|  |  |
| --- | --- |
|  | SAML SSO |
|  | Integrating SSO with Daptiv PPM |

Revision History

|  |  |  |
| --- | --- | --- |
| **Date** | **Version** | **Description** |
| 07/10/2015 | 1.0 | Added Revision History and Sandbox URL |
| 07/10/2015 | 1.1 | Sandbox now reflected in Audience section |
| 09/09/2016 | 1.2 | Added info about Primary IdPs to Step 1. |
| 04/20/2017 | 1.3 | NL Sandbox now reflected in Audience section |

Table of Contents

[Introduction 4](#_Toc461101027)

[Understanding SAML-based SSO for Daptiv PPM 4](#_Toc461101028)

[SP-Initiated Logon 5](#_Toc461101029)

[Getting Started with SAML-based SSO for Daptiv PPM 6](#_Toc461101030)

[Step 1 – Provide details about your IdP to Daptiv 6](#_Toc461101031)

[Step 2 – Add Daptiv as a remote SP in your IdP 6](#_Toc461101032)

[SAML Token Requirements 7](#_Toc461101033)

[FAQ 9](#_Toc461101034)

[Troubleshooting 11](#_Toc461101035)

# Introduction

Security Assertion Markup Language (SAML) is an open XML standard that allows web sites to exchange user authentication and authorization data across security domains. With SAML, users are authenticated by an automated exchange between an online identity provider (IdP) and a service provider (SP). The IdP provides authentication of the user and then passes this information to the SP, which determines whether the authenticated user has access to the secured resource.

Daptiv PPM offers a SAML-based Single Sign-On (SSO) solution to both Production and Sandbox environments. Using the SAML model, Daptiv PPM acts as the service provider (SP). Daptiv customers act as identity providers (IdP) with control of usernames and passwords used to authenticate users to Daptiv PPM. Daptiv SSO is an identity provider (IdP) that issues SAML tokens. Customers that do not have their own IdP can use the Daptiv SSO IdP.

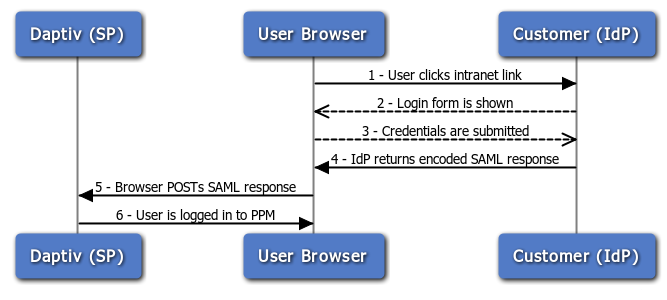
Daptiv’s PPM solution is a SAML v2.0 compliant service provider, and works with any identity provider that can generate SAML v2.0 compliant identity tokens.

Note: SAML based SSO only works for web-based PPM applications, not for Mobile, ProjectTransit, Outlook Integration, or DeskDocs. For these applications you need to use Daptiv credentials.

## Understanding SAML-based SSO for Daptiv PPM

Daptiv natively supports the SAML v2.0 web browser SSO profile using the HTTPS POST binding. This binding uses IdP-initiated logon, and authentication is done by the customer’s IdP, and not Daptiv.

The following diagram shows the steps that happen when a user logs into a SAML enabled enterprise in Daptiv PPM.



**SAML Transaction Steps**

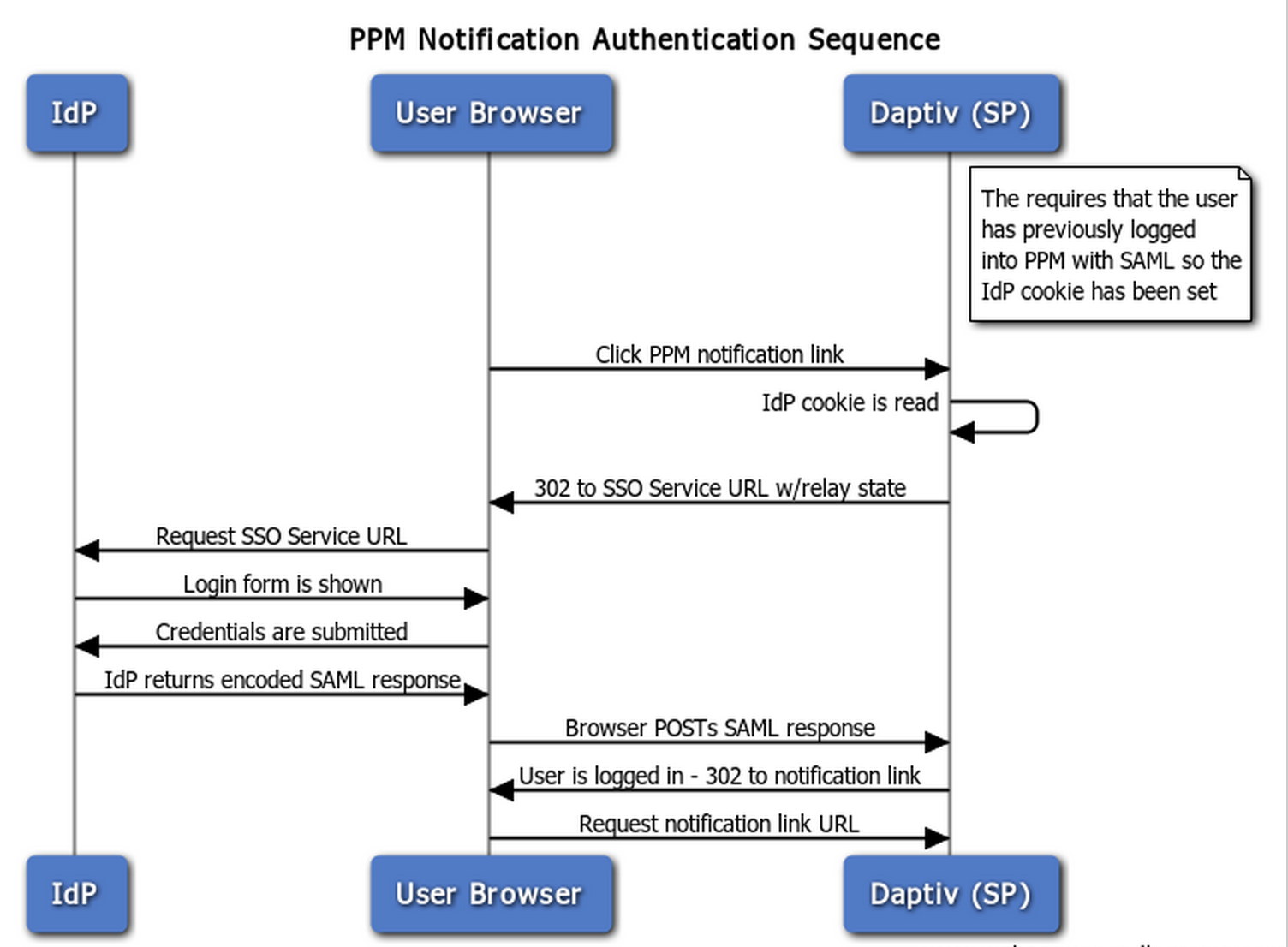
1. The user clicks a link (usually on their intranet) that initiates the logon transaction with the external SP (Daptiv PPM).
2. The IdP shows the logon form to the user (This step may be skipped if the user already has an existing session with the IdP)
3. The user submits their credentials to the IdP (This step may be skipped if the user already has an existing session with the IdP)
4. The IdP returns an encoded SAML response to the browser.
5. The browser POSTs the encoded SAML response to Daptiv PPM.
6. The user is logged into Daptiv PPM.

## SP-Initiated Logon

Daptiv supports SP-initiated logon for users who have previously authenticated with Daptiv PPM via SAML. The primary use case is for users who click on a Daptiv PPM link from a notification email or bookmark a page within Daptiv PPM.

Daptiv PPM’s SP-Initiated logon is reliant upon a cookie (IdpReturnUrl) set in the user’s browser the first time they login via SAML. This cookie stores a unique identifier that is used to lookup the URL to the user’s SSO Service URL.

The following diagram shows the steps that happen when a logged out user clicks on a Daptiv PPM notification email link.



# Getting Started with SAML-based SSO for Daptiv PPM

You need to contact Daptiv Customer Support to request that SAML SSO be enabled for your PPM enterprise. To enable this, there are two steps to complete.

## Step 1 – Provide details about your IdP to Daptiv

The easiest way to provide the necessary information about your IdP to Daptiv Support is to email the entity descriptor metadata included in most SSO products. If this information is not included in your SSO product, you can manually provide Daptiv Support with the following details about your IdP:

* **EntityID** (aka Issuer) – This contains the unique identifier of the IdP. This value is case sensitive.
* **X509 public certificate key** – The public key of your SAML token signing certificate.
* **SSO Service URL** – The URL to which we will redirect the user when their session times out in Daptiv PPM. Here’s an example for ADFS: https://idp.example.com/adfs/ls/

If you plan on using multiple identity providers and/or accessing multiple Daptiv environments (i.e. sandbox, production) then you need to provide details for all IdPs and environments so that our team can add these to our configuration. By default, your primary IdP is the Daptiv IdP, which allows users to access Daptiv PPM through the Daptiv login page or your internal SSO login.  If you would like to restrict access to only your SSO login, you can ask Daptiv Support to set your IdP as the primary.  When the Daptiv IdP is not primary, your enterprise members will be unable to use the Daptiv login page.

## Step 2 – Add Daptiv as a remote SP in your IdP

Configuring your identity provider to work with Daptiv is only a matter of importing our SP metadata into your IdP and configuring any optional policies or access rules. Most IdPs have the ability to import SP metadata from a local file, which you can create by copying and pasting the below metadata into an empty xml file.

**Note:** There should be one SP metadata file per environment.

**US Production PPM service provider metadata (https://ppm.daptiv.com)**

<EntityDescriptor

entityID=**"https://ppm.daptiv.com"**

xmlns=**"urn:oasis:names:tc:SAML:2.0:metadata"**>

<SPSSODescriptor

AuthnRequestsSigned=**"false"**

WantAssertionsSigned=**"true"**

protocolSupportEnumeration=**"urn:oasis:names:tc:SAML:2.0:protocol"**>

<NameIDFormat>

**urn:oasis:names:tc:SAML:2.0:nameid-format:transient**

</NameIDFormat>

<AssertionConsumerService

isDefault=**"true"**

index=**"0"**

Binding=**"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"**

Location=**"https://ppm.daptiv.com/SamlLogin.aspx"** />

</SPSSODescriptor>

</EntityDescriptor>

**US Sandbox PPM service provider metadata (https://sandboxppm.daptiv.com)**

<EntityDescriptor

entityID=**"https://sandboxppm.daptiv.com"**

xmlns=**"urn:oasis:names:tc:SAML:2.0:metadata"**>

<SPSSODescriptor

AuthnRequestsSigned=**"false"**

WantAssertionsSigned=**"true"**

protocolSupportEnumeration=**"urn:oasis:names:tc:SAML:2.0:protocol"**>

<NameIDFormat>

**urn:oasis:names:tc:SAML:2.0:nameid-format:transient**

</NameIDFormat>

<AssertionConsumerService

isDefault=**"true"**

index=**"0"**

Binding=**"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"**

Location=**"https://sandboxppm.daptiv.com/SamlLogin.aspx"** />

</SPSSODescriptor>

</EntityDescriptor>

If you want or need to configure your IdP for Daptiv’s SP manually, it’s easy to do. Daptiv’s Production EntityID is <https://ppm.daptiv.com>, while Daptiv’s Sandbox EntityID is <https://sandboxppm.daptiv.com>. The EntityID for EU Production is <https://ppm.daptiv.nl>, and <https://sandboxppm.daptiv.nl> for EU Sandbox. We only support the HTTPS-POST binding and the NameIDFormat must be “transient”. We require that any SAML assertions be signed and transmitted over SSL. The AssertionConsumerService location changes depending on the PPM environment:

* US Production: <https://ppm.daptiv.com/SamlLogin.aspx>
* EU Production: <https://ppm.daptiv.nl/SamlLogin.aspx>
* US Sandbox: <https://sandboxppm.daptiv.com/SamlLogin.aspx>
* EU Sandbox: <https://sandboxppm.daptiv.nl/SamlLogin.aspx>

These two steps are all it takes to get started with Daptiv PPM SAML integration.

# SAML Token Requirements

Daptiv PPM does not support encrypted SAML tokens, but all tokens must be submitted over a secure channel (https). Any tokens submitted over an unsecure channel (http) will be ignored.

SAML tokens must be digitally signed and validated by the X.509 public cert you provided to Daptiv using SHA-1 or SHA-256. If there is an X.509 certificate in the token, it is ignored. Signature validation is done using the certificate you provided during initial setup

Any SAML token older than its specified NotAfter date will not be accepted; as such you should ensure your IdP’s clock is in sync with a public time server (http://tf.nist.gov/tf-cgi/servers.cgi). Daptiv PPM uses the following two public time servers:

* nist1.symmetricom.com
* time-C.timefreq.bldrdoc.gov.

Additional details about required SAML token XML elements:

* **NameID** – Must be the user’s email address that is registered in Daptiv PPM.
* **NotBefore** – Must be a valid UTC date/time of when the token was issued
* **NotAfter** – Must be set to a valid UTC date/time in the future when the token should expire.
* **Audience** – Ensure you always have the audience set to https://ppm.daptiv.com or https://sandboxppm.daptiv.com if you are using Sandbox
* **SessionIndex** – This identifies a particular user session within the context of the IdP.

# FAQ

**Q**: Does Daptiv PPM support SP-initiated logon?

**A**: Yes, with some restrictions. See the SP-initiated logon section above.

**Q**: Does Daptiv PPM support Single Signout?

**A**: No. However, Daptiv PPM customers have the flexibility to either direct their users to a custom URL or to the standard Daptiv PPM landing page. The standard page indicates to the user that while they have successfully logged out of Daptiv PPM they may still be connected to other systems through their IdP.

**Q**: Does Daptiv PPM support SAML v1.x only IdPs?

**A**: No. We only support SAML v2.0 compatible IdPs.

**Q**: Does Daptiv PPM support encrypted SAML tokens?

**A**: No. We rely on using a secure transport.

**Q**: Which secure signing algorithms does Daptiv PPM support for SAML tokens?

**A**: SHA-1 and SHA-256.

**Q**: What IdPs does PPM support?

**A**: Any SAML v2.0 compliant identity provider.

**Q**: What identity providers do other customers use with Daptiv PPM?

**A**: Microsoft ADFS, CA Siteminder, Oracle Identity Federation, OpenAM

**Q**: When SSO is enabled can a user login using their Daptiv credentials?

**A**: Yes. If the user knows their Daptiv password they can still login without using SSO.

**Q**: Can NameID be something other than email address?

**A**: No, it must use: urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

**Q**: Does PPM support mapping of additional user attributes via SAML?

**A**: No. If this is important to you we encourage you to vote for this feature in our Greenhouse: http://community.daptiv.com/greenhouse/

**Q**: Can SSO be used for ProjectTransit, Outlook Integration, or DeskDocs?

**A**: No. These products require the use of Daptiv credentials.

**Q**: Does Daptiv support the automatic provisioning of user accounts?

**A**: No. User accounts must be manually created by an admin or through Daptiv Connect.

**Q**: Can I use SAML if I have more than one enterprise?

**A**: Yes. Users with multiple enterprise membership will login to their default enterprise. The SAML trust relationship must exist for the user’s default enterprise. Once logged in to their default enterprise users can then switch to another enterprise.

# Troubleshooting

**I’m seeing the Daptiv PPM login page after trying to login using SAML SSO.**

This happens when your IdP is configured to POST the SAML token to the wrong URL. Ensure the browser is POSTing the SAML token to the SamlLogin page, i.e. https://<environment>.daptiv.com/SamlLogin.aspx.

Make sure you are using https and not http.

If you’re using SP-Initiated login ensure you’ve first successfully logged into Daptiv PPM using the IdP initiated workflow at least once in the browser you’re using. Your browser must have an IdpReturnUrl cookie set for the daptiv.com domain.

**Your login email address is not valid. This could mean that you have not been added as a PPM user. Please contact your local PPM administrator to correct this.**

This message displays because there is no associated Daptiv PPM account for the email address given by the IdP. Ensure the user has an account in Daptiv PPM with a matching email address.

**There was an error logging you into PPM. Please contact your local administrator**

If you see this error this means a SAML token was found, but was invalid. Some reasons the token may be invalid include:

* Your IdP server’s clock may be out of sync with Daptiv PPM.
* The audience is incorrect. Ensure you always have the audience set to https://ppm.daptiv.com or https://sandboxppm.daptiv.com if you are using Sandbox depending on which Daptiv environment you are using. This value is case sensitive and must be specified using https.
* The SAML token is failing digital signature verification or is not signed.
* You’re using the assertion consumer service location from the wrong environment.
* If you’re still having trouble you will need to contact Daptiv Support. Daptiv Support has the ability to lookup the specific failure reason.