SAML SSO Microsoft Active Directory Federation Services 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 permits 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 describes a SAML SSO configuration example. It provides the steps used in the Cisco Collaboration Systems test bed to configure Microsoft Active Directory Federation Services (AD FS) 2.0 (Roll-up 3) as Identity Provider (IdP) on a Windows platform, and to integrate AD FS with Cisco Unified Communications Manager (Unified CM).

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.
- AD FS 2.0 (Roll-up 3) was set up to authenticate users through username and password authentication.
- Per node SSO was configured as opposed to cluster-wide SSO.
    - 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.

Configuration

This section provides the high-level tasks and related information used to configure the Cisco Collaboration Systems test bed with AD FS 2.0 (Roll-up 3) as an Identity Provider, and to integrate AD FS with Unified CM, IM and Presence Service, Cisco Unity Connection, and Cisco Prime Collaboration Assurance to use SAML SSO.

- Export Metadata from AD FS
- Configure a Relying Party Trust for SSO
- Enable SSO on Unified Communications Applications

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

Tip: Microsoft AD FS prior to Rollup 3 cannot create multiple relying party trusts for SPs that use the same certificate. If using per node SSO with Multi-SAN certificates with AD FS, install AD FS Roll-up 3 and follow the directions to relax the certificate check policy. Refer to "Issue 3" under the "More Information" section of Description of Update Rollup 3 for Active Directory Federation Services (AD FS) 2.0.

Export Metadata from AD FS

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

Procedure	
Step 1	To export the IdP metadata file from AD FS for use on the Cisco Unified Communications applications, go to this link: https: //<IdP_FQDN>/FederationMetadata/2007-06/FederationMetadata.xml

Configure a Relying Party Trust for SSO

You must create a relying party trust on AD FS for every node in your deployment that you wish to enable SSO access on. Therefore, repeat the prerequisites and steps 1 to 21 for each node.

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 end 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 in this document 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	Choose Start > Programs > AD FS 2.0.
Step 2	Select Add Relying Party Trust.
Step 3	From Add Relying Party Trust Wizard Welcome page, click Start.
Step 4	From the Select Data Source screen, click the Import data about the relying party from a file radio button and browse to the Fedlet metadata XML file, which you downloaded from the SAML single sign-on configuration pages. Click Next.
Step 5	From the Specify Display Name screen, enter a name in the Display name field. Click Next.
Step 6	If you want all users to have access to the SMAL agreement, from the Choose Issuance Authorization Rules screen, choose Permit All Users to access this relying party. Click Next.
Step 7	Review the settings on the Ready to Add trust screen. Click Next.
Step 8	To add the Claim Rules, from the Finish screen, check the Open the Edit Claim Rules dialog for this relying party trust when the wizard closes check box. Click Close.
Step 9	From the Edit Claim Rules screen, click Add Rule.
Step 10	Select the default Claim Rule template Send LDAP Attributes as Claims. Click Next.
Step 11	From the Configure Claim Rule screen, enter a claim rule name (Example: "Send uid attribute") in the Configure rule name field.
Step 12	From the Attribute store drop-down list, choose Active Directory.
Step 13	From the LDAP Attribute drop-down list, choose the attribute in the directory that the Cisco Unified Communications application users are synchronized with (typically "SAM-Account-Name" or "E-Mail-Addresses").
Step 14	From the Outgoing Claim Type drop-down list, enter "uid". Note: "uid" does not appear in the list of drop-down items, you must manually enter it.
Step 15	Click Finish.
Step 16	To add a second rule, click Add Rule.
Step 17	From the Claim rule template drop-down list, select Send Claims Using a Custom Rule.
Step 18	In the Claim rule name field, enter a name (Example: "Send more attributes").

Configuration

<table>
<tr><th colspan="2">Procedure</th></tr>
<tr><td><b>Step 19</b></td><td>In the custom rule text box, enter the following. Change the [ADFS entity ID] and [Cisco Unified Communications application entity ID].
<pre>
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] =>
issue(Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer =
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"
] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient”,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequa
lifier"] = "[ADFS entity ID]”,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnameq
ualifier"] = “[Cisco Unified Communications application entity ID]");
</pre>
ADFS entity ID should match the "entityID" attribute given in the AD FS FederationMetadata.xml file, which you uploaded to the Unified Communications application. Open the XML file with a text editor and search for "entityID" to locate the attribute.

Cisco Unified Communications application entity ID should match the "entityID" attribute given in the Unified CM SP metadata XML file. In a “single SAML connection agreement” configuration (available in Unified CM 11.5+), there is only one Unified CM SP metadata file for the entire cluster. If Unified CM is not configured for a single connection agreement, there will be a metadata file for each Unified CM node in the cluster.</td></tr>
<tr><td><b>Step 20</b></td><td>Click OK.</td></tr>
<tr><td><b>Step 21</b></td><td>Click Apply.</td></tr>
<tr><td><b>Step 22</b></td><td>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 Relying Party Trust 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.</td></tr>
</table>

Tip: This Tip applies only to Unified CM 11.0(1a)SU1, 10.5(2)SU2, 10.5(2)SU1, 10.5(1)SU1, and 10.5(1). For SAML SSO to work on a Federal Information Processing Standard (FIPS) enabled Unified CM integrated with AD FS as the IdP, you must disable encryption on AD FS. To disable encryption, on the AD FS 2.0 computer, choose Start > Administrative Tools > Windows PowerShell Modules. From the Windows PowerShell command prompt, enter: Add-PsSnapIn Microsoft.Adfs.Powershell. Enter: set-ADFSRelyingPartyTrust -TargetName "RELYING PARTY NAME" -EncryptClaims $False. Enter the Display Name of your relying party trust in AD FS in place of "NAM Example".

Enable SSO on Unified Communications Applications

When you have configured the IdP appropriately for every node in the cluster, follow these steps to 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 prompted to supply the IdP's metadata file, use the file obtained in the Export Metadata from ADFS procedure. When prompted to download the Cisco Unified Communications application's SP Metadata File, download the file and click Next. (These files have already been loaded into the IdP in the Configure a Relying Party Trust for SSO 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)