Enable SAML SSO for Jabber Clients Configuration Example

Document ID: 118774

Contributed by A.M.Mahesh Babu, Cisco TAC Engineer.

Jan 23, 2015

Contents

Introduction

This document describes how to configure Cisco Jabber clients and the Infrastructure servers for Security Assertion Markup Language (SAML) Single Sign−on (SSO).

Prerequisites

Infrastructure servers like Cisco Unified Communications Manager (CUCM) IM and Presence, Cisco Unity Connection (UCXN), and CUCM must be provisioned for Jabber users and the basic Jabber client configuration must be in place.

Requirements

Cisco recommends that you have knowledge of these topics:

- CUCM IM and Presence Version 10.5(1) or later
- UCXN Version 10.5(1) or later
- CUCM 10.5(1) or later
- Cisco Jabber Client Version 10.5

Components Used

This document is not restricted to specific software and hardware versions.

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.

Configure

Network Diagram

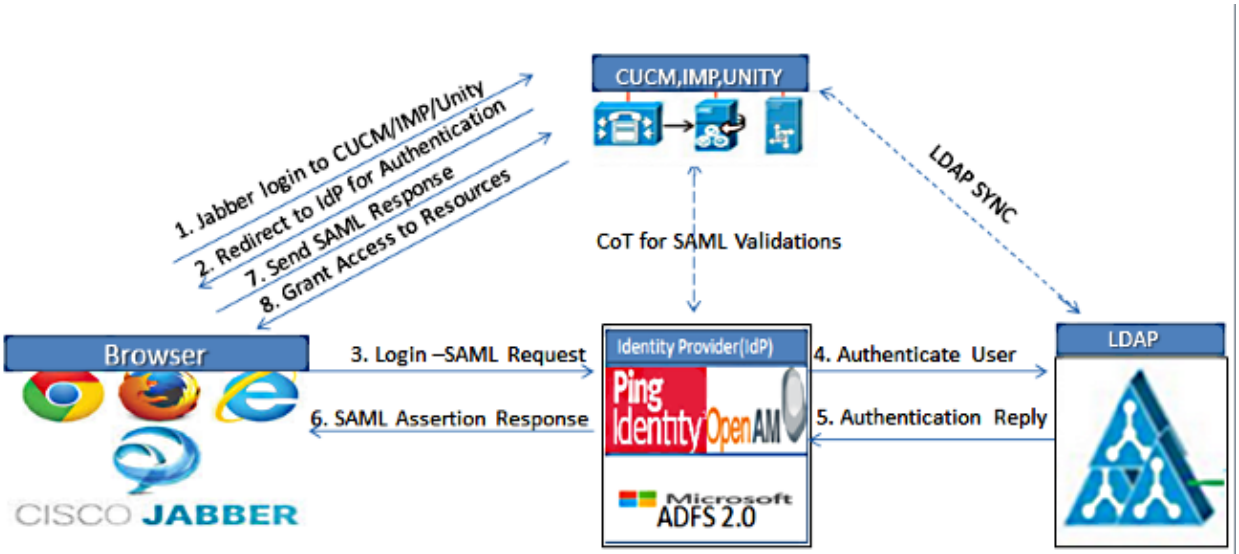

Figure :SAML Single sign SSO Call Flow for Collaboration Servers

1. Deploy certificates on all servers so that the certificate can be validated by a web browser; otherwise users receive warning messages about invalid certificates. For more information about certificate validation, refer to Certificate Validation.

2. Ensure Service Discovery of SAML SSO in the client. The client uses standard Service Discovery in order to enable SAML SSO in the client. Enable Service Discovery with these configuration parameters: ***ServicesDomain***, ***VoiceServicesDomain***, and ***ServiceDiscoveryExcludedServices***.

   For more information about how to enable Service Discovery, refer to How the Client Locates Services.

3. Refer to Unified Communications Manager Version 10.5 SAML SSO Configuration Example in order to enable Jabber use of SSO for Phone services.

4. Refer to Unified Communications Manager Version 10.5 SAML SSO Configuration Example in order to enable Jabber use of SSO for IM Capabilities.

5. Refer to Unity Connection Version 10.5 SAML SSO Configuration Example in order to enable Jabber use of SSO for Voicemail.

6. Refer to SAML SSO Setup with Kerberos Authentication Configuration Example in order to configure the client machine for Automatic Login (Jabber for Windows only)

7. After SSO is enabled on CUCM and IMP, by default all Jabber users sign in with SSO. Administrators can change this on a per user basis so that certain users do not use SSO and instead sign in with their Jabber usernames and passwords. In order to disable SSO for a Jabber user, set the value of the SSO_Enabled parameter to ***FALSE***.

   If you have configured Jabber not to ask users for their email addresses, their first sign in to Jabber might be non−SSO. In some deployments, the ServicesDomainSsoEmailPrompt parameter must be

set to ***ON***. This ensures that Jabber has the information required to perform a first−time SSO sign in. If users signed in to Jabber previously, this prompt is not needed because the required information is available.

Verify

When Jabber for Windows is started, it should automatically log in without prompting for any credentials or inputs. For other Jabber clients, you will be prompted for credentials only once.

Troubleshoot

If you encounter an issue, collect a Jabber Problem report and contact Cisco Technical Assistance Center (TAC).

Updated: Jan 23, 2015 Document ID: 118774