Overview of User Login Single Sign-On (SSO) Authentication

The PPM Pro Single Sign-On (SSO) capability is focused on a standards-based framework based on the Security Assertion Markup Language (SAML) 2.0 protocol to integrate with SSO Identity Providers (IdP's).

About Security Assertion Markup Language (SAML)

Security Assertion Markup Language (SAML) is an XML-based open standard for exchanging authentication and authorization data between security domains, that is, between an Identity Provider (a producer of assertions) and a Service Provider (a consumer of assertions). SAML is a product of the OASIS Security Services Technical Committee[1].

SAML assumes the principal (often a user) has enrolled with at least one identity provider. This identity provider is expected to provide local authentication services to the principal. However, SAML does not specify the implementation of these local services; indeed, SAML does not care how local authentication services are implemented.

For each SSO integration, there are certain metadata fields from the IdP that PPM Pro requires to facilitate the authentication. As each Identity Provider has its own way of extracting the metadata, further instructions on how to extract them will be provided to your organization once it is determined who the IdP is or will be.

[1] Wikipedia: "Security Assertion Markup Language "http://en.wikipedia.org/wiki/Security_Assertion_Markup_Language July 9, 2013.

Requirements:

The minimum requirements are:

1. SAML 2.0 protocol
2. HTTP-Redirect Binding
3. Secure HTTP (HTTPS)
4. IdP assertion must pass the PPM Pro login (userid) in the NameId attribute (e-mail address is strongly recommended)

Below are the fields that are generally required:

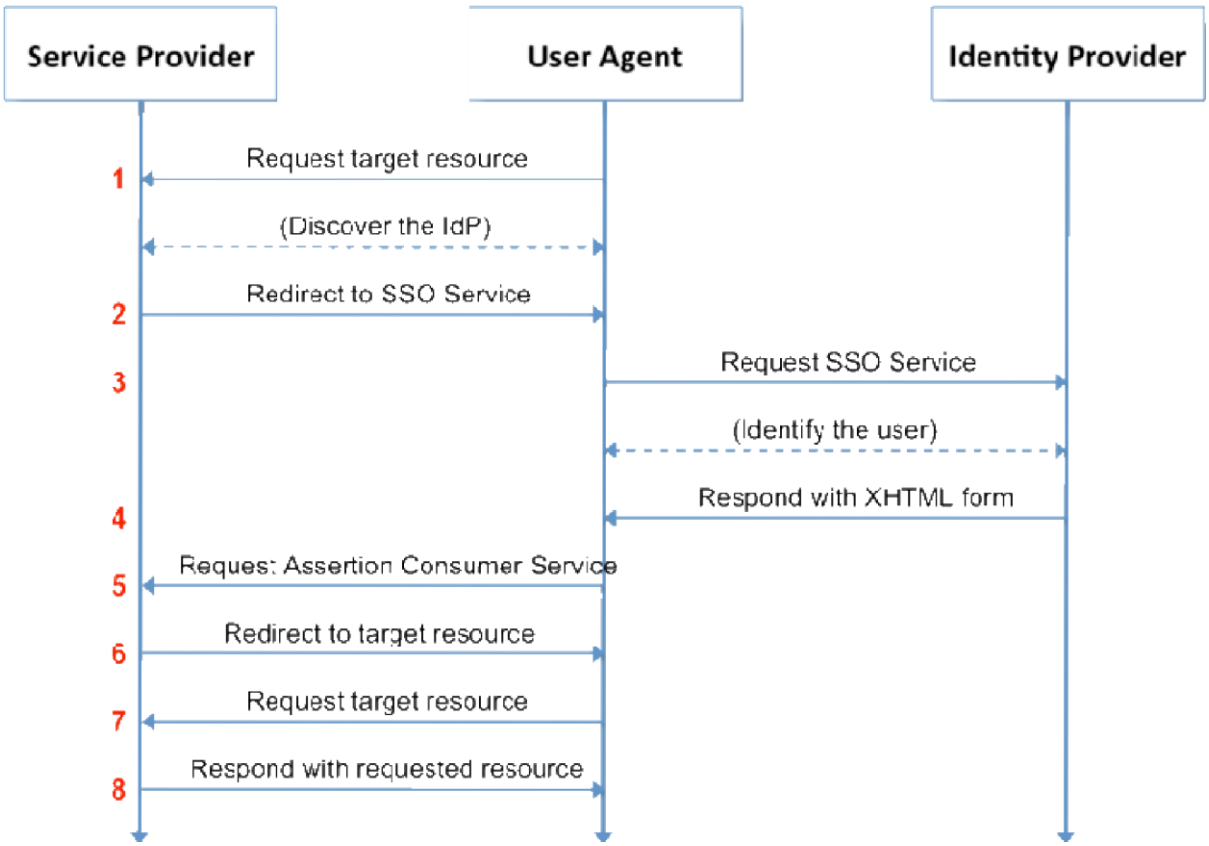
1. SAML Login URL (https://*.*.ppmpro.com/login_sub.pa)
    a. Example: While any Identity Provider that supports SAML 2.0 should be able to be used with PPM Pro, the following is a list of Identity Providers that are known to have been successfully implementedhttps://CustomerABC.ppmpro.com/login_sub.pa
2. SAML Logout URL
3. X.509 Public Certificate (signing)

Types of Single Sign On

PPM Pro supports two types of Single-Sign On: Service Provider (SP) -initiated flow, and Identity Provider (IdP) -initiated flow. Below is a diagram of the flows listed and how it would work.

Service Provider (SP) Initiated Flow (Steps 1-8 in diagram)
1. User browses to assigned custom domain (e.g. https://mycompany.ppmpro.com)
2. User is redirected to the login URL at the IdP with a SAML Request
3-4. User authenticates with the IdP (if not already authenticated)
5-7. User is redirected to https://mycompany.ppmpro.com/login_sub.pa with a signed SAML assertion
8. User is logged into PPM Pro

Identity Provider (IdP) Initiated Flow (Steps 3-8 in diagram)
3-4. User authenticates with the IdP (if not already authenticated)
5-7. User is redirected to https://mycompany.ppmpro.com/login_sub.pa with a signed SAML assertion
8. User is logged into PPM Pro



General documentation for SAML 2.0 can be readily found on the web and further general description beyond the scope of this document.

Identity Providers:

While any Identity Provider that supports SAML 2.0 should be possible to be used with PPM Pro, the following is a list of Identity Providers that are known to have been successfully implemented to date:

- CA Siteminder
- OneLogin
- Centrify
- Oracle OAM (Oracle Access Manager)
- IBM Tivoli
- Ping Identity
- Identity Automation
- SecureAuth
- Layer 7 (CA Technologies)
- InCommon Shibboleth
- Lighthouse
- Symplified
- Microsoft ADFS
- VMware Horizon View
- Okta