

Permiso SAML SSO para el ejemplo de configuración de los clientes del Jabber

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Verificación](#)

[Troubleshooting](#)

Introducción

Este documento describe cómo configurar a los clientes del Jabber de Cisco y los servidores de la infraestructura para el lenguaje de marcado de la aserción de la Seguridad (SAML) escogen Muestra-en (SSO).

Prerrequisitos

Los servidores de la infraestructura como el administrador de las Comunicaciones unificadas de Cisco (CUCM) IM y presencia, el Cisco Unity Connection (UCXN), y CUCM deben ser aprovisionado para los usuarios del Jabber y la configuración del cliente básica del Jabber debe existir.

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- CUCM IM y versión 10.5(1) o posterior de la presencia
- Versión 10.5(1) o posterior UCXN
- CUCM 10.5(1) o más adelante
- Versión de cliente 10.5 del Jabber de Cisco

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Diagrama de la red

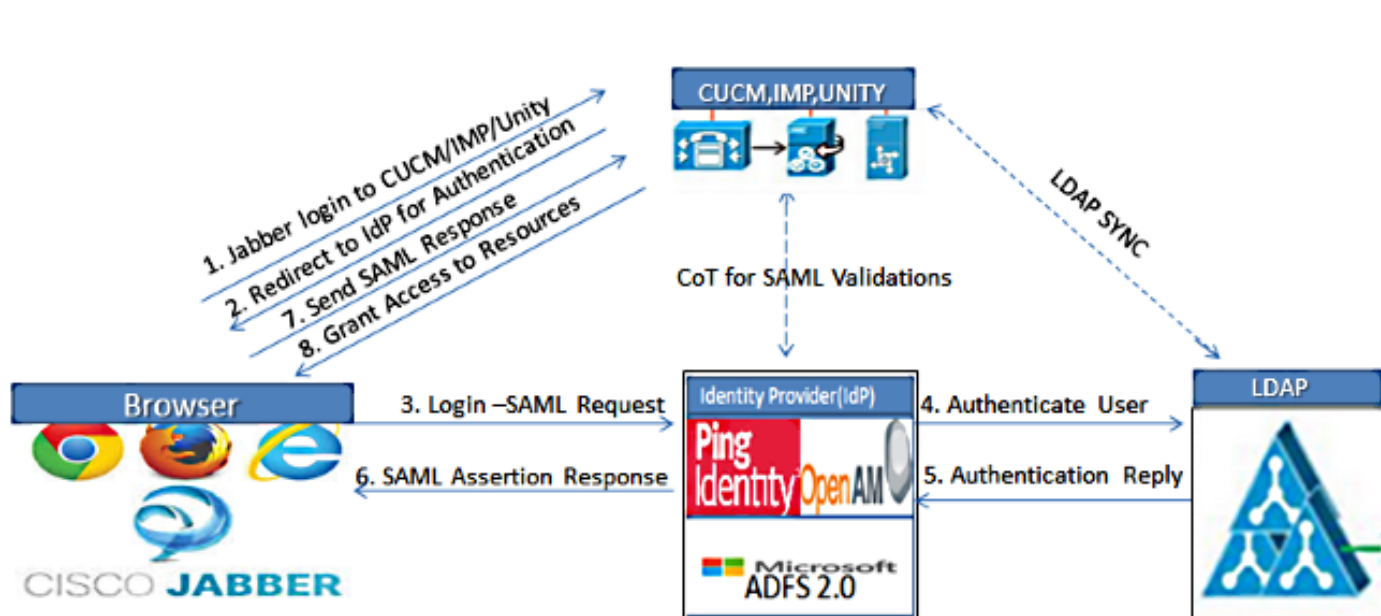


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

1. Despliegue los Certificados en todos los servidores para poder validar el certificado por un buscador Web; si no los usuarios reciben los mensajes de advertencia sobre los Certificados inválidos. Para más información sobre la validación de certificado, refiera a la [validación de certificado](#).
2. Asegure la detección del servicio de SAML SSO en el cliente. El cliente utiliza la detección del servicio estándar para habilitar SAML EL SSO en el cliente. Detección del servicio del permiso con estos parámetros de la configuración: **ServicesDomain**, **VoiceServicesDomain**, y **ServiceDiscoveryExcludedServices**.

Para más información sobre cómo habilitar la detección del servicio, refiérase a [cómo el cliente localiza los servicios](#).

3. Refiera al [ejemplo de configuración de la versión del administrador 10.5 SAML SSO de las Comunicaciones unificadas](#) para habilitar el uso del Jabber del SSO para los servicios telefónicos.
4. Refiera al [ejemplo de configuración de la versión del administrador 10.5 SAML SSO de las Comunicaciones unificadas](#) para habilitar el uso del Jabber del SSO para IM las

capacidades.

5. Refiera al [ejemplo de configuración de la versión 10.5 SAML SSO del Unity Connection](#) para habilitar el uso del Jabber del SSO para el voicemail.
6. Refiera [SAML a la configuración SSO con el ejemplo de configuración de la autenticación de Kerberos](#) para configurar la máquina del cliente para el login automático (el Jabber para Windows solamente)
7. Después de que el SSO se habilite en CUCM y el IMP, por abandono todos los usuarios del Jabber ingresan con el SSO. Los administradores pueden cambiar esto en a por la base del usuario de modo que los ciertos usuarios no utilicen el SSO y en lugar de otro ingresen con sus nombres de usuario y contraseña del Jabber. Para inhabilitar el SSO para un usuario del Jabber, fije el valor del parámetro de SSO_Enabled a **FALSO**.

Si usted ha configurado el Jabber para no pedir a los usuarios sus direcciones de correo electrónico, sus primeros ingresan para farfullar pudieron ser NON-SSO. En algunas implementaciones, el parámetro de ServicesDomainSsoEmailPrompt se debe fijar a **ENCENDIDO**. Esto se asegura de que el Jabber tenga la información requerida para realizar un SSO por primera vez ingrese. Si los usuarios ingresados para farfullar previamente, este prompt no son necesarios porque la Información requerida está disponible.

Verificación

Cuando el Jabber para Windows se comienza, debe iniciar sesión automáticamente sin indicar para cualesquiera credenciales o entrada. Para otros clientes del Jabber, le indicarán para las credenciales solamente una vez.

Troubleshooting

Si usted encuentra un problema, recoja un Centro de Asistencia Técnica de Cisco del informe de problema y del contacto del Jabber (TAC).