SAML SSO PingFederate Identity Provider on Windows 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 rights to and eliminates further prompts when they switch applications during a particular session.

This document is a SAML SSO configuration example. It provides the steps used in the Cisco Collaboration Systems test bed to configure PingFederate 6.10.04 as Identity Provider (IdP) on a Windows platform, and to integrate PingFederate with Cisco Unified Communications Manager (Unified CM), Unified CM IM and Presence Service, Cisco Unity Connection, and Cisco Prime Collaboration Assurance.

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. SAML SSO allows 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 (AD) was used as the LDAP directory service when importing and authorizing users.
- Users were synchronized from AD using the "sAMAccountName" attribute in Active Directory.
- PingFederate 6.10.04 was set up 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.
- PingFederate was configured with proper adapters and data stores to authenticate users using Microsoft AD.
- PingFederate was configured to send claims with no encryption.
- PingFederate was configured to use digital signatures.

Configuration

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

- Configure Active Directory Integration on PingFederate
- Configure Cisco Unified Communications Applications as SAML Service Providers on PingFederate
- Export Metadata File From PingFederate
- 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 Active Directory Integration on PingFederate

Use this procedure to allow PingFederate to access the AD Data Store.

Procedure		More Information
Step 1	Configure a new Data Store which uses an LDAP connection to sync users with PingFederate.	Configuring an LDAP Connection
Step 2	Configure an LDAP Username/Password Credential Validator, which authorizes user sign-ins against Active Directory. When prompted, select the LDAP Data Store created in Step 1.	Configuring the LDAP Credential Validator
Step 3	Create a new Adapter Instance. When prompted, select the Credential Validator created in Step 2.	HTML Form Adapter Configuration

Configure Cisco Unified Communications Applications as SAML Service Providers on PingFederate

Use this procedure to configure SAML SSO for Unified Communications applications such as Unified CM, IM and Presence Service, Cisco Unity Connection, and Cisco Prime Collaboration Assurance.

Note: Repeat these steps for every Cisco Unified Communications application node in your deployment.

Prerequisites

- Configure an LDAP-synchronized user with administrator privileges on the respective Cisco Unified Communications application server. For further 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. As of Unified CM 11.5, the administrator can configure either per node SSO, or cluster wide SSO. See the Test Bed Details topic for more details. 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	From **SP Connections**, click **Create new**.
Step 2	From the **Connection Type** screen, check the **Browser SSO Profiles** check box and click **Next**.
Step 3	From the **Connection Options** screen, check the **Browser SSO** check box and click **Next**.
Step 4	From the **Import Metadata** screen, browse to the **XML metadata** file for the Cisco Unified Communications application node.
Step 5	When the upload is complete, click **Next**.
Step 6	From the **Metadata Summary** screen, verify that the metadata file indicates **unsigned**, and click **Next**.
Step 7	From the General Info screen, verify Partner's Entity ID, Connection Name, and Base URL, and click **Next**. The fields should look similar to the following. Partner's Entity ID (Connection ID) **<CUCM IP/FQDN>** Connection Name **<CUCM IP/FQDN>** BaseURL **https: //<CUCM IP/FQDN>:8443** Logging Mode **Standard**
Step 8	From the Browser SSO screen, click **Configure Browser SSO**.
Step 9	From the SAML Profiles screen, locate **Single Sign-On (SSO) Profiles**, check the **SP-Initiated SSO** check box and click **Next**.
Step 10	From the Assertion Lifetime screen, enter the time (in minutes) for SSO assertion validity and click **Next**. **Note:** Default for **Minutes Before/Minutes After** is 5 minutes.
Step 11	From the **Assertion Creation** screen, click **Configure Assertion Creation**.
Step 12	From the **Identity Mapping** screen, click the **Transient** radio button, check the **Include attributes in addition to the transient identifier** check box, and click **Next**.
Step 13	In the Extend the Contract field, enter **uid** and from the Attribute Name Format drop-down list, choose **urn:oasis:names:tc:SAML:2.0:attrname-format:uri**. Click **Add** and then click **Next**.
Step 14	From the **IdP Adapter Mapping** screen, click **Map New Adapter Instance**. From the **Configuring Active Directory Integration** section, choose the latest adapter instance and click **Next**.
Step 15	From the **Assertion Mapping** screen, click the **Retrieve additional attributes from multiple datastores using one mapping** radio button, and click **Next**.

Procedure	
Step 16	From the **Attribute Sources & User Lookup** screen, click **Add Attribute Source**, enter a value for Source Id and Source Description (Use **LDAPSource**) and from the **Configuring Active Directory Integration** section, choose the latest Data Store. Click **Next**.
Step 17	From the LDAP Directory Search, search for **Base DN** to get user attributes, choose the appropriate **Search Scope** for your LDAP deployment. Choose <**Show All Attributes**>in **Root Object Class**. In Attribute, choose the LDAP attribute which your Cisco Unified application users are synced with (For example, sAMAccountName or mail). Click **Add Attribute** and click **Next**.
Step 18	From LDAP Filter, specify how PingFederate should query the directory to find a match. Click Next, review the **Attribute Source Summary** screen, and click **Done**. **Note:** For example, if users use email address to authorize PingFederate, enter "${username}=mail". If users use only account name to authorize PingFederate, enter "${username}=sAMAccountName". The filter does not need to be the same as the selected attribute in the previous step.
Step 19	Go to the **Attribute Sources & User Lookup** page. Click **Next**.
Step 20	From the **Attribute Contract Fulfillment** screen, ensure that the fields match the following, and then click **Next**. **Attribute Contract** uid **Source** LDAP **Value** sAMAccountName **Note:** Match the uid value with the LDAP attribute that your Cisco Unified Communications application uses to sync users.
Step 21	Review the summary and click **Done**.
Step 22	Click the **IdP Adapter Mapping** tab. Click **Next**, review the configuration summary, and click **Done**.
Step 23	Click the **Assertion Creation** tab. Click **Next**.
Step 24	From the **Protocol Settings** screen, click **Configure Protocol Settings**. Verify that there is one default entry with values similar to the following and then click **Next**. **Binding** POST **Endpoint URL** /ssosp/saml/SSO/alias/<CUCM-IP or FQDN>
Step 25	From the **Allowable SAML Bindings** screen, check all check boxes except Artifact. Click **Done**.
Step 26	Click the **Protocol Settings** tab. Verify the following fields and then click **Done**. **Outbound SSO Bindings** POST **Inbound Bindings** POST, Redirect **Signature Policy** SAML-standard, Authn requests over POST & Redirect **Encryption Policy** No Encryption
Step 27	Click the **Browser SSO** tab and click **Next**.

Procedure	
Step 28	From the **Credentials** screen, click **Configure Credentials**.
Step 29	From the **Back-Channel Authentication** screen, click **Configure**.
Step 30	Check only **Use Digital Signatures to guarantee payload in Browser SSO profile**, click **Next,** and then click **Done**.
Step 31	From the Back Channel Authentication page, click **Next**.
Step 32	From the Digital Signatures Settings screen, choose the signing certificate to use when sending SAML assertions and then click **Next**. For example: **Signing Certificate** 01:3F:76:CA:57:4b (cn=ping-idp.test.lab) **Signing Algorithm** RSA SHA1
Step 33	From the **Signature Verification Settings** screen, click **Manage Signature Verification Settings** and click **Summary**. This information is already populated from the metadata upload. For example: **Trust Model** Unanchored **Selected certificate** <Subject CN of your Unified Communications application>
Step 34	Click **Done**.
Step 35	From the **Signature Verification Settings** screen, click **Done**.
Step 36	From the **Credentials** screen, review the configuration summary and click **Next**.
Step 37	From the **Activation & Summary** screen, select **Active**.
Step 38	From the **Summary** screen, review the information and click **Save**.
Step 39	From the **My IdP Configuration** screen, verify that the SP connection appears in **SP Connections**.
Step 40	Repeat steps 1-21 for each metadata file downloaded from the Unified CM cluster if using per node SSO. If using cluster wide SSO, a single SP Connection is all that is required. See the Test Bed Details section for more details.

Export Metadata File from PingFederate

When you enable SSO on the Cisco application server, you are asked to provide the IdP's metadata file. Use the following procedure to export the metadata file from PingFederate.

Procedure	
Step 1	In Administrative Functions on the PingFederate administrative Main Menu, click **Metadata Export**, click **Select information to include in metadata manually**, and **click** Next.
Step 2	Verify that **SAML 2.0** appears in Protocol and click **Next**.
Step 3	In **Attribute Contract**, click **Next**.

Procedure	
Step 4	From the **Signing Key** drop-down list, choose the signing certificate that PingFederate uses when sending SAML assertions (for example, 01:3F:76:CA:57:4b (cn=ping-idp.test.lab). Click **Next**.
Step 5	Choose the same signing certificate as in the previous step in **Metadata Signing** and **XML Encryption Certificate**. Click **Next**.
Step 6	Review the **Summary** information. To download the metadata.xml file, click **Export**. **Note:** The metadata.xml file uploads to the Cisco Unified Communications application during SSO configuration.

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 configure either 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 File from Ping Federate 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 Cisco Unified Communications Applications as SAML Service Providers on PingFederate 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.

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.