SAML SSO Open Access Manager Identity Provider on Linux Platform Configuration

First Published: Oct 23, 2014
Last Updated: Aug 31, 2017

Introduction

Single sign-on (SSO) is a session or user authentication process that enables a user to provide credentials to access one or more applications. The process authenticates the user for all applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.

This document describes a SAML SSO configuration example. It provides steps used in the Cisco Collaboration Systems test bed to configure Open Access Manager (OpenAM) 10.0.1 as Identity Provider (IdP) on a Linux platform, and integrate OpenAM with Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager IM and Presence Service (IM and Presence Service), Cisco Unity Connection, and Cisco Prime Collaboration Assurance to enable SAML SSO.

For more information about the SAML SSO Solution and generic configuration directions, see: SAML SSO Deployment Guide for Cisco Unified Communications Applications.

Test Bed Details

In the Cisco Collaboration Systems test bed, Unified CM, IM and Presence Service, Cisco Unity Connection, and Cisco Prime Collaboration Assurance servers were configured for SAML SSO for administrator and user accounts to allow users to sign in to any of these servers in the organization without needing to re-enter credentials repeatedly. The test environment had the following characteristics:

- Active Directory was used as the LDAP directory service when importing and authorizing users.
- Users were synchronized from AD using the "sAMAccountName" attribute in Active Directory.
- OpenAM 10.0.1 was set up on a Linux platform to authenticate users through username and password authentication.
- Per node SSO was configured as opposed to cluster wide SSO.
    - **NOTE**: In per node SSO, metadata for each node is imported into the SSO IdP. In cluster wide SSO, introduced in Unified CM 11.5, the administrator configures a multi-server Tomcat certificate on the cluster, and a single metadata file can then be loaded onto the IdP for the entire cluster. For more information, see: Configure Single SAML IdP Connection/Agreement per Cluster with AD FS Version 2.0. Although this document is for AD FS, the process for setting up Unified CM is the same.
- OpenAM was configured with proper data stores to authenticate users using Microsoft AD.
- The OpenAM test certificate was used for signing SAML assertions.

Configuration

This section provides the high-level tasks and related information used to configure the Cisco Collaboration Systems test bed with OpenAM as an Identity Provider on the Linux platform, and to integrate OpenAM with Unified CM, IM and Presence Service, Cisco Unity Connection, or Cisco Prime Assurance to enable SAML SSO.

- Configure User Data Store in OpenAM
- Configure OpenAM as IdP on Linux Platform
- Export Metadata From OpenAM
- Enable SSO on Cisco Unified Communications Applications

Tip: For SAML SSO to work, the Cisco Unified Communications application and the IdP clocks must be synchronized.

Configure User Data Store in OpenAM

In Unified CM, IM and Presence Service, Cisco Unity Connection and Cisco Prime Collaboration deployments, users are added in the LDAP server and are synced to both the Cisco Unified Communications application and the IdP.

Procedure	
Step 1	To configure Active Directory as a Data Store on OpenAM, see the following OpenAM documentation: Add Active Directory as an External Directory.

Configure OpenAM as IdP on Linux Platform

Prerequisites

- Configure an LDAP-synchronized user with administrator privileges on the respective Cisco Unified Communications application server. For more information, refer to "LDAP Integration" in the product documentation. The user synced from Active Directory must have Standard CCM Admin User or Standard CCM Super User access roles assigned.
- Download the SP Metadata XML files for your respective Cisco Unified Communications application servers. Download a .zip file with an SP XML file for each node in the cluster.
    - **Unified CM and IM and Presence Service**: Using a web browser, sign in to Unified CM as administrator, navigate to **System > SAML Single Sign On**, and click **Export all Metadata**.
    - **Cisco Unity Connection**: Using a web browser, sign in to Cisco Unity Connection as administrator, navigate to **System Settings > SAML Single Sign On**, and click **Export all Metadata**.
    - **Cisco Prime Collaboration Assurance**: Using a web browser, sign in to Prime Collaboration Assurance as globaladmin, navigate to **Administration > System Setup > Single Sign On**, and click **Export all Metadata**.
- Use the XML files contained in this .zip in the following Step 4.

Procedure	
Step 1	Access OpenAM for the first time using the FQDN of OpenAM server in the URL (For example, https://openamtest.samlsso.com:8443/opensso. The URL required here varies based on your specific OpenAM installation).
Step 2	When you access OpenAM SSO Enterprise for the first time, you are directed to the Configurator to perform the OpenAM SSO Enterprise initial configuration.

Procedure	
Step 3	Select **Default Configuration**. **Note:** During this step, you are asked to configure the passwords for OpenAM server, configure the passwords and sign-in to OpenAM server user interface.
Step 4	Navigate to **Federation** tab and click **New** in the Circle of Trust section.
Step 5	Create a circle of trust by giving a unique name for the IdP circle of trust.
Step 6	Go to **Common Tasks** tab and click **Create hosted Identity Provider** and create a hosted IdP (keep the default values and save the settings). **Note:** You can see the Circle of Trust created in the previous steps listed in the **Circle of Trust** section.
Step 7	In **Federation** tab, click **hosted Identity Provider** added under **Entity Providers** section. Navigate to **Assertion Content** section and configure **Signing** field value as **test** in the **Certificate Aliases** section. **Test** is a self-signed certificate installed on OpenAM for test and proof-of-concept purposes. **Note:** This is needed for signing SAML assertions with some aliases.
Step 8	In **Federation** tab, click **Import Entity** under **Entity Providers** section, upload the Cisco Unified Communications application metadata file (the .xml file), and **Save** the page. **Note:** Cisco Unified Communications applications support metadata upload only through the file option. Select **File** option during entity provider upload.
Step 9	Click the imported entity and go to **Assertion Processing** section. Add a mapping attribute for **uid** as per the directory and OpenAM settings (for example: uid=sAMAccountName or uid=mail). **Note:** **uid** is a mandatory attribute that has to be configured on the IdP for a given service provider. This is how service provider identifies the identity of authenticated user.
Step 10	In **Federation** tab, click **Circle of Trust** and make sure that you move the IdP (OpenAM server) and Cisco Unified Communications application entities from **Available** to **Selected** sections in the **Entity Providers** section. This assigns IdP and Cisco Unified Communications application to be in the same Circle of Trust.
Step 11	Repeat steps 8-10 for every Cisco Unified Communications application node in the cluster if using per node SSO. If using cluster wide SSO, importing a single entity is all that is required. See the **Test Bed Details** topic in this document for more details about per node SSO and cluster wide SSO.

Tip: For large deployments, change OpenAM maximum sessions to 100000.

In the OpenAM server user interface, select Configuration > Servers and Sites > Default Server Settings> Session and under Session Limits change Maximum Sessions to 100000.

Export Metadata from OpenAM

When you enable SSO on the Cisco application server, you are asked to provide the IdP's metadata file.

Procedure

Procedure	
Step 1	To export the IdP metadata file from OpenAM for use when enabling SSO on the Cisco Unified Communications application, visit this link: https://<IdP_FQDN>:8443/<IdP-uri>/saml2/jsp/exportmetadata.jsp?entityid=https://<IdP_FQDN>:8443/<IdP-uri>&realm=/<realm-name For example: https://openamidp.test.lab:8443/opensso/saml2/jsp/exportmetadata.jsp?entityid=https://openamidp.test.lab:8443/opensso&realm=/

Enable SSO on Cisco Unified Communications Applications

When you have configured the IdP appropriately, enable SSO.

Procedure	
Step 1	Navigate to the following page for each application: ■ **Unified CM and IM and Presence Service**: Using a web browser, sign in to Unified CM as administrator, navigate to **System > SAML Single Sign On**. ■ **Cisco Unity Connection**: Using a web browser, sign in to Cisco Unity Connection as administrator, navigate to **System Settings > SAML Single Sign On**. ■ **Cisco Prime Collaboration Assurance**: Using a web browser, sign in to Prime Collaboration Assurance as globaladmin, navigate to **Administration > System Setup > Single Sign On**.
Step 2	Click **Enable SAML SSO** and follow the steps. **Note:** As of Unified CM 11.5, the administrator can either configure per node SSO or cluster wide SSO. See the **Test Bed Details** topic in this document for more details. When asked to supply the IdP's metadata file, use the file obtained in the **Export Metadata from OpenAM** procedure. When prompted to download the Cisco application's SP metadata file, download the file and click **Next**. These files have already been loaded into the IdP in the **Configure OpenAM as IdP on Linux Platform** procedure.

Related Documentation

- Release Notes for Cisco Unified Communications Manager Release 10.5(1)
- Quick Start Guide for the Cisco Unity Connection SAML SSO Release 10.5(1)
- SAML SSO Deployment Guide for Cisco Unified Communications Applications, Release 10.5

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.