فشل حل إتصالات WebEx عبر الهواتف ذات حماية مستوى الإدارة (MPP) في إعادة التسجيل بعد إعادة ضبط المصنع بسبب الاختلافات الأصلية في طريقة الإلحاق

المحتويات

مسألة

لم تقم هواتف Cisco 8845 و 9871 MPP بإعادة التسجيل تلقائيا إلى الاتصال عبر Webex بعد إعادة ضبط المصنع، وبدلا من ذلك، بقيت في شاشة رمز التنشيط. تتطلب الهواتف المتأثرة الحذف وإعادة البناء في "مركز التحكم" حتى يمكن إدخال رمز تنشيط يدويا لإكمال التسجيل. يتم تسجيل معظم الهواتف الموجودة على نفس الشبكة وشبكة VLAN بشكل طبيعي بعد إعادة ضبط المصنع دون الحاجة إلى التدخل اليدوي.

تؤثر المشكلة على سير عمل توفير الهاتف وتسجيله، مما يتطلب نفقات إدارية إضافية لاستعادة وظائف الهاتف بعد إعادة الضبط في المصنع.

البيئة

- هواتف حماية مستوى الإدارة (MPP) Cisco 8845
- هواتف حماية مستوى الإدارة (MPP) Cisco 9871
- نشر الاتصال عبر Webex
- تم حذف إدخالات خيار DHCP القديم 150 من نشر CUCM السابق
- حوالي 4500 هاتف في البيئة مع تأثر الهواتف المحددة فقط

رارق

تم حل المشكلة عن طريق تغيير طريقة مض الهاتف من رمز التنشيط إلى مض عنوان MAC في "مركز التحكم".

يتم معالجة هذه التحديد في إرتباط "إعادة ضبط المصنع لهاتف Webex CallPhone" المتوفر:

إذا كان الهاتف في الأصل على متن الطائرة باستخدام عنوان MAC الخاص به، فإنه يتصل من جديد بالاتصال عبر Webex. إذا كان الهاتف قد تم تحميله باستخدام رمز تنشيط، فإنه يتطلب رمز تنشيط جديد أو يلزم تضمينه باستخدام عنوان MAC الخاص به لإعادة الاتصال بالاتصال عبر Webex.

التعرف على الهواتف المتأثرة

حدد طريقة الإلحاق المستخدمة للهواتف من خلال فحص ملف status.xml في أداة تقرير المشكلة (PRT):

- تم الحصول عليه بواسطة GDS: يشير إلى وجود GDS (رمز التنشيط) ضمن.
- مكتسب: يشير إلى إدراج EDOS (عنوان MAC) عبر activate.cisco.com.

إعادة إضافة الهواتف باستخدام طريقة عنوان MAC

الخطوة 1: احذف الهاتف المتأثر من لوحة التحكم.

الخطوة 2: أعد إضافة الهاتف باستخدام مض عنوان MAC بدلا من طريقة رمز التنشيط.

الخطوة 3: إجراء إعادة ضبط المصنع على الهاتف.

الخطوة 4: تحقق من تسجيل الهاتف تلقائيا دون الحاجة إلى إدخال رمز التنشيط.

التحقق من الصحة

بعد تنفيذ إدراج عنوان MAC، تمت إعادة تسجيل الهواتف بنجاح بعد إعادة ضبط المصنع دون قيود EDOS مع تدفق البقاء على شاشة رمز التنشيط. تتبع الهواتف الآن عملية توفير EDOS المستند إلى CERT" إلى الداخل بدلا من الحاجة إلى إدخال رمز التنشيط اليدوي.

السبب

السبب الجذري هو الفرق في طرق الإلحاق بين المتأثرين وهواتف العمل. تظهر الهواتف التي تم تحميلها في الأصل باستخدام رموز التنشيط (طريقة GDS) حالة طريقة التوفير "فتح" وتظل في شاشة رمز التنشيط بعد إعادة ضبط المصنع، مما يتطلب إدخال رمز التنشيط اليدوي من خلال عملية تنشيط GDS.

في المقابل، تظهر الهواتف التي تم ضمها في الأصل باستخدام عناوين MAC حالة طريقة التوفير "تم الحصول عليها" وتتابع عملية إدراج EDOS المستندة إلى CERT تلقائيا، مما يسمح بالتسجيل دون تدخل يدوي.

ساهمت إدخالات خيار DHCP 150 القديمة من نشر CUCM سابق في توفير التعقيدات لكنها لم تكن السبب الرئيسي لمتطلبات كود التنشيط.

المحتوى ذي الصلة

- إعادة ضبط هاتف Webex للاتصال عبر Webex في المصنع
- أستكشاف أخطاء هاتف حماية مستوى الإدارة (MPP) وإصلاحها في الاتصال عبر Webex بحثا عن مشاكل تتعلق بالإمداد
- الدعم الفني والتنزيلات من Cisco

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).