إدارة الشهادات المجمعة بين مجموعات CUCM للترحيل عبر الهاتف

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

معلومات أساسية

إجراء إدارة الشهادات المجمعة

تصدير شهادات نظام المجموعة الموحدة

تصدير شهادات نظام المجموعة المصدر

دمج ملفات PKCS12 المصدر والموحدة

استيراد الشهادات إلى مجموعات الموحدة والمصدر

تكوين هاتف نظام المجموعة المصدر باستخدام معلومات خادم TFTP لنظام المجموعة الموحدة

إعادة ضبط هاتف نظام المجموعة المصدر للحصول على ملف ITL/CTL لنظام المجموعة الموحدة لإكمال عملية الترحيل

التحقق من الصحة

استكشاف الأخطاء وإصلاحها

فيديو التكوين

معلومات ذات صلة

المقدمة

يوضح هذا المستند كيفية إدارة الاعتماد المجمع بين مجموعات مدير الاتصالات الموحدة (CUCM) من Cisco لترحيل الهواتف.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:
- خادم بروتوكول نقل الملفات الآمن (SFTP)
- شهادات CUCM

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى CUCM 10.x.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

ملاحظة: ويرد هذا الإجراء أيضا في قسم إدارة الشهادات المجمعة من دليل الإدارة الخاص بإصدار دليل إدارة عمليات حفظ الطبيعة (CUCM) الإصدار 12.5(1)

تسمح إدارة الشهادات المجمعة بمشاركة مجموعة من الشهادات بين مجموعات CUCM. هذه الخطوة هي شرط لوظائف النظام الخاصة بالمجموعات الفردية التي تحتاج إلى الثقة التي سيتم إنشاؤها فيما بينها مثل Extension Mobility Cross Cluster (EMCC)، بالإضافة إلى النقل عبر الهاتف بين المجموعات.

كجزء من الإجراء، يتم إنشاء ملف معايير تشفير المفاتيح العامة #12 (PKCS12) يحتوي على شهادات من جميع العقد في نظام مجموعة. يجب أن يقوم كل نظام مجموعة بتصدير شهادته إلى نفس دليل SFTP على نفس خادم SFTP. يجب إجراء تكوينات إدارة الشهادات المجمعة يدويا على ناشر CUCM لكل من مجموعتي المصدر والوجهة. يجب أن تكون مجموعات المصدر والوجهة نشطة وتشغيلية بحيث يكون للهواتف التي سيتم ترحيلها اتصال بكل من هذه المجموعات. يتم ترحيل هواتف نظام المجموعة المصدر إلى نظام المجموعة الوجهة.

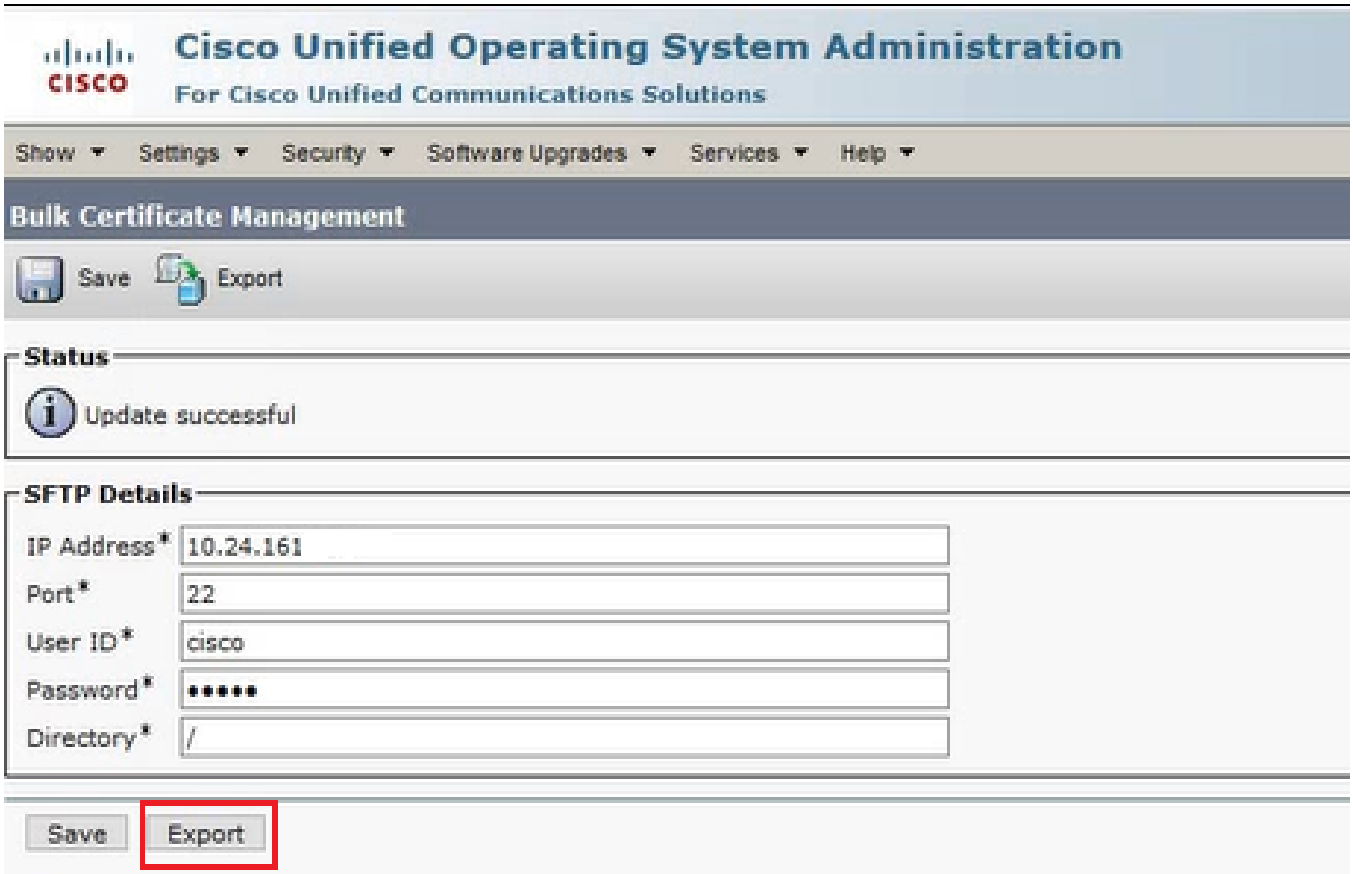
إجراء إدارة الشهادات المجمعة

تصدير شهادات نظام المجموعة الوجهة

الخطوة 1. قم بتكوين خادم SFTP لإدارة الشهادات المجمعة على ناشر CUCM الخاص بمجموعة الوجهة.

في هذا المثال، إصدار CUCM لمجموعة الوجهة هو 11.5.1.

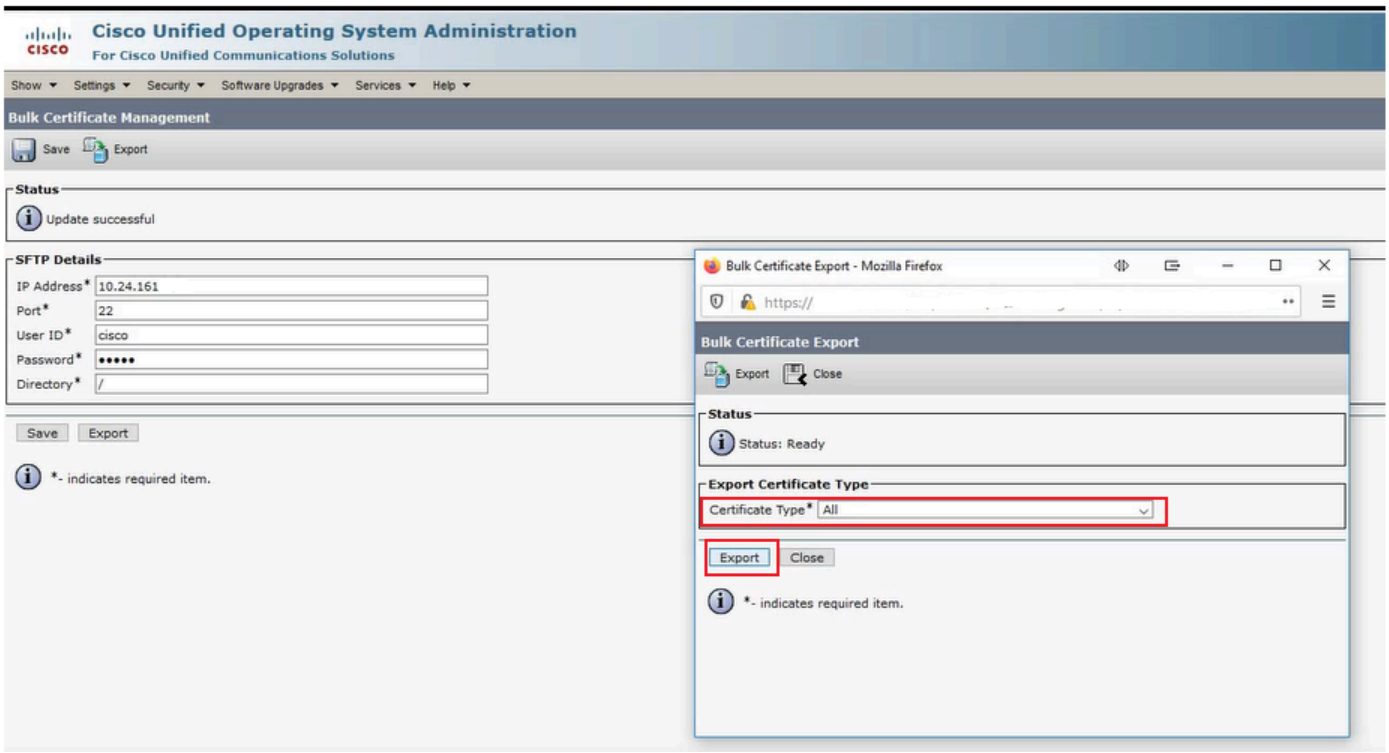
انتقل إلى إدارة نظام التشغيل الموحدة من Cisco > الأمان > إدارة الشهادات المجمعة. أدخل تفاصيل خادم SFTP وانقر فوق تصدير.



أدخل تفاصيل خادم SFTP وانقر فوق تصدير.

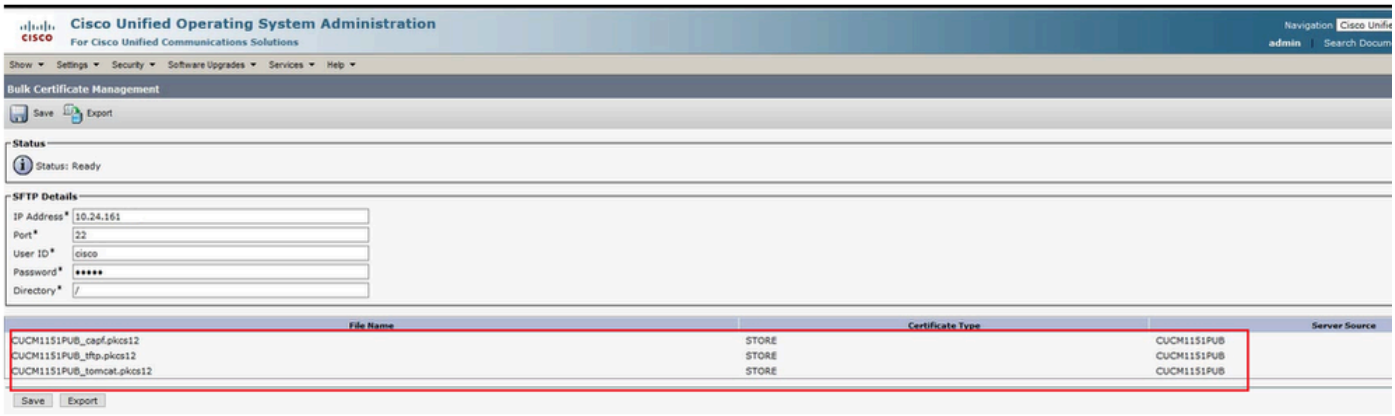
الخطوة 2. تصدير جميع الشهادات من جميع العقد في نظام المجموعة الموجهة إلى خادم SFTP.

في الإطار المنبثق لتصدير الشهادات المجمعة، حدد الكل ل نوع الشهادة ثم انقر على تصدير.



حدد الكل لنوع الشهادة ثم انقر تصدير

قم بإغلاق النافذة وتحديث "إدارة الشهادات المجمعة" باستخدام ملفات PKCS12 التي تم إنشاؤها لكل عقدة من العقد الموجودة في المجموعة الوجهة، حيث يتم تحديث صفحة الويب بهذه المعلومات كما هو موضح في الصورة.



تحديثات إدارة الشهادات المجمعة مع ملفات PKCS12

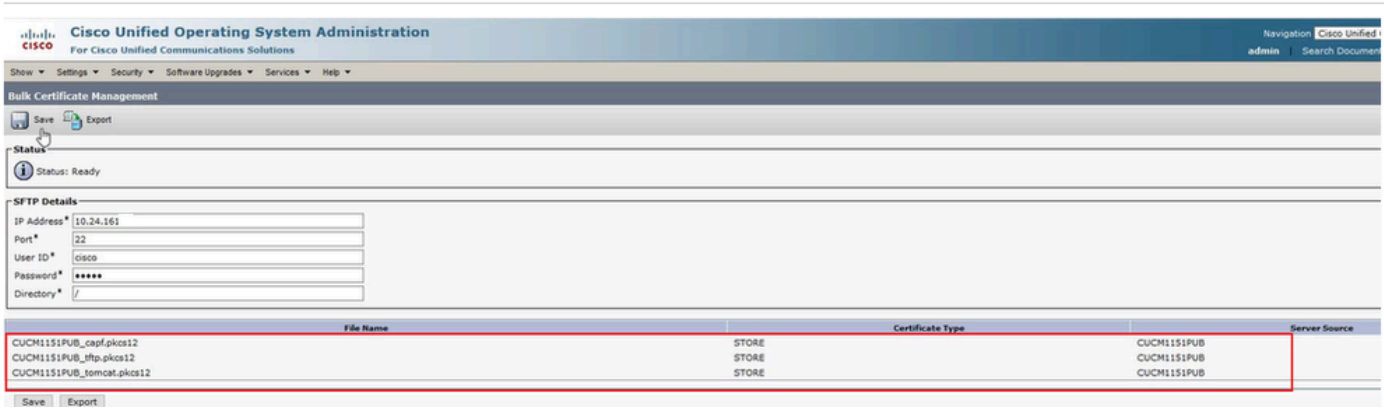
تصدير شهادات نظام المجموعة المصدر

الخطوة 1. قم بتكوين خادم SFTP لإدارة الشهادات المجمعة على ناشر CUCM الخاص بنظام المجموعة المصدر.

في هذا المثال، إصدار CUCM الخاص بنظام المجموعة المصدر هو 10.5.2.

انتقل إلى إدارة نظام التشغيل الموحدة من Cisco > الأمان > إدارة الشهادات المجمعة، وأدخل تفاصيل خادم SFTP وانقر فوق تصدير.

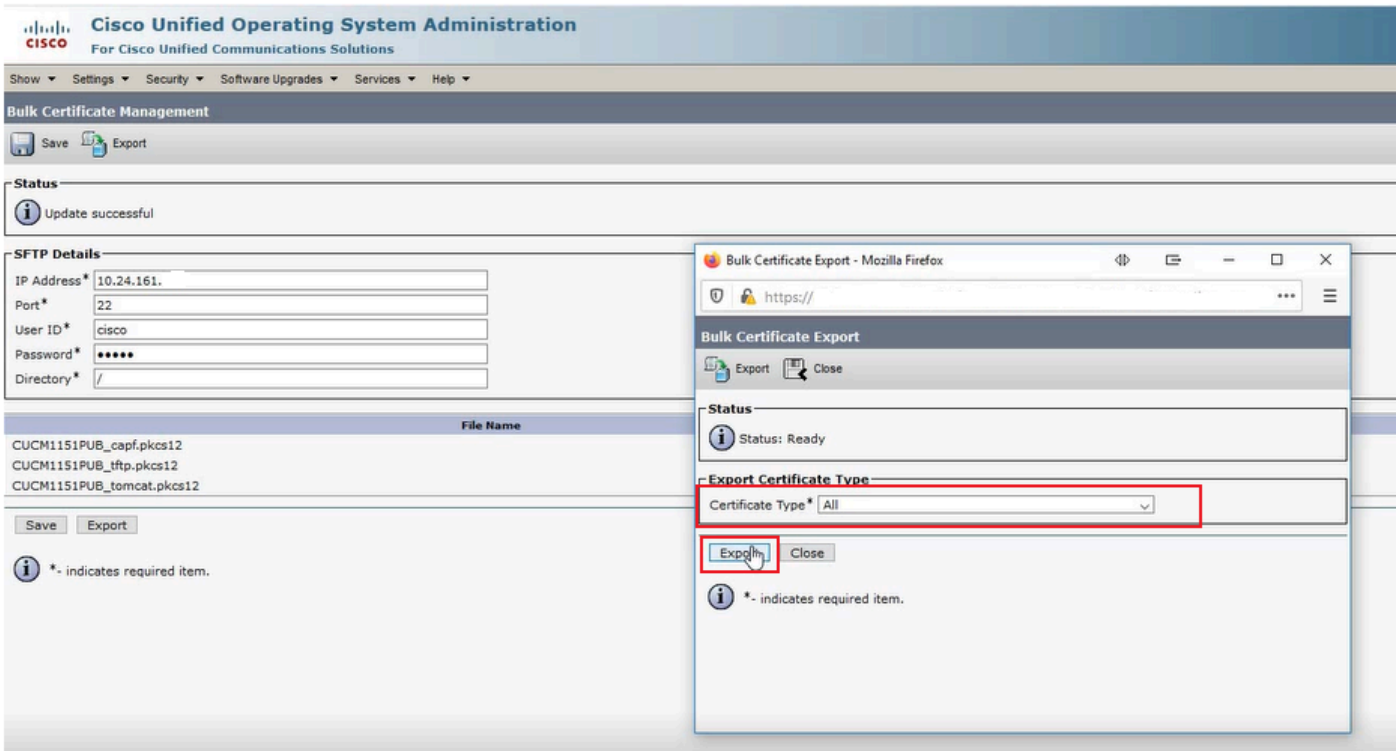
ملاحظة: تظهر ملفات PKCS12 التي تم تصديرها من نظام المجموعة الوجهة إلى خادم SFTP على صفحة الويب المصدر الخاصة بإدارة الشهادات المجمعة لـ CUCM Publisher Bulk Certificate Management عند الوصول إليها.



أدخل تفاصيل خادم SFTP وانقر فوق تصدير

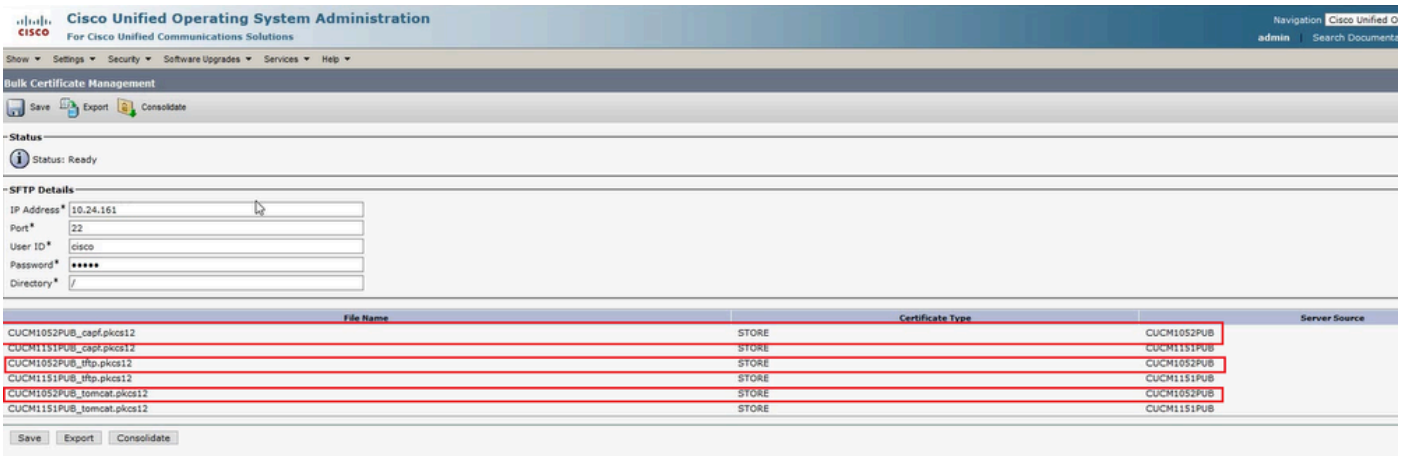
الخطوة 2. تصدير جميع الشهادات من جميع العقد في نظام المجموعة المصدر إلى خادم SFTP.

في الإطار المنبثق لتصدير الشهادات المجمعة، حدد الكل لنوع الشهادة ثم انقر على تصدير:



تصدير نوع الشهادة الكل

انقر فوق إغلاق" لإغلاق هذا الإطار. تقوم "إدارة الشهادات المجمعة" بتحديث ملفات PKCS12 التي تم إنشاؤها لكل عقد في نظام المجموعة المصدر، حيث يتم تحديث صفحة الويب بهذه المعلومات. تعرض صفحة ويب الخاصة بإدارة الشهادات المجمعة الخاصة بنظام المجموعة المصدر الآن كل من ملفات PKCS12 المصدر والوجهة التي تم تصديرها إلى SFTP.

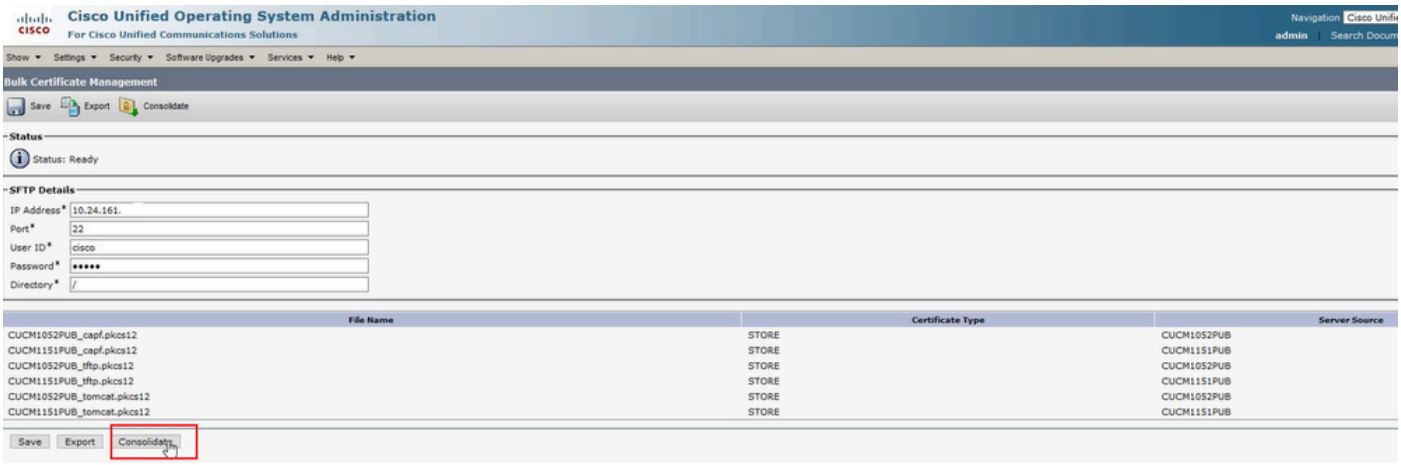


ملفات PKCS12 المصدرة إلى SFTP.

دمج ملفات PKCS12 المصدر والوجهة

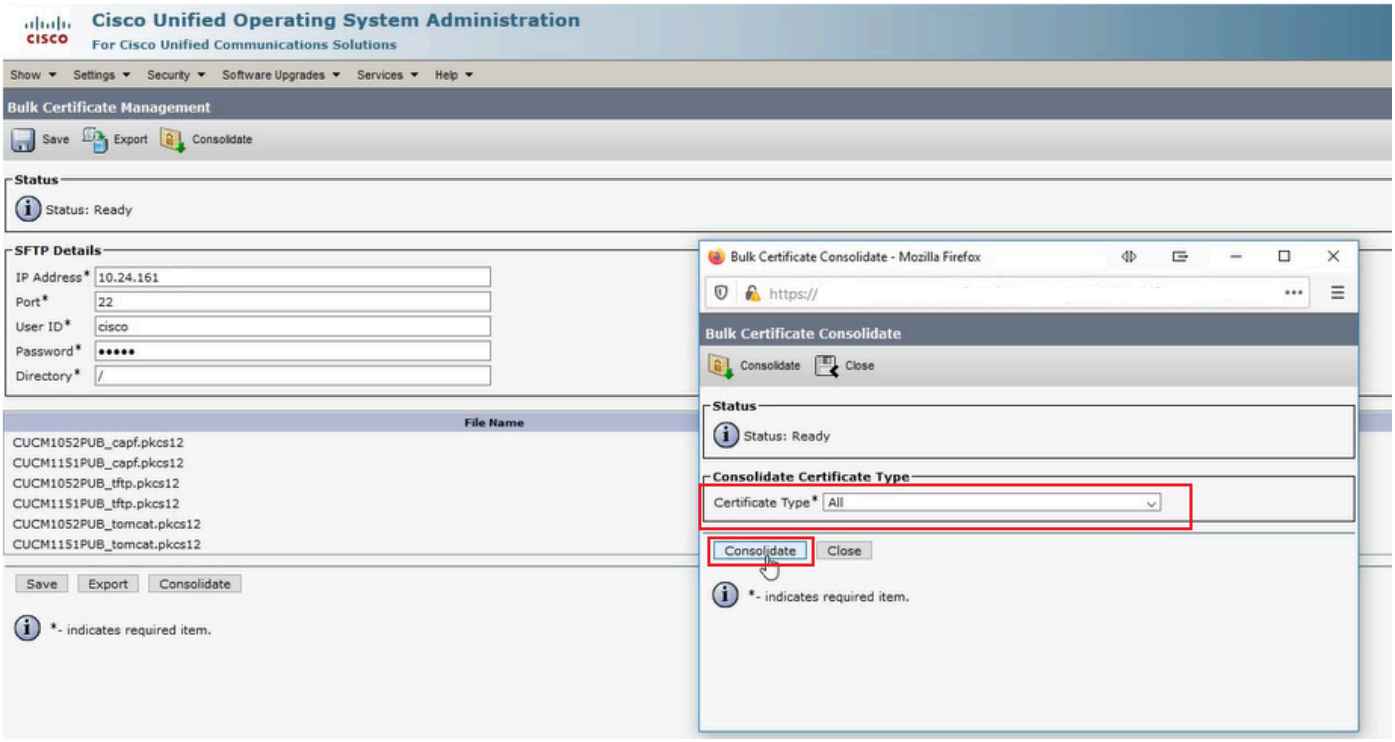
ملاحظة: يتم تصدير "إدارة الشهادات المجمعة" على كل من مجموعات المصدر والوجهة، ويتم الدمج من خلال ناشر CUCM في واحدة فقط من المجموعات.

الخطوة 1. ارجع إلى صفحة إدارة الشهادات المجمعة ل ناشر CUCM نظام المجموعة المصدر وانقر فوق دمج:



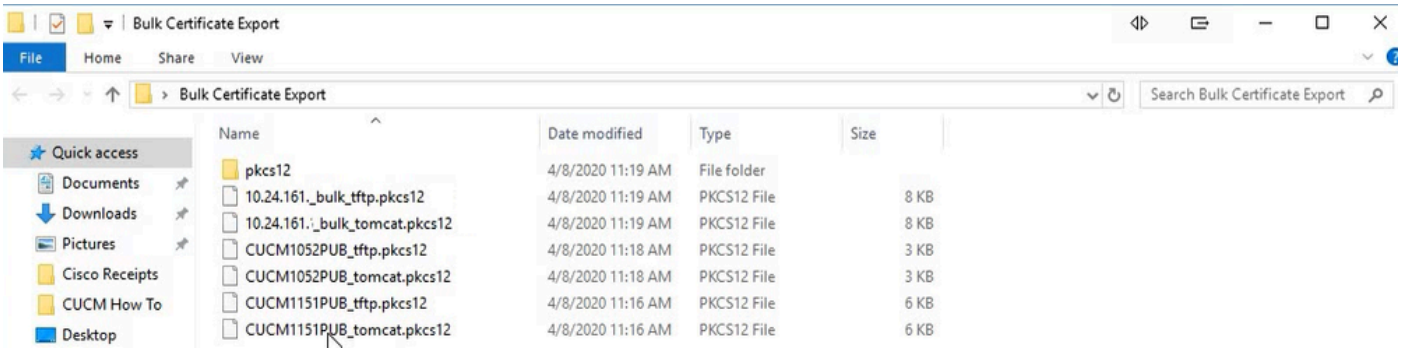
انقر فوق دمج

في الإطار المنبثق الخاص بدمج الشهادات المجمعة، حدد All ل نوع الشهادة ثم انقر فوق دمج. انقر فوق إغلاق لإغلاق هذا الإطار.

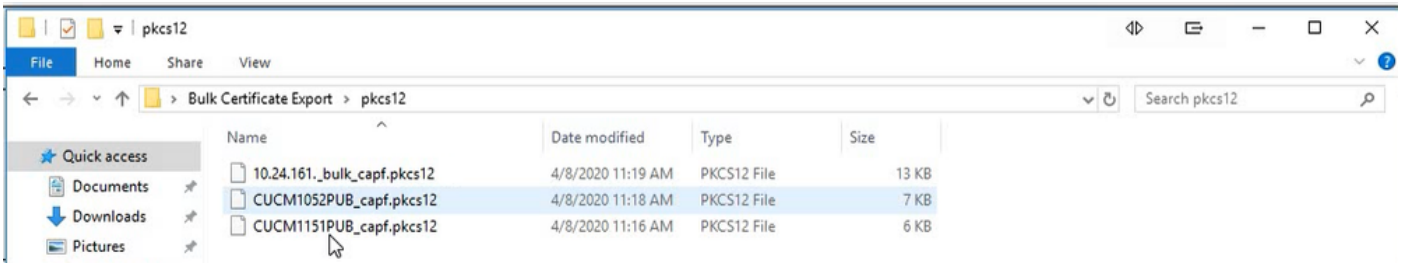


دمج كافة أنواع الشهادات

في أي وقت، يمكنك التحقق من دليل SFTP للتحقق من ملفات PKCS 12 المتضمنة لكل من مجموعات المصدر والوجهة. تم إكمال محتويات دليل SFTP بعد تصدير جميع الشهادات، من كل من مجموعات الوجهة والمصدر. هذا موضح في الصور التالية.



محتويات دليل SFTP بعد تصدير جميع الشهادات

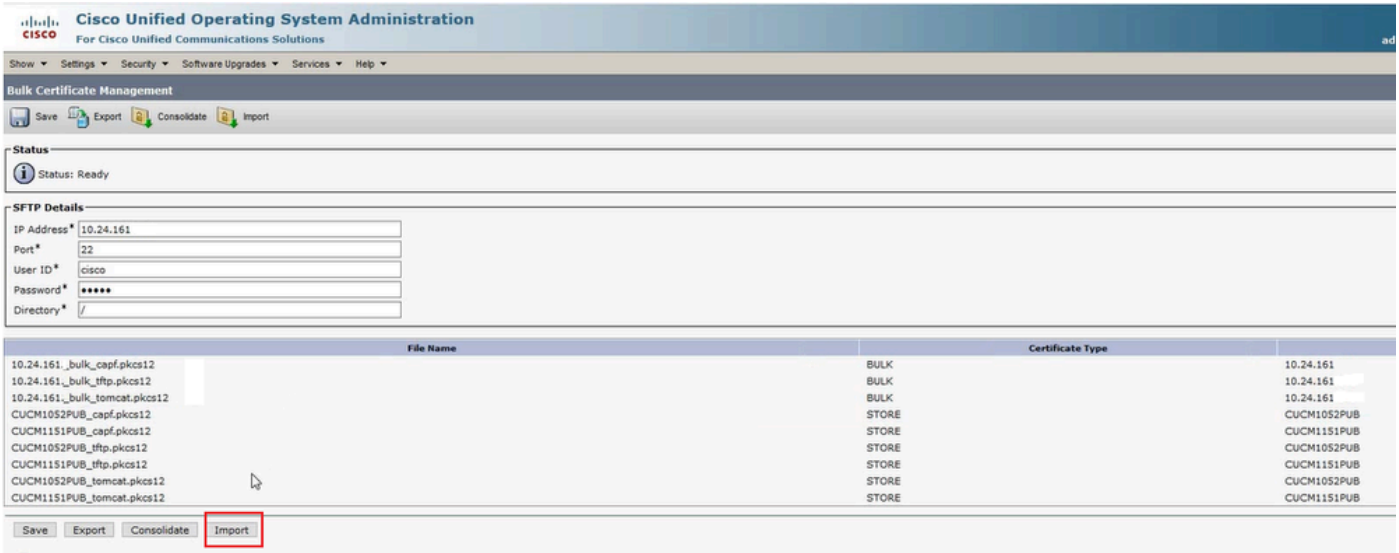


محتويات دليل SFTP

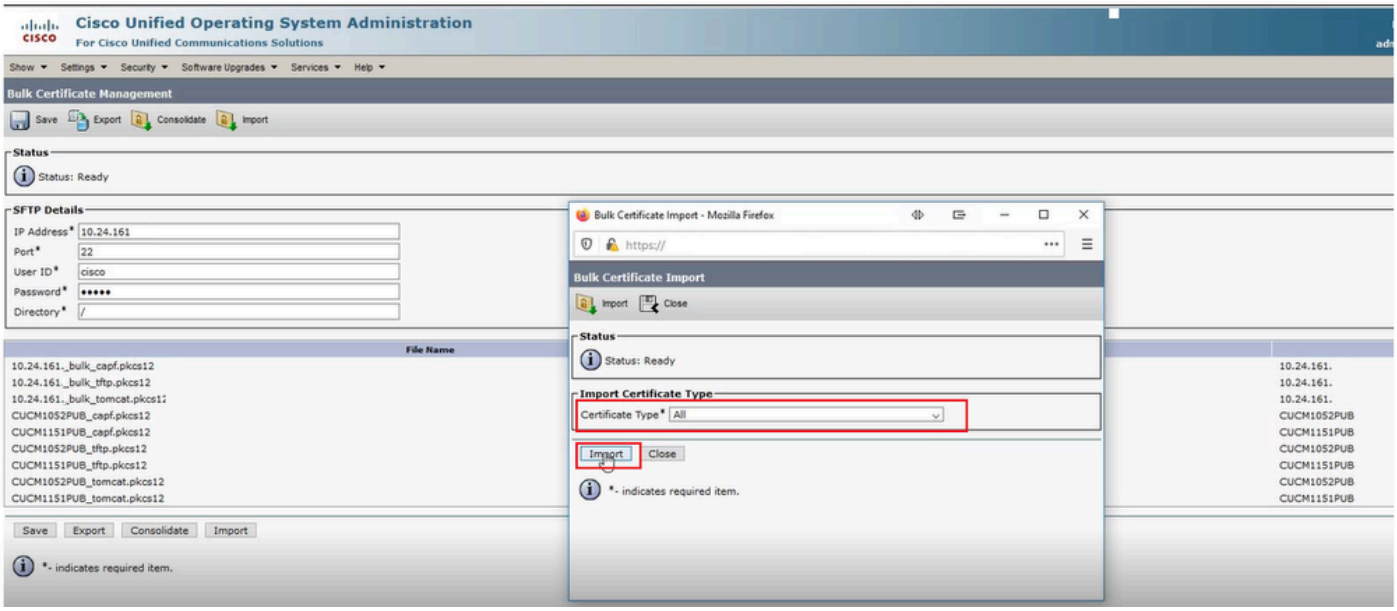
إستيراد الشهادات إلى مجموعات الوجهة والمصدر

الخطوة 1. إستيراد الشهادات إلى مجموعة الوجهة.

في برنامج نشر CUCM الخاص بالمجموعة الوجهة، انتقل إلى إدارة نظام التشغيل الموحد من Cisco > الأمان > إدارة الشهادات المجمعة واترك الصفحة يتم تحديثها، ثم انقر على إستيراد:



في الإطار المنبثق إستيراد الشهادات المجمعة، حدد الكل ل نوع الشهادة ثم انقر على الاستيراد. انقر فوق إغلاق" لإغلاق هذا الإطار.



تحديد الكل ثم الاستيراد

الخطوة 2. كرر الخطوة 1 لنظام المجموعة المصدر.

ملاحظة: عند إجراء إستيراد الشهادات المجمعة، يتم تحميل الشهادات إلى نظام المجموعة البعيد بهذه الطريقة:
- يتم تحميل شهادة "وظيفة وكيل المرجع المصدق" (CAPF) كوضع ثقة CallManager.
- يتم تحميل شهادة Tomcat كوثيقة مراقبة.
- يتم تحميل شهادة CallManager كوثيقة Phone-Ast و CallManager.
- يتم تحميل شهادة إستردادقائمة هوية الثقة (ITLRecovery) كوثيقة Phone-Ast-Trust و CallManager-trust.

تكوين هواتف نظام المجموعة المصدر باستخدام معلومات خادم TFTP لنظام المجموعة الوجهة

قم بتكوين نطاق DHCP لهواتف نظام المجموعة المصدر باستخدام خيار بروتوكول نقل الملفات المبسط (TFTP) 150 للإشارة إلى خوادم نظام المجموعة الوجهة CUCM TFTP.

إعادة ضبط هواتف نظام المجموعة المصدر للحصول على ملف ITL/CTL لنظام المجموعة الوجهة لإكمال عملية الترحيل

كجزء من عملية الترحيل، تحاول هواتف نظام المجموعة المصدر إعداد اتصال آمن بنظام المجموعة المصدر Cisco Trust Verification Service (TVS) للتحقق من صحة نظام المجموعة الوجهة CallManager أو شهادة ITLRecovery.

ملاحظة: يقوم أي من المصدر بتجميع شهادة CallManager من خادم CUCM الذي يشغل خدمة TFTP (المعروفة أيضا بشهادة TFTP) أو شهادة ITLRecovery الخاصة بها بتوقيع مصدر نظام مجموعة مصدر قائمة الشهادات لعقدة CUCM (CTL) و/أو ملف قائمة تأمين الهوية (ITL). وعلى نحو مماثل، إما أن توقع شهادة نظام المجموعة الوجهة CallManager من خادم CUCM الذي يشغل خدمة TFTP أو شهادة ITLRecovery الخاصة بها على CTL و/أو ملف

ملاحظة: عند CUCM يقوم بإنشاء ملفات CTL و ITL على عقدة CUCM لنظام المجموعة الوجهة. يتم تشغيل خدمة TFTP التي تقوم بتشغيل ملف CTL و/أو ITL في حالة عدم التحقق من صحة الهاتف إلى نظام المجموعة الوجهة بواسطة أجهزة التلفزيون المصدر، يفشل ترحيل الهاتف إلى نظام المجموعة الوجهة.

ملاحظة: قبل بدء عملية ترحيل هاتف نظام المجموعة المصدر، تأكد من أن هذه الهواتف تحتوي على ملف CTL و/أو ITL صالح مثبت. تأكد أيضا من أن ميزة المؤسسة إعداد نظام المجموعة للرجوع إلى ما قبل 8.0 تم تعيينه على خطأ لنظام المجموعة المصدر. تحقق بالإضافة إلى ذلك من أن عقد CUCM الخاصة بمجموعة الوجهة التي تقوم بتشغيل خدمة TFTP بها ملفات CTL و/أو ITL صحيحة مثبتة.

هذه هي العملية التي تتم دون تأمين نظام المجموعة للهواتف المصدر للحصول على ملف ITL لنظام المجموعة الوجهة لإكمال ترحيل الهواتف:

الخطوة 1. الا يمكن إستخدام CallManager والشهادة ITLRecovery المضمنة في ملف ITL لنظام المجموعة الوجهة، والتي يتم تقديمها إلى هاتف نظام المجموعة المصدر عند إعادة تعيينه، للتحقق من صحة ملف ITL المثبت حاليا. وهذا يتسبب في قيام هاتف نظام المجموعة المصدر بإنشاء اتصال بأجهزة التلفزيون الخاصة بنظام المجموعة المصدر للتحقق من ملف ITL لنظام المجموعة الوجهة.
الخطوة 2. يثبت الهاتف وجود اتصال بأجهزة التلفاز الخاصة بمجموعة المصدر على منفذ TCP 2445.
الخطوة 3. يقدم نظام المجموعة المصدر TVS شهادته إلى الهاتف. يتحقق الهاتف من صحة الاتصال ويطلب من أجهزة TVS لنظام المجموعة المصدر التحقق من صحة CallManager لنظام المجموعة الوجهة أو شهادة ITLRecovery للسماح للهاتف بتنزيل ملف ITL لنظام المجموعة الوجهة.
الخطوة 4. بعد التحقق من صحة ملف ITL لنظام المجموعة الوجهة وتثبيته، يمكن الآن لهاتف نظام المجموعة المصدر التحقق من صحة ملفات التكوين الموقعة وتنزيلها من نظام المجموعة الوجهة.

هذه هي العملية التي تتم من خلال نظام المجموعة الآمنة للهواتف المصدر للحصول على ملف CTL لنظام المجموعة الوجهة لإكمال عملية ترحيل الهواتف:

الخطوة 1. يجري تمهيد الهاتف ويحاول تنزيل ملف CTL من نظام المجموعة الوجهة.
الخطوة 2. يتم توقيع ملف CTL من قبل نظام المجموعة الوجهة CallManager أو شهادة ITLRecovery التي ليست موجودة في ملف CTL أو ITL الحالي للهاتف.
الخطوة 3. نتيجة لذلك، يتصل الهاتف بالتلفاز في المجموعة المصدر للتحقق من شهادة CallManager أو ITLRovery.

ملاحظة: عند هذه النقطة، الا يزال للهاتف التكوين القديم الخاص به والذي يحتوي على عنوان IP الخاص بخدمة أجهزة التلفزيون الخاصة بمجموعة المصادر. خوادم TVS المحددة في تكوين الهواتف هي نفسها مجموعة CallManager للهواتف.

الخطوة 4. يقوم الهاتف بإعداد اتصال "أمان طبقة النقل" (TLS) بأجهزة التلفزيون في مجموعة المصدر.
الخطوة 5. عندما تقدم المجموعة المصدر TVS شهادتها إلى الهاتف، يتحقق الهاتف من شهادة

TVS هذه مقابل الشهادة في ملف ITL الحالي الخاص بها.
الخطوة 6. إذا كانا متماثلين، تكتمل المصافحة بنجاح.
الخطوة 7. يطلب الهاتف المصدر أن يتحقق نظام المجموعة TVS المصدر من شهادة CallManager أو ITLRecovery من ملف CTL لنظام المجموعة الوجهة.
الخطوة 8. تعثر خدمة TVS المصدر على CallManager أو ITLRecovery لنظام المجموعة الوجهة في مخزن الشهادات الخاص بها، وتتحقق من صحته ويمضي هاتف نظام المجموعة المصدر في التحديث باستخدام ملف CTL لنظام المجموعة الوجهة.
الخطوة 9. يقوم الهاتف المصدر بتنزيل ملف ITL لنظام المجموعة الوجهة الذي تم التحقق من صحته مقابل ملف CTL لنظام المجموعة الوجهة الذي يحتوي عليه الآن. وبما أن ملف CTL الخاص بالهاتف المصدر يحتوي الآن على نظام المجموعة الوجهة CallManager أو شهادة ITLRecovery، يمكن للهاتف المصدر التحقق الآن من شهادة CallManager أو ITLRecovery دون الحاجة إلى الاتصال بأجهزة التلفزيون الخاصة بنظام المجموعة المصدر.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

فيديو التكوين

يوفر هذا الرابط الوصول إلى فيديو يسير في إدارة الشهادات المجمعة بين مجموعات CUCM:

[إدارة الشهادات المجمعة بين مجموعات CUCM]

معلومات ذات صلة

- [إدارة قسم الشهادات المجمعة من دليل الإدارة لـ CUCM الإصدار 12.5(1)]
- [إدارة الشهادات المجمعة بين مجموعات CUCM]
- [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 دائماً إلى المستند الإنجليزي الأصلي (الرابط متوفر).