

Oracle Access Manager SAML SSO

- user login

- Guest, BYOD, My Devices and Sponsor Authentication
- Search a SAML-authenticated User Against Another Identity Store for Authorization

Login is made against the organization's IDP NOT Guest Portal

ISE is Service Provider
Oracle (OAM) is ID Provider

User connects to end portal via Oracle ID Provider weblogic interface and then can access any portal again using SSO.

SAML session stored in cookie on end user device

When accessing ISE portals set with SAML Auth there is built in logic to check for session cookie. If no cookie exists then redirected to weblogic for authentication.

After Authentication to ID Provider then user continues as usual

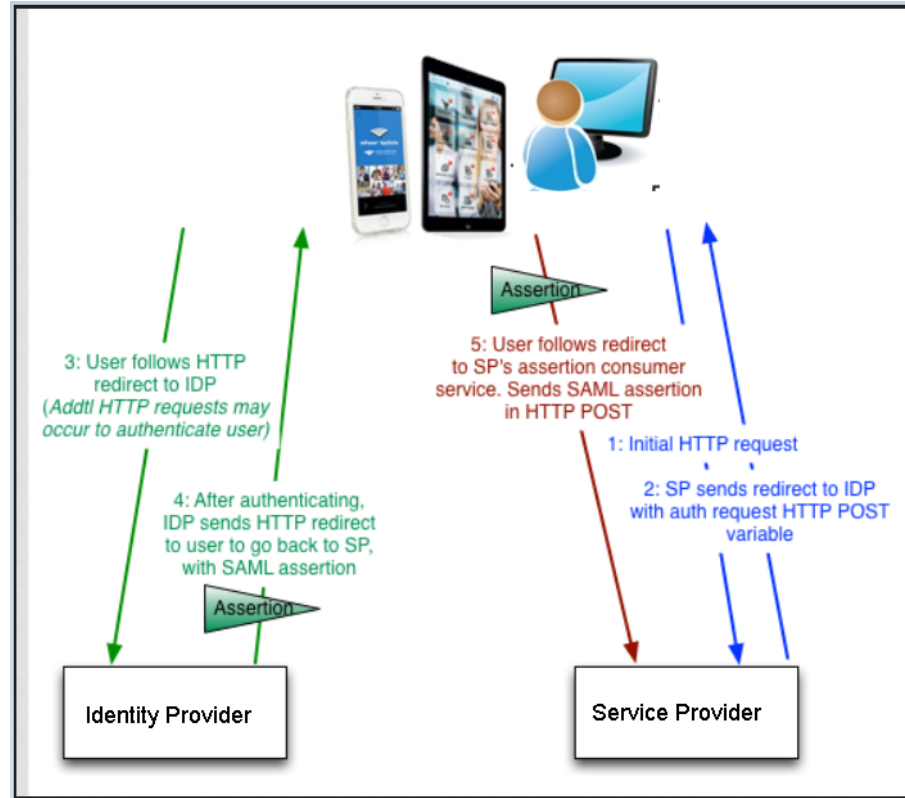
Supported against guest, my devices or sponsor portals

Supported ID Providers:
Oracle Access Manager (OAM)
Oracle Identity Federation (OIF)

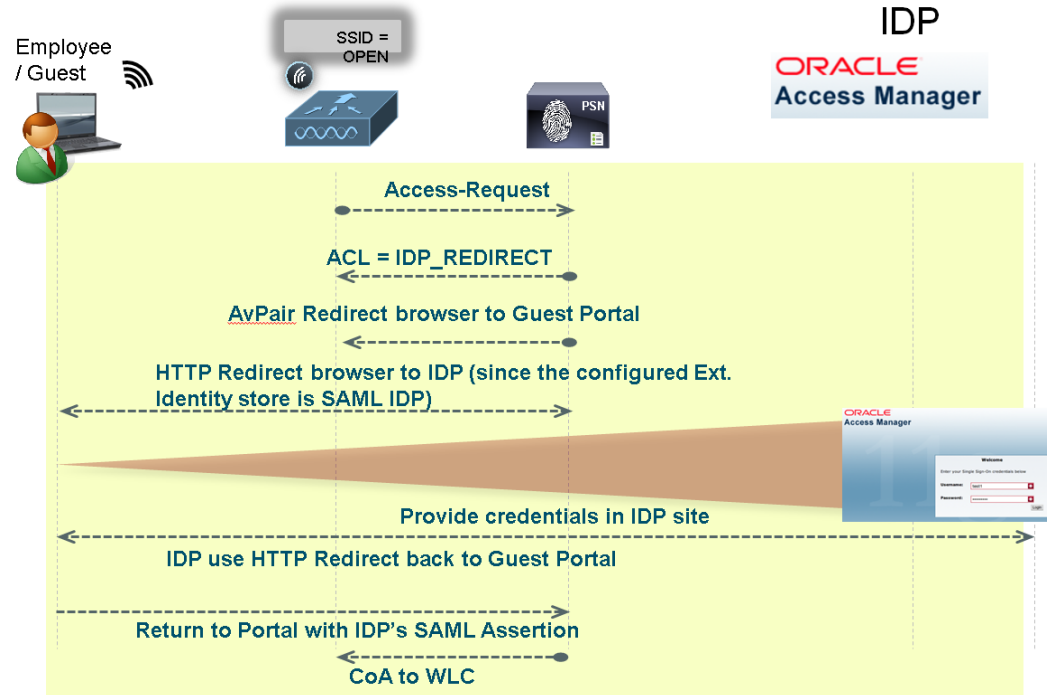
Oracle Access Manager SAML SSO

- SAML Flow

Service Provider – ISE
ID Provider - Oracle



Oracle Access Manager SAML SSO - SAML Flow

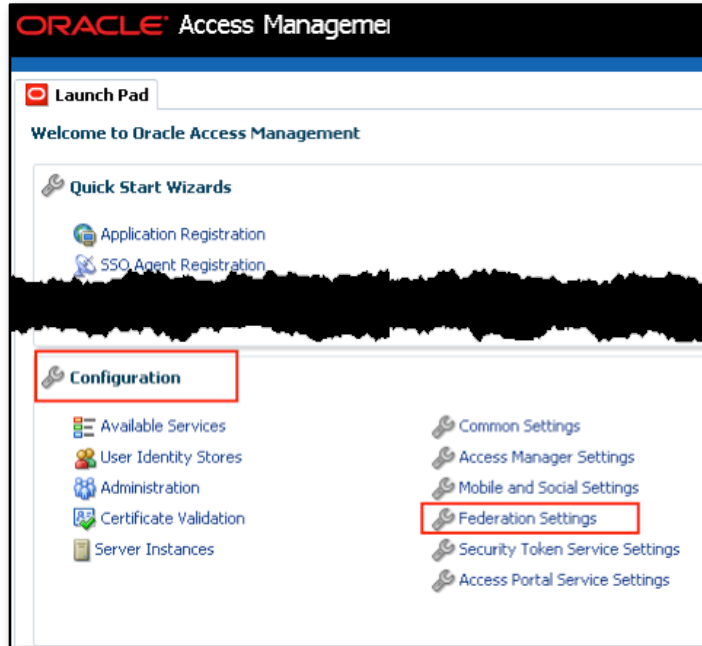


Oracle Access Manager SAML SSO

- Configuration Steps

1. Add SAML Identity Provider by importing the External identity provider's metadata
2. Select SAML Identity Provider at the Portal configuration as the Authentication Method
3. Export ISE service provider's information to the External identity provider

Oracle Access Manager SAML SSO - configure OAM



UseCase ISE 1.4

To start configuration.

Log into Oracle Access Management

From the Launch Pad

Configuration > Federation Settings

Oracle Access Manager SAML SSO

- configure OAM Click Export SAML 2.0 Metadata

OAM
Export SAML 2.0 Metadata

Federation Settings

General

* Provider Id Encryption Key

Succinct Id Custom Trust Anchor File [Export SAML 2.0 Metadata...](#)

Signing Key

Proxy

Enable Proxy

Host

Port

Non-Proxy Hosts

Username

Password

Keystore

Keystore Location

Row	Key ID	Alias	password	Description
1	osts_encryption	stspivatekeyalias	*****	
2	osts_signing	stspivatekeyalias	*****	

Oracle Access Manager SAML SSO

- import ID Providers Root or Self-signed cert into ISE

The ID Provider Self-signed or trusted certificate must be imported into ISE Trusted Certificates

Administration > System >
Certificates > Trusted Certificates

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. Below this, there are tabs for 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', and 'Feed Service'. The 'Certificates' tab is selected, showing sub-tabs for 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Backup & Restore', 'Admin Access', and 'Settings'. The left sidebar shows 'Certificate Management' with options for 'Overview', 'System Certificates', 'Endpoint Certificates', and 'Trusted Certificates'. The main content area is titled 'Trusted Certificates' and features an 'Import' button. Below the buttons is a table listing trusted certificates.

<input type="checkbox"/>	Friendly Name	Status	Trusted For	Serial
<input type="checkbox"/>	*.awmdm.com,*.awmdm.com,awmdm.com#Go Da...	Enabled	Infrastructure	27 DC
<input type="checkbox"/>	alpha-mobileiron.cisco.com,alpha-mobileiron.cisco.c...	Enabled	Infrastructure Cisco Services Endpoints	36 C0
<input type="checkbox"/>	Baltimore CyberTrust Root#Baltimore CyberTrust Ro...	Enabled	Cisco Services Infrastructure	02 00
<input type="checkbox"/>	Certificate Services Endpoint Sub CA - bxb22-11a-p...	Enabled	Infrastructure Endpoints	5D C2

Oracle Access Manager SAML SSO

Configure External Identity Source for SAML ID providers

New External Identity Source for SAML Id Providers

Identity Management > External Identity Sources > SAML Id Providers

Click Add and Fill in Provider Name

Under Identity Provider Config > Browse to Import XML File provided by ID Provider (Oracle)

The ID Provider only needs to be configured once on ISE regardless of how many ISE portals are doing SAML SSO

The screenshot displays the Oracle Access Manager (IAM) configuration interface. The top navigation bar includes 'System', 'Identity Management', 'Network Resources', and 'Device Portal Management'. The 'Identity Management' section is expanded to show 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'External Identity Sources' list on the left includes 'Certificate Authentication Profile', 'Active Directory', 'AD2', 'LDAP', 'RADIUS Token', 'RSA SecurID', and 'SAML Id Providers'. The 'SAML Id Providers' folder is highlighted with a red box. The main content area shows the 'SAML Identity Provider' configuration page, with the 'General' tab selected. The 'Id Provider Name' field is filled with 'BXB_IDP' and the 'Description' field is filled with 'Boxborough IDP'. A red box highlights the 'Identity Provider Config.' tab. Below this, the 'Identity Provider Configuration' section is visible, featuring an 'Import Identity Provider Config File' field with a 'Browse...' button. A red box highlights the 'Import XML file provided by Identity Provider' button, which is indicated by a red arrow from an information icon.

Oracle Access Manager SAML SSO

After XML Import View

Identity Provider List > **New Identity Provider**

SAML Identity Provider

General Identity Provider Config. Service Provider Info.

Identity Provider Configuration

Import Identity Provider Config File ⓘ

Provider Id `http://oamsaml.guest.test:14300/oam/fed`

Single Sign On URL `https://oamsaml.guest.test:14101/oamfed/ldap/samlv20`

Logout Settings

* Logout URL `https://oamsaml.guest.test:14101 /oam/server/logout` ⓘ

* Redirect Param Name `end_url` ⓘ

Signing Certificate

Subject `CN=oamsaml.guest.test`

Issuer `CN=oamsaml.guest.test`

Valid From `Thu Dec 04 22:29:53 EST 2014`

Valid To (Expiration) `Sun Dec 01 22:29:53 EST 2024`

Serial Number `0A`

Filled automatically according to the loaded IDP's Metadata

UseCase ISE 1.4

New External Identity Source for SAML Id Providers

After import of the XML from OAM

Logout URL

When a user logs out of the Sponsor, My Devices portal, the user is redirected to the Logout URL at the IdP to terminate the SSO session and then redirected back to the login page.

Redirect Parameter Name

The Redirect Parameter Name may differ based on the Identity Provider, for example, end_url or returnUrl. The redirect parameter is used to pass the URL of the login page to which the user must be redirected after logging out. This field is case sensitive.

Oracle Access Manager SAML SSO

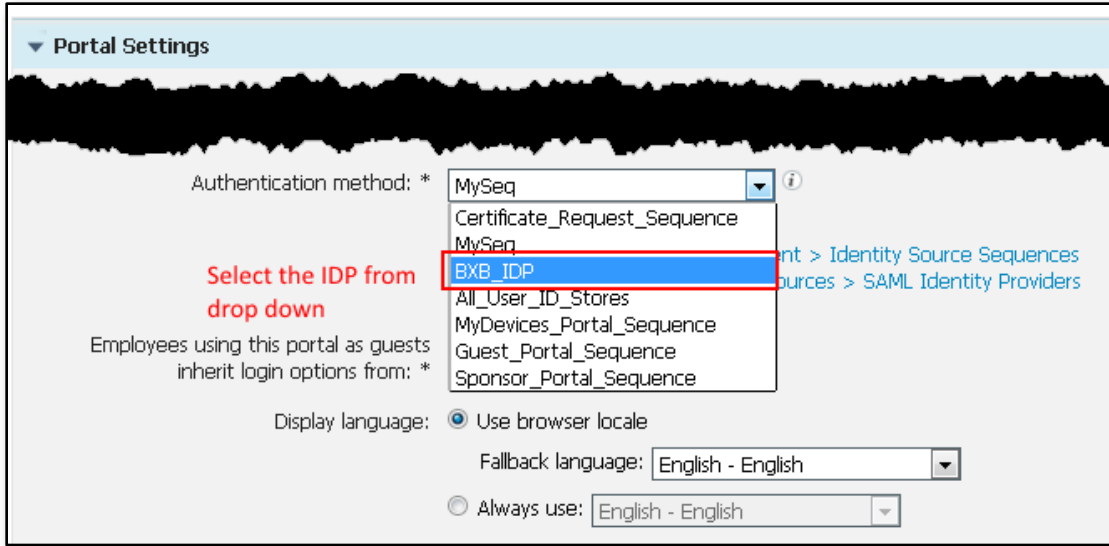
- Portal Settings choose IDP as Authentication Method

Under your portal config choose the authentication method for the new IDP

This method will only support the new IDP as authentication and you cannot add any other sources for this portal.

Supported by Guest, My Devices or Sponsor Portal

For Sponsor Portal you need to setup the sponsor in the SAML provider and in the sponsor group. Otherwise you will get an error



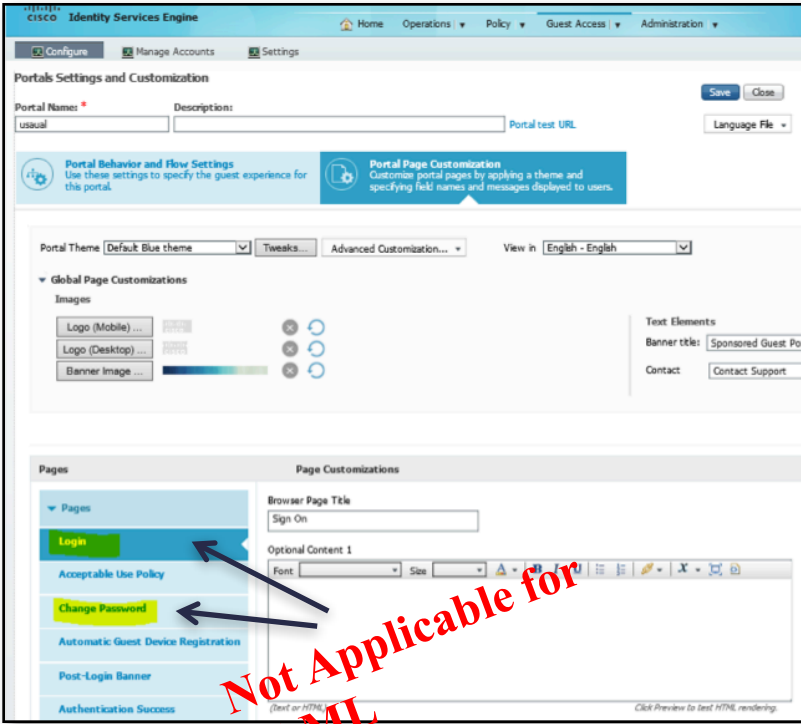
Oracle Access Manager SAML SSO

- Portal Base Customization differences

There is no customization for
Sponsored portals pages
Login
Change Password

These functions are handled by the IDP

self-registration flow is not supported as the IDP stores the information for this



Not Applicable for SAML

Oracle Access Manager SAML SSO

- IDP Authentication & Portal Mapping

Identity Provider List > **BXB_IDP**

SAML Identity Provider

General Identity Provider Config. **Service Provider Info.**

Service Provider Information

Note: it is mandatory to re-export service provider info in case of the following:

- Registration of new node
- Any node's host name or IP address change
- FQDN modification in my devices / sponsor portal

Export Service Provider Info. Export ?

Includes the following portals:

Sponsored Guest Portal (default)

- FQDN modification in my devices / sponsor portal

Export Service Provider Info. Export ?

Includes the following portals:

Export XML file containing Service Provider information for Identity Provider

Sponsored Guest Portal (default)

C:\Users\sampsund\AppData\Local\Temp\BxB_IDP-13.zip\

File Edit View Favorites Tools Help

+ - ✓ ⇨ ⇨ ✕ ⓘ

Add Extract Test Copy Move Delete Info

C:\Users\sampsund\AppData\Local\Temp\BxB_IDP-13.z

Name

Sponsored Guest Portal (default).xml

External Identity Sources > SAML Id Providers > Select the IDP that was created in earlier step.

Service Provider Info.

All the portals that have IDP as the authentication method will be listed in this screen.

Export the XML containing service provider information for the Identity Provider

On Export a zip file containing an XML file will be provided for each of the portals. In this example we are just working with the Sponsored Guest Portal (default).xml

This needs to be done for each portal that is going to use the SSO flow (Sponsor, My Devices, Guest)

These XML files are used for config of the IDP

Oracle Access Manager SAML SSO

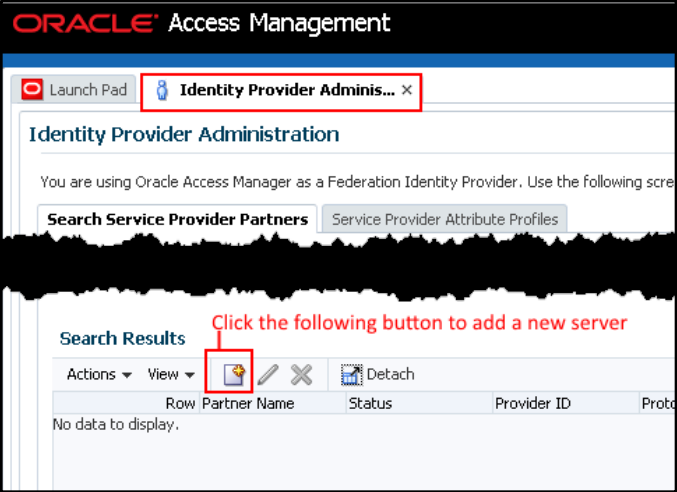
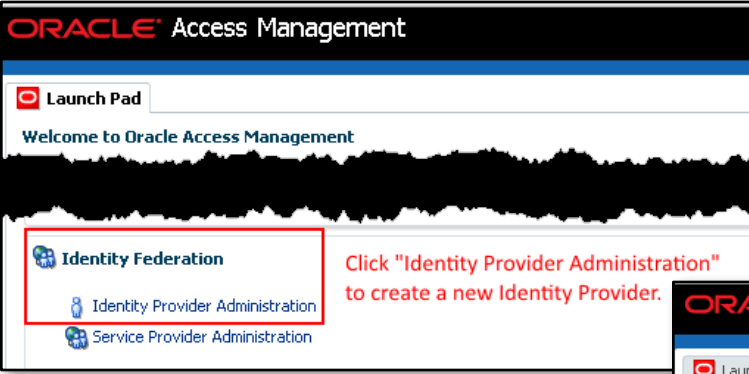
- Identity Federation Setup on OAM

OAM – Launch Pad – Identity Federation – Identity Provider Administration

Create a new Identity Provider

Add a new server

This needs to be done for each ISE portal that is used (Sponsor, My Devices, and Guest)



Oracle Access Manager SAML SSO

- Create Service Provider

UseCase ISE 1.4

This needs to be done for every ISE portal (Guest, Sponsor, My Devices) as a separate Service Provider

Create Service Provider

Give it a name

Load Metadata (XML files exported from ISE)

Choose the NameID Value as User ID Store Attribute as set as cn

ORACLE Access Management

Launch Pad Identity Provider Admins... x Create Service Provider P... x

Service Provider Partners

General

* Name Provide some name for the server entry

Description

Service Information

Protocol

Service Details Load from provider metadata Enter Manually

Metadata has been loaded from file. Click "Load Metadata" to load the file exported from ISE

Provider ID
Signing Certificate Subject
Validity

NameID Format

* NameID Format

* NameID Value The "NameID Value" is cn

Mapping Options

Attribute Mapping

* Attribute Profile

Load Metadata

Load Metadata File

Sponsor Portal (default).xml

Oracle Access Manager SAML SSO

- Sponsored Guest Portal Test URL

Portals Settings and Customization

Portal Name: * Description: **1**

Portal Behavior and Flow Settings
Use these settings to specify the guest experience for this portal.

Portal Page Customization
Customize portal pages by applying a theme and specifying field names and messages displayed to users.

Welcome

Enter your Single Sign-On credentials below

Username:

Password:

Overview

Event: **5231 Guest Authentication Passed**

Username: testuser1

Endpoint Id

Endpoint Profile

Authorization Result

Authentication Details

Source Timestamp: 2015-04-05 08:48:06.245

Received Timestamp: 2015-04-05 08:48:08.268

Policy Server: albarak-vm2

Event: **5231 Guest Authentication Passed**

Failure Reason

Resolution

Root cause

Username: **testuser1**

User Type: NON_GUEST

Endpoint Id

Endpoint Profile

IP Address

Authentication Identity Store: **OAAM4**

Identity Group: Any

Reflected at Authentication logs

Authentications Reports Adaptive Network Con

Misconfigured Supplicants **0** Misc

Show Live Sessions Add or Remove Columns Refresh Reset Repeat Count

Time	Status	Details	Repeat Count	Identity	Endpoint
2015-04-05 08:48:06.268	<input checked="" type="checkbox"/>			testuser1	

Sponsored Guest Portal

Acceptable Use Policy
Please read the Acceptable Use Policy

Please accept the policy. You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web, and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's

Oracle Access Manager SAML SSO

- Service Provider MetaData

Provider ID

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="CiscoISE/f909a220-c0b1-11e4-af90-000c29f746a9" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:metadata urn:oasis:names:tc:SAML:2.0:metadata.xsd">
  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" >
    <md:NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:transient />
    <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress />
    <md:NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:persistent />
    <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified />
    <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName />
    <md:NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos />
    <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:subjectname />
    <md:AssertionURL index="0" Location="https://10.56.24.65:8443/mydevicesportal/SSOLoginResponse.action" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" />
    <md:AssertionURL index="1" Location="https://albarak-vm2.cisco.com:8443/mydevicesportal/SSOLoginResponse.action" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" />
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Assertion URL per host
name / IP address / FQDN

Oracle Access Manager SAML SSO

- 'username' attribute assertion requirements

As part of the SAML Assertion (which is return back as a response from the IDP) ISE **expects** to get **'username'** attribute assertion

'username' attribute assertion should provide the user name which made the authentication and will be shown at ISE logs

'username' attribute assertion is mandatory and should be returned by the IDP

The screenshot displays the 'Mapping Options' section of the Oracle Access Manager configuration. It shows the 'Attribute Mapping' tab selected, with the 'Attribute Profile' set to 'sp-attribute-profile'. Below this, the 'Advanced' section is visible, showing a table of attribute mappings.

Row	Message Attribute Name	Value	Always Send
1	group	\$user.groups	true
2	mobile	\$user.attr.mobile	true
3	username	\$user.userid	true

Important note

SP metadata should be re-export and import to the IDP in the following cases:

- Node is registered to deployment
- IP address change of one of the nodes in deployment
- Host name change of one to the nodes in deployment
- FQDN is set or modified
- If adding or removing a new interface or changing TCP port Portal settings

Oracle Access Manager SAML SSO

- WebLogic user database

Users accessing the SSO base portals (which includes Guest, Sponsor, My Devices) via OAM SSO are stored in the weblogic server (or OAM setup for external to AD which is beyond scope of this document)

ORACLE WebLogic Server® Administration Console

Change Center
View changes and restarts
Click the Lock & Edit button to modify, add or delete items in this domain.
Lock & Edit
Release Configuration

Domain Structure
oam_domain
├ Environment
├ Deployments
├ Services
├ **Security Realms**
├ Interoperability
├ Diagnostics

How do I...
Manage users and groups

Home Log Out Preferences Record Help

Home > Summary of Security Realms > myrealm > **Users and Groups**

Settings for myrealm
Configuration **Users and Groups** Roles and Policies Credential Mappings Providers Migration

Users Groups

This page displays information about each user that has been configured in this security realm.
Some results are not displayed because there are too many matches. Please customize this table to specify more specific criteria.

Customize this table

Users
New Delete

Name	Description
guestUser1095	guestUser1095
guestUser1096	guestUser1096
guestUser1097	guestUser1097
guestUser1098	guestUser1098
guestUser1099	guestUser1099

Oracle Access Manager SAML SSO

- Sponsor Group Membership required

Note: The SAML user must exist in an external identity store (AD or LDAP) for sponsor group membership validation

This external group needs to be added to the sponsor group

The screenshot shows the 'Sponsor Group' configuration interface. At the top left, there is a checkbox labeled 'Disable Sponsor Group' and a 'Save' button. Below this, the 'Sponsor group name:' field contains 'ALL_ACCOUNTS (default)'. The 'Description:' field contains the text: 'Sponsors assigned to this group can manage all guest user accounts. By default, users in the ALL_ACCOUNTS user identity group are members of this sponsor group'. A 'Members...' button is located below the description. Underneath, there is a section titled 'Sponsor Group Members' with a search bar and a 'Search' button. The search results show a table with one entry: 'Name' with the value 'ALL_ACCOUNTS (default)' and the full path 'nyc.us.com:nyc.us.com/Users/Domain Users'. At the bottom of the form, there is a note: 'Verify that these sponsors are included in the identity source sequence associated with the sponsor portal they will use.' and another note: 'This sponsor group can create accounts using these guest types:'.

Oracle Access Manager SAML SSO

- Search a SAML-authenticated User Against Another Identity Store for Authorization

ISE 1.4 allows creating AuthZ rule that with condition involve the identity derived from a SAML SSO-based authentication and group or attribute from other Identity Store such as AD or LDAP

Note: Same SAML user must exist in an external identity store (AD or LDAP)

```

 guest_only_pd49_LDAP if (Network Access:UseCase EQUALS Guest Flow AND Network Access:UseCase NOT_EQUALS Host Lookup AND Network Access:AuthenticationIdentityStore EQUALS idp4 AND pd49_ldap:ExternalGroups EQUALS CN=My_Sponsor_49_Grp,CN=Users,DC=pd49,DC=uk AND pd49_ldap:mail EQUALS pd49@aol.com) then permit_guess

```

IDP user & user's group from LDAP

Oracle Access Manager SAML SSO

- Troubleshooting – Service Provider not recognized by ID Provider

Clicking on test portal or actual SAML flow ends the flow with System error

FIX: Re-Export the SP (ISE) metadata to the Identity Provider (Oracle)

The image shows two overlapping screenshots from the Oracle Access Manager interface. The top screenshot displays an error message:

ORACLE Access Manager

Error

System error. Please re-try your action. If you continue to get this error, please contact the Administrator.

The bottom screenshot shows the **Identity Provider Administration** page. It includes a search tool for Service Provider Partners and a table of search results.

Identity Provider Administration

You are using Oracle Access Manager as a Federation Identity Provider. Use the following screens to manage your partner

Search Service Provider Partners | Service Provider Attribute Profiles

Use the search tool to find your Service Provider partner or register a new partner using the Create Service Provider

Search

Partner Name Provider ID

Status Protocol

Description

Search Results

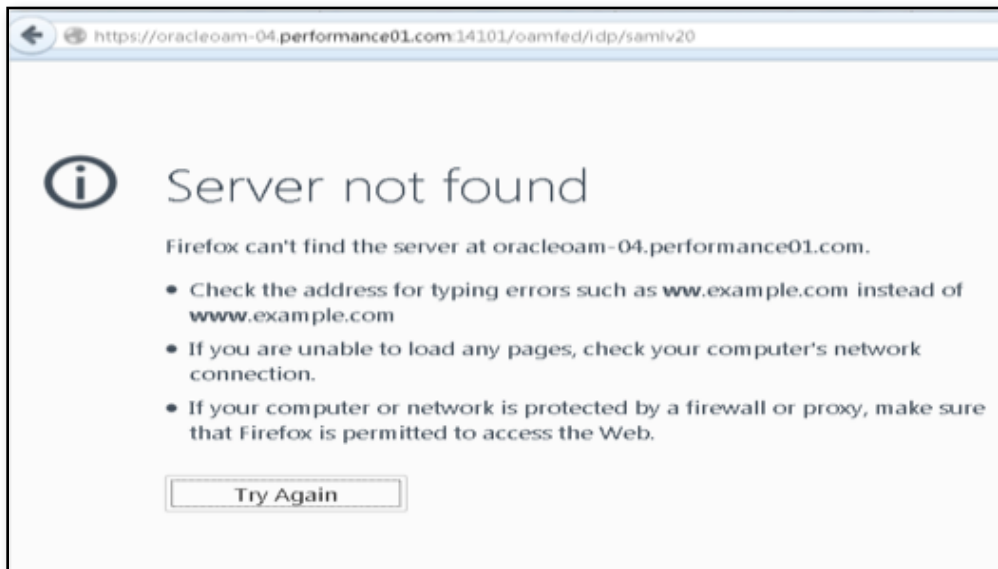
Row	Partner Name	Status	Provider ID
1	zarya5	Enabled	CiscoISE/dbceb440-a214-11e4-a735-000c2960b291
2	vrtipse4	Enabled	CiscoISE/ffb858a0-bb1b-11e4-9eaf-005056bf01c9
3	...	Enabled	...

Oracle Access Manager SAML SSO

- Troubleshooting – DNS Resolution for flow or Portal Test URL

In order to use the Portal Test URL or the user flow with any of the ISE portals (guest, sponsor, my devices), the machine accessing ISE needs to also be able to resolve the name of the ID Provider portal (Oracle)

FIX: Add ID Provider host to DNS



Oracle Access Manager SAML SSO

- Troubleshooting – guest authentication fails ‘username’ assertion is not defined at the Ext. Identity Provider

Problem:
guest authentication fails with unable to find ‘username’ attribute assertion

Resolution:
adding ‘username’ assertion at the External IDP (Oracle) side

Sponsored Guest Portal

Error

There was a problem accessing the site. Please contact help desk for assistance.

Overview

Event	5418 Guest Authentication Failed
Username	
Endpoint Id	
Endpoint Profile	
Authorization Result	

Authentication Details

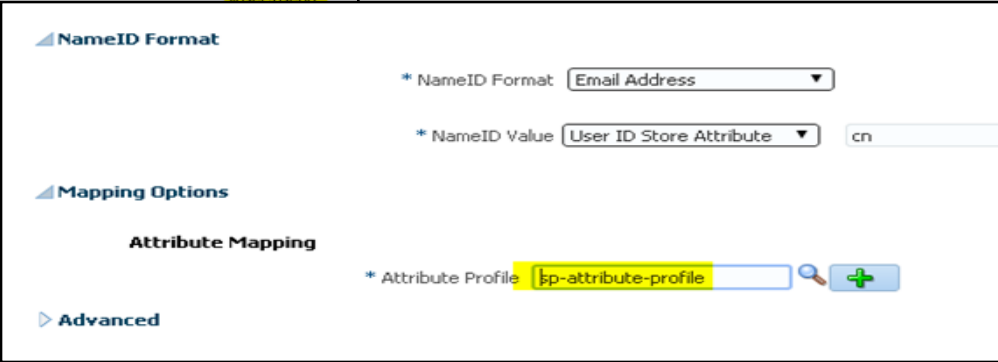
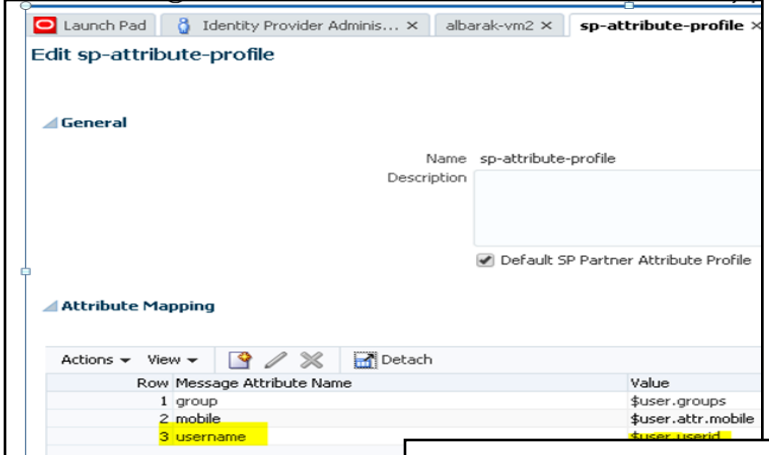
Source Timestamp	2015-04-05 12:29:30.793
Received Timestamp	2015-04-05 12:29:30.8
Policy Server	albarak-vm2
Event	5418 Guest Authentication Failed
Failure Reason	24803 Unable to find 'username' attribute assertion
Resolution	Define 'username' attribute assertion to return at the remote Identity Provider
Root cause	Unable to find 'username' attribute assertion

Oracle Access Manager SAML SSO

- Troubleshooting – resolution add username assertion to ID Provider

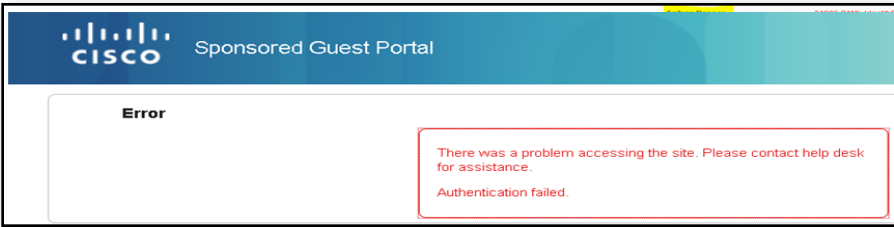
Problem:
guest authentication fails with unable to find 'username' attribute assertion

Resolution:
adding 'username' assertion at the External IDP (Oracle) side



Oracle Access Manager SAML SSO

- Troubleshooting – web portal problem accessing site, authentication failed



Authentication Details

Source Timestamp	2015-04-05 12:58:59.363
Received Timestamp	2015-04-05 12:58:59.368
Policy Server	albarak-vm2
Event	5418 Guest Authentication Failed
Failure Reason	24806 SAML IdentityProvider Certificate is not valid
Resolution	Please check DetailedInfo for more detailed error description. Common problems are: Signature validation or CA trust chain problem.
Root cause	SAML IdentityProvider Certificate is not valid

Other Attributes

ConfigVersionId	61
DetailedInfo	The issuer certificate could not be found. Check Trusted Certificates contain root certificate and intermediate certificates required for validation of the IdP signing certificate
IpAddress	10.149.172.62

Problem:
Can't access portal served by SAML IDP SSO mechanism due to IDP certificate validation failure

Error
There was a problem accessing the site. Authentication failed.

Resolution:
Make sure the IDP certificate root or self-signed cert is present in the trusted certificates store

Oracle Access Manager SAML SSO

- Troubleshooting – other SAML issues

The screenshot shows a web page titled "Sponsored Guest Portal" with the Cisco logo. Below the header, there is an "Error" section with a red border containing the message: "There was a problem accessing the site. Please contact help desk for assistance. Authentication failed." To the left of this message is a detailed error report box. The report is divided into two main sections: "Authentication Details" and "Other Attributes".

Authentication Details

- Source Timestamp
- Received Timestamp
- Policy Server
- Event
- Failure Reason
- Resolution
- Root cause

Other Attributes

- ConfigVersionId
- DetailedInfo

Problem:

There was a problem accessing the site. Authentication failed

Check the authentication logs and act according to the failure reason, resolution or Detailed Info attribute

Common fixes

Re-export metadata to the external IDP (remove any previous configuration)

Check clock skew between ISE and IDP

Oracle Access Manager SAML SSO

- Open Debug logs for SAML Request and Response

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The left sidebar contains a 'Logging' menu with 'Debug Log Configuration' highlighted. The main content area displays the 'Debug Level Configuration' page for the node 'albarak-vm2.cisco.com'. A table lists various components and their log levels, with the 'saml' component highlighted in yellow.

Component Name	Log Level	Description
opensaml	INFO	openSAML messages
org-apache	WARN	Apache internal messages
org-apache-cxf	WARN	CXF messages
org-apache-digester	WARN	XML processing apache internal messages
PanFailover	INFO	Pap Failover related messages
portal	DEBUG	Portal (Guest, Hotspot, BYOD, CP) debug messages
portal-session-manager	DEBUG	Portal Session Manager debug messages
portal-web-action	DEBUG	Base Portal debug messages
posture	INFO	Posture debug messages
previewportal	DEBUG	Preview Portal debug messages
profiler	INFO	profiler debug messages
provisioning	INFO	Client Provisioning client debug messages
prtt-JNI	INFO	prtt policy decision request processing layer related messages
pxgrid	INFO	pxGrid messages
Replication-Deployment	INFO	Logger related to Deployment Registration, Deployment
Replication-JGroup	WARN	Logger related to JGroup Node State
ReplicationTracker	INFO	PSC replication related debug messages
report	INFO	Debug reports on M&T nodes
RuleEngine-Attributes	INFO	Additional rule evaluation attributes in audit logs
RuleEngine-Policy-IDGroups	INFO	Additional policy vs id group audit logging at D
runtime-AAA	WARN	AAA runtime messages (prtt)
runtime-config	WARN	AAA runtime configuration messages (prtt)
runtime-logging	WARN	customer logs center messages (prtt)
saml	DEBUG	SAML messages

SAML SSO Performance Results

- Performance of Guest with SAML SSO tested and compared to Guest with AD
- Performance results are quiet identical