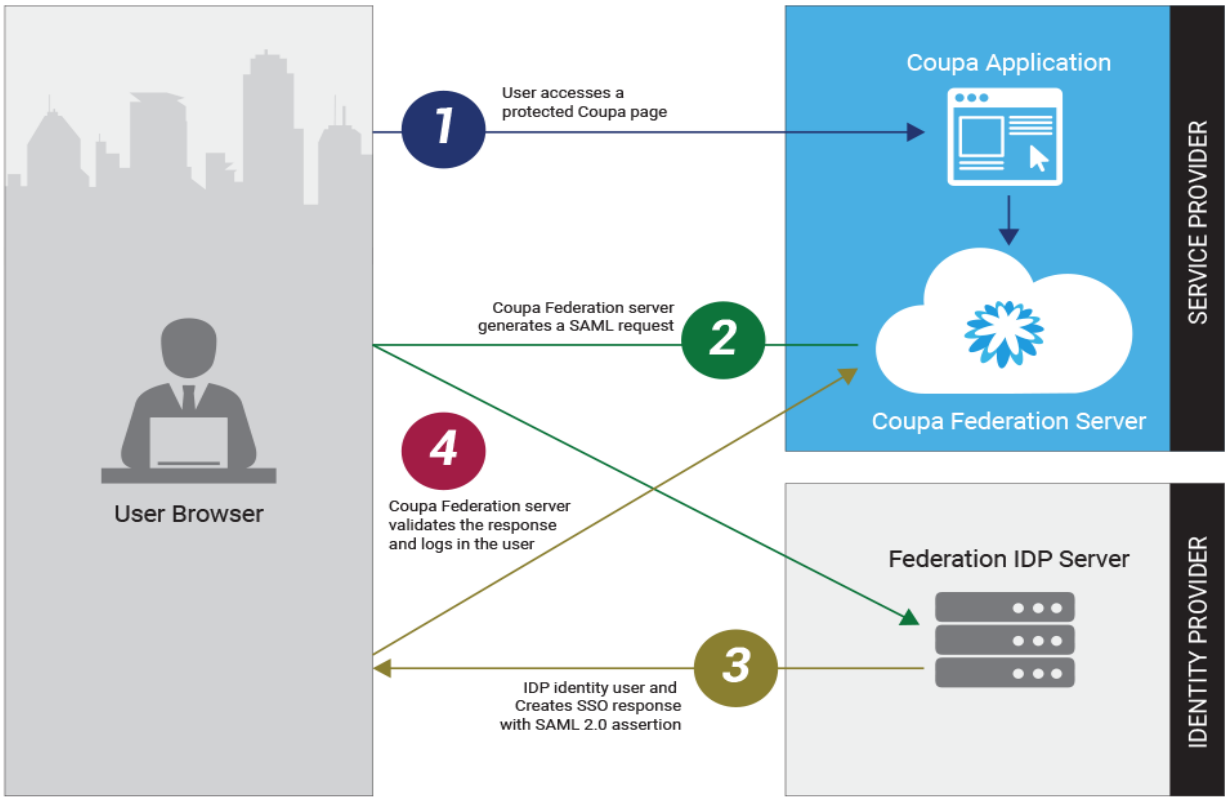
Identity Management

Single sign-on (SSO) is a property of access control that allows end users to log in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords. Similarly, it is a property by which a single action of signing out terminates access to multiple systems. SSO is very helpful to most organizations and is easy to implement and use. Implementing SSO allows to reduce password fatigue from different username and password combinations, reduce time spent re-entering passwords for the same identity and also reduce IT costs due to lower number of IT help desk calls about passwords in general.

In this certification guide we will focus on SSO using SAML. Security Assertion Markup Language (SAML) is an XML based solution for exchanging user security information between an enterprise and a service provider.

Business Process Overview

Coupa supports the use of SAML 2.0 (Security Assertion Markup Language) for SSO (Single Sign On) support between Coupa and your Identity Management platform. This allows the user to click on a link to Coupa and automatically be logged in, if they were already logged in to your SSO.



1. User visits a webpage on their Coupa instance
2. Coupa redirects user to the Identity Provider's Federation server for authentication
3. The Identity Provider returns a webpage directing user's browser to post the SAML response to a Coupa-provided URL
4. Coupa verifies the response. Upon success, the authenticated user will not be required to re-authenticate with the Identity Provider until the session times out. The session timeout can be configured by an administrator

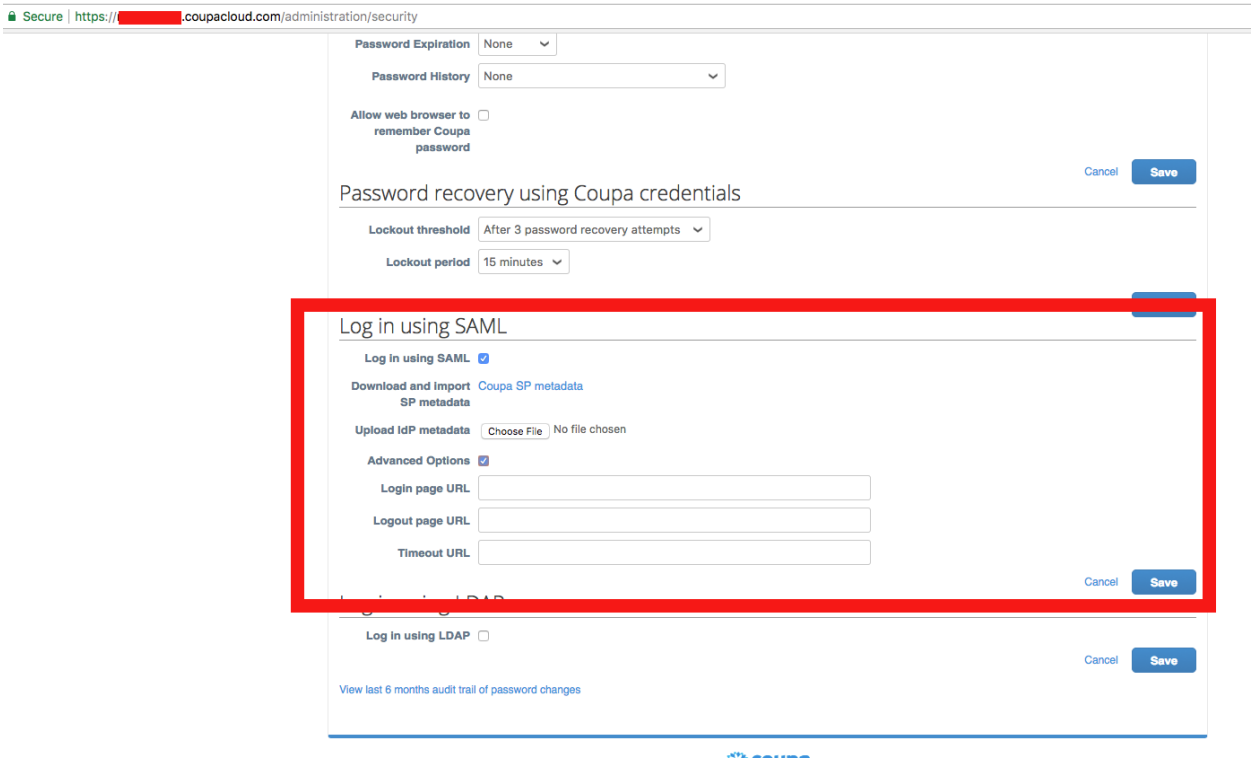
Designing the Solution

As an Identity provider, as long as you support SAML 2.0 protocol, you should be able to provide configure SSO into Coupa.
SAML 2.0 specifications: http://saml.xml.org/saml-specifications

Below are the steps to setup SSO with Coupa

1. Go to your demo Coupa instance - https://<your_site>.coupacloud.com/administration/security.
2. Select the "**Log in using SAML**" checkbox.
3. Import initial the Coupa SP metadata file into your IdP server.
    - If your IDP server does not support Metadata exchange, please open the xml file to extract the information.
    - Coupa's preferred setup is SP-Init-SSO. Coupa can also setup IdP-Init-SSO, IdP-Init-SSO requires your IdP to send the **RelayState** parameter along with SAML request. One way to do this is to add a QueryString to AssertionConsumerService in the xml ..../sp/ACS.saml2?RelayState=https://<coupa-instance-domain-name>/sessions/saml_post. You can change the xml before creating connection.
    - Complete the connection setup at your IdP server.
4. Send the following information to Coupa:
    - Metadata: The export of the metadata xml from your IdP server
        - If your IdP does not support Metadata exchange, please provide Entity ID (a.k.a Connection ID) and X509 Certificate to verify digital signature in SAML response.
    - Login URL: The IdP login page for the user. Required for IdP Initiated SSO.
    - Logout URL: The page Coupa will display when user logout from Coupa application and their session are cleared. This can be internal page, home page or any landing page hosted by the end customer.
    - Test User: Create a test user on your IdP to test the connection.

5. Upload the IdP metadata and complete the connection from SP to IdP.



6. In your demo Coupa instance, enable users to use SAML.
   - Change user settings to enable SAML authentication
   - Set "Single Sign-On ID", this is same as NameID passed in SAML request to Coupa.

Testing the integration

- Configure a new user with SSO. Make sure the user is not logged into SSO. Have the user access the Coupa instance. Validate that user is directed to log into the configured SSO site.
- After the user logs into SSO site, have the user access other pages within the Coupa application. Validate that the user is not directed to login again.
- Have the user logout of the SSO site. Then have the user access a Coupa page. Validate that the user is directed to login to SSO.