

Oracle® Revenue Management and Billing

Version 2.6.0.1.0

Multi-factor Authentication

Revision 1.0

E93827-01

February, 2018

Oracle Revenue Management and Billing Multi-factor Authentication

E93827-01

Copyright Notice

Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

Trademark Notice

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

License Restrictions Warranty/Consequential Damages Disclaimer

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure, and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or de-compilation of this software, unless required by law for interoperability, is prohibited.

Warranty Disclaimer

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

Restricted Rights Notice

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS

Oracle programs, including any operating system, integrated software, any programs installed on the hardware and/or documentation delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware and/or documentation shall be subject to license terms and restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Hazardous Applications Notice

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Third Party Content, Products, and Services Disclaimer

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third party content, products, or services.

Preface

About This Document

This document helps you to configure multi-factor authentication for Oracle Revenue Management and Billing (ORMB) using Oracle SOA Suite and Oracle Access Management.

Intended Audience

This document is intended for the following audience:

- System Administrators
- Consulting Team
- Implementation Team

Note: The person who is setting up multi-factor authentication for ORMB should have basic knowledge on how to install and work with Oracle SOA Suite and Oracle Access Management.

Organization of the Document

The information in this document is organized into the following sections:

Section No.	Section Name	Description
Section 1	Multi-factor Authentication	Explains the multi-factor authentication feature. It also provides the high-level steps on how to configure multi-factor authentication for ORMB.
Section 2	Configuring Oracle User Messaging Service	Explains how to configure the email driver and credentials for the User Messaging Service (UMS).
Section 3	Configuring Adaptive Authentication Service	Explains how to enable and configure the adaptive authentication service. It also explains how to protect the resources on the application domain using the adaptive authentication scheme.
Section 4	Verifying Multi-factor Authentication for ORMB	Explains how to verify whether the multi-factor authentication is successfully configured for ORMB.

Related Documents

You can refer to the following documents for more information:

Document	Description
<i>Oracle Revenue Management and Billing Version 2.6.0.1.0 Release Notes</i>	Provides a brief description about the new features, enhancements, UI and database level changes, supported platforms, framework upgrade, supported upgrades, and technology upgrade made in this release. It also highlights the discontinued features, bug fixes, and known issues in this release.
<i>Oracle Revenue Management and Billing Banking User Guide</i>	Lists and describes various banking features in Oracle Revenue Management and Billing. It also describes all screens related to these features and explains how to perform various tasks in the application.
<i>Oracle Revenue Management and Billing Insurance User Guide</i>	Lists and describes various insurance features in Oracle Revenue Management and Billing. It also describes all screens related to these features and explains how to perform various tasks in the application.

Contents

1. Multi-factor Authentication.....	1
2. Configuring Oracle User Messaging Service	2
2.1 Configuring the Email Driver.....	2
2.2 Setting Credentials for UMS	4
3. Configuring Adaptive Authentication Service.....	8
3.1 Enabling the Adaptive Authentication Service	8
3.2 Configuring the Adaptive Authentication Plugin	9
3.3 Verifying the Adaptive Authentication Plugin Details	14
3.4 Protecting the Resource using Adaptive Authentication Scheme.....	16
4. Verifying Multi-factor Authentication	22

1. Multi-factor Authentication

Oracle Access Management (OAM) provides the adaptive authentication service. This service offers stronger multi-factor (also referred to as second factor) authentication for sensitive applications that require additional security along with the standard user name and password type authentication.

Multi-factor authentication involves more than one stage while verifying the identity of an entity attempting to access services from a server or on a network. For example, when multi-factor authentication is configured, the traditional user name and password is used as the first factor in the authentication process. Additional security is enforced by adding a One Time Pin (OTP) step, or an Access Request (Push) Notification step as a second factor in the authentication process.

Once the first and second factor authentications are successfully validated, the user is directed to the protected resource on the application domain.

To configure multi-factor authentication for ORMB wherein the second factor authentication is done using the One Time Pin (OTP) received on the email, you need to do the following:

1. Configure email address, through which you want to send the OTP, using Oracle SOA Suite
2. Configure the adaptive authentication service using which you want to generate and authenticate the OTP

2. Configuring Oracle User Messaging Service

Oracle SOA Suite provides a component named User Messaging Service (UMS) which enables you to send notifications via various channels, such as Email, Short Message Service (SMS), Instant Messaging (IM) and Voice Mail. Each of these channels needs to be configured before they can be used. This section explains how to configure the Email server as the default mail server for UMS from where you want to send the One Time Pin (OTP) for the second factor authentication.

2.1 Configuring the Email Driver

To set the properties of the email driver:

1. Login to Oracle Enterprise Manager.
2. Expand the **User Messaging Service** node in the left pane of the **Oracle Enterprise Manager 11g Fusion Middleware Control** window.
3. Right-click on the **usermessagingdriver-email (soa_server1)** node. A shortcut menu appears.



Figure 1: usermessagingdriver-email Shortcut Menu

4. Select the **Email Driver Properties** option. The **usermessagingdriver-email** page appears in the right pane of the window.

The screenshot shows a web application window titled "Driver-Specific Configuration". It contains a table with the following columns: Name, Description, Mandatory, Encoded Credential, and Value. The table lists several properties for an email driver.

Name	Description	Mandatory	Encoded Credential	Value
CheckMailFreq	messages from the mail server. The unit is in seconds and the default value is 30 seconds.			30
ReceiveFolder	The name of the folder the driver is polling messages from. The default value is INBOX.			INBOX
OutgoingMailServer	The name of the SMTP server. Mandatory only if e-mail sending is required.			
OutgoingMailServerPort	The port number of SMTP server. Typically 25.			25
OutgoingMailServerSecurity	The security used by SMTP server. Possible values are None, TLS and SSL. Default value is None.			None
OutgoingDefaultFromAddr	The default FROM address (if one is not provided in the outgoing message).			
OutgoingUsername	The username used for SMTP authentication. Required only if SMTP authentication is supported by the SMTP server.			

Figure 2: Driver-Specific Configuration

5. Set the values of the following properties in the **Driver-Specific Configuration** section:

Property	Description	Mandatory (Yes or No)
OutgoingMailServer	Used to specify the name of the SMTP server.	Yes
OutgoingMailServerPort	Used to specify the port number of the SMTP server.	Yes
OutgoingMailServerSecurity	Used to indicate the security setting used by the SMTP server. The valid values are: <ul style="list-style-type: none"> • None • TLS • SSL <div> Note: You must select the None option from the list. </div>	Yes

6. Save the changes and restart the Oracle WebLogic server.

2.2 Setting Credentials for UMS

The adaptive authentication service uses Oracle SOA's User Messaging Service (UMS) to send email notifications. The OAM server needs the UMS credentials to establish the connection to UMS Web service.

To set credentials for UMS:

1. Login to Oracle Enterprise Manager.
2. Expand the **WebLogic Domain** node in the left pane of the **Oracle Enterprise Manager 11g Fusion Middleware Control** window.
3. Right-click on the domain name. A shortcut menu appears.

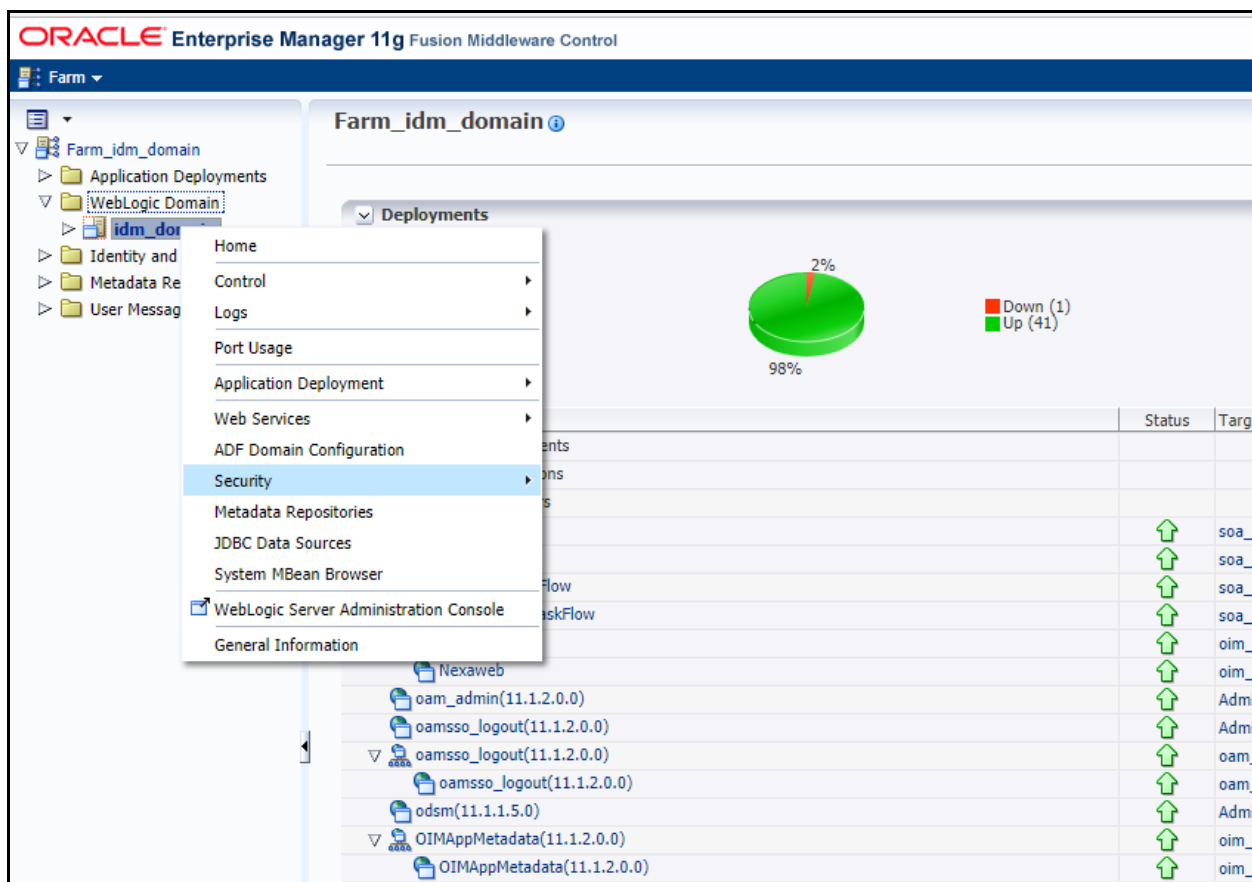


Figure 3: WebLogic Domain Shortcut Menu

4. Select the **Security** option from the shortcut menu. A sub-menu appears.
5. Click the **Credentials** option from the **Security** sub-menu. The **Credentials** screen appears.

idm_domain ⓘ
WebLogic Domain ▼

Credentials

A credential store is the repository of security data that certify the authority of entities used by Java 2,

> **Credential Store Provider**

+ Create Map + Create Key | Edit... ✕ Delete... | Credential Key Name

Credential	Type	Description
▶ ADF		
▶ BPM-CRYPTO		
▶ OAM_CONFIG		
▶ OAM_STORE		
▶ OAM_SYSTEM_CONFIG		
▶ OAMAgent		
▶ OIC_MAP		
▶ oim		
▶ Orade-IAM-Security-Store-Diagnostics		
▶ orade.bi.publisher		
▶ orade.bi.system		
▶ orade.wsm.security		
▶ OSTO_CONFIG		

Figure 4: Credentials Screen

6. Select the **OAM_CONFIG** node and then click **Create Key**. The **Create Key** window appears.

Create Key

Select Map: OAM_CONFIG ▼

* Key:

Type: Password ▼

* User Name:

* Password:

* Confirm Password:

Description:

OK Cancel

Figure 5: Create Key Window

The **Create Key** window contains the following fields:

Field Name	Field Description	Mandatory (Yes or No)
Select Map	Used to indicate the map for which you want to create the key.	Yes
Key	Used to specify the name for the key.	Yes
Type	Used to indicate the type of credential that you want to specify in the key. The valid values are: <ul style="list-style-type: none"> Password Generic 	Yes
User Name	Used to specify the user name using which you want to connect the UMS server.	Yes
Password	Used to specify the password using which you want to connect the UMS server.	Yes
Confirm Password	Used to specify the password using which you want to connect the UMS server.	Yes
Description	Used to specify the description for the key.	No

7. Ensure that the **OAM_CONFIG** option is selected from the **Select Map** list and the **Password** option is selected from the **Type** list.
8. Enter `umsKey` in the **Key** field.
9. Enter the required user name and password in the **Create Key** window.
10. Click **OK**. The key is defined to establish connection with the UMS server.

3. Configuring Adaptive Authentication Service

This section explains how to enable and configure the adaptive authentication service. It also explains how to protect the resources on the application domain using the adaptive authentication scheme.

3.1 Enabling the Adaptive Authentication Service

To enable the adaptive authentication service:

1. Login to Oracle Access Management using the administrator's credentials.
2. Click the **Configuration** button. The **Launch Pad** tab appears.

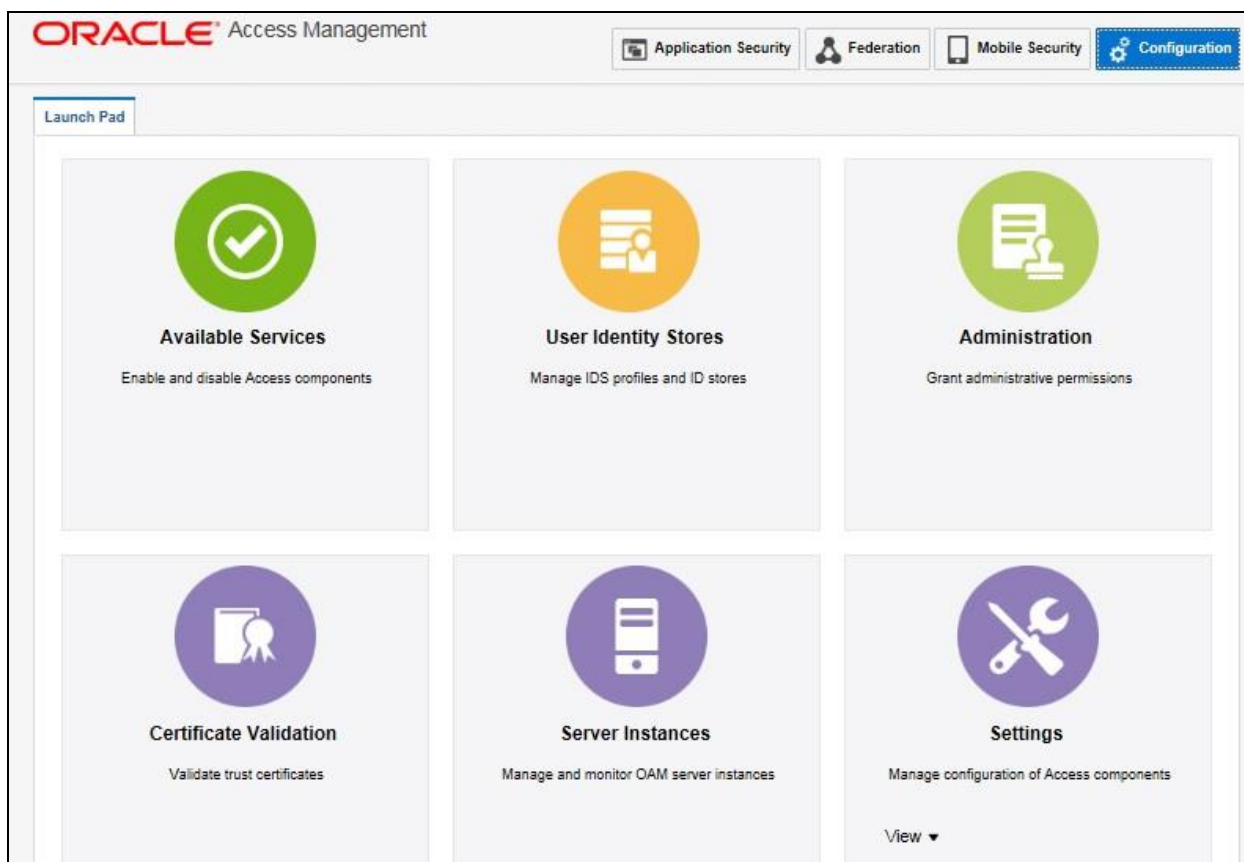


Figure 6: Configuration Launch Pad

- Click the **Available Services** icon. The **Available Services** tab appears.

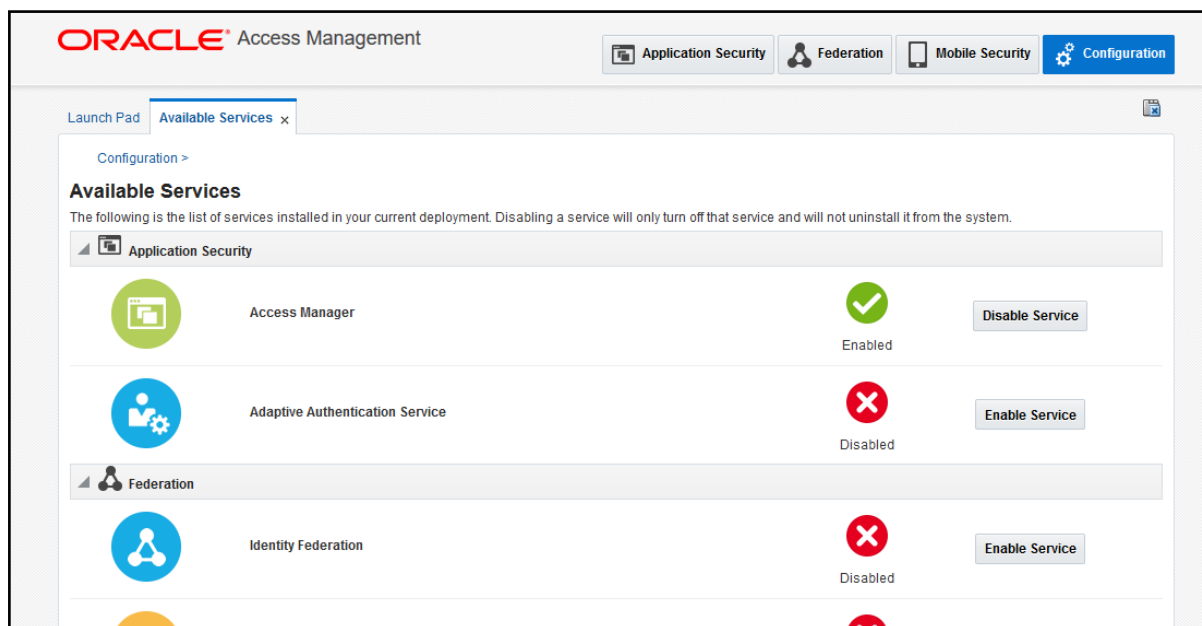


Figure 7: Available Services Tab

- Click the **Enable Service** button corresponding to the adaptive authentication service in the **Application Security** section. The **Enabled** icon appears corresponding to the adaptive authentication service indicating that the service is enabled.

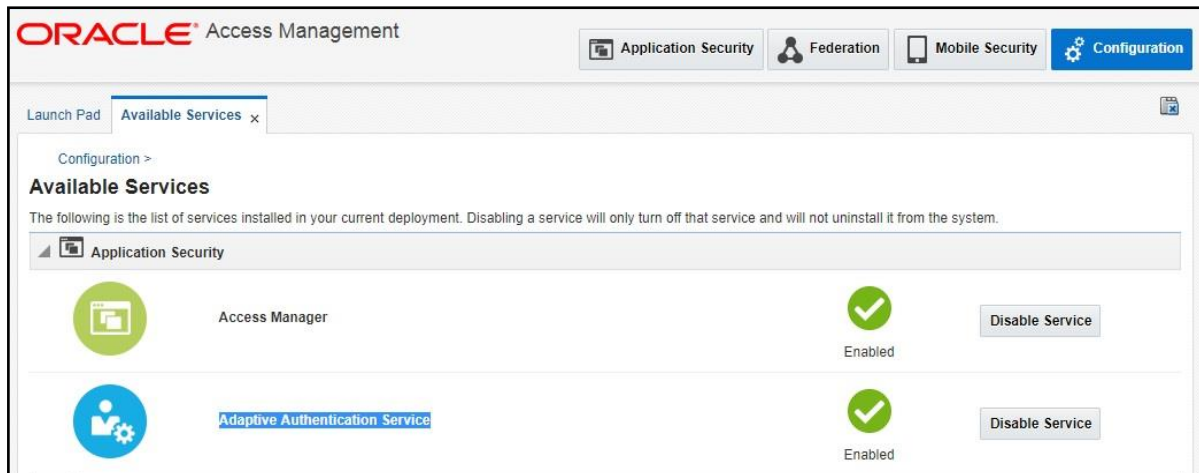


Figure 8: Enabled Adaptive Authentication Service

3.2 Configuring the Adaptive Authentication Plugin

To configure the email related settings in the adaptive authentication plugin:

- Login to Oracle Access Management using the administrator's credentials.

- Click the **Application Security** button. The **Launch Pad** tab appears.

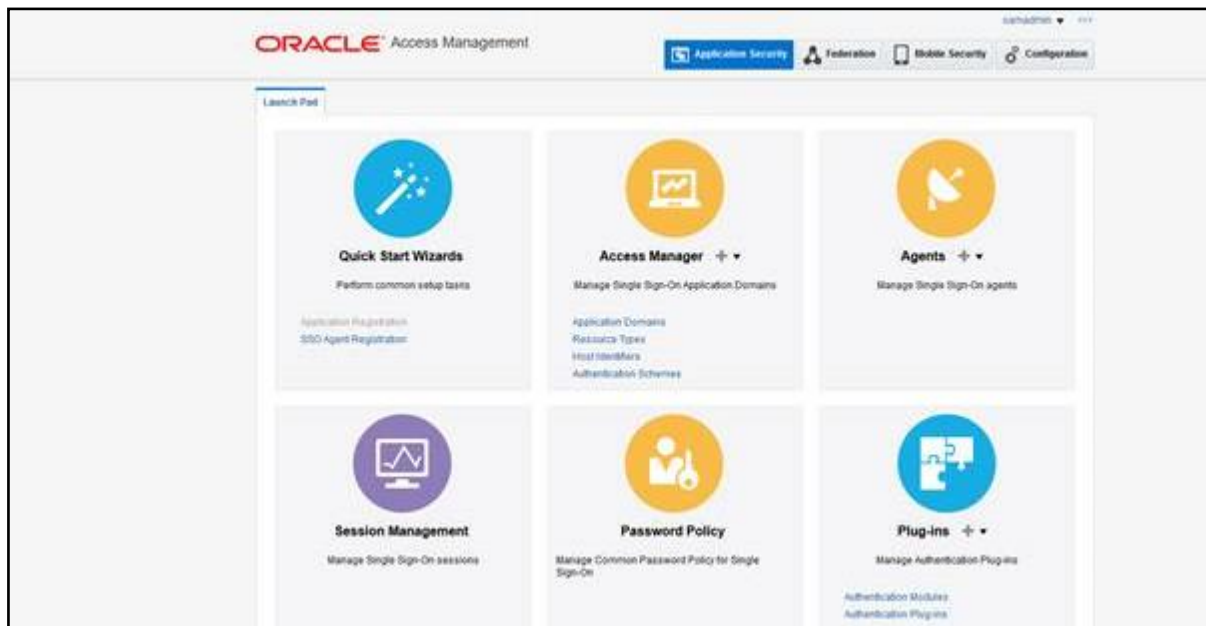


Figure 9: Application Security Launch Pad

- Click the **Authentication Plug-ins** link in the **Plug-ins** section.

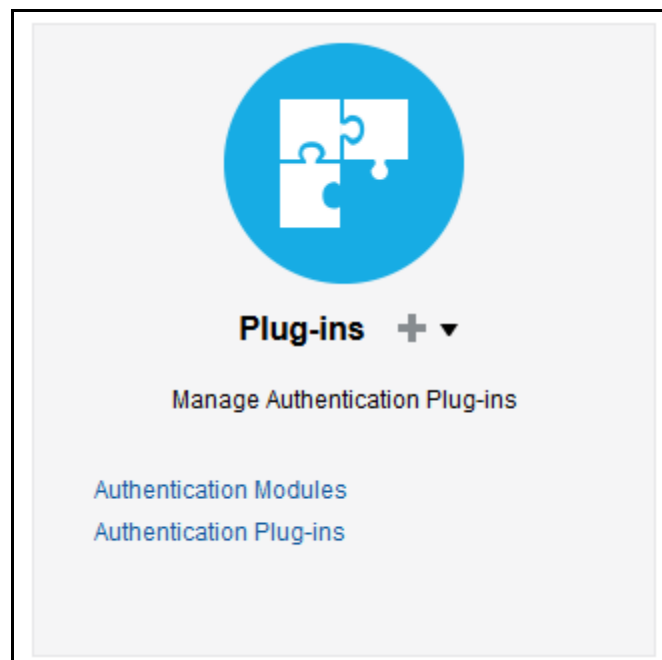


Figure 10: Plug-ins Section

- The **Plug-ins** tab appears.
- Type `AdaptiveAuthenticationPlugin` in the field which is above the **Plug-in Name** column and then press **Enter**. A row appears in the grid.

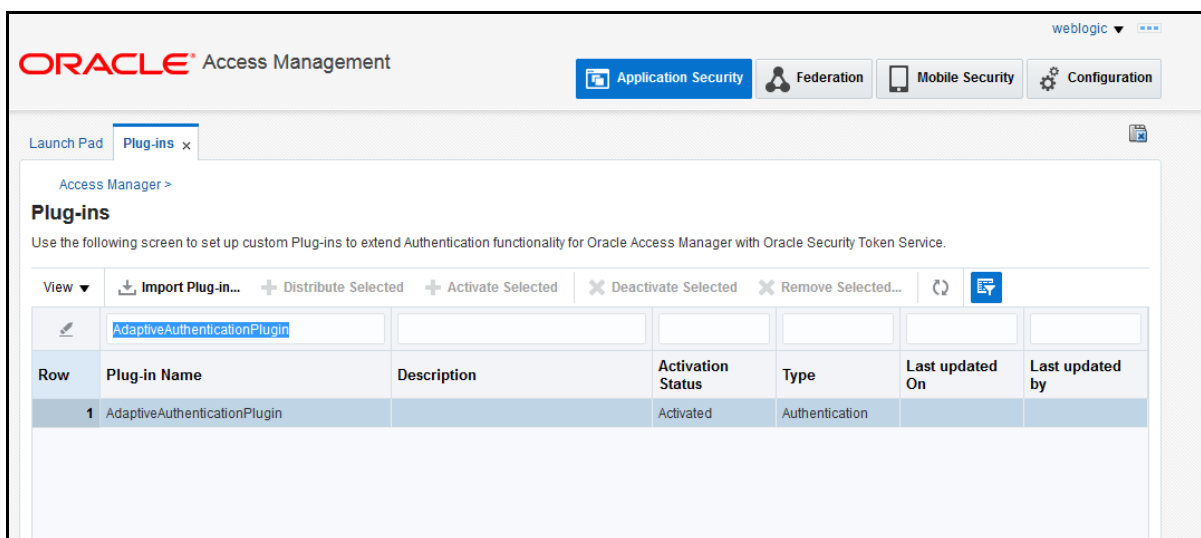


Figure 11: Searching AdaptiveAuthenticationPlugin

6. In the **Plug-in Details: AdaptiveAuthenticationPlugin** section, ensure that the **Configuration Parameters** tab is selected.



Figure 12: Configuration Parameters Tab

7. Enter the values for the following parameters:

Parameter	Description	Mandatory (Yes or No)
SFATypes	Used to indicate the type of second factor authentication. For sending OTP through email, you must specify the email ID as the parameter value.	Yes

Parameter	Description	Mandatory (Yes or No)
Email_Enabled	<p>Used to indicate that you want to send OTP through email. The valid values are:</p> <ul style="list-style-type: none"> • true • false <p>Note: Here, you must set this parameter value to true.</p>	Yes
IdentiyStoreRef	<p>Used to indicate the user identity store using which you want to authenticate the user at the first level.</p> <p>Note: You must specify a user identity store where the directory type is set to OUD.</p>	Yes
UMSAvailable	<p>Used to indicate whether you want the adaptive authentication service to send the email using UMS. The valid values are:</p> <ul style="list-style-type: none"> • true • false <p>Note: Here, you must set this parameter value to true.</p>	Yes
UmsClientUrl	Used to specify the URL of UMS web service.	Yes
EmailField	<p>Used to indicate the field which contains the user's email address (to which you want to send the email) in the user identity store.</p> <p>Note: Here, you must set this parameter value to mail.</p>	Yes
PinLength	Used to specify the length of OTP which you want to send via email.	Yes
PinChars	Used to indicate the characters using which you want to generate the OTP. If you only want digits in OTP, enter 0123456789.	Yes
EmailMsgSubject	Used to specify the subject for the email through which you want to send the OTP.	Yes

Parameter	Description	Mandatory (Yes or No)
EmailMsgFrom	Used to indicate the email address from which you want to send the OTP.	Yes
EmailMsgFromName	Used to specify the sender's name that you want to display in the email.	Yes

8. Click **Save**. The changes are saved.

3.3 Verifying the Adaptive Authentication Plugin Details

To verify the adaptive authentication plugin details:

1. Login to Oracle Access Management using the administrator's credentials.
2. Click the **Application Security** button. The **Launch Pad** tab appears.

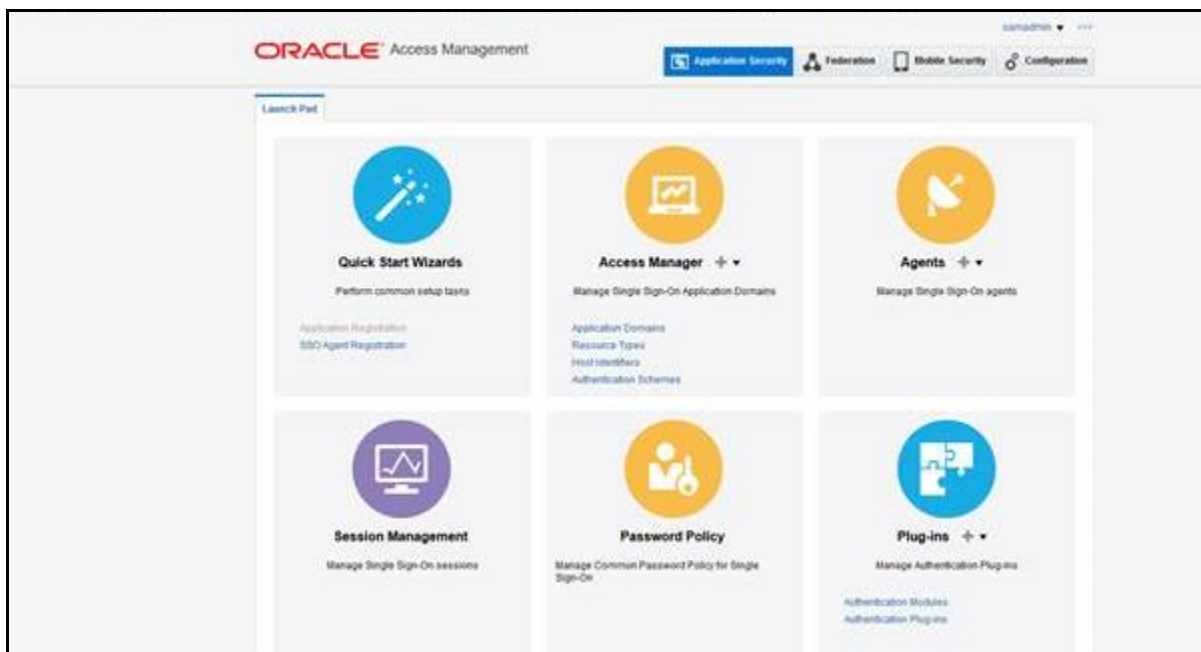


Figure 13: Application Security Launch Pad

3. Click the **Authentication Modules** link in the **Plug-ins** section. The **Authentication Modules** tab appears.

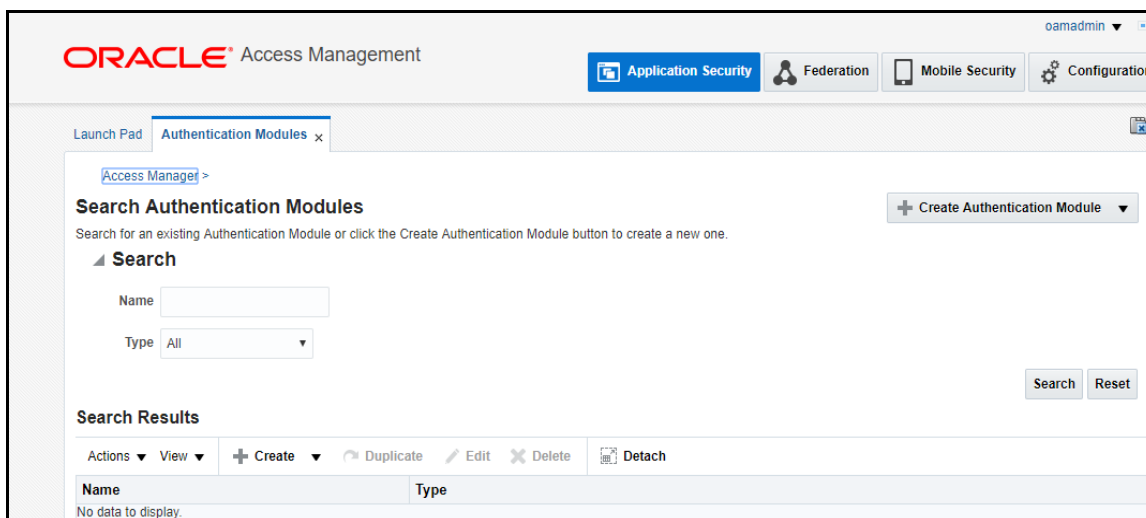


Figure 14: Authentication Modules Tab

4. In the **Search** section, select the **Authentication Plugin** option from the **Type** list.

5. Enter `AdaptiveAuthenticationModule` in the **Name** field and then click **Search**. A row appears in the **Search Results** section.

Launch Pad Authentication Modules x

Access Manager >

Search Authentication Modules

Search for an existing Authentication Module or click the Create Authentication Module button to create a new one.

Search

Name: AdaptiveAuthenticationM

Type: Authentication Plugin

Search Reset

Search Results

Actions View Create Duplicate Edit Delete Detach

Name	Type
AdaptiveAuthenticationModule	Authentication Plugin

Figure 15: Searching AdaptiveAuthenticationModule

6. In the **Search Results** section, click the **AdaptiveAuthenticationModule** link. The **AdaptiveAuthenticationModule** tab appears.

Launch Pad Authentication Modules x AdaptiveAuthenticationMod... x

Access Manager >

Authentication Module Authentication Module

Duplicate Apply

Custom Authentication Module relies on bundled plug-ins (or those that are developed using the Access Manager Authentication Extensibility Java API). This module uses more than one plug-in that you can orchestrate to ensure that each one performs a specific authentication function.

General Steps Steps Orchestration

* Name: AdaptiveAuthenticationMod

Description: Adaptive Authentication Module

Copyright © 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Figure 16: AdaptiveAuthenticationModule Tab

7. Click the **Steps** tab. The **Steps** tab appears.

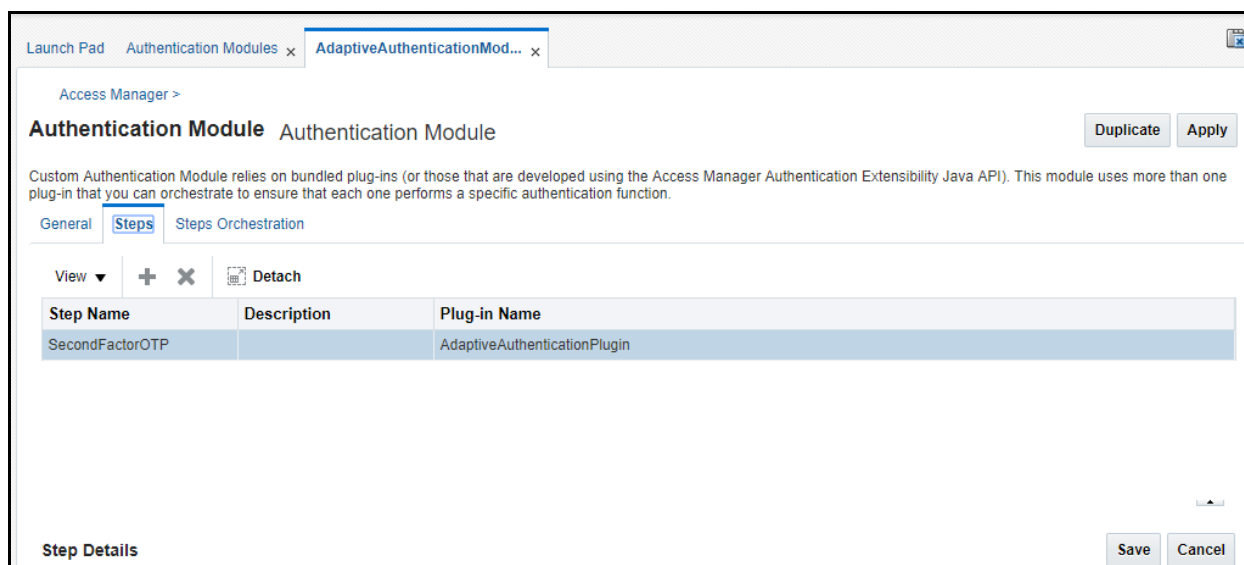


Figure 17: Steps Tab

8. In the **Step Details** section, verify the details specified while configuring the adaptive authentication plugin. You can edit the details, if required.

3.4 Protecting the Resource using Adaptive Authentication Scheme

To protect the resource using the adaptive authentication scheme:

1. Login to Oracle Access Management using the administrator's credentials.
2. Click the **Application Security** button. The **Launch Pad** tab appears.

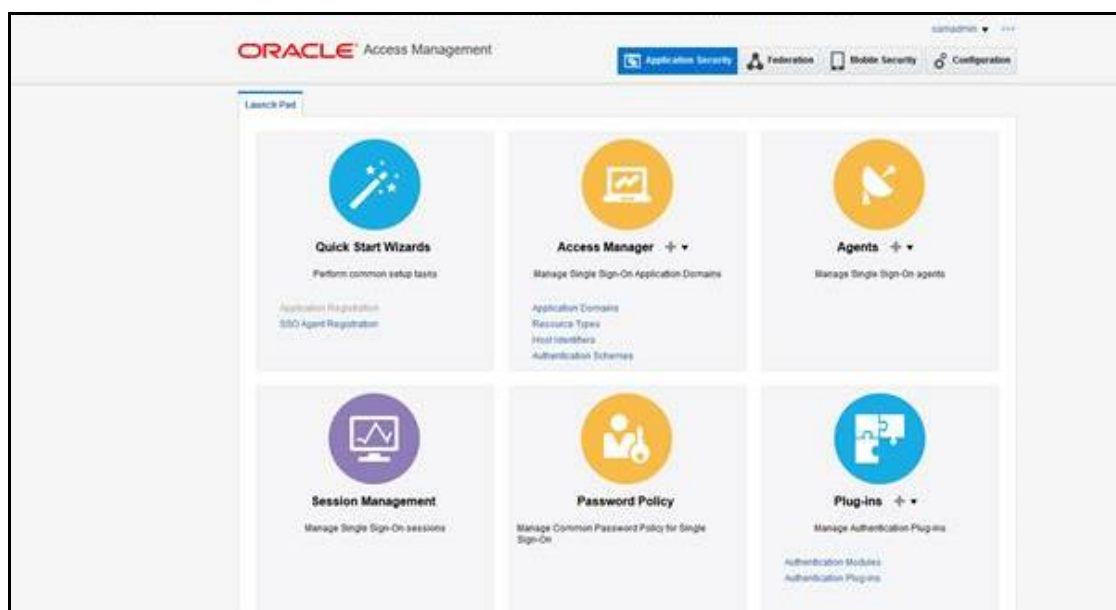


Figure 18: Application Security Launch Pad

- Click the **Application Domains** link in the **Access Manager** section. The **Application Domain** tab appears.

The screenshot shows the 'Application Domain' tab in the 'Access Manager' section. It features a search bar with a 'Name' input field and 'Search' and 'Reset' buttons. A 'Create Application Domain' button is in the top right. Below the search bar, there's a 'Search Results' section with a table header: 'Row', 'Name', and 'Description'. The table currently shows 'No data to display.' Above the table, there are action buttons: '+ Create', 'Edit', 'Delete', and 'Detach'.

Figure 19: Application Domain Tab

- Search for the required application domain in the **Application Domain** tab.
- In the **Search Results** section, click the link in the **Name** column corresponding to the application domain whose resources you want to protect using the authentication policy.

The screenshot shows the 'Webgate_IDM_DEV_11g' Application Domain page. It has a breadcrumb 'Access Manager >' and a title 'Webgate_IDM_DEV_11g Application Domain'. Below the title is a description: 'Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.' There are tabs for 'Summary', 'Resources', 'Authentication Policies', 'Authorization Policies', 'Token Issuance Policies', and 'Administration'. The 'Summary' tab is active. It contains fields for 'Name' (Webgate_IDM_DEV_11g) and 'Description' (Application Domain created through Remote Regis). There's a 'Session Idle Timeout (minutes)' field set to 0. At the bottom, there are three checkboxes: 'Allow OAuth Token', 'Allow Session Impersonation', and 'Enable Policy Ordering'. An 'Apply' button is in the top right.

Figure 20: {Application Domain} – Summary Tab

- Click the **Authentication Policies** tab. The **Authentication Policies** tab appears.

Access Manager >

Webgate_IDM_11g Application Domain

Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

Summary Resources **Authentication Policies** Authorization Policies Token Issuance Policies Administration

Select an existing Authentication Policy from the list or click the Create Authentication Policy button to create a new one.

Actions View **Create** Duplicate Edit Delete Detach

Row	Name	Description
1	Public Resource Policy	Policy set during domain creation. Add resources to this policy to allow anyone access.
2	Protected Resource Policy	Policy set during domain creation. Add resources to this policy to protect them.

Figure 21: {Application Domain} – Authentication Policies Tab

- Click the **Protected Resource Policy** link in the **Name** column. The **{Application Domain}: Protected Resource Policy** tab appears.

Launch Pad Application Domain x Webgate_IDM_11g x **Webgate_IDM_11g : Protect...** 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 trust for Access Manager to grant access. A policy can be defined to protect one or more resources in the Application Domain.

* Name Protected Resource Policy Success URL

Description Policy set during domain creation. Add resources to this policy to protect them. Failure URL

* Authentication Scheme LDAPScheme

Resources Responses Advanced Rules

Resources + Add X Delete			
Resource Type	Host Identifier	Resource URL	Query String
HTTP	IAMSuiteAgent	/**	

Figure 22: {Application Domain}: Protected Resource Policy Tab

- Click the **Advanced Rules** tab. The **Advanced Rules** tab appears.

Launch Pad Application Domain x Webgate_IDM_DEV_11g x Webgate_IDM_DEV_11g : Pro... x

Access Manager >

Protected Resource Policy Authentication Policy

Duplicate Apply

Authentication Policy defines the type of verification that must be performed to provide a sufficient level of trust for Access Manager to grant access to the user making the request. A single policy can be defined to protect one or more resources in the Application Domain.

* Name Protected Resource Policy Success URL

Description Policy set during domain creation. Add resources to Failure URL

* Authentication Scheme LDAPScheme

Resources Responses **Advanced Rules**

Pre-Authentication Post-Authentication

View + Add Delete Top Up Down Bottom Detach

Order	Rule Name	Description
This Policy does not have any Pre-Authentication rules		

Figure 23: Advanced Rules Tab

- Click the **Post-Authentication** tab. The **Post-Authentication** tab appears.

Launch Pad Application Domain x Webgate_IDM_DEV_11g x Webgate_IDM_DEV_11g : Pro... x

Access Manager >

Protected Resource Policy Authentication Policy

Duplicate Apply

Authentication Policy defines the type of verification that must be performed to provide a sufficient level of trust for Access Manager to grant access to the user making the request. A single policy can be defined to protect one or more resources in the Application Domain.

* Name Protected Resource Policy Success URL

Description Policy set during domain creation. Add resources to Failure URL

* Authentication Scheme LDAPScheme

Resources Responses **Advanced Rules**

Pre-Authentication **Post-Authentication**

View + Add Delete Top Up Down Bottom Detach

Order	Rule Name	Description
This Policy does not have any Post-Authentication rules		

Figure 24: Post-Authentication Tab

- Click **Add** in the **Post-Authentication** tab. The **Add Rule** window appears.

The image shows a software window titled "Add Rule" with a close button (X) in the top right corner. Inside the window, there are several input fields and controls. At the top, there is a field for "Rule Name" with an asterisk (*) indicating it is required. Below it is a "Description" field. Further down is a larger field for "Condition" with an asterisk (*) indicating it is required. Below the condition field, there is a "Deny Access" checkbox. Underneath that, there is a label "If condition is true" followed by a field for "Switch Authentication Scheme to" with an asterisk (*) indicating it is required. This field has a dropdown arrow on its right side. At the bottom right of the window, there are two buttons: "Add" and "Cancel".

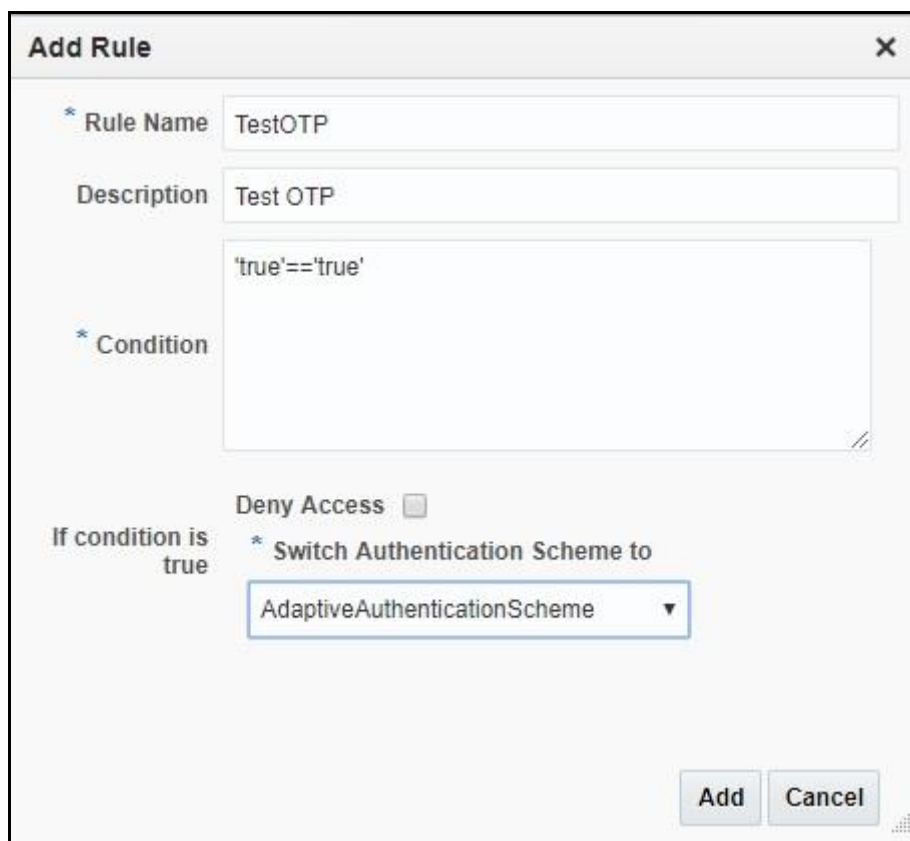
Figure 25: Add Rule Window

11. Create a rule with the following condition:

'true'=='true'

Note: It indicates that OTP should be generated and sent through the email when the first factor authentication is successful.

12. Select the **AdaptiveAuthenticationScheme** option from the **If condition is true** list.



The image shows a dialog box titled "Add Rule" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- * Rule Name:** A text input field containing "TestOTP".
- Description:** A text input field containing "Test OTP".
- * Condition:** A large text area containing the expression "'true'=='true'".
- Deny Access:** A checkbox that is currently unchecked.
- If condition is true:** A label positioned to the left of the "Switch Authentication Scheme to" dropdown.
- * Switch Authentication Scheme to:** A dropdown menu with "AdaptiveAuthenticationScheme" selected.
- Buttons:** "Add" and "Cancel" buttons are located at the bottom right of the dialog.

Figure 26: Adding a Rule

13. Click **Add**. The rule appears in the **Post-Authentication** tab.
14. Click **Apply**.

4. Verifying Multi-factor Authentication

Once you setup the multi-factor authentication, you need to verify whether the first and second factor authentication is working properly for ORMB.

To verify the multi-factor authentication:

1. Login to Oracle Revenue Management and Billing. The **Oracle Access Manager Welcome** screen appears.

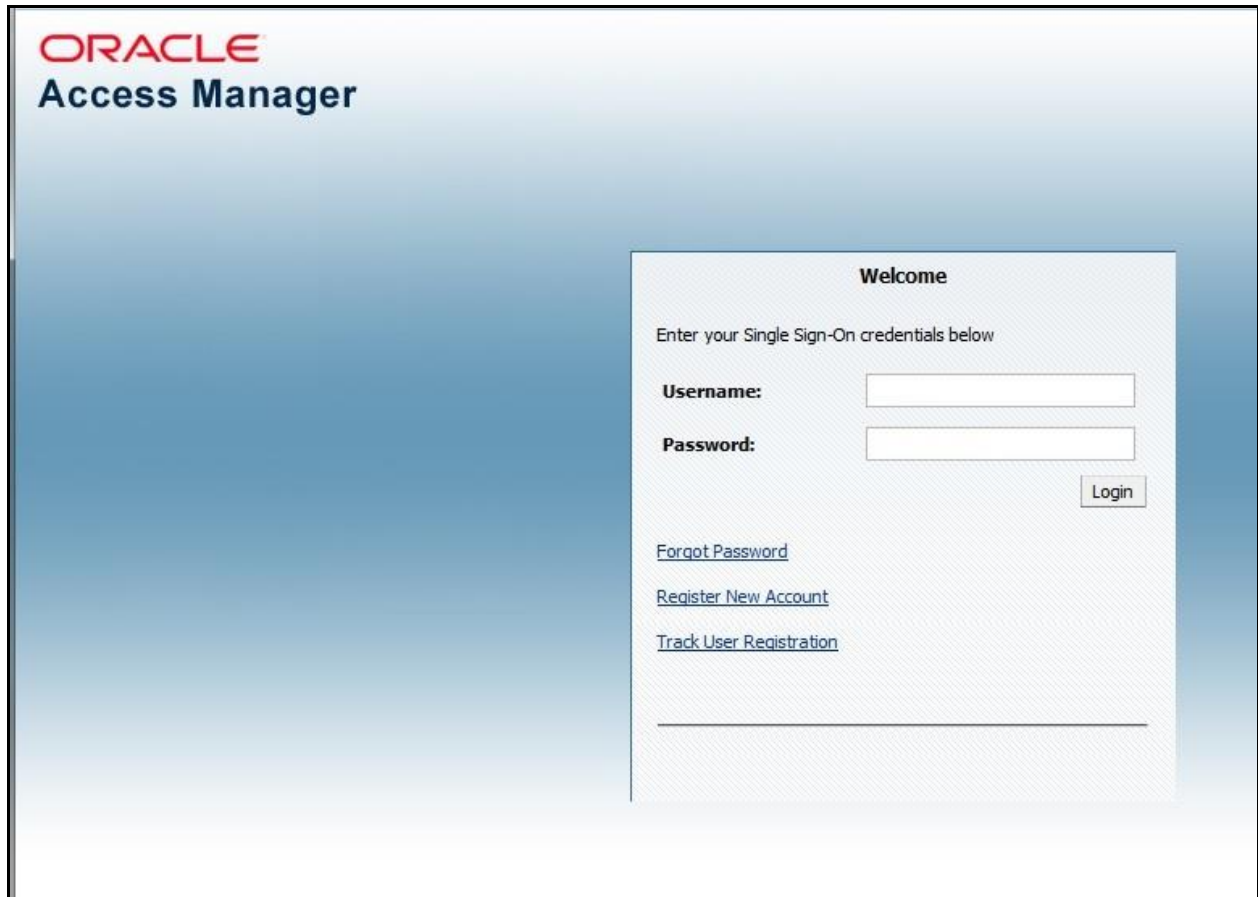


Figure 27: Oracle Access Manager Welcome Screen

2. Enter the user name and password in the respective fields.
3. Click **Login**. The **Second Factor Authentication** screen appears.

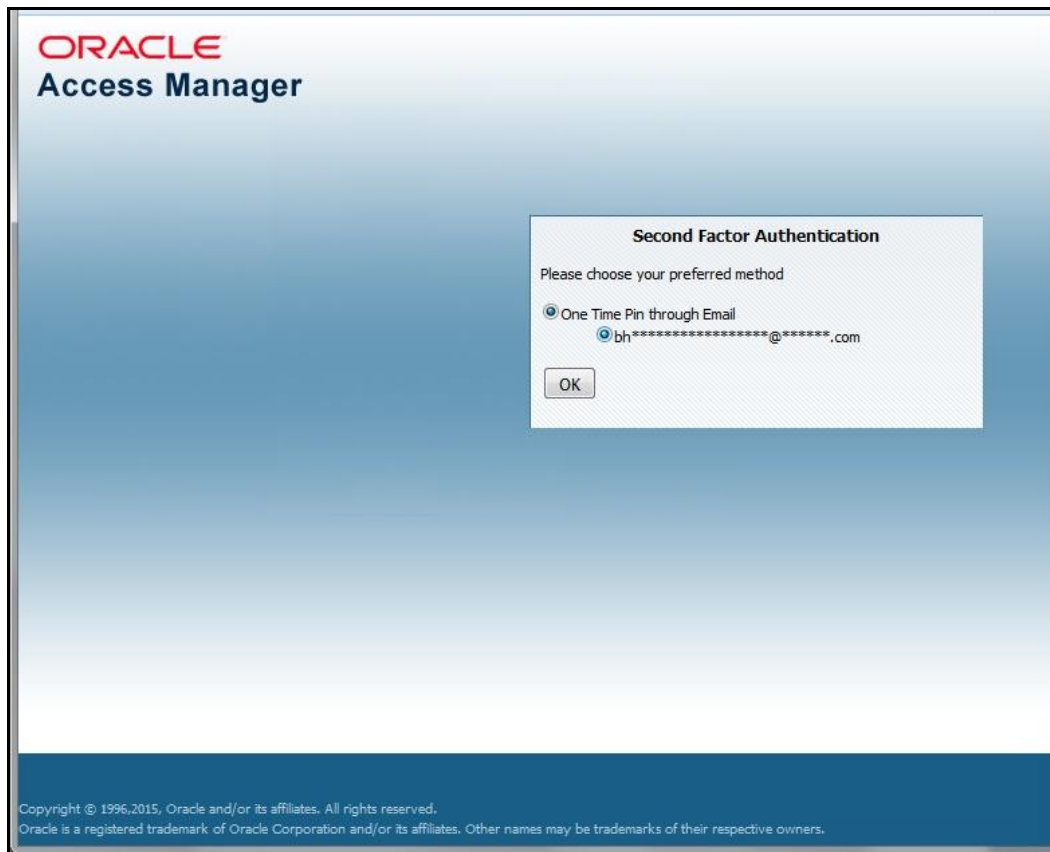


Figure 28: Second Factor Authentication Screen

4. Ensure that the **One Time Pin through Email** option is selected.
5. Click **OK**. The **Second Factor Authentication** screen appears where you can enter the One Time Pin (OTP) which you have received through an email.



Figure 29: Second Factor Authentication – One Time Pin

6. Enter the One Time Pin (OTP) and then click **Login**. The **Oracle Revenue Management and Billing** window appears.