



Value-Added Module (VAM)

# Oracle Access Manager MFA Plugin VAM Deployment Guide

**Copyright information**

©2020. SecureAuth<sup>®</sup> is a registered trademark of SecureAuth Corporation. SecureAuth's Identity Platform software, appliances, and other products and solutions are copyrighted products of SecureAuth Corporation.

**Document revision history**

Version	Date	Notes
1.0	February 2018	First draft
2.0	February 2020	Second draft

For information on support for this module, contact your SecureAuth support or sales representative:

Email: [support@secureauth.com](mailto:support@secureauth.com) inside-  
[sales@secureauth.com](mailto:sales@secureauth.com)

Phone: +1-949-777-6959  
+1-866- 859-1526  
Website: <https://www.secureauth.com/support>  
<https://www.secureauth.com/contact>

## Contents

Introduction .....	4
Prerequisites .....	4
VAM deployment .....	5
Testing the application .....	18
Upgrade information.....	21

## Introduction

This guide explains how to deploy the Oracle Access Manager (OAM) Multi-Factor Authentication (MFA) Plugin Value-Added Module (VAM) to connect SecureAuth IdP with OAM and its supporting servers.

## Prerequisites

The hardware and software that must be installed before deploying the OAM MFA Plug-In VAM includes:

- Install and configure Oracle Servers
- Make sure the latest version of Oracle Access Manager is on the Oracle servers
- Install one or more SecureAuth IdP appliances with required realms

## VAM deployment

The following steps describe how to deploy this VAM.

1. In SecureAuth IdP Web Admin, create a realm or access an existing realm to enable the Authentication API. This SecureAuth API realm negotiates communications between SecureAuth IdP and OAM.

The API can be included in any realm with any Post Authentication event if the appropriate directory is integrated and the necessary features are configured, based on the endpoints you are using.

For more information on creating an API realm, refer to the [Authentication API Guide](#).

2. Click the **API** tab.
3. In the API Key section, set **Enable API for this realm**.
4. In the API Credentials subsection, click **Generate Credentials**.

The Application ID and Application Key fields are populated with the required credential.

5. Click **Select & Copy** to copy the contents of these fields to a text file; copy the credentials to the required header configuration.

The application ID and key values are required in the header configuration. For more on creating and using the header, refer to the [Authentication API Guide](#).

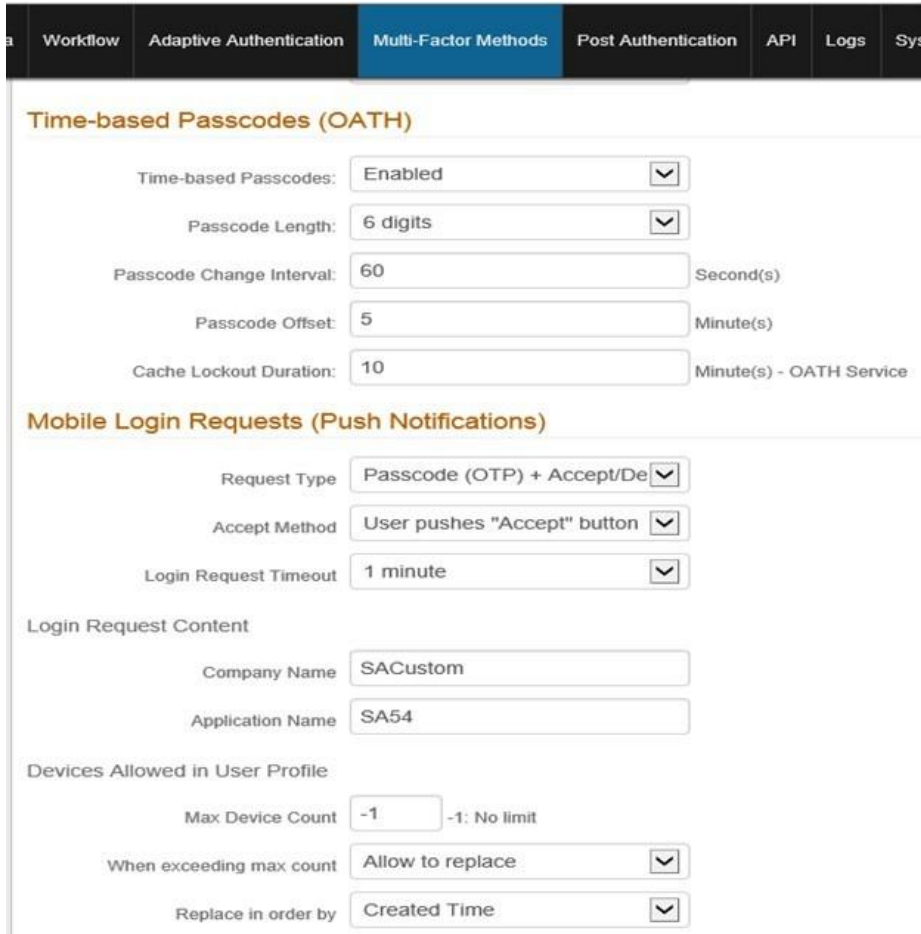
6. In the API Permissions section, set **Enable Authentication API**.

The screenshot shows two sections of the configuration page:

- API Key**: This section has a checkbox labeled "Enable API for this realm" which is checked. Below it is the "API Credentials" subsection, which includes a "Generate Credentials" button. Two input fields are shown: "Application ID" with the value "93821f72c7f04171b8ead2c7398eae33" and "Application Key" with the value "dbdb86180b034c13703dce0e2e364ca6d1d175539a92c66f". Each field has a "Select & Copy" button to its right.
- API Permissions**: This section has a subsection titled "Authentication" with a checkbox labeled "Enable Authentication API" which is checked.

7. Fill out the rest of this page as required
8. Save your changes.

9. Include instructions for handling time-based passcodes and push notifications.
- a. From the SecureAuth IdP Web Admin, click the **Multi-Factor Methods** tab and scroll down to the Timebased Passcodes (OATH) section.



**Time-based Passcodes (OATH)**

Time-based Passcodes:

Passcode Length:

Passcode Change Interval:  Second(s)

Passcode Offset:  Minute(s)

Cache Lockout Duration:  Minute(s) - OATH Service

**Mobile Login Requests (Push Notifications)**

Request Type:

Accept Method:

Login Request Timeout:

**Login Request Content**

Company Name:

Application Name:

**Devices Allowed in User Profile**

Max Device Count:  -1: No limit

When exceeding max count:

Replace in order by:

- b. Specify a passcode type by setting values explained in the following table.

Options	Descriptions and recommendations
Time-based Passcodes	Select <b>Enabled</b> .
Passcode Length	Select a preferred length for the passcode. Default is 6 digits.
Passcode Change Interval	Enter the number of seconds this passcode is valid.

Passcode Offset	Enter the total number of minutes available for passcodes to be attempted (including passcode refresh) before lockout
Cache Lockout Duration	Enter the number of minutes required before another passcode attempt can be attempted

- c. Specify parameters for push notification in the Mobile Login Requests (Push Notifications) section by settings values explained in the following table.

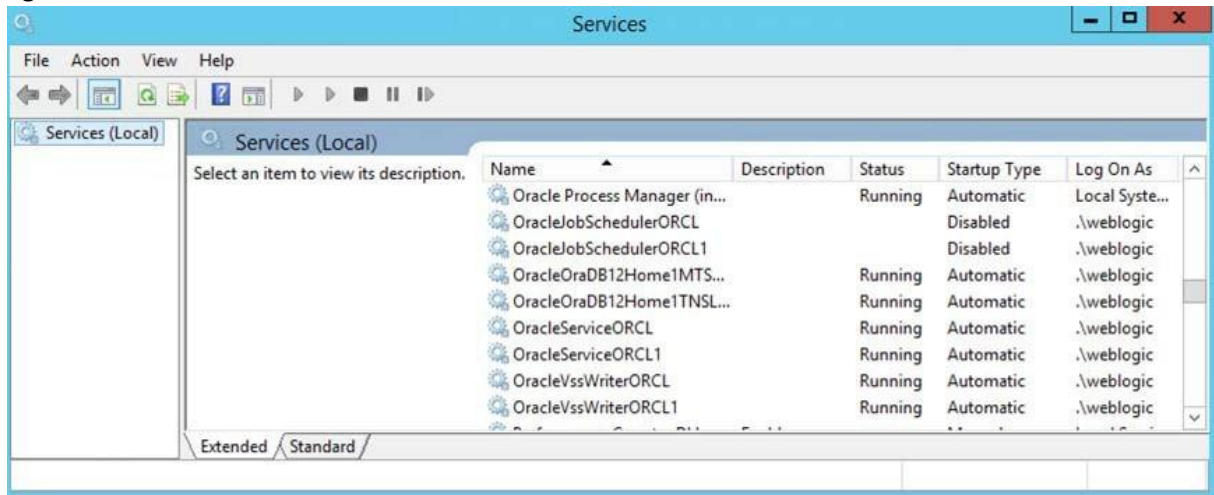
Options	Descriptions and recommendations
Request Type	Select <b>Passcode OTP + Accept/Decline</b>
Accept Method	Select <b>User pushes "Accept" button</b>
Login Request Timeout	Enter the time this OTP is valid before timeout occurs
Login Request Content	
Company Name	Supply a name for the company/organization seeking the login request
Application Name	Supply a name for the application that is being requested
Max Device Count	Enter the maximum devices allowed to request login at the same time. -1 = no limit.
When exceeding mass count	Select an option specifying the response that results once the maximum device count has been exceeded In this case, select <b>Allow to replace</b>
Replace in order by	When allowing a device to be replaced, select the option specifying the method used for that replacement In this case, select <b>Created Time</b>

- d. Click **Save** to confirm your changes.
- e. Set up a mobile device to use push notification.  
Before end users can receive and respond to a push notification on a mobile device, they must first download the SecureAuth Authenticate mobile app to their device and connect the account to their user profile through QR code or a URL. See [Connect an account to your user profile](#) for steps.

If OTP or push notification is not required, skip this step and proceed to Step 10.

10. In a browser, download the `SecureAuth.war` and `SaPlugin.jar` files from the share file designated by your SecureAuth Sales Engineer.
11. Start the OAM servers on Windows.

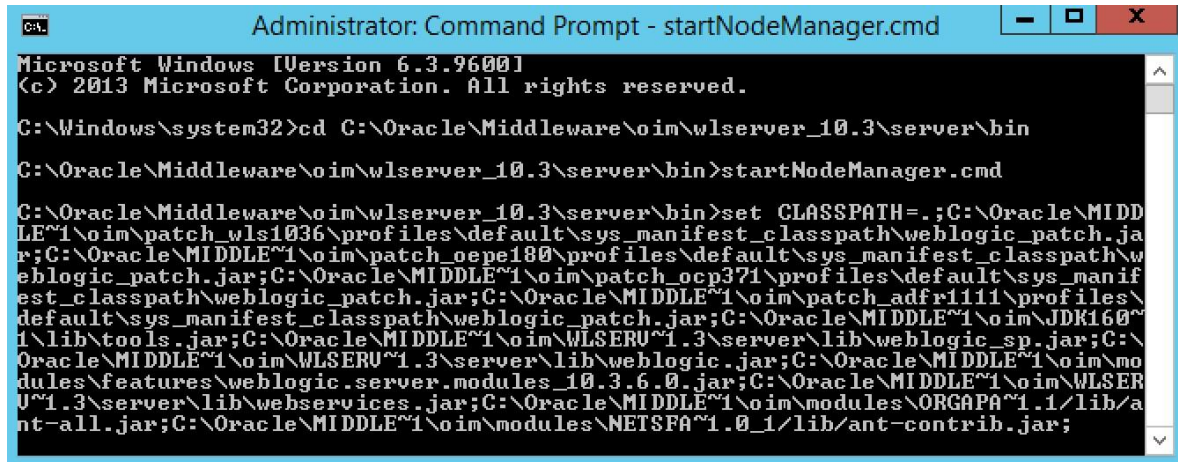
- a. Open Windows Services.
- b. Scroll down to the OAM server names.
- c. Right-click each server in turn and start the service.



12. Open the Command Prompt and enter the required location and command to start the Oracle database components, shown in the following table and image.

Oracle database component	From Command Prompt, enter:
Node Manager	<code>cd C:\Oracle\Middleware\oim\wlserver_10.3\server\bin startNodeManager.cmd</code>
WebLogic server	<code>cd C:\Oracle\Middleware\oim\user_projects\domains\oam_domain\bin\ startWebLogic.cmd</code>
OAM server	<code>cd C:\Oracle\Middleware\oim\user_projects\domains\oam_domain\bin startManagedWebLogic oam_server1</code>
Policy Manager	<code>cd C:\Oracle\Middleware\oim\user_projects\domains\oam_domain\bin startManagedWebLogic oam_policy_mgr1</code>





```

Administrator: Command Prompt - startNodeManager.cmd
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

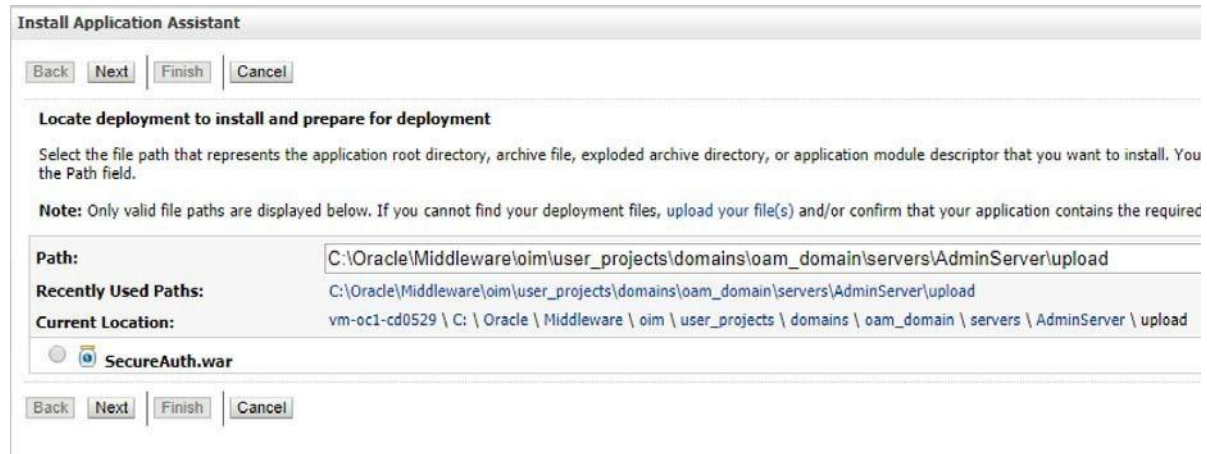
C:\Windows\system32>cd C:\Oracle\Middleware\oim\wlserver_10.3\server\bin
C:\Oracle\Middleware\oim\wlserver_10.3\server\bin>startNodeManager.cmd

C:\Oracle\Middleware\oim\wlserver_10.3\server\bin>set CLASSPATH=.;C:\Oracle\MIDDLE~1\oim\patch_wls1036\profiles\default\sys_manifest_classpath\weblogic_patch.jar;C:\Oracle\MIDDLE~1\oim\patch_oepe180\profiles\default\sys_manifest_classpath\weblogic_patch.jar;C:\Oracle\MIDDLE~1\oim\patch_ocp371\profiles\default\sys_manifest_classpath\weblogic_patch.jar;C:\Oracle\MIDDLE~1\oim\patch_adfr111\profiles\default\sys_manifest_classpath\weblogic_patch.jar;C:\Oracle\MIDDLE~1\oim\JDK160~1\lib\tools.jar;C:\Oracle\MIDDLE~1\oim\WLSEU~1.3\server\lib\weblogic_sp.jar;C:\Oracle\MIDDLE~1\oim\WLSEU~1.3\server\lib\weblogic.jar;C:\Oracle\MIDDLE~1\oim\modules\features\weblogic.server.modules_10.3.6.0.jar;C:\Oracle\MIDDLE~1\oim\WLSEU~1.3\server\lib\webservices.jar;C:\Oracle\MIDDLE~1\oim\modules\ORGAP~1.1\lib\ant-all.jar;C:\Oracle\MIDDLE~1\oim\modules\NETSFA~1.0_1\lib\ant-contrib.jar;

```

### 13. Deploy `SecureAuth.war` on WebLogic.

- a. From the command prompt, navigate to the domain directory where the WebLogic server exists. WebLogic is the platform where you deploy the OAM Console.
- b. Run the server startup script.  
Windows: `startWebLogic.cmd`  
UNIX: `startWeb-Logic.sh`
- c. In a browser, start the WebLogic Server Console. Enter your username and password when prompted.
- d. Set the server to edit mode by clicking **Lock & Edit** in the Change Center section.
- e. In the Domain Structure section, click the **Deployments** link.
- f. In the Summary of Deployments section, click **Install**.
- g. In the Install Application Assistant, click the **upload your file(s)** link.
- h. Click the **Browse** button next to the Deployment Archive field. Browse to where you have the `SecureAuth.war` file installed, select the file, and click **Open**.
- i. Upload the file to the Oracle WebLogic server by clicking **Next**.
- j. Continue the deployment by clicking the radio button next to the `SecureAuth.war` file, then clicking **Next**.
- k. Accept the default value to install the deployment as an application and click **Next**.
- l. Start the deployment process by accepting all other default values and clicking **Finish**.



14. Install `SaPlugin.jar` on the OAM server.

- a. Open the Access Manager on the OAM server. Click the **Plug-ins** tab and then click **Import Plug-in**.
- b. Browse to the `SaPlugin.jar` file and click **Open**. The jar file displays in the Plug-ins screen.

Launch Pad Plug-ins x

Access Manager >

## Plug-ins

Use the following screen to set up custom Plug-ins to extend Authentication functionality for Oracle Access Manager with O

View ▾ [↓ Import Plug-in...](#) [+ Distribute Selected](#) [+ Activate Selected](#) [X Deactivate Selected](#)

Row	Plug-in Name	Description	Activation Status
35	CredentialChallengePlugin		Activated
36	TAPResponseValidationPlugin		Activated
37	SaPlugin		Activated
38	MFAExamplePlugin		Uploaded
39	MfaPlugin		Removed

### Plug-in Details: SaPlugin

Configuration Parameters [Activation Status](#)

\* host

\* API ID

\* API Key

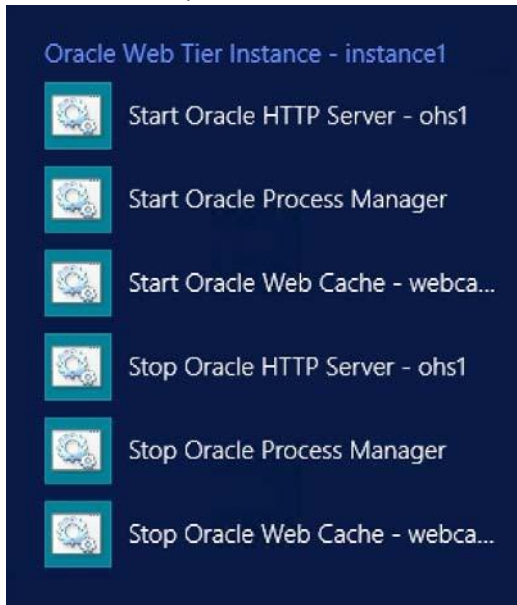
\* API EndPoint

\* API Realm

\* Fail mode

- c. Click the **SaPlugin** file. The Configuration Parameters tab displays in the Plug-in Details section.
- d. Enter the host name as specified in SecureAuth IdP.
- e. Copy the API ID and API Key you saved in step 5 on page 2 to the API ID and API Key fields.
- f. Enter the URL for the endpoint you specified in the SecureAuth IdP API realm in the API EndPoint field.
- g. Enter the URL for the SecureAuth IdP API realm in the API Realm text field.

- h. Specify the Fail Mode as required.
  - i. Save this information and exit.
15. Start Oracle http server/ WebGate, which is the first choice in the following image.



This service can be start using command prompt also.

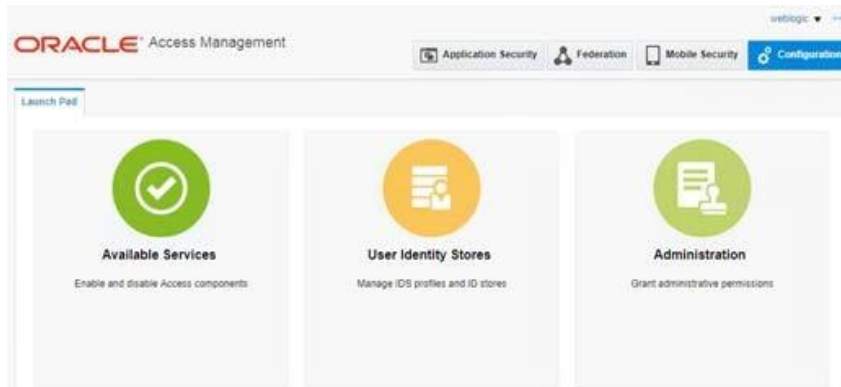
- i. Run command prompt as Administrator
- ii. Go to "C:\Oracle\Middleware\Oracle\_Home\user\_projects\domains\oam\_domain\bin\" folder
- iii. Execute "startComponent.cmd ohs1" command.

Here "oh1" is system component name and it is same name you have selected while setup Oracle HTTP Server.

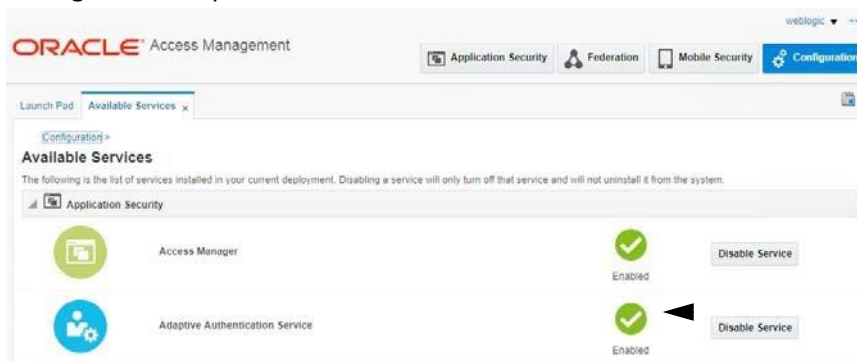
**Note:** - Location of "startComponent.cmd" file can be different based on OAM version and how you have configured environment.

16. In a browser window, enter the URL to the Oracle Access Management Console.
17. Enter the correct username and password.

The Access Management Console launchpad is displayed.



18. Click **Available Services**, then click the **Configuration** tab at the upper right. Be sure both the access manager and adaptive authentication services are enabled as shown in Figure 9.



19. Add the saPlugIn to the Authentication Module.
- From the Access Manager section of the Access Management console, click **Authentication Modules**. b. Click the **Steps** tab.
  - Add the plugin by clicking the + icon.
  - Select the SaPlugin entry you added to WebLogic in step 14 on page 7.

### Authentication Module Authentication Module

Custom Authentication Module relies on bundled plug-ins (or those that are developed using the plug-in that you can orchestrate to ensure that each one performs a specific authentication function).

General **Steps** Steps Orchestration

---

View + × Detach

Step Name	Description	Plug-in Name
Sa MFA		SaPlugin

#### Step Details

Step Name Sa MFA

Description

Plug-in Name SaPlugin

API EndPoint

host

API ID

API Key

Fail mode

API Realm

- e. Ensure the plugin is set up to respond correctly for authentication success, failure, and error. Click the **Steps Orchestration** tab to view the settings.

General Steps **Steps Orchestration**

---

You can specify the initial step

\* Initial Step Sa MFA ▼

Name	Description	On Success	On Failure	On Error
Sa MFA		success ▼	failure ▼	failure ▼

20. Designate the appropriate authentication scheme when this VAM is negotiating communication between SecureAuth IdP and OAM servers. To do this:
  - a. At the Access Manager menu, click to select **Authentication Scheme**. The Authentication Scheme page appears.
  - b. Supply values for each field in the following image, using the values explained in the table.

[Access Manager](#) >**Sa** Authentication Scheme

An Authentication Scheme defines the challenge mechanism required to authenticate a user.

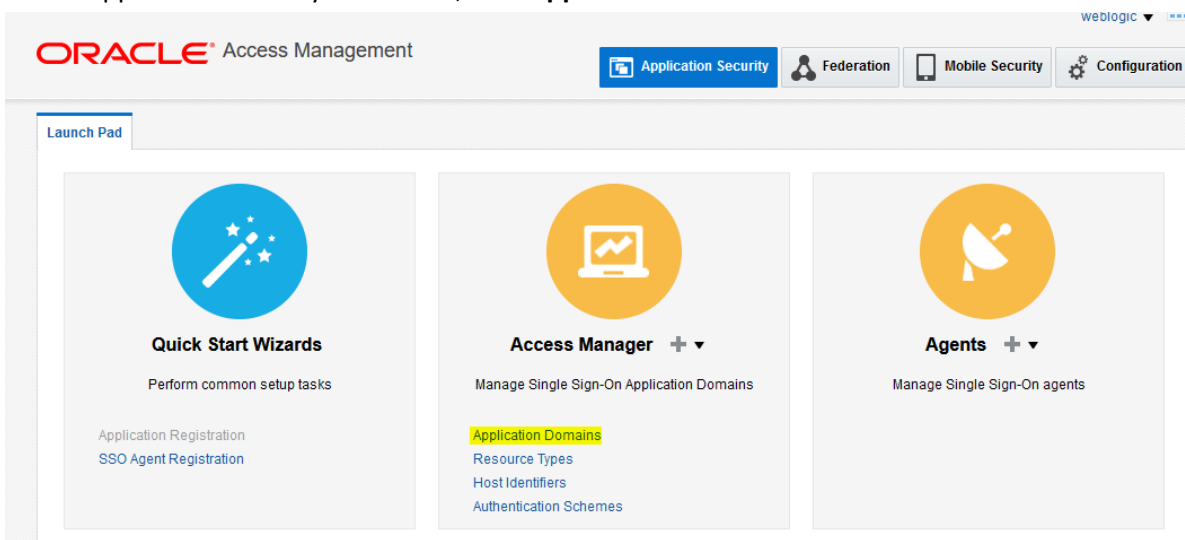
* Name	<input type="text" value="Sa"/>
Description	<input type="text"/>
* Authentication Level	<input type="text" value="2"/> ^ v
Default	<input type="checkbox"/>
* Challenge Method	<input type="text" value="FORM"/> ▼
Challenge Redirect URL	<input type="text" value="/oam/server"/>
* Authentication Module	<input type="text" value="Sa"/> ▼
* Challenge URL	<input type="text" value="/saplugin.jsp"/>
* Context Type	<input type="text" value="customWar"/> ▼
* Context Value	<input type="text" value="/SecureAuth"/>
Challenge Parameters	<input type="text"/>

Options	Descriptions and recommendations
Name	Enter a unique name of this scheme.
Description	If required, enter a description for this scheme.
Authentication Level	Select a level from the drop-down list. Recommended is 2.
Default	Uncheck this box since all values below are custom.
Challenge Method	Select <b>FORM</b> from the drop-down list.
Authentication Module	Select the saplug-in VAM name from the drop-down list.
Challenge URI	Enter the <code>saplugin.jsp</code> file name.
Context Type	Select <b>customWar</b> from the drop-down list.

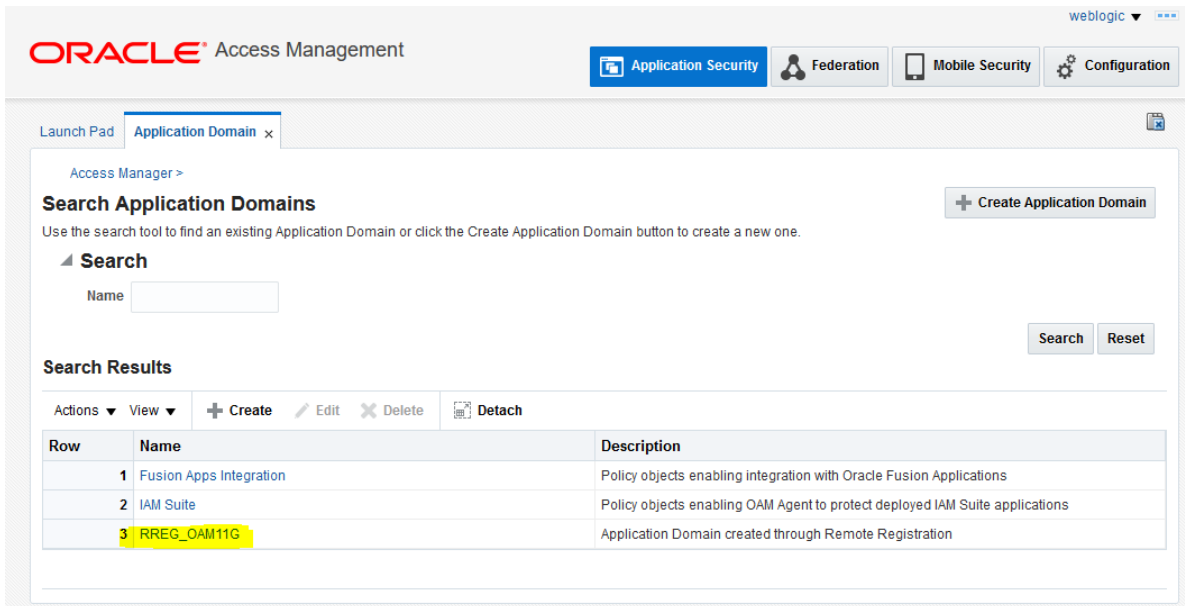
Context Value	Enter <code>/SecureAuth</code> since this represents the directory where the SecureAuth IdP software resides.
---------------	---

21. Specify the application domain for this authentication policy.

- a. At the Application Security dashboard, click **Application Domain**.



- b. Select custom created WebGate agent. E.g. **RREG\_OAM11G** (This name can be anything. When you create new WebGate agent, it will here in the list.)



- c. At the Access Manager menu, click **Authentication Policy** -> **Protected Resource Policy** -> **Advance Rules** -> **Post-Authentication**.



- d. Provide a name and description for the new policy, and select an authentication scheme, such as LDAPScheme.

Launch Pad Application Domain x RREG\_OAM11G x RREG\_OAM11G : Protected R... x

Access Manager >

**Protected Resource Policy** Authentication Policy

Authentication Policy defines the type of verification that must be performed to provide a sufficient level of security. A policy can be defined to protect one or more resources in the Application Domain.

\* Name

Description

\* Authentication Scheme

Resources Responses **Advanced Rules**

Pre-Authentication **Post-Authentication**

View ▼ + Add ✕ Delete ✕ Top ^ Up v Down ✕ Bottom

Order	Rule Name	Description
1	Sa MFA	

FIGURE 13. Authentication Policy Page

- e. Add a new rule by clicking +.
- f. In the Add Rule screen, supply values explained in the following table.

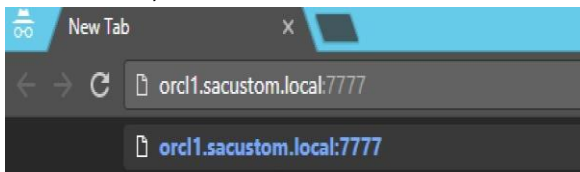
Options	Descriptions and recommendations
Rule Name	Enter a unique name for this rule.
Description	If required, enter a description for this rule.
Condition	Enter code indicating the condition under which this rule will apply.
Deny Access	Check or uncheck this box to indicate whether access should be denied if this condition occurs.
If condition is true	From the drop-down list, select the name of the policy created in this procedure.

22. Save your changes and exit.

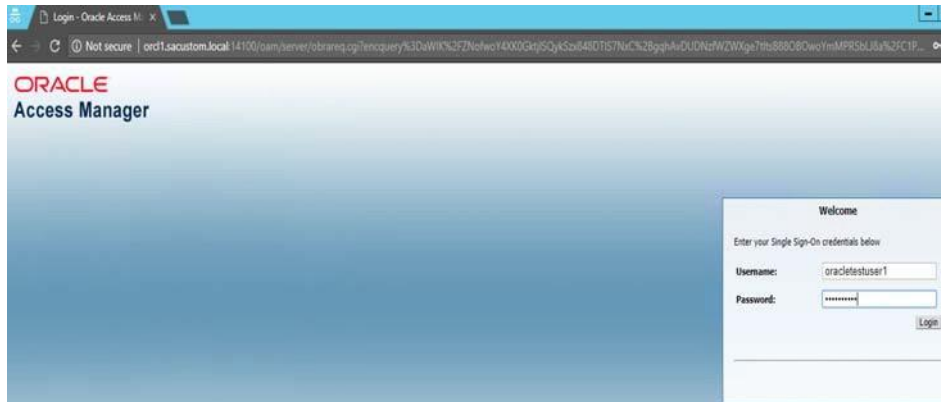
## Testing the application

After you have deployed the VAM and configured both SecureAuth IdP and Oracle Access Manager servers to use it, you are ready to test it.

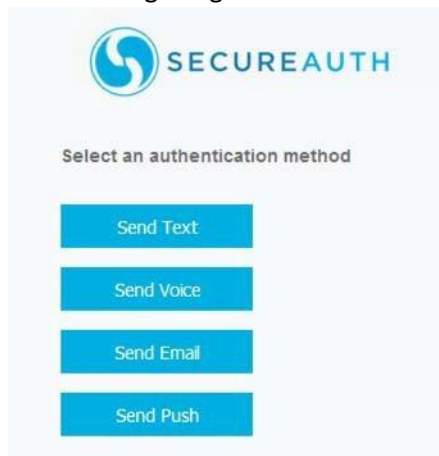
1. In a browser, enter the URI for OAM.



2. In the Oracle Access Manager, enter the correct username and password, then click **Login**.

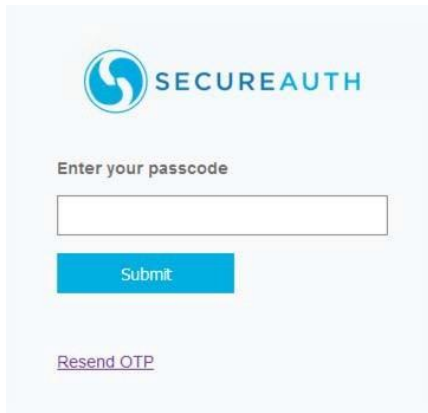


If the VAM is correctly configured, the first factor, username, and password for OAM is displayed. The following image shows the first screen, which prompts for the correct authentication method.



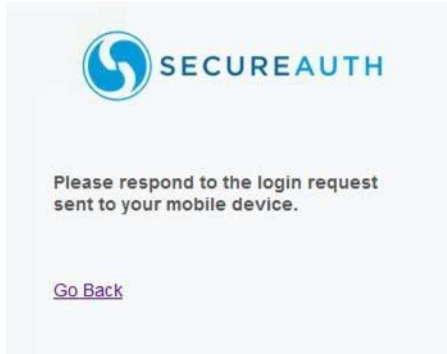
3. Click the authentication method you want to use.

If you select **Send Text**, **Send Voice**, or **Send Email**, you will see the following screen.



The image shows a SecureAuth login interface. At the top left is the SecureAuth logo, which consists of a blue circular icon with a white stylized 'S' and the word 'SECUREAUTH' in blue capital letters. Below the logo, the text 'Enter your passcode' is displayed. Underneath this text is a white rectangular input field. Below the input field is a blue rectangular button with the word 'Submit' in white. At the bottom of the form, there is a purple underlined link that says 'Resend OTP'.

If you select **Send Push**, you are prompted to respond to the login request sent to your mobile device.



The image shows a SecureAuth mobile response screen. At the top left is the SecureAuth logo, which consists of a blue circular icon with a white stylized 'S' and the word 'SECUREAUTH' in blue capital letters. Below the logo, the text 'Please respond to the login request sent to your mobile device.' is displayed. At the bottom of the screen, there is a purple underlined link that says 'Go Back'.

4. Perform one of these steps:

- If a passcode is sent to your device (through text, voice, or email), enter the passcode in the Enter your passcode text box, then click Submit.
- After you receive a push notification on your mobile device, respond to the notification. The Oracle Access Manager login screen is displayed.

TO ORACLE FUSION MIDDLEWARE 11g

**UNIFIED, STANDARDS-BASED INFRASTRUCTURE** Complete, integrated, hot-pluggable, and best of breed middlew

**AGILE AND ADAPTIVE BUSINESS APPLICATIONS** Unified business process platform, common enterprise portal, m

**MODERN DATA CENTERS** Leverage new hardware and software architectures to improve

**EXPLORE INTERACTIVE OVERVIEWS**

**OVERVIEW FOR ORACLE SOA**

SOA

- WebCenter
- WebLogic Server
- Identity Management
- Enterprise Manager
- Grid Infrastructure
- Portal, Forms, Reports & Discoverer

Online Documentation

Oracle Service Bus, Rules, Mediator, Human Task, BPEL, BAM, B2B, Event, UDDI Registry, Metadata Repository, Oracle Adapters, JDeveloper, WS Policy Manager, CEP, Enforcement Point

## Upgrade information

Before upgrading SecureAuth software, open a Support ticket. The process of upgrading to a newer SecureAuth software version might cause the SecureAuth VAM to become invalid and stop working. When your site is ready to upgrade SecureAuth software, get started by [creating a support ticket](#) and selecting **I have a question or issue regarding SecureAuth Value-Added Modules (VAMs)** from the "Submit a request" list. A SecureAuth Tailoring engineer will contact you to evaluate and ensure that the VAM will work with updated SecureAuth software.