How to Setup Oracle Access Manager 12C as Service Provider for Workspace ONE

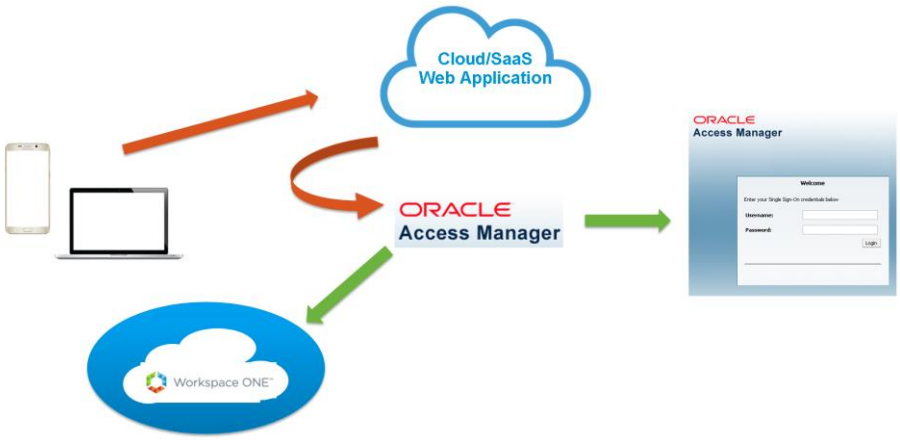
Technical Guide

Last updated: Nov-17

Contents

Overview

This guide provides step by step instructions to configure and test Workspace ONE as a trusted federation identity provider with Oracle Access Manager 12c.



Prerequisites.

- Test Instance of Oracle Access Manager v 12.2.1.0.0 (or higher) installed and configured.
- Workspace ONE tenant
- Configured Service Providers (ie. Salesforce, O365 etc..)

Assumptions

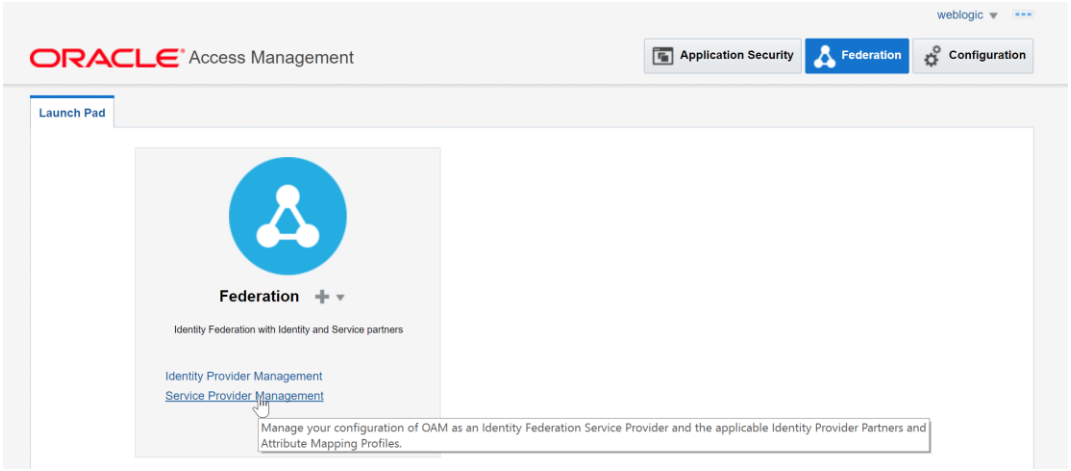
- This document assumes you have a configured Service Provider with the name “SFDC”. You can substitute with the correct name in your environment.

Download Workspace ONE IDP Metadata

1. Log into Workspace ONE Administration console and go to:
    a. Catalog -> Settings -> SAML Metadata -> Identity Provider (IDP) metadata
2. Download and Save the file.

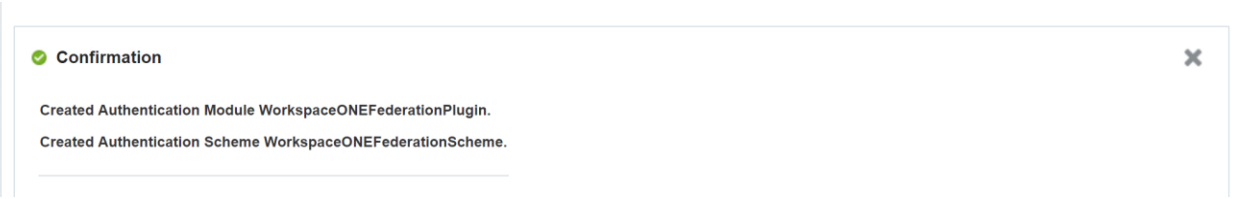
Create Workspace ONE as an Identity Provider in OAM

1. Log into the OAM Console
2. Click on the Federation Tab
3. Click on Service Provider Management



4. Click on Create Identity Provider

5. In the Name field, enter “WorkspaceONE”
6. Under Service Information, upload your Workspace ONE IDP Metadata.
7. Choose the correct Attribute Mapping to match the value being sent by Workspace ONE in the NameID attribute.
8. Click Save
9. Click Create Authentication Scheme and Module



Configure OAM as a SP in Workspace ONE

1. Download the Oracle Access Manager SP Metadata
   http://[OAM_HOST]:14100/oamfed/sp/metadata
2. Log into Workspace ONE Administration -> Catalog
3. Click on Add Application -> Create a new one
4. Provide a name ie. Oracle Access Manager
5. Leave SAML 2.0 Post as the profile and Click Next
6. Under Configuration, paste the SAML Metadata and Click Save

7. Select Sign Assertion
8. Select the correct NameID value to match the value that OAM is expecting.
9. Click on Entitlements and add the necessary entitlements.
10. Click Save

Update Workspace ONE Policies (optional)

1. Log into the Workspace ONE Administration -> Identity and Access Management
2. Configure the appropriate authentication policies as per your requirements Refer to VMware Documentation on how to configure policies.

Update SP Partners to use WS1 for Authentication using WLST

1. Set Environment Variable
    a. $DOMAIN_HOME/bin/setDomainEnv.sh

```
[oracle@localhost ~]$ cd /home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/idm_domain/
[oracle@localhost idm_domain]$ cd bin
[oracle@localhost bin]$ ./setDomainEnv.sh
[oracle@localhost bin]$
```

2. Start WLST
    a. $ORACLE_HOME/oracle_common/common/bin/wlst.sh

```
[oracle@localhost bin]$ cd /home/oracle/Oracle/Middleware/Oracle_Home/oracle_common/common/bin
[oracle@localhost bin]$ ./wlst.sh
```

3. Connect to OAM
    a. Connect('weblogic','WeblogicPassword','t3://localhost:7001')

```
Initializing WebLogic Scripting Tool (WLST) ...

Jython scans all the jar files it can find at first startup. Depending on the sy

Welcome to WebLogic Server Administration Scripting Shell

Type help() for help on available commands

wls:/offline> connect('weblogic','WeblogicPassword','t3://localhost:7001')
```

    b. You should now be logged into WLST and ready to issue WLST Commands:

```
Connecting to t3://localhost:7001 with userid weblogic ...
Successfully connected to Admin Server "AdminServer" that belongs to domain "idm_domain".

Warning: An insecure protocol was used to connect to the server.
To ensure on-the-wire security, the SSL port or Admin port should be used instead.

wls:/idm_domain/serverConfig/>
```

4. Type "domainRuntime()"

5. Type the following:
   setSPPartnerAlternateScheme("SFDC", "true", httpHeaderName="User-Agent", httpHeaderExpression=".*((Android)|(iPhone)).*", authnScheme="WorkspaceONEFederationScheme")

   NOTE: Replace “SFDC” with the correct partner name as per your configuration. If you named your Workspace ONE IDP instance differently from the steps in the document, replace with the correct name in the command above.

```
wls:/idm_domain/domainRuntime/> setSPPartnerAlternateScheme("SFDC", "true", httpHeaderName="User-Agent", httpHeaderExpression=".*((Android)|(iPhone)).*", authnScheme="WorkspaceONEFederationScheme")
Command was successful.
Command was successful.
Command was successful.
wls:/idm_domain/domainRuntime/>
```

For more information on this WLST command and other available commands, please refer to the following documentation:

https://docs.oracle.com/cd/E52734_01/oam/STIAM/if_wlst.htm#STIAM13030

6. Type “exit()”

   Note: There could be a slight delay when updating the configuration via WLST until the changes are propagated across all OAM nodes.