# Exemplo de configuração de ativação de SAML SSO para clientes Jabber

## Contents



## Introduction

Este documento descreve como configurar clientes Cisco Jabber e os servidores de infraestrutura para Security Assertion Markup Language (SAML) Single Sign-on (SSO).

## Prerequisites

Servidores de infraestrutura como Cisco Unified Communications Manager (CUCM) IM e Presence, Cisco Unity Connection (UCXN) e CUCM devem ser provisionados para usuários Jabber e a configuração básica do cliente Jabber deve estar em vigor.

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- CUCM IM e Presence versão 10.5(1) ou posterior
- UCXN Versão 10.5(1) ou posterior
- CUCM 10.5(1) ou posterior
- Cisco Jabber Client Versão 10.5

### Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

# Configurar

## Diagrama de Rede

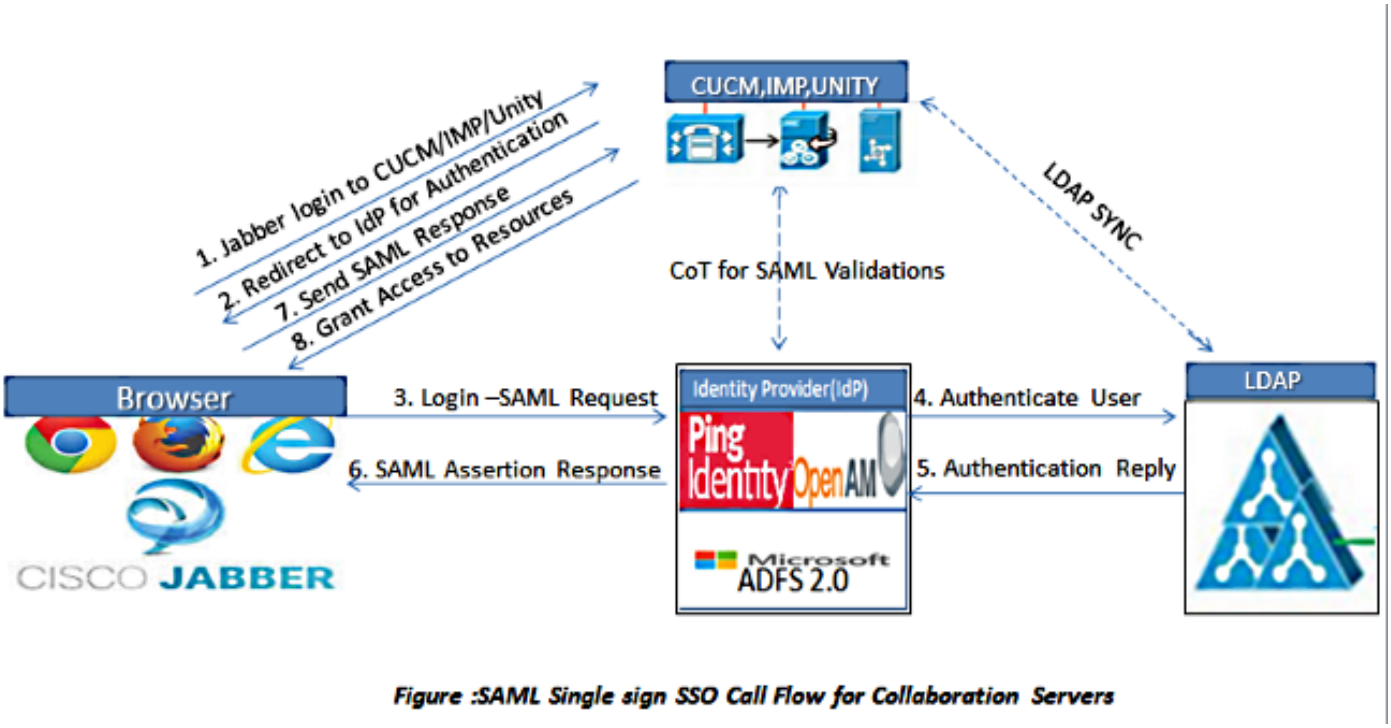


***Figure :SAML Single sign SSO Call Flow for Collaboration Servers***

1. Implantar certificados em todos os servidores para que o certificado possa ser validado por um navegador da Web; caso contrário, os usuários receberão mensagens de aviso sobre certificados inválidos. Para obter mais informações sobre validação de certificado, consulte Validação de Certificado.

2. Assegure a descoberta de serviço do SAML SSO no cliente. O cliente usa a Descoberta de Serviço padrão para habilitar o SAML SSO no cliente.  Habilitar Descoberta de Serviços com estes parâmetros de configuração: **ServicesDomain**, **VoiceServicesDomain** e **ServiceDiscoveryExcludedServices**.

   Para obter mais informações sobre como habilitar a descoberta de serviços, consulte Como o cliente localiza serviços.

3. Consulte Exemplo de Configuração de SSO SAML Versão 10.5 do Unified Communications Manager para habilitar o uso Jabber de SSO para serviços de telefone.

4. Consulte Exemplo de Configuração de SSO SAML do Unified Communications Manager Versão 10.5 para habilitar o uso Jabber de SSO para Recursos IM.

5. Consulte Unity Connection Version 10.5 SAML SSO Configuration Example para habilitar o uso Jabber do SSO para correio de voz.

6. Consulte Exemplo de Configuração de Configuração de SAML SSO com Autenticação Kerberos para configurar a máquina cliente para Logon Automático (somente Jabber para

Windows)

7. Depois que o SSO estiver ativado no CUCM e no IMP, por padrão, todos os usuários Jabber entram com o SSO. Os administradores podem alterar isso em uma base por usuário para que determinados usuários não usem SSO e, em vez disso, entrem com seus nomes de usuário e senhas Jabber. Para desabilitar o SSO para um usuário Jabber, defina o valor do parâmetro SSO_Enabled como **FALSE**.

   Se você configurou o Jabber para não solicitar os endereços de e-mail dos usuários, a primeira entrada deles no Jabber pode ser não SSO. Em algumas implantações, o parâmetro ServicesDomainSsoEmailPrompt deve ser definido como **ON**. Isso garante que o Jabber tenha as informações necessárias para executar uma primeira entrada SSO. Se os usuários entraram no Jabber anteriormente, esse prompt não será necessário porque as informações necessárias estão disponíveis.

# Verificar

Quando o Jabber para Windows é iniciado, ele deve fazer logon automaticamente sem solicitar nenhuma credencial ou entrada. Para outros clientes Jabber, você será solicitado a fornecer credenciais somente uma vez.

# Troubleshoot

Se você encontrar um problema, colete um relatório de problemas do Jabber e entre em contato com o Cisco Technical Assistance Center (TAC).