Oracle Access Manager Configuration Guide for On-Premises

Oracle
Primavera

Version 20
December 2020

ORACLE®

Contents

Introduction

Scope

This guide contains the necessary information and procedures to enable form-based Single Sign-On (SSO) and identity federation using SAML 2.0 authentication for the following products

Single Sign-On (SSO)

- P6 EPPM (P6, P6 mobile, and P6 Team Member Web)
- Primavera Unifier
- Primavera Gateway
- Primavera Analytics and the web-based Configuration Utility

SAML 2.0

- P6 EPPM (P6, P6 mobile, P6 Team Member Web, P6 Integration API, P6 Professional Cloud Connect, and P6 EPPM Web Services)
- Primavera Unifier
- Primavera Gateway
- Primavera Analytics and the web-based Configuration Utility

> **Note**: SAML authentication is not supported for P6 Professional when using Primavera Virtual Desktop.

Audience

This guide is intended to be used by system or network administrators.

Using this Guide

Consider the following workflow when setting up SSO and SAML authentication:

1) Learn more about SSO and SAML Authentication. For more information, see **Configuring Single Sign-On** (on page 7) and **Configuring Identity Federation Using SAML 2.0 Authentication** (on page 23).
2) Ensure that you have completed the prerequisites for configuring SSO. For more information about the prerequisites, see **Prerequisites for Configuring Single Sign-On** (on page 7) and the *Tested Configurations* documents for each product that you plan to configure with SSO or SAML.
3) Implement SSO in Oracle Access Manager using the procedures that are documented in **Configuring Oracle Access Manager and the Oracle HTTP Server WebGate for Single Sign-On** (on page 11).
4) Use the product-specific configurations for SSO using the procedures from the following sections:
   - **Configuring P6 EPPM for Single Sign-On** (on page 19)
   - **Configuring Primavera Unifier for Single Sign-On** (on page 19)

- ▸ **Configuring Primavera Gateway for Single Sign-On** (on page 20) and **Configuring WebLogic for Single Sign-On** (on page 20)

- ▸ **Configuring Primavera Analytics and the Web-Based Configuration Utility for Single Sign-On** (on page 19) and **Configuring WebLogic for Single Sign-On** (on page 20)

5) Ensure that you have completed the prerequisites for identity federation using SAML 2.0. For more information about the prerequisites, see **Prerequisites for Configuring Identity Federation Using SAML 2.0** (on page 25) and the *Tested Configurations* document for each product that you plan to enable identity federation.

6) Implement identity federation using the procedures that are documented in **Configuring Oracle Access Manager for Federated Identity Using SAML 2.0** (on page 25), **Configuring P6 Professional for SAML Authentication** (on page 30), or **Configuring P6 Integration API for SAML Authentication** (on page 33).

Configuring Single Sign-On

Login is the action the user takes to authenticate and gain access to a desired application. SSO is a process that gives users the ability to access multiple protected resources (web pages and applications) with a single authentication. SSO is enabled by Access Manager to eliminate the need for additional or different logins to access other applications at the same (or lower) authentication level during the same session.

Access Manager enables administrators to create a web of trust in which a user's credentials are verified once and are provided to each application the user runs. Using these credentials, the application does not need to re-authenticate the user with its own mechanism.

Application SSO allows users who have been authenticated by Access Manager to access applications without being re-authenticated.

In This Section

Prerequisites for Configuring Single Sign-On

The following prerequisites must be completed for all of the Primavera applications.

Installing Oracle HTTP Server

To learn more about installing Oracle HTTP Server 12c, see:

Installing and Configuring Oracle HTTP Server, which can be found on Oracle Technical Network at http://docs.oracle.com/middleware/1213/core/WTINS/toc.htm.

> **Note:** After you navigate to *Installing and Configuring Oracle HTTP Server,* see the following chapters:
>
> - Chapter 1: *Planning Your Oracle HTTP Server Installation*
> - Chapter 2: *Installing the Oracle HTTP Server Software*

The following documents on My Oracle Support:

How To Install Oracle HTTP Server(OHS)12c In Standalone And Colocated (Managed through WebLogic Server) Domains (Doc ID: 1575618.1)

How To Install Oracle HTTP Server(OHS)12c In Colocated (Managed through WebLogic Server) Domains (Doc ID: 1606339.1)

> **Note:** Oracle Access Manager 12c is bundled with the Oracle HTTP Server 12c download. When you install Oracle HTTP Server 12c, you can install Oracle Access Manager 12c at the same time.

Configuring the Proxy Plugin Module for Oracle HTTP Server for P6 EPPM

To learn more about configuring OHS as a proxy, see:

Using Oracle WebLogic Server Proxy Plug-Ins 12.1.3, which can be found on Oracle Technical Network at
https://docs.oracle.com/middleware/1213/webtier/develop-plugin/overview.htm#PLGWL391.

> **Note:** After you navigate to *Using Oracle WebLogic Server Proxy Plug-Ins 12.1.3,* see the following sections:
> - Section 2.1: *Prerequisites for Configuring the WebLogic Proxy Plug-In*
> - Section 2.4: *Configuring the WebLogic Proxy Plug-In Manually*

The following My Oracle Support document:

How To Configure Oracle HTTP Server (OHS) WebLogic Proxy Plugin For Primavera P6 EPPM Web Applications (Doc ID: 1446675.1)

Installing the LDAP Directory Server

You must have a supported LDAP server. You also need to create a group of users who you want to have access to the application. See the *Tested Configurations* document for supported LDAP servers.

Installing Primavera Applications

Install the most recent version of the Primavera applications that you want to configure for SSO. For more information about installing each of the Primavera products, refer to the installation and configuration documents from the relevant product libraries at Oracle Technical Network.

Installing and Configuring Oracle Access Manager

To install and configure Oracle Access Manager, see the *Installing and Configuring Oracle Identity and Access Management* chapter of the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management guide.*

Configuring and Registering Oracle HTTP Server WebGate for Oracle Access Manager

WebGate is an access client for enforcing access policies on HTTP-based resources. The WebGate client runs as a plugin that intercepts HTTP requests for web resources and forwards them to the access server where access control policies are applied. You must configure it on the same Oracle HTTP Server on which you have installed your product instances. WebGate is automatically bundled with Oracle HTTP Server 12c.

To configure Oracle HTTP Server 12c, see the *Configuring Oracle HTTP Server 12c WebGate* section of the *Oracle Fusion Middleware Installing and Configuring Oracle HTTP Server*.

After your WebGate has been configured with an Oracle HTTP Server, you must register your WebGate with Oracle Access Manager by using the Oracle Access Manager Administration Console.

To register your WebGate with Oracle Access Manager, see the *Registering and Managing OSSO Agents Using the Console* section of the *Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service* guide.

Adding OAMIdentityAsserter Provider in WebLogic

In order to add the OAMIdentityAsserter provider in WebLogic for the web-based Configuration Utility and Primavera Gateway, you must download and install Oracle Application Development Framework (ADF) and extend your WebLogic domain using Oracle Java Required Files (JRF) templates. The Oracle JRF template configures components that are not included in the WebLogic Server installation and is used to configure domains that contain applications that are developed using Oracle ADF and other core components.

Use the following list for guidance to ensure that you can access the OAMIdentityAsserter provider:

1) Verify that you don't have Oracle JRF as a deployment option in the Fusion Middleware Configuration Wizard. For more information, see ***Verifying that the WebLogic Domain Contains Oracle Java Required Files*** (on page 9).
2) If you have determined that you don't have Oracle JRF in the WebLogic domain, complete the tasks outlined in section ***Installing Oracle ADF and Manually Enabling The OAMIdentityAsserter Provider*** (on page 10).

Verifying that the WebLogic Domain Contains Oracle Java Required Files

Before you install Oracle ADF and extending your WebLogic domain with Oracle JRF, ensure that you have not already extended your WebLogic domain to include Oracle JRF. To confirm that your domain is extended by Oracle JRF:

> **Note:** The following steps verify Oracle JRF deployments for one WebLogic domain. If you intend to enable SSO and SAML for both Primavera Gateway and the web-based Configuration Utility, then you must repeat these steps for the domain that you did not verify.

1) Navigate to the bin folder of your WebLogic server at
   `<Middleware_Home>\Oracle_Home\wlserver\common\bin`.

2) Run **config.cmd** (for Windows) **config.sh** (for Linux). This launches the Fusion Middleware Configuration Wizard.

3) On the **Configuration Type** screen, complete the following:

   a. Under **What Do you want to do?**, select **Update an existing domain**.

   b. Browse to the WebLogic domain that contains Primavera Gateway or web-based Configuration Utility servers.

   c. Click **Next**.

4) On the **Templates** screen, complete the following:

   a. In the **Template Categories** list, select **All Templates**.

   b. Ensure that **Oracle JRF - <Version_Number> [oracle_common]** is selected.

If Oracle `JRF - <Version_Number> [oracle_common]` is not on the All Templates list or if it is not selected by default, refer to ***Installing Oracle ADF and Manually Enabling The OAMIdentityAsserter Provider*** (on page 10) for instructions on how to add it to the Fusion Middleware Configuration Wizard.

Installing Oracle ADF and Manually Enabling The OAMIdentityAsserter Provider

Starting in WebLogic 12c, WebLogic and Oracle ADF are required to connect and use the Oracle Repository Creation Utility (RCU) when extending a domain with Oracle JRF because Oracle JRF natively uses a data source and database for parts of its provided functionality. However, the additional functionality provided by Oracle JRF is not required for the SSO and SAML implementation of Primavera Gateway and the web-based Configuration Utility. The following instructions provide the steps to install Oracle ADF and manually enable the OAMIdentityAsserter provider using a database or data source.

> **Notes:**
>
> - For more information about extending a WebLogic domain to include Oracle JRF templates with a database connection, refer to the *Extending a Domain to Support Additional Components* section of the *Oracle Fusion Middleware Administering Oracle Fusion Middleware* guide.
>
> - For more information about additional functionality provided by Oracle JRF templates, refer to the *Fusion Middleware Product Templates* section of the *Oracle Fusion Middleware Domain Template Reference* guide.

To install Oracle ADF and manually enable the OAMIdentityAsserter Provider:

1) Download and install Oracle ADF into your WebLogic deployment. For more information about downloading and installing Oracle ADF, refer to the *Oracle Application Development Framework – Oracle ADF* page at http://www.oracle.com/technetwork/developer-tools/adf/overview/index.html.

2) Complete the following to add the OAMIdentityAsserter provider to the Fusion Middleware Configuration Wizard:

a. Navigate to the **oracle.oamprovider_<version_number>** folder at
`<Middleware_Home>/Oracle_Home/oracle_common/modules/`
`oracle.oamprovider_<version_number>`.

b. Copy the **oamAuthnProvider.jar** file.

c. Navigate to the **mbeantype** folder at
`<Middleware_Home>/Oracle_Home/wlserver\server\lib\mbeantypes`.

d. Paste the **oamAuthnProvider.jar** file to the **mbeantypes** folder.

e. Restart your WebLogic domain.

Configuring Oracle Access Manager and the Oracle HTTP Server WebGate for Single Sign-On

There are several supported authentication schemes that you can use to enable SSO for your Primavera applications, such as: Form (LDAP), X509 (Certificate), WNA (Windows Native Authentication); however, this document covers the necessary procedures for form based authentication. If you prefer to use one of the other authentication schemes, you should review *Managing Access Manager SSO, Policies, and Testing* in the *Fusion Middleware Administrator's Guide for Oracle Access Management* guide.

The following list represents the tasks that you need to complete configure SSO for your P6 EPPM applications:

1) *Registering an Identity Store* (on page 11)
2) *Creating an Authentication Module* (on page 12)
3) *Configuring a Host Identifier* (on page 12)
4) *Configuring an Authentication Scheme* (on page 13)
5) *Protecting Your Resources* (on page 15)
6) *Configuring Protected Resources under an Application Domain* (on page 17)
7) *Mapping Your Authentication Scheme to Your Authentication Policy* (on page 18)
8) *Testing Your Single Sign-On Implementation* (on page 18)

Registering an Identity Store

Oracle Access Manager needs to be configured with a data source that will hold a connection to your LDAP directory server.

For more information about managing data sources for Oracle Access Manager, see Section 4 and 4.2 in the *Fusion Middleware Administrator's Guide for Oracle Access Management* guide, which can be found at the following URL:

http://docs.oracle.com/cd/E27559_01/admin.1112/e27239/datasrc.htm#AIAAG244

To configure a data source in Oracle Access Manager to connect to an LDAP server, follow the instructions in Section 4.3, *Managing User Identity Stores*, in the *Fusion Middleware Administrator's Guide for Oracle Access Management* guide.

> **Note:** You only need to complete steps 1-5 for Section 4.3.2, *Registering a New User Identity Store*.

Creating an Authentication Module

After you have your directory store registered in Oracle Access Manager, you need to create an Authentication Module that links to it. The authentication module needs to be linked to an authentication scheme.

To create an authentication module:

1) Log in to the Oracle Access Manager Administration Console.
2) Navigate to the System Configuration tab.
3) Expand **Access Manager** and then expand **Authentication Modules**.
4) Click **LDAP Authentication Module**.
5) Click **Create**.
6) In the Create LDAP Authentication Module dialog box, do the following:
   a. In the **Name** field, enter a name for the authentication module that you want to create.
   b. From the **User Identity Store** list, select the link that matches the LDAP data source that you created.
   c. Click **Apply** to save the changes.

Configuring a Host Identifier

Oracle Access Manager needs to be configured with a host identifier that matches the host identifier variable that you created when you registered Oracle HTTP Server WebGate with Oracle Access Manager. When you registered your WebGate with the Oracle Access Manager, this step was completed automatically for you.

> **Note:** You need to create a host identifier for each application server in your environment.

If a host identifier was not created or was deleted after you created your WebGate, you will need to create a new host identifier.

To create a new host identifier, follow the instructions in *Managing Host Identifiers* section of the *Fusion Middleware Administrator's Guide for Oracle Access Management*, which can be found at the following URL.

To *confirm* that you have a configured Host Identifier:

1) Log in to the Oracle Access Manager Administration Console.
2) Navigate to the Policy Configuration tab.
3) Click **Host Identifier** and then click **Open**.
4) Click **Search**.
5) Select the link for your Host Identifier.
6) In the **Host Identifier** dialog box, complete the following:

In the Host Name Validation list, ensure that the name of your host identifier under Host Name matches the host identifier that you setup when you registered your WebGate with Oracle Access Manager.

> **Note:** The host identifier field is a value that replaces `hostname:port` in requests from the web server to the Oracle Access Manager.
>
> For example, your WebGate has a host identifier set to `P6EPPM` and you make a request in the browser for a resource, such as `http://ohs_<server_name>:<port>/p6`. The WebGate makes an IsProtected call to the Oracle Access Manager managed server to determine whether the resource is protected; in this instance, the resource is `/p6`. The WebGate will pass the resource from itself to OAM as `http://P6EPPM/p6` — this can be seen in trace mode logs of Oracle Access Manager — and then it will attempt to match a policy created in OAM. As a result of this substitution, redirection to Oracle Access Manager for authentication will occur if the actual `<host_name>:<port>` of the web server is not set as the host identifier value.

Configuring an Authentication Scheme

Once you have a data source that stores a connection to your LDAP server, you have to create an authentication scheme for your Primavera applications. An authentication scheme is a named component that defines the challenge mechanism that is required to authenticate a user. For example, the authentication scheme determines if you will use form based authentication, basic authentication, Windows Native Authentication, and so on.

To create a new authentication scheme, follow the instructions in the *Managing Authentication Schemes* section of the *Fusion Middleware Administrator's Guide for Oracle Access Management*, which can be found at the following URL.

If you already have an authentication scheme, you can use it as a template to provide form based authentication for your P6 EPPM applications.

To duplicate an authentication scheme:

1) Log in to the Oracle Access Manager Administration Console.
2) Navigate to the **Policy Configuration** tab.
3) Expand **Authentication Schemes**.
4) Click **LDAP Scheme**.
5) Click **Duplicate**.
6) In the **Authentication Schemes** dialog box, complete the following:

> **Note:** When you duplicate an existing authentication scheme and are use it as a template for your Primavera applications, many of the fields in the Authentication Scheme dialog box will be prepopulated. You do not need to alter the following fields:
>
> - Description
> - Authentication Level
> - Default
> - Challenge Method
> - Challenge Redirect URL
> - Challenge URL
> - Context Type
> - Context Value
> - Challenge Parameters

a. In the **Name** field, enter a name for your Authentication Scheme.
b. In the **Authentication Module** field, select the authentication module that you created for your LDAP data source.
c. Click **Apply** to create the new authentication scheme.

> **Note:** By default, the ssoCookie:httponly challenge parameter is enabled in an authentication scheme. This parameter helps to prevent JavaScript running in the browser from accessing the ObSSOCookie; however, it is necessary to read ObSSOCookie in order to give applets and iFrames the ability to read from an existing authenticated session.
>
> If this challenge parameter is turned on it will result in the following two issues when using P6 EPPM over SSO:
>
> - Error: "java.lang.ClassFormatError: Incompatible magic value 1008813135 in class file Applet" or "Prompt For Re-authentication When Loading Any Applet When Configured For Oracle Access Manager (OAM)". For more information about these prompts, see Doc ID = 1242418.1 at My Oracle Support.
> - Applets In P6 Are Generating A "Java Authentication Required" Prompt After Reaching The Oracle Access Manager Session Lifetime Threshold. For more information about this prompt, see Doc ID = 1596987.1 at My Oracle Support.
>
> To prevent these prompts from occurring, the following challenge parameters should be added to the authentication scheme created:
>
> - ssoCookie=disablehttponly
> - miscCookies=disablehttponly
>
> For more information about the cookies used during SSO, see *Understanding SSO Cookies* of the *Fusion Middleware Administrator's Guide for Oracle Access Management.*

Protecting Your Resources

After you have Oracle Access Manager configured with a connection to your LDAP server, a host identifier that links to your Oracle HTTP Server WebGate for Oracle Access Manager, and an authentication scheme, you need to create an application domain so that you can setup policies to protect your resources and to configure a policy that points to the authentication scheme that you want to use.

For more information about resource policies, refer to the *Managing Policies to Protect Resources and Enable SSO* section of the *Fusion Middleware Administrator's Guide for Oracle Access Management*, which can be found at the following URL. For the steps to protect your resources, refer to **Configuring Protected Resources under an Application Domain** (on page 17).

Oracle recommends that you protect your context roots with the following conventions:

▸ `/context`

For example, the connection `http://<host_name>:<port>/<context>` will be recognized as a protected resource.

▸ `/context/`

For example, the connection `http://<host_name>:<port>/<context>/` will be recognized as a protected resource.

▸ `/context/** or /context/.../**`

For example, the connection `http://<host_name>:<port>/<context>/<additional_context_roots>` will be recognized as a protected resource.

The following list provides the context roots that need to be protected for each Primavera application:

> **Notes:**
>
> ▪ If you require additional context roots, you must use two asterisks at the end of your connection string (for example, `.../<context>/**)`.
>
> ▪ Protect the P6 Professional Cloud Connect resource if you intend to configure SAML authentication for P6 Professional instances that connect to a P6 EPPM database.

▸ P6

```
/p6
/p6/
/p6/**
```

▸ P6 mobile

```
/p6tmws
/p6tmws/
/p6tmws/**
```

▸ P6 Team Member Web

```
/p6tmweb
/p6tmweb/
/p6tmweb/**
```
▸ P6 Integration API
```
/PrimaveraAPI/APIAPPS
/PrimaveraAPI/APIAPPS/**
```
▸ P6 Professional Cloud Connect
```
/p6procloudconnect
/p6procloudconnect/**
```
▸ P6 EPPM Web Services
```
/p6ws/services
/p6ws/services/**
/p6ws/token
/p6ws/downloadtoken
```
▸ Primavera Gateway
```
/gatewayapi
/gatewayapi/
/gatewayapi/**
```
▸ Primavera Unifier
```
/bluedoor
/bluedoor/
/bluedoor/**
/bp/**
/m/**
```
▸ Primavera Data Warehouse
```
/p6rdb
```

In some instances, you must create a resource definition for context roots with an excluded protection level. For example, Primavera Gateway deployments including P6 integrations and direct AutoVue integrations without VueLink require you to configure context roots with excluded protection levels. When you attempt to connect to an application using a URL that contains an excluded context root, an SSO authentication request will not be generated.

You must configure the context roots below with an excluded protection level because they can cause SSO authentication requests to fail during connection attempts:

▸ Primavera Gateway
```
/gatewayapi/restapi/**
/gatewayapi/restapisession/usersession
```
▸ P6 AutoVue integration without VueLink
```
/p6/VueServlet/**
/p6/jvueDMS/**
/p6/P6AutovueJNLPLauncher
```

```
/p6/P6AutovueJNLPLauncher/**
/p6/applets/jogl.jar
/p6/applets/jsonrpc4j.jar
/p6/applets/gluegen-rt.jar
/p6/applets/jvue.jar
```

> **Note:** If you have setup AutoVue integration using VueLink, you do not need to configure the preceding excluded protection context roots for AutoVue.

For the steps to exclude resources, refer to Configuring Excluded Resources under an Application Domain.

Configuring Protected Resources under an Application Domain

When you registered your Oracle HTTP Server WebGate with the Oracle Access Manager, an application domain was automatically created for you.

To protect the context roots of your Primavera applications:

1) Log in to the Oracle Access Manager Administration Console.
2) Navigate to the Policy Configuration tab.
3) Click **Application Domains** and then click 📁 **Open**.
4) Click **Search** and then search for the name of the application domain that matches your registered WebGate name.
5) Navigate to the Resource tab.
6) Click **New Resource** and then do the following:
    a. In the **Type** field, select **HTTP**.
    b. In the **Host Identifier** field, select the name of the host identifier that you created.
    c. In the **Resource URL** field, enter a protected context root (for example, */p6*)
    d. In the **Protection Level** field, select **Protected**.
    e. In the **Authentication Policy** field, select **Protected Resource Policy**.
    f. Click **Apply**.
7) In the **Resources** tab, highlight the entire field to the right of the Resource Type column and then close it.
8) Click ✖ **Close**.
9) Repeat this procedure for each protected resource.

Configuring Excluded Resources under an Application Domain

When you registered your Oracle HTTP Server WebGate with the Oracle Access Manager, an application domain was automatically created for you.

To exclude the context roots of your Primavera applications:

1) Log in to the Oracle Access Manager Administration Console.

2) Navigate to the **Policy Configuration** tab.

3) Click **Application Domains** and then click 📁 **Open**.

4) Click **Search** and then search for the name of the application domain that matches your registered WebGate name.

5) Navigate to the Resource tab.

6) Click **New Resource** and then do the following:

   a. In the **Type** field, select **HTTP**.

   b. In the **Host Identifier** field, select the name of the host identifier that you created.

   c. In the **Resource URL** field, enter an excluded context root (for example, `/p6ws`

   d. In the **Protection Level** field, select **Excluded**.

   e. Click **Apply**.

7) In the **Resources** tab, highlight the entire field to the right of the Resource Type column and then close it.

8) Click ✖ **Close**.

9) Repeat this procedure for each protected resource.

Mapping Your Authentication Scheme to Your Authentication Policy

After you create your resources and tie them to the Authentication Policy that was created for you when the application domain was created (for example, Protected Resource Policy), you need to map your authentication scheme to your authentication policy so that your resources will present the login form to users for authentication:

1) Log in to the Oracle Access Manager Administration Console.

2) Navigate to the Authentication Policies tab.

3) Select **Protected Resource Policy**.

4) In the Authentication Scheme menu, select the authentication scheme that you created.

5) Click **Apply**.

Testing Your Single Sign-On Implementation

After your Oracle HTTP Server is configured with Oracle HTTP Server WebGate for Oracle Access Manager is restarted, you can test the SSO integration before you configure SSO with your P6 EPPM applications.

To test your SSO implementation:

1) Close all of your open browsers.

2) Open a new browser.

3) Enter the URL of a Primavera application with the following Oracle HTTP Server convention `<server_name>/<port>`. For example: `http://<OHS_Server_Name>:<ohs_port>/p6`

   You are redirected to a SSO form for authentication.

4) Enter the required information.

After you have been successfully authenticated, you will be redirected to the P6 EPPM application login page. The redirection from the SSO login page to the P6 EPPM application landing page confirms the successful setup of the Access Manager.

5) Access a Primavera application that has been enabled for SSO. If you are able to log in to the application without having to enter your user credentials, then you have been successful in implementing SSO.

Configuring P6 EPPM for Single Sign-On

After Oracle Access Manager has been configured to protect the P6 EPPM applications and the WebGate has been configured with the Oracle HTTP Server to intercept requests and confirm resource protection, the P6 EPPM applications must be configured for WebSSO. You need to configure the applications to accept the Header Key username from a successful Oracle Access Manager authentication in order to automatically log in to the P6 EPPM applications.

To configure P6 EPPM for WebSSO:

1) Log in to P6 Administrator application.
2) Navigate to the **Authentication** tab.
3) Expand your P6 configuration and then do the following:
   a. Expand **Authentication**.
   b. In the **Login Mode** field, select **WebSSO**.
   c. Expand **Database Instance** for your P6 EPPM database instance.
   d. In the **Authentication Mode** field, select **WebSSO**.
   e. Collapse your P6 configuration.
4) Click **Save**.
5) Repeat the previous steps for any additional configurations that you might have.

Configuring Primavera Unifier for Single Sign-On

To configure Primavera Unifier for SSO:

1) Run **configure.bat** (with Windows) or **configure.sh** (with UNIX or Linux) under <Unifier_Home>/weblogic.
2) Select **OIM/OAM Enabled** to turn it on.
3) Complete the **sso.logout** field.
   <Unifier_Home>: unifier installation home directory
   sso.logout: for example, `http://<OAM_server>:14100/oam/server/logout`
4) Restart Unifier.

Configuring Primavera Analytics and the Web-Based Configuration Utility for Single Sign-On

To enable SSO for Primavera Analytics, refer to the *Enabling SSO Authentication* section of the *Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition* guide.

To enable SSO for the web-based Configuration Utility, complete the instructions in **Configuring WebLogic for Single Sign-On** (on page 20).

Configuring Primavera Gateway for Single Sign-On

User authentication information is stored both in the user's session data and in the context of a server or virtual host that is targeted by a web application. Primavera Gateway requires a logout URL to log out a user, which invalidates the application session after a user attempts to log in to the application in a new session.

To configure the Logout URL:

1) Log in to WebLogic Enterprise Manager.

   http://<Application_Server_Hostname>:<Port>/em)

2) Select **WebLogic Domain, Security**, and **Security Provider Configuration**.

3) Select **Configure** for the **Single Sign On Provider** option.

4) In the **Logout URL** field, enter the Oracle Access Manager global logout URL:

```
http://<OAM_Server_Hostname:14100/oam/server/logout>
```

5) Select **OK** and restart the WebLogic administration server.

After you have completed this procedure, complete the task in **Configuring WebLogic for Single Sign-On** (on page 20).

Configuring WebLogic for Single Sign-On

WebLogic supports a variety of LDAP providers (for example, Oracle Internet Directory). See the Tested Configurations documents for the products with which you intend to enable with SSO to determine the supported LDAP providers and see your LDAP provider documentation for details on adding users and groups to the store. One of the requirements for the web-based applications is that you create groups in the LDAP store and assign each user that requires access to your applications to these groups in WebLogic.

The following groups are created during the initial deployment of Primavera Gateway:

▸ PrimaveraGatewayProductionAdministrator
▸ PrimaveraGatewayAdminNoData
▸ PrimaveraGatewayProductionDeveloper
▸ PrimaveraGatewayProductionUser
▸ PrimaveraGatewayUserNoData

The following group was created during the deployment of the Primavera Data Warehouse web-based Configuration Utility:

▸ PrimaveraAnalyticsProduction

> **Note**: If you have modified the name of a group in WebLogic, you must also modify the name of the group in your LDAP provider.

Also, you must configure SSO providers in the WebLogic security realm. See *Creating Single Sign-On Authentication Providers* (on page 21) for information on creating authentication providers.

Creating Single Sign-On Authentication Providers

To create SSO authentication providers:

1) Log in to the WebLogic Administration Console as an administrative user for either Primavera Gateway or Primavera Analytics.
2) In the **Change Center** pane select **Lock & Edit**.
3) In the **Domain Structure** pane, select **Security Realms**.
4) Select **myrealm** in the security realm list.
5) In the **Settings for myrealm** page, select the **Providers** tab**.**
6) Select **New** and enter information for a new authenticator provider.
   a. In the **Name** field**,** enter a name for the authenticator provider. For example, OAMIdentityAsserter.
   b. In the **Type** field, select *OAMIdentityAsserter*.
   c. Edit the newly created Authenticator and set the **Control Flag** to *Required*.
   d. Move the following Active Types to the **Chosen** column:
      ▪ OAM_REMOTE_USER
      ▪ OAM_IDENTITY_ASSERTION
      ▪ ObSSOCookie
   e. Select **Save**.
7) Select **New** to enter information for a new authenticator provider.
   a. In the **Name** field**,** enter a name for the provider. For example, PrimaveraAuthenticator.
   b. In the **Type** field, select *OracleInternetDirectoryAuthenticator.*
   c. In the **Common** tab, select the newly created provider and set the **Control Flag** to *SUFFICIENT***,** and select **Save**.
   d. In the **Provider Specific** tab, enter the LDAP information from OAM LDAP store. Ensure you enter information in the following sections: **Connection, Users, Groups, Static Groups, Dynamic Groups (optional)**, and **General**.
   e. Select **Save**.
8) In the **Domain Structure** pane, select **Security Realms, myrealm,** and **Providers**.
9) Edit all other Authenticators and change the **Control Flag** to *SUFFICIENT*.
10) In the **Providers** screen, select the **Reorder Authentication Providers** button and reorder the providers in the following sequence:
   a. OAMIdentityAsserter
   b. PrimaveraAuthenticator
   c. DefaultAuthenticator

    d.   DefaultIdentityAsserter

11) Select **OK** to save your changes

12) In the **Change Center** pane, select **Activate Changes**.

13) Log out of the WebLogic Administration Console.

Configuring Identity Federation Using SAML 2.0 Authentication

SAML Authentication

Security Assertions Markup Language (SAML) associates a principal with additional identity information that can be used to determine the principal's access rights within a specific domain.

SAML is a standard that provides a means for exchanging security information across security domains. In a typical exchange between SAML messages between two domains, one party acts as a relying party while the other acts as an asserting party. The asserting party asserts information, such as whether a user has been authenticated, authorized to perform a certain action, and so forth. The relying party uses information provided by the asserting party to make security-related decisions (for example, what types of access to a specific resource the user should be granted).

When a user signs into a SAML-compliant service of a relying party, the service sends a "request for authentication assertion" to the issuing authority. The issuing authority returns an "authentication assertion" reference stating that the user was authenticated by a particular method at a specific time. The service then passes this assertion reference to other relying parties to validate the user's credentials. When the user accesses another SAML-compliant site that requires authentication, that site uses the reference to request the "authentication assertion" from the issuing authority, which states that the user has already been authenticated. At the issuing authority, an assertion layer handles request and response messages using SAML, which can bind to various communication and transport protocols (for example, HTTP, SOAP, and so on).

While the user who requests an assertion always consumes assertions, the issuing authority can act as producer and consumer since it can both create and validate assertions.

Identity Federation

Federated identity is the mapping of user credentials across security domains (identity providers and service providers) to allow access to hosted computing resources and services. In a federated environment, businesses that utilize federated identity can obtain identity information about an individual or other entity from the user's home organization or security domain. This provides twin benefits:

▸ End users do not need to enter login information to access each entity, or site, where business is conducted. This eliminates the need for users to remember and manage multiple passwords. Users will still need accounts for each site so that the accounts can be mapped.

▸ Enterprises do not need to create additional accounts to manage the identities of users who are already known to a partner organization.

Logging in to an Application that Utilizes Identity Federation with SAML authentication

The following diagram provides a general overview of the processes that occur when a user attempts to log in to a Primavera application after SAML authentication and identity federation has been successfully configured using Oracle Access Manager.
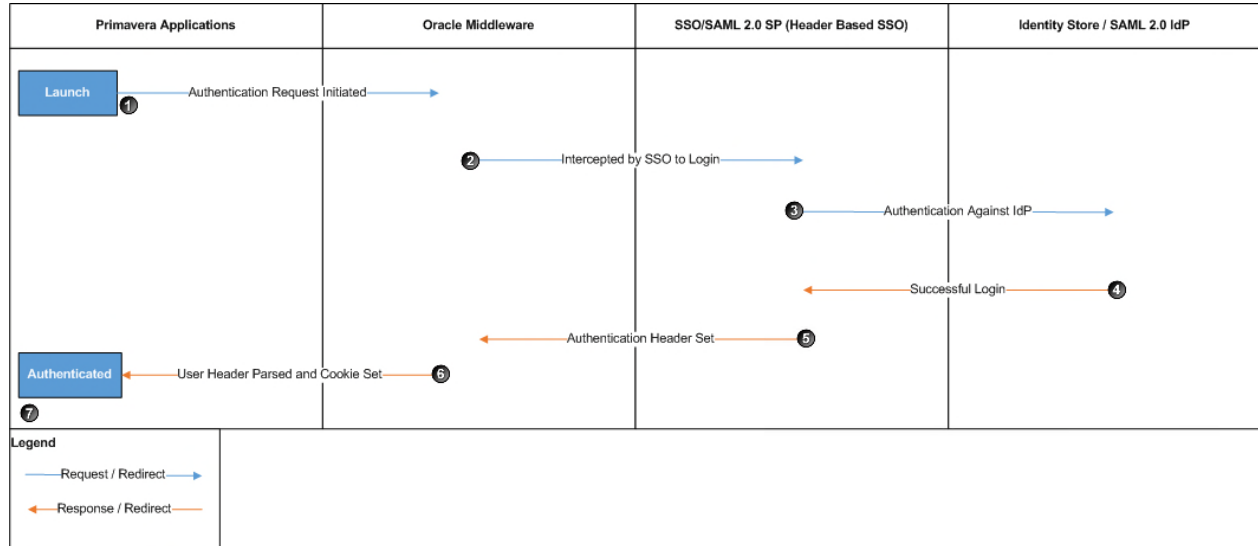
When a user attempts to log in to a Primavera application instance that requires SAML authentication, the following processes occur:

1) The Primavera application sends an authentication request.
2) The authentication request is intercepted by SSO in an embedded browser in which a user is required to enter their login information.
3) The user is authenticated against the identity provider (IdP).
4) After the user is authenticated, the IdP redirects the SAML assertion to the Service Provider (SP).
5) The SP parses the SAML assertion and sets the authentication header.
6) WebLogic reads the header and sets the authentication cookie. The Primavera application reads the cookie and establishes a session.
7) The user is logged in to the application.

> **Note**: SAML authentication is not supported for P6 Professional when using Primavera Virtual Desktop.

In This Section

Prerequisites for Configuring Identity Federation Using SAML 2.0

Prior to configuring your Primavera applications for SAML authentication and identity federation, ensure that you have completed the following prerequisites:

▶ Configure your Primavera applications for SSO

For information to configure SSO, see **Configuring Single Sign-On** (on page 7).

▶ Configure P6 Professional with a P6 EPPM database using P6 Professional Cloud Connect

For information to connect P6 Professional with a P6 EPPM database using P6 Professional Cloud Connect, refer to *P6 Professional for EPPM Installation and Configuration Guide.*

▶ Obtain A SAML 2.0 metadata file that was exported from an IdP

For more information about exporting SAML 2.0 metadata, see your IdP documentation.

Configuring Oracle Access Manager for Federated Identity Using SAML 2.0

The procedures in this section have been described from the perspective of the service provider. Refer to your IdP documentation for instructions on configuring your IdP for federated identity. After your IdP has been enabled for identity federation, complete the tasks from the in the order that they appear:

1) Oracle Access Manager Administration Console as an administrator.
2) **Enabling Identity Federation** (on page 25)
3) **Creating an Identity Store for Account Linking** (on page 26)
4) (Optional) **Enabling Automatic User Provisioning for the Local Identity Store used by Service Providers** (on page 26)
5) **Creating an Identity Provider Partner** (on page 27)
6) **Exporting SAML 2.0 Service Provider Metadata** (on page 28)
7) **Creating a SAML Authentication Policy** (on page 29)
8) **Assigning an Authentication Policy to Application Resources** (on page 29)

Enabling Identity Federation

Prior to configuring Oracle Access Manager for Federated Identity using SAML, you need to enable Identity Federation and Security Token Service.

Enabling **Security Token Services** provides the following capabilities across security domains:

▶ Cross domain SSO for browser based Web SSO flows
▶ Cross domain Web Services Security (WSS) for SOAP clients and servers by means of the WS-Trust protocol

Enabling **Identity Federation** establishes trust between services by exchanging the following:

▶ X.509 certificates used for sign/verify and encrypt/decrypt the Federated messages
▶ Locations of the Federated services
▶ SAML 2.0 metadata

To enable identity federation:

1) In the Launch **Pad** tab, under **Configuration**, select the **Available Services**.
2) In the **Available Services** tab, click **Enable** for the following services:
    ▸ **Identity Federation**
    ▸ **Security Token Service**

Creating an Identity Store for Account Linking

When defining an identity provider partner record, the service provider requires local user accounts to be mapped for imposing its access control model. The process of mapping SAML user accounts from the IdP to the local user accounts at the service provider is known as account linking. In this case, external user accounts that are authenticated by the identity provider need to be mapped to generic local user accounts with permission to access resources.

To create an identity store for account linking:

1) In the **Launch Pad** tab, under **Configuration**, click **User Identity Stores**.
2) In the **User Identity Stores** tab, under **OAM ID Stores**, complete the following:
    a. Select the identity store that you use for SSO and then click **Edit**.
    b. For later use, record the values in the identity store fields.

    > **Note:** The name of the tab reflects the name of the identity store that you select.

3) In the **User Identity Stores** tab, under **OAM ID Stores**, click **Create**.
4) In the **Create: User Identity Store** tab, complete the following:
    a. In the **Store Name** field, enter a name for the identity store.
       For example, *FederationStore*
    b. In the **Login ID Attribute**, under **Users and Groups**, enter the LDAP attribute which identifies a unique login ID for your users.
    c. In the relevant fields, enter the information that you recorded from the identity store earlier.
    d. Click **Apply**.
5) (Optional) Enable automatic user provisioning for the local identity store used by service providers by completing the tasks in *Enabling Automatic User Provisioning for the Local Identity Store used by Service Providers* (on page 26).

Enabling Automatic User Provisioning for the Local Identity Store used by Service Providers

When creating a local identity store mapping for SAML users, it is recommended that you ensure a corresponding user account for an identity provider user ahead of time. For example, if a user does not exist in the local store, the SAML assertion map to that user in the local identity store will fail. To handle an identity mapping failure, Oracle Access Manager Identity Federation features a plug-in that you can enable to automatically provision a missing identity to the local identity store during a federated SSO operation which enables the federated SSO to proceed.

> **Note:** This is an optional task. If you do not enable automatic user provisioning and a user does not exist in this generic LDAP server, then the authentication / SAML assertion can fail.

To enable automatic user provisioning for the local identity store used by service providers:

1) Navigate to <Oracle_Access_Manager_Middleware_Home>/common/bin and then complete the following based on your operating system to open the WebLogic Scripting Tool:
   - If using Linux, run `wlst.sh`.
   - If using Windows, run `wlst.cmd`.

2) Connect to the WLS admin server by running the following:
   ```
   connect()
   ```

3) Navigate to the domain runtime branch by running the following:
   ```
   domainRuntime()
   ```

4) Enable automatic user provisioning by running the following:
   ```
   putBooleanProperty("/fedserverconfig/userprovisioningenabled",
   "true")
   ```

5) Exit the WebLogic Scripting Tool environment by running the following:
   ```
   exit()
   ```

Creating an Identity Provider Partner

An identity provider is responsible for managing, authenticating, and asserting a set of user identities for its service provider partners. In order for the Identity Federation service to perform SSO with external identity providers, they must be defined as trusted partners.

To create an Identity Provider Partner:

1) In the **Launch Pad** tab, under **Identity Federation**, click **Service Provider Administration**.
2) In the **Service Provider Administration** tab, click **Create Identity Provider Partner**.
3) In the **Create Identity Provider Partner** tab, under **General**, complete the following:
   a. In the **Name** field, enter a unique name for the identity provider partner.
      For example, *FederatedProviderPartner*
   b. In the **Description** field, enter a unique description for the identity provider partner.
   c. Select the **Enable Partner** check box.
   d. Deselect the **Default Identity Provider Partner** check box.
4) In the **Create Identity Provider Partner** tab, under **Service Information**, complete the following:
   a. In the **Protocol** list, select **SAML 2.0**.
   b. For **Service Details**, select **Load from provider metadata**.
   c. For **Metadata File**, click **Browse** and then select a metadata file.

   > **Note:** The XML metadata file should be provided by an IdP.

5) In the **Create Identity Provider Partner** tab, under **User Mapping**, complete the following:

a. In the **User Identity Store** list, select the identity store that you created in ***Creating an Identity Store for Account Linking*** (on page 26).

   For example, *FederationStore*

b. Select the **Map assertion Name ID to User ID Store attribute** option.

c. In the **Map assertion Name ID to User ID Store attribute** field, enter the LDAP attribute which identifies the unique login ID for your users. This should match the defined value in ***Creating an Identity Store for Account Linking*** (on page 26).

d. Click **Save**.

6) In the identity provider partner tab, complete the following:

> **Notes:**
>
> - This tab opens automatically after you save the identity provider partner that you create.
> - The name of tab has the name of the identity provider partner that you entered.

a. Click **Create Authentication Scheme and Module**.

> **Note:** The name of the authentication scheme and module is a combination of the name of the identity provider that you created with either FederationScheme or FederationModule appended to it.
>
> For example, *FederatedProviderPartnerFederationScheme* or *FederatedProviderPartnerFederationModule*

b. In the **Advanced** pane, complete the following:
   - Select **Enable global logout**.
   - Select **HTTP POST SSO Response Binding**.
   - In the **Authentication Request NameID Format** list, select **None**.

c. Click **Save**.

Exporting SAML 2.0 Service Provider Metadata

Establishing trust between federation partners is a pre-requisite to perform any federation SSO operation between federation servers. Establishing trust involves exchanging certificate information. If a protocol relies on PKI X.509 certificates to secure message exchanges, as well as the locations and URLs of the services that implement the federation protocol, you can create a service provider SAML 2.0 metadata file in XML format for use by IdP containing information about profiles that the service provider supports. Sites acting as identity providers can import this metadata file to establish a relationship with the service provider.

To export SAML 2.0 service provider metadata:

1) In the **Launch Pad** tab, under **Configuration**, click **Federation Settings**.
2) In the **Federation Settings** tab, under **General**, click **Export SAML 2.0 Metadata...**
3) For later use, record the location to which you export the SAML 2.0 metadata.
4) Provide the metadata file to the IdP when establishing a service provider partner.

Creating a SAML Authentication Policy

When the IdP partner is created, an authentication module and scheme were also created to impose an access control model to protect Primavera application resources. The authentication scheme and module must then be mapped to an authentication policy in the application domain that is created to protect Primavera application resources.

To create an authentication policy and map the federated identity authentication scheme:

1) In the **Launch Pad** tab, under **Access Manager**, click Application Domains.
2) In the **Application Domain** tab, complete the following:
   a. Click **Search**.
   b. Click the name of an application domain.
3) In the application domain tab, open the **Authentication Policies** tab.

> **Note:** The name of the tab is the name of the application domain that you clicked.

4) In the **Authentication Policies** tab, click **Create Authentication Policy**.
5) In the Create Authentication Policy tab, complete the following:
   a. In the **Name** field, enter a name for the authentication policy.
      For example,
   b. (Optional) In the **Description** field, enter a description of the authentication policy.
   c. In the **Authentication Scheme** list, select the authentication scheme that you created in *Creating an Identity Provider Partner* (on page 27).
      For example, *FederatedProviderPartnerFederationScheme*
   d. Click **Apply**.

Assigning an Authentication Policy to Application Resources

To assign an authentication policy to application resources:

1) In the **Launch Pad** tab, under **Access Manager**, click Application Domains.
2) In the **Application Domain** tab, complete the following:
   a. Click **Search**.
   b. Click the name of an application domain.
3) In the application domain tab, open the **Resources** tab.

> **Note:** The name of the tab is the name of the application domain that you clicked.

4) In the **Resources** tab, complete the following:
   a. Select a resource.

> **Note:** You can only select one resource at a time. Select the resources that apply to your P6 EPPM and P6 Professional deployment. For

> example, if you want to enable federated identity for P6 Professional, select P6 Professional Cloud Connect.

    b. In the **Search Results** toolbar, click **Edit**.

5) In the resource tab, complete the following:

> **Note:** The name of the tab is the name of the resource that you clicked.

    a. In the Authentication Policy list, under Protection, select the authentication policy that you created using *Creating a SAML Authentication Policy* (on page 29).

    b. Click **Apply**.

6) Repeat this procedure for each resource in every application domain that is associated with a Primavera application.

Configuring P6 Professional for SAML Authentication

SAML can be enabled to employ LDAP authentication for P6 Professional deployments using P6 Professional Cloud Connect when P6 EPPM has implemented Web Single Sign-In (WebSSO).

> **Note:** This implementation is not meant to enable SSO for P6 Professional. If you have already authenticated a P6 EPPM application with an identity store, logging in to P6 Professional with SAML will require the entry of your username and password in a configured authentication scheme (for example, form based authentication scheme).

Prior to running the procedures in this section, you must have already enabled federated identity for P6 EPPM applications using the procedures that are described in *Configuring Oracle Access Manager for Federated Identity Using SAML 2.0* (on page 25) and have protected your resources for P6 Professional Cloud Connect using *Protecting Your Resources* (on page 15) and *Configuring Protected Resources under an Application Domain* (on page 17). After you have met these conditions, complete the tasks from the following list in the order that they are listed:

1) *Configuring Oracle HTTP Server WebLogic Proxy Plugin for P6 Professional Cloud Connect* (on page 30)
2) *Configuring the P6 Professional to Recognize SAML Authentication* (on page 31)
3) *Configuring P6 Administrator application for P6 Professional SAML Authentication* (on page 32)

Configuring Oracle HTTP Server WebLogic Proxy Plugin for P6 Professional Cloud Connect

After the application domain has been modified in Oracle Access Manager, the Oracle HTTP Server WebLogic proxy plugin must be updated to include a reference to your P6 Professional Cloud Connect URL; this allows the webgate to intercept requests and redirect users to the federated authentication login which was configured in the application domain.

To configure Oracle HTTP Server WebLogic Proxy Plugin for P6 Professional Cloud Connect:

1) Go to `<OHS_Middleware_Home>/user_projects/domains/<P6 EPPM_Domain>/config/fmwconfig/components/OHS/instances/<instance_name e>`.

2) Edit `mod_wl_ohs.conf`.

3) Add the following directives within the <IfModule weblogic_module> element based on your OHS version and WebLogic server environment:
   For non-clustered managed servers:
   <IfModule weblogic_module>
   #For Cloud Connect
   <Location /p6procloudconnect>
       WLSRequest On
       WebLogicHost <WLS_Host_Name>
       WebLogicPort <WLS_Port>
   </Location>
   </IfModule>

   For clustered managed servers:
   <IfModule weblogic_module>
   #For Cloud Connect
   <Location /p6procloudconnect>
     WLSRequest On
     WebLogicCluster <WLS_Host_Name1>:<WLS_Port1>,<WLS_Host_Name2>:<WLS_Port2>
   </Location>
   </IfModule>

4) Save the file.

5) Restart Oracle HTTP Server.
   a. Go to `<OHS_Middleware_Home>/user_projects/domains/base_domains/bin`.
   b. Depending on your operating system, complete the following:
      - For UNIX, run the following in a terminal:
        ```
        ./stopComponent.sh <component_name>
        ./startComponent.sh <component_name>
        ```
      - For Windows, run the following in a command prompt:
        ```
        stopComponent.bat <component_name>
        startComponent.bat <component_name>
        ```

Configuring the P6 Professional to Recognize SAML Authentication

To configure P6 Professional to recognize authentication through SAML:

1) Create or modify the P6 Professional Cloud Connect database alias using the OHS host and port that was configured with the webgate. For instructions on how to create or modify the P6 Professional Cloud Connect database alias, refer to *How To Create Or Modify A Database Alias For Project Management (Also Known As P6 Professional or Optional Client), Methodology Management, Job Services or Contractor (Doc ID 899068.1)* at https://mosemp.us.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=211956235835694&id=899068.1&_afrWindowMode=0&_adf.ctrl-state=17jza9qzmg_4.

   For example, <database_name>@<OHS_Host_Name>:<OHS_Port>/p6procloudconnect

2) On the machines used to launch P6 Professional, go to `dbconfig.exe`. For example, `C:\Program Files\Oracle\Primavera P6\P6 Professional`. This opens the **Database Configuration** dialog box.

3) On the **Welcome to DB Config** page, in the **Database Configuration** dialog box, click Next.

4) On the **Select Database Alias Task** page, in the **Database Configuration** dialog box, complete the following:

   a. Click **Modify an existing database alias**.

   b. Click **Next**.

5) On the **Select Database Alias Task** page, in the **Database Configuration** dialog box, complete the following:

   a. In the **Database alias** field, enter the database alias that you created earlier in this section.

   b. In the **Driver type** field, select **P6 Pro Cloud Connect**.

   c. Click **Next**.

6) On the **Configure P6 Professional Cloud Connect Server** page, in the **Database Configuration** dialog box, complete the following:

   a. In the **Database** field, enter the connection details for your P6 EPPM database.

   b. In the **URL** field, enter the P6 Professional Cloud Connect URL.

   c. In the **Read Timeout** field, enter the amount of time P6 Professional will wait to receive a response from the P6 Professional Cloud Connect server.

   d. Select **Use SAML SSO**.

   e. (Optional) Select **Enable Client-side Cache**.

   f. Click **Next**.

7) Click **Next**.

8) Click **Finish**.

Configuring P6 Administrator application for P6 Professional SAML Authentication

To configure P6 Administrator application for P6 Professional SAML Authentication:

1) Open P6 Administrator application.

2) In the Configurations tab, expand your configuration.

3) Expand **P6ProCloudConnect**, and then complete the following:

   a. Expand **Authentication**.

   b. In the **Mode** field, select **SAML Token Profile**.

4) Click **Save Changes**.

5) Ensure that Login Mode and Authentication have been set to WebSSO. For information on setting Login Mode and Authentication to WebSSO, see *Configuring P6 EPPM for Single Sign-On* (on page 19).

6) Restart the managed servers that host P6 Professional Cloud Connect.

Configuring P6 Integration API for SAML Authentication

To configure P6 Integration API for SAML authentication:

1) Open P6 Administrator application.

2) In the Configurations tab, expand your configuration.

3) Expand **Integration API Server**, and then complete the following:

   a. Expand **Authentication**.

   b. In the **Mode** field, select **SAML Token Profile**.

4) Click **Save Changes**.

5) Ensure that Login Mode and Authentication have been set to WebSSO. For information on setting Login Mode and Authentication to WebSSO, see *Configuring P6 EPPM for Single Sign-On* (on page 19).

6) Restart the managed servers that host P6 Integration API.

Copyright

Oracle Primavera Oracle Access Manager Configuration Guide for On-Premises