SAML-Based SLO

Support for SAML-Based Single Logout (SLO)

Unified CM supports SAML-based Single Logout (SLO). The SLO allows you to log out simultaneously from all sessions of a browser that you have signed in using Single Sign-on (SSO).

Cisco Tomcat and Cisco SSOSP Tomcat services must be restarted if you are altering the IdP metadata and using root access to replace the idp.xml on the server. You need not restart any services if you are configuring SLO while enabling SSO. Also, if you are altering the IdP metadata and using update IdP metadata option on SAML SSO page to replace the idp.xml on server.

SLO does not close all the running sessions at the same time. For example, if there are four sessions running in two different browsers, the sessions associated with the browser that initiates the log out is closed. The sessions that are associated with the other browser are still open.

The following IdPs (Identity Providers) support Single Logout:

- OpenAM 10.0.1
- F5 BIG-IP 11.6.0
- Okta 2017.38
- Microsoft Active Directory Federation Services idPs 2.0 (AD FS 2.0). To Log out using Microsoft Active Directory Federation Services idPs 2.0, configure the logout URL in the idp.xml file.

Note The PingFederate 6.10.0.4 IdP does not support Single Logout.

For more information on sample IdPs configuration on SLO, see Configuration Examples and TechNotes.

Example Configuration of SAML-Based Single Logout with ADFS 2.0

Unified Communications Manager supports SAML-based Single Logout (SLO). The SLO allows you to log out simultaneously from all sessions of a browser that you have signed in using Single Sign-on (SSO). SLO does not close all the running sessions at the same time.

Attention This procedure is only an example configuration using Microsoft ADFS 2.0. We strongly recommend that you refer to your IdP documentation for official documentation in case they are any new IdP configuration changes or enhancements.

If SAML SSO mode is enabled with Microsoft ADFS 2.0 configuration on your system, then after a successful upgrade to Unified CM Release 14 or above, ensure that you perform the following procedure:

Step 1 For configuration at the Microsoft ADFS 2.0 side, ensure the following points:

a) Select **Relying Party Trust**. From the **Properties**, select **Endpoints**.
b) Select **Add SAML**.
c) Choose SAML Logout as **Endpoint** and Binding as **Post**.
d) Configure the URL `<url>/adfs/ls/?wa=wsignout1.0`.
e) Select **Save** and **Restart** ADFS 2.0 service.

Step 2 To log out using Microsoft ADFS 2.0, configure the logout URL in the *idp.xml* file. Follow the mentioned steps on your product server:

a) Search for **Location** in <SingleLogoutService> tag of *idp.xml* file.
b) Update the URL as `<url>/adfs/ls/?wa=wsignout1.0`.

Step 3 From the SAML Single Sign-On page, click **Update IdP Metadata File** to reimport the updated IdP metadata on Unified Communications Manager server.

Step 4 Click **Run SSO Test**.

After successful authentication, the following message is displayed:

```
SSO Metadata Test Succeesful
```

Step 5 Click **Finish** to complete the SAML SSO setup.

This step completes enabling SSO on all the servers in this cluster and all the web applications participating in SAML SSO are restarted. It may take one to two minutes for the web applications to restart.