SafeNet Agent for Oracle Access Manager (R2 & R3) and 12c 1.2.2

INSTALLATION AND CONFIGURATION GUIDE

Document Information

Product Version	1.2.2
Document Part Number	007-013752-001, Rev. E
Release Date	June 2021

Trademarks, Copyrights, and Third-Party Software

Disclaimer

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as “Thales”) information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

> The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.

> This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make **any change or** improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

PREFACE

This document describes how to install and configure the SafeNet Agent for Oracle Access Manager (OAM) R2 & R3 and 12c versions.

Customer Release Notes

The Customer Release Notes (CRN) document provides important information about this release that is not included in other customer documentation. It is strongly recommended that you read the CRN to fully understand the capabilities, limitations, and known issues for this release.

Audience

This document is targeted at system administrators who are familiar with OAM and are interested in adding Multi-Factor Authentication (MFA) capabilities using the SafeNet solution.

All products manufactured and distributed by Thales are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Oracle Access Manager (OAM) R2 & R3 and 12c versions.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Document Conventions

This section describes the conventions used in this document.

Command Syntax and Typeface Conventions

This document uses the following conventions for command syntax descriptions, and to highlight elements of the user interface.

Convention	Description
bold	The bold attribute is used to indicate the following: > Command-line commands and options (Type **dir /p**.) > Button names (Click **Save As**.)

	> Check box and radio button names (Select the **Print Duplex** check box.) > Window titles (On the **Protect Document** window, click **Yes**.) > Field names (**User Name:** Enter the name of the user.) > Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) > User input (In the **Date** box, type **April 1**.)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
Double quote marks	Double quote marks enclose references to other sections within the document. For example: Refer to "**Error! Reference source not found.**" on page **Error! Bookmark not defined.**.
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[optional] [<optional>]	Square brackets enclose optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
[a | b | c] [<a> | <b> | <c>]	Square brackets enclose optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

{ a | b | c }
{ <a> | <b> | <c> }
	Braces enclose required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.

Notifications and Alerts

Notifications and alerts are used to highlight important information or alert you to the potential for data loss or personal injury.

Tips

Tips are used to highlight information that helps to complete a task more efficiently.

> **TIP:** This is some information that will allow you to complete your task more efficiently.

Notes

Notes are used to highlight important or helpful information.

> **NOTE:** Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss.

> **CAUTION!** Exercise caution. Contains important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury.

> ****WARNING** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.**

Related Documents

The following document contains related information:

- *SafeNet Agent for Oracle Access Manager 1.2.2: Customer Release Notes*

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click the **REGISTER** link.

Telephone Support

The support portal also lists telephone numbers for voice contact (Contact Us).

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.

CHAPTER 1: Introduction

Overview

Authentication is the process of proving that a user is who he or she claims to be. An Access System enables the user to configure authentication rules in the policy domains that protect the resources. Authentication rules contain authentication schemes, which provide the methods for performing verification of a user's identity.

The Oracle Access Manager (OAM) delivers risk-aware, end-to-end user authentication, single sign-on, and authorization protection, providing enterprises with secure access from mobile devices and seamless integration of social identities with applications.

The SafeNet MFA solution delivers fully automated, highly secure authentication-as-a-service, with flexible token options tailored to the unique needs of your organization, substantially reducing the total cost of operation.

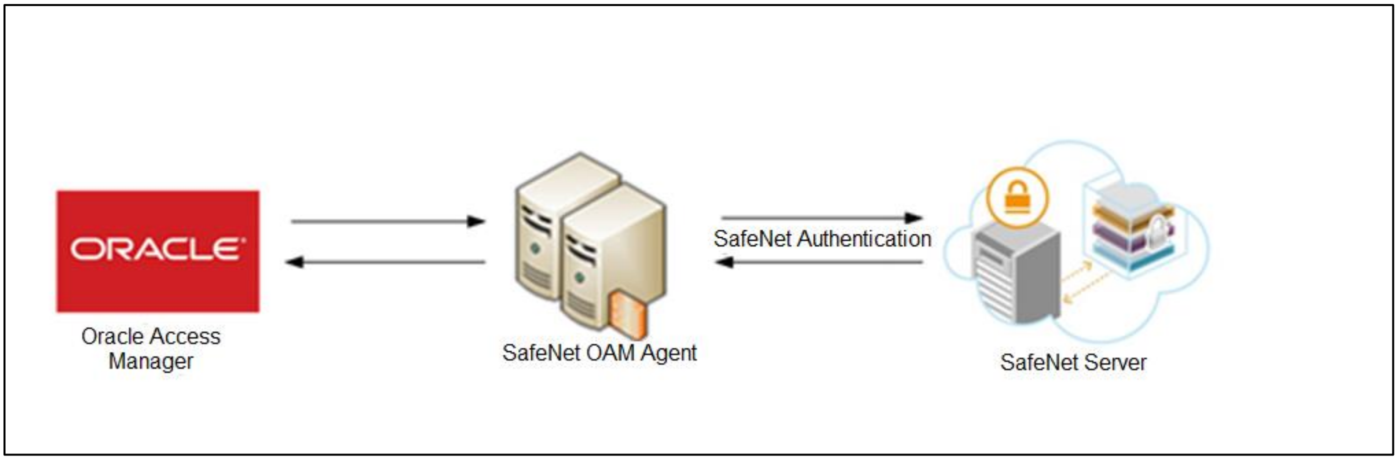
Strong authentication is made easy through the flexibility and scalability of SafeNet's automated workflows, vendor-agnostic token integrations, and broad APIs. In addition, management capabilities and processes are fully automated and customizable—providing a seamless and enhanced user experience.

The SafeNet solution enables a quick migration to a multi-tier, multi-tenant cloud environment, protecting everything, from cloud-based and on-premises applications to networks, users, and devices.

This document describes how to:

- Deploy Multi-Factor Authentication (MFA) in OAM (R2 or R3) or 12c using One-Time Password (OTP) or Challenge-Response authenticators, managed by the SafeNet solution.
- Deploy and configure OAM (R2 or R3) or 12c using the SafeNet Agent.

The following diagram illustrates the logical flow to implement SafeNet authentication on OAM (R2 or R3) and 12c:



> **NOTE:** If you are using an Active Directory (AD) to authenticate user credentials, the SafeNet can be integrated with Active Directory Federation Services (AD FS) infrastructure, by using an agent called SafeNet Agent for AD FS. To know more about the SafeNet Agent for AD FS, visit the SafeNet Authentication Service Downloads page.

Prerequisites

- It is assumed that the OAM environment is already configured and working with LDAP passwords, prior to implementing MFA using the SafeNet solution.
- The administrator must have rights/permissions to access OAM user accounts.
- Remove the below Bouncy Castle related jars from `/home/oracle/Oracle/Middleware/Oracle_Home/oracle_common/modules/thirdparty`

  `bcprov-ext-jdk15on-1.60.jar`

  `bcprov-jdk15on-1.60.jar`

> **NOTE:** You need to do this only in case of 12c version.

Applicability

The information in this document applies to the following:

> **SafeNet Authentication Service - Service Provider Edition (SAS SPE)** — The on-premises, server version targeted at service providers interested in hosting SafeNet in their data center(s).

> **SafeNet Authentication Service - Private Cloud Edition (SAS PCE)** — The on-premises, server version targeted at organizations interested in hosting SafeNet in their private cloud environment.

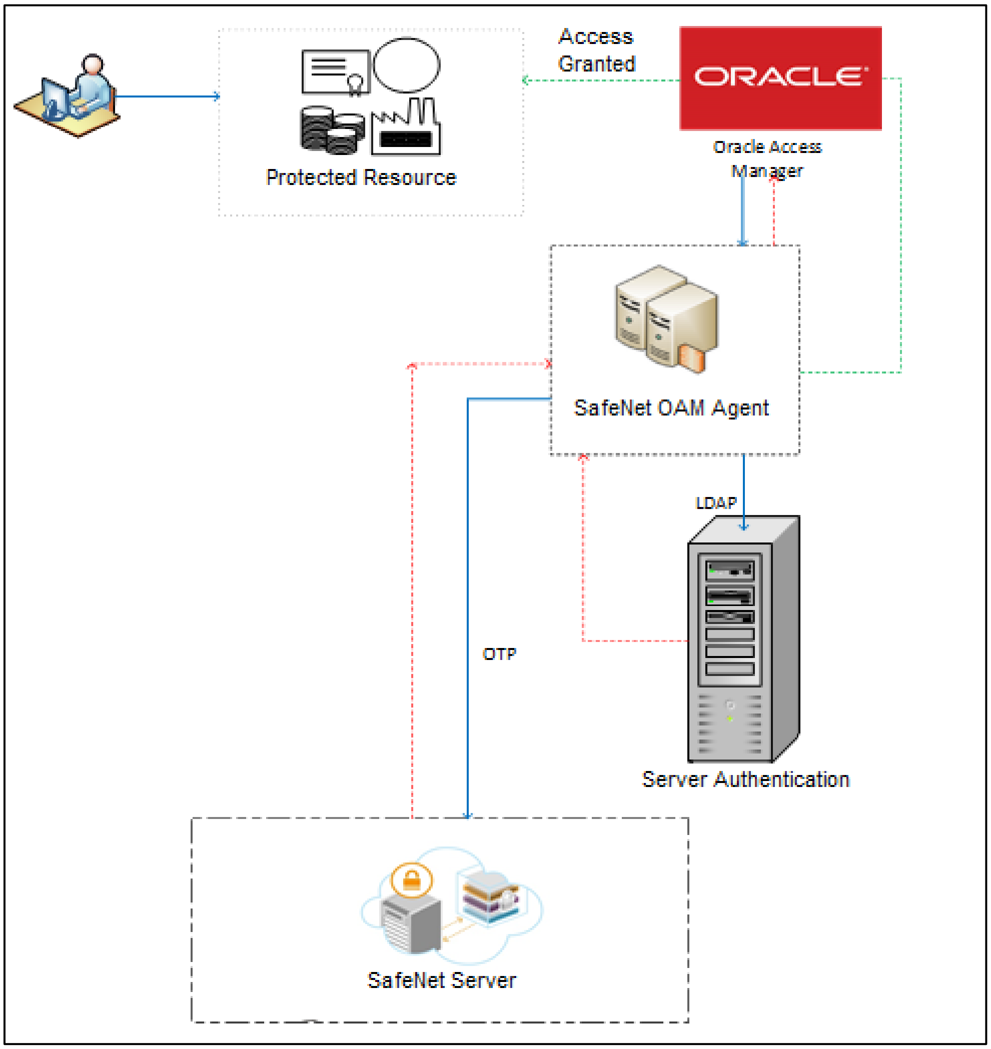
> **SafeNet Trusted Access (earlier, SAS Cloud)** — The SafeNet's cloud-based authentication service.

> **Oracle Access Manager (OAM)** – R2 & R3 and 12c versions.

Multi-Factor Authentication

The SafeNet Agent for OAM is an MFA adapter that provides a way to authenticate users using SafeNet as a secondary authenticator. The following steps broadly illustrate the flow of an MFA transaction for OAM using the SafeNet Agent.

1. The user attempts to access a resource which is protected with OAM.
2. The OAM displays the SafeNet Agent login page.
3. The user enters his or her credentials (for example, LDAP and OTP).
4. The SafeNet Agent validates OTP.
5. The LDAP credentials are then verified against the configured LDAP server. After successful validation, the user is redirected to access the protected resource.


Protected Resource
Access
Granted
ORACLE
Oracle Access
Manager
SafeNet OAM Agent
LDAP
OTP
Server Authentication
SafeNet Server

CHAPTER 2: Oracle Access Manager Configuration for R2 Version

To install and configure the SafeNet Agent on OAM (R2), follow the steps:

1. Installing SafeNet Agent Plugin
2. Configuring the .ini File of the SafeNet Agent
3. Importing the SafeNet Agent Plugin Using the Oracle Access Manager Console
4. Creating an Authentication Module
5. Creating the Authentication Scheme
6. Forcing the SafeNet Agent Authentication Scheme on a Protected Resource
7. Configuring the WebLogic Server
8. Deploying the Agent on the WebLogic Server

> **NOTE:** Before proceeding, make sure you back up your OAM configuration.
>
> In case you have any issues, you can always roll back OAM/WLS configuration files to restore OAM to its original state. All XML files can be located at:
>
> **`/apps/FMW/Middleware/user_projects/domains/oam/config`**
>
> The **config.xml** file must be backed up.
> You can find both applications on the same physical server.

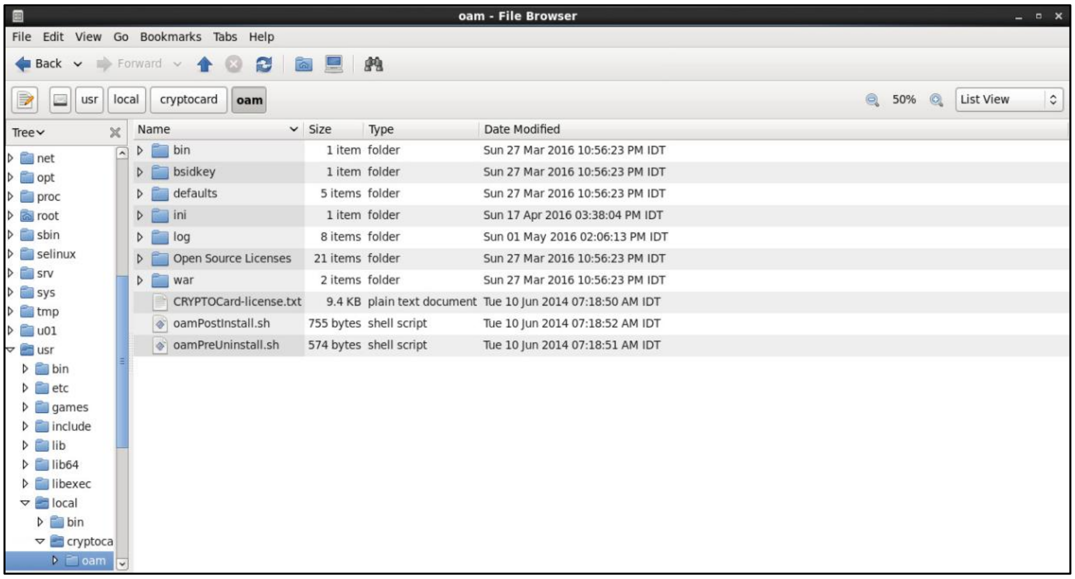
Installing SafeNet Agent Plugin

Install the SafeNet Agent `rpm`.

1. Run the following command:

   ```
   rpm –ivh SafeNet-Agent-For-OAM-[your installation build].rpm
   ```

2. The installation package will be installed at the following location: `/usr/local/cryptocard/oam/`



Name	Size	Type	Date Modified
bin	1 item	folder	Sun 27 Mar 2016 10:56:23 PM IDT
bsidkey	1 item	folder	Sun 27 Mar 2016 10:56:23 PM IDT
defaults	5 items	folder	Sun 27 Mar 2016 10:56:23 PM IDT
ini	1 item	folder	Sun 17 Apr 2016 03:38:04 PM IDT
log	8 items	folder	Sun 01 May 2016 02:06:13 PM IDT
Open Source Licenses	21 items	folder	Sun 27 Mar 2016 10:56:23 PM IDT
war	2 items	folder	Sun 27 Mar 2016 10:56:23 PM IDT
CRYPTOCard-license.txt	9.4 KB	plain text document	Tue 10 Jun 2014 07:18:50 AM IDT
oamPostInstall.sh	755 bytes	shell script	Tue 10 Jun 2014 07:18:52 AM IDT
oamPreUninstall.sh	574 bytes	shell script	Tue 10 Jun 2014 07:18:51 AM IDT

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

NOTE: The administrator must have rights/permissions to access OAM user accounts.

Configuring .ini File

Modify the .ini file of the SafeNet Agent by adding details such as BSID server details, protocol, and others. Configure following variables in the `/usr/local/cryptocard/oam/ini/JCryptoWrapper.ini` file:

PrimaryProtocol	Select **http/https**.
PrimaryServer	Enter the primary SafeNet server host.
PrimaryServerPort	Enter the port number (for example, **80/443**).
SecondaryProtocol	Select **http/https**.
SecondaryServer	Enter the secondary SafeNet server host.
SecondaryServerPort	Enter the port number (for example, **80/443**).
LogLevel	Select level of the log that will be created. By default, the value is set to 3, in a range of 1-5, with 1 being the lowest and 5 being the highest level. The higher the log level is, the more detailed information it contains. Each log level also contains information for all its following log levels.
REDIRECT-LOCATION-AFTER-AUTHENTICATION	Enter the OAM redirection URL (For example, http://<iamdemo.oracle.com>:14100/oam/server/auth_cred_submit).

OTP_LOGIN_PAGE	Set to False, if all three inputs (User Name, LDAP Password and OTP) must be required for SafeNet server authentication, even after LDAP authentication. Default value: True
USER_LOGIN_ID_NAME	Required only if **OTP_LOGIN_PAGE** is set as True. Set name of cookie variable to provide LDAP User Name. Default value: **USER_ID** (can be set to any other value, but this value must match the **Cookie name value** set in Cookie Settings for Step-Up Authentication section.
IGNORE_CERTIFICATE_ERRORS	This parameter is only valid for the **HTTPS** protocol. Default Value: **0** The value **0** ensures that the security certificate checks will be forced while communicating with SafeNet Servers. This setting is recommended if the SafeNet server is in use. If set to **1**, the certificate checks will be ignored. This setting is recommended for in-house SafeNet server deployments, with self-signed certificates. If the setting is changed back to **0** (from **1**), ensure that the SafeNet server (in use) has a valid certificate.

> **NOTE:** If your organization uses a proxy server to access extranet or intranet, you must also configure the proxy settings in the .ini file. The agent software works only with HTTP proxy (basic or anonymous authentication). Any settings changed (at any time) require a Web Logic Server (WLS) and OAM restart.

Agent Encryption Key File

The agent encryption key file is used to encrypt/decrypt the data. By default, the key file is available at the following location:

```
/usr/local/cryptocard/oam/bsidkey
```

If you are moving from one SafeNet server version to another, the key file can be downloaded by following the steps:

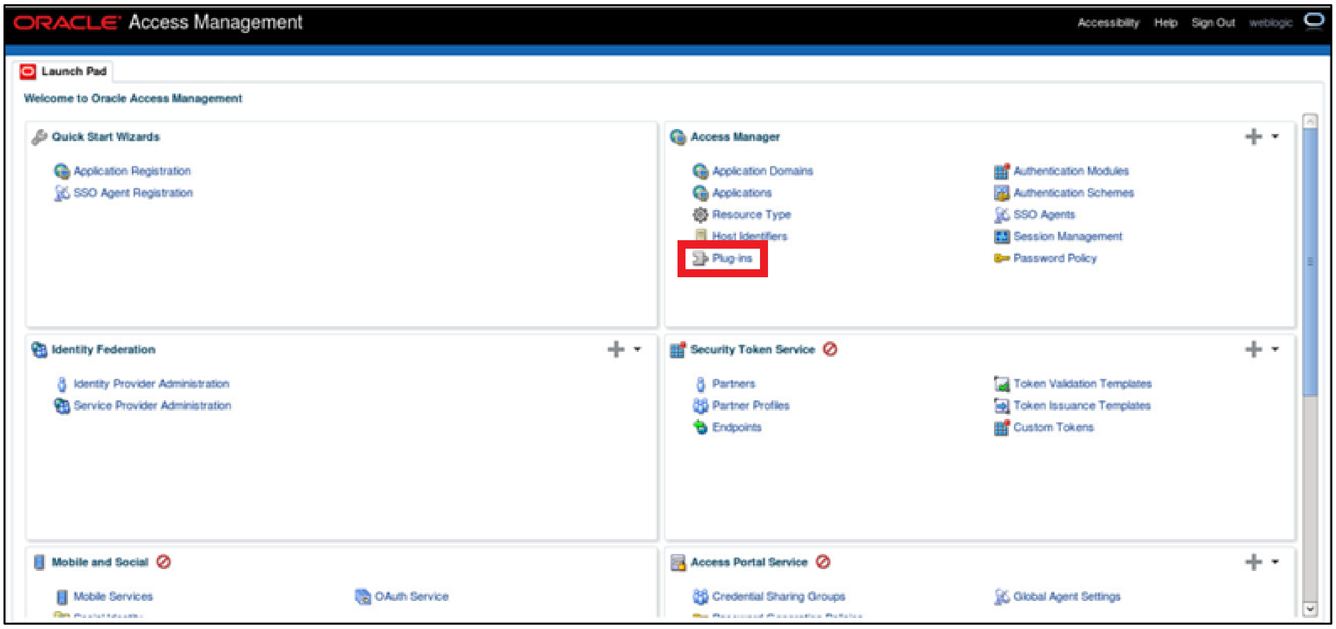
1. Login to SafeNet account, and navigate to **COMMS** > **Authentication Processing** section.
2. Under the **Task** list, click **Authentication Agent Settings** link and download the key.

> **NOTE:** The key file must be kept at a location accessible by all the authorized users.

Importing SafeNet Agent Plugin

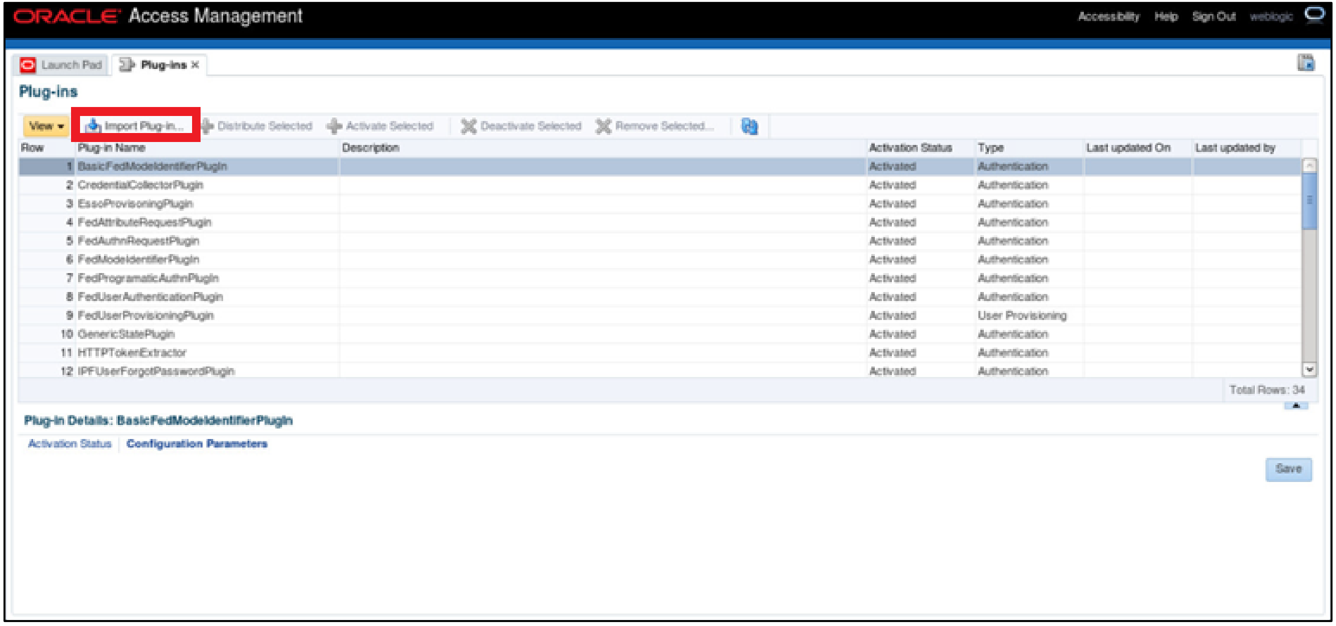
In this section, you will import the SafeNet Agent Plugin to the OAM, using the Oracle Access Management portal.

1. Login to Oracle Access Management portal as an administrator.
2. Under **Access Manager**, click **Plug-ins**.



(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

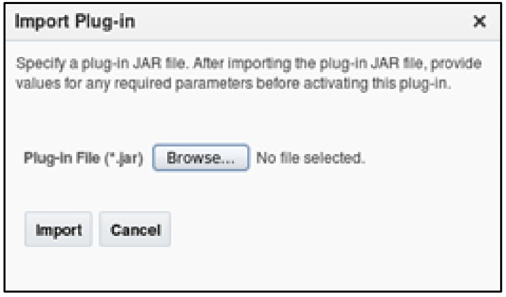
3. On the **Plug-ins** tab, click **Import Plug-in**.



Row	Plug-in Name	Description	Activation Status	Type	Last updated On	Last updated by
1	BasicFedModelIdentifierPlugin		Activated	Authentication		
2	CredentialCollectorPlugin		Activated	Authentication		
3	EssoProvisioningPlugin		Activated	Authentication		
4	FedAttributeRequestPlugin		Activated	Authentication		
5	FedAuthnRequestPlugin		Activated	Authentication		
6	FedModelIdentifierPlugin		Activated	Authentication		
7	FedProgramaticAuthnPlugin		Activated	Authentication		
8	FedUserAuthenticationPlugin		Activated	Authentication		
9	FedUserProvisioningPlugin		Activated	User Provisioning		
10	GenericStatePlugin		Activated	Authentication		
11	HTTPTokenExtractor		Activated	Authentication		
12	IPFUserForgotPasswordPlugin		Activated	Authentication		

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

4. The **Import Plug-in** popup window is displayed. Click **Browse**.

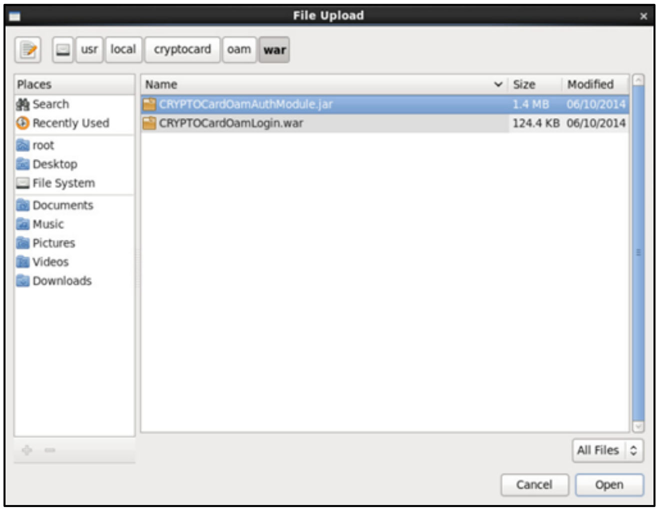


Specify a plug-in JAR file. After importing the plug-in JAR file, provide values for any required parameters before activating this plug-in.

Plug-in File (*.jar) Browse... No file selected.

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

5. On the **File Upload** window, select the agent.jar file (for example, `/usr/local/cryptocard/oam/war/CRYPTOCardOamAuthModule.jar`), and click **Open**.

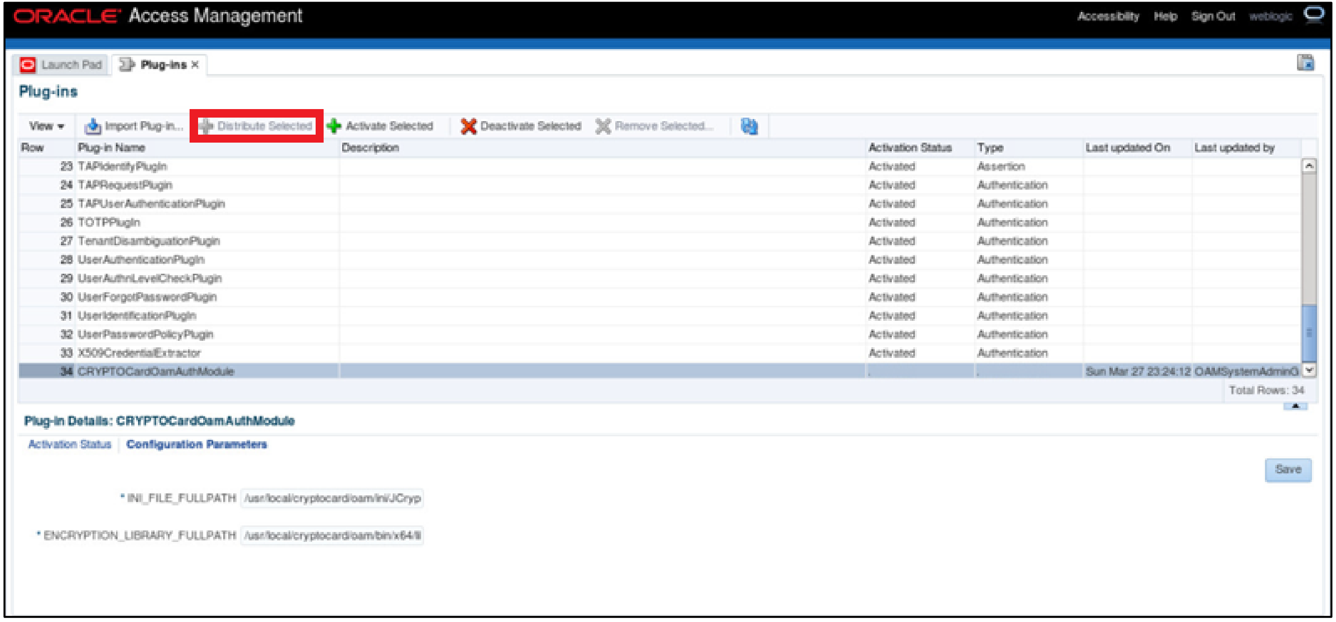


Name	Size	Modified
CRYPTOCardOamAuthModule.jar	1.4 MB	06/10/2014
CRYPTOCardOamLogin.war	124.4 KB	06/10/2014

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

6. On the **Import Plug-in** window, click **Import**.

7. The SafeNet Agent plugin is listed. Select the plug-in, and click **Distribute Selected**.



Row	Plug-in Name	Description	Activation Status	Type	Last updated On	Last updated by
23	TAPIdentifyPlugin		Activated	Assertion		
24	TAPRequestPlugin		Activated	Authentication		
25	TAPUserAuthenticationPlugin		Activated	Authentication		
26	TOTPPlugin		Activated	Authentication		
27	TenantDisambiguationPlugin		Activated	Authentication		
28	UserAuthenticationPlugin		Activated	Authentication		
29	UserAuthnLevelCheckPlugin		Activated	Authentication		
30	UserForgotPasswordPlugin		Activated	Authentication		
31	UserIdentificationPlugin		Activated	Authentication		
32	UserPasswordPolicyPlugin		Activated	Authentication		
33	X509CredentialExtractor		Activated	Authentication		
34	CRYPTOCardOamAuthModule		.	.	Sun Mar 27 23:24:12	OAMSystemAdminG

Total Rows: 34

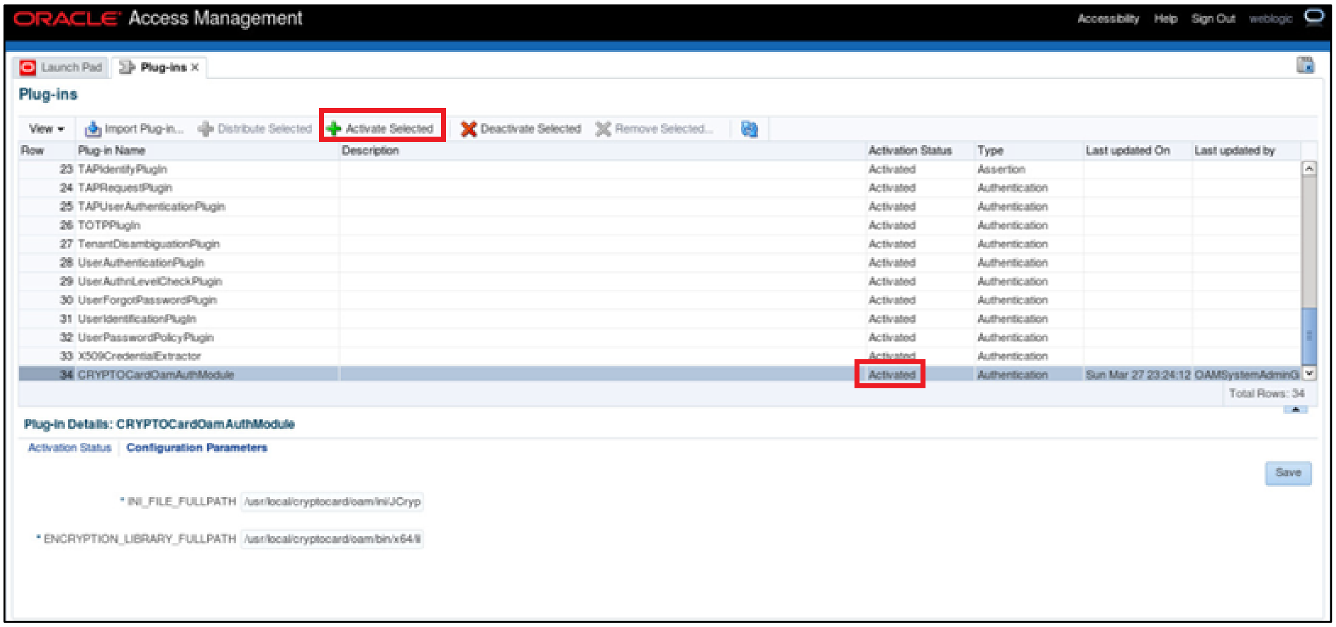
Plug-in Details: CRYPTOCardOamAuthModule

* INI_FILE_FULLPATH /usr/local/cryptocard/oam/ini/JCryp

* ENCRYPTION_LIBRARY_FULLPATH /usr/local/cryptocard/oam/bin/x64/li

(The screen image above is from Oracle Access Manager. Trademarks are the property of their respective owners.)

8. The **Activation Status** for the plug-in is populated to **Distributed**.
9. Select the SafeNet Agent plug-in, and click **Activate Selected**. The **Activation Status** is changed to **Activated**.



Row	Plug-in Name	Description	Activation Status	Type	Last updated On	Last updated by
23	TAPIdentifyPlugin		Activated	Assertion		
24	TAPRequestPlugin		Activated	Authentication		
25	TAPUserAuthenticationPlugin		Activated	Authentication		
26	TOTPPlugin		Activated	Authentication		
27	TenantDisambiguationPlugin		Activated	Authentication		
28	UserAuthenticationPlugin		Activated	Authentication		
29	UserAuthnLevelCheckPlugin		Activated	Authentication		
30	UserForgotPasswordPlugin		Activated	Authentication		
31	UserIdentificationPlugin		Activated	Authentication		
32	UserPasswordPolicyPlugin		Activated	Authentication		
33	X509CredentialExtractor		Activated	Authentication		
34	CRYPTOCardOamAuthModule		Activated	Authentication	Sun Mar 27 23:24:12	OAMSystemAdminG

Total Rows: 34

Plug-in Details: CRYPTOCardOamAuthModule

Activation Status | Configuration Parameters

Save

* INI_FILE_FULLPATH /usr/local/cryptocard/oam/ini/JCryp

* ENCRYPTION_LIBRARY_FULLPATH /usr/local/cryptocard/oam/bin/x64/l

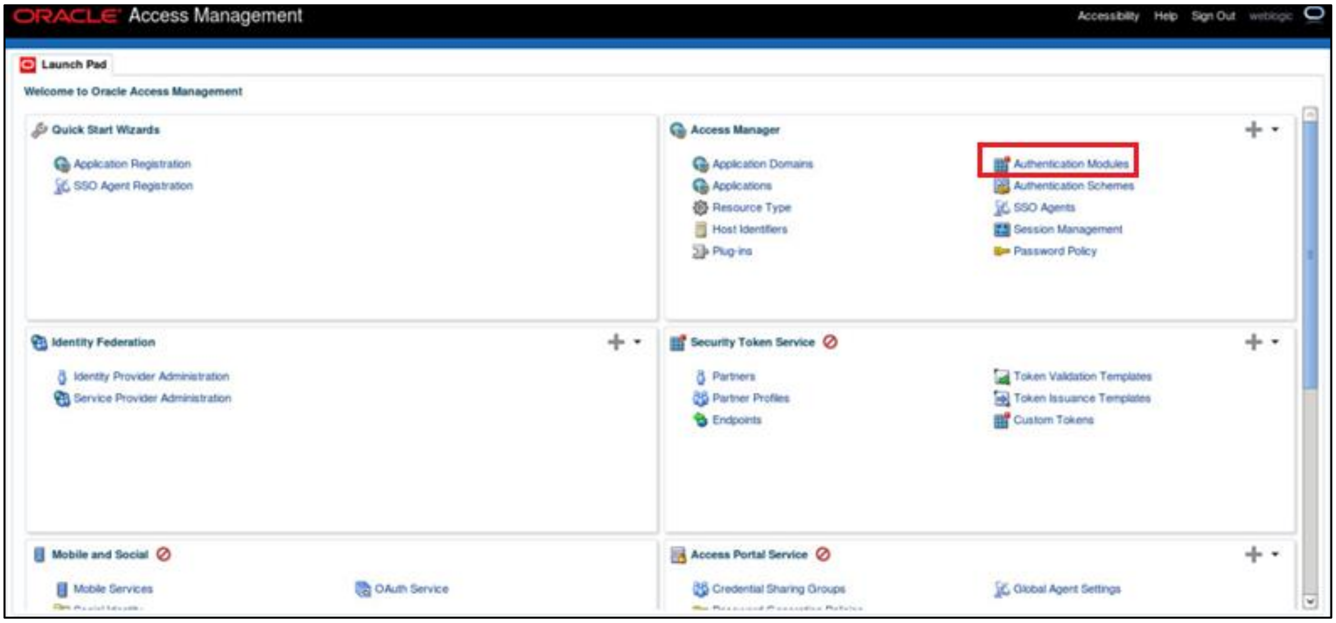
(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

> **NOTE:** If the plugin is not deployed at the default location, change the required plugin parameters (as shown previously) and set the appropriate parameters in the **.ini** file.

Creating Authentication Module

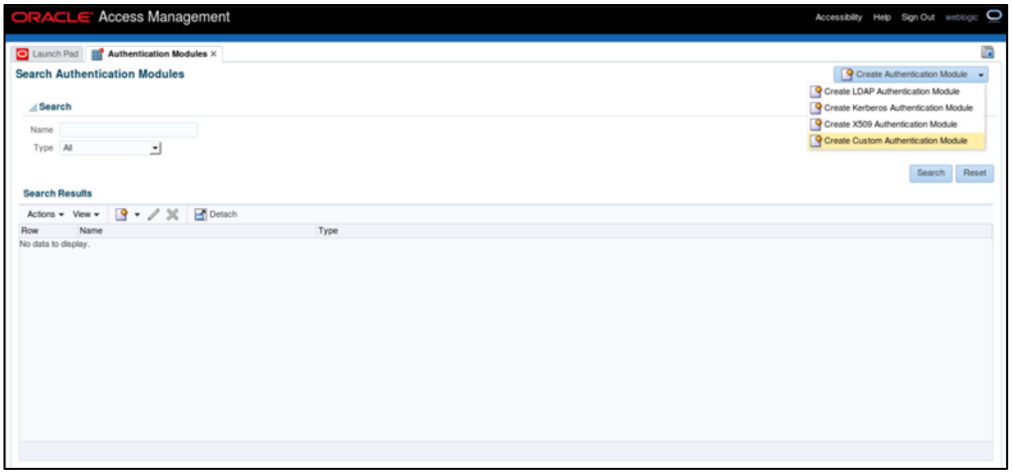
To define the type and order of the authentication, configure the authentication module. In the authentication module, you will configure the OTP authentication that will be used by the SafeNet Agent.

1. On the Oracle Access Management portal, under **Access Manager**, click **Authentication Modules**.



(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

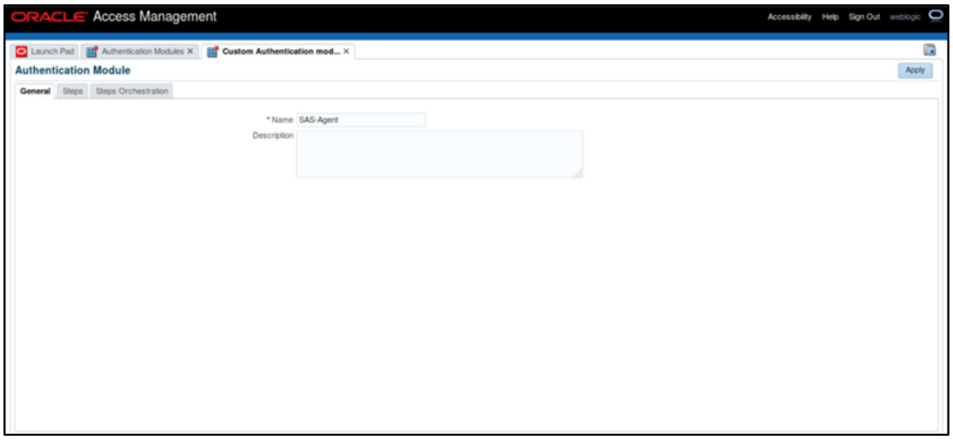
2. Click **Create Authentication Module** > **Create Custom Authentication Module**.


ORACLE Access Management
Accessibility
Help
Sign Out
weblogic
Launch Pad
Authentication Modules
Search Authentication Modules
Search
Name
Type
All
Create Authentication Module
Create LDAP Authentication Module
Create Kerberos Authentication Module
Create X509 Authentication Module
Create Custom Authentication Module
Search
Reset
Search Results
Actions
View
Detach
Row
Name
Type
No data to display.

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

3. On the **Authentication Module** window, on the **General** tab, complete the following fields:

Name	Enter a name for the module.
Description	Enter a description for the module, if required.

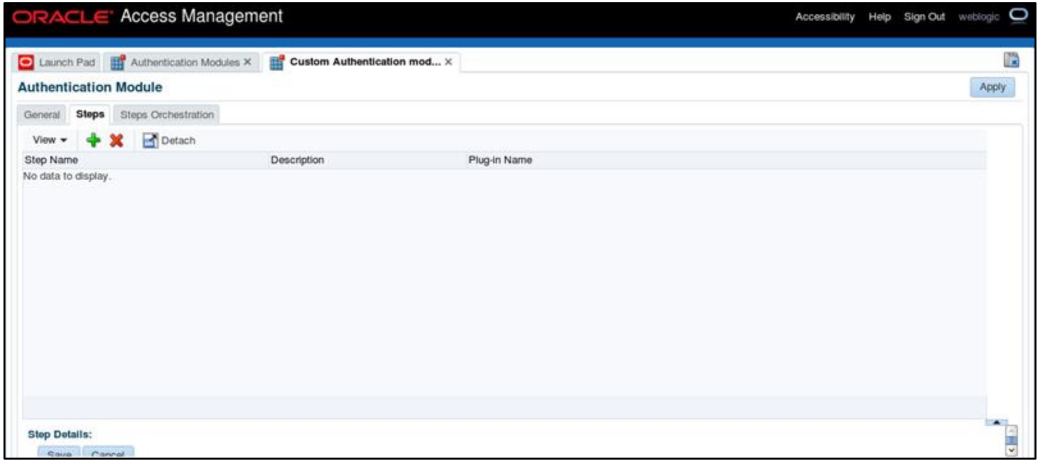


* Name SAS-Agent

Description

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

4. Click **Steps** tab, and click Create ✚ icon to add a new step to the authentication module.

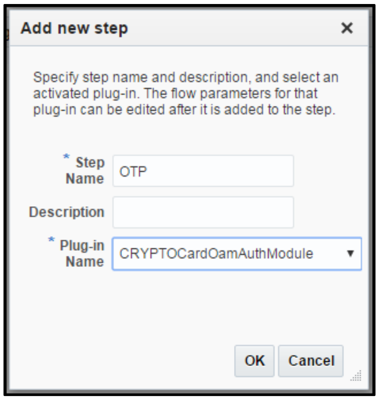


Step Name	Description	Plug-in Name
No data to display.		

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

5. Perform the following to configure OTP authentication:
On **Add new step** window, complete the following fields, and click **OK**.

Step Name	Enter a name for the module.
Plug-in Name	Select **CRYPTOCardOamAuthModule**.



Specify step name and description, and select an activated plug-in. The flow parameters for that plug-in can be edited after it is added to the step.

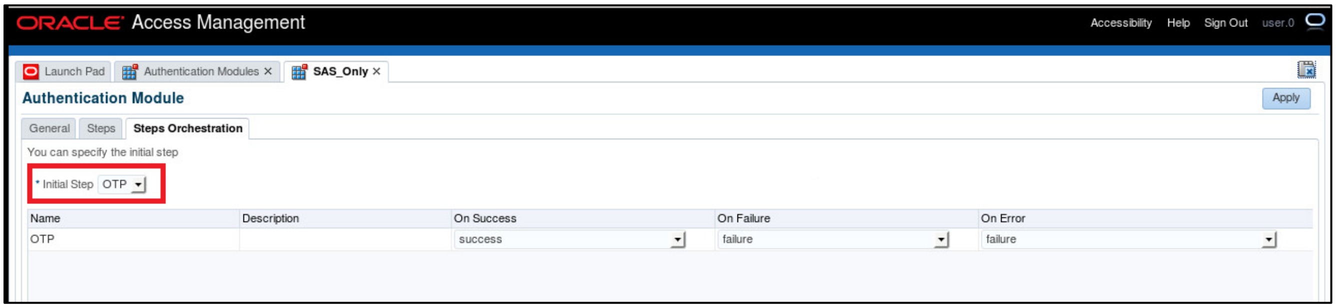
* Step Name OTP

Description

* Plug-in Name CRYPTOCardOamAuthModule

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

6. Click **Steps Orchestration** tab, and verify that in the **Initial Step** field, **OTP** option is selected. Also verify success, failure and error conditions, as illustrated in the screenshot below:



Authentication Module

You can specify the initial step

* Initial Step OTP

Name	Description	On Success	On Failure	On Error
OTP		success	failure	failure

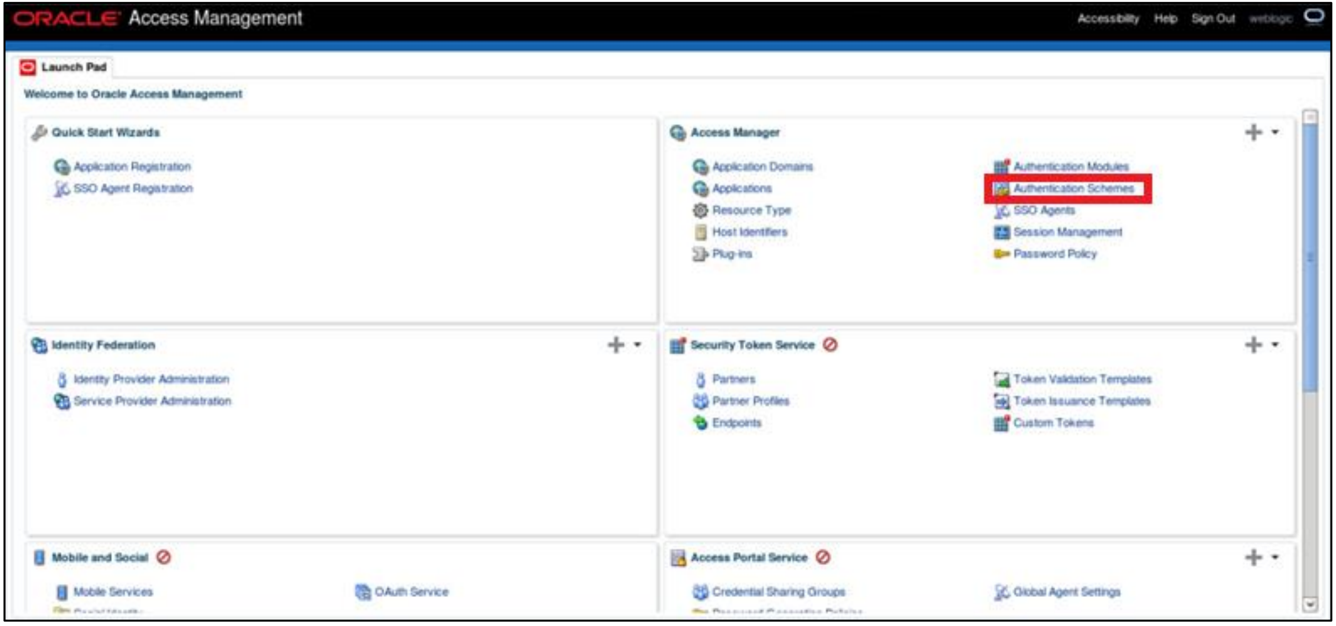
(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

7. Click **Apply**.

Creating Authentication Scheme

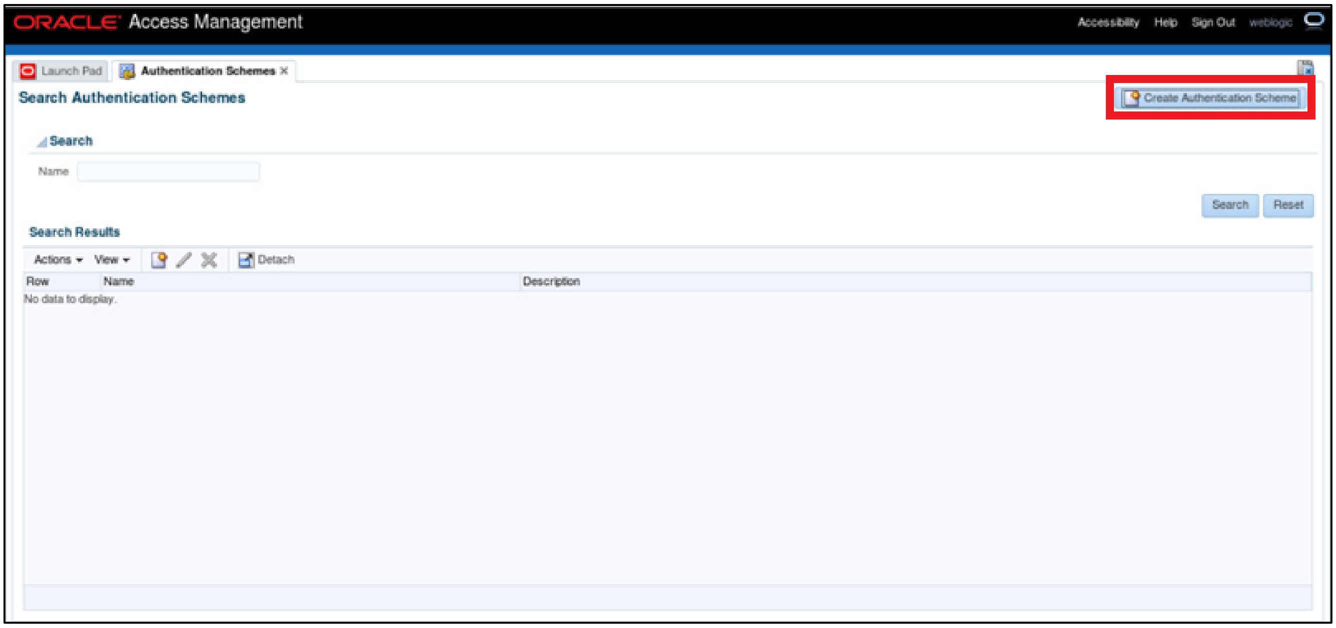
Create the authentication scheme that will use the authentication module created in the previous section.

1. On the Oracle Access Management portal, under **Access Manager**, click **Authentication Schemes**.



(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

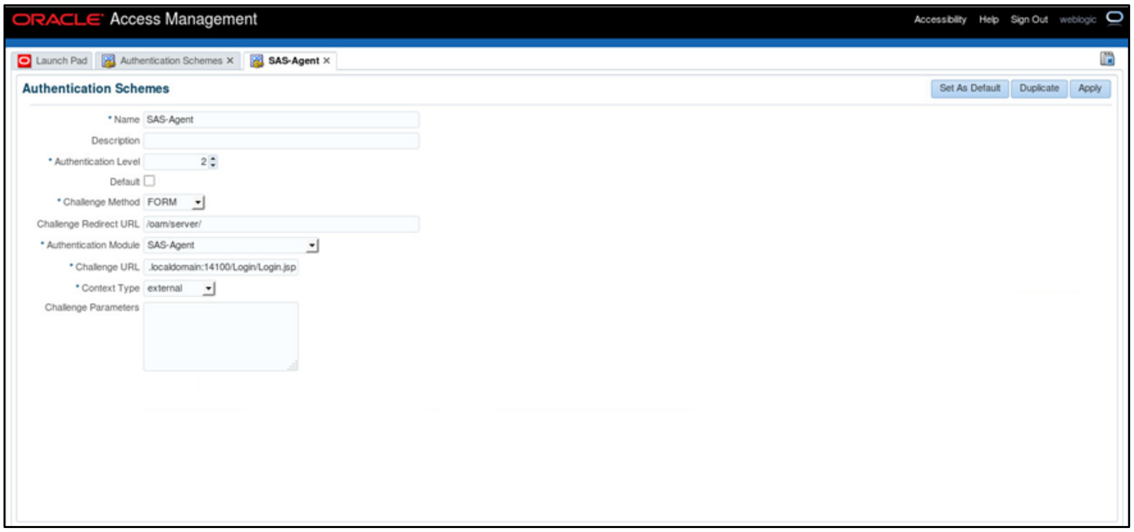
2. Click **Create Authentication Scheme**.



(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

3. Complete the following fields, and click **Apply**.

Name	Enter a name for the authentication scheme.
Authentication Level	Select **2**.
Challenge Method	Select **FORM**.
Challenge Redirect URL	Enter `/oam/server/`.
Authentication Module	Select the authentication module (for example, **SafeNet Agent**) that you created earlier (in step 3 of Creating Authentication Module).
Challenge URL	Enter URL of the credentials collector (for example, http://oamserver1.localdomain:14100/Login/Login.jsp).
Context Type	Select **external**.



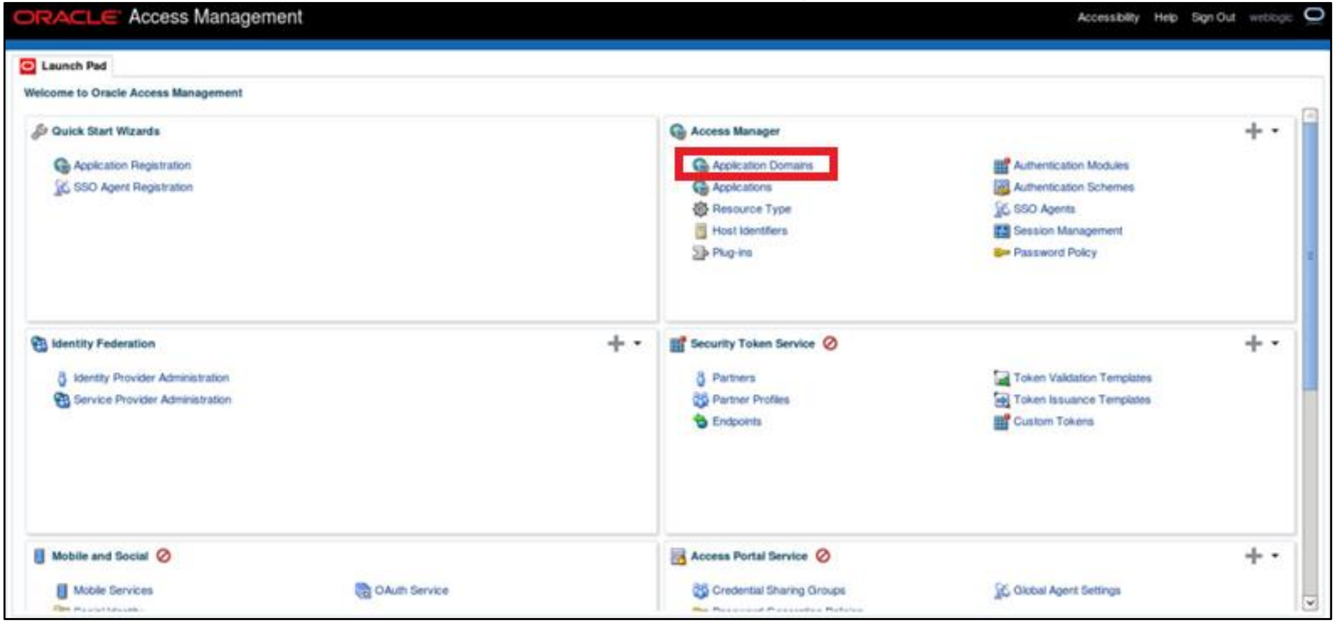
* Name: SAS-Agent
Description:
* Authentication Level: 2
Default: □
* Challenge Method: FORM
Challenge Redirect URL: /oam/server/
* Authentication Module: SAS-Agent
* Challenge URL: .localdomain:14100/Login/Login.jsp
* Context Type: external
Challenge Parameters:

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

Forcing Authentication Scheme on Protected Resource

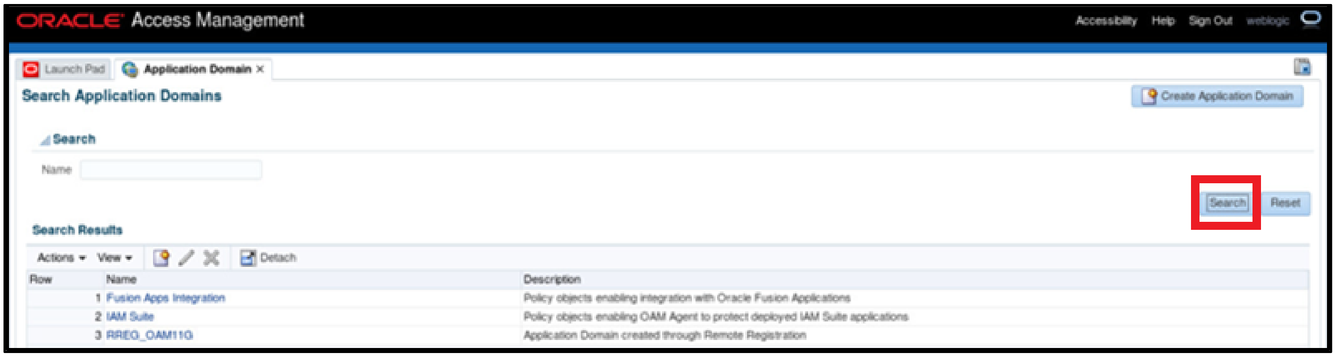
Force the SafeNet Agent authentication scheme on the protected resource in OAM. This will cause the client to immediately authenticate using the specified scheme.

1. On the Oracle Access Management portal, under **Access Manager**, click **Application Domains**.



(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

2. Click **Search**. Under **Search Results**, click the protected resource (for example, TestAgentDec).

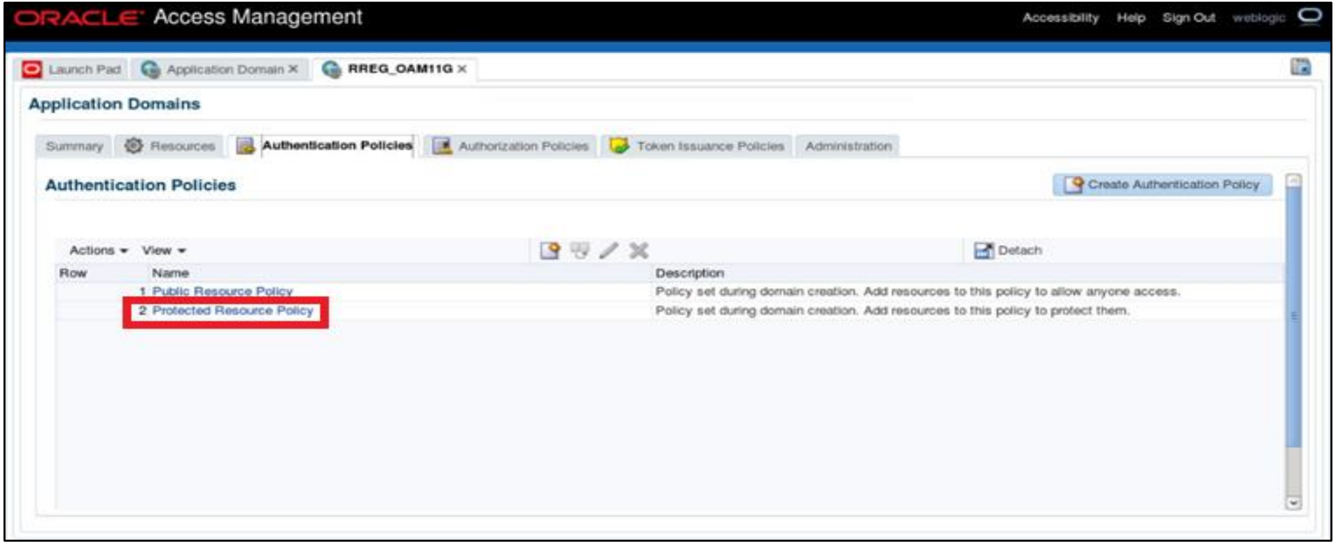


Name

Row	Name	Description
1	Fusion Apps Integration	Policy objects enabling integration with Oracle Fusion Applications
2	IAM Suite	Policy objects enabling OAM Agent to protect deployed IAM Suite applications
3	RREG_OAM11G	Application Domain created through Remote Registration

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

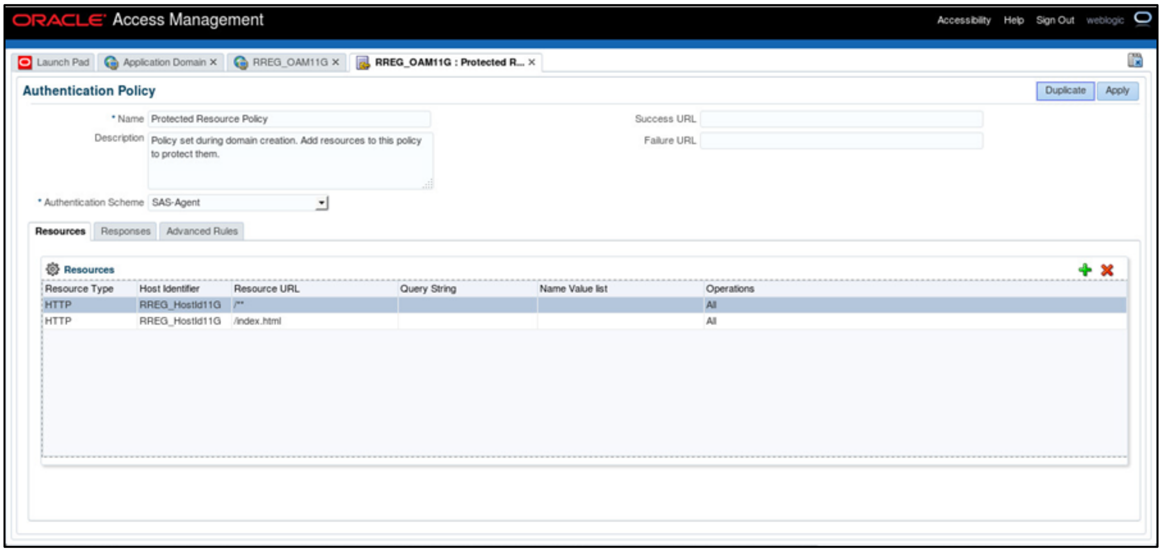
3. On **Authentication Policies** tab, click **Protected Resource Policy**.



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.

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

4. In **Authentication Scheme** field, select the authentication scheme (for example, **SafeNet Agent**), and click **Apply**.



* Name	Protected Resource Policy
Description	Policy set during domain creation. Add resources to this policy to protect them.
* Authentication Scheme	SAS-Agent
Success URL	
Failure URL	

Resource Type	Host Identifier	Resource URL	Query String	Name Value list	Operations
HTTP	RREG_HostId11G	/**			All
HTTP	RREG_HostId11G	/index.html			All

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

Configuring WebLogic Server

1. Login to Linux server hosting WLS using SSH.
2. Shut down the entire domain, including the WebLogic Admin server and all the OAM managed servers.
3. Create a backup of the existing file before editing.
4. In the `oam-config.xml` file, locate the version number that needs to be incremented by one to ensure that the changes are not overwritten by the console. The version number will occur near the top of the file.

```
<Setting xmlns="http://www.w3.org/2001/XMLSchema" Name="NGAMConfiguration"
Type="htf:map">

...

<Setting Name="Version" Type="xsd:integer">175</Setting>

...

</Setting>
```

5. Add the following XML code (if not already present):

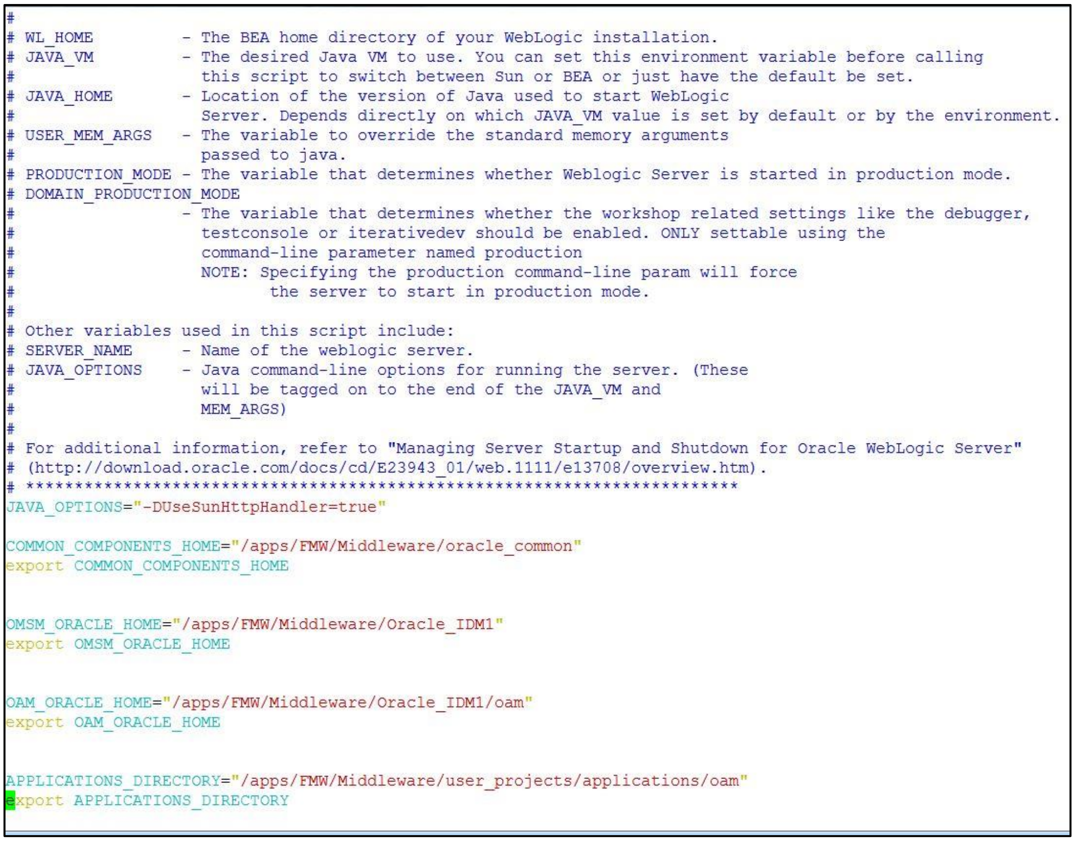
```
<Setting xmlns="http://www.w3.org/2001/XMLSchema" Name="NGAMConfiguration"
Type="htf:map">

...

<Setting Name="Server" Type="htf:map">

<Setting Name="NGAMServer" Type="htf:map">

...

   <Setting Name="Profile" Type="htf:map">

   <Setting Name="Security" Type="htf:map">

   <Setting Name="TrustedInput" Type="htf:map">

   <Setting Name="DEFAULT" Type="xsd:string">4000-null-false</Setting>

<Setting Name="DEFAULT_PARAMETER" Type="xsd:string">4000-null-false</Setting>

  </Setting>

  </Setting>

...

 </Setting>
```

6. Save changes. Restart the WebLogic Admin server, followed by the OAM managed servers.
7. To verify, check `<DOMAIN_HOME>/config/fmwconfig/oam-config.xml` on each of the OAM managed server nodes, to ensure that the updated version has been propagated correctly.

For SSL-enabled SafeNet Server Machines

If the certificate policy is different in WebLogic and stand-alone Java programs, it is advised to use the standard Sun SSL implementation. The following setting is mandatory, if you are using the **HTTPS** protocol.

1. Set `-DUseSunHttpHandler` flag to `true` in the WLS startup script (below comments block) available at the following location:
   `<WLS-INSTALL-PATH>/oracle/Middleware/user_projects/domains/OAMdomain/bin/setDomainEnv.sh`



```
#
# WL_HOME        - The BEA home directory of your WebLogic installation.
# JAVA_VM        - The desired Java VM to use. You can set this environment variable before calling
#                  this script to switch between Sun or BEA or just have the default be set.
# JAVA_HOME      - Location of the version of Java used to start WebLogic
#                  Server. Depends directly on which JAVA_VM value is set by default or by the environment.
# USER_MEM_ARGS  - The variable to override the standard memory arguments
#                  passed to java.
# PRODUCTION_MODE - The variable that determines whether Weblogic Server is started in production mode.
# DOMAIN_PRODUCTION_MODE
#                - The variable that determines whether the workshop related settings like the debugger,
#                  testconsole or iterativedev should be enabled. ONLY settable using the
#                  command-line parameter named production
#                  NOTE: Specifying the production command-line param will force
#                         the server to start in production mode.
#
# Other variables used in this script include:
# SERVER_NAME    - Name of the weblogic server.
# JAVA_OPTIONS   - Java command-line options for running the server. (These
#                  will be tagged on to the end of the JAVA_VM and
#                  MEM_ARGS)
#
# For additional information, refer to "Managing Server Startup and Shutdown for Oracle WebLogic Server"
# (http://download.oracle.com/docs/cd/E23943_01/web.1111/e13708/overview.htm).
# *************************************************************************
JAVA_OPTIONS="-DUseSunHttpHandler=true"

COMMON_COMPONENTS_HOME="/apps/FMW/Middleware/oracle_common"
export COMMON_COMPONENTS_HOME


OMSM_ORACLE_HOME="/apps/FMW/Middleware/Oracle_IDM1"
export OMSM_ORACLE_HOME


OAM_ORACLE_HOME="/apps/FMW/Middleware/Oracle_IDM1/oam"
export OAM_ORACLE_HOME


APPLICATIONS_DIRECTORY="/apps/FMW/Middleware/user_projects/applications/oam"
export APPLICATIONS_DIRECTORY
```

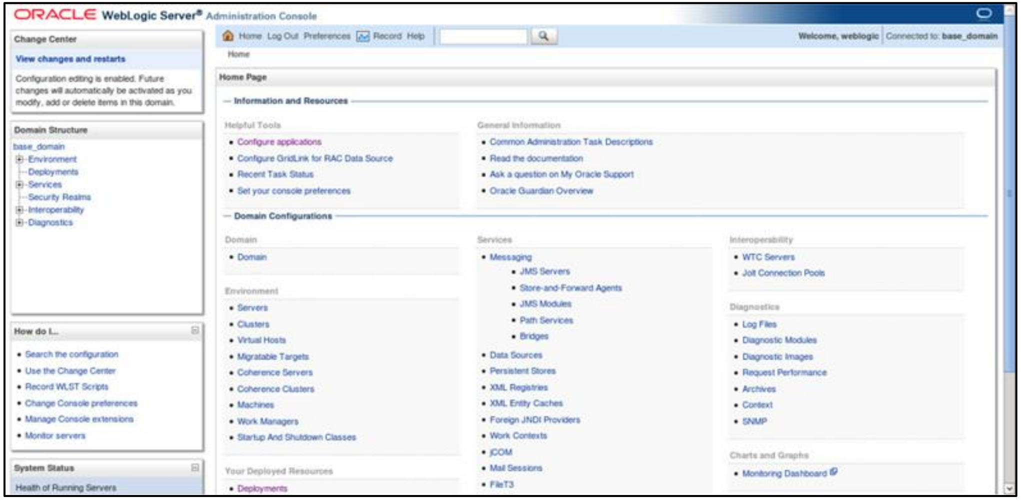
2. Restart the WebLogic Server.

> **NOTE:** Configuring WebLogic Server is important to avoid SSL connection, certificate validation, and SSL handshake errors.

Deploying Agent on WebLogic Server

Deploy agent’s `.war` file on the WLS.

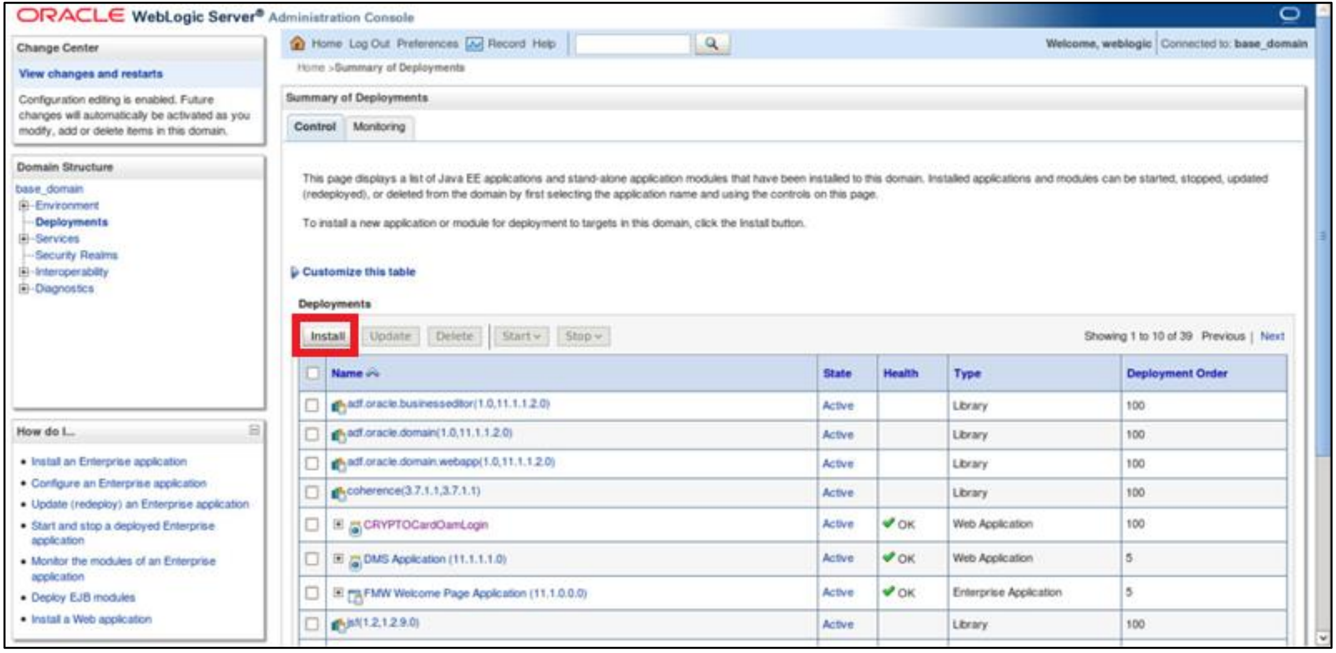
1. Login to WLS web interface.



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

2. From the left pane, under **Domain Structure**, click **Deployments**. In the right pane, click **Install**.


ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic | Connected to: base_domain
Home >Summary of Deployments
Change Center
View changes and restarts
Summary of Deployments
Control
Monitoring
Domain Structure
base_domain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
Customize this table
Deployments
Install
Update
Delete
Start
Stop
Showing 1 to 10 of 39 Previous | Next
How do I...
Install an Enterprise application
Configure an Enterprise application
Update (redeploy) an Enterprise application
Start and stop a deployed Enterprise application
Monitor the modules of an Enterprise application
Deploy EJB modules
Install a Web application

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

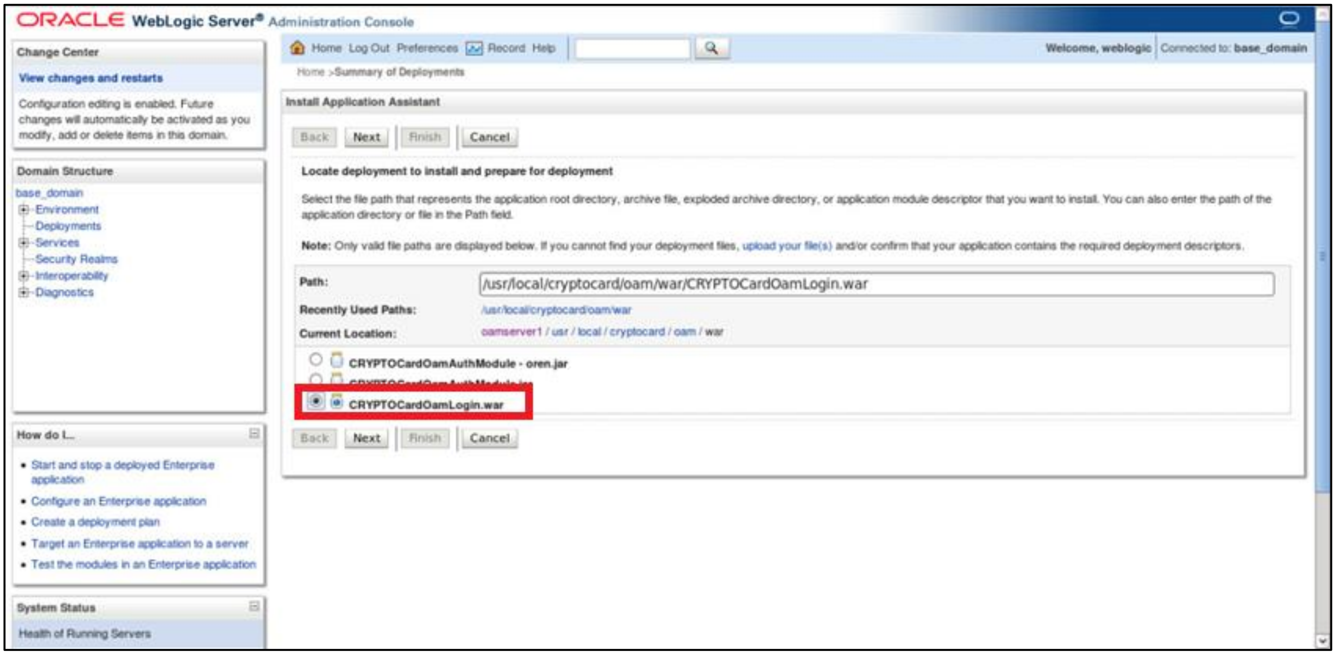
This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on this page.

To install a new application or module for deployment to targets in this domain, click the Install button.

□	Name	State	Health	Type	Deployment Order
□	adf.oracle.businesseditor(1.0,11.1.1.2.0)	Active		Library	100
□	adf.oracle.domain(1.0,11.1.1.2.0)	Active		Library	100
□	adf.oracle.domain.webapp(1.0,11.1.1.2.0)	Active		Library	100
□	coherence(3.7.1.1,3.7.1.1)	Active		Library	100
□	CRYPTOCardOamLogin	Active	✓ OK	Web Application	100
□	DMS Application (11.1.1.1.0)	Active	✓ OK	Web Application	5
□	FMW Welcome Page Application (11.1.0.0.0)	Active	✓ OK	Enterprise Application	5
□	jsf(1.2,1.2.9.0)	Active		Library	100

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

3. On **Install Application Assistant**, select the **CRYPTOCardOamLogin.war** file from the agent installation folder (`/usr/local/cryptocard/oam/war/`), and click **Next**.


ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic
Connected to: base_domain
Home >Summary of Deployments
Change Center
View changes and restarts
Domain Structure
base_domain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Start and stop a deployed Enterprise application
Configure an Enterprise application
Create a deployment plan
Target an Enterprise application to a server
Test the modules in an Enterprise application
System Status
Health of Running Servers
Back
Next
Finish
Cancel

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Install Application Assistant

Locate deployment to install and prepare for deployment

Select the file path that represents the application root directory, archive file, exploded archive directory, or application module descriptor that you want to install. You can also enter the path of the application directory or file in the Path field.

Note: Only valid file paths are displayed below. If you cannot find your deployment files, upload your file(s) and/or confirm that your application contains the required deployment descriptors.

Path: /usr/local/cryptocard/oam/war/CRYPTOCardOamLogin.war

Recently Used Paths: /usr/local/cryptocard/oam/war

Current Location: oamserver1 / usr / local / cryptocard / oam / war

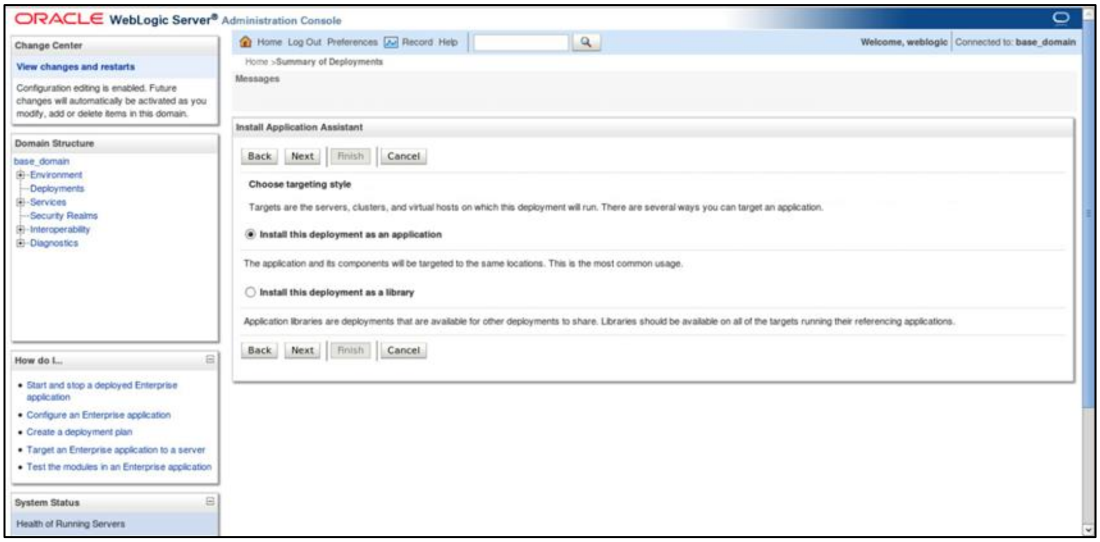
○ CRYPTOCardOamAuthModule - oren.jar

○ CRYPTOCardOamAuthModule.jar

● CRYPTOCardOamLogin.war

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

4. Under **Choose targeting style**, select **Install this deployment as an application**, and click **Next**.


ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic
Connected to: base_domain
Home >Summary of Deployments
Messages
Change Center
View changes and restarts
Domain Structure
base_domain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Start and stop a deployed Enterprise application
Configure an Enterprise application
Create a deployment plan
Target an Enterprise application to a server
Test the modules in an Enterprise application
System Status
Health of Running Servers
Back
Next
Finish
Cancel

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Install Application Assistant

Choose targeting style

Targets are the servers, clusters, and virtual hosts on which this deployment will run. There are several ways you can target an application.

● Install this deployment as an application

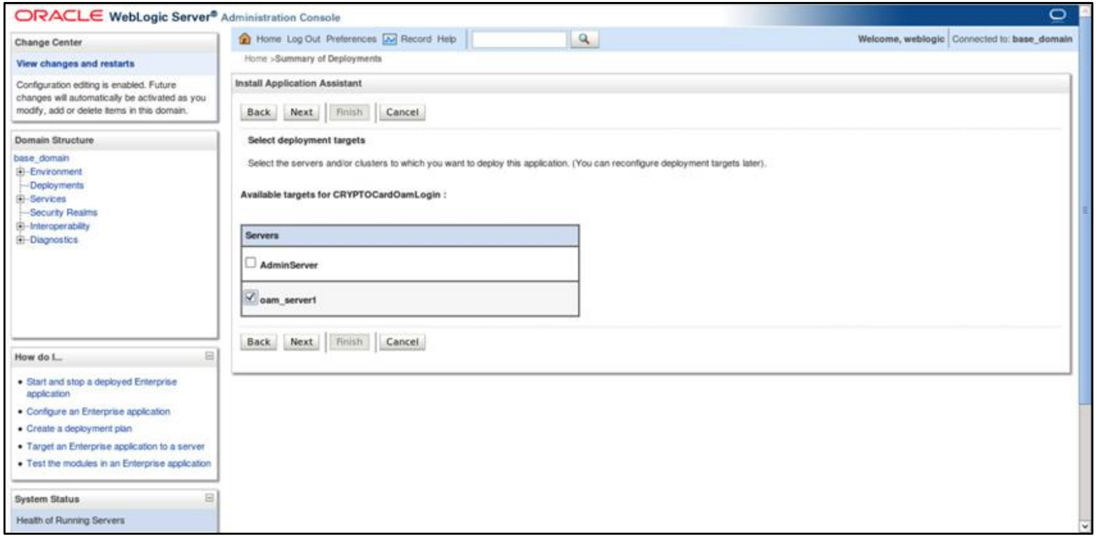
The application and its components will be targeted to the same locations. This is the most common usage.

○ Install this deployment as a library

Application libraries are deployments that are available for other deployments to share. Libraries should be available on all of the targets running their referencing applications.

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

5. Under **Select deployment targets**, select the OAM server, and click **Next**.



ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: base_domain
Home >Summary of Deployments
Change Center
View changes and restarts
Domain Structure
base_domain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Start and stop a deployed Enterprise application
Configure an Enterprise application
Create a deployment plan
Target an Enterprise application to a server
Test the modules in an Enterprise application
System Status
Health of Running Servers

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Install Application Assistant

Back Next Finish Cancel

Select deployment targets

Select the servers and/or clusters to which you want to deploy this application. (You can reconfigure deployment targets later).

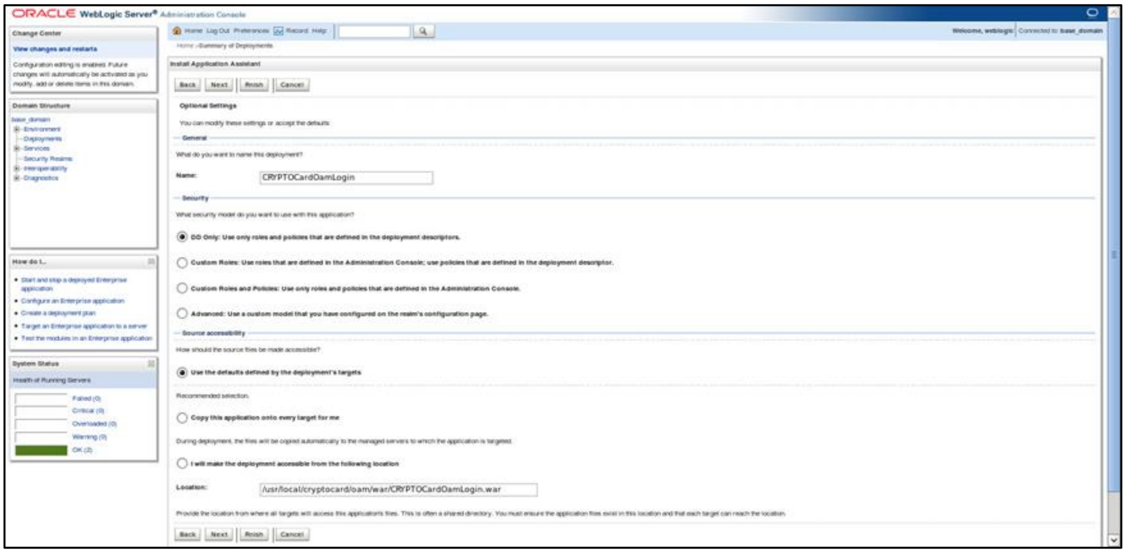
Available targets for CRYPTOCardOamLogin :

Servers
☐ AdminServer
☑ oam_server1

Back Next Finish Cancel

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

6. Under **Optional Settings**, make no changes to the default configurations. Click **Finish**.



ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: base_domain
Home >Summary of Deployments
Change Center
View changes and restarts
Domain Structure
base_domain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Start and stop a deployed Enterprise application
Configure an Enterprise application
Create a deployment plan
Target an Enterprise application to a server
Test the modules in an Enterprise application
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (2)

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Install Application Assistant

Back Next Finish Cancel

Optional Settings

You can modify these settings or accept the defaults

General

What do you want to name this deployment?

Name: CRYPTOCardOamLogin

Security

What security model do you want to use with this application?

● DD Only: Use only roles and policies that are defined in the deployment descriptors.

○ Custom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor.

○ Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console.

○ Advanced: Use a custom model that you have configured on the realm's configuration page.

Source accessibility

How should the source files be made accessible?

● Use the defaults defined by the deployment's targets

Recommended selection.

○ Copy this application onto every target for me

During deployment, the files will be copied automatically to the managed servers to which the application is targeted.

○ I will make the deployment accessible from the following location

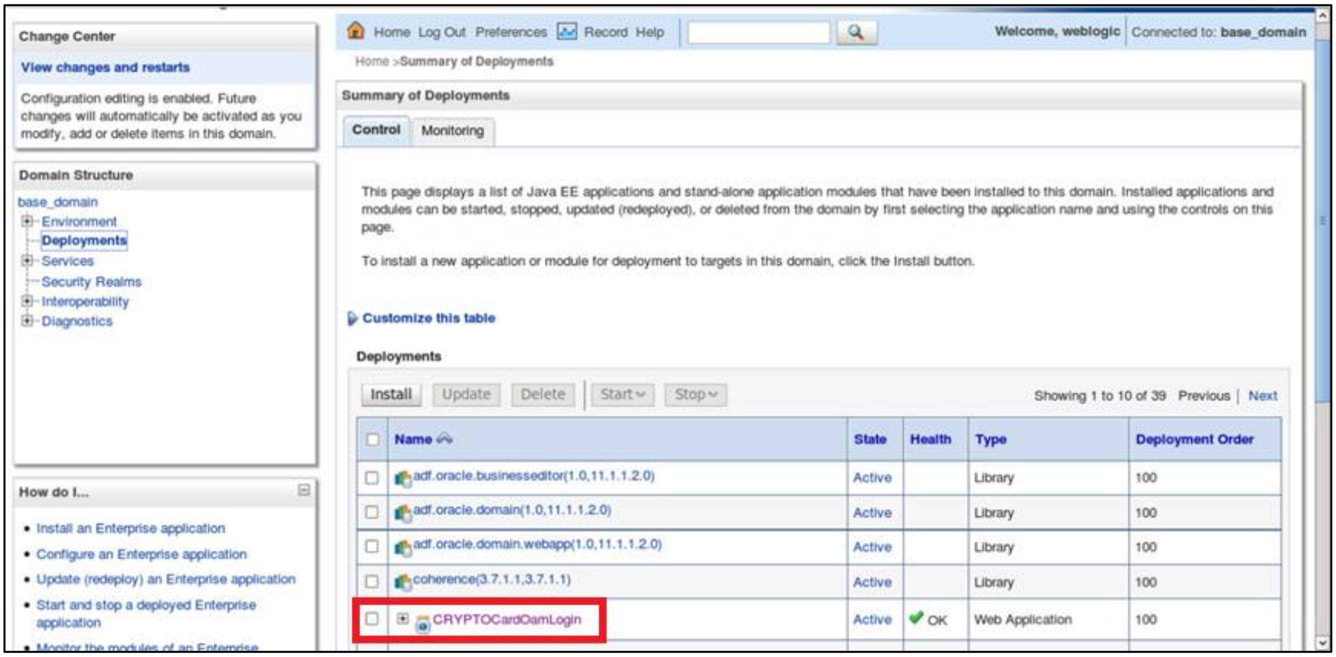
Location: /usr/local/cryptocard/oam/war/CRYPTOCardOamLogin.war

Provide the location from where all targets will access this application's files. This is often a shared directory. You must ensure the application files exist in this location and that each target can reach the location.

Back Next Finish Cancel

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

7. From the left pane, under **Domain Structure**, click **Deployments**. In the right pane under listed **Deployments**, verify if the **State** of the **CRYPTOCardOamLogin** agent is **Active**.



Home Log Out Preferences Record Help
Welcome, weblogic Connected to: base_domain

Change Center

View changes and restarts

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Domain Structure

- base_domain
  - Environment
  - Deployments
  - Services
  - Security Realms
  - Interoperability
  - Diagnostics

How do I...

- Install an Enterprise application
- Configure an Enterprise application
- Update (redeploy) an Enterprise application
- Start and stop a deployed Enterprise application
- Monitor the modules of an Enterprise

Home >Summary of Deployments

Summary of Deployments

This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on this page.

To install a new application or module for deployment to targets in this domain, click the Install button.

Customize this table

Deployments

Showing 1 to 10 of 39 Previous | Next

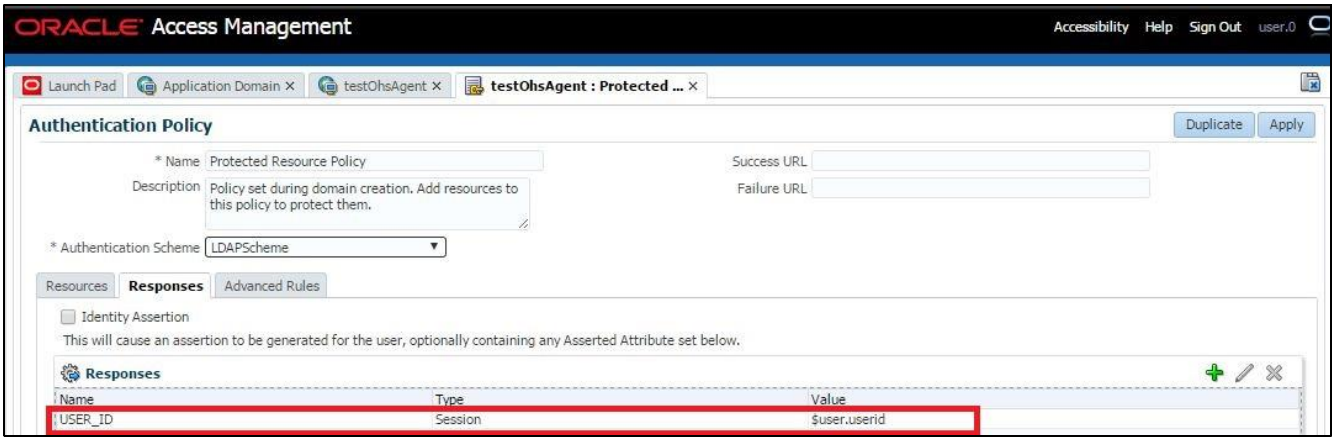
□	Name	State	Health	Type	Deployment Order
□	adf.oracle.businesseditor(1.0,11.1.1.2.0)	Active		Library	100
□	adf.oracle.domain(1.0,11.1.1.2.0)	Active		Library	100
□	adf.oracle.domain.webapp(1.0,11.1.1.2.0)	Active		Library	100
□	coherence(3.7.1.1,3.7.1.1)	Active		Library	100
□	CRYPTOCardOamLogin	Active	✓ OK	Web Application	100

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

Cookie Settings for Step-Up Authentication

1. On the Oracle Access Management portal, under **Access Manager**, click **Application Domains**.
2. Click **Search**. Under **Search Results**, click the Level 1 protected resource **Application Domain**. Level 1 protected resource is a resource protected with Level 1 (Username and Password) authentication.
3. On **Authentication Policies** tab, click **Protected Resource Policy**.
4. Click **Responses** tab.
5. Click **Add**, and add the cookie with following settings.

Name	USER_ID Cookie name (USER_ID) must match the name of cookie variable set using USER_LOGIN_ID_NAME variable in Configuring .ini File section.
Type	Cookie
Value	$user.userid



Authentication Policy

* Name: Protected Resource Policy

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

Success URL:

Failure URL:

* Authentication Scheme: LDAPScheme

□ Identity Assertion

This will cause an assertion to be generated for the user, optionally containing any Asserted Attribute set below.

Responses

Name	Type	Value
USER_ID	Session	$user.userid

For information on Step-Up Authentication, including how the authentication flow differs based on the resource type, click here.

CHAPTER 3: Oracle Access Manager Configuration for R3 and 12c Version

To install and configure the SafeNet Agent on OAM R3 and 12c, follow the steps:

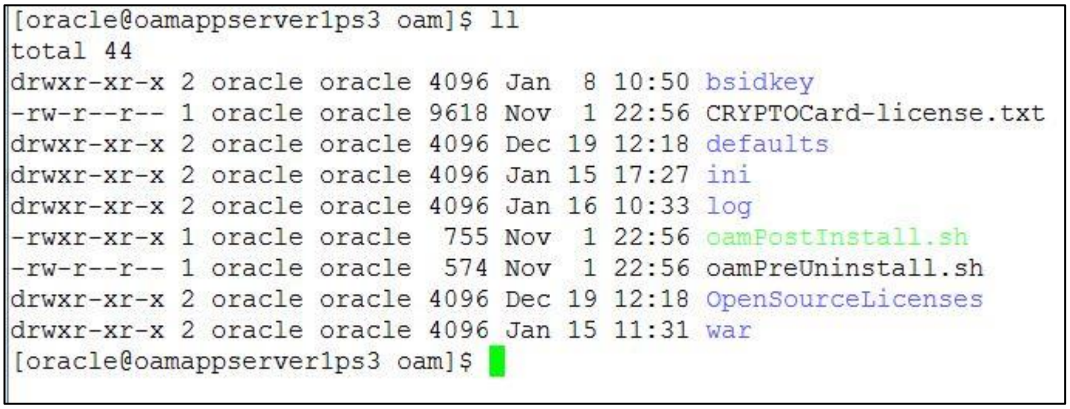
1. Installing the SafeNet Agent Plugin
2. Configuring the .ini File of the SafeNet Agent
3. Importing the SafeNet Agent Plugin Using the Oracle Access Manager Console
4. Creating an Authentication Module
5. Creating the Authentication Scheme
6. Forcing the SafeNet Agent Authentication Scheme on a Protected Resource
7. Configuring the WebLogic Server
8. Deploying the Agent on the WebLogic Server

> **NOTE:** Before proceeding, make sure you back up your OAM configuration.
>
> In case you have any issues, you can always roll back OAM/WLS configuration files to restore OAM to its original state. All XML files can be located at:
>
> **`Oracle_Home/user_projects/domains/OAM/config`**
>
> The **oam-config.xml** file must be backed up.
> You can find both applications on the same physical server.

Installing SafeNet Agent Plugin

Install the SafeNet Agent `rpm`.

1. Run the following command:
   ```
   rpm -ivh cryptocard-oam-agent-[your installation build].x86_64.rpm
   ```
2. The installation package will be installed at the following location:
   ```
   /usr/local/cryptocard/oam/
   ```



```
[oracle@oamappserver1ps3 oam]$ ll
total 44
drwxr-xr-x 2 oracle oracle 4096 Jan  8 10:50 bsidkey
-rw-r--r-- 1 oracle oracle 9618 Nov  1 22:56 CRYPTOCard-license.txt
drwxr-xr-x 2 oracle oracle 4096 Dec 19 12:18 defaults
drwxr-xr-x 2 oracle oracle 4096 Jan 15 17:27 ini
drwxr-xr-x 2 oracle oracle 4096 Jan 16 10:33 log
-rwxr-xr-x 1 oracle oracle  755 Nov  1 22:56 oamPostInstall.sh
-rw-r--r-- 1 oracle oracle  574 Nov  1 22:56 oamPreUninstall.sh
drwxr-xr-x 2 oracle oracle 4096 Dec 19 12:18 OpenSourceLicenses
drwxr-xr-x 2 oracle oracle 4096 Jan 15 11:31 war
[oracle@oamappserver1ps3 oam]$ 
```

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

> **NOTE:** The administrator must have rights/ permissions to access OAM user accounts.

Configuring .ini File

Modify the .ini file of the SafeNet Agent by adding details such as BSID server details, protocol, and others. Configure following variables in the `/usr/local/cryptocard/oam/ini/CryptoWrapper.ini` file:

PrimaryProtocol	Select **http/https**.
PrimaryServer	Enter the primary SafeNet server host.
PrimaryServerPort	Enter the port number (for example, **80/443**).
SecondaryProtocol	Select **http/https**.
SecondaryServer	Enter the secondary SafeNet server host.
SecondaryServerPort	Enter the port number (for example, **80/443**).
LogLevel	Select level of the log that will be created. By default, the value is set to 3, in a range of 1-5, with 1 being the lowest and 5 being the highest level. The higher the log level is, the more detailed information it contains. Each log level also contains information for all its following log levels.
REDIRECT-LOCATION-AFTER-AUTHENTICATION	Enter the OAM redirection URL (For example, http://<iamdemo.oracle.com>:14100/oam/server/auth_cred_submit).
OTP_LOGIN_PAGE	Set to False, if all three inputs (User Name, LDAP Password and OTP) must be required for SafeNet server authentication, even after LDAP authentication. Default value: True
USER_LOGIN_ID_NAME	Required only if **OTP_LOGIN_PAGE** is set as True.

	Set name of cookie variable to provide LDAP User Name. Default value: **USER_ID** (can be set to any other value, but this value must match the **Cookie name value** set in Cookie Settings for Step-Up Authentication section.
IGNORE_CERTIFICATE_ERRORS	This parameter is only valid for the **HTTPS** protocol. Default Value: **0** The value **0** ensures that the security certificate checks will be forced while communicating with SafeNet Servers. This setting is recommended if the SafeNet server is in use. If set to **1**, the certificate checks will be ignored. This setting is recommended for in-house SafeNet server deployments, with self-signed certificates. If the setting is changed back to **0** (from **1**), ensure that the SafeNet server (in use) has a valid certificate.

NOTE: If your organization uses a proxy server to access extranet or intranet, you must also configure the proxy settings in the .ini file. The agent software works only with HTTP proxy (basic or anonymous authentication). Any settings changed (at any time) require a WLS and OAM restart.

Agent Encryption Key File

The agent encryption key file is used to encrypt/decrypt the data. By default, the key file is available at the following location:

```
/usr/local/cryptocard/oam/bsidkey
```

If you are moving from one SafeNet server version to another, the key file can be downloaded by following the steps:

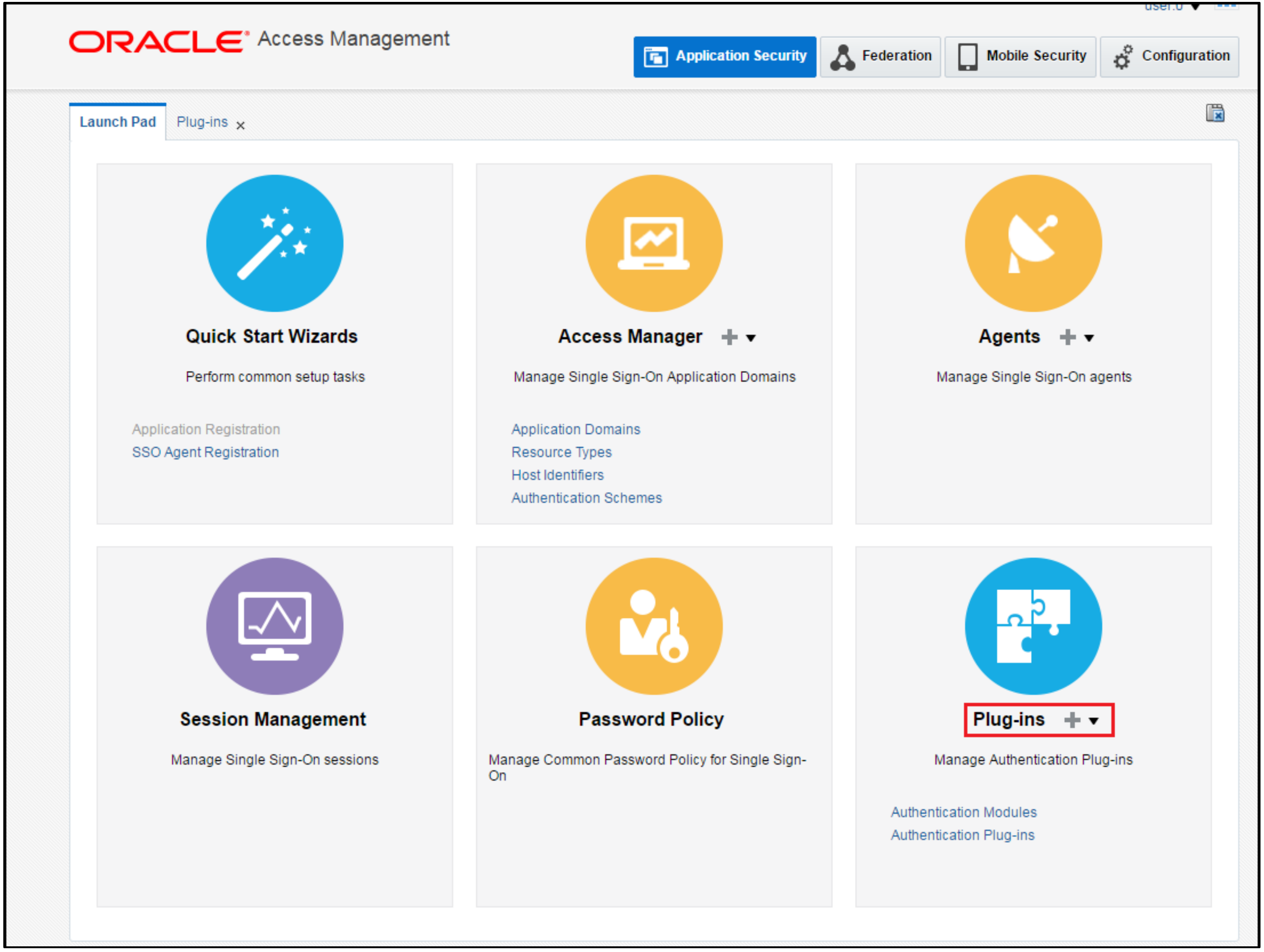
1. Login to SafeNet account, and navigate to **COMMS** > **Authentication Processing** section.
2. Under the **Task** list, click **Authentication Agent Settings** link and download the key.
   The key file must be kept at a location accessible by all the authorized users.

Importing SafeNet Agent Plugin

In this section, you will import the SafeNet Agent Plugin to the OAM, using the Oracle Access Management portal.

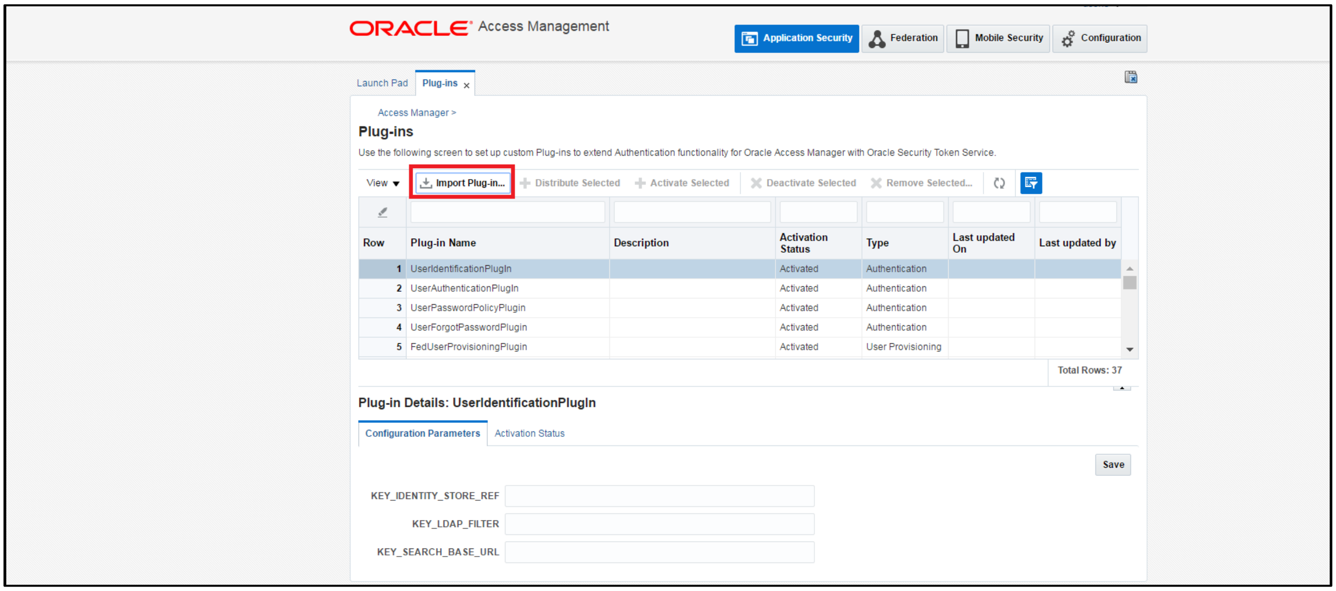
1. Login to Oracle Access Management portal as an administrator.

2. Click **Plug-ins**.



(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

3. On the **Plug-ins** tab, click **Import Plug-in**.



Plug-ins

Use the following screen to set up custom Plug-ins to extend Authentication functionality for Oracle Access Manager with Oracle Security Token Service.

Row	Plug-in Name	Description	Activation Status	Type	Last updated On	Last updated by
1	UserIdentificationPlugIn		Activated	Authentication		
2	UserAuthenticationPlugIn		Activated	Authentication		
3	UserPasswordPolicyPlugin		Activated	Authentication		
4	UserForgotPasswordPlugin		Activated	Authentication		
5	FedUserProvisioningPlugin		Activated	User Provisioning		

Total Rows: 37

Plug-in Details: UserIdentificationPlugIn

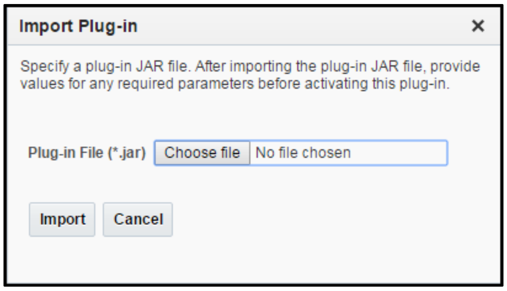
KEY_IDENTITY_STORE_REF

KEY_LDAP_FILTER

KEY_SEARCH_BASE_URL

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

4. The **Import Plug-in** popup window is displayed. Click **Choose file**.

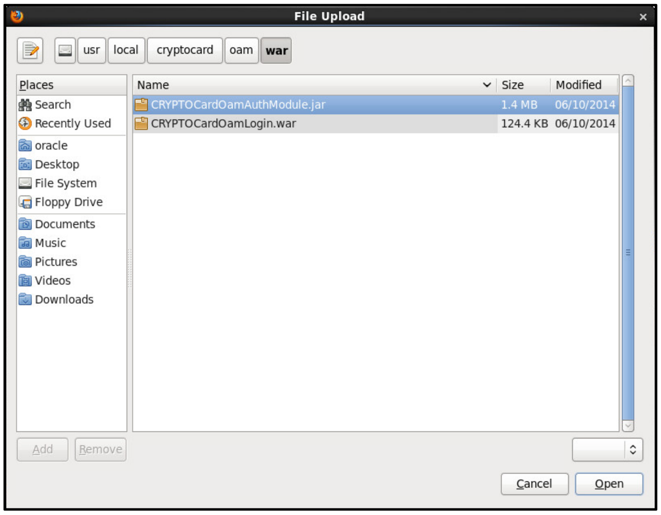


Specify a plug-in JAR file. After importing the plug-in JAR file, provide values for any required parameters before activating this plug-in.

Plug-in File (*.jar) No file chosen

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

5. On the **File Upload** window, select the agent.jar file (for example, `/usr/local/cryptocard/oam/war/CRYPTOCardOamAuthModule.jar`), and click **Open**.

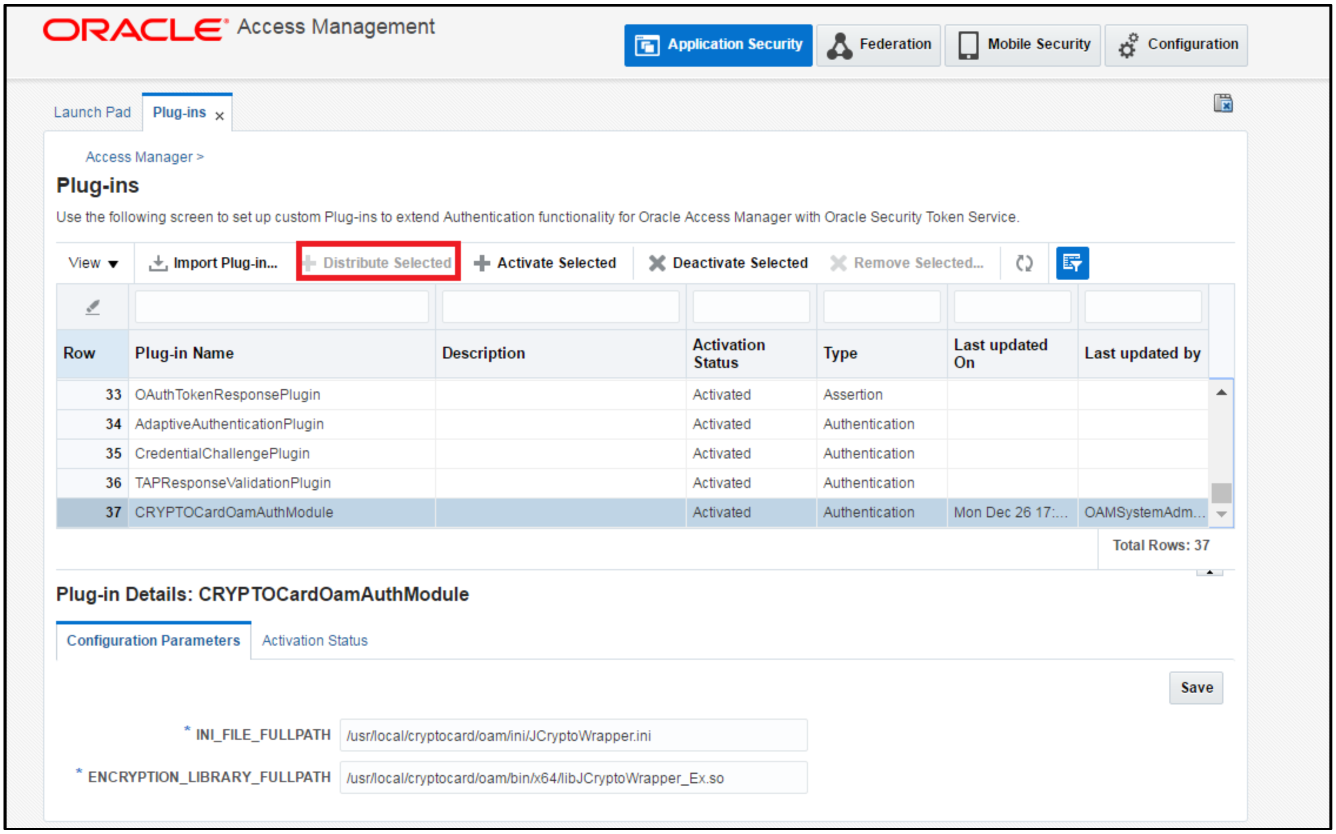


Name	Size	Modified
CRYPTOCardOamAuthModule.jar	1.4 MB	06/10/2014
CRYPTOCardOamLogin.war	124.4 KB	06/10/2014

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

6. On the **Import Plug-in** window, click **Import**.

7. The SafeNet Agent plugin is listed. Select the plug-in, and then click **Distribute Selected**.



Plug-ins

Use the following screen to set up custom Plug-ins to extend Authentication functionality for Oracle Access Manager with Oracle Security Token Service.

Row	Plug-in Name	Description	Activation Status	Type	Last updated On	Last updated by
33	OAuthTokenResponsePlugin		Activated	Assertion		
34	AdaptiveAuthenticationPlugin		Activated	Authentication		
35	CredentialChallengePlugin		Activated	Authentication		
36	TAPResponseValidationPlugin		Activated	Authentication		
37	CRYPTOCardOamAuthModule		Activated	Authentication	Mon Dec 26 17:...	OAMSystemAdm...

Total Rows: 37

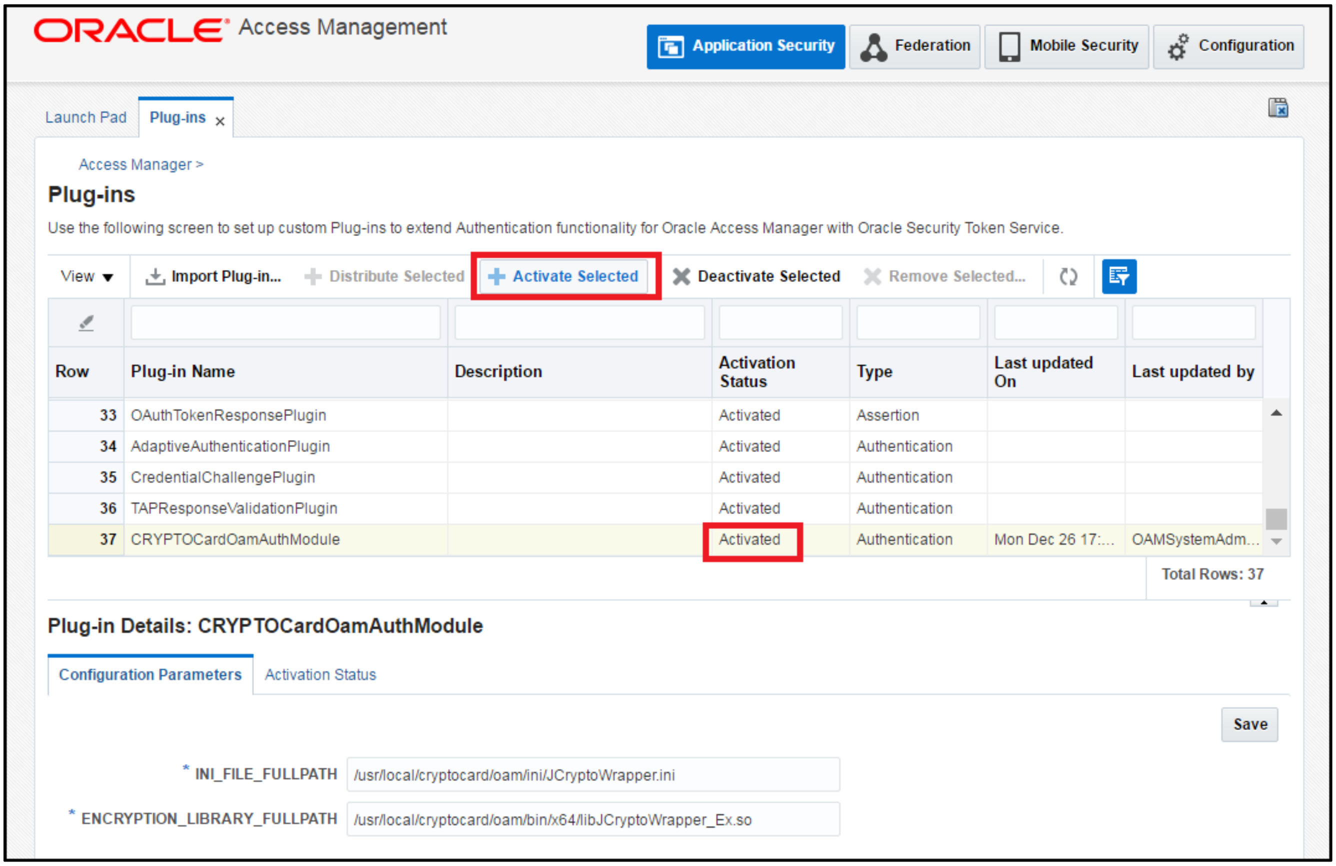
* INI_FILE_FULLPATH /usr/local/cryptocard/oam/ini/JCryptoWrapper.ini

* ENCRYPTION_LIBRARY_FULLPATH /usr/local/cryptocard/oam/bin/x64/libJCryptoWrapper_Ex.so

(The screen image above is from Oracle Access Manager. Trademarks are the property of their respective owners.)

8. The **Activation Status** for the plug-in is populated to **Distributed**.

9. Select the SafeNet Agent plug-in, and click **Activate Selected**. The **Activation Status** is changed to **Activated**.



Access Manager >

Plug-ins

Use the following screen to set up custom Plug-ins to extend Authentication functionality for Oracle Access Manager with Oracle Security Token Service.

Row	Plug-in Name	Description	Activation Status	Type	Last updated On	Last updated by
33	OAuthTokenResponsePlugin		Activated	Assertion		
34	AdaptiveAuthenticationPlugin		Activated	Authentication		
35	CredentialChallengePlugin		Activated	Authentication		
36	TAPResponseValidationPlugin		Activated	Authentication		
37	CRYPTOCardOamAuthModule		Activated	Authentication	Mon Dec 26 17:...	OAMSystemAdm...

Total Rows: 37

Plug-in Details: CRYPTOCardOamAuthModule

* INI_FILE_FULLPATH /usr/local/cryptocard/oam/ini/JCryptoWrapper.ini

* ENCRYPTION_LIBRARY_FULLPATH /usr/local/cryptocard/oam/bin/x64/libJCryptoWrapper_Ex.so

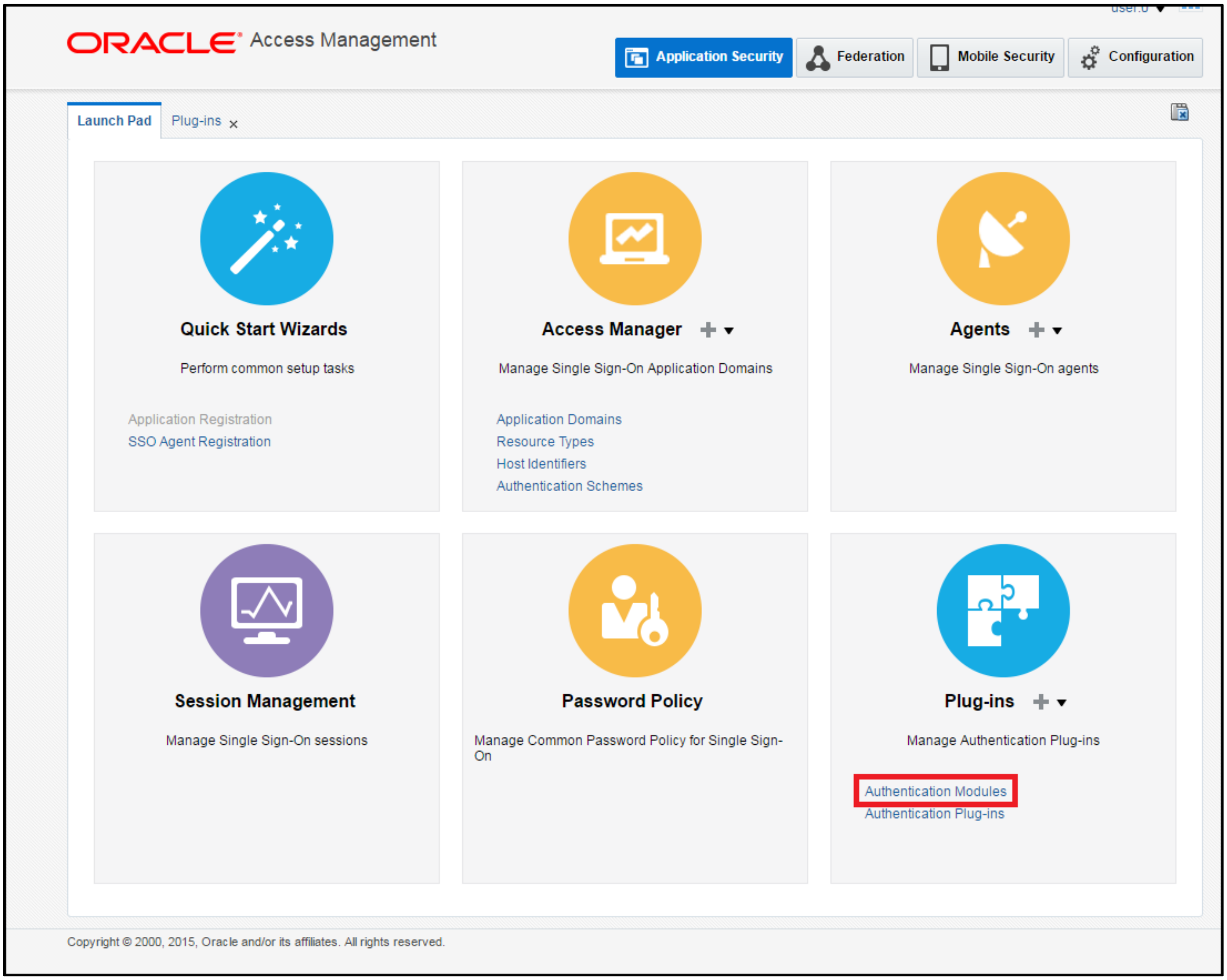
(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

> **NOTE:** If the plugin is not deployed at the default location, change the required plugin parameters (as shown previously) and set the appropriate parameters in the **.ini** file.

Creating Authentication Module

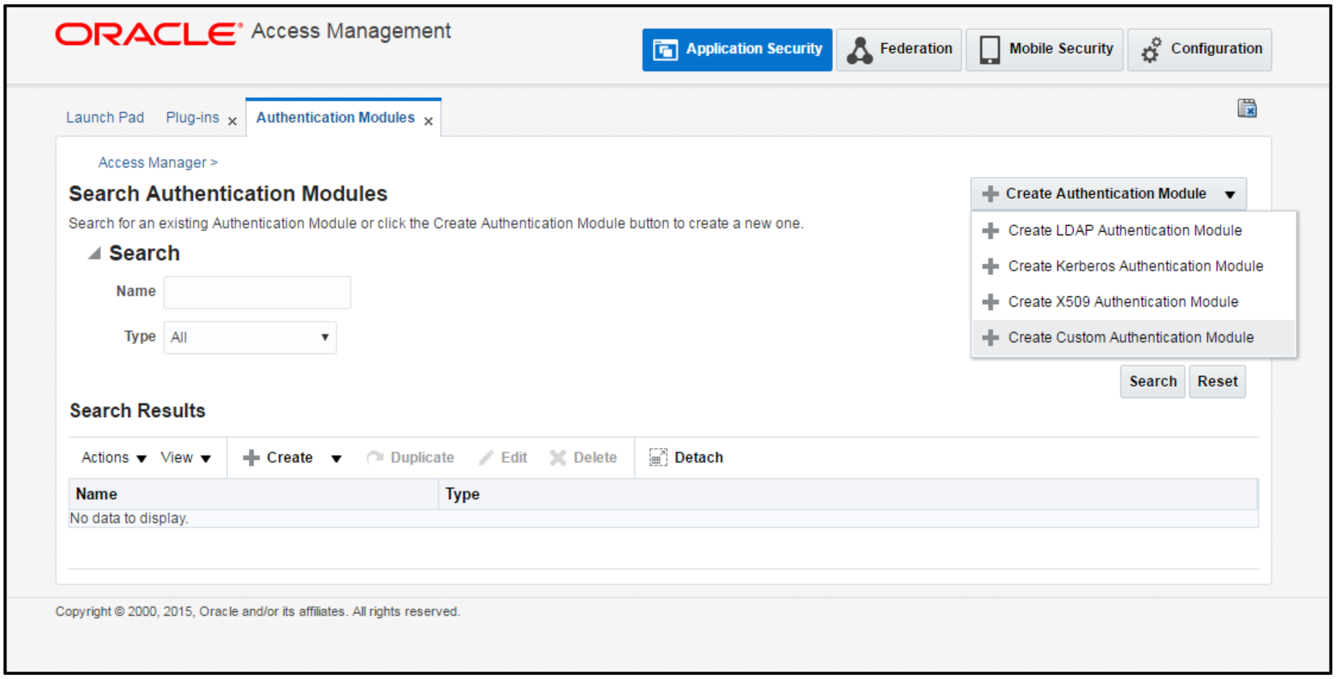
To define the type and order of the authentication, configure the authentication module. In the authentication module, you will configure the OTP authentication that will be used by the SafeNet Agent.

1. On the Oracle Access Management portal, under **Plug-ins**, click **Authentication Modules**.



(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

2. Click **Create Authentication Module** > **Create Custom Authentication Module**.



Search Authentication Modules

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

Search

Name

Type: All

Search Results

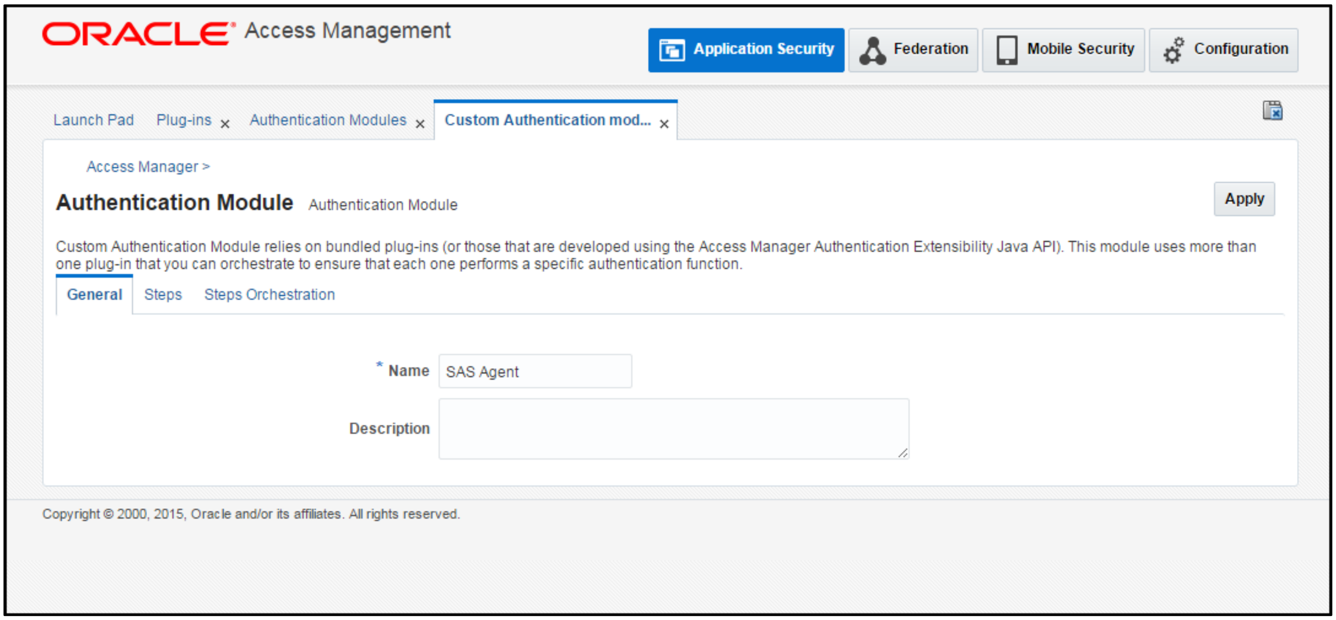
Name	Type
No data to display.	

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

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

3. On the **Authentication Module** window, on the **General** tab, complete the following fields:

Name	Enter a name for the module.
Description	Enter a description for the module, if required.



Authentication Module Authentication Module

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.

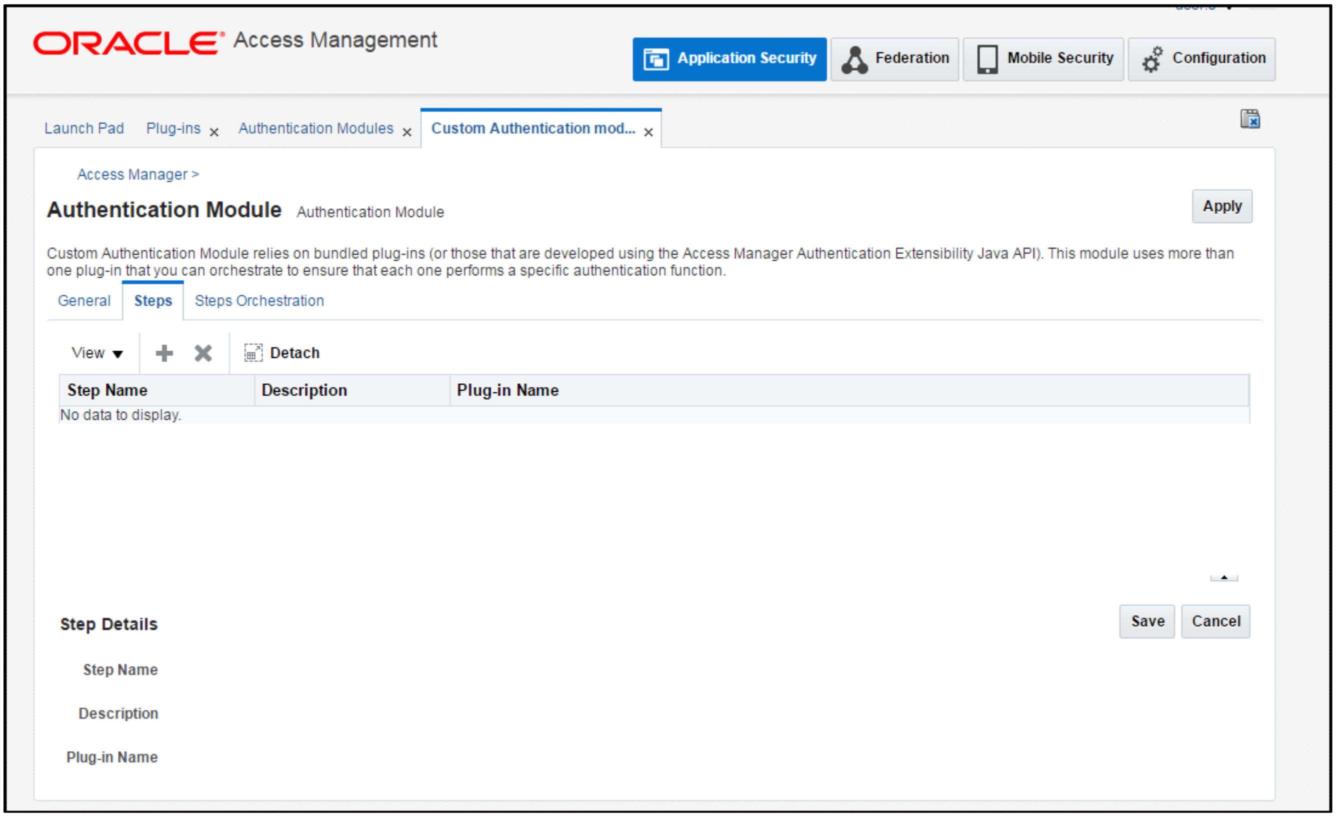
* Name: SAS Agent

Description:

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

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

4. Click **Steps** tab, and click Create ✚ icon to add a new step to the authentication module.



Authentication Module Authentication Module

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.

Step Name	Description	Plug-in Name
No data to display.		

Step Details

Step Name

Description

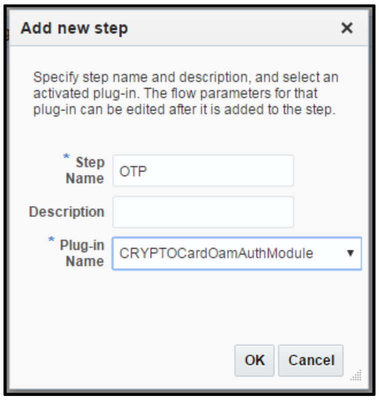
Plug-in Name

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

5. Perform the following to configure OTP authentication:

   On **Add new step** window, complete the following fields, and click **OK**.

Step Name	Enter a name for the module.
Plug-in Name	Select **CRYPTOCardOamAuthModule**.



Specify step name and description, and select an activated plug-in. The flow parameters for that plug-in can be edited after it is added to the step.

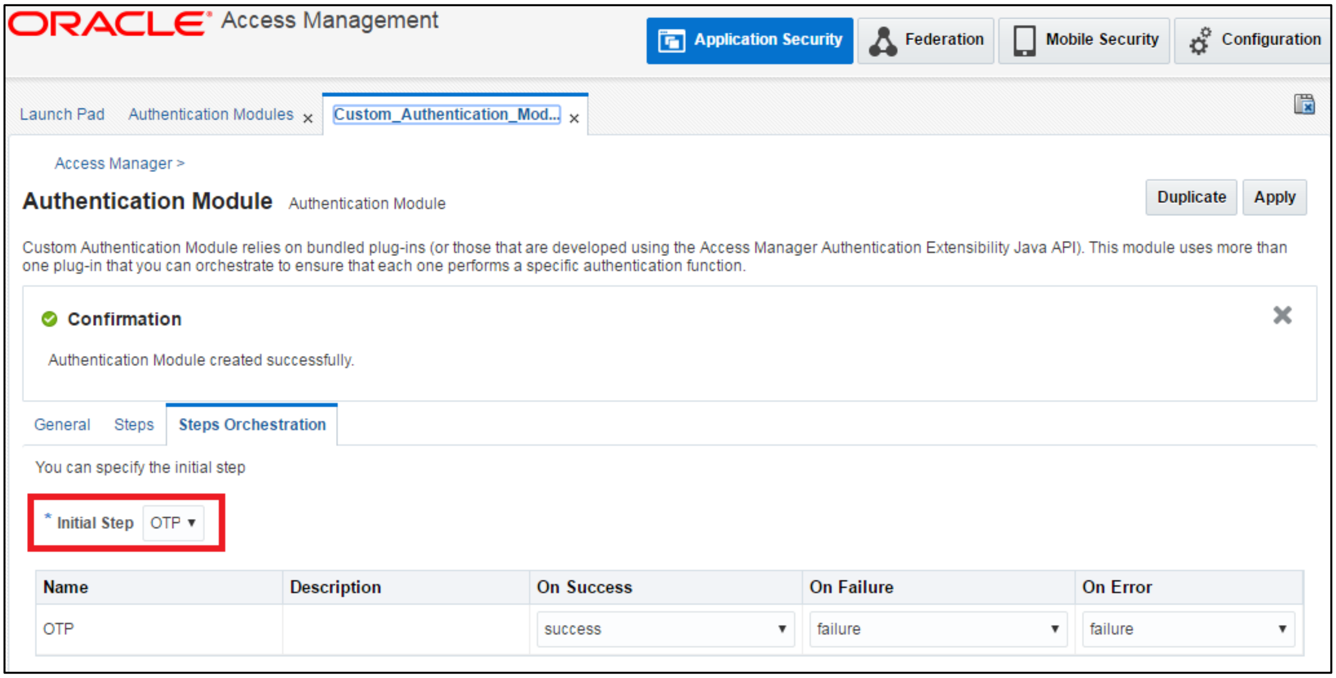
* Step Name: OTP

Description:

* Plug-in Name: CRYPTOCardOamAuthModule

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

6. Click **Steps Orchestration** tab, and verify that in the **Initial Step** field, **OTP** option is selected. Also verify success, failure and error conditions, as illustrated in the screenshot below:



Authentication Module Authentication Module

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.

Confirmation

Authentication Module created successfully.

You can specify the initial step

* Initial Step OTP

Name	Description	On Success	On Failure	On Error
OTP		success	failure	failure

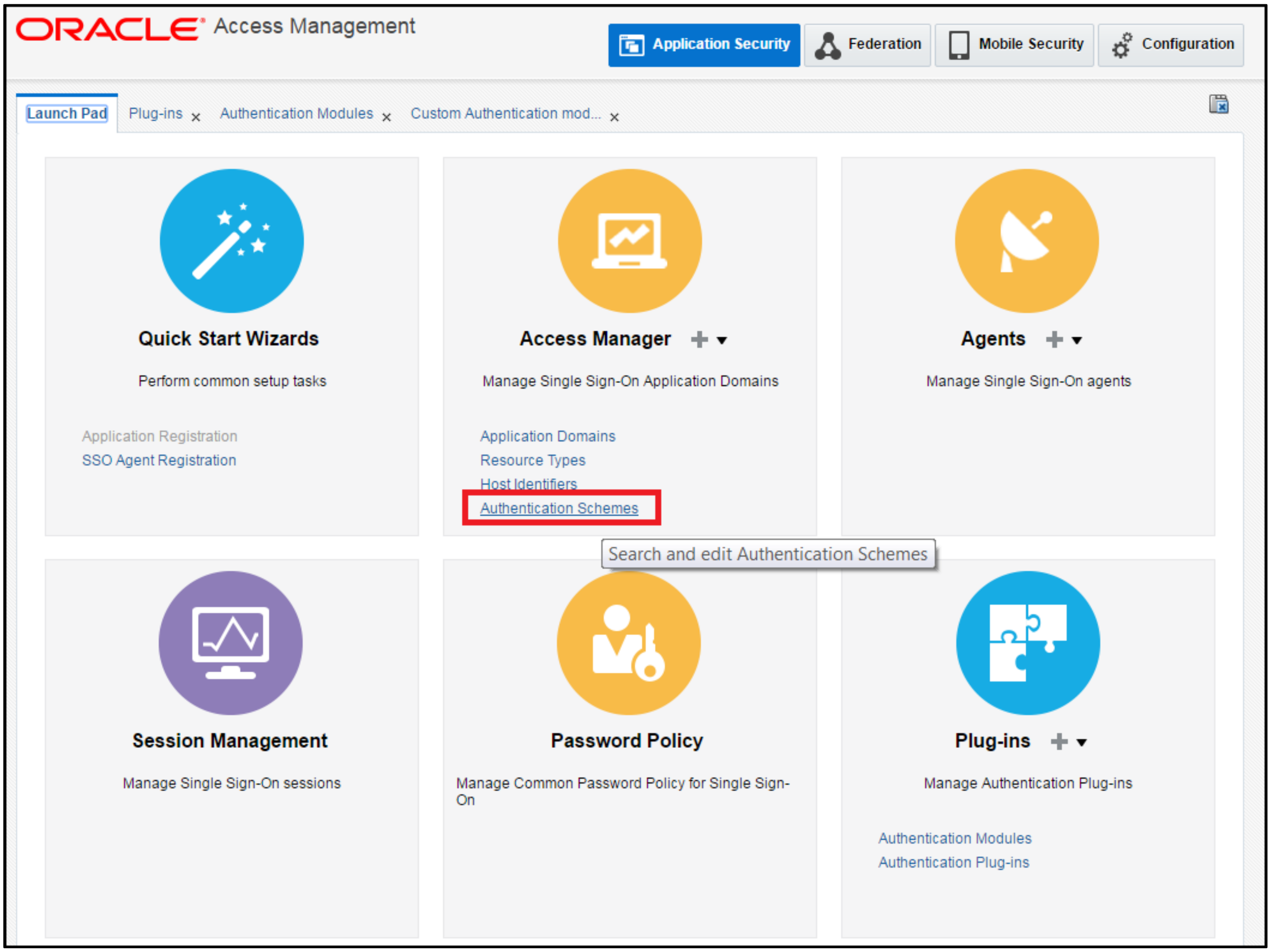
(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

7. Click **Apply**.

Creating Authentication Scheme

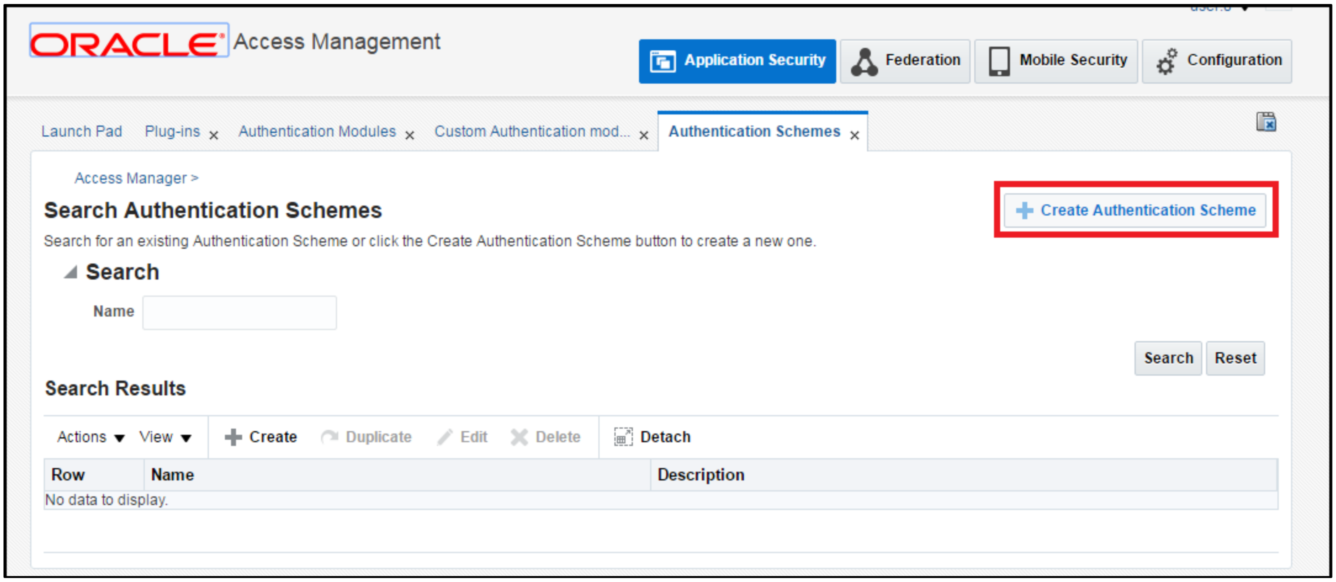
Create the authentication scheme that will use the authentication module created in the previous section.

1. On the Oracle Access Management portal, under **Access Manager**, click **Authentication Schemes**.



(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

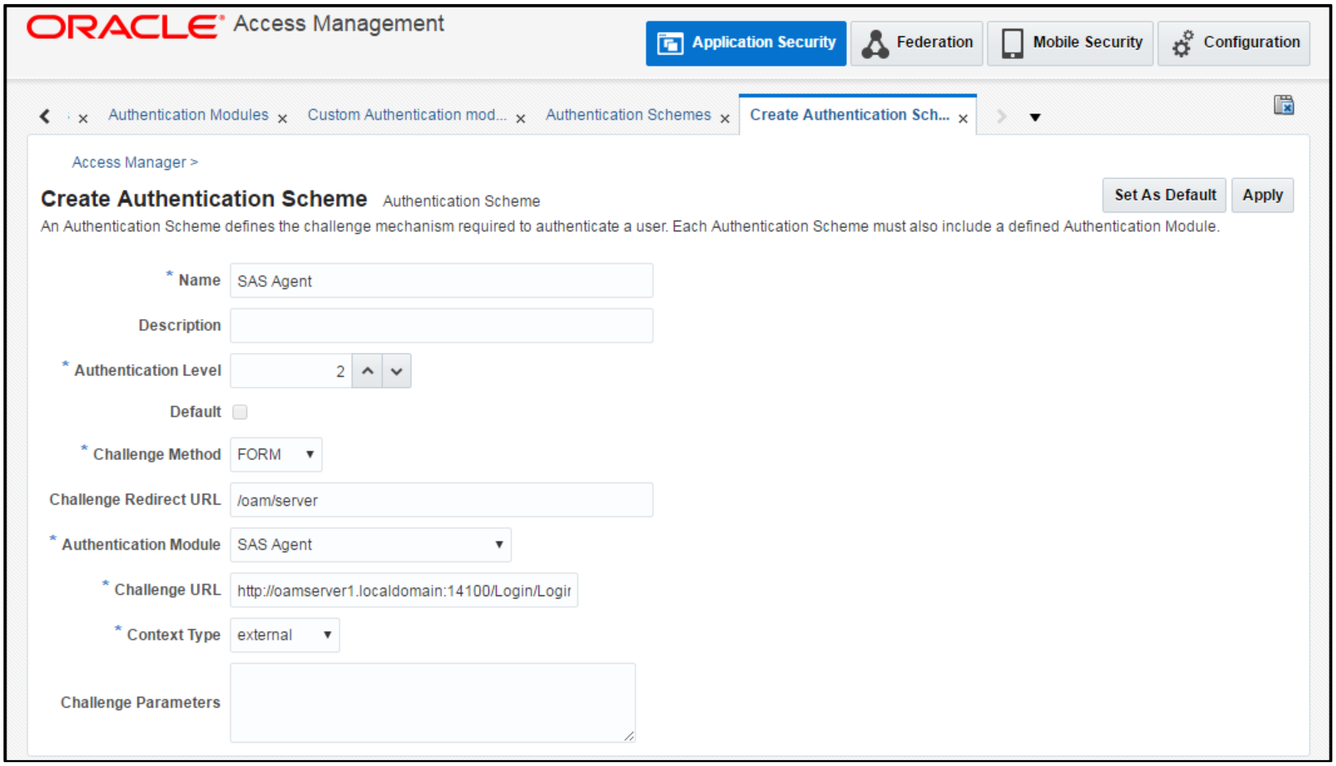
2. Click **Create Authentication Scheme**.



(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

3. Complete the following fields, and click **Apply**.

Name	Enter a name for the authentication scheme.
Authentication Level	Select **2**.
Challenge Method	Select **FORM**.
Challenge Redirect URL	Enter `/oam/server/`.
Authentication Module	Select the authentication module (for example, **SafeNet Agent**) that you created earlier (in step 3 of Creating Authentication Module).
Challenge URL	Enter URL of the credentials collector (for example, http://oamserver1.localdomain:14100/Login/Login.jsp).
Context Type	Select **external**.



Create Authentication Scheme Authentication Scheme

An Authentication Scheme defines the challenge mechanism required to authenticate a user. Each Authentication Scheme must also include a defined Authentication Module.

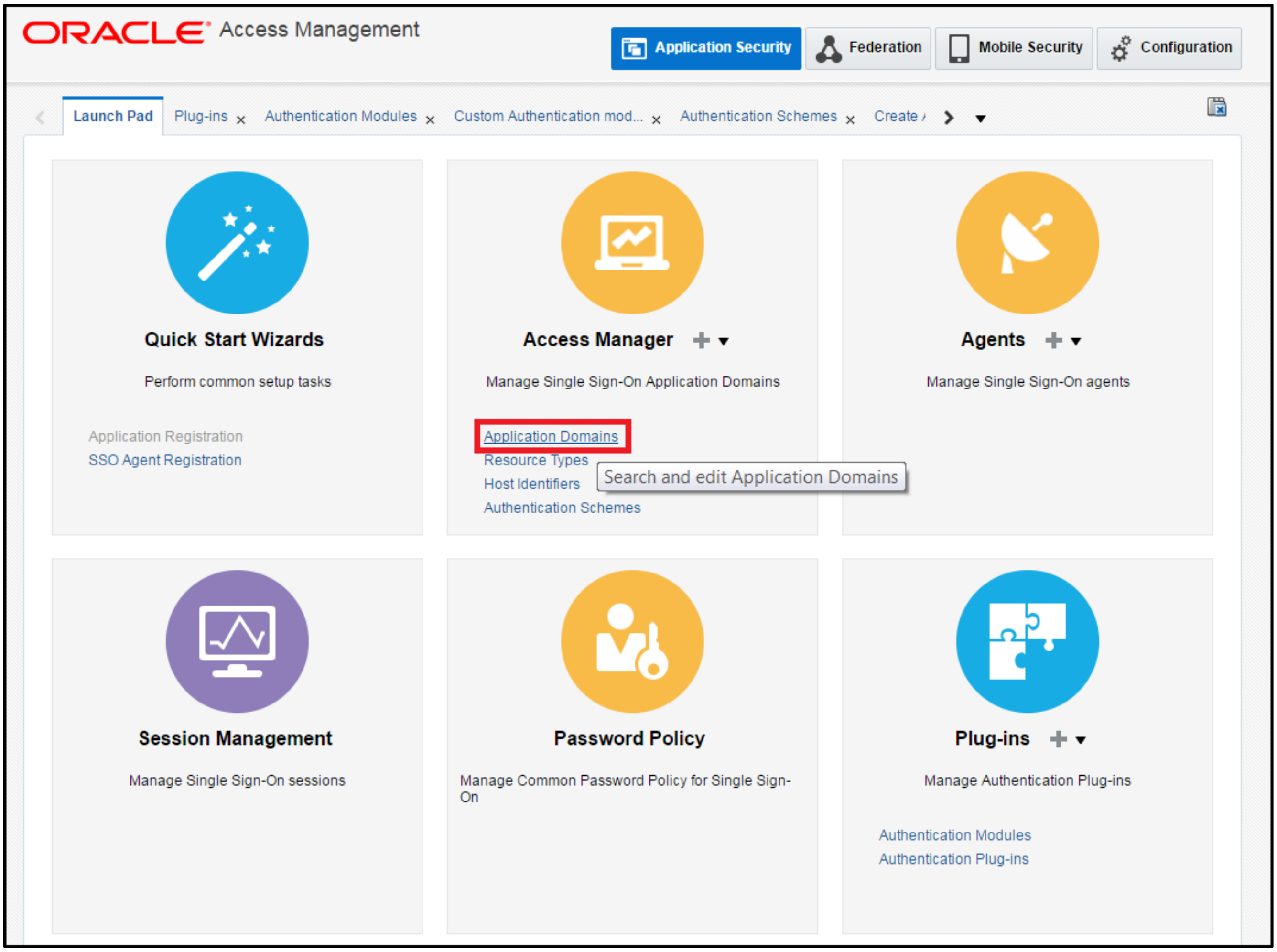
* Name	SAS Agent
Description	
* Authentication Level	2
Default	□
* Challenge Method	FORM
Challenge Redirect URL	/oam/server
* Authentication Module	SAS Agent
* Challenge URL	http://oamserver1.localdomain:14100/Login/Logir
* Context Type	external
Challenge Parameters	

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

Forcing Authentication Scheme on Protected Resource

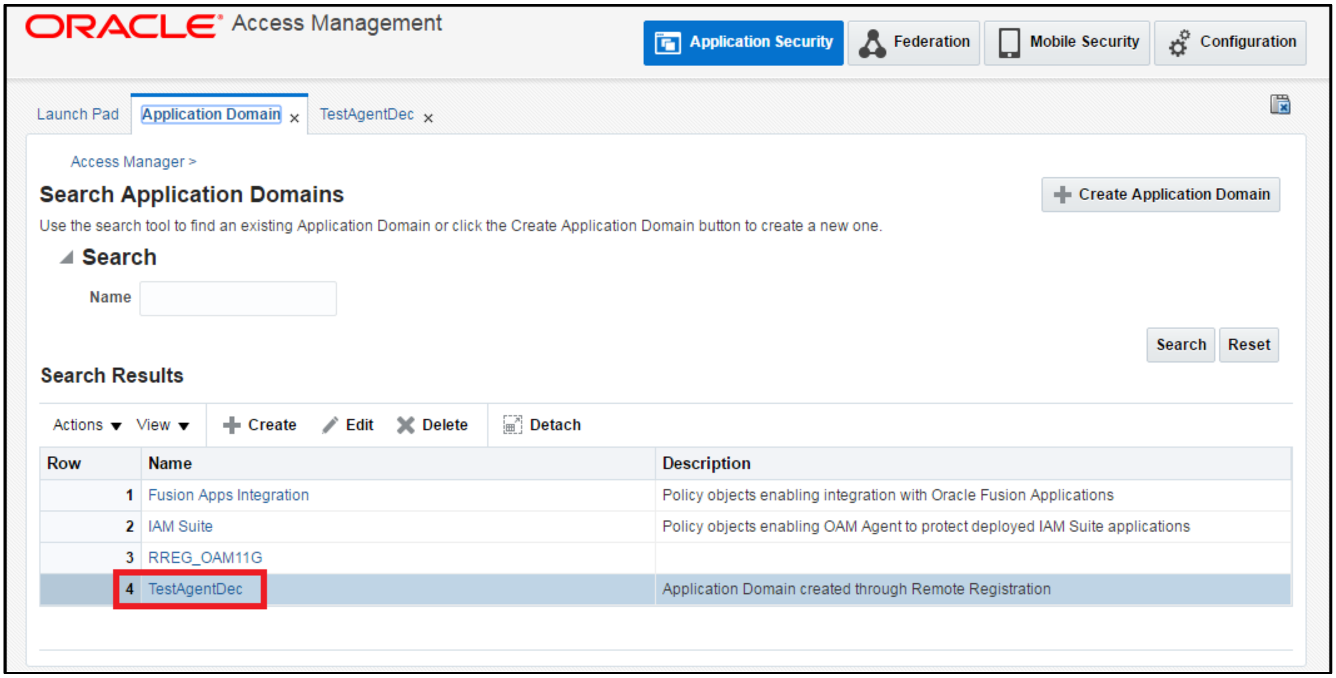
Force the SafeNet Agent authentication scheme on the protected resource in OAM. This will cause the client to immediately authenticate using the specified scheme.

1. On the Oracle Access Management portal, under **Access Manager**, click **Application Domains**.



(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

2. Click **Search**. Under **Search Results**, click the protected resource (for example, TestAgentDec).



Search Application Domains

Use the search tool to find an existing Application Domain or click the Create Application Domain button to create a new one.

Search

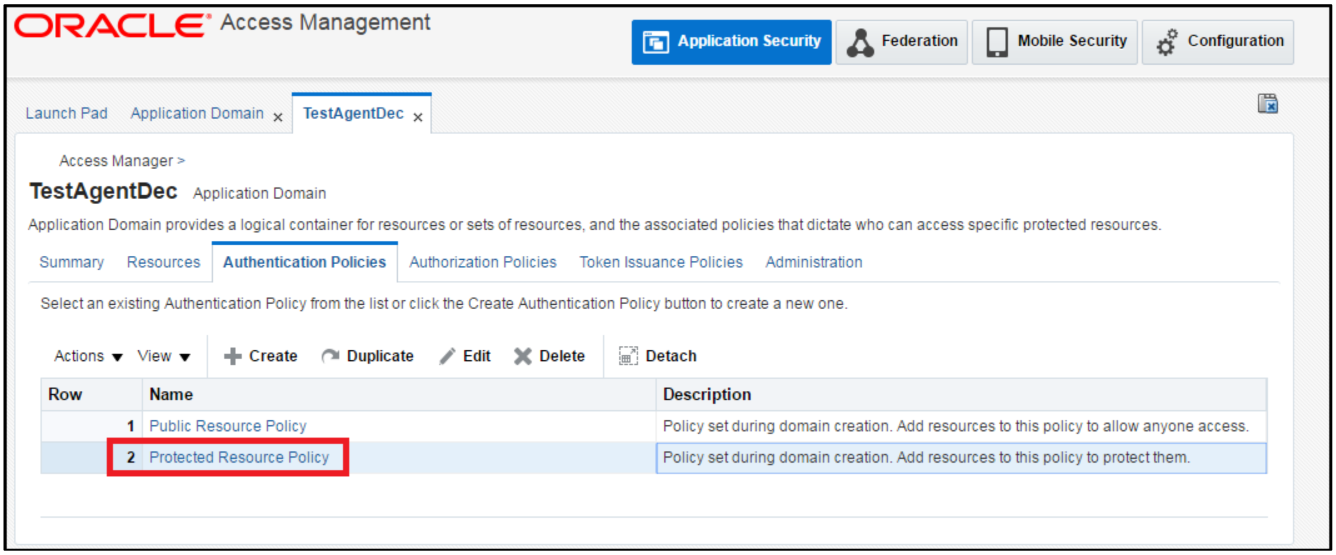
Name

Search Results

Row	Name	Description
1	Fusion Apps Integration	Policy objects enabling integration with Oracle Fusion Applications
2	IAM Suite	Policy objects enabling OAM Agent to protect deployed IAM Suite applications
3	RREG_OAM11G	
4	TestAgentDec	Application Domain created through Remote Registration

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

3. On **Authentication Policies** tab, click **Protected Resource Policy**.



TestAgentDec Application Domain

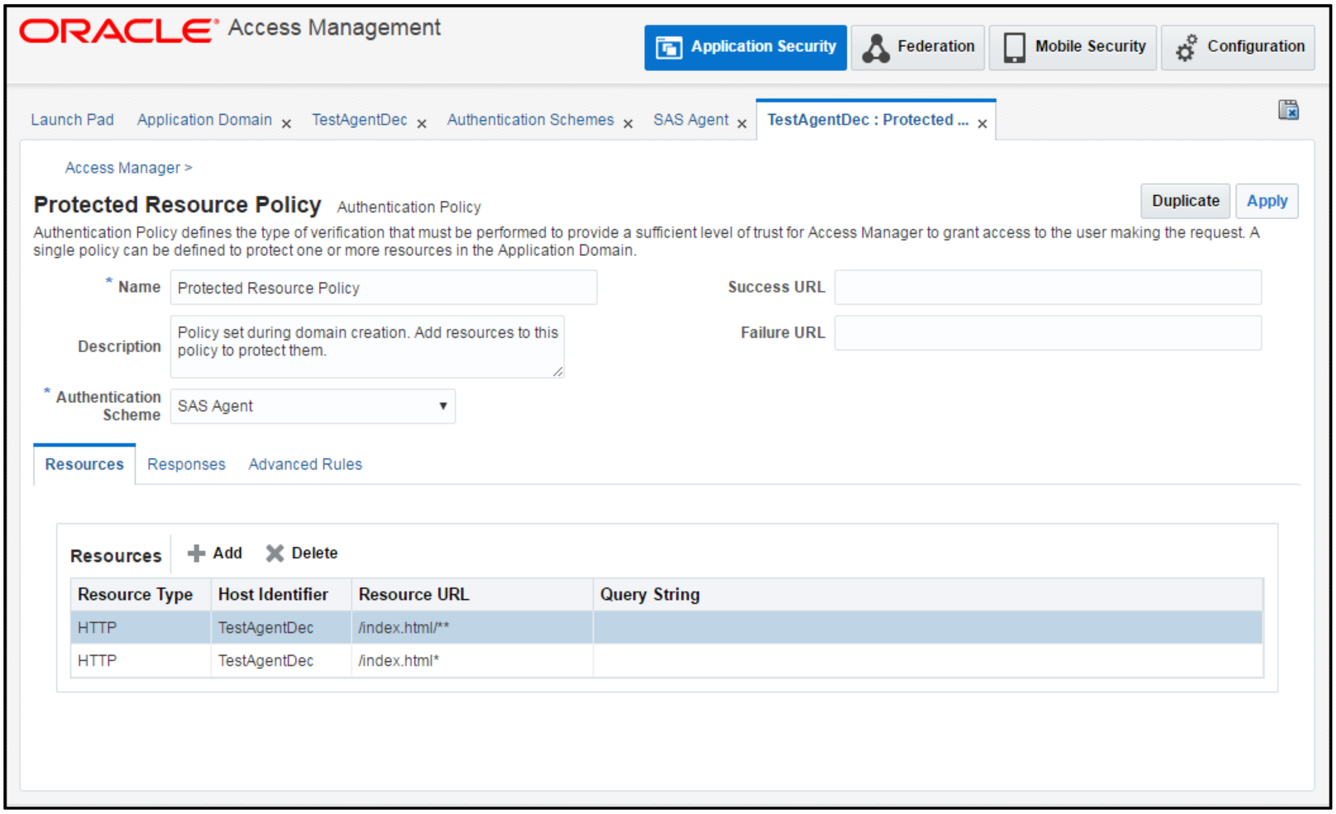
Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

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

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.

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

4. In **Authentication Scheme** field, select the authentication scheme (for example, **SafeNet Agent**), and click **Apply**.



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 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

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

* Authentication Scheme: SAS Agent

Success URL:

Failure URL:

Resources

Resource Type	Host Identifier	Resource URL	Query String
HTTP	TestAgentDec	/index.html/**	
HTTP	TestAgentDec	/index.html*	

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

Configuring WebLogic Server

1. Login to Linux server hosting WLS using SSH.
2. Shut down the entire domain, including the WebLogic Admin server and all the OAM managed servers.
3. Create a backup of the existing file before editing.
4. In the `oam-config.xml` file, locate the version number that needs to be incremented by one to ensure that the changes are not overwritten by the console. The version number will occur near the top of the file.

```
<Setting xmlns="http://www.w3.org/2001/XMLSchema" Name="NGAMConfiguration"
Type="htf:map">

...

<Setting Name="Version" Type="xsd:integer">175</Setting>

...

</Setting>
```

5. After the Profile Node, mentioned in step 4, add the following XML code (if not already present):

```
<Setting xmlns="http://www.w3.org/2001/XMLSchema" Name="NGAMConfiguration"
Type="htf:map">

...

<Setting Name="Server" Type="htf:map">

<Setting Name="NGAMServer" Type="htf:map">

...

   <Setting Name="Profile" Type="htf:map">

   <Setting Name="Security" Type="htf:map">

   <Setting Name="TrustedInput" Type="htf:map">

   <Setting Name="DEFAULT" Type="xsd:string">4000-null-false</Setting>

<Setting Name="DEFAULT_PARAMETER" Type="xsd:string">4000-null-false</Setting>

  </Setting>

<!--

 <Setting Name="blockUrls" Type="htf:list">
    <Setting Name="0" Type="xsd:string">/oam/server/auth_cred_submit</Setting>
    <Setting Name="1"
Type="xsd:string">/oam/server/sso/auth_cred_submit</Setting>
    <Setting Name="2" Type="xsd:string">/oam/server/authentication</Setting>
    <Setting Name="3" Type="xsd:string">/oam/server/oaam/cred_submit</Setting>
    <Setting Name="4" Type="xsd:string">/oam/server/dap/cred_submit</Setting>
    <Setting Name="5" Type="xsd:string">/oam/server/osso_auth</Setting>
    <Setting Name="6"
Type="xsd:string">/oam/server/imp_consent_submit</Setting>
    <Setting Name="7" Type="xsd:string">/oam/server/changePassword</Setting>
  </Setting> -->

  </Setting>

...

 </Setting>
```

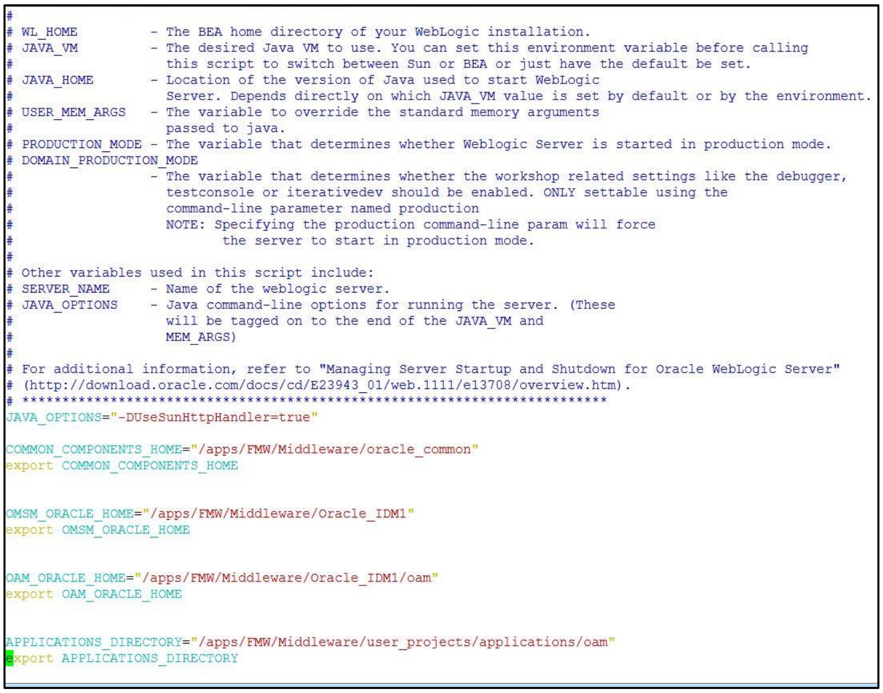
> **NOTE:** Uncomment (remove <!-- and -->) the commented section in case of 12c version.

6. Save changes. Restart the WebLogic Admin server, followed by the OAM managed servers.
7. To verify, check `<DOMAIN_HOME>/config/fmwconfig/oam-config.xml` on each of the OAM managed server nodes, to ensure that the updated version has been propagated correctly.

For SSL-enabled SafeNet Server Machines

If the certificate policy is different in WebLogic and stand-alone Java programs, it is advised to use the standard Sun SSL implementation. The following setting is mandatory, if you are using the **HTTPS** protocol.

1. Set `-DUseSunHttpHandler` flag to `true` in the WLS startup script (below comments block) available at the following location:
   `<WLS-INSTALL-PATH>/oracle/Middleware/user_projects/domains/OAMdomain/bin/setDomainEnv.sh`



```
#
# WL_HOME         - The BEA home directory of your WebLogic installation.
# JAVA_VM         - The desired Java VM to use. You can set this environment variable before calling
#                   this script to switch between Sun or BEA or just have the default be set.
# JAVA_HOME       - Location of the version of Java used to start WebLogic
#                   Server. Depends directly on which JAVA_VM value is set by default or by the environment.
# USER_MEM_ARGS   - The variable to override the standard memory arguments
#                   passed to java.
# PRODUCTION_MODE - The variable that determines whether Weblogic Server is started in production mode.
# DOMAIN_PRODUCTION_MODE
#                 - The variable that determines whether the workshop related settings like the debugger,
#                   testconsole or iterativedev should be enabled. ONLY settable using the
#                   command-line parameter named production
#                   NOTE: Specifying the production command-line param will force
#                          the server to start in production mode.
#
# Other variables used in this script include:
# SERVER_NAME     - Name of the weblogic server.
# JAVA_OPTIONS    - Java command-line options for running the server. (These
#                   will be tagged on to the end of the JAVA_VM and
#                   MEM_ARGS)
#
# For additional information, refer to "Managing Server Startup and Shutdown for Oracle WebLogic Server"
# (http://download.oracle.com/docs/cd/E23943_01/web.1111/e13708/overview.htm).
# *************************************************************************
JAVA_OPTIONS="-DUseSunHttpHandler=true"

COMMON_COMPONENTS_HOME="/apps/FMW/Middleware/oracle_common"
export COMMON_COMPONENTS_HOME


OMSM_ORACLE_HOME="/apps/FMW/Middleware/Oracle_IDM1"
export OMSM_ORACLE_HOME


OAM_ORACLE_HOME="/apps/FMW/Middleware/Oracle_IDM1/oam"
export OAM_ORACLE_HOME


APPLICATIONS_DIRECTORY="/apps/FMW/Middleware/user_projects/applications/oam"
export APPLICATIONS_DIRECTORY
```

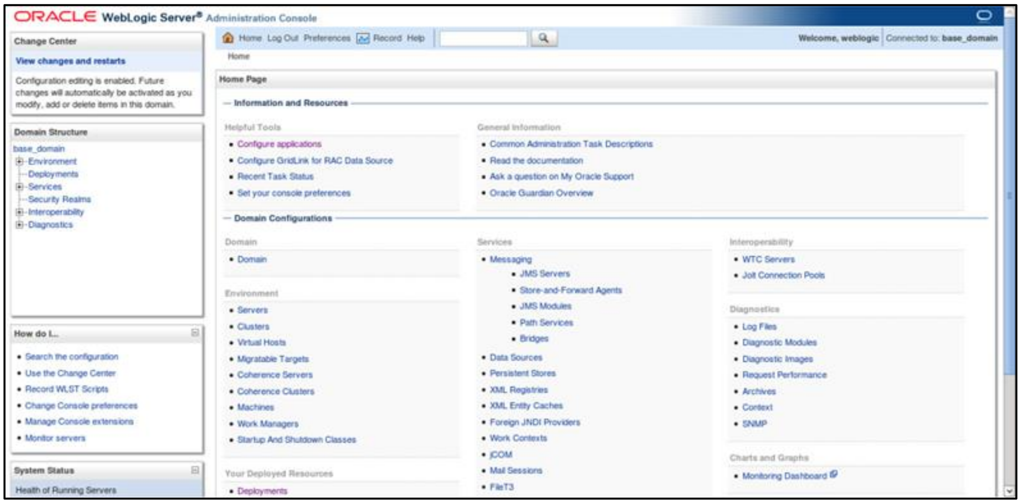
2. Restart the WebLogic Server.

> **NOTE:** Configuring WebLogic Server is important to avoid SSL connection, certificate validation, and SSL handshake errors.

Deploying Agent on WebLogic Server

Deploy agent's `.war` file on the WLS.

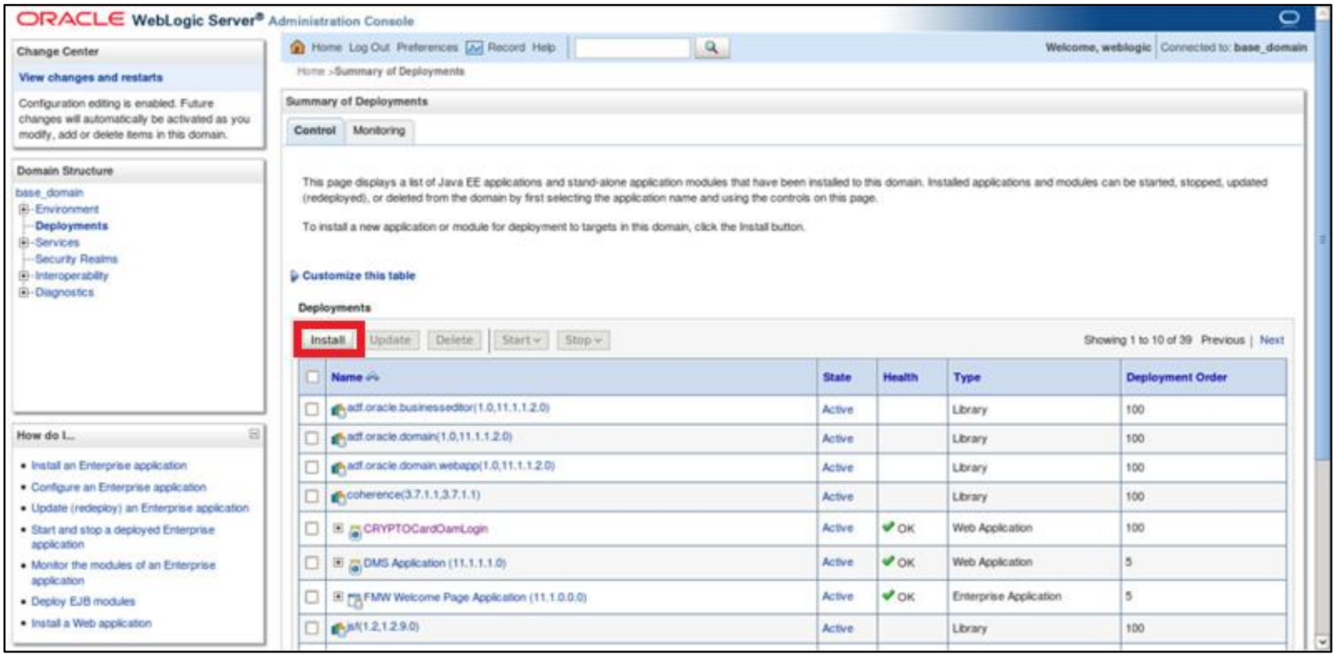
1. Login to WLS web interface.



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

2. From the left pane, under **Domain Structure**, click **Deployments**. In the right pane, click **Install**.


ORACLE WebLogic Server® Administration Console
Change Center
View changes and restarts
Domain Structure
base_domain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Install an Enterprise application
Configure an Enterprise application
Update (redeploy) an Enterprise application
Start and stop a deployed Enterprise application
Monitor the modules of an Enterprise application
Deploy EJB modules
Install a Web application
Home Log Out Preferences Record Help
Welcome, weblogic
Connected to: base_domain
Home >Summary of Deployments
Control
Monitoring
Customize this table
Install
Update
Delete
Start
Stop
Showing 1 to 10 of 39 Previous | Next

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Summary of Deployments

This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on this page.

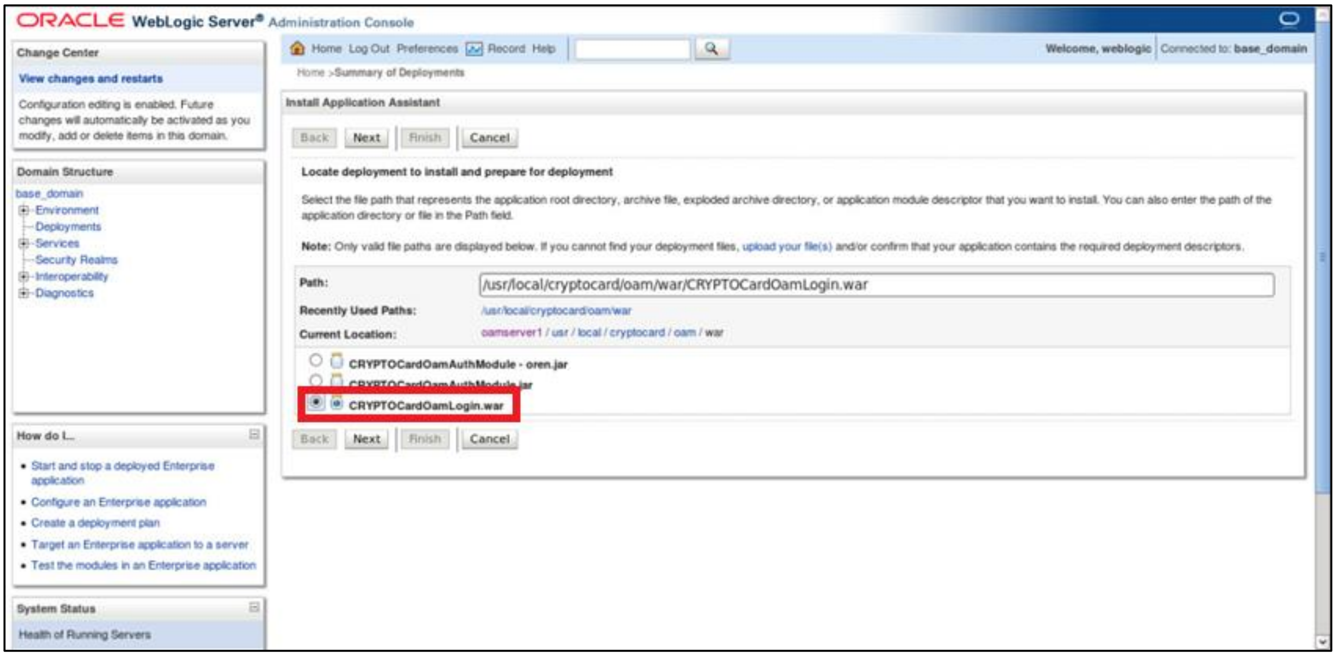
To install a new application or module for deployment to targets in this domain, click the Install button.

Deployments

□	Name	State	Health	Type	Deployment Order
□	adf.oracle.businesseditor(1.0,11.1.1.2.0)	Active		Library	100
□	adf.oracle.domain(1.0,11.1.1.2.0)	Active		Library	100
□	adf.oracle.domain.webapp(1.0,11.1.1.2.0)	Active		Library	100
□	coherence(3.7.1.1,3.7.1.1)	Active		Library	100
□	CRYPTOCardOamLogin	Active	✓ OK	Web Application	100
□	DMS Application (11.1.1.1.0)	Active	✓ OK	Web Application	5
□	FMW Welcome Page Application (11.1.0.0.0)	Active	✓ OK	Enterprise Application	5
□	jsf(1.2,1.2.9.0)	Active		Library	100

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

3. On **Install Application Assistant**, select the **CRYPTOCardOamLogin.war** file from the agent installation folder (`/usr/local/cryptocard/oam/war/`), and click **Next**.


ORACLE WebLogic Server® Administration Console
Change Center
View changes and restarts
Domain Structure
base_domain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Start and stop a deployed Enterprise application
Configure an Enterprise application
Create a deployment plan
Target an Enterprise application to a server
Test the modules in an Enterprise application
System Status
Health of Running Servers
Home Log Out Preferences Record Help
Welcome, weblogic
Connected to: base_domain
Home >Summary of Deployments
Back
Next
Finish
Cancel

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Install Application Assistant

Locate deployment to install and prepare for deployment

Select the file path that represents the application root directory, archive file, exploded archive directory, or application module descriptor that you want to install. You can also enter the path of the application directory or file in the Path field.

Note: Only valid file paths are displayed below. If you cannot find your deployment files, upload your file(s) and/or confirm that your application contains the required deployment descriptors.

Path: /usr/local/cryptocard/oam/war/CRYPTOCardOamLogin.war

Recently Used Paths: /usr/local/cryptocard/oam/war

Current Location: oamserver1 / usr / local / cryptocard / oam / war

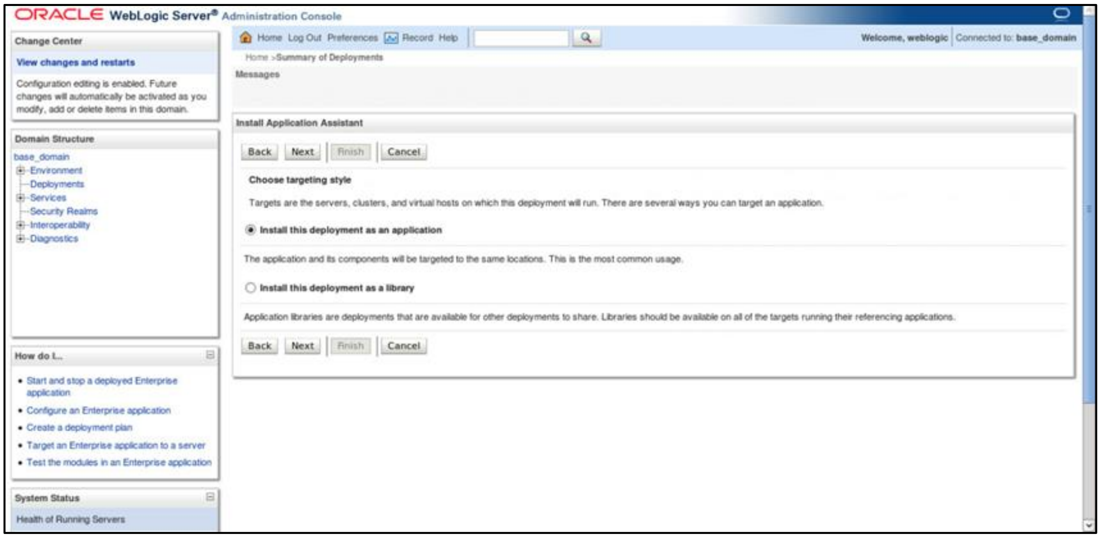
○ CRYPTOCardOamAuthModule - oren.jar

○ CRYPTOCardOamAuthModule.jar

● CRYPTOCardOamLogin.war

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

4. Under **Choose targeting style**, select **Install this deployment as an application**, and click **Next**.


ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic
Connected to: base_domain
Change Center
View changes and restarts
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.
Domain Structure
base_domain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Start and stop a deployed Enterprise application
Configure an Enterprise application
Create a deployment plan
Target an Enterprise application to a server
Test the modules in an Enterprise application
System Status
Health of Running Servers
Home >Summary of Deployments
Messages
Back
Next
Finish
Cancel

Install Application Assistant

Choose targeting style

Targets are the servers, clusters, and virtual hosts on which this deployment will run. There are several ways you can target an application.

● Install this deployment as an application

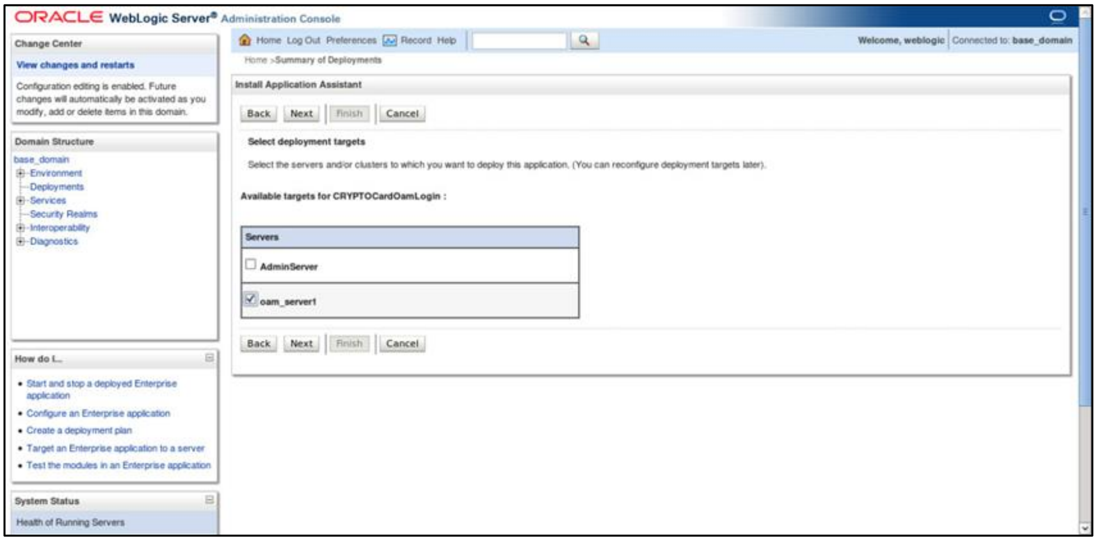
The application and its components will be targeted to the same locations. This is the most common usage.

○ Install this deployment as a library

Application libraries are deployments that are available for other deployments to share. Libraries should be available on all of the targets running their referencing applications.

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

5. Under **Select deployment targets**, select the OAM server, and click **Next**.


ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic
Connected to: base_domain
Change Center
View changes and restarts
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.
Domain Structure
base_domain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Start and stop a deployed Enterprise application
Configure an Enterprise application
Create a deployment plan
Target an Enterprise application to a server
Test the modules in an Enterprise application
System Status
Health of Running Servers
Home >Summary of Deployments
Back
Next
Finish
Cancel

Install Application Assistant

Select deployment targets

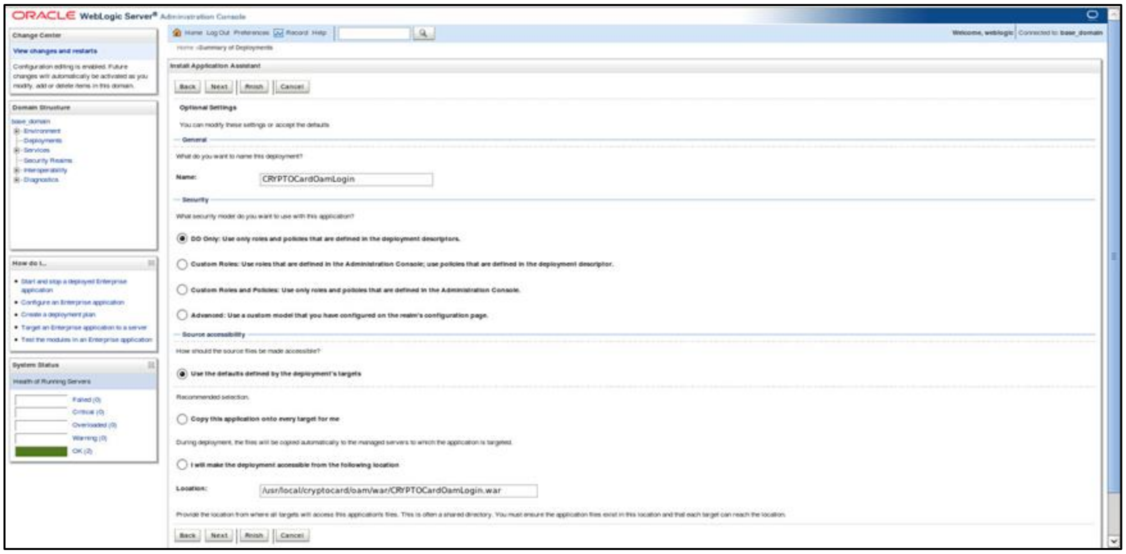
Select the servers and/or clusters to which you want to deploy this application. (You can reconfigure deployment targets later).

Available targets for CRYPTOCardOamLogin :

Servers
☐ AdminServer
☑ oam_server1

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

6. Under **Optional Settings**, make no changes to the default configurations. Click **Finish**.



ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: base_domain
Home >Summary of Deployments
Back Next Finish Cancel

Install Application Assistant

Optional Settings

You can modify these settings or accept the defaults

General

What do you want to name this deployment?

Name: CRYPTOCardOamLogin

Security

What security model do you want to use with this application?

● DD Only: Use only roles and policies that are defined in the deployment descriptors.

○ Custom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor.

○ Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console.

○ Advanced: Use a custom model that you have configured on the realm's configuration page.

Source accessibility

How should the source files be made accessible?

● Use the defaults defined by the deployment's targets

Recommended selection.

○ Copy this application onto every target for me

During deployment, the files will be copied automatically to the managed servers to which the application is targeted.

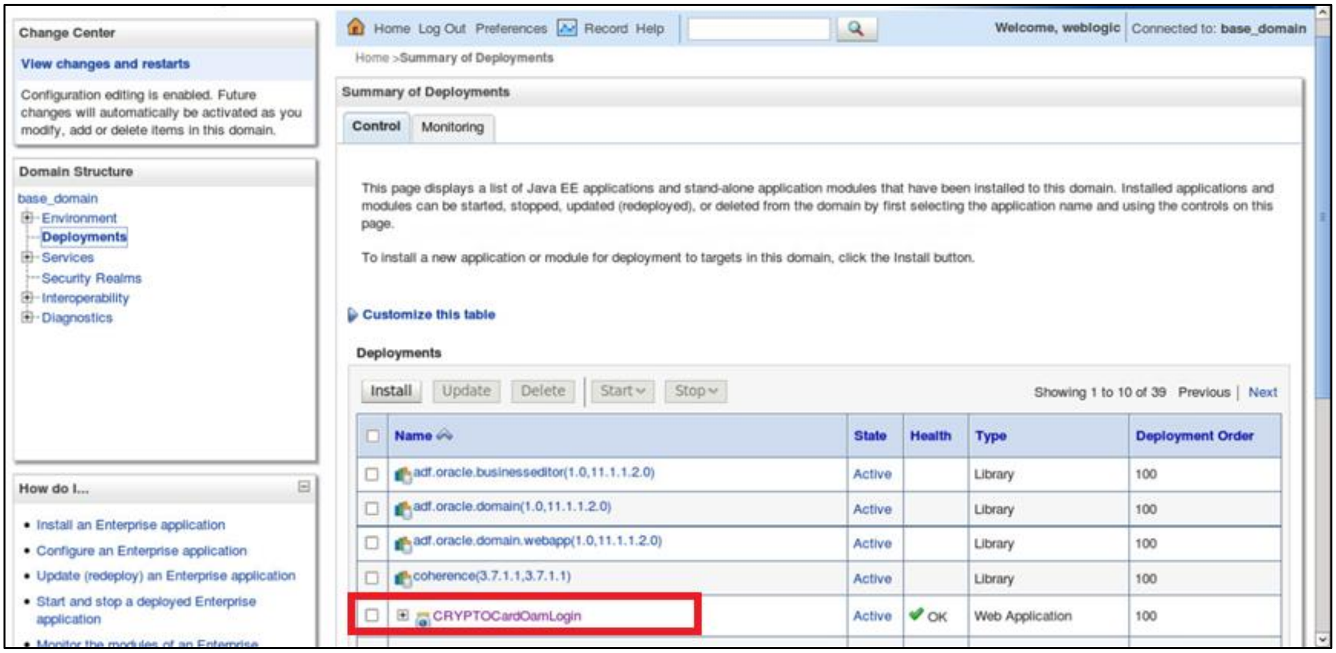
○ I will make the deployment accessible from the following location

Location: /usr/local/cryptocard/oam/war/CRYPTOCardOamLogin.war

Provide the location from where all targets will access this application's files. This is often a shared directory. You must ensure the application files exist in this location and that each target can reach the location.

(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

7. From the left pane, under **Domain Structure**, click **Deployments**. In the right pane under listed **Deployments**, verify if the **State** of the **CRYPTOCardOamLogin** agent is **Active**.



Home Log Out Preferences Record Help
Welcome, weblogic Connected to: base_domain
Home >Summary of Deployments
Change Center
View changes and restarts
Domain Structure
base_domain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Install an Enterprise application
Configure an Enterprise application
Update (redeploy) an Enterprise application
Start and stop a deployed Enterprise application
Monitor the modules of an Enterprise
Control
Monitoring
Customize this table
Install Update Delete Start Stop
Showing 1 to 10 of 39 Previous | Next

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Summary of Deployments

This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on this page.

To install a new application or module for deployment to targets in this domain, click the Install button.

Deployments

□	Name	State	Health	Type	Deployment Order
□	adf.oracle.businesseditor(1.0,11.1.1.2.0)	Active		Library	100
□	adf.oracle.domain(1.0,11.1.1.2.0)	Active		Library	100
□	adf.oracle.domain.webapp(1.0,11.1.1.2.0)	Active		Library	100
□	coherence(3.7.1.1,3.7.1.1)	Active		Library	100
□	CRYPTOCardOamLogin	Active	✓ OK	Web Application	100

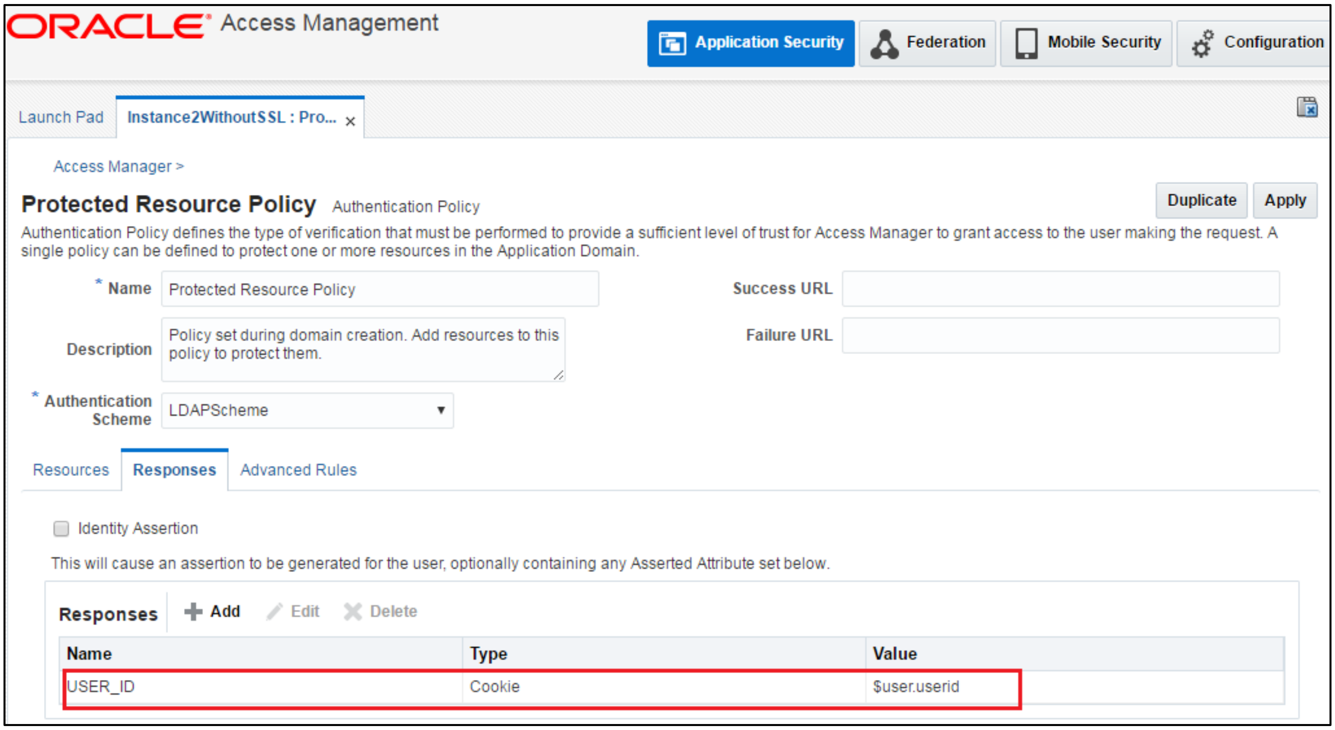
(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

Cookie Settings for Step-Up Authentication

1. On the Oracle Access Management portal, under **Access Manager**, click **Application Domains**.
2. Click **Search**. Under **Search Results**, click the Level 1 protected resource **Application Domain**.
   Level 1 protected resource is a resource protected with Level 1 (Username and Password) authentication.
3. On **Authentication Policies** tab, click **Protected Resource Policy**.
4. Click **Responses** tab.

5. Click **Add**, and add the cookie with following settings.

Name	USER_ID Cookie name (USER_ID) must match the name of cookie variable set using USER_LOGIN_ID_NAME variable in Configuring .ini File section.
Type	Cookie
Value	$user.userid



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 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
Description	Policy set during domain creation. Add resources to this policy to protect them.
* Authentication Scheme	LDAPScheme
Success URL	
Failure URL	

□ Identity Assertion

This will cause an assertion to be generated for the user, optionally containing any Asserted Attribute set below.

Responses

Name	Type	Value
USER_ID	Cookie	$user.userid

For information on Step-Up Authentication, including how the authentication flow differs based on the resource type, click here.

CHAPTER 4: SafeNet Server Configuration

The deployment of MFA with OAM using SAML authentication requires:

1. Creating Users' Store in SafeNet Server
2. Assigning an Authenticator in SafeNet Server
3. Configuring SafeNet Server Auth Node and Encryption Key

Creating Users' Store

Before SafeNet server can start authenticating users, you need to create a users' store that reflects the users who will be required to use MFA. User records are created in the SafeNet server user store using one of the following methods:

- Manually,
  - One user at a time, using the **Create User** shortcut.
  - By importing one or more user records via a flat file.
- Automatically, by synchronizing with your AD/LDAP server using the SafeNet Synchronization Agent.

For additional details on importing users to SafeNet server, refer "Creating Users" section in the ***SafeNet Authentication Service Subscriber Account Operator Guide***.

Assigning Authenticator

The SafeNet server supports a number of authentication methods that can be used as the second authentication factor for users authenticating through OAM. The following authenticators are supported:

- eToken PASS
- SMS tokens
- MP-1 software token
- GrIDsure
- MobilePASS

Authenticators can be assigned to users in two ways:

- **Manual Provisioning** — Assign an authenticator to users one at a time.
- **Provisioning Rules** — The administrator can set provisioning rules in SafeNet server, in such a way that the rules will be triggered when group memberships and other user attributes change. In such cases, an authenticator will be assigned automatically to users.

Refer “Provisioning Rules” section in the ***SafeNet Authentication Service Subscriber Account Operator Guide*** to learn how to provision different authentication methods to users in the SafeNet server users’ store.

Configuring SafeNet Server Auth Node

If the SafeNet server is not installed on the same machine as AD, the following steps must be performed:

1. Click **Virtual Servers** > **Comms** > **Auth Nodes**.
2. Click **Auth Nodes** link and select **Add**.
3. Complete the following fields, and click **Save**.

Agent Description	Type a description for this node (for example, **DC**).
Host Name	Type a host name.
Low IP Address In Range	Type the low IP address.
High IP Address In Range	Type the high IP address. (The low and high IP addresses may be the same since the node is referencing a single machine.)
Exclude from PIN change requests	Do not select this check box.

CHAPTER 5: Running the Solution

Step-Up Authentication

An application can have both low and high (containing sensitive data) value resources, and requirements for accessing them must be different. With **Step-Up Authentication**, the administrators can set different authentication rules for different types of resources. Instead of having a user go through the complete login process (if the user is accessing a high value resource after accessing a low value resource), the step-up authentication invokes a friendlier flow, which enquires only for the relevant, second factor of authentication.

Based on the type of resource, the authentication flow differs.

1. Level 1 Protected Resource
   [Resources Protected with Level 1 (Username and Password) Authentication]
2. Level 2 Protected Resources
   [Resources Protected with Level 2 (Username, Password and Token) Authentication]
   a. With Existing LDAP Authentication
   b. Without Existing LDAP Authentication

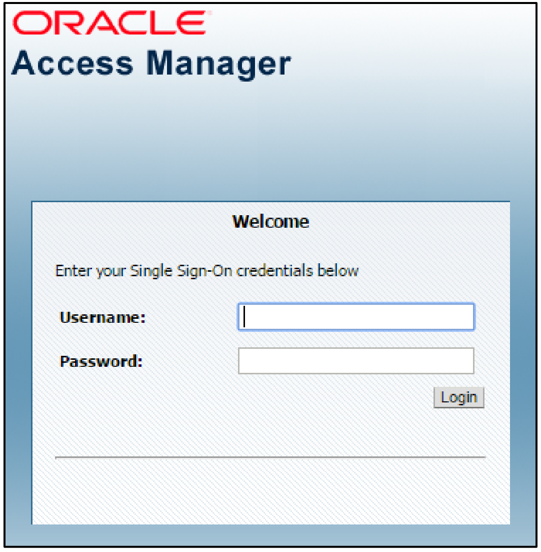
> **NOTE:** For the step-up authentication to work, the cookie must be added (refer Cookie Settings for Step-Up Authentication section).

Level 1 Protected Resources

Once the configurations are complete, login to the protected resource and test the solution, by following the steps.

1. Open a browser and visit the resource.

2. You will be redirected to the LDAP login window.



ORACLE
Access Manager

Welcome

Enter your Single Sign-On credentials below

Username:

Password:

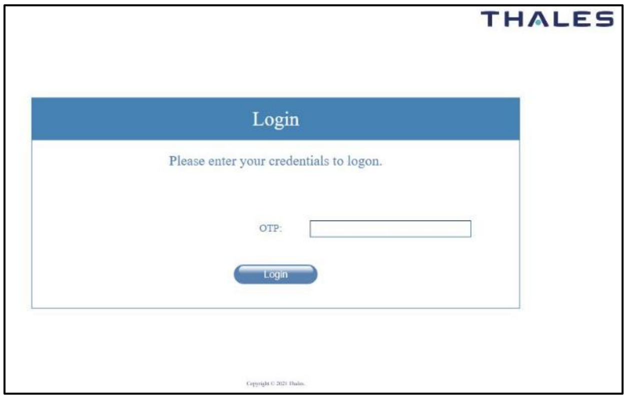
3. Enter your **Username** and **Password**, and click **Login**.
4. After successful LDAP authentication, the user will be redirected to access the resource.

Hello World

Level 2 Protected Resources - With Existing LDAP Authentication

Once the configurations are complete, login to the protected resource and test the solution, by following the steps. This process assumes that the user has already done the LDAP authentication and wants to access another resource protected with a higher authentication level.

1. Open a browser and visit the resource.
2. You will be redirected to the SafeNet login window.
3. Follow the steps, based on the type of token selected:
    i. If the selected token type is OTP, enter **OTP**, and click **Login**.

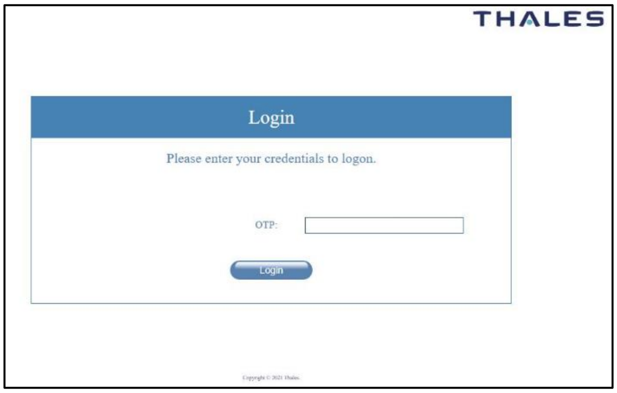


Login

Please enter your credentials to logon.

ii. If the selected token type is **GrIDsure** or **Challenge-Response**,

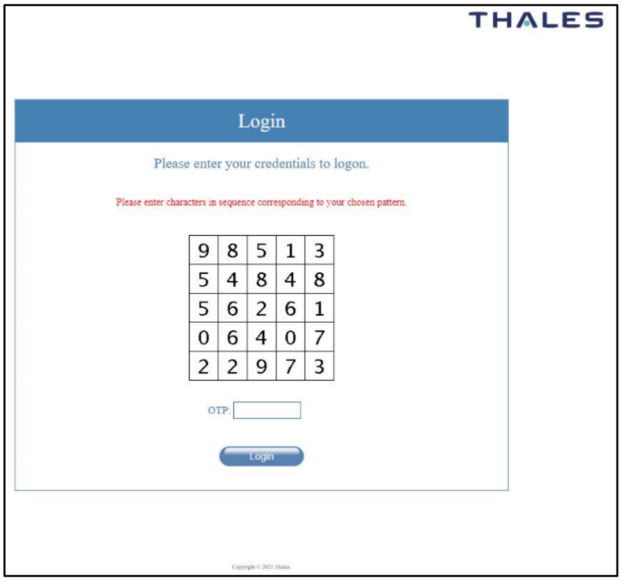
a. Keeping the **OTP** field, blank, click **Login**.



Login

Please enter your credentials to logon.

b. The following window will be displayed, that will help the user to complete authentication by the selected token type.



Login

Please enter your credentials to logon.

Please enter characters in sequence corresponding to your chosen pattern.

9	8	5	1	3
5	4	8	4	8
5	6	2	6	1
0	6	4	0	7
2	2	9	7	3

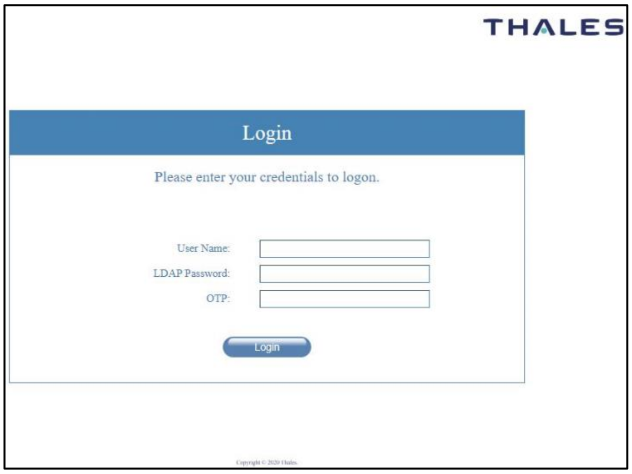
4. After successful authentication, the user will be redirected to access the protected resource.

Hello World

Level 2 Protected Resources - Without Existing LDAP Authentication

Once the configurations are complete, login to the protected resource and test the solution, by following the steps.

1. Open a browser and visit the resource.
2. You will be redirected to the SafeNet login window.
3. Follow the steps, based on the type of token selected:
   i. If the selected token type is **OTP**, enter your **User Name**, **LDAP Password**, and **OTP**, and click **Login**.



Login

Please enter your credentials to logon.

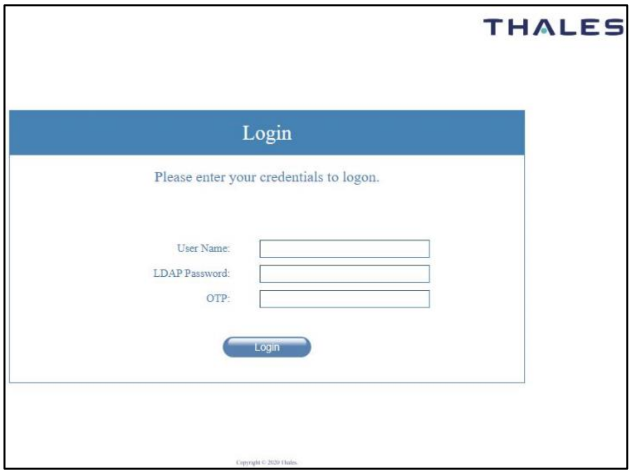
User Name:

LDAP Password:

OTP:

Copyright © 2020 Thales.

   ii. If the selected token type is **GrIDsure** or **Challenge-Response**,
      a. Enter your **User Name**, **LDAP Password**, and click **Login** (keeping the OTP field, blank).



Login

Please enter your credentials to logon.

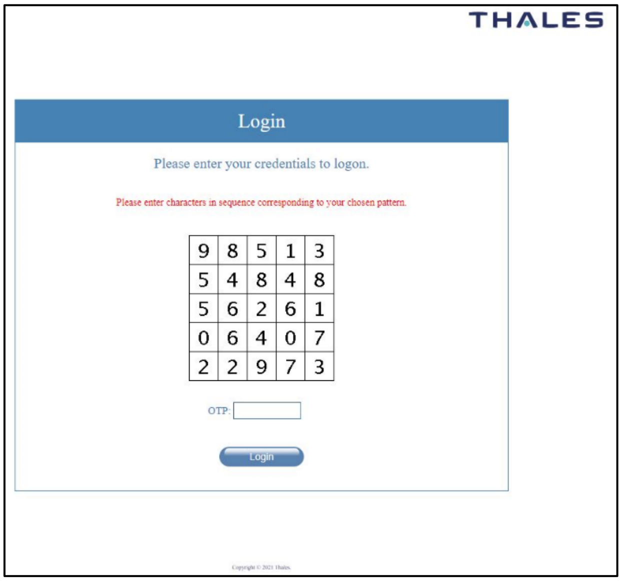
User Name:

LDAP Password:

OTP:

Copyright © 2020 Thales.

b. The following window will be displayed, that will help the user to complete authentication by the selected token type.



Login

Please enter your credentials to logon.

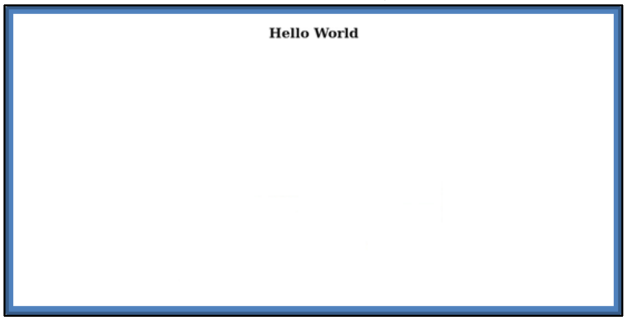
Please enter characters in sequence corresponding to your chosen pattern.

9	8	5	1	3
5	4	8	4	8
5	6	2	6	1
0	6	4	0	7
2	2	9	7	3

OTP:

Copyright © 2021 Thales.

4. After successful authentication, the user will be redirected to access the protected resource.



Hello World

CHAPTER 6: Troubleshooting

Settings File and Directory Permissions

Administrators must secure file and directory access permissions.
For example,

- The READ-ONLY access permission must be set to the **.ini** file for the WLS or OAM process owner. The plugin and web applications will require READ-ONLY permissions for the **.ini** file, key file, resource directory, as well as files in the same directory.
- The WRITE access permission must be set to log directory for the WLS/OAM process owner.