعلم المستخدمين بالآثار المترتبة على المكالمات أثناء تشغيل الوضع والاتصال وغير ذلك. **ملاحظة** لتعطيل "توفير الطاقة الإضافي"، يجب إلغاء تحديد خانة اختيار "السماح بتجاوز EnergyWise". إذا ظل اختيار "السماح بتجاوز EnergyWise" محددًا دون تحديد أيام في حقل "توفير الطاقة الإضافي"، فلا يتم تعطيل "توفير الطاقة الإضافي".
وقت تشغيل الهاتف	لتحديد الوقت الذي يتم خلاله تشغيل الهاتف تلقائيًا وفقًا للأيام الموجودة في حقل "تمكين توفير الطاقة الإضافي". أدخل الوقت في هذا الحقل بتنسيق 24 ساعة، حيث يشير التنسيق 00:00 إلى منتصف الليل. على سبيل المثال، لتشغيل الهاتف تلقائيًا في الساعة 07:00 صباحًا (0700)، أدخل 07:00. لتشغيل الهاتف الساعة 02:00 ظهرًا (1400)، أدخل 14:00. القيمة الافتراضية فارغة، مما يعني أنها 00:00. **ملاحظة** يجب أن يكون "وقت تشغيل الهاتف" بعد "وقت إيقاف تشغيل الهاتف" بمدة مقدارها 20 دقيقة على الأقل. على سبيل المثال، إذا كان "وقت إيقاف تشغيل الهاتف" الساعة 07:00، فيجب ألا يكون "وقت تشغيل الهاتف" قبل الساعة 07:20.
وقت إيقاف تشغيل الهاتف	يتم تحديد الوقت الذي يتم خلاله إبطال تشغيل الهاتف تلقائيًا في اليوم وفقًا لما هو محدد في حقل "تمكين توفير الطاقة الإضافي". إذا كان حقلا "وقت تشغيل الهاتف" و"وقت إيقاف تشغيل الهاتف" يحتويان على القيمة نفسها، فلا يتم إبطال تشغيل الهاتف. أدخل الوقت في هذا الحقل بتنسيق 24 ساعة، حيث يشير التنسيق 00:00 إلى منتصف الليل. على سبيل المثال، لإيقاف تشغيل الهاتف تلقائيًا في الساعة 7:00 صباحًا (0700)، أدخل 7:00. لإيقاف تشغيل الهاتف الساعة 2:00 ظهرًا (1400)، أدخل 14:00. القيمة الافتراضية فارغة، مما يعني أنها 00:00. **ملاحظة** يجب أن يكون "وقت تشغيل الهاتف" بعد "وقت إيقاف تشغيل الهاتف" بمدة مقدارها 20 دقيقة على الأقل. على سبيل المثال، إذا كان "وقت إيقاف تشغيل الهاتف" الساعة 7:00، فيجب ألا يكون "وقت تشغيل الهاتف" قبل الساعة 7:20.

الحقل	الوصف
انتهاء مهلة خمول إيقاف تشغيل الهاتف	يجب أن يكون طول الفترة الزمنية التي يكون الهاتف خلالها في حالة خمول قبل إبطال تشغيل الهاتف. تنتهي المهلة بموجب الشروط التالية: • إذا كان الهاتف في وضع "توفير الطاقة الإضافي" وفقًا للجدول الزمني، وتم إخراجه من وضع "توفير الطاقة الإضافي" نظرًا لضغط مستخدم الهاتف على مفتاح "**تحديد**". • عند إعادة تشغيل الهاتف من خلال جهاز التبديل المتصل. • عند الوصول إلى "وقت إيقاف تشغيل الهاتف"، ولكن الهاتف قيد الاستخدام. نطاق الحقل يتراوح بين 20 إلى 1440 دقيقة. القيمة الافتراضية هي 60 دقيقة.
تمكين التنبيه المسموع	عند تمكينه، يتم توجيه الهاتف إلى تشغيل تنبيه مسموع يبدأ قبل 10 دقائق من الوقت المحدد في حقل "وقت إيقاف تشغيل الهاتف". يستخدم التنبيه الصوتي نغمة رنين الهاتف، حيث يصدر لفترة وجيزة في أوقات معينة أثناء فترة التنبيه البالغة 10 دقائق. يتم تشغيل نغمة رنين التنبيه عند مستوى الصوت الذي يخصصه المستخدم. يكون الجدول الزمني للتنبيه الصوتي: • قبل إيقاف تشغيل الطاقة بـ 10 دقائق، تشتغل نغمة الرنين أربع مرات. • قبل إيقاف تشغيل الطاقة بـ 7 دقائق، تشتغل نغمة الرنين أربع مرات. • قبل إيقاف تشغيل الطاقة بـ 4 دقائق، تشتغل نغمة الرنين أربع مرات. • قبل إيقاف تشغيل الطاقة بـ 30 ثانية، يتم تشغيل نغمة الرنين 15 مرة أو لحين إيقاف تشغيل الهاتف. يتم تطبيق خانة الاختيار هذه فقط إذا كانت خانة قائمة "توفير الطاقة الإضافي" تحتوي على يوم واحد أو أكثر من يوم مختار.
مجال EnergyWise	مجال EnergyWise الذي يوجد به الهاتف. أقصى طول لهذا الحقل 127 حرفاً.
كلمة سر EnergyWise	كلمة مرور الأمان السرية المستخدمة للاتصال بنقاط النهاية الموجودة بنطاق EnergyWise. أقصى طول لهذا الحقل 127 حرفاً.

الحقل	الوصف
السماح بتجاوز EnergyWise.	تحدد خانة الاختيار هذه ما إذا كنت تسمح لسياسة وحدة التحكم في نطاق EnergyWise بإرسال تحديثات مستوى الطاقة إلى الهواتف أم لا. تنطبق الشروط التالية: • يجب تحديد يوم واحد أو أكثر من يوم في حقل "تمكين توفير الطاقة الإضافي". • تسري الإعدادات الموجودة في إدارة Cisco Unified Communications Manager وفقًا للجدول الزمني حتى إذا أرسل EnergyWise تجاوزًا. على سبيل المثال، بافتراض تعيين "وقت إيقاف تشغيل الهاتف" إلى 22:00 (الساعة 10:00 مساءً)، فإن القيمة الموجودة داخل حقل "وقت تشغيل الهاتف" تكون 06:00 (الساعة 6:00 صباحًا) ويحتوي وضع "تمكين توفير الطاقة الإضافي" على يوم واحد أو أكثر من يوم محدد. • إذا وجه EnergyWise الهاتف إلى إيقاف التشغيل عند 20:00 (الساعة 8:00 مساءً)، فيظل هذا التوجيه ساريًا (بافتراض عدم حدوث تدخل من مستخدم الهاتف) إلى أن يحين "وقت تشغيل الهاتف" المكون الساعة 6:00 صباحًا. • يتم تشغيل الهاتف الساعة 6:00 صباحًا ويستأنف الهاتف تلقي تغييرات مستوى الطاقة من إدارة Unified Communications Manager. • لتغيير مستوى الطاقة في الهاتف مرة أخرى، يجب أن يعيد EnergyWise إصدار أمر جديد لتغيير مستوى الطاقة. **ملاحظة** لتعطيل "توفير الطاقة الإضافي"، يجب إلغاء تحديد خانة اختيار "السماح بتجاوز EnergyWise". إذا ظل اختيار "السماح بتجاوز EnergyWise" محددًا دون تحديد أيام في حقل "توفير الطاقة الإضافي"، فلا يتم تعطيل "توفير الطاقة الإضافي".

الخطوة 4 حدد **حفظ**.

الخطوة 5 حدد **تطبيق التكوين**.

الخطوة 6 أعِد تشغيل الهاتف.

إعداد ميزة عدم الإزعاج

عند تشغيل عدم الإزعاج (DND)، يضيء الرأس الموجود على شاشة هاتف المؤتمر باللون الأحمر.

لمزيد من المعلومات، راجع معلومات عدم الإزعاج في الوثائق الخاصة بإصدار Cisco Unified Communications Manager الخاص بك.

اجراء

الخطوة 1 في إدارة Cisco Unified Communications Manager، حدد **الجهاز** > **الهاتف**.

الخطوة 2 حدد موقع الهاتف المطلوب تكوينه.

الخطوة 3 قم بتعيين المعلمات التالية.

- عدم الإزعاج: تتيح لك خانة الاختيار هذه تمكين DND على الهاتف.
- خيار DND: إيقاف الرنين، أو رفض المكالمة، أو استخدام إعداد ملف تعريف الهاتف العام.
- DND عند التنبيه بالمكالمات الواردة: اختر نوع التنبيه، إن وجد، الذي تريد تشغيله على الهاتف للمكالمات الواردة عندما تكون ميزة DND نشطة.

ملاحظة توجد هذه المعلمة في نافذة ملف تعريف الهاتف العام ونافذة تكوين الهاتف. وتكون الأسبقية لقيمة نافذة تكوين الهاتف.

الخطوة 4 حدد **حفظ**.

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14

إعداد الإعلام بإعادة توجيه مكالمة

يمكنك التحكم في إعدادات إعادة توجيه مكالمة.

اجراء

الخطوة 1 في إدارة Cisco Unified Communications Manager، حدد **الجهاز** > **الهاتف**.

الخطوة 2 حدد موقع الهاتف المطلوب إعداده.

الخطوة 3 قم بتكوين حقول الإعلام بإعادة توجيه مكالمة.

الحقل	الوصف
Caller Name	عند تحديد خانة الاختيار هذه، يتم عرض اسم المتصل في نافذة الإعلام. بشكل افتراضي، يتم تحديد خانة الاختيار هذه.
Caller Number	عند تحديد خانة الاختيار هذه، يتم عرض رقم المتصل في نافذة الإعلام. بشكل افتراضي، لا يتم تحديد خانة الاختيار هذه.
الرقم المعاد توجيهه	عند تحديد خانة الاختيار هذه، يتم عرض معلومات حول المتصل الذي أعاد توجيه المكالمة مؤخرًا في نافذة الإعلام. مثال: إذا اتصل المتصل "أ" بالشخص "ب"، ولكن "ب" أعاد توجيه جميع المكالمات إلى الشخص "ج" وأعاد "ج" توجيه جميع المكالمات إلى الشخص "د"، فإن مربع الإعلام الذي يراه "د" يحتوي على معلومات الهاتف الخاص بالمتصل "ج". بشكل افتراضي، لا يتم تحديد خانة الاختيار هذه.
الرقم المطلوب	عند تحديد خانة الاختيار هذه، يتم عرض معلومات المتلقي الأصلي للمكالمة في نافذة الإعلام. مثال: إذا اتصل المتصل "أ" بالشخص "ب"، ولكن "ب" أعاد توجيه جميع المكالمات إلى الشخص "ج" وأعاد "ج" توجيه جميع المكالمات إلى الشخص "د"، فإن مربع الإعلام الذي يراه "د" يحتوي على معلومات الهاتف الخاص بالمتصل "ب". بشكل افتراضي، يتم تحديد خانة الاختيار هذه.

الخطوة 4 حدد **حفظ**.

إعداد UCR 2008

المعلمات التي تدعم UCR 2008 موجودة داخل إدارة Cisco Unified Communications Manager. يصف الجدول التالي المعلمات ويشير إلى مسار تغيير الإعداد.

الجدول *21*: موقع معلمة *UCR 2008*

المعلمة	مسار الإدارة
وضع FIPS	**الجهاز** > **إعدادات الجهاز** > **ملف التعريف الشائع للهاتف**
	النظام > **تكوين هاتف المؤسسة**
	الجهاز > **الهواتف**
الوصول إلى SSH	**الجهاز** > **الهاتف**
	الجهاز > **إعدادات الجهاز** > **ملف التعريف الشائع للهاتف**
الوصول إلى الويب	**الجهاز** > **الهاتف**
	النظام > **تكوين هاتف المؤسسة**
	الجهاز > **إعدادات الجهاز** > **ملف التعريف الشائع للهاتف**
النظام > **تكوين هاتف المؤسسة**	
وضع عنونة IP	**الجهاز** > **إعدادات الجهاز** > **تكوين الجهاز العام**
تفضيل وضع عنونة IP لإرسال الإشارة	**الجهاز** > **إعدادات الجهاز** > **تكوين الجهاز العام**

إعداد UCR 2008 في تكوين الجهاز العام

استخدم هذا الإجراء لتعيين معلمات UCR 2008 التالية.

- وضع عنونة IP
- تفضيل وضع عنونة IP لإرسال الإشارة

اجراء

الخطوة 1 في إدارة Cisco Unified Communications Manager، اختر **الجهاز** > **إعدادات الجهاز** > **تكوين الجهاز العام**.

الخطوة 2 قم بتعيين معلمة "وضع عنونة IP".

الخطوة 3 قم بتعيين معلمة "تفضيل وضع عنونة IP لإرسال الإشارة".

الخطوة 4 حدد **حفظ**.

إعداد UCR 2008 في ملف تعريف الهاتف العام

استخدم هذا الإجراء لتعيين معلمات UCR 2008 التالية.

- وضع FIPS
- الوصول إلى SSH
- الوصول إلى الويب

اجراء

الخطوة 1	في إدارة Cisco Unified Communications Manager، اختر **الجهاز** > **إعدادات الجهاز** > **ملف تعريف الهاتف العام**.
الخطوة 2	قم بتعيين معلمة "وضع FIPS" إلى **ممكّن**.
الخطوة 3	قم بتعيين معلمة "الوصول إلى SSH" إلى **معطل**.
الخطوة 4	قم بتعيين معلمة "الوصول إلى الويب" إلى **معطل**.
الخطوة 5	قم بتعيين معلمة "□80 SRTCP بت" إلى **ممكّن**.
الخطوة 6	حدد **حفظ**.

إعداد UCR 2008 في تكوين هاتف المؤسسة

استخدم هذا الإجراء لتعيين معلمات UCR 2008 التالية.

- وضع FIPS
- الوصول إلى الويب

اجراء

الخطوة 1	في إدارة Cisco Unified Communications Manager، اختر **النظام** > **تكوين هاتف المؤسسة**.
الخطوة 2	قم بتعيين معلمة "وضع FIPS" إلى **ممكّن**.
الخطوة 3	قم بتعيين معلمة "الوصول إلى الويب" إلى **معطل**.
الخطوة 4	حدد **حفظ**.

إعداد UCR 2008 في الهاتف

استخدم هذا الإجراء لتعيين معلمات UCR 2008 التالية.

- وضع FIPS
- الوصول إلى SSH
- الوصول إلى الويب

اجراء

الخطوة 1	في إدارة Cisco Unified Communications Manager، اختر **الجهاز** > **الهاتف**.
الخطوة 2	قم بتعيين معلمة "الوصول إلى SSH" إلى **معطل**.
الخطوة 3	قم بتعيين معلمة "وضع FIPS" إلى **ممكّن**.

الخطوة 4 قم بتعيين معلمة "الوصول إلى الويب" إلى **معطل**.

الخطوة 5 حدد **حفظ**.

تقنية الوصول عن بعد ومن الأجهزة المتنقلة من خلال الخادم Expressway

تقنية الوصول عن بعد ومن الأجهزة المتنقلة من خلال الخادم Expressway(MRA) تتيح للعاملين عن بُعد الاتصال بسهولة وأمان بشبكة الشركة دون استخدام اتصال نفقي عميل عبر شبكة خاصة ظاهرية (VPN). يستخدم Expressway أمان طبقة النقل (TLS) لتأمين حركة مرور الشبكة. حتى يمكن لهاتف مصادقة شهادة Expressway وإنشاء جلسة TLS، يقوم مرجع مصدق عام يثق فيه برنامج الهاتف الثابت بالتوقيع على شهادة Expressway. لا يمكن تثبيت شهادات أخرى من مرجع مصدق (CA) آخر أو الثقة بها على الهاتف لمصادقة شهادة Expressway.

تتوفر قائمة شهادات CA المضمنة في برنامج الهاتف الثابت على موقع http://www.cisco.com/c/en/us/support/collaboration—endpoints/unified—ip—phone—8800—series/products—technical—reference—list.html.

تقنية الوصول عن بعد ومن الأجهزة المتنقلة من خلال الخادم Expressway (MRA) يعمل مع Cisco Expressway. يجب أن تكون على دراية بوثائق Cisco Expressway، بما في ذلك دليل مسؤول *Cisco Expressway* ودليل نشر تهيئة *Cisco Expressway* الأساسية. تتوفر وثائق Cisco Expressway على http://www.cisco.com/c/en/us/support/unified—communications/expressway—series/tsd—products—support—series—home.html.

بروتوكول IPv4 فقط مدعوم لمستخدمي تقنية الوصول عن بعد ومن الأجهزة المتنقلة من خلال الخادم Expressway.

للحصول على مزيد من المعلومات حول التعامل مع تقنية الوصول عن بعد ومن الأجهزة المتنقلة من خلال الخادم Expressway، راجع:

- بنية تعاون المؤسسات المفضلة لدى *Cisco*، نظرة عامة على التصميم
- بنية تعاون المؤسسات المفضلة لدى *Cisco*، برنامج *CVD*
- *Mobile Remote Access via Cisco VCS Deployment Guide* لـ *Unified Communications*
- *Cisco TelePresence Video Communication Server (VCS)*، أدلة التكوين
- *Mobile and Remote Access* من خلال دليل *Cisco Expressway Deployment*

أثناء عملية تسجيل الهاتف، يقوم الهاتف بمزامنة التاريخ والوقت المعروضين مع خادم بروتوكول وقت الشبكة (NTP). باستخدام MRA، يتم استخدام علامة خيار DHCP 42 لتحديد عناوين IP لخوادم NTP المخصصة لمزامنة الوقت والتاريخ. في حالة عدم العثور على علامة DHCP option 42 في معلومات التهيئة، فيبحث الهاتف عن علامة tandberg.pool.ntp.org.0 لتحديد هوية خوادم NTP.

بعد التسجيل، يستخدم الهاتف المعلومات الواردة من رسالة SIP لمزامنة الوقت والتاريخ المعروضين، وذلك ما لم يوجد خادم NTP مهيئًا في تهيئة Cisco Unified Communications Manager على الهاتف.

ملاحظة إذا تم تحديد "تكوين تشفير TFTP" في ملف تعريف أمان أي من هواتفك، فلا يمكنك استخدام الهاتف مقترنًا بإمكانية "الوصول من الأجهزة المتنقلة وعن بُعد". لا يدعم حل MRA تفاعل الأجهزة مع وظيفة وكيل جهة منح الشهادات (CAPF).

وضع SIP OAuth مدعوم لـ MRA. يتيح لك هذا الوضع استخدام رموز وصول OAuth للمصادقة في بيئات آمنة.

ملاحظة بالنسبة إلى SIP OAuth في وضع الوصول عن بُعد والجوال (MRA)، استخدم فقط إعداد رمز التنشيط مع الوصول عبر الهاتف المحمول والبعيد عند نشر الهاتف. التنشيط باستخدام اسم مستخدم وكلمة مرور غير مدعومين.

يتطلب وضع SIP OAuth استخدام Expressway x14.0(1) والإصدارات الأحدث أو Cisco Unified Communications Manager 14.0(1) والإصدارات الأحدث.

للحصول على معلومات إضافية حول وضع SIP OAuth، راجع دليل تكوين الميزات لبرنامج *Cisco Unified Communications Manager*، الإصدار 14.0(1) أو أحدث.

سيناريوهات النشر

يبين الجدول التالي مجموعة من سيناريوهات النشر المختلفة لـ تقنية الوصول عن بعد ومن الأجهزة المتنقلة من خلال الخادم Expressway.

السيناريو	الإجراءات
يُسجل المستخدم الداخلي الدخول إلى شبكة المؤسسة بعد نشر تقنية الوصول عن بعد ومن الأجهزة المتنقلة من خلال الخادم Expressway.	يتم اكتشاف شبكة المؤسسة، ويتم تسجيل الهاتف من خلال Cisco Unified Communications Manager كالمعتاد.
يُسجل المستخدم الخارجي الدخول إلى شبكة المؤسسة من خلال تقنية الوصول عن بعد ومن الأجهزة المتنقلة من خلال الخادم Expressway.	يكتشف الهاتف أنه في الوضع الخارجي، تظهر نافذة تسجيل الدخول تقنية الوصول عن بعد ومن الأجهزة المتنقلة من خلال الخادم Expressway ويتصل المستخدم بشبكة الشركة. يجب أن يمتلك المستخدمون اسم خدمة واسم مستخدم وكلمة مرور صالحة للاتصال بالشبكة. يجب على المستخدمين أيضا إعادة تعيين وضع الخدمة لمسح إعداد خادم TFTP البديل قبل يتسنى لهم الوصول إلى شبكة الشركة. يؤدي هذا إلى مسح إعداد "خادم TFTP البديل"، ولذا يكتشف الهاتف اكتشاف الشبكة الخارجية. إذا تم نشر الهاتف وأصبح جاهزًا للاستخدام، يستطيع المستخدمون تخطي طلب إعادة تعيين إعدادات الشبكة. إذا كان خيار DHCP 150 أو 66 ممكنًا على موجه الشبكة لدى المستخدمين، فقد لا يتمكنوا من تسجيل الدخول إلى شبكة الشركة. ينبغي على المستخدمين تعطيل إعدادات DHCP أو تكوين عنوان IP الثابت مباشرة.

استمرار تسجيل الدخول إلى Expressway ببيانات اعتماد المستخدم

عند قيام مستخدم بتسجيل الدخول إلى الشبكة باستخدام تقنية الوصول عن بعد ومن الأجهزة المتنقلة من خلال الخادم Expressway، تتم مطالبة المستخدم بمجال خدمة واسم المستخدم وكلمة المرور. إذا قمت بتمكين "معلمة بيانات اعتماد المستخدم المستمرة لمعلمة Expressway"، يتم تخزين بيانات اعتماد تسجيل دخول المستخدم حتى إذا لم تكن بحاجة إلى إعادة إدخال هذه المعلومات. يتم تعطيل هذه المعلمة بشكل افتراضي.

يمكنك إعداد بيانات اعتماد لمواصلة لهاتف واحد أو مجموعة من الهواتف أو كل الهواتف.

موضوعات ذات صلة

تكوين ميزات الهاتف, في الصفحة 91
التكوين الخاص بالمنتج, في الصفحة 93

أداة الإبلاغ عن المشكلات

يرسل المستخدمون تقارير بالمشكلات إليك باستخدام "أداة الإبلاغ عن المشكلات".

ملاحظة تتم المطالبة بسجلات "أداة الإبلاغ عن المشكلات" من خلال Cisco TAC عند استكشاف المشكلات وإصلاحها. يتم مسح السجلات إذا أعدت تشغيل الهاتف. قم بتجميع السجلات قبل إعادة تشغيل الهواتف.

لإصدار تقرير بالمشكلة، يتاح للمستخدمين الوصول إلى "أداة الإبلاغ عن المشكلات" وذكر وقت وتاريخ حدوث المشكلة وتقديم وصف لها.

إذا فشل تحميل PRT، يمكنك الوصول إلى ملف PRT للهاتف من عنوان URL **<http://<phone-ip-address>/FS/<prt-file-name>**. ويتم عرض عنوان URL على الهاتف في الحالات التالية:

- إذا كان الهاتف في حالة المصنع الافتراضية. يظل عنوان URL نشطًا لمدة ساعة واحدة. بعد ساعة واحدة، يجب أن يجرب المستخدم إرسال سجلات الهاتف مرة أخرى.
- إذا تم تنزيل ملف تهيئة على الهاتف وسمح نظام التحكم في المكالمة بوصول الويب إلى الهاتف.

يجب أن تضيف عنوان خادم إلى حقل **عنوان URL الخاص بتحميل دعم العملاء** في Cisco Unified Communications Manager.

إذا كنت بصدد نشر أجهزة مزودة بإمكانية "الوصول من الأجهزة المتنقلة وعن بُعد" من خلال Expressway، فيجب أيضًا أن تضيف عنوان خادم PRT إلى قائمة "السماح لخادم HTTP" على خادم Expressway.

تكوين عنوان URL لتحميل دعم العملاء

يجب أن تستخدم خادمًا مقترنًا ببرنامج نصي للتحميل لتلقي ملفات PRT. يستخدم PRT آلية HTTP POST، مع تضمين المعلمات التالية في التحميل (مستفيدًا من ترميز MIME متعدد الأجزاء):

- اسم الجهاز (على سبيل المثال: "SEP001122334455")
- السيناريو (على سبيل المثال: "FCH12345ABC")
- اسم المستخدم (اسم المستخدم الذي تم تهيئته في Cisco Unified Communications Manager، مالك الجهاز)
- prt_file (على سبيل المثال: "probrep-20141021-162840.tar.gz")

يظهر برنامج نصي نموذجي أدناه. تم عرض هذا البرنامج النصي للرجوع إليه فقط. لا توفر Cisco الدعم لبرنامج التحميل النصي الذي تم تثبيته على أحد خوادم العميل.

```
php?>

// NOTE: you may need to edit your php.ini file to allow larger
                                    // size file uploads to work.
                          // Modify the setting for upload_max_filesize
                                  // I used:  upload_max_filesize = 20M

                                  // Retrieve the name of the uploaded file
                              $filename = basename($_FILES['prt_file']['name']);

// Get rid of quotes around the device name, serial number and username if they exist
                                        $devicename = $_POST['devicename'];
                                    $devicename = trim($devicename, "'\"");

                                        $serialno = $_POST['serialno'];
                                    $serialno = trim($serialno, "'\"");

                                        $username = $_POST['username'];
                                    $username = trim($username, "'\"");

                                              // where to put the file
                              $fullfilename = "/var/prtuploads/".$filename;
```

```
// If the file upload is unsuccessful, return a 500 error and
                                        // inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
                                header("HTTP/1.0 500 Internal Server Error");
                    ;(".        die("Error: You must select a file to upload
                                                                        {

                                                                        <?
```

ملاحظة لا تدعم الهواتف سوى عناوين URL لـ HTTP.

اجراء

الخطوة 1 قم بإعداد خادم يمكن من خلاله تشغيل برنامج تحميل نصي لملفات PRT.

الخطوة 2 اكتب برنامجًا نصيًا يمكن من خلاله معالجة المعلمات المذكورة أعلاه أو حرّر البرنامج النصي النموذجي الوارد ليناسب احتياجاتك.

الخطوة 3 حمِّل برنامجك النصي إلى خادمك.

الخطوة 4 في Cisco Unified Communications Manager، انتقل إلى منطقة "مخطط التهيئة الخاص بالمنتج" في نافذة تهيئة الجهاز الفردي او نافذة "ملف تعريف الهاتف العام" أو نافذة "تهيئة هاتف المؤسسة".

الخطوة 5 تحقق من **عنوان URL للتحميل الخاص بدعم العملاء** وأدخل عنوان UR لخادم التحميل.

أمثلة:

http://example.com/prtscript.php

الخطوة 6 قم بحفظ التغييرات التي قمت بإجرائها.

تعيين تسمية الخط

يمكنك إعداد الهاتف لعرض تسمية نصية بدلاً من رقم الدليل. استخدم هذه التسمية لتحديد الخط حسب الاسم أو الوظيفة. على سبيل المثال، إذا كان المستخدم لديك يشارك خطوطًا على الهاتف، فيمكنك تحديد هوية الخط المقترن باسم الشخص الذي يشارك الخط.

عند إضافة تسمية إلى وحدة توسيع أساسية، فإنه يتم عرض الـ 25 حرفًا الأولى فقط على الخط.

اجراء

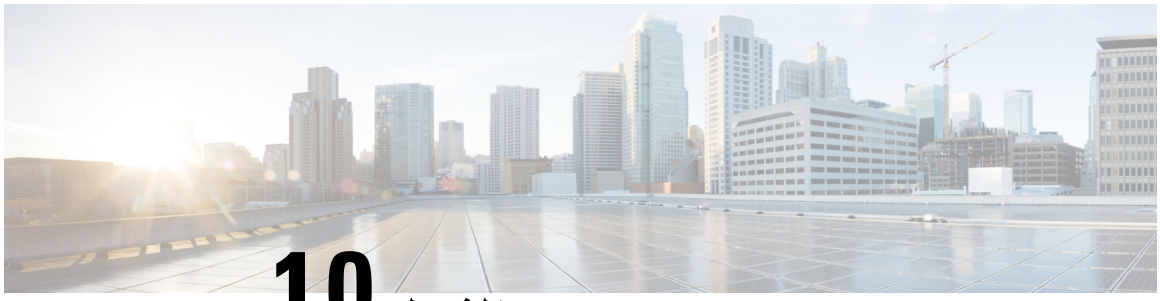
الخطوة 1 في إدارة Cisco Unified Communications Manager، حدد **الجهاز** > **الهاتف**.

الخطوة 2 حدد موقع الهاتف المطلوب تكوينه.

الخطوة 3 حدد مثيل الخط وقم بتعيين حقل "التسمية النصية للخط".

الخطوة 4 (اختياري) إذا كان يلزم تطبيق التسمية على أجهزة أخرى تقوم بمشاركة الخط، فحدد خانة اختيار "تحديث إعدادات الجهاز المشترك" والنقر فوق **نشر ما تم تحديده**.

الخطوة 5 حدد **حفظ**.



الفصل 10

دليل الشركة والدليل الشخصي

إعداد دليل الشركة

يتيح "دليل الشركة" للمستخدم البحث في أرقام الهواتف عن زملاء العمل. لدعم هذه الميزة، يجب أن تقوم بتهيئة أدلة الشركة.

يستخدم دليل Cisco Unified Communications Manager Lightweight Directory Access Protocol (LDAP) لتخزين معلومات المصادقة والتخويل المتعلقة بمستخدمي تطبيقات Cisco Unified Communications Manager التي تتفاعل مع Cisco Unified Communications Manager. تؤسس المصادقة حقوق المستخدم في الوصول إلى النظام. وتحدد المصادقة مصادر الهاتفية المصرح للمستخدم باستخدامها، مثل امتداد هاتف محدد.

للحصول على مزيد من المعلومات، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.S

بعد إكمال تهيئة دليل LDAP، يمكن للمستخدمين استخدام خدمة "دليل الشركة" على هاتفهم للبحث في المستخدمين الموجودين في دليل الشركة.

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14

إعداد الدليل الشخصي

يتيح "الدليل الشخصي" للمستخدم تخزين مجموعة من الأرقام الشخصية.

يشتمل "الدليل الشخصي" على الميزات التالية:

- دفتر العناوين الشخصي (PAB)
- الطلب السريع

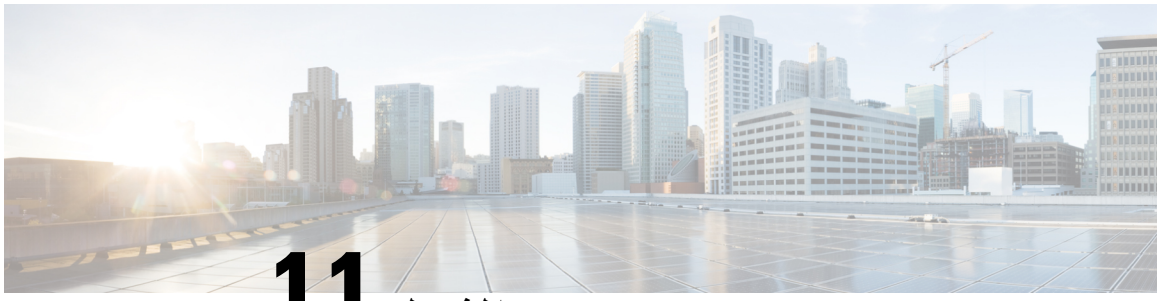
يمكن للمستخدمين استخدام هذه الطرق للوصول إلى ميزات "الدليل الشخصي":

- من مستعرض ويب — يمكن للمستخدمين الوصول إلى ميزات PAB والطلبات السريعة من مدخل Cisco Unified Communications Self Care.
- من هاتف CiscoIP - اختر **جهات الاتصال** المراد البحث عنها في دليل الشركة أو الدليل الشخصي للمستخدم.

لتهيئة "الدليل الشخصي" من مستعرض ويب، يجب على المستخدمين الوصول إلى مدخل Self Care لديهم. يجب أن تمد المستخدمين بعنوان URL ومعلومات تسجيل الدخول.

الجزء IV

استكشاف أخطاء هاتف مؤتمر Cisco IP وإصلاحها



الفصل 11

مراقبة أنظمة الهواتف

نظرة عامة على مراقبة أنظمة الهواتف

يمكنك عرض مجموعة متنوعة من المعلومات المتعلقة بالهاتف باستخدام قائمة حالة الهاتف الموجودة على الهاتف وصفحات الهاتف على الويب. وتشمل هذه المعلومات ما يلي:

- معلومات الجهاز
- معلومات إعداد الشبكة
- إحصائيات الشبكة
- سجلات الأجهزة
- إحصائيات التدفق

يصف الفصل المعلومات التي يمكنك الحصول عليها من صفحة الهاتف على الويب. يمكنك استخدام هذه المعلومات لمراقبة تشغيل الهاتف عن بُعد والمساعدة في استكشاف المشكلات وإصلاحها.

موضوعات ذات صلة

استكشاف أخطاء الهاتف وإصلاحها, في الصفحة 145

حالة هاتف Cisco IP

تصف الأقسام التالية كيفية عرض معلومات الطراز ورسائل الحالة وإحصاءات الشبكة على هاتف Cisco IP .

- معلومات الطراز: يعرض معلومات الأجهزة والبرامج المتعلقة بالجهاز.
- قائمة الحالة: يوفر إمكانية الوصول إلى الشاشات التي تعرض رسائل الحالة وإحصاءات الشبكة والإحصاءات الخاصة بالمكالمة الحالية.

يمكنك استخدام المعلومات التي يتم عرضها على هذه الشاشات لمراقبة تشغيل الهاتف والمساعدة في استكشاف المشكلات وإصلاحها.

يمكنك أيضًا الحصول على الكثير من هذه المعلومات وعلى غيرها من المعلومات ذات الصلة، وذلك من خلال صفحة ويب الهاتف عن بُعد.

عرض نافذة معلومات الهاتف

اجراء

الخطوة 1 اضغط على **الإعدادات** > **معلومات النظام**.
الخطوة 2 للخروج من القائمة، اضغط على **خروج**.

عرض قائمة الحالة

اجراء

الخطوة 1 اضغط على **الإعدادات** > **الحالة**.
الخطوة 2 للخروج من القائمة، اضغط على **خروج**.

عرض نافذة رسائل الحالة

اجراء

الخطوة 1 اضغط على **الإعدادات** > **الحالة** > **رسائل الحالة** .
الخطوة 2 للخروج من القائمة، اضغط على **خروج**.

حقول رسائل الحالة

يصف الجدول التالي رسائل الحالة التي يتم عرضها على شاشة "رسائل الحالة" الخاصة بالهاتف.

الجدول *22*: رسائل الحالة على هاتف *Cisco IP*

أدخل الرسالة في الحقل الرسالة.	الوصف	التوضيح والإجراء المحتملان
تعذر الحصول على عنوان IP من DHCP	لم يحصل الهاتف سابقًا على عنوان IP من خادم DHCP. قد يحدث ذلك عند إجراء إعادة تعيين الجهاز لأول مرة أو إعادة تعيين إعدادات المصنع.	تأكد من توفر خادم DHCP وعنوان IP للهاتف
خطأ في حجم TFTP	حجم ملف التكوين كبير جدًا بالنظر إلى سعة نظام الملفات على الهاتف.	أعد تشغيل دورة الطاقة للهاتف.
خطأ مجموع اختباري ROM	تعرض ملف البرامج الذي تم تنزيله للتلف.	احصل على نسخة جديدة من البرامج الثابتة للهـ يجب أن تنسخ الملفات إلى هذا الدليل فقط عند تتعرض الملفات للتلف.
IP مكرر	يستخدم جهاز آخر عنوان IP المعين إلى الهاتف.	إذا كان للهاتف عنوان IP ثابت، فتحقق من أنك إذا كنت تستخدم DHCP، فتحقق من تكوين خ

أدخل الرسالة في الحقل الرسالة.	الوصف	التوضيح والإجراء المحتملان
مسح ملفات CTL وITL	مسح ملف CTL أو ITL.	لا يوجد. هذه الرسالة إعلامية فقط.
خطأ في تحديث الإعدادات المحلية	تعذر العثور على أحد الملفات أو أكثر من ملف ترجمة في دليل "مسار TFTP" أو أصبح غير صالح. لم يتم تغيير الإعدادات المحلية.	من "إدارة نظام تشغيل Cisco الموحد"، تحقق من و الفرعية في "إدارة ملفات TFTP". • يوجد في الدليل الفرعي بالاسم نفسه الموجود • tones.xml • يوجد في الدليل الفرعي بالاسم نفسه الموجود • glyphs.xml • dictionary.xml • kate.xml
الملف غير موجود <Cfg File>	لم يتم العثور على ملف التكوين المستند إلى اسم والافتراضي على "خادم TFTP".	يتم إنشاء ملف التكوين لهاتف عند إضافة الهاتف إلى Communications Manager. في حالة عدم و sco Unified Communications Manager **لم يتم العثور على ملف CFG**. • لا يتم تسجيل الهاتف باستخدام unications Manager. يجب أن تضيف الهاتف يدويًا إلى ications Manager إذا كنت لا تسمح بالتسجيل التلقائ • إذا كنت تستخدم DHCP، فتحقق من أن خادم الصحيح. • إذا كنت تستخدم عناوين IP ثابتة، فتحقق من
الملف غير موجود <CTLFile.tlv>	يتم عرض هذه الرسالة على شاشة الهاتف عندما لا تكون مجموعة Cisco Unified Communications Manager في وضع آمن.	لا يتأثر الهاتف، حيث لا يزال يمكنه التسجيل في d Communications Manager.
تم تحرير عنوان IP	يتم تكوين الهاتف لتحرير عنوان IP.	يظل الهاتف في حالة خمول إلى أن يتم تدوير الطاقة DHCP.
مهلة IPv4 DHCP	لم يستجب خادم IPv4 DHCP.	الشبكة مشغولة: يجب أن يتم تحليل الأخطاء ذاتيًا ع لا يوجد اتصال على الشبكة بين خادم Pv4 DHCP الشبكة. خادم IPv4 DHCP معطل: تحقق من تكوين خادم استمرار حدوث الأخطاء: ضع في اعتبارك تعيين

أدخل الرسالة في الحقل الرسالة.	الوصف	التوضيح والإجراء المحتملان
مهلة IPv6 DHCP	لم يستجب خادم IPv6 DHCP.	الشبكة مشغولة - يجب أن يتم تحليل الأخطاء ذ لا يوجد اتصال على الشبكة بين خادم DHCP الشبكة. خادم IPv6 DHCP معطل: تحقق من تكوين استمرار حدوث الأخطاء: ضع في اعتبارك تع
مهلة IPv4 DNS	لم يستجب خادم IPv4 DNS.	الشبكة مشغولة: يجب أن يتم تحليل الأخطاء ذا لا يوجد اتصال على الشبكة بين خادم DNS 4 الشبكة. خادم IPv4 DNS معطل: تحقق من تكوين خ
مهلة IPv6 DNS	لم يستجب خادم IPv6 DNS.	الشبكة مشغولة: يجب أن يتم تحليل الأخطاء ذا لا يوجد اتصال على الشبكة بين خادم DNS 6 الشبكة. خادم IPv6 DNS معطل: تحقق من تكوين خ
مضيف IPv4 غير معروف لـ DNS	تعذر على IPv4 DNS تحليل اسم خادم TFTP أو Cisco Unified Communications Manager.	تحقق مما إذا كانت أسماء مضيف خادم TFTP Communications Manager مكونة بشك ضع في اعتبارك استخدام عناوين IPv4 بدلاً
مضيف IPv6 غير معروف لـ DNS	تعذر على IPv6 DNS تحليل اسم خادم TFTP أو Cisco Unified Communications Manager.	تحقق مما إذا كانت أسماء مضيف خادم TFTP Communications Manager مكونة بشك ضع في اعتبارك استخدام عناوين IPv6 بدلاً
تحميل HC مرفوض	التطبيق الذي تم تنزيله غير متوافق مع أجهزة الهاتف.	يحدث ذلك إذا حاولت تثبيت نسخة من البرامج الأجهزة عليه. تحقق من معرف التحميل المعين إلى الهاتف (Communications Manager، اختر **الج** الذي يتم عرضه على الهاتف.
لا يوجد موجه افتراضي	تكوين DHCP أو التكوين الثابتة لم تحدد موجهًا افتراضيًا.	إذا كان للهاتف عنوان IP ثابت، فتحقق من تكو إذا كنت تستخدم DHCP، فلم يوفر خادم HCP خادم DHCP.
لا يوجد ملقم IPv4 DNS	تم تحديد اسم ولكن تكوين DHCP أو IP الثابت لم تحدد عنوان خادم IPv4 DNS.	إذا كان للهاتف عنوان IP ثابت، فتحقق من تكو إذا كنت تستخدم DHCP، فلم يوفر خادم ICP تكوين خادم DHCP.
لا يوجد ملقم IPv6 DNS	تم تحديد اسم ولكن تكوين DHCP أو IP الثابت لم تحدد عنوان خادم IPv6 DNS.	إذا كان للهاتف عنوان IP ثابت، فتحقق من تكو إذا كنت تستخدم DHCP، فلم يوفر خادم ICP تكوين خادم DHCP.

أدخل الرسالة في الحقل الرسالة.	الوصف	التوضيح والإجراء المحتملان
لم يتم تثبيت أي قائمة ثقة	لم يتم تثبيت ملف CTL أو ملف ITL على الهاتف.	لم يتم تكوين قائمة الثقة في nications Manager والذي لا يدعم الأمان بشكل افتراضي. لم يتم تكوين قائمة الثقة. للحصول على مزيد من المعلومات حول قوائم الثقة sco Unified Communications Manager
فشل تسجيل الهاتف. حجم مفتاح الشهادة غير متوافق مع FIPS.	يتطلب FIPS أن تكون شهادة خادم RSA بحجم مقداره 2048 بت أو بحجم أكبر.	قم بتحديث الشهادة.
يطلب Cisco Unified Communications Manager إعادة التشغيل	تتم إعادة تشغيل الهاتف بناءً على طلب من Cisco Unified Communications Manager.	جرت على الأرجح تغييرات في التكوين على الهاتف Communications Manager، وتم الضغط على التغييرات سارية.
خطأ وصول إلى TFTP	يشير خادم TFTP إلى دليل غير موجود.	إذا كنت تستخدم DHCP، فتحقق من أن خادم CP الصحيح. إذا كنت تستخدم عناوين IP ثابتة، فتحقق من تكوين
خطأ TFTP	لا يتعرف الهاتف على رمز الخطأ الذي أورده خادم TFTP.	اتصل بـ Cisco TAC.
مهلة TFTP	خادم TFTP لم يستجب.	الشبكة مشغولة: يجب أن يتم تحليل الأخطاء ذاتيًا ع لا يوجد اتصال على الشبكة بين خادم TFTP والها خادم TFTP معطل: تحقق من تكوين خادم TFTP
انقضت المهلة	حاول العميل إجراء معاملة X802.1 ولكن المهلة انتهت بسبب عدم وجود مصدّق.	عادةً ما تنتهي مهلة المصادقة في حالة عدم تكوين

أدخل الرسالة في الحقل الرسالة.	الوصف	التوضيح والإجراء المحتملان
فشل تحديث قائمة الثقة	فشل تحديث ملفي CTL وITL.	يشتمل الهاتف على ملفي CTL وITL المثبتين الجديدين. الأسباب المحتملة للفشل: • حدث فشل في الشبكة. • كان خادم TFTP معطلاً. • وتوفر رمز الأمان الجديد الذي استُخدم TFTP التي استُخدمت لتوقيع ملف ITL وITL في الهاتف. • حدث عطل داخلي في الهاتف. الحلول الممكنة: • تحقق من اتصال الشبكة. • تحقق مما إذا كان خادم TFTP نشطًا و • إذا كان خادم Vsam للمعاملات (TVS) Communications Manager، فتح ويعمل بشكل طبيعي أم لا. • تحقق مما إذا كان رمز الأمان وخادم TP احذف ملفي CTL وITL يدويًا إذا فشلت جميع للحصول على مزيد من المعلومات حول قوائ Unified Communications Manager
تم تحديث قائمة الثقة	يتم تحديث ملف CTL أو ملف ITL أو كليهما معًا.	لا يوجد. هذه الرسالة إعلامية فقط. للحصول على مزيد من المعلومات حول قوائ Unified Communications Manager
خطأ إصدار	اسم ملف تحميل الهاتف غير صحيح.	تأكد من أن ملف تحميل الهاتف يحمل الاسم الم
يتوافق XmlDefault.cnf.xml أو cnf.xml. مع اسم جهاز الهاتف.	اسم ملف التكوين.	لا يوجد. تشير الرسالة إلى اسم ملف تكوين اله

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14

عرض نافذة إحصاءات الشبكة

اجراء

الخطوة 1 اضغط على **الإعدادات** > **الحالة** > **إحصاءات المكالمة**.

الخطوة 2 للخروج من القائمة، اضغط على **خروج**.

حقول إحصاءات الشبكة

يصف الجدول التالي المعلومات الواردة في شاشة "إحصاءات الشبكة".

الجدول *23*: حقول إحصاءات الشبكة

العنصر	الوصف
Tx Frames	عدد الحزم المرسلة عبر الهاتف
Tx broadcast	عدد حزم البث المرسلة عبر الهاتف
Tx unicast	إجمالي عدد الحزم أحادية البث المرسلة عبر الهاتف
Rx Frames	عدد الحزم المتلقاة عبر الهاتف
Rx broadcast	عدد الحزم المتلقاة عبر الهاتف
Rx unicast	إجمالي عدد الحزم أحادية البث المتلقاة عبر الهاتف
معرف جهاز الجوار لـ CDP	معرف الجهاز المتصل بهذا المنفذ المكتشف بواسطة بروتوكول CDP.
عنوان IP للجوار لـ CDP	معرف الجهاز المتصل بهذا المنفذ المكتشف بواسطة بروتوكول CDP باستخدام IP.
منفذ الجوار لـ CDP	معرف الجهاز المتصل بهذا المنفذ المكتشف بواسطة بروتوكول CDP.
سبب إعادة التشغيل: إحدى هذه القيم: • إعادة تعيين الأجهزة (إعادة التعيين عند التشغيل) • إعادة تعيين البرامج (تتم إعادة تعيين وحدة التحكم في الذاكرة أيضًا) • إعادة تعيين البرامج (لا تتم إعادة تعيين وحدة التحكم في الذاكرة) • إعادة تعيين مراقب النظام • تمت التكوين • غير معروف	سبب آخر عملية لإعادة تعيين الهاتف
Port 1	حالة ارتباط منفذ الشبكة واتصاله (على سبيل المثال، يعني **الازدواج الكامل التلقائي بسرعة 100 ميجابت** أن منفذ PC في حالة ارتباط نشطة وأنه تفاوض تلقائيًا على اتصال مزدوج كامل بسرعة 100 ميجابت)

العنصر	الوصف
IPv4	المعلومات المعروضة في حالة DHCP. يتضمن ذلك ما يلي: • CDP مرتبط • تهيئة CDP • DHCP مرتبط • DHCP معطل • تهيئة DHCP • DHCP غير صالح • إعادة ربط DHCP • إعادة تشغيل DHCP • تجديد DHCP • طلب DHCP • إعادة مزامنة DHCP • لم يتم التعرف على DHCP • DHCP في انتظار انتهاء مهلة إعادة التشغيل العادية • IP المكرر معطل • تعيين انتهاء مهلة DHCP • تعيين DHCP معطلاً • تعيين DHCP سريعًا

العنصر	الوصف
IPv6	المعلومات المعروضة في حالة DHCP. يتضمن ذلك ما يلي: • تهيئة CDP • DHCP6 مرتبط • DHCP6 معطل • تجديد DHCP6 • إعادة ربط DHCP6 • تهيئة DHCP6 • اتصال DHCP6 • طلب DHCP6 • تحرير DHCP6 • تم تحرير DHCP6 • تعطيل DHCP6 • رفض DHCP • تم رفض DHCP • طلب معلومات DHCP6 • تم طلب معلومات DHCP6 • DHCP6 غير صالح • IPV6 المكرر معطل • IP المكرر مرفوض من DHCP6 • إعلان الموجه • DHCP6 في انتظار انتهاء مهلة إعادة التشغيل العادية • انتهاء مهلة DHCP6 باستخدام القيمة المستعادة • تتعذر استعادة انتهاء مهلة DHCP6 • تم إيقاف تشغيل مكدس IPV6 • إعلان الموجه • إعلان الموجه • لم يتم التعرف عليه عند إدارته بواسطة • حالة IPV6 غير قانونية

عرض نافذة إحصاءات المكالمة

اجراء

الخطوة 1 اضغط على **الإعدادات** > **الحالة** > **إحصاءات المكالمة**.

الخطوة 2 للخروج من القائمة، اضغط على **خروج**،

حقول إحصاءات المكالمات

يصف الجدول التالي العناصر المعروضة على شاشة "إحصاءات المكالمة".

الجدول *24*: عناصر إحصاءات المكالمات

العنصر	الوصف
برنامج الترميز للمستلم	نوع الدفق المستلم (صوت بدفق RTP من الترميز): • G.729 • G.722 • G.722 AMR WB • G.711 mu—law • G.711 A—law • iLBC • OPUS
برنامج الترميز للمرسل	نوع الدفق المرسل (صوت بدفق RTP من الترميز): • G.729 • G.722 • G.722 AMR WB • G.711 mu—law • G.711 A—law • iLBC • OPUS
حجم الحزم المستلمة	حجم حزم الصوت RTP، بالمللي ثانية، خلال استلام دفق الصوت (صوت بدفق RTP).
حجم الحزم المرسلة	حجم حزم الصوت RTP، بالمللي ثانية، خلال إرسال دفق الصوت.

العنصر	الوصف
حزم مستقبَلة	عدد حزم صوت RTP المستلمة منذ فتح دفق الصوت. **ملاحظة** ليس من الضروري أن يكون هذا العدد مطابقًا لعدد حزم صوت RTP المستلمة منذ بدء المكالمة لأن المكالمة ربما قد تم وضعها قيد الانتظار.
حزم مرسلة	عدد حزم صوت RTP المرسلة منذ فتح دفق الصوت. **ملاحظة** ليس من الضروري أن يكون هذا العدد مطابقًا لعدد حزم صوت RTP المرسلة منذ بدء المكالمة لأن المكالمة ربما قد تم وضعها قيد الانتظار.
متوسط التشويش	متوسط تشويش حزمة RTP المقدّر (تأخير ديناميكي تتعرض له الحزمة عند المرور عبر الشبكة)، بالمللي ثانية، والذي تم رصده منذ استلام دفق الصوت المفتوح.
أقصى تشويش	الحد الأقصى للتشويش، بالمللي ثانية، الذي تم رصده منذ استلام دفق الصوت المفتوح.
تم تجاهل الحزم المستلمة	عدد حزم RTP خلال استلام دفق الصوت والتي تم تجاهلها (الحزم السيئة والمتأخرة للغاية وما إلى ذلك). **ملاحظة** يتجاهل الهاتف 19 حزمة ذات ضوضاء خفيفة صادرة عن بوابات Cisco وفقًا لنوع الحمولة، وذلك نظرًا لأنها تؤدي إلى زيادة هذا العداد.
حزم مستقبلة مفقودة	حزم RTP المفقودة (تم فقدها أثناء النقل)
قياسات جودة الصوت	
نسبة الإخفاء التراكمية	إجمالي عدد إطارات الإخفاء مقسومًا على إجمالي عدد إطارات الكلام التي تم استلامها منذ بدء دفق الصوت.
نسبة الإخفاء الفاصلة	نسبة إطارات الإخفاء إلى إطارات الكلام في فاصل الكلام النشط السابق الذي مدته 3 ثوانٍ. في حالة استخدام ميزة اكتشاف نشاط الصوت (VAD)، قد يلزم وجود فاصل زمني أطول لتجميع ثلاث ثوانٍ من الكلام النشط.
أقصى نسبة إخفاء	أعلى نسبة إخفاء للفاصل الزمني منذ بدء الدفق الصوتي.
ثواني الإخفاء	عدد الثواني التي بها أحداث إخفاء (إطارات مفقودة) منذ بداية دفق الصوت (وتشمل الثواني المخفية بصرامة).
ثواني الإخفاء التام	يتجاوز عدد الثواني التي بها أحداث إخفاء نسبة 5 بالمائة (إطارات مفقودة) منذ بدء دفق الصوت.
زمن وصول	تقدير زمن وصول الشبكة، معبرًا عنه بالمللي ثانية. يمثل متوسطًا متحركًا لتأخر الرحلة ذهابًا وعودة، ويتم قياسه عند استلام كتل تقرير مستلم RTCP.

صفحة هاتف Cisco IP على الويب

يمتلك كل هاتف Cisco IP صفحة ويب يمكنك من خلالها عرض مجموعة متنوعة من المعلومات المتعلقة بالهاتف، والتي تشمل:

- معلومات الجهاز: يعرض إعدادات الجهاز والمعلومات ذات الصلة بالهاتف.
- إعداد الشبكة: يعرض معلومات إعداد الشبكة ومعلومات حول إعدادات الهاتف الأخرى.

- إحصاءات الشبكة: تعرض الارتباطات التشعبية التي توفر معلومات حول حركة مرور الشبكة.
- سجلات الجهاز: تعرض الارتباطات التشعبية التي توفر معلومات يمكنك استخدامها لاستكشاف المشكلات وإصلاحها.
- إحصاءات الدفق: يعرض ارتباطات تشعبية لمجموعة متنوعة من إحصاءات الدفق.

يصف هذا القسم المعلومات التي يمكنك الحصول عليها من صفحة الهاتف على الويب. يمكنك استخدام هذه المعلومات لمراقبة تشغيل الهاتف عن بُعد والمساعدة في استكشاف المشكلات وإصلاحها.

يمكنك أيضًا الحصول على الكثير من هذه المعلومات مباشرة من الهاتف.

الوصول إلى صفحة الهاتف على الويب

ملاحظة إذا تعذر عليك الوصول إلى صفحة الويب، فقد تكون معطلة افتراضيًا.

اجراء

الخطوة 1 احصل على عنوان IP الخاص بهاتف Cisco IP باستخدام إحدى هذه الطرق:

a) ابحث عن الهاتف في إدارة Cisco Unified Communications Manager باختيار **الجهاز** > **الهاتف**. تعرض الهواتف التي يتم تسجيلها باستخدام Cisco Unified Communications Manager عنوان IP في نافذة "بحث في الهواتف وسردها" وفي أعلى نافذة "تكوين الهاتف".

b) على الهاتف، اضغط على **الإعدادات** > **معلومات النظام**، ثم قم بالتمرير إلى حقل عنوان IPv4..

الخطوة 2 افتح مستعرض ويب وأدخل عنوان URL التالي، حيث يكون *IP_address* هو عنوان IP الخاص بهاتف Cisco IP :

http://<IP_address>

صفحة معلومات الجهاز على الويب

تعرض منطقة معلومات الجهاز الموجودة على صفحة ويب الهاتف إعدادات الجهاز والمعلومات ذات الصلة بالهاتف. يصف الجدول التالي هذه العناصر.

لعرض منطقة معلومات الجهاز، ادخل إلى صفحة ويب الهاتف، ثم انقر فوق الارتباط التشعبي **معلومات الجهاز**.

الجدول *25*: حقول صفحة معلومات الجهاز على الويب

الحقل	الوصف
وضع الخدمة	وضع الخدمة للهاتف.
مجال الخدمة	المجال للخدمة.
حالة الخدمة	حالة الخدمة الحالية.
عنوان MAC	عنوان التحكم في الوصول إلى الوسائط (MAC) الخاص بالهاتف.
اسم المضيف	اسم فريد وثابت تم تعيينه تلقائيًا إلى الهاتف بناءً على عنوان MAC.

الحقل	الوصف
DN للهاتف	رقم الدليل المعين للهاتف.
معرف تحميل التطبيق	يحدد إصدار تحميل التطبيق.
معرف تحميل التمهيد	يشير إلى إصدار تحميل التمهيد.
الإصدار	محدد البرامج الثابتة التي تعمل على الهاتف.
مراجعة الأجهزة	قيمة المراجعة الصغرى لأجهزة الهاتف.
الرقم المسلسل	الرقم التسلسلي الفريد للهاتف.
رقم الطراز	رقم طراز الهاتف.
رسالة في الانتظار	يشير إلى ما إذا كانت هناك رسالة صوتية في وضع الانتظار على الخط الأساسي لهذا الهاتف أم لا.
UDI	يعرض معلومات معرف الجهاز الفريد (UDI) Cisco حول الهاتف: • نوع الجهاز • اسم طراز الهاتف • معرف المنتج • معرف الإصدار (VID) — يحدد رقم إصدار الجهاز الرئيسي. • الرقم المسلسل
الوقت	وقت مجموعة التاريخ/الوقت التي ينتمي إليها الهاتف. يتم الحصول على هذه المعلومات من Cisco Unified Communications Manager.
المنطقة الزمنية	المنطقة الزمنية لمجموعة التاريخ/الوقت التي ينتمي إليها الهاتف. يتم الحصول على هذه المعلومات من Cisco Unified Communications Manager.
التاريخ	تاريخ مجموعة التاريخ/الوقت التي ينتمي إليها الهاتف. يتم الحصول على هذه المعلومات من Cisco Unified Communications Manager.
ذاكرة فارغة للنظام	حجم ذاكرة النظام المتوفرة.
ذاكرة كومة فارغة لـ Java	حجم الذاكرة الحرة لكومة الذاكرة المؤقتة لـ Java.
ذاكرة مخزن فارغة لـ Java	حجم الذاكرة الحرة لمخزن Java.
تم تمكين وضع FIPS	يشير إلى ما إذا كان قد تم تمكين وضع المقياس الفيدرالي لمعالجة المعلومات (FIPS).

صفحة ويب إعداد الشبكة

تعرض منطقة إعداد الشبكة على صفحة ويب الهاتف معلومات إعداد الشبكة ومعلومات حول إعدادات الهاتف الأخرى. يصف الجدول التالي هذه العناصر.

يمكنك عرض وتعيين العديد من هذه العناصر من قائمة إعداد الشبكة على هاتف Cisco IP .

لعرض منطقة إعداد الشبكة، ادخل إلى صفحة ويب الهاتف، ثم انقر فوق الارتباط التشعبي **إعداد الشبكة**.

الجدول 26: عناصر منطقة إعداد الشبكة

العنصر	الوصف
عنوان MAC	عنوان التحكم في الوصول إلى الوسائط (MAC) الخاص بالهاتف.
اسم المضيف	اسم المضيف الذي عينه خادم DHCP للهاتف.
اسم المجال	اسم مجال نظام اسم المجال (DNS) الذي يوجد به الهاتف.
ملقم DHCP	عنوان IP الخاص بخادم بروتوكول تكوين المضيف الديناميكي (DHCP) الذي يحصل الهاتف من خلاله على عنوا
ملقم BOOTP	يشير إلى ما إذا كان الهاتف يحصل على التكوين من خادم بروتوكول تمهيد تشغيل الجهاز (BootP).
DHCP	يشير إلى ما إذا كان الهاتف يستخدم DHCP.
عنوان IP	عنوان بروتوكول الإنترنت (IP) للهاتف.
قناع الشبكة الفرعية	قناع الشبكة الفرعية الذي يستخدمه الهاتف.
موجه افتراضي 1	الموجه الافتراضي الذي يستخدمه الهاتف.
ملقم DNS 1-3	خادم نظام اسم المجال الرئيسي (DNS) (خادم DNS 1) وخوادم DNS الاحتياطية الاختيارية (خادم DNS 2 و3) الهاتف.
TFTP بديل	يشير إلى ما إذا كان الهاتف يستخدم خادم TFTP بديلاً.
خادم TFTP 1	خادم □بروتوكول نقل الملفات المبسط الأساسي (TFTP) المستخدم الذي يستخدمه الهاتف.
ملقم TFTP 2	خادم □بروتوكول نقل الملفات المبسط الاحتياطي (TFTP) المستخدم الذي يستخدمه الهاتف.
تم تحرير عنوان DHCP	يشير إلى إعداد خيار عنوان DHCP الذي تم إصداره.
VLAN ID للتشغيل	شبكة المنطقة المحلية الظاهرية (VLAN) القابلة للتشغيل المكونة على مفتاح تحويل Cisco Catalyst التي يوجد به
معرف VLAN للإدارة	شبكة VLAN الإضافية التي يوجد بها الهاتف كعضو.
Unified CM 1-5	أسماء المضيف أو عناوين IP، مرتبة حسب الأولوية، الخاصة بخوادم Unified Communications Manager يمكن للهاتف التسجيل من خلالها. يمكن لأحد العناصر أيضًا إظهار عنوان IP الخاص بموجه SRST الذي يمكنه تو Cisco Unified Communications Manager، إذا كان هذا الموجه متوفرًا. بالنسبة للخادم المتوفر، يُظهر أحد العناصر عنوان IP الخاص بخادم Unified Communications Manager و الحالات التالية: • نشط: خادم Cisco Unified Communications Manager الذي يتلقى الهاتف من خلاله خدمات معالجة الوقت الحالي • استعداد: خادم Cisco Unified Communications Manager الذي يتم تبديل الهاتف إليه في حالة عدم تو • فارغ: لا يوجد اتصال حالي بخادم Cisco Unified Communications Manager هذا يمكن أيضًا أن يشتمل أحد العناصر على وجهة هاتفية موقع بعيد متين (SRST)، التي تحدد موجه SRST الذي يمكن Cisco Unified Communications Manager، مع مجموعة ميزات محدودة. يفترض هذا الموجه التحكم في م في حالة تعذر الوصول إلى جميع خوادم Cisco Unified Communications Manager الأخرى. يظهر isco Unified Communications Manager بشكل دائم في آخر قائمة الخوادم، حتى إذا كان نشطًا. يمكنك تكوين عنوان في قسم مجمّع الأجهزة في نافذة تكوين Cisco Unified Communications Manager.

العنصر	الوصف
URL للمعلومات	عنوان URL الخاص بنص التعليمات الذي يظهر على الهاتف.
URL للدلائل	عنوان URL الخادم الذي يحصل الهاتف من خلاله على معلومات الدليل.
URL للرسائل	عنوان URL الخادم الذي يحصل الهاتف من خلاله على خدمات الرسائل.
URL للخدمات	عنوان URL الخادم الذي يحصل الهاتف من خلاله على خدمات هاتف Cisco IP .
URL خامل	عنوان URL الذي يعرضه الهاتف عندما يكون في وضع الخمول، الذي يستمر طوال الفترة التي يحددها حقل وقت عنوا الخامل، ولا توجد أي قائمة مفتوحة.
وقت URL الخامل	عدد الثواني التي يكون الهاتف خلالها في وضع الخمول ولا توجد أي قائمة مفتوحة قبل أن يتم تنشيط خدمة XML التي يح URL الخامل.
URL الملقم الوكيل	عنوان URL خادم الوكيل، الذي يجعل HTTP يطلب عناوين مضيف غير محلية نيابة عن عميل HTTP الخاص بالهات ردودًا من المضيف غير المحلي إلى عميل HTTP الخاص بالهاتف.
URL المصادقة	عنوان URL الذي يستخدمه الهاتف للتحقق من صحة الطلبات المرسلة إلى خادم ويب الهاتف.
إعداد منفذ SW	السرعة والإرسال المزدوج في منفذ مفتاح التحويل، حيث: • A = التفاوض التلقائي • H10 = 10-BaseT/أحادي الاتجاه • F10 = 10-BaseT/ازدواج كامل • H100 = 100-BaseT/أحادي الاتجاه • F100 = 100-BaseT/ازدواج كامل • F = 1000-BaseT1000/ازدواج كامل • لا يوجد ارتباط = لا يوجد اتصال بمنفذ مفتاح التحويل
الإعدادات المحلية للمستخدم	الإعدادات المحلية للمستخدم المقترنة بمستخدم الهاتف. تحدد مجموعة من المعلومات التفصيلية لدعم المستخدمين، بما في والخط وتنسيق التاريخ والوقت ومعلومات نص لوحة المفاتيح الأبجدية الرقمية.
الإعدادات المحلية للشبكة	الإعدادات المحلية للشبكة المقترنة بمستخدم الهاتف. تحدد مجموعة من المعلومات التفصيلية لدعم الهاتف في موقع محدد، تعريفات النغمات والإيقاعات التي يستخدمها الهاتف.
إصدار إعداد محلي لمستخدم	نسخة الإعدادات المحلية للمستخدم المحملة على الهاتف.
إصدار الإعدادات المحلية للشبكة	نسخة الإعدادات المحلية للشبكة المحملة على الهاتف.
مكبر ممكّن	يشير إلى ما إذا كان منفذ مكبر الصوت ممكنًا على الهاتف أم لا.
الاستماع الجماعي	يشير إلى ما إذا كانت ميزة الاستماع الجماعي ممكنة على الهاتف أم لا. تتيح لك ميزة الاستماع الجماعي إمكانية التحدث ب سماعة الهاتف والاستماع عبر مكبر الصوت في الوقت نفسه.
تم تمكين GARP	يشير إلى ما إذا كان الهاتف يعلم عناوين MAC من ردود ARP المجانية.
تحديد خط تلقائي ممكّن	يشير إلى ما إذا كان الهاتف يحول تركيز المكالمة إلى مكالمات واردة على جميع الخطوط أم لا.
DSCP للتحكم في المكالمة	تصنيف DSCP IP لإرسال إشارة التحكم في المكالمة.
DSCP للتهيئة	تصنيف DSCP IP لأي عملية نقل في تهيئة الهاتف.

العنصر	الوصف
DSCP للخدمات	تصنيف DSCP IP للخدمات المستندة إلى الهاتف.
وضع الأمان	وضع الأمان المعين للهاتف.
تمكين الوصول للويب	يشير إلى ما إذا كان وصول الويب ممكنًا (نعم) أم معطلاً (لا) للهاتف.
الوصول للويب ممكّن	يشير إلى ما إذا كان الهاتف يقبل اتصالات SSH أو يحظرها.
CDP: منفذ SW	يشير إلى ما إذا كان دعم CDP موجودًا على منفذ المحول أم لا (ممكنًا بشكل افتراضي). تمكين CDP على منفذ مفتاح التحويل لتعيين VLAN للهاتف، وتفاوض الطاقة، وإدارة QoS، وأمان x802.1. تمكين CDP على منفذ مفتاح التحويل عندما يتصل الهاتف بمفتاح تحويل Cisco. عندما يكون CDP معطلاً في Cisco Unified Communications Manager، يظهر تحذير، يشير إلى أنه يجب على منفذ مفتاح التحويل فقط في حالة اتصال الهاتف بمفتاح تحويل غير تابع لـ Cisco. تظهر قيم CDP الخاصة بمنفذ PC ومنفذ مفتاح التحويل على قائمة الإعدادات.
LLDP-MED: منفذ SW	يشير إلى ما إذا كان استكشاف نقطة نهاية وسائط □بروتوكول استكشاف طبقة الارتباط (LLDP-MED) ممكنًا على التحويل.
LLDP Power Priority	يعلن أولوية طاقة الهاتف إلى مفتاح التحويل، وبالتالي يعمل على تمكين التبديل لتوفير الطاقة على نحو مناسب للهواتف. ت • غير معروف: هذه هي القيمة الافتراضية. • منخفضة • مرتفعة • حرج
LLDP Asset ID	يحدد معرف الأصل المعين للهاتف لإدارة المخزون.
ملف CTL	يحدد ملف CTL.
ملف ITL	يحتوي ملف ITL على قائمة الثقة الأولية.
توقيع CTL	يعزز الأمان باستخدام خوارزمية التجزئة الآمنة (SHA-1) في ملفات CTL وITL.
ملقم CAPF	اسم خادم CAPF المستخدم بواسطة الهاتف.
TVS	المكون الأساسي للأمان بشكل افتراضي. تُمكن خدمات المصادقة الموثوقة (TVS) هواتف هاتف sco Unified IP خوادم التطبيقات، مثل خدمات EM والدليل وMIDlet أثناء تأسيس HTTPS.
ملقم TFTP	اسم خادم TFTP المستخدم بواسطة الهاتف.
مزامنة تلقائية للمنفذ	لمزامنة المنافذ إلى السرعة الأقل التي تمنع فقد الحزمة.
تهيئة منفذ مفتاح التبديل عن بُعد	للسماح للمسؤول بتكوين السرعة ووظيفة منفذ جدول تجربة Cisco Desktop Collaboration عن بُعد باستخدام Unified Communications Manager.
تهيئة منفذ الكمبيوتر الشخصي عن بُعد	تشير إلى ما إذا كان تكوين المنفذ البعيد للسرعة والوضع المزدوج لمنفذ PC ممكنًا أم معطلاً.
وضع عنونة IP	تعرض وضع عنونة IP المتوفر على الهاتف.

العنصر	الوصف
عنصر تحكم وضع تفضيلات IP	يشير إلى نسخة عنوان IP التي يستخدمها الهاتف أثناء إرسال الإشارة من خلال Cisco Unified Communications Manager عند توفر كل من IPv4 وIPv6 على الهاتف.
وضع تفضيلات IP للوسائط	يشير إلى أن الوسائط التي تستخدم عنوان IPv4 تتصل بـ Cisco Unified Communications Manager.
تهيئة IPv6 تلقائية	لعرض ما إذا كان التكوين التلقائي ممكّنًا أم معطلاً على الهاتف.
IPv6 DAD	يتحقق من تفرد عناوين IPv6 أحادية البث الجديدة قبل تعيين العناوين إلى الواجهات.
قبول الرسالة المعاد توجيهها IPv6	يشير إلى ما إذا كان الهاتف يقبل إعادة توجيه الرسائل من نفس الموجه المستخدم لرقم الوجهة.
الرد على طلب الصدى متعدد البث IPv6	يشير إلى أن الهاتف يُرسل رسالة رد الصدى للرد على رسالة طلب الصدى المرسلة إلى عنوان IPv6.
خادم تحميل IPv6	يُستخدم لتحسين وقت تثبيت ترقيات البرامج الثابتة على الهاتف وتخفيف حمل WAN من خلال تخزين الصور محليًا، وإلغاء الحاجة إلى اجتياز ارتباط WAN لكل عملية ترقية تتم للهاتف.
خادم تسجيل IPv6	يشير إلى عنوان IP ومنفذ جهاز التسجيل البعيد الذي يرسل إليه الهاتف رسائل السجل.
ملقم IPv6 CAPF	الاسم العام (من شهادة Cisco Unified Communications Manager) لـ CAPF المستخدَم بواسطة الهاتف.
DHCPv6	يعين بروتوكول تكوين الاستضافة الديناميكية (DHCP) عنوان IPv6 تلقائيًا إلى الأجهزة عندما تقوم بتوصيلها بالشبكة. يكون DHCP على هواتف هاتف Cisco Unified IP بشكل افتراضي.
عنوان IPv6	يعرض عنوان IPv6 الحالي للهاتف أو يسمح للمستخدم بإدخال عنوان IPv6 جديد.
طول بادئة IPv6	يعرض طول البادئة الحالية للشبكة الفرعية أو يسمح للمستخدم بإدخال طول بادئة جديد.
موجه افتراضي IPv6 1	يعرض الموجه الافتراضي المستخدم من قبل الهاتف أو يسمح للمستخدم بإدخال موجه افتراضي IPv6 جديد.
ملقم IPv6 DNS 1	يعرض خادم DNSv6 الأساسي المستخدم من قبل الهاتف أو يسمح للمستخدم بإدخال خادم جديد.
خادم IPv6 DNS 2	يعرض خادم DNSv6 الثانوي المستخدم من قبل الهاتف أو يسمح للمستخدم بتعيين خادم DNSv6 ثانوي جديد.
TFTP بديل IPv6	يسمح للمستخدم بتمكين استخدام خادم IPv6 TFTP (الثانوي) البديل.
ملقم IPv6 TFTP 1	يعرض خادم IPv6 TFTP الأساسي المستخدم من قبل الهاتف أو يسمح للمستخدم بتعيين خادم TFTP أساسي جديد.
ملقم IPv6 TFTP 2	يعرض خادم IPv6 TFTP الثانوي المستخدم في حالة عدم توفر خادم IPv6 TFTP الأساسي أو يسمح للمستخدم بتعيين خادم TFTP ثانوي جديد.
تم تحرير عنوان IPv6	يسمح للمستخدم بإصدار المعلومات ذات الصلة بـ IPv6.
مستوى طاقة Energywise	قياس الطاقة المستهلكة بواسطة الأجهزة الموجودة على شبكة EnergyWise.
مجال EnergyWise	تجميع إداري للأجهزة بغرض مراقبة الطاقة والتحكم بها.

صفحة معلومات الإيثرنت على الويب

يصف الجدول التالي محتويات صفحة ويب معلومات الإيثرنت.

الجدول 27: عناصر معلومات الإيثرنت

العنصر	الوصف
Tx Frames	إجمالي عدد الحزم التي يرسلها الهاتف.
Tx broadcast	إجمالي عدد حزم البث التي يرسلها الهاتف.
Tx multicast	إجمالي عدد الحزم متعددة البث التي يرسلها الهاتف.
Tx unicast	إجمالي عدد الحزم أحادية البث التي يرسلها الهاتف.
Rx Frames	إجمالي عدد الحزم التي تلقاها الهاتف.
Rx broadcast	إجمالي عدد حزم البث التي يتلقاها الهاتف..
Rx multicast	إجمالي عدد الحزم متعددة البث التي يتلقاها الهاتف.
Rx unicast	إجمالي عدد الحزم أحادية البث التي يتلقاها الهاتف.
Rx PacketNoDes	إجمالي عدد الحزم الساقطة التي يسببها واصف الوصول المباشر إلى الذاكرة (DMA).

صفحات ويب الشبكة

يصف الجدول التالي المعلومات الواردة في صفحات ويب منطقة الشبكة.

ملاحظة عندما تقوم بالنقر فوق ارتباط **الشبكة** ضمن إحصاءات الشبكة، تحمل الصفحة عنوان "معلومات المنفذ".

الجدول 28: عناصر منطقة الشبكة

العنصر	الوصف
Rx totalPkt	إجمالي عدد الحزم التي تلقاها الهاتف.
Rx multicast	إجمالي عدد الحزم متعددة البث التي تلقاها الهاتف.
Rx broadcast	إجمالي عدد حزم البث التي تلقاها الهاتف.
Rx unicast	إجمالي عدد الحزم أحادية البث التي تلقاها الهاتف.
Rx tokenDrop	إجمالي عدد الحزم التي تم إبعادها بسبب نقص الموارد (على سبيل المثال، تجاوز FIFO).
Tx totalGoodPkt	إجمالي عدد الحزم الجيدة (الحزم متعددة البث، وحزم البث، وأحادية البث) التي تلقاها الهاتف.
Tx broadcast	إجمالي عدد حزم البث التي أرسلها الهاتف.
Tx multicast	إجمالي عدد الحزم متعددة البث التي أرسلها الهاتف.
LLDP FramesOutTotal	إجمالي عدد إطارات LLDP التي أرسلها الهاتف.
LLDP AgeoutsTotal	إجمالي عدد إطارات LLDP التي انتهت مهلتها في ذاكرة التخزين المؤقت.

العنصر	الوصف
LLDP FramesDiscardedTotal	إجمالي عدد إطارات LLDP التي تم تجاهلها عند فقد أي من TLVs الإلزامية، أو بسبب عدم ترتيبها، أو بسبب احتوائها على سلسلة يتجاوز طولها النطاق المحدد.
LLDP FramesInErrorsTotal	إجمالي عدد إطارات LLDP التي تم تلقيها مع اكتشاف وجود خطأ واحد أو أكثر.
LLDP FramesInTotal	إجمالي عدد إطارات LLDP التي يتلقاها الهاتف.
LLDP TLVDiscardedTotal	إجمالي عدد LLDP TLVs التي تم تجاهلها.
LLDP TLVUnrecognizedTotal	إجمالي عدد LLDP TLVs التي لم يتم التعرف عليها على الهاتف.
معرف جهاز الجوار لـ CDP	معرف الجهاز المتصل بهذا المنفذ الذي اكتشفه CDP.
عنوان IP للجوار لـ CDP	عنوان IP للجهاز المجاور المكتشف بواسطة CDP.
عنوان IP للجوار لـ CDP	عنوان IPv6 للجهاز المجاور المكتشف بواسطة CDP.
منفذ الجوار لـ CDP	منفذ الجهاز المجاور الذي يتصل به الهاتف المكتشف بواسطة CDP.
معرف جهاز الجوار لـ LLDP	معرف الجهاز المتصل بهذا المنفذ المكتشف بواسطة بروتوكول LLDP.
عنوان IP للجوار لـLLDP	عنوان IP للجهاز المجاور المكتشف بواسطة LLDP.
عنوان IP للجوار لـLLDP	عنوان IPv6 للجهاز المجاور المكتشف بواسطة CDP.
منفذ الجوار لـ LLDP	منفذ الجهاز المجاور الذي يتصل به الهاتف المكتشف بواسطة LLDP.
معلومات المنفذ	معلومات السرعة والإرسال المزدوج.

سجلات وحدة التحكم، وعمليات التفريغ الأساسية، وصفحات عرض تصحيح الأخطاء على الويب.

تحت عنوان "سجلات الجهاز "، توفر سجلات وحدة التحكم، وعمليات التفريغ الأساسية، ورسائل الحالة، والارتباطات التشعبية لعرض تصحيح الأخطاء المعلومات التي تساعد على مراقبة الهاتف واستكشاف الأخطاء فيه وإصلاحها.

- سجلات وحدة التحكم — تشتمل على ارتباطات تشعبية لملفات السجل الفردية. تشتمل ملفات سجل وحدة التحكم على رسائل الأخطاء تصحيح الأخطاء التي تلقاها الهاتف.
- عمليات التفريغ الأساسية — تشتمل على ارتباطات تشعبية لملفات التفريغ الفردية. تشتمل ملفات التفريغ الأساسية على بيانات من عطل الهاتف.
- رسائل الحالة — تعرض أحدث 10 رسائل من رسائل الحالة التي أنشأها الهاتف منذ آخر عملية تشغيل. يمكنك أيضًا الحصول على هذه المعلومات من شاشة رسائل الحالة على الهاتف.
- عرض تصحيح الأخطاء — يعرض رسائل تصحيح الأخطاء التي قد تكون مفيدة لـ Cisco TAC إذا احتجت إلى المساعدة بشأن استكشاف المشكلات وإصلاحها.

صفحة إحصاءات التدفق على الويب

يمكن لهاتف Cisco IP دفق المعلومات من وإلى ما يصل إلى خمسة أجهزة في نفس الوقت. يدفق الهاتف المعلومات أثناء إجراء مكالمة أو تشغيل خدمة ترسل أو تستقبل الصوت أو البيانات.

توفر مناطق إحصاءات الدفق على صفحة ويب الهاتف معلومات حول عمليات الدفق.

لعرض منطقة إحصاءات الدفق، أدخل إلى صفحة ويب الهاتف، ثم انقر فوق **ارتباط الدفق** التشعبي.

يصف الجدول التالي العناصر الواردة في مناطق إحصاءات الدفق.

الجدول *29*: حقول إحصاءات التدفق

العنصر	الوصف
عنوان بعيد	عنوان IP ومنفذ UDP لوجهة الدفق.
عنوان محلي	عنوان IP ومنفذ UPD للهاتف.
وقت البدء	يشير الطابع الزمني الداخلي إلى وقت مطالبة Cisco Unified Communications Manager للهاتف ب الحزم.
حالة التدفق	إشارة إلى ما إذا كان الدفق نشطًا أم لا.
اسم المضيف	اسم فريد وثابت تم تعيينه تلقائيًا إلى الهاتف بناءً على عنوان MAC.
حزم مرسلة	إجمالي عدد حزم بيانات RTP التي أرسلها الهاتف منذ أن بدأ هذا الاتصال. وتكون القيمة 0 إذا تم تعيين الاتص الاستقبال فقط.
ثمانيات إرسال	إجمالي عدد ثمانيات الحمولة التي أرسلها الهاتف في حزم بيانات RTP منذ أن بدأ هذا الاتصال. وتكون القيمة الاتصال على وضع الاستقبال فقط.
برنامج الترميز للمرسل	نوع الترميز الصوتي الخاص بالدفق المرسل.
تم إرسال تقارير الإرسال (انظر الملاحظة)	عدد المرات التي تم فيها إرسال تقرير مرسل RTCP.
تم إرسال وقت تقرير الإرسال (انظر الملاحظة)	إشارة الطابع الزمني الداخلي فيما يتعلق بوقت إرسال تقرير مرسل RTCP الأخير.
حزم مستقبلة مفقودة	إجمالي عدد حزم بيانات RTP التي تم فقدها منذ أن بدأ استقبال البيانات في هذا الاتصال. ويعرف بأنه عدد ال الذي يكون أقل عددًا من الحزم المستلمة بالفعل، حيث يشمل عدد الحزم المستلمة أي حزم يتم استلامها في وق تكون مكررة. ويتم عرض القيمة 0 إذا كان قد تم تعيين الاتصال على وضع الإرسال فقط.
متوسط التشويش	تقدير الانحراف المتوسط في فاصل وصول حزمة بيانات RTP، مقيسًا بالملي ثانية. ويتم عرض القيمة 0 إذ تعيين الاتصال على وضع الإرسال فقط.
برنامج الترميز للمستلم	نوع الترميز الصوتي المستخدم للدفق المستلم.
تم إرسال تقارير الاستلام (انظر الملاحظة)	عدد المرات التي تم فيها إرسال تقارير مستلم RTCP.
وقت إرسال تقرير الاستلام (انظر الملاحظة)	إشارة الطابع الزمني الداخلي فيما يتعلق بوقت إرسال تقرير مستلم RTCP.
حزم مستقبَلة	إجمالي عدد حزم بيانات RTP التي تلقاها الهاتف منذ أن بدأ استقبال البيانات في هذا الاتصال. وتشمل الحزم الت من مصادر مختلفة إذا كانت هذه الدعوة عبارة عن دعوة إرسال متعدد. ويتم عرض القيمة 0 إذا كان قد تم تع على وضع الإرسال فقط.

العنصر	الوصف
ثمانيات المستقبل	إجمالي عدد ثمانيات الحمولة التي تلقاها الجهاز في حزم بيانات RTP منذ أن بدأ الاستقبال على هذا الاتصال. وتشم التي تم استلامها من مصادر مختلفة إذا كانت هذه الدعوة عبارة عن دعوة إرسال متعدد. ويتم عرض القيمة 0 إذا ك تعيين الاتصال على وضع الإرسال فقط.
نسبة الإخفاء التراكمية	إجمالي عدد إطارات الإخفاء مقسومًا على إجمالي عدد إطارات الكلام التي تم استلامها منذ بداية دفق الصوت.
نسبة الإخفاء الفاصلة	نسبة إطارات الإخفاء إلى إطارات الكلام في الفاصل السابق، للكلام النشط، الذي تقدر مدته بـ 3 ثوان. إذا كانت ميزة نشاط الصوت (VAD) قيد الاستخدام، فقد يلزم وجود فاصل زمني أطول لتجميع ثلاث ثوانٍ من الكلام النشط.
أقصى نسبة إخفاء	أعلى نسبة إخفاء للفاصل الزمني من بداية الدفق الصوتي.
ثواني الإخفاء	عدد الثواني التي بها أحداث إخفاء (إطارات مفقودة) منذ بداية دفق الصوت (وتشمل الثواني المخفية بصرامة).
ثواني الإخفاء التام	عدد الثواني التي بها أحداث إخفاء تتجاوز خمسة بالمائة (إطارات مفقودة) منذ بداية دفق الصوت.
زمن وصول (انظر الملاحظة)	تقدير زمن وصول الشبكة، معبرًا عنه بالمللي ثانية. يمثل متوسطًا متحركًا لتأخر الرحلة ذهابًا وعودة، ويتم قياسه ع كتل تقرير مستلم RTCP.
أقصى تشويش	الحد الأقصى لقيمة التشويش اللحظي، بالمللي ثانية.
حجم الحزم المرسلة	حجم حزمة RTP، بالمللي ثانية، للدفق المرسل.
تم تلقي تقارير الإرسال (انظر الملاحظة)	عدد المرات التي تم فيها استلام تقارير مرسل RTCP.
تم تلقي وقت تقرير الإرسال (انظر الملاحظة)	أحدث وقت تم فيه استلام تقرير مرسل RTCP.
حجم الحزم المستلمة	حجم حزمة RTP، بالمللي ثانية، للدفق المستلم.
تم تجاهل الحزم المستلمة	حزم RTP التي تم استلامها من الشبكة ولكن تم تجاهلها من مخازن التشويش المؤقتة.
تم تلقي تقارير الاستلام (انظر الملاحظة)	عدد المرات التي تم فيها استلام تقارير مستلم RTCP.
وقت تلقي تقرير الاستلام (انظر الملاحظة)	أحدث وقت تم فيه استلام تقرير مستلم RTCP.

ملاحظة عندما يتم تعطيل بروتوكول التحكم RTP، لا يتم إنشاء أي بيانات لهذا الحقل، وبالتالي يتم عرض قيمة 0.

طلب معلومات من الهاتف بتنسيق XML

لأغراض استكشاف المشكلات وإصلاحها، يمكنك طلب معلومات من الهاتف. المعلومات الناتجة بتنسيق XML. المعلومات التالية متوفرة:

- CallInfo هي معلومات جلسة مكالمة لخط محدد.

- LineInfo هي معلومات تكوين للهاتف.
- ModeInfo هي معلومات وضع الهاتف.

قبل البدء

يحتاج وصول الويب إلى أن يتم تمكينه للحصول على المعلومات.

يجب أن يكون الهاتف مقترنًا بمستخدم.

اجراء

الخطوة 1 بالنسبة لمعلومات المكالمة، أدخل عنوان URL التالي في المتصفح: **http://<phone ip address>/CGI/Java/CallInfo<x>**

حيث

- <*phone ip address*>هو عنوان IP الخاص بالهاتف
- <*x*> هو رقم الخط المطلوب الحصول على معلومات عنه.

يُرجع الأمر مستند XML.

الخطوة 2 بالنسبة لمعلومات الخط، أدخل عنوان URL التالي في المتصفح: **http://<phone ip address>/CGI/Java/LineInfo**

حيث

- <*phone ip address*>هو عنوان IP الخاص بالهاتف

يُرجع الأمر مستند XML.

الخطوة 3 بالنسبة لمعلومات الطراز، أدخل عنوان URL التالي في المتصفح: **http://<phone ip address>/CGI/Java/ModeInfo**

حيث

- <*phone ip address*>هو عنوان IP الخاص بالهاتف

يُرجع الأمر مستند XML.

مخرجات الأمر CallInfo النموذجية

يُعد رمز XML التالي مثالاً للمخرجات الناتجة عن الأمر CallInfo.

```
xml version="1.0" encoding="UTF-8"?>?>
<CiscoIPPhoneCallLineInfo>
<Prompt/>
<Notify/>
<Status/>
<LineDirNum>1030</LineDirNum>
<LineState>CONNECTED</LineState>
<CiscoIPPhoneCallInfo>
<CallState>CONNECTED</CallState>
```

```
<CallType>INBOUND</CallType>
<CallingPartyName/>
<CallingPartyDirNum>9700</CallingPartyDirNum>
<CalledPartyName/>
<CalledPartyDirNum>1030</CalledPartyDirNum>
<HuntPilotName/>
<CallReference>30303060</CallReference>
<CallDuration>12835</CallDuration>
<CallStatus>null</CallStatus>
<CallSecurity>UNAUTHENTICATED</CallSecurity>
<CallPrecedence>ROUTINE</CallPrecedence>
<FeatureList/>
</CiscoIPPhoneCallInfo>
<VisibleFeatureList>
<Feature Position="1" Enabled="true" Label="End Call"/>
<Feature Position="2" Enabled="true" Label="Show Detail"/>
</VisibleFeatureList>
<</CiscoIPPhoneCallLineInfo
```

مخرجات الأمر LineInfo النموذجية

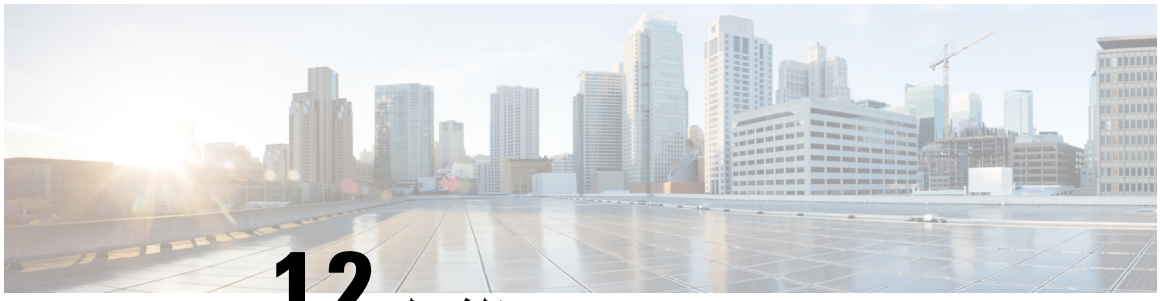
يُعد رمز XML التالي مثالاً للمخرجات الناتجة عن أمر LineInfo.

```
CiscoIPPhoneLineInfo>>
<Prompt/>
<Notify/>
<Status>null</Status>
<CiscoIPPhoneLines>
<LineType>9</LineType>
<lineDirNum>1028</lineDirNum>
<MessageWaiting>NO</MessageWaiting>
<RingerName>Chirp1</RingerName>
<LineLabel/>
<LineIconState>ONHOOK</LineIconState>
</CiscoIPPhoneLines>
<CiscoIPPhoneLines>
<LineType>9</LineType>
<lineDirNum>1029</lineDirNum>
<MessageWaiting>NO</MessageWaiting>  <RingerName>Chirp1</RingerName>
<LineLabel/>
<LineIconState>ONHOOK</LineIconState>
</CiscoIPPhoneLines>
<CiscoIPPhoneLines>
<LineType>9</LineType>
<lineDirNum>1030</lineDirNum>
<MessageWaiting>NO</MessageWaiting>
<RingerName>Chirp1</RingerName>
<LineLabel/>
<LineIconState>CONNECTED</LineIconState>
</CiscoIPPhoneLines>
<CiscoIPPhoneLines>
<LineType>2</LineType>
<lineDirNum>9700</lineDirNum>
<MessageWaiting>NO</MessageWaiting>
<LineLabel>SD9700</LineLabel>
<LineIconState>ON</LineIconState>
</CiscoIPPhoneLines>
<</CiscoIPPhoneLineInfo
```

مخرجات الأمر ModeInfo النموذجية

يُعد رمز XML التالي مثالاً للمخرجات الناتجة عن أمر ModeInfo.

```
xml version="1.0" encoding="utf-8"?>?>
                <CiscoIPPhoneModeInfo>
 <PlaneTitle>Applications</PlaneTitle>
 <PlaneFieldCount>12</PlaneFieldCount>
<PlaneSoftKeyIndex>0</PlaneSoftKeyIndex>
 <PlaneSoftKeyMask>0</PlaneSoftKeyMask>
                     <Prompt></Prompt>
                     <Notify></Notify>
                     <Status></Status>
                  <CiscoIPPhoneFields>
               <FieldType>0</FieldType>
                <FieldAttr></FieldAttr>
   <fieldHelpIndex>0</fieldHelpIndex>
  <FieldName>Call History</FieldName>
            <FieldValue></FieldValue>
                </CiscoIPPhoneFields>
                 <CiscoIPPhoneFields>
               <FieldType>0</FieldType>
                <FieldAttr></FieldAttr>
   <fieldHelpIndex>0</fieldHelpIndex>
   <FieldName>Preferences</FieldName>
            <FieldValue></FieldValue>
                </CiscoIPPhoneFields>
                                  ...
              <</CiscoIPPhoneModeInfo
```



الفصل 12

استكشاف أخطاء الهاتف وإصلاحها

معلومات عامة عن استكشاف المشكلات وإصلاحها

يعرض الجدول التالي معلومات عامة حول استكشاف المشكلات وإصلاحها في هاتف Cisco IP .

الجدول *30*: استكشاف مشكلات هاتف *Cisco IP* وإصلاحها

ملخص	الشرح
قد تتسبب عواصف الإرسال الممتدة لفترات طويلة في إعادة تعيين هواتف IP، أو عدم قدرتها على إجراء مكالمات أو الرد عليها.	قد تتسبب عاصفة الإرسال من الطبقة 2 الممتدة لفترة طويلة (تستغرق عدة دقائق) على VLAN للـ تعيين هواتف IP أو فقط مكالمة نشطة أو عدم القدرة على بدء مكالمة أو الرد عليها. وقد لا تعود الهو حتى تنتهي عاصفة الإرسال.
نقل اتصال الشبكة من الهاتف إلى محطة العمل	إذا كنت تصل هاتفك بالطاقة من خلال اتصال الشبكة، فيجب أن تتوخى الحذر إذا قررت فصل اتـ عن الهاتف وتوصيل الكبل في جهاز كمبيوتر سطح المكتب. **تنبيه** لا يمكن أن تستقبل بطاقة الشبكة في الكمبيوتر الطاقة من خلال اتصال الشبكة؛ وف خروج طاقة من خلال الاتصال، قد تتعرض بطاقة الشبكة للتلف. لحماية بطاقة الش 10 ثوانٍ أو أكثر بعد فصل الكبل من الهاتف قبل توصيله بجهاز الكمبيوتر. فهذه ا المفتاح وقتًا كافيًا ليدرك أن الهاتف لم يعد موجودًا على الخط ويتوقف عن إمداد ا الكبل.

ملخص	الشرح
تغيير تكوين الهاتف	بشكل افتراضي، يتم تأمين إعدادات كلمة مرور المسؤول لمنع المستخدمين من إجراء تغييرا كفاءة اتصال الشبكة. يجب عليك إلغاء تأمين إعدادات كلمة مرور المسؤول قبل أن تتمكن من راجع تطبيق كلمة مرور الهاتف, في الصفحة 40 للحصول على تفاصيل. **ملاحظة** إذا كانت كلمة مرور المسؤول غير معينة في ملف تعريف الهاتف العام، فيمك تعديل إعدادات الشبكة.
عدم تطابق الترميز بين الهاتف وجهاز آخر	تُظهر إحصاءات RxType وTxType الترميز المستخدم لمحادثة بين هاتف Cisco IP وج أن تتطابق قيم هذه الإحصاءات. وإذا لم تتطابق، فتحقق من أن الجهاز الآخر يمكنه ترميز المح محول شفرات لمعالجة الخدمة. راجع عرض نافذة إحصاءات المكالمة, في الصفحة 130 للحص
عدم تطابق عينة الصوت بين الهاتف وجهاز آخر	تُظهر إحصاءات RxSize وTxSize حجم حزم الصوت المستخدمة في محادثة بين هاتف P آخر. يجب أن تتطابق قيم هذه الإحصاءات. راجع عرض نافذة إحصاءات المكالمة, في الصفح على تفاصيل.
حالة الاسترجاع	يمكن أن تحدث حالة الاسترجاع عند تحقق الشروط التالية: • خيار تكوين منفذ SW على الهاتف معين على Half 10 (10BaseT/أحادي الاتجاه • يستقبل الهاتف الطاقة من مصدر إمداد طاقة خارجي. • تنخفض طاقة البطارية (تم فصل مصدر إمداد الطاقة). في هذه الحالة، يمكن أن يصبح منفذ المفتاح الموجود في الهاتف معطلاً وتظهر الرسالة التالي تحكم المفتاح: HALF_DUX_COLLISION_EXCEED_THRESHOLD لحل هذه المشكلة، أعد تمكين المنفذ من المفتاح.

مشكلات بدء التشغيل

بعد تثبيت أحد الهواتف في شبكتك وإضافته إلى Cisco Unified Communications Manager، من المفترض أن يبدأ تشغيل الهاتف على النحو الموضح في الموضوع ذي الصلة أدناه.

إذا لم يبدأ تشغيل الهاتف على نحوٍ صحيح، فراجع الأقسام التالية للاطلاع على معلومات استكشاف المشكلات وإصلاحها.

موضوعات ذات صلة

التحقق من بدء تشغيل الهاتف, في الصفحة 50

هاتف Cisco IP لا يتم عملية بدء التشغيل العادية

المشكلة

عند توصيل هاتف Cisco IP بمنفذ الشبكة، لا يكمل الهاتف عملية بدء التشغيل العادية على النحو الموضح في الموضوع ذي الصلة ولا تعرض شاشة الهاتف أي معلومات.

السبب

إذا لم يكمل الهاتف عملية بدء التشغيل، فقد يتمثل السبب في وجود كبلات تالفة أو وصلات سيئة أو انقطاع الشبكة أو عدم وجود طاقة أو قد يكون الهاتف لا يعمل.

الحل

لتحديد ما إذا كان الهاتف يعمل أم لا، استخدم الاقتراحات التالية للقضاء على المشكلات الأخرى المحتملة.

- تحقق من أن منفذ الشبكة يعمل:
  - استبدل كبلات إيثرنت بكبلات تعرف أنها تعمل بشكل سليم.
  - افصل هاتف Cisco IP الذي يعمل من منفذ آخر وقم بتوصيله بمنفذ هذه الشبكة للتحقق من أن المنفذ نشط.
  - صِل هاتف Cisco IP الذي لم يبدأ التشغيل بمنفذ شبكة مختلف تعرف أنه يعمل بشكل جيد.
  - صِل هاتف Cisco IP الذي لم يبدأ التشغيل مباشرة بالمنفذ الموجود بالمفتاح، لإزالة اتصال لوحة مقابس التوصيل في المكتب.
- تحقق من أن الهاتف يستقبل الطاقة:
  - إذا كنت تستخدم مصدر طاقة خارجيًا، فتحقق من أن مأخذ التيار الكهربائي يعمل بشكل سليم.
  - إذا كنت تستخدم تيارًا خطيًا، فاستخدم مصدر إمداد طاقة مباشرًا بدلاً منه.
  - إذا كنت تستخدم مصدر إمداد طاقة خارجي، فبدله بوحدة تعرف أنها تعمل بشكل سليم.
- إذا لم يبدأ تشغيل الهاتف بشكل سليم، فصِل الهاتف بالطاقة من صورة برنامج النسخة الاحتياطية.
- إذا لم يبدأ تشغيل الهاتف بشكل سليم، فقم بإجراء إعادة تعيين إعدادات المصنع للهاتف.
- بعد محاولة تنفيذ هذه الحلول، إذا لم تعرض شاشة هاتف Cisco IP أي حروف بعد خمس دقائق على الأقل، فاتصل بممثل الدعم الفني لدى Cisco للحصول على مساعدة إضافية.

موضوعات ذات صلة

التحقق من بدء تشغيل الهاتف, في الصفحة 50

لا يتم تسجيل Cisco IP باستخدام Cisco Unified Communications Manager

إذا تابع الهاتف إتمام المرحلة الأولى من عملية بدء التشغيل (يضيء ويميض أزرار LED وينطفئ) ولكنه استمر في تكرار دورته عبر الرسائل التي يتم عرضها على شاشة الهاتف، فذلك يدل على عدم بدء تشغيل الهاتف بشكل صحيح. يتعذر بدء تشغيل الهاتف بنجاح ما لم يتصل بشبكة الإيثرنت ويتم تسجيله باستخدام خادم Cisco Unified Communications Manager.

بالإضافة إلى ذلك، قد تمنع المشكلات المتعلقة بالأمان بدء تشغيل الهاتف بشكل صحيح. راجع إجراءات استكشاف المشكلات وإصلاحها, في الصفحة 156 للحصول على مزيد من المعلومات.

يعرض الهاتف رسائل أخطاء

المشكلة

تعرض رسائل الحالة الأخطاء التي تحدث أثناء بدء التشغيل.

الحل

أثناء دوران الهاتف من خلال عملية بدء التشغيل، يمكنك الوصول إلى رسائل الحالة التي قد توفر لك معلومات حول سبب المشكلة. راجع قسم "نافذة عرض رسائل الحالة" للحصول على تعليمات حول الوصول إلى رسائل الحالة وقائمة بالأخطاء المحتملة، وشروحها، وحلولها.

موضوعات ذات صلة

عرض نافذة رسائل الحالة, في الصفحة 122

يتعذر على الهاتف الاتصال بخادم TFTP أو Cisco Unified Communications Manager

المشكلة

إذا كان اتصال الشبكة معطلاً بين الهاتف وخادم TFTP أو Cisco Unified Communications Manager، فيتعذر بدء تشغيل الهاتف بشكل صحيح.

الحل

تأكد من أن الشبكة قيد التشغيل في الوقت الحالي.

يتعذر على الهاتف الاتصال بخادم TFTP

المشكلة

قد لا تكون إعدادات خادم TFTP صحيحة

الحل

تحقق من إعدادات TFTP

موضوعات ذات صلة

التحقق من إعدادات TFTP, في الصفحة 157

يتعذر على الهاتف الاتصال بالخادم

المشكلة

قد لا يكون حقلا عنونة IP وتوجيه مسار IP مهيأين على نحو صحيح.

الحل

يجب أن تتحقق من صحة إعدادات عنونة IP وتوجيه مسار IP على الهاتف. إذا كنت تستخدم DHCP، فيجب أن يوفر خادم DHCP هذه القيم. إذا كنت قد عينت عنوان IP ثابتًا إلى الهاتف، فيجب إدخال هذه القيم يدويًا.

موضوعات ذات صلة

التحقق من إعدادات DHCP, في الصفحة 157

يتعذر على الهاتف الاتصال باستخدام DNS

المشكلة

قد تكون إعدادات DNS غير صحيحة.

الحل

إذا كنت تستخدم DNS للوصول إلى خادم TFTP أو Cisco Unified Communications Manager، فيجب أن تتأكد من تحديد خادم DNS.

موضوعات ذات صلة

التحقق من إعدادات DNS, في الصفحة 159

يتعذر تشغيل Cisco Unified Communications Manager وخدمات TFTP

المشكلة

إذا كان يتعذر تشغيل Cisco Unified Communications Manager أو خدمات TFTP، فربما تكون الهواتف غير قادرة على بدء التشغيل بشكل صحيح. وفي هذه الحالة، من الأرجح أن تواجه فشلاً على مستوى النظام، كما يتعذر بدء تشغيل الهواتف والأجهزة الأخرى بشكل صحيح.

الحل

إذا كان يتعذر تشغيل خدمة Cisco Unified Communications Manager، فتتأثر جميع الأجهزة الموجودة على الشبكة التي تعتمد عليها في إجراء المكالمات الهاتفية. إذا كان يتعذر تشغيل خدمة TFTP، فلا تستطيع العديد من الأجهزة بدء التشغيل بنجاح. للحصول على مزيد من المعلومات، ارجع إلى بدء الخدمة, في الصفحة 159.

تلف ملف التهيئة

المشكلة

إذا استمر وجود مشكلات لديك متعلقة بهاتف معين لا تنجح في حلها الاقتراحات الأخرى الواردة في هذا الفصل، فقد يكون ملف التهيئة تالفًا.

الحل

أنشئ ملف تهيئة جديدًا للهاتف.

موضوعات ذات صلة

إنشاء ملف تهيئة هاتف جديد, في الصفحة 158

تسجيل هاتف Cisco Unified Communications Manager

المشكلة

لا يتم تسجيل الهاتف باستخدام Cisco Unified Communications Manager.

الحل

يمكن تسجيل هاتف Cisco IP باستخدام خادم Cisco Unified Communications Manager فقط إذا تمت إضافة الهاتف إلى الخادم أو إذا تم تمكين التسجيل التلقائي. راجع المعلومات والإجراءات الواردة في أساليب إضافة الهاتف, في الصفحة 57 لضمان إضافة الهاتف إلى قاعدة بيانات Cisco Unified Communications Manager.

للتحقق من وجود الهاتف في قاعدة بيانات Cisco Unified Communications Manager، اختر **الجهاز** > **الهاتف** من "إدارة Cisco Unified Communications Manager". انقر فوق **بحث** للبحث عن الهاتف استنادًا إلى عنوان MAC. للحصول على معلومات حول تحديد عنوان MAC، راجع تحديد عنوان MAC للهاتف, في الصفحة 57.

إذا كان الهاتف موجودًا في قاعدة بيانات Cisco Unified Communications Manager بالفعل، فقد يكون ملف التهيئة تالفًا. راجع تلف ملف التهيئة, في الصفحة 149 لمزيد من المساعدة.

يتعذر على هاتف Cisco IP الحصول على عنوان IP

المشكلة

إذا تعذر على الهاتف الحصول على عنوان IP عند بدء تشغيله، فقد لا يكون الهاتف موجودًا على نفس الشبكة أو VLAN كخادم DHCP، أو قد يكون منفذ مفتاح التحويل الذي يتصل به الهاتف معطلاً.

الحل

تأكد من أن الشبكة أو VLAN التي يتصل بها الهاتف تمتلك إمكانية الوصول إلى خادم DHCP، وتأكد من أن منفذ مفتاح التحويل ممكن.

مشكلات إعادة تعيين الهاتف

إذا أبلغ المستخدمون عن أن هواتفهم تقوم بإعادة التعيين أثناء المكالمات أو عندما تكون خاملة، فيجب أن تتحقق من السبب. إذا كان اتصال الشبكة واتصال Cisco Unified Communications Manager مستقرين، فيجب عدم إعادة تعيين الهاتف.

وعادةً ما تتم إعادة تعيين الهاتف إذا واجهته مشكلات في الاتصال بالشبكة أو بـ Cisco Unified Communications Manager.

تتم إعادة تعيين الهاتف بسبب أعطال الشبكة المتقطعة

المشكلة

قد تتعرض شبكتك لأعطال متقطعة.

الحل

تؤثر أعطال الشبكة المتقطعة على البيانات ونقل حركة الصوت بشكل مختلف. ربما تكون شبكتك تواجه أعطالاً متقطعة دون اكتشافها. فإذا كان الأمر كذلك، فقد يقوم نقل حركة البيانات بإعادة إرسال حزم مفقودة والتحقق من استقبال الحزم وإرسالها. ومع ذلك، فإن خدمة نقل حركة الصوت لا يمكنها إعادة التقاط الحزم المفقودة. وبدلاً من إعادة نقل اتصال الشبكة المفقود، يقوم الهاتف بإعادة التعيين ومحاولة إعادة الاتصال بالشبكة. اتصل بمسؤول النظام للحصول على معلومات حول المشكلات المعروفة في الشبكة الصوتية.

تتم إعادة تعيين الهاتف بسبب وجود أخطاء في إعداد DHCP

المشكلة

قد تكون إعدادات DHCP غير صحيحة.

الحل

تحقق من أنك قد قمت بتهيئة الهاتف لاستخدام DHCP بشكل صحيح. تحقق من أنه قد تم إعداد خادم DHCP بشكل صحيح. تحقق من مدة تأجير DHCP. نوصي بتعيين مدة التأجير لمدة 8 أيام.

موضوعات ذات صلة

التحقق من إعدادات DHCP, في الصفحة 157

تتم إعادة تعيين الهاتف نظرًا لعدم صحة عنوان IP الثابت

المشكلة

قد يكون عنوان IP الثابت الذي تم تعيينه إلى الهاتف غير صحيح.

الحل

إذا تم تعيين عنوان IP ثابت إلى الهاتف، فتحقق من أنك أدخلت الإعدادات الصحيحة.

تتم إعادة تعيين الهاتف أثناء استخدام الشبكة الكثيف

المشكلة

إذا تعرض الهاتف لإعادة التعيين أثناء استخدام الشبكة الكثيف، فمن الأرجح ألا يكون قد تم تهيئة VLAN للصوت لديك.

الحل

يؤدي عزل الهواتف على شبكة VLAN إضافية منفصلة إلى زيادة مستوى جودة حركة مرور الصوت.

تتم إعادة تعيين الهاتف بسبب إعادة التعيين المتعمد

المشكلة

إذا لم تكن المسؤول الوحيد المخول بالوصول إلى Cisco Unified Communications Manager، فيجب أن تتحقق من عدم قيام شخص آخر بإعادة تعيين الهواتف بشكل متعمد.

الحل

يمكنك التحقق مما إذا كان هاتف Cisco IP قد تلقى أمرًا من Cisco Unified Communications Manager لإعادة تعيينه عن الطريق الضغط على **الإعدادات** على الهاتف واختيار **إعدادات المسؤول** > **الحالة** > **إحصاءات الشبكة**.

- إذا كان حقل "سبب إعادة التشغيل" يعرض `Reset–Reset`، فيتلقى الهاتف أمر Reset/Reset من "إدارة Cisco Unified Communications Manager".
- إذا كان حقل "سبب إعادة التشغيل" يعرض `Reset-Restart`، فإن الهاتف مغلق لأنه تلقى أمر Reset/Restart من Cisco Unified Communications Manager.

تتم إعادة تعيين الهاتف بسبب حدوث مشكلات في DNS أو غيرها من مشكلات الاتصال

المشكلة

تستمر إعادة تعيين الهاتف وتشتبه في وجود مشكلات في DNS أو غيرها من مشكلات الاتصال.

الحل

إذا استمرت إعادة تعيين الهاتف، فتخلص من الأخطاء الموجودة في DNS أو غيرها من أخطاء الاتصال من خلال اتباع الإجراء الوارد في تحديد مشكلات DNS أو الاتصال, في الصفحة 157.

لا تصل الطاقة إلى الهاتف

المشكلة

لا يبدو اتصال الهاتف بالطاقة.

الحل

في معظم الحالات، تتم إعادة تشغيل الهاتف إذا اتصل بمصدر طاقة خارجي ولكنه يفقد ذلك الاتصال ويتحول إلى الطاقة عبر إيثرنت (PoE). وعلى نحو مشابه، قد تتم إعادة تشغيل الهاتف إذا اتصل بالطاقة عبر إيثرنت (PoE)، ثم يتصل بمصدر خارجي لإمداده بالطاقة.

يتعذر على الهاتف الاتصال بشبكة LAN

المشكلة

قد يكون الاتصال المادي بشبكة LAN مقطوعًا.

الحل

تحقق من أن وصلة الإيثرنت التي يتصل بها هاتف Cisco IP تعمل. على سبيل المثال، تحقق مما إذا كان أحد المنافذ أو أجهزة التبديل التي يتصل الهاتف بها معطلاً أم لا، وتحقق أيضًا مما إذا كانت تتعذر إعادة تشغيل جهاز التبديل أم لا. تأكد أيضًا من عدم وجود قطع في الكبل.

مشكلات أمان هاتف Cisco IP

تعرض الأقسام التالية معلومات حول استكشاف المشكلات وإصلاحها لميزات الأمان على هاتف Cisco IP . للحصول على معلومات حول حلول أي من هذه المشكلات، وللحصول على معلومات إضافية حول استكشاف مشكلات الأمان وإصلاحها، راجع دليل أمان *Cisco Unified Communications Manager*.

مشكلات ملف CTL

تصف الأقسام التالية المشكلات المتعلقة باستكشاف مشكلات ملف CTL وإصلاحها.

حدث خطأ في المصادقة، حيث تتعذر على الهاتف مصادقة ملف CTL

المشكلة

حدث خطأ في مصادقة الجهاز.

السبب

لا يحتوي ملف CTL على شهادة Cisco Unified Communications Manager أو يحتوي على شهادة غير صحيحة.

الحل

قم بتثبيت شهادة صحيحة.

يتعذر على الهاتف مصادقة ملف CTL

المشكلة

يتعذر على الهاتف مصادقة ملف CTL.

السبب

رمز الأمان الذي وقع على ملف CTL المحدث غير موجود في ملف CTL على الهاتف.

الحل

قم بتغيير رمز الأمان في ملف CTL، ثم قم بتثبيت الملف الجديد على الهاتف.

تتم مصادقة ملف CTL، إلا أن ملفات تكوين أخرى تتعذر مصادقتها

المشكلة

تتعذر على الهاتف مصادقة أي من ملفات التكوين باستثناء ملف CTL.

السبب

يوجد سجل TFTP تالف أو يتعذر اعتماد ملف التكوين بشهادة مقابلة في قائمة الثقة للهواتف.

الحل

تحقق من سجل TFTP والشهادة الموجودة في قائمة الثقة.

تتم مصادقة ملف ITL ولكن تتعذر مصادقة ملفات التكوين الأخرى

المشكلة

تتعذر على الهاتف مصادقة أي من ملفات التكوين باستثناء ملف ITL.

السبب

قد لا يتم اعتماد ملف التكوين بشهادة مقابلة في قائمة الثقة للهواتف.

الحل

أعِد اعتماد ملف التكوين باستخدام الشهادة الصحيحة.

فشل تفويض TFTP

المشكلة

يبلغ الهاتف عن فشل تفويض TFTP.

السبب

عنوان TFTP للهاتف غير موجود في ملف CTL.

إذا قمت بإنشاء ملف CTL جديد مع سجل CTL جديد، فقد لا يحتوي ملف CTL الموجود على الهاتف على سجل لخادم TFTP الجديد.

الحل

تحقق من تكوين عنوان TFTP في ملف CTL الخاص بالهاتف.

لا يتم تسجيل الهاتف

المشكلة

لا يتم تسجيل الهاتف من خلال Cisco Unified Communications Manager.

السبب

لا يحتوي ملف CTL على المعلومات الصحيحة لخادم Cisco Unified Communications Manager.

الحل

قم بتغيير معلومات خادم Cisco Unified Communications Manager في ملف CTL.

لم يتم طلب ملفات التكوين الموقعة

المشكلة

لا يطلب الهاتف ملفات التكوين الموقعة.

السبب

لا يشتمل ملف CTL على أي إدخالات TFTP مقترنة بشهادات.

الحل

كوّن إدخالات TFTP باستخدام الشهادات الموجودة في ملف CTL.

مشكلات الصوت

تصف الأقسام التالية كيفية حل مشكلات الصوت.

لا يوجد مسار للكلام

المشكلة

يتعذر على شخص أو أكثر في المكالمة سماع أي صوت.

الحل

عندما لا يستقبل شخص واحد على الأقل صوتًا أثناء مكالمة، فإن هذا معناه أنه لم يتم إنشاء اتصال IP بين الهواتف. تحقق من تكوين الموجهات ومفاتيح التحويل للتأكد من أنه تم تكوين اتصال IP بشكل صحيح.

الكلام متقطع

المشكلة

يشكو المستخدم من أن الكلام متقطع أثناء المكالمة.

السبب

قد توجد حالة عدم مطابقة في تكوين التشويش.

الحل

تحقق من إحصاءات AvgJtr وMaxJtr. قد يشير التباين الكبير بين هذه الإحصاءات إلى وجود مشكلة في معدل التشويش على الشبكة أو ارتفاع المعدلات الدورية لنشاط الشبكة.

لا يعمل الهاتف الأول في وضع Daisy Chain

المشكلة

في وضع سلسلتين، أحد هواتف المؤتمر لا يعمل.

الحل

تأكد أن الكبلات المتصلة بالمحول الذكي هي الكبلات الصحيحة. يقوم الكبلان الأكبر سمكًا بتوصيل الهواتف بالمحول الذكي. يقوم الكبل الأكثر نحافة بتوصيل المحول الذكي بمحول الطاقة.

موضوعات ذات صلة

وضع سلسلتين, في الصفحة 30
تثبيت هاتف المؤتمر في وضع Daisy Chain, في الصفحة 36

المشكلات العامة للمكالمات الهاتفية

توفر الأقسام التالية المساعدة لاستكشاف مشكلات المكالمات الهاتفية وإصلاحها.

يتعذر إنشاء مكالمة هاتفية

المشكلة

يشكو المستخدم من عدم القدرة على إجراء مكالمة

السبب

يتعذر على الهاتف الذي لا يتوفر له عنوان IP لـ DHCP التسجيل في Cisco Unified Communications Manager. تعرض الهواتف المزودة بشاشة LCD رسالة تكوين IP أو تسجيل. تقوم الهواتف غير المزودة بشاشة LCD بتشغيل رنين إعادة الطلب (بدلاً من رنين الطلب) في سماعة الهاتف عند محاولة المستخدم إجراء مكالمة.

الحل

1. تحقق من الإجراءات التالية:
   1. كبل الإيثرنت متصل.
   2. خدمة Cisco CallManager قيد التشغيل على خادم Cisco Unified Communications Manager.
   3. كلا الهاتفين مسجلان في Cisco Unified Communications Manager نفسه.
2. تصحيح أخطاء خادم الصوت والتقاط السجلات ممكّنان لكلا الهاتفين. إذا لزم الأمر، فقم بتمكين تصحيح أخطاء Java.

لا يتعرف الهاتف على أرقام DTMF أو تأخر إرسال الأرقام

المشكلة

يشكو المستخدم من فقدان أو تأخرها عند استخدام لوحة المفاتيح.

السبب

قد يؤدي الضغط على المفاتيح سريعًا إلى فقدان الأرقام أو تأخرها.

الحل

يجب عدم الضغط على المفاتيح سريعًا.

إجراءات استكشاف المشكلات وإصلاحها

يمكن استخدام هذه الإجراءات لتحديد المشكلات وتصحيحها.

إنشاء تقرير بمشكلات الهاتف من Cisco Unified Communications Manager

يمكنك إنشاء تقرير بمشكلات الهاتف من Cisco Unified Communications Manager. يُنتج هذا الإجراء نفس المعلومات التي يُنشئها المفتاح الوظيفي لأداة الإبلاغ عن المشكلات (PRT) على الهاتف.

يحتوي تقرير المشكلات على معلومات حول الهاتف وسماعات الهاتف.

اجراء

الخطوة 1	في إدارة Cisco Unified CM، حدد **الجهاز** > **الهاتف**.
الخطوة 2	انقر فوق **بحث** وحدد هاتف Cisco IP واحدًا أو أكثر.
الخطوة 3	انقر فوق **إنشاء أداة الإبلاغ عن المشكلات لما تم تحديده** لجمع سجلات أداة الإبلاغ عن المشكلات لسماعات الهاتف المستخدمة في هواتف Cisco IP المحددة.

التحقق من إعدادات TFTP

	اجراء
الخطوة 1	تحقق من حقل خادم TFTP رقم 1. إذا كنت قد عينت عنوان IP ثابتًا إلى الهاتف، فيجب إدخال إعداد لخيار "خادم TFTP الأول". إذا كنت تستخدم DHCP، فيحصل الهاتف على عنوان خادم TFTP من خادم DHCP. تحقق من تهيئة عنوان IP في الخيار 150.
الخطوة 2	يمكنك أيضًا تمكين الهاتف من استخدام خادم TFTP بديل. حيث يكون هذا الإعداد مفيدًا تحديدًا إذا تم نقل الهاتف مؤخرًا من موقع إلى آخر.
الخطوة 3	إذا كان DHCP المحلي لا يوفر عنوان TFTP الصحيح، فمكّن الهاتف من استخدام خادم TFTP بديل. حيث يُعد ذلك ضروريًا في سيناريوهات VPN.

تحديد مشكلات DNS أو الاتصال

	اجراء
الخطوة 1	استخدم قائمة إعادة تعيين الإعدادات لإعادة تعيين إعدادات الهاتف إلى قيمها الافتراضية.
الخطوة 2	تعديل إعدادات DHCP وIP: a) قم بتعطيل DHCP. b) قم بتعيين قيم IP الثابت إلى الهاتف. استخدم إعداد الموجّه الافتراضي نفسه الذي تستخدمه الهواتف الأخرى التي تعمل بشكل سليم. c) قم بتعيين خادم TFTP. استخدم خادم TFTP نفسه الذي تستخدمه الهواتف الأخرى التي تعمل بشكل سليم.
الخطوة 3	على خادم Cisco Unified Communications Manager، تحقق من أن ملفات المضيف المحلية تحتوي على اسم خادم Cisco Unified Communications Manager الصحيح معيّنًا لعنوان IP الصحيح.
الخطوة 4	من Cisco Unified Communications Manager، اختر **النظام** > **الخادم** وتحقق من أن الإشارة إلى الخادم تتم عن طريق عنوان IP وليس عن طريق اسم DNS.
الخطوة 5	من Cisco Unified Communications Manager، اختر **الجهاز** > **الهاتف**. انقر فوق **بحث** للبحث عن هذا الهاتف. تحقق من أنك قد قمت بتعيين عنوان MAC الصحيح لهاتف Cisco IP .
الخطوة 6	أعد تشغيل دورة الطاقة للهاتف.

موضوعات ذات صلة

تحديد عنوان MAC للهاتف, في الصفحة 57
إعادة تشغيل أو إعادة تعيين هاتف المؤتمر, في الصفحة 161

التحقق من إعدادات DHCP

	اجراء
الخطوة 1	على الهاتف، اضغط على **الإعدادات**.

الخطوة 2 حدد **إعدادات المسؤول** > **إعداد إيثرنت** > **إعداد IPv4**.

الخطوة 3 تحقق من حقل خادم DHCP.

إذا عينت عنوان IP ثابتًا إلى الهاتف، فلا تحتاج إلى إدخال قيمة لخيار "خادم DHCP". ومع ذلك، إذا كنت تستخدم خادم DHCP، فيجب أن يشتمل هذا الخيار على قيمة. في حالة عدم وجود قيمة، تحقق من تهيئة توجيه IP وشبكة VLAN. راجع وثائق استكشاف مشكلات منفذ وواجهة المحول وإصلاحها والمتوفرة في عنوان URL التالي:

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

الخطوة 4 تحقق من حقول عنوان IP وقناع الشبكة الفرعية وجهاز التوجيه الافتراضي.

إذا قمت بتعيين عنوان IP ثابت إلى الهاتف، فيجب عليك إدخال الإعدادات لهذه الخيارات يدويًا.

الخطوة 5 إذا كنت تستخدم DHCP، فتحقق من عناوين IP التي يوزعها خادم DHCP لديك.

راجع وثائق فهم واستكشاف مشكلات *DHCP* في محول *Catalyst* أو شبكات المؤسسات وإصلاحها والمتوفرة في عنوان URL التالي:

https://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml

إنشاء ملف تهيئة هاتف جديد

عند إزالة هاتف من قاعدة بيانات Cisco Unified Communications Manager، يتم حذف ملف التهيئة من خادم TFTP الخاص بـ Cisco Unified Communications Manager. يظل رقم أو أرقام دليل الهاتف موجودة في قاعدة بيانات Cisco Unified Communications Manager. وتسمى DNs غير معينة ويمكن استخدامها للأجهزة الأخرى. في حالة عدم استخدام DNs بواسطة الأجهزة الأخرى، احذف DNs هذه من قاعدة بيانات Cisco Unified Communications Manager. يمكنك استخدام تقرير خطة المسار لعرض أرقام المرجع غير المعينة وحذفها. للحصول على مزيد من المعلومات، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.

قد يتسبب تغيير الأزرار على قالب زر الهاتف، أو تعيين قالب زر هاتف مختلف إلى هاتف، في عدم إمكانية الوصول إلى أرقام الدليل من الهاتف. لا تزال أرقام الدليل معينة على الهاتف في قاعدة بيانات Cisco Unified Communications Manager، ولكن الهاتف لا يشتمل على زر يمكن من خلاله الرد على المكالمات. يجب إزالة أرقام الدليل هذه من الهاتف وحذفها إذا لزم الأمر.

اجراء

الخطوة 1 من Cisco Unified Communications Manager، اختر **الجهاز** > **الهاتف** وانقر فوق **بحث** لتحديد موقع الهاتف الذي يواجه مشكلات.

الخطوة 2 اختر **حذف** لإزالة الهاتف من قاعدة بيانات Cisco Unified Communications Manager.

ملاحظة عند إزالة هاتف من قاعدة بيانات Cisco Unified Communications Manager، يتم حذف ملف التهيئة من خادم TFTP الخاص بـ Cisco Unified Communications Manager. يظل رقم أو أرقام دليل الهاتف موجودة في قاعدة بيانات Cisco Unified Communications Manager. وتسمى DNs غير معينة ويمكن استخدامها للأجهزة الأخرى. في حالة عدم استخدام DNs بواسطة الأجهزة الأخرى، احذف DNs هذه من قاعدة بيانات Cisco Unified Communications Manager. يمكنك استخدام تقرير خطة المسار لعرض أرقام المرجع غير المعينة وحذفها.

الخطوة 3 أضف الهاتف مرة أخرى إلى قاعدة بيانات Cisco Unified Communications Manager.

الخطوة 4 أعد تشغيل دورة الطاقة للهاتف.

موضوعات ذات صلة

أساليب إضافة الهاتف, في الصفحة 57
وثائق Cisco Unified Communications Manager, في الصفحة 14

التحقق من إعدادات DNS

اجراء

الخطوة 1 على الهاتف، اضغط على **الإعدادات**.

الخطوة 2 حدد **إعدادات المسؤول** > **إعداد إيثرنت** > **إعداد IPv4**.

الخطوة 3 تحقق من أنه تم تعيين حقل خادم DNS رقم 1 بشكل صحيح.

الخطوة 4 يجب أن تتحقق أيضًا من إجراء إدخال CNAME في خادم DNS بدلاً من خادم TFTP وكذلك نظام Cisco Unified Communications Manager.

كما يجب أن تتأكد من تكوين DNS لإجراء عمليات البحث العكسية.

بدء الخدمة

يجب تنشيط الخدمة قبل التمكن من بدئها أو إيقافها.

اجراء

الخطوة 1 من إدارة Cisco Unified Communications Manager، اختر **Cisco Unified Serviceability** من قائمة "التنقل" المنسدلة، ثم انقر فوق **انتقال**.

الخطوة 2 اختر **أدوات** > **مركز التحكم — خدمات الميزات**.

الخطوة 3 اختر خادم Cisco Unified Communications Manager الأساسي من قائمة "الخادم" المنسدلة.

تعرض النافذة أسماء الخدمات الخاصة بالخادم الذي تختاره وحالة الخدمات ولوحة التحكم بالخدمة لبدء الخدمة أو إيقافها.

الخطوة 4 إذا توقفت الخدمة، فانقر فوق زر الراديو المقابل، ثم انقر فوق **بدء**.

يتغير رمز "حالة الخدمة" من مربع إلى سهم.

التحكم في معلومات تصحيح الأخطاء من Cisco Unified Communications Manager

إذا كنت تواجه مشكلات في الهاتف لا يمكنك حلها، فيمكن لـ Cisco TAC أن يساعدك. سيلزمك تشغيل تصحيح الأخطاء على الهاتف وإعادة طرح المشكلة وإيقاف تشغيل تصحيح الأخطاء وإرسال السجلات إلى TAC لتحليلها.

نظرًا لأن تصحيح الأخطاء يعمل على جمع معلومات تفصيلية، قد تؤدي حركة مرور الاتصال إلى إبطاء الهاتف، مما يقلل من سرعة استجابته. بعد جمع السجلات، يجب أن توقف تشغيل تصحيح الأخطاء لضمان تشغيل الهاتف.

قد تشتمل معلومات تصحيح الأخطاء على رمز مكون من رقم واحد يعكس مدى خطورة الموقف. يتم تقييم المواقف على النحو التالي:

- 0 - طوارئ
- 1 - تنبيه

- 2 - حرج
- 3 - خطأ
- 4 - تحذير
- 5 - إعلام
- 6 - معلومات
- 7 - تصحيح الأخطاء

اتصل بـ Cisco TAC للحصول على مزيد من المعلومات والمساعدة.

اجراء

الخطوة 1 في "إدارة Cisco Unified Communications Manager"، حدد إحدى النوافذ التالية:

- **الجهاز** > **إعدادات الجهاز** > **ملف التعريف الشائع للهاتف**
- **النظام** > **تكوين هاتف المؤسسة**
- **الجهاز** > **الهاتف**

الخطوة 2 قم بتعيين المعلمات التالية:

- ملف السجل - القيم: معين مسبقًا (افتراضي)، الافتراضي، الهاتفية، SIP، واجهة المستخدم، الشبكة، الوسائط، ترقية، ملحقات، الأمان، Wi-Fi، VPN، الشبكة الظاهرية الخاصة، Energywise، الوصول من الأجهزة المتنقلة وعن بُعد
- سجل الوصول عن بُعد - القيم: تعطيل (افتراضي)، تمكين
- خادم سجل IPv6 أو خادم السجل - عنوان IP (عنوان IPv4 أو IPv6)

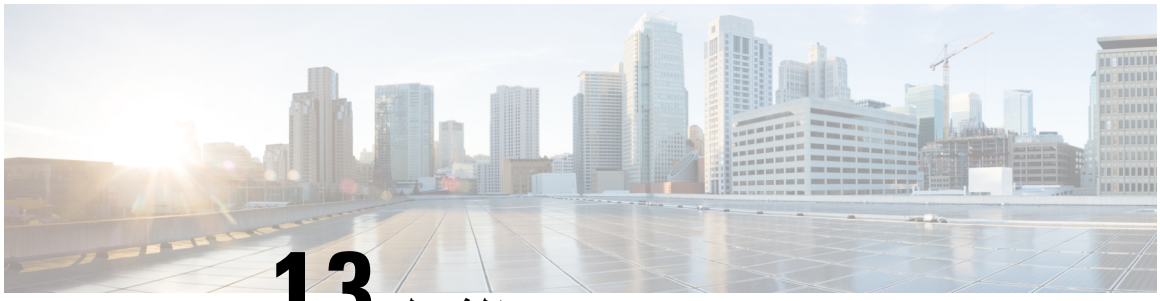
ملاحظة عندما يتعذر الوصول إلى خادم السجل، يتوقف الهاتف عن إرسال رسائل تصحيح الأخطاء.

- تنسيق عنوان خادم سجل IPv4 هو **العنوان:<0-1>;pfs=<0-7>@@base=<port>**
- تنسيق عنوان خادم سجل IPv4 هو **[العنوان]:<0-1>;pfs=<0-7>@@base=<port>**
- حيث:
  - يتم فصل عنوان IPv4 بنقطة (.)
  - يتم فصل عنوان IPv6 بعلامة النقطتين (:)

معلومات إضافية عن استكشاف المشكلات وإصلاحها

إذا كانت لديك أسئلة إضافية متعلقة باستكشاف مشكلات هاتفك وإصلاحها، فانتقل إلى موقع Cisco التالي على الويب وانتقل إلى طراز الهاتف المطلوب:

https://www.cisco.com/cisco/web/psa/troubleshoot.html



الفصل 13

الصيانة

إعادة تشغيل أو إعادة تعيين هاتف المؤتمر

تنفذ أنت عملية إعادة تعيين أساسية للهاتف للاسترداد في حالة تعرض الهاتف لخطأ. كما يمكنك استعادة التكوين وإعدادات الأمان إلى الإعدادات الافتراضية.

إعادة تشغيل هاتف المؤتمر

عند إعادة تشغيل الهاتف، يتم فقدان أي تغييرات على إعداد الشبكة والمستخدم لم يتم الالتزام بها في ذاكرة الفلاش في الهاتف.

اجراء

اضغط على **الإعدادات** > **إعدادات المسؤول** > **إعادة تعيين الإعدادات** > **إعادة تعيين الجهاز** .

موضوعات ذات صلة

إدخال النصوص والدخول إلى القوائم من الهاتف, في الصفحة 40

إعادة تعيين إعدادات هاتف المؤتمر من قائمة الهاتف

اجراء

الخطوة 1 اضغط على **إعدادات**.

الخطوة 2 اختر **إعدادات المسؤول** > **إعادة تعيين الإعدادات**.

الخطوة 3 حدد نوع إعادة التعيين.

- **الكل** — استعادة إعدادات المصنع.
- **إعادة تعيين الجهاز**—إعادة تعيين الجهاز. لا تتغير الإعدادات الموجودة.

- **الشبكة** — إعادة تعيين تكوين الشكة إلى الإعدادات الافتراضية.
- **وضع الخدمة**—مسح وضع الخدمة الحالي وإلغاء تنشيط VPN وإعادة تشغيل الهاتف.
- **الأمان** — إعادة تعيين تكوين الأمان إلى الإعدادات الافتراضية. يحذف هذا الخيار ملف CTL.

الخطوة 4 اضغط على **إعادة تعيين** أو **إلغاء** .

موضوعات ذات صلة

إدخال النصوص والدخول إلى القوائم من الهاتف, في الصفحة 40

إعادة تعيين هاتف المؤتمر إلى إعدادات المصنع الافتراضية من لوحة المفاتيح

عندما تقوم بإعادة تعيين الهاتف من لوحة المفاتيح، يعود الهاتف إلى إعدادات المصنع.

اجراء

الخطوة 1 افصل الهاتف:

- إذا كنت تستخدم PoE، فافصل كبل LAN.
- إذا كنت تستخدم محول الطاقة، فافصله.

الخطوة 2 انتظر 5 ثوان.

الخطوة 3 اضغط مع الاستمرار على # وأعد توصيل الهاتف مرة أخرى.

الخطوة 4 عند إعادة تشغيل الهاتف، يضيء شريط LED. عند إيقاف تشغيل شريط LED، اضغط على **123456789*0#** في التسلسل.

بعد الضغط على هذه الأزرار، يُكمل الهاتف عملية إعادة تعيين إعدادات المصنع.

إذا ضغطت على الأزرار بدون ترتيب، ستجد أن الهاتف يعمل بشكل عادي.

تنبيه لا توقف تشغيل الهاتف حتى يُكمل عملية إعادة تعيين إعدادات المصنع، وتظهر الشاشة الرئيسية.

موضوعات ذات صلة

إدخال النصوص والدخول إلى القوائم من الهاتف, في الصفحة 40

مراقبة جودة الصوت

لقياس جودة صوت المكالمات المرسلة والمستلمة داخل الشبكة، تستخدم هواتف Cisco IP Phone هذه القياسات الإحصائية المستندة إلى أحداث الإخفاء. يعمل DSP على تشغيل إطارات الإخفاء نظرًا لفقدان إطار القناع أثناء تدفق حزمة الصوت.

- قياسات نسبة الإخفاء — تعرض نسبة إطارات الإخفاء عبر إجمالي إطارات الكلام. تُحسب نسبة الإخفاء الفاصلة كل 3 ثوان.
- قياسات الثانية المخفية — تعرض عدد الثواني التي يعمل خلالها DSP على تشغيل إطارات الإخفاء نظرًا لفقدان الإطارات. تُعد "الثانية المخفية بدرجة كبيرة" ثانية يعمل خلالها DSP على تشغيل نسبة تزيد عن خمسة في المئة من إطارات الإخفاء.

ملاحظة تُعد نسبة الإخفاء وثواني الإخفاء قياسين أساسيين يستندان إلى فقدان الإطارات. تشير نسبة الإخفاء بالقيمة صفر إلى أن شبكة IP تعمل على توصيل الإطارات والحزم في الوقت المحدد دون فقدان.

يمكنك الوصول إلى قياسات جودة الصوت من Cisco IP باستخدام شاشة "إحصاءات المكالمة" أو باستخدام "إحصاءات التدفق" عن بُعد.

تلميحات حول استكشاف مشكلات جودة الصوت وإصلاحها

عندما تلاحظ وجود تغييرات كبيرة ومستمرة للقياسات، استخدم الجدول التالي لمعرفة معلومات عامة حول استكشاف المشكلات وإصلاحها.

الجدول *31*: التغييرات التي تحدث لقياسات جودة الصوت

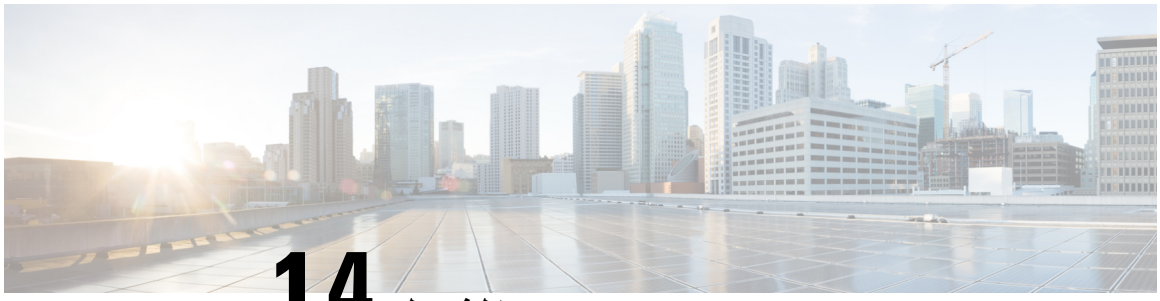
تغيير المقياس	الحالة
تزيد "نسبة الإخفاء" و"ثواني الإخفاء" بشكل كبير	يوجد عيب في الشبكة ناتج عن فقد حزمة أو تشويش بدرجة عالية.
تقترب "نسبة الإخفاء" من القيمة صفر أو تساويها، ولكن جودة الصوت رديئة.	• الضوضاء أو التشويهات الموجودة في قناة الصوت مثل مستويي الصدى والصوت. • المكالمات المترادفة التي تخضع إلى الترميز/فك الترميز المتعدد مثل المكالمات الصادرة إلى شبكة خلوية أو شبكة بطاقة الاتصال. • المشكلات الصوتية الناتجة عن مكبر صوت أو هاتف خلوي بدون استخدام يدوي أو سماعة هاتف لاسلكية. تحقق من عدادي إرسال الحزم (TxCnt) وتلقي الحزم (RxCnt) للتأكد من صحة تدفق حزم الصوت.
تقل درجات MOS LQK بشكل كبير	عيب في الشبكة ناتج عن فقد حزمة أو مستويات تشويش عالية: • قد يشير انخفاض MOS LQK المتوسط إلى وجود عيب واسع النطاق وموحد. • قد تشير معدلات انخفاض MOS LQK إلى وجود عيب متقطع. تحقق من نسبة الإخفاء وثواني الإخفاء بحثًا عن دليل لفقد الحزمة والتشويش.
تزيد درجات MOS LQK بشكل كبير	• تحقق لمعرفة ما إذا كان الهاتف يستخدم ترميزًا مختلفًا عن الترميز المتوقع (RxType وTxType) أم لا. • تحقق لمعرفة ما إذا كان إصدار MOS LQK قد تغير بعد ترقية البرامج الثابتة أم لا.

ملاحظة لا يعتد بقياسات جودة الصوت في تفسير سبب الضوضاء أو التشويه، بل يعتد بها فقط عند فقدان الإطارات.

تنظيف هاتف Cisco IP

لتنظيف هاتف Cisco IP ، لا تستخدم سوى قطعة قماش ناعمة جافة لمسح الهاتف وشاشته برفق. لا تضف أي سوائل أو مساحيق مباشرةً إلى الهاتف. وكما هو الحال مع جميع الإلكترونيات غير المقاومة لأحوال الطقس، قد تؤدي السوائل والمساحيق إلى إتلاف المكونات وتتسبب في حدوث أعطال.

عندما يكون الهاتف في وضع السكون، ستكون الشاشة فارغة وزر التحديد غير مضيء. وعندما يكون الهاتف في هذه الحالة، يمكنك تنظيف الشاشة، ما دامت علي دراية بأن الهاتف سيظل في وضع السكون حتى بعد الانتهاء من التنظيف.



الفصل 14

دعم المستخدمين الدولي

أداة تثبيت الإعدادات المحلية لنقاط نهاية Unified Communications Manager

يتم تعيين هواتف Cisco IP s إلى الإعدادات المحلية للغة الإنجليزية (الولايات المتحدة) بشكل افتراضي. لاستخدام هواتف Cisco IP بإعدادات محلية أخرى، يتعين عليك تثبيت نسخة أداة تثبيت الإعدادات المحلية لنقاط نهاية مدير الاتصال الموحد الخاصة بالإعدادات المحلية على كل خادم Cisco Unified Communications Manager في نظام المجموعة. تثبّت أداة تثبيت الإعدادات المحلية أحدث نص مترجم لواجهة مستخدم الهاتف ونغمات الهاتف الخاصة بالدولة على نظامك حتى تتوفر لهواتف Cisco IP s.

للوصول إلى أداة تثبيت الإعدادات المحلية اللازمة للإصدار، ادخل إلى صفحة تنزيل البرنامج، ثم انتقل إلى طراز هاتفك، وحدد ارتباط أداة تثبيت الإعدادات المحلية لارتباط Unified Communications Manager Endpoints.

للحصول على مزيد من المعلومات، راجع الوثائق الخاصة بإصدار Cisco Unified Communications Manager الذي لديك.S

ملاحظة قد لا تتوفر أداة تثبيت الإعدادات المحلية الأحدث على الفور؛ استمر في البحث عن التحديثات في موقع الويب.

موضوعات ذات صلة

وثائق Cisco Unified Communications Manager, في الصفحة 14

دعم تسجيل المكالمة الدولية

إذا كان نظام الهاتف لديك مهيئًا لتسجيل المكالمة الدولية (تسوية الطرف المتصل)، فقد يتم عرض رمز الجمع (+) ضمن إدخالات سجلات المكالمات أو إعادة الطلب أو دليل المكالمة ليمثل شفرة الإلغاء الدولية لموقعك. استنادًا إلى تهيئة نظام الهاتف لديك، قد يستعاض عن الرمز + بشفرة الطلب الدولية الصحيحة أو قد تحتاج إلى تحرير الرقم قبل الطلب لإبدال الرمز + يدويًا بشفرة الإلغاء الدولية لموقعك. بالإضافة إلى ذلك، ففي حين أن سجل أو دليل المكالمات قد يعرض الرقم الدولي الكامل للمكالمة المستلمة، قد تعرض شاشة الهاتف نسخة محلية مختصرة للرقم، وذلك دون شفرات دولية أو خاصة بالبلدان.

تحديد اللغة

لا يوجد أي دعم للوحات مفاتيح إدخال النص الأبجدية الرقمية (KATE) المترجمة للغات الآسيوية التالية:

- الصينية (الصين)
- الصينية (هونج كونج)
- الصينية (تايوان)
- اليابانية (اليابان)
- الكورية (جمهورية كوريا)

الإعداد الافتراضية لـ KATE هو اللغة الإنجليزية (الولايات المتحدة) ويكون معروضًا للمستخدم بدلاً من ذلك.

على سبيل المثال، ستعرض شاشة الهاتف النص بالكورية، لكن سيعرض مفتاح **2** على لوحة المفاتيح الرقمية **a b c 2 A B C**.