

ءالمع نيوكت لاثمل SAML SSO نيكمم Jabber

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [التكوين](#)
- [الرسم التخطيطي للشبكة](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)

المقدمة

يصف هذا المستند كيفية تكوين عملاء Cisco Jabber وخوادم البنية الأساسية لـ "لغة تمييز تأكيد الأمان" (SAML) لتسجيل الدخول الأحادي (SSO).

المتطلبات الأساسية

يجب توفير خوادم البنية الأساسية مثل Cisco Unified Communications Manager (CUCM) IM and Presence، و Cisco Unity Connection (UCXN)، و CUCM لمستخدمي Jabber ويجب أن يكون تكوين عميل Jabber الأساسي في موضعه.

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- CUCM IM and Presence، الإصدار 10.5(1) أو إصدار أحدث
- UCXN الإصدار 10.5(1) أو إصدار أحدث
- CUCM 10.5(1) أو إصدار أحدث
- Cisco Jabber Client، الإصدار 10.5

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

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

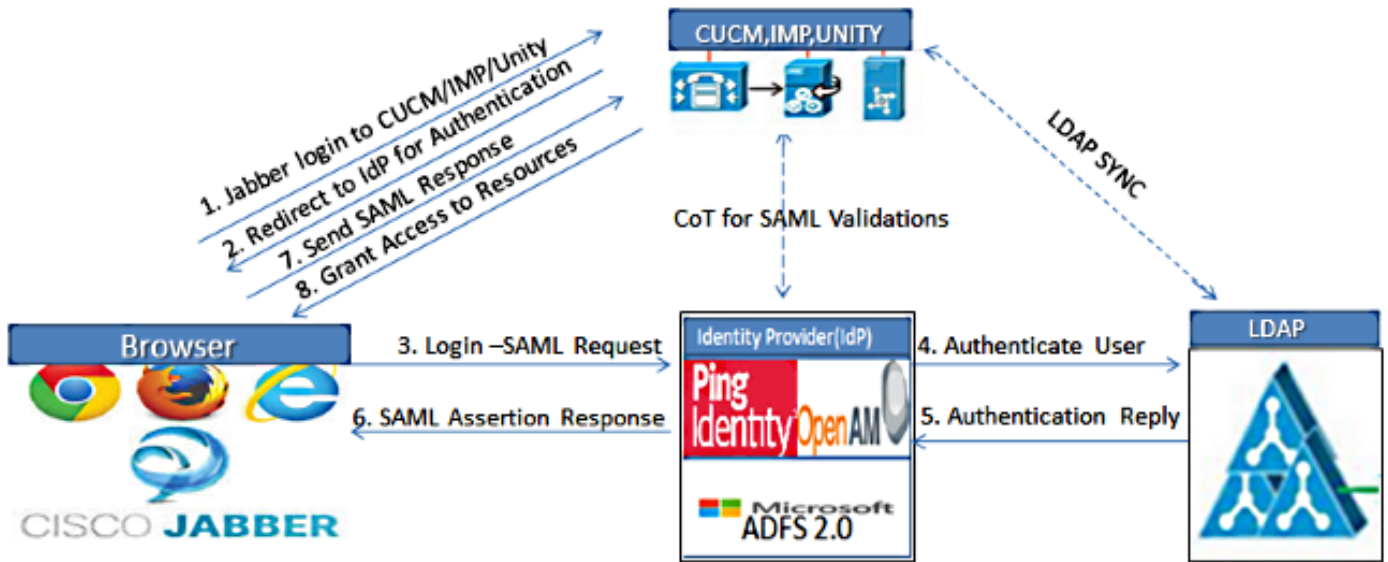


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

قم بنشر الشهادات على كافة الخوادم حتى يمكن التحقق من الشهادة من خلال مستعرض ويب، وإلا فسيتلقى المستخدمون رسائل تحذير حول الشهادات غير الصالحة. للحصول على مزيد من المعلومات حول التحقق من صحة الشهادة، ارجع إلى [التحقق من صحة الشهادة](#).

تأكد من اكتشاف الخدمة ل SAML SSO في العميل. يستخدم العميل ميزة اكتشاف الخدمة القياسية لتمكين SAML SSO في العميل. قم بتمكين اكتشاف الخدمة باستخدام معلمات التكوين التالية: **ServiceDiscoveryExcludedServices**، **VoiceServicesDomain**

لمزيد من المعلومات حول كيفية تمكين اكتشاف الخدمة، ارجع إلى [كيفية تحديد موقع العميل للخدمات](#).

ارجع إلى [مثال تكوين SSO ل Unified Communications Manager الإصدار SAML 10.5](#) لتمكين استخدام Jabber ل SSO لخدمات الهاتف.

ارجع إلى [مثال تكوين SSO ل Unified Communications Manager الإصدار SAML 10.5](#) لتمكين استخدام Jabber ل SSO لإمكانات IM.

ارجع إلى [مثال تكوين SSO للإصدار 10.5 من Unity Connection](#) لتمكين استخدام Jabber ل SSO للبريد الصوتي.

ارجع إلى [إعداد SAML SSO باستخدام مثال تكوين مصادقة Kerberos](#) لتكوين جهاز العميل لتسجيل الدخول التلقائي (Jabber ل Windows فقط)

7. بعد تمكين SSO على CUCM و IMP، يقوم جميع مستخدمي Jabber بتسجيل الدخول بشكل افتراضي باستخدام SSO. يمكن للمسؤولين تغيير هذا الأمر على أساس كل مستخدم بحيث لا يستخدم بعض

المستخدمين SSO ويقومون بدلا من ذلك بتسجيل الدخول باستخدام أسماء مستخدمي Jabber وكلمات المرور الخاصة بهم. من أجل تعطيل SSO لمستخدم Jabber، قم بتعيين قيمة المعلمة SSO_Enabled إلى FALSE.

إذا قمت بتكوين Jabber بحيث لا يطلب من المستخدمين الحصول على عناوين البريد الإلكتروني الخاصة بهم، فقد يكون أول تسجيل دخول لهم إلى Jabber غير SSO. في بعض عمليات النشر، يجب تعيين المعلمة ServicesDomainSsoEmailPrompt على ON. وهذا يضمن أن Jabber لديه المعلومات المطلوبة لتنفيذ تسجيل دخول SSO لأول مرة. إذا قام المستخدمون بتسجيل الدخول إلى Jabber مسبقا، فلن تكون هناك حاجة إلى هذه المطالبة لأن المعلومات المطلوبة متوفرة.

التحقق من الصحة

عند بدء تشغيل Jabber ل Windows، يجب تسجيل الدخول تلقائيا بدون المطالبة بأي بيانات اعتماد أو إدخلات. بالنسبة لعملاء Jabber الآخرين، سيتم مطالبتك بإدخال بيانات الاعتماد مرة واحدة فقط.

استكشاف الأخطاء وإصلاحها

إن يواجه أنت إصدار، يجمع Jabber مشكلة تقرير واتصل cisco مساعدة التقنية مركز (TAC).

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إل دن تسمل