

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

Copyright © 2021 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

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 noninfringement. 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	
Customer Release Notes	6
Audience	6
Third-Party Software Acknowledgement	6
Document Conventions	6
Command Syntax and Typeface Conventions	6
Notifications and Alerts	
Related Documents	8
Support Contacts	8
Customer Support Portal	8
Telephone Support	
Email Support	8
CHAPTER 1: Introduction	9
Overview	9
Prerequisites	
Applicability	
Multi-Factor Authentication	10
CHAPTER 2: Oracle Access Manager Configuration for R2 Version	
Installing SafeNet Agent Plugin	
Configuring .ini File	
Agent Encryption Key File	
Importing SafeNet Agent Plugin	
Creating Authentication Module	
Creating Authentication Scheme	
Forcing Authentication Scheme on Protected Resource	
Configuring WebLogic Server	
For SSL-enabled SafeNet Server Machines	
Deploying Agent on WebLogic Server	
Cookie Settings for Step-Up Authentication	
CHAPTER 3: Oracle Access Manager Configuration for R3 and 12c	Version 31
Installing SafeNet Agent Plugin	
Configuring .ini File	
Agent Encryption Key File	
Importing SafeNet Agent Plugin	
Creating Authentication Module	
Creating Authentication Scheme	
Forcing Authentication Scheme on Protected Resource	
Configuring WebLogic Server	
For SSL-enabled SafeNet Server Machines	47
Deploying Agent on WebLogic Server	
Cookie Settings for Step-Up Authentication	51

Creating Users' Assigning Authe	SafeNet Server Configuration Store enticator eNet Server Auth Node	53 53
Step-Up Auther Level 1 Protec Level 2 Protec	Running the Solution tication cted Resources cted Resources - With Existing LDAP Authentication cted Resources - Without Existing LDAP Authentication	55 55 56
	Troubleshooting d Directory Permissions	

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 <i>Installation Guide</i> 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></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>]</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.</variable></variables>
[a b c] [<a> <c>]</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> <c> }</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.</variables>

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 <u>Thales</u> <u>Customer Support</u>.

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 <u>https://supportportal.thalesgroup.com</u>, 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 <u>technical.support.DIS@thalesgroup.com</u>.

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.

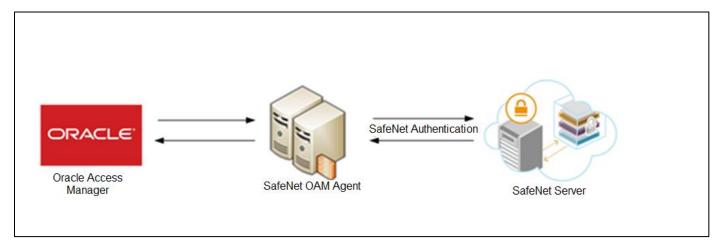
Strong authentication is made easy through the flexibility and scalability of SafeNet's automated workflows, vendor-agnostic token integrations, and broad APIs. In addition, management capabilities and processes are fully automated and customizable—providing a seamless and enhanced user experience.

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 <u>SafeNet Authentication Service Downloads</u> 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

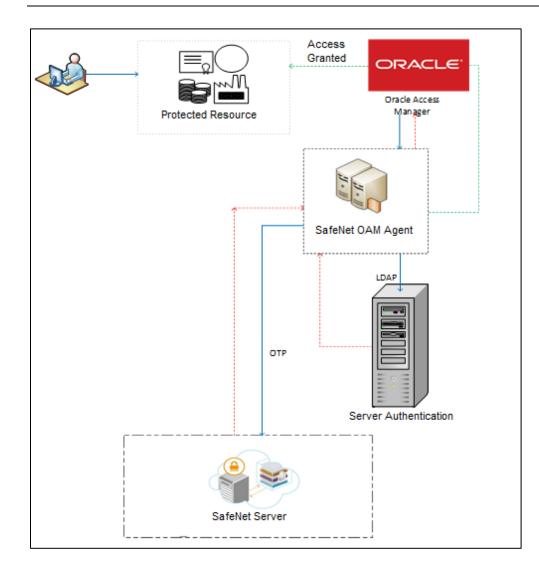
The information in this document applies to the following:

- > 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.



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. <u>Deploying the Agent on the WebLogic Server</u>

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/

					oar	n - File Browser				_ = x
File Edit View	Go	Bookmarks Tabs He	lp							
Back 🗸 🔳	Forv	vard 🗸 🛧 🙆 😭			£9.					
📄 💷 usr	local	cryptocard oam					Q	50% 🤇	List View	0
Tree∨	×	Name	~	Size	Туре	Date Modified				
👂 🚞 net	~	> 🚞 bin		1 item	folder	Sun 27 Mar 2016 10:56:23 PM IDT				
P i opt	C	bsidkey		1 item	folder	Sun 27 Mar 2016 10:56:23 PM IDT				
proc	0	🕨 🚞 defaults		5 items	folder	Sun 27 Mar 2016 10:56:23 PM IDT				
🕨 📷 root	C	> 🚞 ini		1 item	folder	Sun 17 Apr 2016 03:38:04 PM IDT				
Þ 🚞 sbin	0	o 💼 log		8 items	folder	Sun 01 May 2016 02:06:13 PM IDT				
👂 🚞 selinux	C	> 🚞 Open Source Lice	enses	21 items	folder	Sun 27 Mar 2016 10:56:23 PM IDT				
Image: Single		🗧 🚞 war		2 items	folder	Sun 27 Mar 2016 10:56:23 PM IDT				
 sys tmp 		CRYPTOCard-lice	nse.txt	9.4 KB	plain text document	Tue 10 Jun 2014 07:18:50 AM IDT				
Unp		oamPostinstall.s	h	755 bytes	shell script	Tue 10 Jun 2014 07:18:52 AM IDT				
✓ in usr		oamPreUninstall	sh	574 bytes	shell script	Tue 10 Jun 2014 07:18:51 AM IDT				
Þ 🚞 bin	=									
Þ 🚞 etc										
👂 🚞 games										
Include										
Þ 🚞 lib										
Iib64										
Iibexec										
Ideal										
	a									
▶ 🛅 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 <u>BSID</u> 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).</iamdemo.oracle.com>

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 <u>Cookie</u> <u>name value</u> set in <u>Cookie Settings for Step-Up Authentication</u> section.
IGNORE_CERTIFICATE_ERR ORS	 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.

ORACLE Access Management	Accessibility Help Sign	Out weblogic S
Launch Pad		
Welcome to Oracle Access Management		0
& Quick Start Wizards	G Access Manager	+•
C Application Registration	Application Domains Applications Applicatio	
Identity Federation + • Identity Provider Administration Identity Federation Identity Service Provider Administration ••••••••••••••••••••••••••••••••••••	Security Token Service Image: Constraint of the service Image: Partners Image: Constraint of the service	+•
Mobile and Social Mobile Services CAuth Service	Access Portal Service Access Portal Service Codential Sharing Groups Codential Sharing Groups Codential Sharing Codential Service	+•

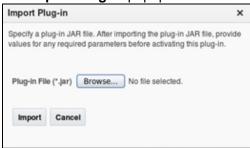
(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

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

New Import Plug-in Distribute Selected X Deactivate Selected X Remove Selected Import Plug-in Activation Status Type Last updated iow Plug-in Name Description Activated Authentication Activated Authentication Import Plug-in Import Plug-in Import Plug-in Import Plug-in Activated Authentication Import Plug-in Import Plug-in	Last updated by
Pkup in Name Description Activation Status Type Last updated in II Basic/FedModelidentBerPlugin Activation Status Type Last updated in 2 CredentIalColectPrUpin Activation Activation Activation 3 EssoProvisioningPlugin Activation Activated Authentication 4 FedAthrbuckRequestPlugin Activated Authentication Activated 5 FedAuhnRequestPlugin Activated Authentication Activated 6 FedAuhnRequestPlugin Activated Authentication Activated	Last updated by
I Bask/FedModeldentRerPlugin Activated Authentication 2 CredentalColectorPlugin Activated Authentication 3 EsseProvisioningPlugin Activated Authentication 4 FedMtmbueRequestPlugin Authentication Authentication 5 FedMumRequestPlugin Activated Authentication 6 FedModeldentifierPlugin Activated Authentication	
2 CredentaColectorPlugin Activated Authentication 3 EssOProvisioning/Plugin Activated Authentication 4 FedAttributeRequestPlugin Activated Authentication 5 FedAturRequestPlugin Activated Authentication 6 FedModaldertifierPlugin Activated Authentication	
4 FedAtributeRequesiPlugin Activated Authentication 5 FedAuthnRequestPlugin Activated Authentication 6 FedNodeldentifierPlugin Activated Authentication	
5 FedAuthnRequestPlugin Activated Authentication 6 FedModeldentifierPlugin Activated Authentication	
6 FedModelentiferPlugin Activated Authentication	
7 FedProgramaticAuthrPlugin Activated Authentication	
8 FedUserAuthenticationPlugin Activated Authentication	
9 FedUserProvisioningPlugin Activated User Provisioning	
10 GenericStatePlugin Activated Authentication	
11 HTTPTokenExtractor Activated Authentication	
12 IPFUserForgotPasswordPlugin Activated Authentication	
	Total Row
Plug-In Details: BasicFedModeldentIfierPlugin Activation Status Configuration Parameters	

(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.



(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.

	File Upload			
📄 💷 usr loca	l cryptocard oam war			
Places	Name	~	Size	Modified
🙀 Search	CRYPTOCardOamAuthModule.jar			06/10/2014
Recently Used	CRYPTOCardOamLogin.war		124.4 KB	06/10/2014
is root root File System				
Documents				
Pictures				
💼 Videos				
Downloads				
ф. н.				All Files
		(Cancel	Open

(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.

lug-	ins									
View	 Import Plug-in Distribute Selection 	ed 💠 Activate Selected	X Deactivate Selected	X Remove Selected	8					
low	Plug-in Name	Description				Activation Status	Type	Last updated On	Last updated by	
	23 TAPIdentityPlugIn					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 23:24:1	2 OAMSystemAdmi	i
									Total Rows	
	n Details: CRYPTOCardOamAuthModule									
	tion Status Configuration Parameters * INI_FILE_FULLPATH /usr/local/or								Se	5
• EN	CRYPTION_LIBRARY_FULLPATH /usr/local/cr	ryptocardioam/bin/x64/8								

SafeNet Agent for Oracle Access Manager 1.2.2: Installation and Configuration Guide 007-013752-001, Rev. E, June 2021, Copyright © 2021 Thales Group. All rights reserved.

- 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.

Plug-ins Vew • Import Plug-in	Activation Status Type Last updated On Last updated by Activated Assertion
Row Plug-in Name Description 23 TAPIdentify Plugin 24 TAPRequestPlugin	Activation Status Type Last updated On Last updated by
23 TAPidentifyPlugin 24 TAPRequestPlugin	
24 TAPRequestPlugin	Actuated Acception
	Activatory Accession
	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 UseridentficationPlugIn	Activated Authentication
32 UserPasswordPolicyPlugin	Activated Authentication
33 X509CredentialExtractor	Activated Authentication
34 CRYPTOCardOamAuthModule	Activated Authentication Sun Mar 27 23:24:12 OAMSystemAdm
	Total Rows
Plug-in Details: CRYPTOCardOamAuthModule	
Activation Status Configuration Parameters	
	s
* INI_FILE_FULLPATH /usr/local/cryptocard/oam/ini/JCryp	
* ENCRYPTION_LIBRARY_FULLPATH_/usr/local/cryptocard/oam/bin/x64/li	

(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.

Launch Pad		
letoome to Oracle Access Management		
Oulck Skart Wizards Coolcation Registration S SSO Agent Registration	Applications Applications Resource Type Host Identifiers	Authentication Modules Authentication Schemes SSO Agents Session Management Password Policy
Identity Federation + • Identity Provider Administration Identity Provider Administration	👸 Partner Profiles 🗃	Token Valdstion Templates Token Issuance Templates Custom Tokens
Mobile and Social 🖉	Access Portal Service 🔗	+ •

(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 Q
C Laurch Padi Mathentication Modules × Search Authentication Modules	Create Authentication Module Create LAPP Authentication Module Create Robers Authentication Module Create Robers Authentication Module Create Custom Authentication Module
Search Results Actions * View * 💽 * / 💥 🖾 Detach Row Name Type	Search Reset
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.

DRACLE Access Management	Acce	ssibility Help Sign Out weblogic Ϙ
Launch Pad Authentication Modules X Custom Authentication	on mod X	
Authentication Module		Apply
General Steps Orchestration		
* Name	IAS 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.

Launch Pad	Authentication Me	iodules × E Custom Authentication	ion mod ×		Ľ
thentication	Module				Apply
neral Steps	Steps Orchestration	n			
/iew 🕶 👍	🗙 🛃 Detach				
ep 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.

Add new st	ep	×
activated plu	name and description, and select a g-in. The flow parameters for that se edited after it is added to the step	
* Step Name	OTP	
Description		
* Plug-in Name	CRYPTOCardOamAuthModule	•
	OK Cance	1 i

(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:

ORACLE Acc	cess Management						Accessibility	Help	Sign Out	user.0 Q
Launch Pad H Aur	thentication Modules × SAS_Only ×]								Apply
General Steps Step You can specify the initial step OTP -										
Name	Description	On Success		On Failure		On Error				
OTP		success	<u>-</u>	failure	<u>.</u>	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.

Launch Pad			
Velcome to Oracle Access Management			
Outok Start Wizards Concentration SSO Agent Registration	Access Manager Application Domains Applications Resource Type Host Identifiers Plug-ins	Authentication Modules Authentication Schemes SSD Agents Session Management Password Policy	+.
Identity Federation 	Security Token Service Partners Partners Partners Endpoints	Custom Tokens	+ •
Mobile and Social	Access Portal Service 🔗	SC, Global Agent Settings	+ •

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

2. Click Create Authentication Scheme.

ORACLE Access Management	Accessibility Help Sign Out weblogic Q
Laurch Pad Authentication Schemes × Search Authentication Schemes	Create Authentication Scheme
Search Results	Search Reset
Actors + Vew + P 2 C Detach Row Name Description	
No data to display.	

(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 <u>Creating Authentication Module</u>).
Challenge URL	Enter URL of the credentials collector (for example, http://oamserver1.localdomain:14100/Login/Login.jsp).
Context Type	Select external .

thentication Sche	tication Schemes × SAS-Agent ×	Set As Default Duplicate
inentication Sche	nes	Set As Denaut Dupicate
* Name	SAS-Agent	
Description		
Authentication Level	2 🗘	
Default		
Challenge Method	FORM -	
challenge Redirect URL	ioam/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.

Launch Pad			
Velcome to Oracle Access Management			
Ourick Start Wizards Generation Registration SSO Agent Registration	Access Manager	Authentication Modules Authentication Schemes So SO Agents Session Management Password Policy	+•
Sentity Provider Administration	Security Token Service Partners Partner Profiles Endpoints	Custom Tokens	+ •
Mobile and Social O Mobile Services OAuth Service	Access Portal Bervice 🖉	😥 Okobal Agent Settings	+ -

(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).

ORACLE: Access Management	Accessibility Help Sign Out weblogic 🥥
Launch Pad G Application Domain × Search Application Domains	Create Application Domain
⊿ Search	
Name Search Results	Search Reset
Actions 🕶 View 💌 📑 🥒 💥 📑 Detach	
	Description
	Policy objects enabling integration with Oracle Fusion Applications
	Policy objects enabling OAM Agent to protect deployed IAM Suite applications
3 RREG_OAM110	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.

Summary	Presources	Authentication Policies	Authorization Policies		Token Issuance Policies	Administration		
Authentic	ation Policie	s						Create Authentication Policy
Actions	• View •		9	13	×		Detach	
Row	Name				Description			
	1 Public Resol 2 Protected Re				Policy set during domai Policy set during domai			
	No. of Concession, Name							

(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.

Duplicate
4 1

SafeNet Agent for Oracle Access Manager 1.2.2: Installation and Configuration Guide 007-013752-001, Rev. E, June 2021, Copyright © 2021 Thales Group. All rights reserved.

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="Security" 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.

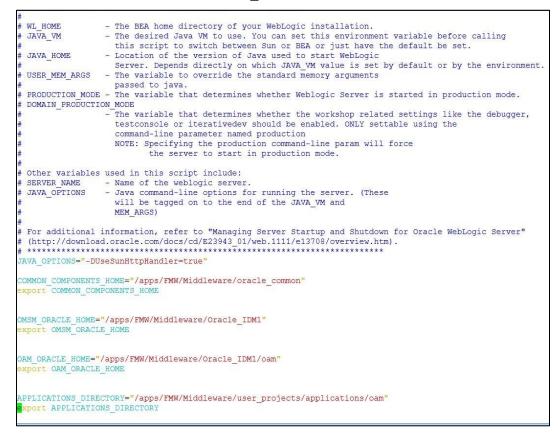
For SSL-enabled SafeNet Server Machines

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



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.

Change Center	Ame Log Out Preferences 🔝 Record Help	Q	Welcome, weblogic Connected to: base_doma
View changes and restarts	Home		
Configuration editing is enabled. Future	Home Page		
changes will automatically be activated as you modify, add or delete items in this domain.	- Information and Resources		
Iomain Structure	Helpful Toola	General Information	
ase domain	Configure applications	Common Administration Task Descriptions	
B-Environment	 Configure GridLink for RAC Data Source 	Read the documentation	
Deploymenta	Recent Task Status	 Ask a question on My Oracle Support 	
-Services Security Realma	Set your console preferences	Oracle Guardian Overview	
E-Interoperability E-Diagnostics	- Domain Configurations		
	Domain	Services	Interoperability
	• Domain	Messaging JMS Servers	WTC Servers Joit Connection Pools
	Environment	Store-and-Forward Agents	
	Servers	 JMS Modules 	Diagnostica
ew do L. 🛛	Clusters	Path Services	Log Files
aw do L.	Virtual Hosta	Bridges	Diagnostic Modules
Search the configuration	Migratable Targets	Data Sources	Diagnostic Images
Use the Change Center	Coherence Servers	Persistent Stores	Request Performance
Record WLST Scripts	Coherence Clusters	XML Registries	Archives
Change Console preferences	Machines	XML Entity Caches	Context
Manage Console extensions	Work Managers	Foreign JNDt Providers	SNMP
Monitor servers	Startup And Shutdowh Classes	Work Contexts	
		• (COM	Charts and Graphs
ystem Status 🖂	Your Deployed Resources	Mail Sessions	Monitoring Dashboard
Health of Running Servers	Deployments	• Fiel73	Semicourtes with a second s

(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.

Change Center	A Home Log Out Preferences 🔛 Record Help		Welcome,	weblogic Connected to: base_domail			
View changes and restarts	Home >Gummary of Deployments	1005 (
Configuration editing is enabled. Future	Summary of Deployments						
changes will automatically be activated as you modify, add or delete items in this domain.	Control Monitoring						
Domain Structure	This page displays a list of Java EE applications and stand-alone application module		n. Installed applications and modules	can be started, stopped, updated			
e-Environment	(redeployed), or deleted from the domain by first selecting the application name and						
- Deployments E-Services	To install a new application or module for deployment to targets in this domain, click to	the instal button.					
Security Realms El-Interoperability	Customize this table						
Degnostics							
	Professional						
	Deployments						
	Deployments Install Update Delete Start v Stop v		Sh	owing 1 to 10 of 39 Previous Next			
		State Health		owing 1 to 10 of 39 Previous Next			
	Install Update Delete Start v Stop v	State Health Active					
How do L. 🕀	Install Update Delete Start v Stop v		Туре	Deployment Order			
200 CO 100 CO	Install Update Delete Start v Stop v Name & Moderation businesseditor(1.0,11.1.1.2.0)	Active	Type Library	Deployment Order 100			
Instal an Enterprise application Configure an Enterprise application	Install Update Delete Start v Step v Name % Image: Start v Step v Image: Start v Step v Image: Start v Image: Start v Step v Image: Start v Step v Image: Start v Image: Start v Step v Image: Start v Step v Image: Start v Image: Start v Step v Image: Start v Step v	Active Active	Type Library Library	Deployment Order 100 100			
Install an Enterprise application Configure an Enterprise application Update (redepicy) an Enterprise application Start and size a deployed Enterprise	Install Update Delete Start v Stap v Name Image: Start v Stap v Image: Start v Stap v Image: Start v Start v Start v Stap v Image: Start v Start v Start v Stap v Image: Start v Start v Start v Stap v Image: Start v Start v Start v Stap v Image: Start v Start v Start v Stap v Image: Start v Start v Start v Stap v Image: Start v Start v Start v Stap v Image: Start v Start v Start v Start v Image: Start v Start v Start v Start v	Active Active Active	Type Lbrary Lbrary Lbrary Lbrary	Deployment Order 100 100 100			
Install an Enterprise application Configure an Enterprise application Update (redeptoy) an Enterprise application Start and stop a deployed Enterprise application Monfor the modules of an Enterprise	Install Update Delete Start v Stap v Name ~	Active Ac	Type Lbrary Lbrary Lbrary Lbrary Lbrary Web Application	Deployment Order 100 100 100 100 100			
Install an Enterprise application Configure an Enterprise application Update (redeploy) an Enterprise application Start and step a deployed Enterprise application	Install Update Delete Start v Stop v Name A Image: Start v Stop v Image: Start v Stop v Image: Start v Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image: Stop v Image	Active Ac	Type Lbrary Lbrary Lbrary Lbrary Lbrary Web Application Web Application	Deployment Order 100 100 100 100 100 100			

(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®	1.22		Q
Change Center	Home Log Out Preferences M Record Help	9	Welcome, weblogic Connected to: base_domain
View changes and restarts	Home >Summary of Deployments		
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		
Domain Structure	Locate deployment to install and prepare for deployment		
base_domain	application directory or file in the Path field.		n module descriptor that you want to install. You can also enter the path of the nfirm that your application contains the required deployment descriptors.
Interoperability Diagnostics	Path: //usr/local/cryptocard	/oam/war/CRYPTOCardOamLogin.war	1
E manore	Recently Used Paths: /usr/local/cryptocard/oam/w Current Location: oamserver1 / usr / local / cr		
	CRYPTOCardOamAuthModule - oren.jar		
How do L. 🗄	Back Next Finish Cancel		
 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			

(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		Q
Change Center	A Home Log Out Preferences 🖂 Record Help	Q	Welcome, weblogic Connected to: base_domain
View changes and restarts	Home >Summary of Deployments		
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.	Messages		
	Install Application Assistant		
Domain Structure Domain Structure Des Goman	Back Mext Termin Cancel Choose targeting style Targets are the servers, clusters, and virbuil hosts on which this Image is a point of the servers in the servers in the servers in the servers. Image is a server in the server is an application The application and its components will be targeted to the same loc Image is a server in the server is an application The application and its components will be targeted to the same loc Image is a server in the server in the server is a server in the server is a server in the server in	ations. This is the most common usage.	
How do I	Back Next Finish Cancel		
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			

(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		<u> </u>
Change Center	A Home Log Out Preferences 🔜 Record Help	2	Welcome, weblogic Connected to: base_domain
View changes and restarts	Home >Summary of Deployments		
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.	Install Application Assistant		
Domain Structure	Select deployment targets		
base_domain B_Environment -Deployments B_Services -Services	Select file servers and/or clusters to which you want to deploy this application. (Y Available targets for CRYPTOCardOamLogin :	ou can reconfigure deployment targets later).	
Interoperability Diagnostics	Servers		
	AdminServer		
	🗹 oam_server1		
How do I_	Back Next Finish Cancel		
 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			

(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		2
Change Center	A Here Lag Out Preserves (2) Record Here (0)	Welcome, weblogs: Converted to base, domain	
View changes and restarts	Interne - Journeau y al Departymenta		1
Configuration editing is enabled. Fullure changes will automatically be activated as you	Instal Application Assistant		
modify, add or deterts terms in this domain.	Back Next Print Cancel		
Domain Diructure	Optional Bettings		
base domain B-Endormant	You can ready here untirgs or accept her details		
Digzoymens 8- Services			
- Security Realms	. Mana qo Joon waxa pi unawa para qafavihinasay		
B - Dragnostos	Name: CR/PTOCardOamLogin		
	becuty		
	What security model do you wait to use with the approximent?		
	OO Only: Use only roles and policies that are defined in the deployment descriptors.		
Haw do L. II	Custom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor.		
 Dart and stop a deproyed Everyment application 	Custom Roles and Polities: Use anly roles and policies that are defined in the Administration Console.		
Configure an Enterprise application			
Create a deployment plan	Advanced: Use a custom model that you have configured on the readm's configuration page.		
 Target an Enterprise application to a server Test the modules in an Enterprise application 	- Bears accessibility		
	Hare should the source ties be made accessible?		
Bystem Blatus () Insetti of Running Services	Use the defaults defined by the deployment's targets		
Faled (0)	Recommended windlan.		
Critica (A	Copy this application onto every larget for me		
Overtoaded (0)			
Warring (i) OK (2)	During displayment, the files will be capited automatically to the managed servers to which the approach is targetest.		
	O I will make the deployment accessible from the following location		
	Lesates: //usr/locat/cryptocard/oam/war/CRYPTOCardOamLogin.war		
	Provide the coultion from where all largests will accesse The application's fires. This is often a shered directory. You must ensure the application files exist in this location and that each target can need the coultion.		
	Back Need Read Careet		
	Frances Frances Frances Frances		-

(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**.

	Hom Hom	e Log Out Preferences 🛃 Record Help	Q		Welcome, weblog	gic Connected to: base_dom
View changes and restarts	Home >	Summary of Deployments				
Configuration editing is enabled. Future	Summary of Deployments					
changes will automatically be activated as you modify, add or delete items in this domain.	Control	Monitoring				
Domain Structure base_domain - Environment - Deployments - Services	module page.	age displays a list of Java EE applications and stand-alone is can be started, stopped, updated (redeployed), or delete all a new application or module for deployment to targets i	d from the domain by fin	st selecting	the application name a	
- Security Realms - Interoperability - Diagnostics						
	Insta	II Update Delete Start~ Stop~			Showing 1 t	to 10 of 39 Previous Next
		lame 🏟	State	Health	Туре	Deployment Order
law da L		lame 🙈 6adf.oracle.businesseditor(1.0,11.1.1.2.0)	State Active	Health	Type Library	Deployment Order
	0			Health		
Install an Enterprise application		adf.oracle.businesseditor(1.0,11.1.1.2.0)	Active	Health	Library	100
Install an Enterprise application Configure an Enterprise application		adf.oracle.businesseditor(1.0,11.1.1.2.0) adf.oracle.domain(1.0,11.1.1.2.0)	Active	Health	Library Library	100
How do I Install an Enterprise application Configure an Enterprise application Update (redeploy) an Enterprise application Start and stop a deployed Enterprise application		adf.oracie.businesseditor(1.0,11.1.1.2.0) adf.oracie.domain(1.0,11.1.1.2.0) adf.oracie.domain.webapp(1.0,11.1.1.2.0)	Active Active	Health Health	Library Library	100 100 100

(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 <u>USER_LOGIN_ID_NAME</u> variable in <u>Configuring ini File</u> section.
Туре	Cookie
Value	\$user.userid

Launch Pad	G Applica	tion Domain ×	testOhsAgent ×	testOhsAgent : Protected	×		
uthentica	tion Policy	1				Duplicate	Appl
	* Name	Protected Resour	ce Policy		Success URL		
	Description	Policy set during this policy to pro	domain creation. Add r cect them.	esources to	Failure URL		
* Authentic	ation Scheme	LDAPScheme	۲)				
Resources	Responses	Advanced Rule	s				
🔲 Identit	ty Assertion						
This will o	ause an asser	tion to be generat	ed for the user, option	ally containing any Asserted Attribut	e set below.		
🖓 Resp	onses					+ /	8
Name			Ту	De	Value	 	
USER ID			Se	ssion	\$user.userid		

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

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/

drwxr-xr-x	2	oracle	oracle	4096	Jan	8	10:50	bsidkey
								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-rr	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

(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 <u>BSID</u> 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).</iamdemo.oracle.com>
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.

SafeNet Agent for Oracle Access Manager 1.2.2: Installation and Configuration Guide 007-013752-001, Rev. E, June 2021, Copyright © 2021 Thales Group. All rights reserved.

	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 <u>Cookie</u> name value set in <u>Cookie Settings for Step-Up Authentication</u> section.					
IGNORE_CERTIFICATE_ERR ORS	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.

ORACLE[®] Access Management Application Security Mobile Security Configuration A Federation Launch Pad Plug-ins x **Quick Start Wizards** Access Manager + -Agents + -Perform common setup tasks Manage Single Sign-On Application Domains Manage Single Sign-On agents Application Registration Application Domains SSO Agent Registration Resource Types Host Identifiers Authentication Schemes Session Management **Password Policy** Plug-ins + 🔻 Manage Common Password Policy for Single Sign-On Manage Single Sign-On sessions Manage Authentication Plug-ins Authentication Modules Authentication Plug-ins

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.

Launch Pacess Plug-in Use the foll View Row 1 2 3	lowing screen to set up custom Plug-ins to exter	 X Deactivate Selected Activation Activated Activated Activated Activated	h Oracle Security To Remove Sele Type Authentication Authentication	ken Service.	ity Configuration
5 Plug-in Configura KEY_ID	Details: UserldentificationPlugin Details: UserldentificationPlugin ation Parameters Activation Status DentTITY_STORE_REF KEY_LDAP_FILTER SEARCH_BASE_URL	Activated Activated	Authentication User Provisioning		Total Rows: 37

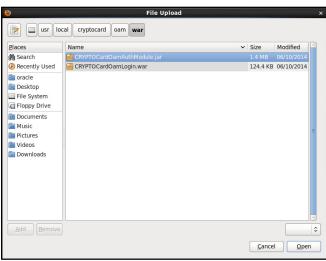
(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

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

Import Plug-in ×							
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) Choose file No file chosen							
Import Cancel							

(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.



(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**.

aunch Pao	d Plug-ins x							
Access Plug-in	s Manager > S							
se the foll View ▼	owing screen to set up cust	tom Plug-ins to extend Au	thentication functionality fo	r Oracle Access Manager			7	
s.			-					
Row	Plug-in Name	De	scription	Activation Status	Туре	Last updated On	Last updated by	
33	OAuthTokenResponsePlu	igin		Activated	Assertion			•
34	AdaptiveAuthenticationPlu	ugin		Activated	Authentication			
35	CredentialChallengePlugi	in		Activated	Authentication			
36	TAPResponseValidationPl	lugin		Activated	Authentication			
37	CRYPTOCardOamAuthMo	odule		Activated	Authentication	Mon Dec 26 17:	OAMSystemAdm	-
							Total Rows: 37	_
-	Details: CRYPTOCa ation Parameters Activa	rdOamAuthModul	e					_
							Save	
			rd/oam/ini/JCryptoWrapper					

(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.

Launch Pa	d Plug-ins x					
Plug-ir	s Manager > IS lowing screen to set up custom Plug-ins t	io extend Authentication functionality for	Oracle Access Manager wit	h Oracle Security 1	Foken Service.	
View v	🛃 Import Plug-in 🕂 Distribute	e Selected + Activate Selected	X Deactivate Selected	🗙 Remove Se	lected 🎝	7
Row	Plug-in Name	Description	Activation Status	Туре	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
Plug-in	Details: CRYPTOCardOamAu	thModule				Total Rows: 37
Configur	ation Parameters Activation Status					
						Sav

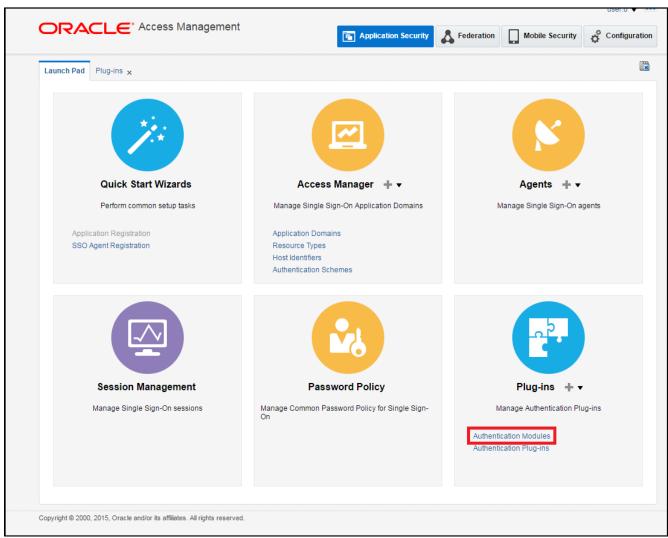
(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

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.

Launch Pad Plug-ins 🗙	Authentication Modules	×				
Access Manager >						
Search Authentica	tion Modules			+ Create Authentie	cation Module	•
Search for an existing Authen	tication Module or click the	e Create Authentication Module I	button to create a new one.	 + Create LDAP Au	thentication M	odule
Search				Create Kerberos	Authentication	n Modul
Name				 Create X509 Aut 	hentication Mo	odule
Type All	T			Create Custom A	Authentication I	Module
Search Results					Search R	eset
	Create 🔻 🖓 Dupli	cate 🧪 Edit 💥 Delete	Detach			
Name		Туре				
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.

Launch Pad Plug-ins × Authentication Modu	ules x Custom Authentica	tion mod ×		Ĩ
Access Manager > Authentication Module Authenticat	tion Module			Apply
Custom Authentication Module relies on bundled one plug-in that you can orchestrate to ensure that			Authentication Extensibility Java API). This module uses more than
General Steps Steps Orchestration				
*	Name SAS Agent			
Desc	cription			

(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.

	ccess Manageme	Ē	Application Security	Federation	Mobile Security	¢ o	configuration
aunch Pad Plug-ins _× A	withentication Modules \times	Custom Authentication mod ×					
Access Manager >							
uthentication Mod	ule Authentication Mod	lule					Apply
ne plug-in that you can orche		s (or those that are developed using one performs a specific authenticatio		entication Extensibilit	y Java API). This module	e uses m	ore than
View ▼ + ×	Detach						
Step Name	Description	Plug-in Name					
							-
Step Details						Save	Cancel
Step Details Step Name					[Save	
Step Details Step Name Description					(Save	

(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.

Add new st	ep	×
activated plu	name and description, and select ar g-in. The flow parameters for that se edited after it is added to the step.	_
* Step Name	OTP	
Description		
* Plug-in Name	CRYPTOCardOamAuthModule	•
	OK Cancel	

(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:

RACLE	 Access Management 	Application Se	ecurity 👗 Federation	n Mobile Security	Configuration
unch Pad Authenticat	tion Modules x Custom_Authen	tication_Mod) ×			
Access Manager >					
uthentication M	Iodule Authentication Module			Dupli	cate Apply
		those that are developed using the Access Mana erforms a specific authentication function.	ger Authentication Extensi	bility Java API). This module us	es more than
Confirmation					×
Authentication Module	created successfully.				
General Steps Step	os Orchestration				
You can specify the initia	il step				
* Initial Step OTP V]				
Name	Description	On Success	On Failure	On Error	
Hame					

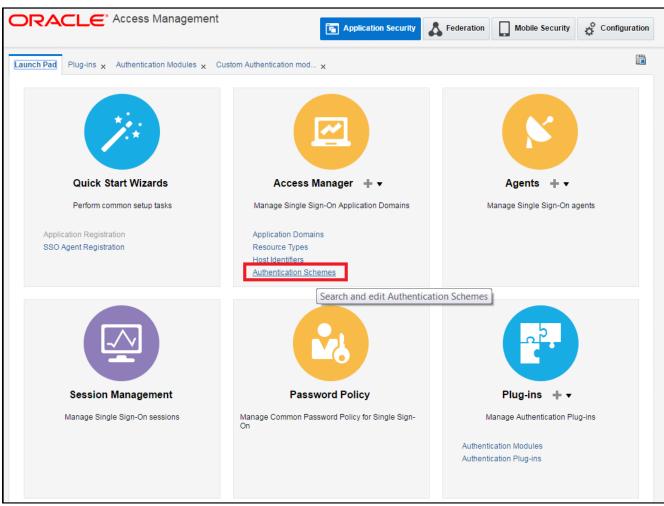
(The image above is from the Oracle Access Manager. Trademarks are the property of their respective owners.)

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.

		Access Manag	·	Application Security	Federation	Mobile Security	Configuratio
aunch Pad	Plug-ins :	< Authentication Modu	ules 🗙 Custom Authentication n	nod x Authentication Schemes x			
Access M	lanager >						
earch A	uthenti	cation Schemes	s			+ Create Auther	ntication Scheme
earch for an	existing Au	thentication Scheme or c	lick the Create Authentication Sci	heme button to create a new one.			
⊿ Sear	ch						
Name							
Name							
Name							Search Reset
	esults					[Search Reset
Name Search Re Actions		+ Create 🔿 Dup	licate 🧪 Edit 💥 Delete	∰] Detach		[Search Reset
Search Re		+ Create 🔿 Dup	iicate 🧪 Edit 💥 Delete	Detach Description		(Search Reset

(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 <u>Creating Authentication Module</u>).
Challenge URL	Enter URL of the credentials collector (for example, http://oamserver1.localdomain:14100/Login/Login.jsp).
Context Type	Select external .

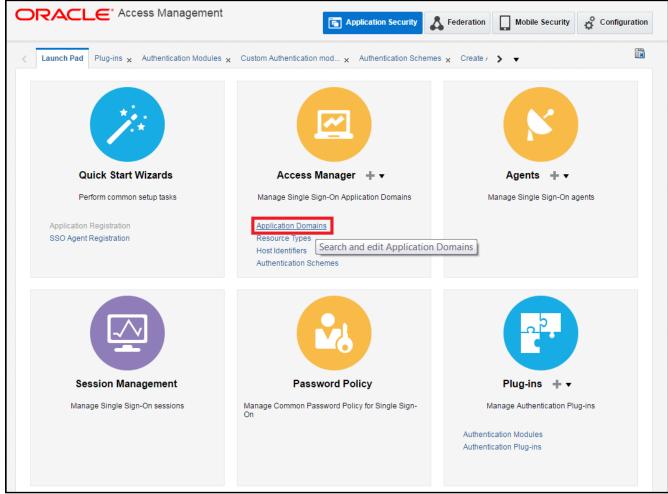
DRACLE	Access Management	Application Sec	curity 👗 Federation 🔲 Mobile	e Security
Authentication Mo	dules \mathbf{x} Custom Authentication mod \mathbf{x} Authentic	ation Schemes × Create	Authentication Sch ×	[
Access Manager >				
	tion Scheme Authentication Scheme lefines the challenge mechanism required to authentical	te a user. Each Authenticatio	n Schame must also include a defined A	Set As Default Apply
In Autoentication Scheme (leines die chanenge niechanism equired to autoentica			dulentication module.
* Name	SAS Agent			
Description				
* Authentication Level	2 🔨 🗸			
Default				
* Challenge Method	FORM V			
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).

Application Domain * TestAgentDec *	JI () – (CLE	* Access M	anagement		Application Security	Federation	Mobile Security	Configuration
Search Application Domains	aunch Pad	Applicati	on Domain × Te	estAgentDec 🗙					Ē
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 Actions < View < + Create Edit Delete Emil Detach 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	Access Ma	anager >							
▲ Search Name Search Results Actions ▼ View ▼ + Create Lett Delete Actions ▼ View ▼ + Create Lett Delete Row Name 1 Fusion Apps Integration 2 IAM Suite 3 REG_OAM11G	Search A	pplicat	tion Domain	S				+ Create Ap	oplication Domain
Name Search Reset Search Results Actions ▼ View ▼ + Create ✓ Edit X Delete Central Content of the conte	Jse the search	n tool to fin	id an existing Appli	ication Domain or click	the Create Applicatio	on Domain button to create a nev	vone.		
Search Reset Search Reset Actions View V + Create V Edit X Delete Delech Row + Create V Edit X Delete Delech 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_OAM116 Reset	Searce	:h							
Search Reset Search Reset Actions * Vew * + Create * Edit * Delete Delete 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_OAM116 Policy objects enabling OAM Agent to protect deployed IAM Suite applications	Name								
Image: State of the state o									Search Resot
IAM Suite Policy objects enabling OAM Agent to protect deployed IAM Suite applications RREG_OAM11G			+ Create	🖉 Edit 🗙 Delete	Detach				Search Reset
3 RREG_OAM11G	Actions 🔻 🕚	View 🔻	+ Create	🖉 Edit 💥 Delete	∰] Detach	Description			Search Reset
	Actions v	View ▼ Name		🖋 Edit 💥 Delete	Detach	•	egration with Oracle	Fusion Applications	Search Reset
4 TestAgentDec Application Domain created through Remote Registration	Actions ▼ Row 1	View ▼ Name Fusion A	Apps Integration	🖋 Edit X Delete	i Detach	Policy objects enabling int	-		
	Actions V Row 1 2	View ▼ Name Fusion A IAM Suit	Apps Integration	🖻 Edit 🗶 Delete	[論] Detach	Policy objects enabling int	-		
	Actions Row 1 2 3	View View View View View View View View	Apps Integration ie DAM11G	🕈 Edit 🗶 Delete	المعرفي Detach	Policy objects enabling int Policy objects enabling OA	M Agent to protect d	eployed IAM Suite applic	

(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.

	CLE	Access Managem	ent	C	Application Security	Federation	Mobi	le Security	Configuratio
unch Pad	Application	Domain × TestAgentDe	×						
Access N	lanager >								
estAge	ntDec Ap	plication Domain							
plication D	omain provide	es a logical container for res	ources or sets of resources, a	nd the a	ssociated policies that dict	ate who can access	specific prote	ected resourd	ces.
ummary	Resources	Authentication Policies	Authorization Policies To	ken Issu	ance Policies Administr	ation			
elect an e	kisting Authen	tication Policy from the list o	r click the Create Authenticati	on Polic	y button to create a new or	ne.			
Actions •	View 🔻	🕂 Create 🛛 🗖 Duplica	te 🖌 Edit 🗙 Delete	(in the second s	Detach				
Row	Name				Description				
_	1 Public Re	esource Policy			Policy set during domain	creation. Add resou	irces to this p	olicy to allow	anyone access.
F	2 Protected	Resource Policy			Policy set during domain	creation. Add resou	irces to this p	olicy to prote	ct 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.

	~	tAgentDec X Authentication Sche	emes x SAS Agent x TestAgent	Dec : Protected ×	
Access Manage	er >				
rotected Re	esource Policy	Authentication Policy			Duplicate App
		fication that must be performed to pr r more resources in the Application I	ovide a sufficient level of trust for Acces Domain.	ss Manager to grant access to th	ne user making the request. A
* Name	Protected Resource Po	licy	Success URL		
Description	Policy set during domai policy to protect them.	in creation. Add resources to this	Failure URL		
Authentication Scheme	SAS Agent	¥			
esources Re	sponses Advanced Ru	ules			
_	I Add 90 Delete				
Resources	+ Add X Delete	Pessures UPI	Query String		
Resources Resource Ty HTTP	ype Host Identifier	Resource URL	Query String		
Resource Ty		Resource URL /index.html/** /index.html*	Query String		

(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	E - The variable that determines whether Weblogic Server is started in production mode.
# DOMAIN PRODUCT	
# -	- 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	s used in this script include:
	- Name of the weblogic server.
	- 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"
	ad.oracle.com/docs/cd/E23943 01/web.1111/e13708/overview.htm).
JAVA OPTIONS="-DU	UseSunHttpHandler=true"
COMMON COMPONENTS	S HOME="/apps/FMW/Middleware/oracle common"
export COMMON COM	
chport contron_con	
OMSM ORACLE HOME-	="/apps/FMW/Middleware/Oracle IDM1"
export OMSM ORACI	
chiporte onom_ontres	
OAM OPACLE HOME	//apps/FMW/Middleware/Oracle IDM1/oam"
export OAM ORACLE	
CAPOLO ONI_ONNODI	
APPLICATIONS DIR	ECTORY="/apps/FMW/Middleware/user projects/applications/oam"
export APPLICATIO	

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.

Change Center	Home Log Out Preferences Record Help	Q	Welcome, weblogic Connected to: base_domain
View changes and restarts	Home		
Configuration editing is enabled. Future	Home Page		
changes will automatically be activated as you modify, add or delete items in this domain.	- Information and Resources		
	Helpful Tools	General Information	
omain Structure	Configure applications	Common Administration Task Descriptions	
se_domain	Configure GridLink for RAC Data Source	Read the documentation	
Deployments	Recent Task Status	Ask a guestion on My Oracle Support	
8-Services	Set your console preferences	Oracle Guardian Overview	
-Security Realma	bei your console preferences	Oracle Guardian Overview	
E-Interoperability E-Diagnostics	- Domain Configurations		
	Domain	Services	Interoperability
	Domain	Messaging	WTC Servers
		 JMS Servers 	Joil Connection Pools
	Environment	 Store-and-Forward Agents 	
	Servers	 JMS Modules 	Diagnostica
	Chusters	 Path Services 	Log Files
low do L	Vetual Hosts	Bridges	Diagnostic Modules
Search the configuration	Migratable Targets	Data Sources	Disgnostic Images
Use the Change Center	Coherence Servers	Persistent Stores	Request Performance
Record WLST Scripts	Coherence Clusters	XML Registries	Archiven
Change Console preferences	Machines	XML Entity Caches	Context
Manage Console extensions	Work Managers	Foreign JNDt Providers	• SNMP
Monitor servers	Startup And Shutdown Classes	Work Contexts	Shine
1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.		• (COM	Charts and Graphs
yatem Status	Your Deployed Resources	Mail Sessions	Monitoring Dashboard
lealth of Running Servers	Depkyments	• Fiel73	 Monitoring Clashoolard w

(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.

Change Center	Ho Ho	me Log Out Preferences 🐼 Record Help	Q		Welcome	e, weblogic Connected to: base_domain		
View changes and restarts	Home	-Summary of Deployments	- Mathematican					
Configuration editing is enabled. Future	Summary of Deployments							
changes will automatically be activated as you modify, add or delete items in this domain.	Contr	ol Montoring						
Domain Structure	The	page displays a list of Java EE applications and stand-alone application	modules that have been installed to	this doctain bi	saturations and most include	beteine beende betele ed eo a		
ase_domain B-Environment		page displays a list of Java EC applications and stand atom application apoyed), or deleted from the domain by first selecting the application na			istaled approaches and moose	es can de stanied, stopped, updated		
Deployments	Toir	stall a new application or module for deployment to targets in this doma	in, click the Install button.					
El-Services								
Security Realma E-Interoperability	D Cust	tomize this table						
Diagnostics								
	Deployments							
	Depo	syments						
	-	tall Update Delete Start + Stop +			s	Rowing 1 to 10 of 39 Previous Next		
	-		State	Health	S	Showing 1 to 10 of 39 Previous Next		
	-	tall Update Delete Start + Stop +	State Active	Health				
tow do L. 🕄	-	tall Update Delete Start - Stop -	1774	Health	Туре	Deployment Order		
	-	Image: Start Control Stop Name A Start Control Stop	Active	Health	Type Library	Deployment Order 100		
Install an Enterprise application Configure an Enterprise application	-	Update Delete Start Stop Name	Active Active	Health	Type Lbrary Lbrary	Deployment Order 100 100		
Install an Enterprise application Configure an Enterprise application Update (redeploy) an Enterprise application Start and stop a deployed Enterprise	-	Update Delete Start - Stop - Name ->	Active Active Active	Health Health	Type Library Library Library	Deployment Order 100 100 100		
Install an Enterprise application Configure an Enterprise application Update (redeploy) an Enterprise application Bart and stop a deployed Enterprise application Monitor the modules of an Enterprise		Anne Anne Anne Anne Anne Anne Anne Anne	Active Active Active Active		Type Library Library Library Library	Deployment Order 100 100 100 100 100		
Install an Enterprise application Configure an Enterprise application Update (redepby) an Enterprise application Start and stop a deployed Enterprise		Vupdate Delete Start - Stop - Name	Active Active Active Active Active	С. С	Type Library Library Library Library Library Web Application	Deployment Order 100 100 100 100 100 100 100		

(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.

Change Center	A Home Log Out Preferences 🐼 Record Help	Q	Welcome, weblogic Connected to: base_domain
	Home >Summary of Deployments		
View changes and restarts 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		
induly, and of objects storing in this domain.	Back Next Hosh Cancel		
Domain Structure	Locate deployment to install and prepare for deploy	yment	
base_domain - Environment - Deployments - Services - Services	application directory or file in the Path field.		lication module descriptor that you want to install. You can also enter the path of the for confirm that your application contains the required deployment descriptors.
-Interoperability	Path: //usr/local/crypt	tocard/oam/war/CRYPTOCardOamLogin.w	ar
⊕-Diagnostics	Recently Used Paths: /usr/local/cryptocar		
	CRYPTOCardOamAuthModule - oren.jar		
How do L 🖂	Back Next Finish Cancel		
 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			

(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		Q
Change Center	A Home Log Out Preferences 🔝 Record Help	Q	Welcome, weblogic Connected to: base_domain
View changes and restarts	Home >Summary of Deployments		
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.	Messages		
	Install Application Assistant		
Domain Structure	Back Next Finish Cancel		
base, Gomain Environment I-Deptyments Services I-S	Choose targeting style Targets are the servers, clusters, and virtual hosts on w Choose targeting style Targets are the servers, clusters, and virtual hosts on w Choose targeting the servers, clusters, and virtual hosts on w Choose targeting the servers clusters, and virtual hosts on w Choose targeting style Targets are the servers and servers that are available for		
How do L.	Back Next Finish Cancel		
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			Ψ.

- (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		Q
Change Center	A Home Log Out Preferences 💽 Record Help	Q	Welcome, weblogic Connected to: base_domain
View changes and restarts	Home >Summary of Deployments		
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 Cancel		
Domain Structure	Select deployment targets		
base_domain ⊕ Environment → Deployments ⊕ Services → Security Realms	Select the servers and/or clusters to which you want to deploy th Available targets for CRYPTOCardOamLogin :	is application. (You can reconfigure deploys	ment targets later).
Interoperability Diagnostics	Servers		
	AdminServer		
How do L.	Back Next Finish Cancel		
 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			

(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*	Adminutration	Q -
Change Cester	🔞 Hame Log Clut Preterinoss 🔐 Rocord Help:	Welcome, weblogie: Command to base_domain
View changes and restarts	Traces - Businessy of Deployments	
Configuration editing is enabled. Future changes witr automatically be activated as your modify, add or deteleritems in this domain.	and Application Associate	
Demain Diructure	Optional Settings	
sae, Journ B. I-Inducional B.	Vici can valid Yeal utility or a longe the datume General Web day to wait to mate the dephysicet Meen: CRYPTOCAre@ComeGogin - Search Web anouty mode daysueset to use with the approximant Web anouty mode daysueset to use with the approximant descriptions.	
Now do L. II	Custom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor.	
Darl and step a teptoyet Enterprise application Condigue as Enterprise application Consta a diployment plan Target an Enterprise application to a server Test the modules in an Enterprise application	Courses Rains and Paintes: Use only uses and paintes had an addited to the Additional datase. Advanced: Use a sustaine model thad you have configured to: the readin's configured tice page. Secure advantationality. Advanced: The advantationality.	
Gystern Matus II	How simulatine source this be made accessible?	
Health of Running Servers	Use the defaults defined by the deployment's largels	
Fand (b) Onixie (b) Onixie (b) Wavery (b) Wavery (b) Or (b)	Proceedings of the application with each every larget for me Comp approver, the file with the capital accordingly to be measured to every to write the approximation is segmed. I will make the deployment according to the indexed gelecation Learnine According approver, the file will be capital according to the indexed gelecation Learnine According approver, the file will be capital according to the indexed gelecation According approver, the file will be capital according to the indexed gelecation Learnine According according to the indexed gelecation Accordi	

(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**.

Configuration editing is enabled. Future changes will activated as you modify, add or delete items in this domain. Summary of Deployments Domain Structure base_domain	Change Center	A Home Log Out Preferences 🔤 Record Help	Q	Welcome, weblo	gic Connected to: base_don			
that ages will automatically be activated as you modify, add or delete items in this domain. Demain Structure asse_domain Environment Deployments Sevenices	View changes and restarts	Home >Summary of Deployments						
Control Monitoring comain Structure This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on modules can be started, stopped, updated (redeployed), or deleted from the domain, click the Install button. Services To install a new application or module for deployment to targets in this domain, click the Install button. Customize this table Deployments Services Install update Deployments State Health Type Deployments State Install an Enterprise application Active Cordigre an Enterprise application Active Library Output (redeploy) an Enterprise application Active Library Update (redeploy) an Enterprise application Active Library 100 Stat and stop a deployed Enterprise Conterprise Library 100		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 modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on page. To install a new application or module for deployment to targets in this domain, click the Install button. Control of the started stopped control of the started stopped started stopped started stopped started stopped started stopped stopped started stopped stopped started stopped started stopped stopped started stopped stop		Control Monitoring						
e_domain Environment Deployments Services Security Realms - Interoperability Diagnostics Deployments - Customize this table Deployments - Customize this table Deployments - Name $\stackrel{\circ}{\longrightarrow}$ Customize this table Deployments - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type Deployment Or 39: Previous - Name $\stackrel{\circ}{\longrightarrow}$ Staty Health Type ID (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	main Structure							
w do I •••••••••••••••••••••••••••••	Environment Deployments Services Security Realms Interoperability	modules can be started, stopped, updated (redeployed), or deleted fro page. To install a new application or module for deployment to targets in thi Customize this table Deployments	om the domain by first selec	ting the application name a	and using the controls on this			
w do I Image: Constraint of the con		Name 🏟	State Heat	th Type	Deployment Order			
Image: Start and stop a deployed Enterprise Image: St	n do l	defadf.oracle.businesseditor(1.0, 11.1.1.2.0)	Active	Library	100			
Configure an Enterprise application Image: Configure an Enterprise application Active Library 100 Update (redeploy) an Enterprise application Image: Configure and Enterprise application Active Library 100				Library	100			
Active Library 100		adf.oracle.domain.webapp(1.0,11.1.1.2.0)	Active	Library	100			
tart and stop a deployed Enterprise		coherence(3.7.1.1,3.7.1.1)	Active	Library	100			
		CRYPTOCardOamLogin	Active 🗸 O	K 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.
- 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 <u>USER_LOGIN_ID_NAME</u> variable in <u>Configuring ini File</u> section.
Туре	Cookie
Value	\$user.userid

JRACI	_e Access Management		Application Security	Federation	Mobile Security	¢ ^{° Cor}	nfiguration
Launch Pad	ance2WithoutSSL : Pro ×						
Access Manag	jer >						
Authentication Polic	esource Policy Authentication Policy Authentication Policy defines the type of verification that must e defined to protect one or more resources	be performed to provid		s Manager to grant ac		Duplicate	Apply est. A
* Name	Protected Resource Policy		Success URL				
Description	Policy set during domain creation. Add repolicy to protect them.	esources to this	Failure URL				
* Authentication Scheme							
Resources Res	sponses Advanced Rules						
Identity Ass	sertion						
This will cause	an assertion to be generated for the user,	optionally containing a	ny Asserted Attribute set below.				
Responses	s 🕂 Add 💉 Edit 💥 Delete						
Name		Туре		Value			
USER_ID		Cookie		\$user.userid	1		

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

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 <u>Level 1 Protected Resource</u> [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 <u>Cookie</u> <u>Settings for Step-Up Authentication</u> 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.

CCC33 Mia	inager
	Welcome
Enter your Single Si	gn-On credentials below
Username:	
Password:	
	Login

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



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.

	THALE
Login	
Please enter your credentials to logon.	
OTP:	
Login	
Copyright 0.2021 Bulan.	

- ii. If the selected token type is GrIDsure or Challenge-Response,
 - a. Keeping the OTP field, blank, click Login.

	THALES
Login	
Please enter your credentials to logon.	
OTP:	
Logn	
Copyright © 2021 Thulos.	

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

							THALES
		I	.ogi				
Please	e ente	r you	r crea	dentia	als to	logon.	
Please enter chara	ecters in	sequen	ce com	espondi	ng to y	our chosen pattern.	
			-		-	1	
	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		
	0	TP:					
			Login				
		Capya	ight (> 2121	Thales.			

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



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.

	THALES
Login	
Please enter your credentials to logon.	
User Name: LDAP Password: OTP:	
Login	
Convert © 2021 Hales	

- 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).

	THALES
Login	
Please enter your credentials to logon.	
User Name: LDAP Password: OTP:	
Login	
Completic 2007 Males	

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

					THALES
	I	.ogi			
Please ente	er you	r cree	lentia	als to	o logon.
Please enter characters in	sequen	ce com	espondi	ng to y	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	
c	TP:				
		Login			
	Copyr	ight († 2621	I hales.		

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



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.