Oracle® Fusion Middleware

Help Reference for Oracle Access Management Consoles

12*c* (12.2.1.3.0)
E97180-01
June 2018

Oracle Fusion Middleware Help Reference for Oracle Access Management Consoles, 12*c* (12.2.1.3.0)

E97180-01

Primary Author: Binitha Monnappa

Contents

5 Password Policy Help

6 Plug-ins Help

Part II Federation Help

7 Federation Help

Part III Configuration Help

8 Available Services Help

9 User Identity Stores Help

10 Administration Help

11 Certificate Validation Help

12 Server Instances Help

13 Settings Help

Preface

This guide contains the contents of the online help that is included with the Oracle Access Managers consoles.

Audience

This document is intended for Systems Administrators who use the Oracle Access Manager Console.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Fusion Middleware 12*c* (12.2.1.3.0) documentation set:

- *Oracle Fusion Middleware Administrator’s Guide for Oracle Access Management*
- *Oracle Fusion Middleware Installing and Configuring Oracle Identity and Access Management*
- *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*
- *Oracle Fusion Middleware High Availability Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware Administering Oracle Mobile Security Suite*
- *Oracle Fusion Middleware Administering Mobile Security Access Server*
- *Oracle Fusion Middleware Administering Oracle Identity Governance*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Part I

Application Security Help

This part contains online help for the console sections on the Application Security Launch Pad.

- Quick Start Wizards Help
- Agents Help
- Access Manager Help
- Session Management Help
- Password Policy Help
- Plug-ins Help

1
Quick Start Wizards Help

The Quick Start Wizard helps you build a process definition from scratch using a process definition template. The Quick Start Wizard creates a new type for your process, prompting you for the minimum required information.

The following topic is covered:

- SSO Agent Registration

1.1 SSO Agent Registration

Agent Type

Select the agent type to register and click **Next**. The following table describes the elements in the Agent Type section of the SSO Agent Registration page:

Element	Description
Agent Type	Choose the agent type from the drop-down menu: • **Webgate**
Cancel	Click **Cancel** to cancel the changes made to the page.
Next	Click **Next** to continue to register and configure the agent.

Configure Webgate

Configure Webgate describes SSO Agent registration parameters of agent type Webgate. The following table describes the elements on the Configure Webgate page:

Element	Description
Name	The unique identifying name for this Agent registration. This is often the name of the computer that is hosting the Web server used by the WebGate. A unique identifying name for each Agent registration is preferred, However: • If the Agent Name exists, no error occurs and the registration does not fail. Instead, Access Manager creates the policies if they are not already in place. • If the host identifier exists, the unique Agent Base URL is added to the existing host identifier and registration proceeds.
Description	Type a short meaningful description for this Agent registration.
Base URL	The host and port of the computer on which the Web server for the WebGate is installed. **For example:** http://*example_host:port* or https://*example_host:port,* the port number is optional. **Note:**A particular Base URL can be registered once only. There is a one-to-one mapping from this Base URL to the Web server domain on which the WebGate is installed (as specified with the Host identifier element). However, one domain can have multiple Base URLs.

Element	Description
Access Client Password	Unique password for this WebGate, which can be assigned during this registration process. This field is optional. When a registered WebGate connects to an OAM Server, the password is used for authentication to prevent unauthorized WebGates from connecting to OAM Servers and obtaining policy information.
Host Identifier	This identifier represents the Web server host. This is automatically seeded with the value in the agent name field. **Note:** You can register multiple OAM WebGates (or Access Clients) under a single host identifier with the same Application Domain and policies, as follows: • When you register a WebGate, allow the process to create a host identifier (a name of your choice), and enable “Auto Create Policies". • Register a second WebGate with the same host identifier as Step1, and clear the “Auto Create Policies" box to eliminate policy creation.
User Defined Parameters	Parameters you can enter to enable specific WebGate behaviors.
Security	Level of communication transport security between the Agent and the OAM Server (this must match the level specified for the OAM Server), choose any of the following: • **Open** - No transport security. • **Simple** - SSL v3/TLS v1.0 secure transport using dynamically generated session keys. • **Cert** - SSL v3/TLS v1.0 secure transport using server side x.509 certificates. Choosing this option displays a field where you can enter the Agent Key Password.
Agent Key Password	The private key file (aaa_key.pem) is encrypted using DES algorithm. The Agent Key Password is saved in obfuscated format in password.xml and is required by the server to generate password.xml. However, this password is not retained by the server. **Note:** When editing an webGate registration, password.xml is updated only when the mode is changed from Open to Cert or Simple to Cert. In Cert mode, once generated, password.xml cannot be updated. Editing the Agent Key Password does not result in creation of a new password.xml.
Virtual host	Check the box if you have installed a WebGate on a Web server that contains multiple Web site and domain names. The WebGate must reside in a location that enables it to protect all of the Web sites on that server.
Auto Create Policies	During agent registration, you can have authentication and authorization policies created automatically. This option is checked (enabled) by default. **Shared Registration and Policies:** Multiple WebGates (or Access Clients) installed on different Web servers can share a single registration and policies to protect the same resources. This is useful in a high - availability fail over environment. To do this: • WebGate1 - Register the first WebGate and enable Auto Create Policies to generate a host identifier and policies. • WebGate2 - Register the second WebGate, specify the same host identifier as the first WebGate, and disable Auto Create Policies. After registering the second agent, both WebGates use the same host identifier and policies.
IP Validation	Check the box to ensure a client's IP address is as the IP address stored in the ObSSOCookie generated for single sign-on. Selecting this option displays a field where you can enter the IP Validation Exceptions.

Element	Description
IP Validation Exceptions	Enter any IP addresses to be excluded from validation using standard notation for the addresses. **For Example:** 10.20.30.123. The IP address stored in the ObSSOCookie must match the client's IP address. Otherwise, the cookie is rejected and the user must re-authenticate.
Back	Click **Back** to move backwards in the Agent Registration wizard.
Finish	Click **Finish** to complete the registration.
Cancel	Click **Cancel** to cancel the changes made to the page.

Resource Lists

The following table describes the elements in the Resource Lists section of the Configure Webgate page:

Element	Description
Protected Resource List	URIs for the protected application, For Example: /myapp/login. Each URI for the protected application should be specified in a new row of the table for the Protected Resource List. Default URI: /** The default matches any sequence of characters within zero or more intermediate levels spanning multiple directories.
Public Resource List	Each public application should be specified in a new row of the table for the Public Resource List.
Add	**Add Protected Resources**—Click Add button to add a resource to the Protected Resource list. Each URI should be specified in a new row of the table. **For Example**: If you add `/financial` (and repeat to add /myfinancial) the following URLs are seeded into the designated policies of the Application Domain when Auto Create Policies is selected): • `/financial` yields Resource URL `/financial/**` • `/myfinancial` yields Resource URL `/myfinancial/**` • `/**` **Add Public Resources**— Click Add button to add a resource to the Public Resource List. **For Example**: If you add `/people` the following URLs are included here and in the Application Domain (when Auto Create Policies is selected): `/people`
Delete	Select a row and click **Delete** to remove the row.
▲	Click to sort the items in the column in ascending order.
▼	Click to sort the items in the column in descending order.

Related Topics

Introduction to Agents and Registration in *Administrator's Guide for Oracle Access Management*

2 Agents Help

The Agents page is used to register and configure Webgates.

The Agents page is arranged in the following sections:

- Create Webgate
- Registered OAM Agent Configuration Parameters

2.1 Create Webgate

Create Webgate describes SSO Agent registration parameters of agent type Webgate. The following table describes the elements on the Create Webgate page:

Element	Description
Name	The unique identifying name for this Agent registration. This is often the name of the computer that is hosting the Web server used by the WebGate. A unique identifying name for each Agent registration is preferred, However: • If the Agent Name exists, no error occurs and the registration does not fail. Instead, Access Manager creates the policies if they are not already in place. • If the host identifier exists, the unique Agent Base URL is added to the existing host identifier and registration proceeds.
Description	Type a short meaningful description for this Agent registration.
Base URL	The host and port of the computer on which the Web server for the WebGate is installed. **For example**: http://*example_host:port* or https://*example_host:port,* the port number is optional. **Note**: A particular Base URL can be registered once only. There is a one-to-one mapping from this Base URL to the Web server domain on which the WebGate is installed (as specified with the Host identifier element). However, one domain can have multiple Base URLs.
Access Client Password	Unique password for this WebGate, which can be assigned during this registration process. This field is optional. When a registered WebGate connects to an OAM Server, the password is used for authentication to prevent unauthorized WebGates from connecting to OAM Servers and obtaining policy information.
Host Identifier	This identifier represents the Web server host. This is automatically seeded with the value in the agent name field. **Note:** You can register multiple OAM WebGates (or Access Clients) under a single host identifier with the same Application Domain and policies, as follows: • When you register a WebGate, allow the process to create a host identifier (a name of your choice), and enable “Auto Create Policies". • Register a second WebGate with the same host identifier as Step1, and clear the “Auto Create Policies" box to eliminate policy creation.

Element	Description
User Defined Parameters	Parameters you can enter to enable specific WebGate behaviors.
Security	Level of communication transport security between the Agent and the OAM Server (this must match the level specified for the OAM Server), choose any of the following: • **Open** - No transport security. • **Simple** - SSL v3/TLS v1.0 secure transport using dynamically generated session keys. • **Cert** - SSL v3/TLS v1.0 secure transport using server side x.509 certificates. Choosing this option displays a field where you can enter the Agent Key Password.
Agent Key Password	The private key file (aaa_key.pem) is encrypted using DES algorithm. The Agent Key Password is saved in obfuscated format in password.xml and is required by the server to generate password.xml. However, this password is not retained by the server.
Virtual host	Check the box if you have installed a WebGate on a Web server that contains multiple Web site and domain names. The WebGate must reside in a location that enables it to protect all of the Web sites on that server.
Auto Create Policies	During agent registration, you can have authentication and authorization policies created automatically. This option is checked (enabled) by default. **Shared Registration and Policies:** Multiple WebGates (or Access Clients) installed on different Web servers can share a single registration and policies to protect the same resources. This is useful in a high - availability fail over environment. To do this: • WebGate1 - Register the first WebGate and enable Auto Create Policies to generate a host identifier and policies. • WebGate2 - Register the second WebGate, specify the same host identifier as the first WebGate, and disable Auto Create Policies. After registering the second agent, both WebGates use the same host identifier and policies.
IP Validation	Check the box to ensure a client's IP address is as the IP address stored in the ObSSOCookie generated for single sign-on. Selecting this option displays a field where you can enter the IP Validation Exceptions.
IP Validation Exceptions	Enter any IP addresses to be excluded from validation using standard notation for the addresses. **For Example:** 10.20.30.123. The IP address stored in the ObSSOCookie must match the client's IP address. Otherwise, the cookie is rejected and the user must re-authenticate.
Back	Click **Back** to move backwards in the Agent Registration wizard.
Finish	Click **Finish** to complete the registration.
Cancel	Click **Cancel** to cancel the changes made to the page.

Resource Lists

The following table describes the elements in the Resource Lists section of the Configure Webgate page:

Element	Description
Protected Resource List	URIs for the protected application, For Example: /myapp/login. Each URI for the protected application should be specified in a new row of the table for the Protected Resource List. Default URI: /** The default matches any sequence of characters within zero or more intermediate levels spanning multiple directories.
Public Resource List	Each public application should be specified in a new row of the table for the Public Resource List.
Add	**Add Protected Resources** —Click Add button to add a resource to the Protected Resource list. Each URI should be specified in a new row of the table. **For Example:**If you add `/financial` (and repeat to add /myfinancial) the following URLs are seeded into the designated policies of the Application Domain when Auto Create Policies is selected): • `/financial` yields Resource URL `/financial/**` • `/myfinancial` yields Resource URL `/myfinancial/**` • `/**` **Add Public Resources** —Click Add button to add a resource to the Public Resource List. **For Example:** If you add `/people` the following URLs are included here and in the Application Domain (when Auto Create Policies is selected): `/people`
Delete	Select a row and click **Delete** to remove the row.
▲	Click to sort the items in the column in ascending order.
▼	Click to sort the items in the column in descending order.

Related Topics

Introduction to Agents and Registration in *Administrator's Guide for Oracle Access Management*

2.2 Search Webgates

Use this page to create a new webgate registration or search for a specific WebGate or group of WebGates.

Search

The following table describes the elements in the search section of the webgate page:

Element	Description
Name	Enter the name (or partial name and wild card (*)) as defined on the registration page. For example: Entering a* could return Agent_WebGate_AccessDebugNew in the result table.

Element	Description
Preferred Host	Enter all (or part of with a wild card (*)) hostname as it appears in HTTP requests. For example: iam* could return IAMSuiteAgent in the result stable.
State	Choose a state to narrow the search and results: • **Enabled** • **Disabled**
Primary Server	Enter the entire (or partial with a wild card (*)) Primary Server name.
Secondary Server	Enter the entire (or partial with a wild card (*)) Secondary Server name.
Create Webgate	Click to open a fresh WebGate registration page.
Search	Click **Search** to display search results in the table.
Reset	Click **Reset** to reset the search criteria.

Search Results

Search results displays the webgates that met the conditions specified in the search fields. The following table describes the elements in the search results section of the webgate page:

Element	Description
Actions	Choose options from the menu to perform the following operations: • **Create** - Select **Create** to create a new webgate using the WebGate registration page. • **Duplicate** - Select a row in the table and choose **Duplicate** to open the existing record in edit mode, user can make changes and save the record. • **Edit** - Select a row in the table and choose **Edit** to open the record in edit mode. After edit, click **OK** to save the changes or **Cancel** to cancel the changes. • **Delete** - Select a row in the table and choose **Delete**, in the confirm pop-up click **Yes** to remove the row or click **No** to retain the row.
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Sort** - Click to sort the column in ascending or descending order. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Create	Click **Create** to create a new webgate using the WebGate registration page.
Duplicate	Click **Duplicate** to select a row in the table and choose **Duplicate** to open the existing record in edit mode, user can make changes and save the record.
Edit	Click **Edit** to select a row in the table and choose **Edit** to open the existing record in edit mode, user can make changes and save the record.

Element	Description
Delete	Select a row in the table and click **Delete**, in the confirm pop-up click **Yes** to remove the row or click **No** to retain the row.
Detach	Click to open the table in a larger window.
Row	Displays the row number.
Name	Displays the webgate name.
Version	Displays the webgate version.
Preferred Host	Displays the hostname.
State	Displays the state of the webgate.
Primary Server	Displays the primary server name.
Secondary Server	Displays the secondary server name.

Related Topics

Introduction to Agents and Registration in *Administrator's Guide for Oracle Access Management*

2.3 Registered OAM Agent Configuration Parameters

After you register the agent using Oracle Access Management console, double-click SSO agents in the console, search for a registered OAM agent, click the agent name in the results table and you can view/edit the agent configuration page in the console. The following table describes the elements when you view the registered agent:

Element	Description
Version	Displays OAM Webgate
Name	Displays the name of the agent.
Description	Displays the description for the agent.
Access Client Password	Displays the password registered with the agent.
Security	Displays the chosen level of communication transport security between the Agent and the OAM Server
State	Specifies whether this registration is enabled or disabled. Default = Enabled
Max Cache Elements	Number of elements maintained in the cache. Caches are the following: • Resource to Authentication Scheme—This cache maintains information about Resources (URLs), including whether it is protected and, if so, the authentication scheme used for protection. • Resource to Authorization Policy—This cache maintains information about Resources and associated authorization policy—This cache stores authentication scheme information for a specific authentication scheme ID. The value of this setting refers to the maximum consolidated count for elements in these caches. Default = 100000

Element	Description
Cache Timeout (seconds)	Amount of time cached information remains in the WebGate caches (Resource to Authentication Scheme, Authentication Schemes, and Resource to Authorization Policy) when the information is neither used nor referenced. Default = 1800 (seconds)
Token Validity Period (seconds)	Maximum valid time period for an agent token (the content of OAMAuthnCookie). This value is the validity period for the obsso cookie. Within this period, only authorization nap calls will pass to the OAM server. Once this period has passed, the obsso cookie will be considered invalid and an 'obrareq.cgi' redirect will occur. The OAM Server will validate the OAM_ID cookie and re-issue a new obsso cookie, or challenge the user if the server side session is expired/deleted/timed out. Default = 3600 (seconds)
Max Connections	The maximum number of connections that this WebGate can establish with the OAM Server. This number must be the same as (or greater than) the number of connections that are actually associated with this agent. Default = 1
Max Session Time (hours)	Maximum time to keep WebGate connections to OAM Server network alive. After this time all WebGate to OAM Server network connections will be shutdown and replaced with new ones. The unit is based on the maxSessionTimeUnits user-defined parameter which can be 'minutes' or 'hours'. When maxSessionTimeUnits is not defined, the unit is defaulted to 'hours'.
Failover Threshold	Number representing the point when this WebGate opens connections to a Secondary OAM Server. Default = 1 For example, if you type 30 in this field and the number of connections to primary OAM Server falls to 29, this Agent opens connections to secondary OAM Server.
AAA Timeout Threshold	Number (in seconds) to wait for a response from the OAM Server. If this parameter is set, it is used as an application TCP/IP timeout instead of the default TCP/IP timeout. Default = -1 (default network TCP/IP timeout is used) If using a simple mode WebGate, you can improve the response time of the OAM login page by changing the aaaTimeoutThreshold time parameter in the WebGate profile from -1 to 10. A typical value for this parameter is between 30 and 60 seconds. If set to a very low value, the socket connection can be closed before a reply from OAM Server is received, resulting in an error.
Preferred Host	Specifies how the hostname appears in all HTTP requests as users attempt to access the protected Web server. The hostname within the HTTP request is translated into the value entered into this field regardless of the way it was defined in a user's HTTP request. The Preferred Host function prevents security holes that can be inadvertently created if a host's identifier is not included in the Host Identifiers list. However, it cannot be used with virtual Web hosting. For virtual hosting, you must use the Host Identifiers feature. Defaults to Name (of WebGate registration)

Element	Description
Logout URL	The Logout URL triggers the logout handler, which removes the cookie (ObSSOCookie; OAMAuthnCookie) and requires the user to re-authenticate the next time he accesses a resource protected by Access Manager. Default = [] (not set)
Logout Callback URL	The URL to oam_logout_success, which clears cookies during the call back. This can be a URI format without host:port (recommended), where the OAM Server calls back on the host:port of the original resource request. For example: Default = /oam_logout_success This can also be a full URL format with a host:port, where OAM Server calls back directly without reconstructing callback URL.
Logout Redirect URL	This parameter is automatically populated after agent registration completes.By default, this is based on the OAM Server host name with a default port of 14200. For example: Default = http://OAMServer_host:14200/oam/server/logout
Logout Target URL	The value is the name for the query parameter that the OPSS applications passes to WebGate during logout; the query parameter specifies the target URL of the landing page after logout completes. Default: end_url
User Defined Parameters	Parameters you can enter to enable specific WebGate behaviors.
Sleep for (seconds)	The frequency (in seconds) with which the OAM Server checks its connections to the directory server. For example, if you set a value of 60 seconds, the OAM Server checks its connections every 60 seconds from the time it comes up. Default: 60 (seconds)
Cache Pragma Header Cache Control Header WebGate only (not Access Clients)	These settings apply only to WebGates and control the browser's cache. By default, both parameters are set to no-cache. This prevents WebGate from caching data at the Web server application and the user's browser. However, this may prevent certain operations such as downloading PDF files or saving report files when the site is protected by a WebGate. You can set the Access Manager SDK caches that the WebGate uses to different levels. See http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html section 14.9 for details. All of the cache-response-directives are allowed. For example, you may need to set both cache values to public to allow PDF files to be downloaded. Defaults: no-cache
Debug	Debugging can be enabled or not.
IP Validation	Check the box to ensure a client's IP address is as the IP address stored in the ObSSOCookie generated for single sign-on. Selecting this option displays a field where you can enter the IP Validation Exceptions.

Element	Description
Allow Management Operations	This Agent Privilege function enables the provisioning of session operations per agent, as follows: • Terminate session • Enumerate sessions • Add or Update attributes for an existing session • List all attributes for a given session ID or read session Default: Disabled
Allow Token Scope Operations	Allows the ASDK code to scope the OAM_ID cookie to the domain level instead of host level.
Allow Master Token Retrieval	Allows the ASDK code to retrieve the OAM_ID cookie.
Allow Credential Collector Operations	Activates WebGate detached credential collector functionality for simple-form or dynamic multi-factor authentication. Default: Disabled
IIS Impersonation User	The trusted user for impersonation, in Active Directory. This user should not be used for anything other than impersonation. The constraints are the same as any other user in Active Directory.
IIS Impersonation Password	This is the trusted user password for impersonation. The constraints are the same as any other user password in Active Directory.
Primary Server List	Identifies Primary Server details for this Agent. The default is based on the OAM Server: • Server Name • Host Name • Host Port • Max Number (maximum connections this WebGate will establish with the OAM Server (not the maximum total connections the WebGate can establish with all OAM Servers).)
Secondary Server List	Identifies Secondary OAM Server details for this agent, which must be specified manually: • Server Name • Host Name • Host Port • Max Number (maximum connections this WebGate will establish with the OAM Server (not the maximum total connections the WebGate can establish with all OAM Servers).)
Apply	You can make any changes if required and click on **Apply** to submit the registration.
Download	Click **Download** to download the generated artifacts.

Related Topics

Introduction to Agents and Registration in *Administrator's Guide for Oracle Access Management*

3

Access Manager Help

Access Manager is an enterprise level solution that centralizes critical access control services. It is used to provide an integrated solution that delivers authentication, authorization, web single sign-on, policy administration, enforcement agent management, session control, systems monitoring, reporting, logging and auditing.

The following topics are covered:

- Create Application Domain
- Create Resource Type
- Create Host Identifier
- Create Authentication Scheme

3.1 Create Application Domain

Use the Create Application Domain page to manually create an Application Domain.

Summary

The following table describes the elements on the Create Application Domain page:

Element	Description
Name	Type a unique name for the Application Domain.
Description	Type a short description for the Application Domain.
Session Idle Timeout (minutes)	Enter the amount of time in minutes, that a user's authentication session remains valid without accessing any Oracle Access Manager protected resources. When the user is idle for a longer period, they are asked to re-authenticate.
Allow OAuth Token	Check this box to allow use of OAuth Token.
Allow Session Impersonation	Check this box to allow an end user to designate one or more users to act on his behalf within a constrained window of time.
Enable Policy Ordering	Select to enable Policy Ordering section.
Apply	Click **Apply** to submit the changes.

Policy Ordering

Use this section to order policies if the **Enable Policy Ordering** option is selected.

Element	Description
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Add	Click **Add** to add a Resource Prefix using Resource Prefix dialog box.
Edit	Select a row from the table, click **Edit** to make changes using Resource Prefix dialog box.
Delete	Select a row from the table, click **Delete** to remove the row.
Resource Prefix	Displays all the Resource Prefix added using the dialog box.
Resource Type	Displays all the Resource Type added using the dialog box.
Host Identifier	Displays all the Host Identifier added using the dialog box.

Resource Prefix dialog box

The following table describes the elements in the Resource Prefix dialog box:

Element	Description
Resource Type	Choose a Resource Type from the drop-down menu: • **wl_authen** - This resource type is used for Fusion Middleware application scenarios. • **TokenServiceRP** - This resource type is used to represent the Token Service Relying Party. • **HTTP** - This resource type covers resources that are accessed using either HTTP or HTTPS protocol. Policies that govern a particular resource apply to all operations defined for the resource.
Host Identifier	Add an optional Host Identifier. **Note:** Host Identifier is mandatory for an HTTP Resource Type.
Resource Prefix	Add the Resource Prefix. **For Example:** If the policy Resource being protected is /em/**, the Resource Prefix is /em. If the policy Resource being protected is /blog/**, the Resource Prefix is /blog.
Add	Click **Add** to add the entries to the Policy Ordering table.
Cancel	Click **Cancel** to cancel the changes.
✕	Click to close the dialog box.

Search Application Domain

Use the Search Application Domains page to perform an advanced search for specific application domains. The following table describes the elements in Search section of the Application Domains page:

Element	Description
Name	Enter a name of the Application Domain (or a partial name with wild card (*)), or leave the Name field blank to show all the domains.

Element	Description
Create Application Domain	Click to create a new Application Domain using the **Create Application Domain** page.
Search	Click **Search** to initiate the search and populate results in the Search Results table.
Reset	Click **Reset** to reset the search criteria.

Search Results

Search results returned are the application domains that met the conditions specified in the search fields. The following table describes the elements in the Search Results section of the Application Domains page:

Element	Description
Actions	Choose options from the menu to perform the following operations: • **Create** - Select Create to create a new Application Domain using the **Create Application Domain** page. • **Duplicate** - Select a row in the table and choose **Duplicate** to open the existing record in edit mode, user can make changes and save the record. • **Edit** - Select a row in the table and choose **Edit** to open the record in edit mode. After edit, click **OK**to save the changes, or **Cancel** to cancel the changes. • **Delete** - Select a row in the table and choose **Delete**, in the confirm pop-up click **Yes** to remove the row, or click **No** to retain the row.
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Create	Click to create a new Application Domain using the **Create Application Domain** page.
Edit	Select a row in the table and click **Edit** to open the record in edit mode. After edit, click **OK** to save the changes, or **Cancel** to cancel the changes.
Delete	Select a row in the table and click **Delete**, in the confirm pop-up click **Yes** to remove the row, or click **No** to retain the row.
Detach	Click to expand the Search Results table to a full page.
Row	Displays the Row number.
Name	Displays the searched Application Domain names.
Description	Displays the descriptions for the Application Domain searched.
▲	Click to sort the items in the column in descending order.
▼	Click to sort the items in the column in descending order.

Related Topics

Managing Policies to protect Resources and Enable SSO in *Administrator's Guide for Oracle Access Management*

3.2 Create Resource Type

Use the Create Resource Type page to define a custom resource type. Any defined custom resource type is listed with default resource types when adding resources to an authentication or authorization policy.

The following table describes the elements on the Create Resource Type page:

Element	Description
Name	Type a unique name of up to 30 alpha or numeric characters. It is a required field. **Note:** A non-HTTP Resource Type name cannot match a Host Identifier (and vice versa).
Description	Type a short description to describe the purpose of this resource type using up to 20 alpha or numeric characters. **For Example:** Resources representing WebLogic Authentication schemes.
Apply	Click **Apply** to submit this custom resource definition.

Operations

You can add (or remove) Operations. The following table describes the elements in the Operations section of the Create Resource Type page:

Element	Description
Operation	Policies that govern a particular resource apply to all specified operations defined for the resource. There is no limit to the number of operations that can be added to the resource type. • Get • Post • Put • Head • Issue (`TokenServiceRP`) • Login (`wl_authen`) • Delete • Trace • Options • Connect • Other
✚	Click to add a new row to the table.
✖	Select a row and click ✖ to remove the row.

Search Resource Type

Use the Search Resource Types page to perform an advanced search for a specific Resource Type. The following table describes the elements in the Search section of the Resource Type page:

Element	Description
Name	Enter the name of the Resource Type (or a partial name with wild card (*)).
Create Resource Type	Click to create a new Resource Type using the **Create Resource Type** page.
Search	Click **Search** to initiate the search and populate results in the Search Results table.
Reset	Click **Reset** to reset the search criteria.

Search Results

Search results are the Resource Type that met the conditions specified in the search fields. The following table describes the elements in the Search Results section of the Resource Type page:

Element	Description
Actions	Choose options from the menu to perform the following operations: • **Create** - Select Create to create a new Resource Type using the **Create Resource Type** page. • **Duplicate** - Select a row in the table and choose **Duplicate** to open the existing record in edit mode, user can make changes and save the record. • **Edit** - Select a row in the table and choose **Edit** to open the record in edit mode. After edit, click **OK** to save the changes, or **Cancel** to cancel the changes. • **Delete** - Select a row in the table and choose **Delete**, in the confirm pop-up click **Yes** to remove the row, or click **No** to retain the row.
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Create	Click to create a new Resource Type using the**Create Resource Type** page.
Duplicate	Click to create a copy of the existing record. Select a row and click **Duplicate** to open the existing record in edit mode, user can make changes and save the record.
Edit	Select a row in the table and click **Edit** to open the record in edit mode. After edit, click **OK** to save the changes, or **Cancel** to cancel the changes.
Delete	Select a row in the table and click **Delete**, in the confirm pop-up click **Yes** to remove the row, or click **No** to retain the row.
Detach	Click to expand the Search Results table to a full page.
Row	Displays the row number.

Element	Description
Name	Displays the searched Resource Type names.
Description	Displays the descriptions for the Resource Types searched.
▲	Click to sort the items in the column in ascending order.
▼	Click to sort the items in the column in descending order.

Related Topics

Managing Authentication and Shared Policy Components in *Administrator's Guide for Oracle Access Management*

3.3 Create Host Identifier

Use the Create Host Identifier page to create a host identifier definition manually, this is needed if an application and resources are manually added to a host and has no mapped host identifier. If you choose Auto Create Policies while registering an Agent, this is done automatically.

The following table describes the elements on the Create Host Identifier page:

Element	Description
Name	Type a unique name for this definition. Use only upper and lower case alpha characters. No punctuation or special characters are allowed.
Description	Type a description that explains the use of this configuration, you can type up to 200 characters.
Apply	Click to submit this Host Identifier.

Host Name Variations

Add (or remove) host name and port variations in the Operations list. The following table describes the elements in the Host Name Variations section of the Create Host Identifier page:

Element	Description
Host Name	A list of various host names or permutations added that users might use when accessing the application.
Port	The Web server port used by each host or permutation.
✚	Click to add a new row to the table. Enter a new host name and port combination to identify variables that map to the Host Identifier Name.
✖	Select any row, then click ✖ button to remove the row.

Search Host Identifiers

Use the Search Host Identifiers page to perform an advanced search for a specific Host Identifier. The following table describes the elements in the Search section of the Host Identifiers page:

Element	Description
Name	Enter a name of the Host Identifier (or a partial name with wild card (*)), or leave the Name field blank to show all Host Identifiers.
Search	Click **Search**to initiate the search and populate results in the Search Results table.
Reset	Click **Reset** to reset the search criteria.
Create Host Identifier	Click to create a new Host Identifier using the **Create Host Identifier** page.

Search Results

Search results are the Host Identifiers that met the conditions specified in the search fields. The following table describes the elements in the Search Results section of the Host Identifiers page:

Element	Description
Actions	Choose options from the menu to perform the following operations: • **Create** - Select Create to create a new Host Identifier using the **Create Host Identifier** page. • **Duplicate** - Select a row in the table and choose **Duplicate** to open the existing record in edit mode, user can make changes and save the record. • **Edit** - Select a row in the table and choose **Edit** to open the record in edit mode. After edit, click **OK** to save the changes, or **Cancel** to cancel the changes. • **Delete** - Select a row in the table and choose **Delete**, in the confirm pop-up click **Yes** to remove the row, or click **No** to retain the row.
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Create	Click to create a new Host Identifier using the**Create Host Identifier** page.
Duplicate	Click to create a copy of the existing record. Select a row and click **Duplicate** to open the existing record in edit mode, user can make changes and save the record.
Edit	Select a row in the table and click **Edit** to open the record in edit mode. After edit, click **OK** to save the changes, or **Cancel** to cancel the changes.
Delete	Select a row in the table and click **Delete**, in the confirm pop-up click **Yes** to remove the row, or click **No** to retain the row.
Detach	Click to expand the Search Results table to a full page.
Row	Displays the row number.
Name	Displays the searched Host Identifier names.
Description	Displays the descriptions for the Host Identifiers searched.
▲	Click to sort the items in the column in ascending order.

Element	Description
▼	Click to sort the items in the column in descending order.

Related Topics

Managing Authentication and Shared Policy Components in *Administrator's Guide for Oracle Access Management*

3.4 Create Authentication Scheme

Use the Create Authentication Scheme page to create a new Authentication scheme that defines the challenge mechanism required to authenticate a user.

The following table describes the elements on the Create Authentication Scheme page:

Element	Description
Name	Type a unique name for this scheme, this appears in the navigation tree.
Description	Type a short description that explains the use of this scheme, you can enter up to 200 characters.
Authentication Level	Enter the trust level of the authentication scheme, the trust level is expressed as an integer value between 0 (no trust) and 99 (highest level of trust). This reflects the challenge method and degree of trust used to protect transport of credentials from the user. **Note:** • Level 0 is unprotected. Only unprotected resources can be added to an Authentication Policy that uses an authentication scheme at protection level 0. • After a user is authenticated for a resource at a specified level, the user is automatically authenticated for other resources in the same Application Domain or in different Application Domains, if the resources have the same or a lower trust level as the original resource.
Default	A non-editable box that is checked when the **Set as Default** button is clicked.
Challenge Method	Select any Challenge Method from the following options in the drop-down menu: • FORM • BASIC • X509 • WNA • NONE • DAP

Element	Description
Challenge URL	This URL is associated with the selected Challenge Method. • **FORM Challenge Method** —Out of the box authentication scheme (LDAPScheme and LDAPNoPasswordValidationScheme), Challenge URL is "/pages/login.jsp". The context type and context values are used to build the final URL. • **X509 Challenge Method**— The Challenge URL takes the form: `https://managed_server_host:managed_server_ssl_port/oam/CredCollectServlet/X509`. **Note:** The default Challenge URL is based on the credential collector embedded with the OAM Server (ECC).
Context Type	This field is displayed only for Schemes using Challenge Method FORM, X509, or DAP. This is used to build the final URL for the Embedded Credential Collector (ECC only, DCC does not use this) based on the following possible values: • **default** - The Context value to construct the final URL to forward to credential collection. **For Example:** With a challenge URL of "/pages/login.jsp", and a context value of /oam, the server forwards to "/oam/pages/login.jsp" for credential collection by the ECC. • **customWar** - Use this Context Type, if a customized credential collector page "customlogin.jsp" is deployed in a WAR file (with context root, "custom") within the same domain, it should be used to collect credentials. Then set the following values to have server forward to the WEB application page "/custom/customlogin.jsp" to collect credentials: – challenge_url = "/customlogin.jsp" – contextType = "customWar" – contextValue = "/contextroot of custom application" • **external**- If the login page is external, the file can be placed in a location that is accessible to the application. Set the following values to have the server redirect to the challenge URL for credential collection. The username and password are collected by the external form (HTML or jsp) and submitted to the OAM Server: – challenge_url = "http://host:port/externallogin – contextType = "external" – contextValue = Not applicable
Context Value	Used to build the final URL for the credential collector. The default value is /oam.
Challenge Redirect URL	This URL declares the endpoint referencing the Credential Collector (ECC or DCC). **For Example:** ECC: `/oam/server` DCC: `http: //<doc-host:port>/`

Element	Description
Authentication Module	Identifies the pre-configured authentication module to be used to challenge the user for credentials. Following modules or plug-ins specified identifies the exact user identity store to be used: • FederationMTPlugin • FederationPlugin • KerberosPlugin (Authentication Modules and Custom Authentication Modules) • MTLDAPBasic • MTLDAPPlugin • OIFMTLDAPPlugin • Password Policy Validation Module • TAPModule • x509Plugin (under the X509 Authentication Modules node)
Challenge Parameters	Type short text strings that are consumed and interpreted by Webgates and Credential Collector modules to operate in the manner indicated by those values. The syntax for specifying any challenge parameter is: <parametername> = <value> **Note:** This syntax is not specific to any Webgate release. Authentication schemes are independent of Webgate release.
Set as Default	Click **Set as Default**button to select the non-editable Default check box.
Apply	Click to submit this Authentication Scheme.

Search Authentication Schemes

Use the Search Authentication Schemes page to perform an advanced search for a specific Authentication Scheme. The following table describes the elements in the Search section of the Authentication Scheme page:

Element	Description
Name	Enter a name of the Authentication Scheme (or a partial name with wild card (*)).
Search	Click **Search** to initiate the search and populate results in the Search Results table.
Reset	Click **Reset** to reset the search criteria.
Create Authentication Scheme	Click to create a new Authentication Scheme using the**Create Authentication Scheme** page.

Search Results

Search results are the Authentication Schemes that met the conditions specified in the search fields. The following table describes the elements in the Search Results section of the Authentication Scheme page:

Element	Description
Actions	Choose options from the menu to perform the following operations: • **Create** - Select Create to create a new Authentication Scheme using the **Create Authentication Scheme** page. • **Duplicate** - Select a row in the table and choose **Duplicate** to open the existing record in edit mode, user can make changes and save the record. • **Edit** - Select a row in the table and choose **Edit** to open the record in edit mode. After edit, click **OK**to save the changes or **Cancel** to cancel the changes. • **Delete** - Select a row in the table and choose **Delete**, in the confirm pop-up click **Yes** to remove the row, or click **No** to retain the row.
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Create	Click to create a new Authentication Scheme using the**Create Authentication Scheme** page.
Duplicate	Click to create a copy of the existing record. Select a row and click **Duplicate** to open the existing record in edit mode, user can make changes and save the record.
Edit	Select a row in the table and click **Edit** to open the record in edit mode. After edit, click **OK** to save the changes or **Cancel** to cancel the changes.
Delete	Select a row in the table and click **Delete**, in the confirm pop-up click **Yes** to remove the row, or click **No** to retain the row.
Detach	Click to expand the Search Results table to a full page.
Row	Displays the row number.
Name	Displays the searched Authentication Scheme names.
Description	Displays the descriptions for the Authentication Scheme searched.
▲	Click to sort the items in the column in ascending order.
▼	Click to sort the items in the column in descending order.

Related Topics

Managing Authentication and Shared Policy Components in *Administrator's Guide for Oracle Access Management*

4 Session Management Help

Use the Session Management page to locate and delete one or more access sessions for a single user, or for all users.

4.1 Session Management

Use the Session Management page to locate and delete one or more access sessions for a single user and to delete all user sessions. Use the search section to search Session Management page to perform an advanced search for specific sessions, user can create query based on filter conditions and add fields to the query to further refine the search.

Search

The following table describes the elements in the Search area of the Session Management page:

Element	Description
Delete All User Sessions	Choose this command button to delete the active sessions of all users. A confirmation window appears where you can confirm or decline the operation.
User ID	Enter a specific user ID and click **Search** button to display all active sessions for this user. Incomplete strings and wild cards are allowed. Use the drop-down menu to choose options like **Starts with**, **Equals**, **Contains**, and the like to further assist in your search.
Client IP Address	Enter a Client IP Address and click **Search** button to display all active sessions for this user. Incomplete strings and wild cards are allowed. Use the drop-down menu to choose options like **Starts with**, **Equals**, **Contains**, and the like to further assist in your search.
Search	Click this button to initiate a search based on criteria in the form.
Reset	Click this button to clear the form of all criteria.
Add Fields	Displays a menu from which you can select additional criteria to add to the search form, this can include **ID Store**, **Last Access Time**, **Session ID**, and so on. Click the **Add Fields** button, select the items in the list and add them to the form and click **Save**.
Reorder	Displays a dialog box that lets you change the order of the search fields.

Search Results

Search results are the Sessions that met the conditions specified in the search fields. The following table describes the elements in the Search Results section of the Session Management page:

Element	Description
View	Choose commands from the View menu (located above the search results table) to control how the search results are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Delete	Click a row in the results table to select it (the row should be highlighted), then choose the Delete button to delete the row. A confirmation window appears where you can confirm or decline the operation. **Note**: When session search criteria is generic, using just a wild card (*), for example, there is a limitation on deleting a session from a large list of sessions. Your session search criteria should be fine-grained enough to obtain a relatively small set of results (ideally 20 or less).
Detach	Click to expand the results table to a full-page view. If the page is already detached, click to restore the results table to the Session Management page.
Results table	Displays search results consisting of active sessions.
Client IP Address	The IP address that the client is logged on from.
Creation Instant	Time stamp showing when the session was created.
Expiry Instant	Date and time that the session is set to expire.
ID Store	The identity store in which the user who owns the session is defined.
Impersonating	Shows **true** if the session is impersonated; otherwise, **false**.
Last Access Time	Time stamp showing when the last session access occurred.
Last Update Time	Time stamp showing when the last update occurred.
Session ID	A unique, OAM-generated session identifier.
User ID	The unique identifier that identifies the user.

Related Topics

Maintaining Access Manager Sessions in *Administrator's Guide for Oracle Access Management*

5 Password Policy Help

Use the Password Policy page to define password policy based on enterprise requirements.

5.1 Password Policy

Use the Password Policy page to configure the Password policy based on enterprise requirements.

Password Options

The following table describes the elements on the Password Policy page:

Element	Description
Minimum Uppercase Characters	Define the minimum number of uppercase characters required in a password.
Minimum Lowercase Characters	Set the minimum number of lowercase characters required in a password.
Minimum Alphabetic Characters	Define the minimum number of alphabetic characters allowed in the password.
Minimum Numeric Characters	Set the minimum number of numeric characters required in a password.
Minimum Alphanumeric Characters	Define the minimum number of alphanumeric characters required in a password.
Minimum Special Characters and Maximum Special Characters	Define the minimum and maximum number of Special Characters required in a password.
Minimum Unicode Characters and Maximum Unicode Characters	Define the minimum and maximum number of Unicode characters required in a password.
Minimum Password Length and Maximum Password Length	Define the total minimum and maximum number of characters allowed in a password.

Element	Description
Minimum Unique Characters	Define the minimum unique characters allowed in a password.
Maximum Repeated Characters	Define the maximum repeated characters allowed in a password.
Minimum Password Age (days)	Define the minimum password age in days.
Characters Required	Define the specific characters that are required in a password. No delimiter is needed or allowed in this definition.
Characters Not Allowed	Define the specific characters that cannot be used in a password. No delimiter is needed or allowed in this definition.
Characters Allowed	Define all allowed characters in a password. No delimiter is needed or allowed in this definition.
Substrings Not Allowed	Specify the character strings that are not allowed in a password. Use a comma as the delimiter in this definition.
Alphabetic Character Must Start Password	Select this box to specify that the first character in a password must be alphabetic, when checked.
Can Include User's Last Name	Select this box to specify that the user's last name is allowed in the password, when checked.
Can Include User's First Name	Select this box to specify that the user's first name is allowed in the password, when checked.
Can Include User ID	Select this box to specify that the user's User ID is allowed in the password, when checked.
Warn After (days)	Define the number of days before a designated date in which a user will be warned about password expiration. For example, you enter 30 in the Expires After (days) field, and 20 in the Warn After (days) field, and the password is created on November 1. On November 21, the user will be informed that the password will expire on December 1. This field accepts values from 0 to 999.
Maximum Attempts	Define the maximum number of login attempts a user can make before a lockout.
Expire After (days)	Define the period of time (in days) that the password is valid.
Permanent Lockout	Select this box to specify permanent lockout after the designated number of failed login attempts.
Disallow Previous Passwords	Define the number of previous passwords that cannot be used when the user changes her password.
Lockout Duration (minutes)	Define the period of time the user is locked out (in minutes) after the designated number of failed login attempts. After this period, the user can attempt a fresh login.
Password Dictionary File	Specify the physical file on OAM Servers that contain the list of restricted words that can not be specified in a password.

Element	Description
Password File Delimiter	Define the delimiter used in the Password Dictionary file to separate various words. For example, if the file contains abc, def, welcome and the dictionary delimiter is comma(,), the words that are restricted and cannot be used in a user password are abc def and welcome.
Password Service URL	The location of various password pages.
Apply	Click on **Apply** to submit the policy.

Related Topics

Using Password Policy in *Administrator's Guide for Oracle Access Management*.

6 Plug-ins Help

Authentication is governed by specific authenticating schemes which rely on one or more plug-ins to test the credentials provided by a user when he or she tries to access a resource. The plug-ins can be taken from a standard set provided with OAM Server installation, or the custom plug-ins created by your own Java developers.

Following topics are covered:

- Create LDAP Authentication Module
- Create Kerberos Authentication Module
- Create X509 Authentication Module
- Create Custom Authentication Module
- Authentication Modules
- Authentication Plug-ins

6.1 Create LDAP Authentication Module

LDAP Authentication module matches the credentials (username and password) of the user who requests a resource to a user definition stored in LDAP directory service, an LDAP module is required for Basic and Form challenge methods. Use the Create LDAP Authentication Module page to create a new LDAP Authentication Module.

The following table describes the elements on the Create LDAP Authentication Module page:

Element	Description
Name	Type a unique name for this module.
User Identity Store	Select the registered User Identity Store from the drop-down menu. The designated LDAP user identity store must contain any user credentials required for authentication by this module. The LDAP store must be registered with Access Manager. **Note:** Multiple identity store vendors are supported. Upon installation, there is only one User Identity Store which is also the designated System Store. If you add more identity stores and designate a different store as the System Store, be sure to change the LDAP module to point to the System Store. The authentication Scheme `OAMAdminConsoleScheme` relies on the LDAP module for Administrator Roles and credentials.
Apply	Click **Apply** to submit the LDAP Authentication module.

Related Topics

Managing Authentication and Shared Policy Components in *Administrator's Guide for Oracle Access Management*.

6.2 Create Kerberos Authentication Module

Kerberos Authentication module identifies the key tab file and krb5.configuration file names and Principal. This plug-in is used while configuring Access Manager for Windows Native Authentication. Use the Create Kerberos Authentication Module page to create a new Kerberos Authentication Module.

The following table describes the elements in the Create Kerberos Authentication Module page:

Element	Description
Name	Type a unique ID for this module, you can include upper and lower case alpha characters as well as numbers and spaces.
Key Tab File	Provide the path to the encrypted, local, on-disk copy of the host's key, required to authenticate to the key distribution center (KDC). **For example:**/etc/krb5.keytab. The KDC authenticates the requesting user and confirms that the user is authorized for access to the requested service. If the authenticated user meets all prescribed conditions, the KDC issues a ticket permitting access based on a server key. The client receives the ticket and submits it to the appropriate server. The server can verify the submitted ticket and grant access to the user submitting it. **Note:** The key tab file should be readable only by root, and should exist only on the machine's local disk. It should not be part of any backup, unless access to the backup data is secured as tightly as access to the machine's root password itself.
Principal	Provide the HTTP host for the principal in the Kerberos database, which enables generation of a key tab for a host.
KRB Config File	Provide a path to the configuration file that controls certain aspects of the Kerberos installation. A krb5.conf file must exist in the /etc directory on each UNIX node that is running Kerberos. krb5.conf contains configuration information required by the Kerberos V5 library (the default Kerberos realm and the location of the Kerberos key distribution centers for known realms).
Apply	Click **Apply** to submit this Kerberos Authentication Module.

Related Topics

Managing Authentication and Shared Policy Components in *Administrator's Guide for Oracle Access Management*.

6.3 Create X509 Authentication Module

X509 Authentication module is similar to LDAP Plug-in with additional properties that indicate which attribute of the client's X.509 certificate should be validated against the user attribute in LDAP. Use the Create X509 Authentication Module page to create a new X509 Authentication module.

The following table describes the elements on the Create X509 Authentication Module page:

Element	Description
Name	Type a unique name for this module.
Match LDAP Attribute	Specify the LDAP distinguished name attribute to be searched against given the X509 Cert Attribute value. **For example:** If the certificate subject EMAIL is me@example.com and it must be matched against the “mail" LDAP Attribute, an LDAP query must search LDAP against the “mail" attribute with a value "me@example.com (cn)".
X509 Cert Attribute	Specify the certificate attribute to be used to bind the public key. **For Example**, Attributes within subject, issuer scope to be extracted from the certificate: subject.DN, issuer.DN, subject.EMAIL.
Cert Validation Enabled	Check to enable the X.509 Certificate validation. Disabled when not checked. When enabled, the OAM Server performs the certificate validation (rather than having the WebLogic server intercept and validate the certificate before passing it to the OAM Server). Access Manager performs the entire certificate path validation.
OCSP Enabled	Check to enable the Online Certificate Status Protocol. Disabled when not checked. Values will be either true or false. **For example:** OCSP Enabled - true. **Note:**OCSP Server Alias, OCSP Responder URL and OCSP Responder Timeout are required only when OCSP Enabled is selected.
OCSP Server Alias	Provide an alias name for the OSCSP responder pointing to CA certificates in oamkeystore file--a mapping between the aliased name and the actual instance name or the IP address and the OSCSP Responder instance.
OCSP Responder URL	Provides the URL of the Online Certificate Status Protocol responder. **For example**: OpenSSL Responder URL: http: *//localhost:6060*.
OCSP Responder Timeout	Specify the grace period for users with expired certificates to enable them access OAM Servers for a limited time before renewing the certificate.
Apply	Click **Apply** to submit this X509 Authentication module.

Related Topics

Managing Authentication and Shared Policy Components in *Administrator's Guide for Oracle Access Management*.

6.4 Create Custom Authentication Module

Custom type Authentication module relies on bundled plug-ins. It generally uses more than one plug-in that you can orchestrate to ensure that each one performs a specific authentication function. Depending on the success or failure action defined for each plug-in, another authentication plug-in is called. Use the Create Custom Authentication Module page to create a new custom authentication module.

General

General section identifies the unique name and optional description for the individual plug-in.

The following table describes the elements in the General section of the Create Custom Authentication Module page:

Element	Description
Name	Type a unique name up to 60 characters.
Description	Type a short description up to 250 characters.
Apply	Click to submit this Custom Authentication module.

Steps

Steps section identifies the specific plug-ins to use, and their execution order based on the configuration details of each plug-in (including the user identity store to use).

The following table describes the elements in the Steps section of the Create Custom Authentication Module page:

Element	Description
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
✚	Click to add a new step using the Add new step dialog box.
✖	Select a row and click ✖ to remove the row from the table.
Detach	Click to expand the table to a full page.
Step Name	Displays the added Step Name.
Description	Displays the description added for the Step Name.
Plug-in Name	Displays the added Plug-in Name.
Step Details	Details are displayed depending on the chosen plug-in and its requirements. Plug-in configuration details must be specified to ensure proper operation.
Save	Click **Save** to save the changes.
Cancel	Click **Cancel** to cancel the changes.
Apply	Click **Apply** to submit this Custom Authentication Module.

Add new step dialog box

The following table describes the elements in the Step Details section of the Create Custom Authentication Module page:

Element	Description
Step Name	Type a unique name to identify this step, you can enter up to 60 characters.
Description	Type a short description for this step, you can enter up to 250 characters.
Plug-in Name	Choose a Plug-in for a particular step from the list of imported and activated plug-ins.

Steps Orchestration

Step Orchestration section specifies the action to be taken on success or on failure or on error.

The following table describes the elements in the Steps Orchestration section of the Create Custom Authentication Module page:

Element	Description
Initial Step	Choose the starting step from those listed. The list includes only those steps defined for this module.
Name	Each step added to this module is listed by the name that was entered when the step was added.
Description	The description for this step, entered when this step was added.
On Success	The action selected for successful operation, you can choose from the drop-down list: • **Success** • **Failure** • **StepName** (activates the next step)
On Failure	The action selected for failure of this step, you can choose from the drop-down list: • **Success** • **Failure** • **StepName** (activates the next step)
On Error	The action selected for an error when executing this step, you can choose from the drop-down list: • **Success** • **Failure** • **StepName** (activates the next step)
Apply	Click **Apply** to submit the Custom Authentication Module.

Related Topics

Managing Authentication and Shared Policy Components in *Administrator's Guide for Oracle Access Management*.

6.5 Authentication Modules

Search Authentication Modules

Use the Search Authentication Modules page to perform an advanced search for a specific Authentication Module.

The following table describes the elements in the Search section of the Authentication Module page:

Element	Description
Name	Enter a name of the Authentication Module.

Element	Description
Type	Select a type from the drop-down menu: • **All** • **Authentication Module** • **Authentication Plug-in**
Search	Click **Search** to initiate the search and populate results in the Search Results table.
Reset	Click **Reset** to reset the search criteria.
Create Authentication Module	From the drop-down select the desired option to create a new Authentication Module.

Search Results

The following table describes the elements in the Search Results section of the Authentication Modules page:

Element	Description
Actions	Choose options from the menu to perform the following operations: • **Create** - Select Create to create a new Authentication module using the **Custom Authentication Module** page. • **Duplicate** - Select a row in the table and choose **Duplicate** to open the existing record in edit mode, user can make changes and save the record. • **Edit** - Select a row in the table and choose **Edit** to open the record in edit mode. After edit, click **OK** to save the changes or **Cancel** to cancel the changes. • **Delete** - Select a row in the table and choose **Delete**, in the confirm pop-up click **Yes** to remove the row or click **No** to retain the row.
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Create	From the drop-down select the desired option to create a new Authentication Module.
Duplicate	Select a row in the table and choose**Duplicate** to open the existing record in edit mode, user can make changes and save the record.
Edit	Select a row in the table and click **Edit** to open the record in edit mode. After edit, click **OK** to save the changes or **Cancel** to cancel the changes.
Delete	Select a row in the table and click **Delete**, in the confirm pop-up click **Yes** to remove the row or click **No** to retain the row.
Detach	Click to expand the Search Results table to a full page.
Name	Displays the searched Authentication Module name.
Type	Displays the type of the Authentication module.
▲	Click to sort the items in the column in ascending order.

Element	Description
▼	Click to sort the items in the column in descending order.

Related Topics

Managing Authentication and Shared Policy Components in *Administrator's Guide for Oracle Access Management*.

6.6 Authentication Plug-ins

The plug-ins created must be deployed on the AdminServer as a JAR file and will be validated automatically. After validation, an Administrator can configure and distribute the plug-in using Oracle Access Management Console. The server processes the XML configuration file within the plug-in JAR file to extract data about the plug-in. After the plug-in is imported, an Administrator can see and modify the various plug-in states based on information available from the AdminServer.

Plug-ins

The Plug-ins page includes a tool bar with command buttons, most of which operate on the plug-in that is selected in the table. The following table provides information about the existing custom plug-ins and their state.

Element	Description
View	Choose commands from the menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns. • **Query By Example** - Click to show or hide the filter row that is displayed above the column headers to query on the columns.

Element	Description
Import Plug-in	Adds the plug-in JAR file to the AdminServer $DOMAIN_HOME/oam/plugins and begins plug-in validation: • **Same JAR Name**—If the new plug-in JAR name (in $DOMAIN_HOME/oam/plugins) matches an existing plug-in JAR name (in $DOMAIN_HOME/config/fmwconfig/oam/plugins), Oracle Access Manager extracts new configuration metadata from the XML file in the JAR (in $DOMAIN_HOME/oam/plugins) and checks the version of the new plug-in. • **XML Version**— If the new plug-in XML version (in $DOMAIN_HOME/oam/plugins) is greater than the existing XML version (in $DOMAIN_HOME/config/fmwconfig/oam/plugins), validation is successful. Otherwise, "invalid plugin name with invalid version" is returned and the new plug-in JAR is removed (from $DOMAIN_HOME/oam/plugins). • **Different JAR Name**— If the new plug-in JAR name (in $DOMAIN_HOME/oam/plugins) is different then existing plug-in JAR names (in $DOMAIN_HOME/config/fmwconfig/oam/plugins), the new plug-in JAR is uploaded and validation is successful. **On Success**— Status is reported as "Uploaded" (even if an OAM Server is down). If all registered OAM Servers report “Uploaded”, then the status on AdminServer is also “Uploaded”. **On Failure**—Status is reported as “Upload Failed”.
Distribute Selected	• Propagates the plug-in to all registered OAM Servers. • Sets the plug-in flag in oam-config.xml to “Distribute=true". • Starts the distribution listener and notification mechanism between AdminServer and OAM Servers. • Distributes the plug-in JAR from AdminServer node to each OAM Server node under $DOMAIN_HOME/config/fmwconfig/oam/plugins. **On Success** — Status is reported as “Distributed" (even if an OAM Server is down). If all registered OAM Servers report “Distributed", then the status on AdminServer is also “Distributed". **On Failure** — Status is reported as “Distribution Failed".
Activate Selected	After successful distribution the plug-in can be activated on all registered OAM Servers. Activation: • Updates the plug-in flag in oam-config.xml to “Activate=true". • Starts the message listener and notification mechanism between AdminServer and OAM Servers. • AdminServer sends message “Activate" to all registered OAM Servers. **On Success** — Status is reported as “Activated” (even if an OAM Server is down). If all registered OAM Servers report “Activated", then the status on AdminServer is laso “Activated”. **On Failure** — Status is reported as “Activation Failed”. Following activation on all OAM Servers, the plug-in can be used and executed in any authentictaion module construction or orchestration.

Element	Description
Deactivate Selected	Following plug-in activation, an Administrator can choose to deactivate the plug-in, if the plug-in is not used in any authentication module or scheme. Deactivate: • Updates the plug-in flag in oam-config.xml to "De-activate=true". • Starts the Distribution listener and notification mechanism between AdminServer and OAM Servers. • Removes the plug-in JAR from AdminServer and each registered OAM Server ($DOMAIN_HOME/config/fmwconfig/oam/plugins). • AdminServer sends message "De-activation" to all registered OAM Servers. • OAM Servers sends status message to AdminServer using the "Message" listeners on both AdminServer and OAM Server. **On Success**— Status is reported as "De-activation" (even if an OAM Server is down). If all registered OAM Servers report "De-activation", then the status on AdminServer is also "De-activation". Plug-in configuration is removed from oam-config.xml. **Note:** After deactivation, the plug-in cannot be used or executed in any authentication module or orchestration. **On Failure**—Status is reported as "De-activation Failed".
Remove Selected	Following plug-in deactivation, an Administrator can delete the selected plug-in. During this process, Access Manager: Delete: • Updates the plug-in flag in oam-config.xml to "Remove=true". • Starts the Distribution listener and notification mechanism between AdminServer and OAM Servers. • Removes the plug-in JAR from AdminServer and each registered OAM Server ($DOMAIN_HOME/config/fmwconfig/oam/plugins). • AdminServer sends message "Activate" to all registered OAM Servers. **On Success**— Status is reported as "Removed" (even if an OAM Server is down). If all registered OAM Servers report "Removed", then the status on AdminServer is also "Removed". Plug-in configuration is removed from oam-config.xml. **On Failure**—Status is reported as "Removal Failed".
⟳	Click to update the screen with any changes made on the (back-end) server.
▼	Click to show or hide the filter row that is displayed above the column headers to query on the columns.
✎	Click to clear all entries in the filter row.
Row	Displays the row number.
Plug-in Name	Extracted from the Plugin name element of the XML metadat file.
Description	Extracted from the description element of the XML metadata file.
Activation Status	Reported activation status based on information from AdminServer.
Type	Extracted from the type element of the XML metadata file.
Last updated On	Extracted from the creation date element of the XML metadata file.
Last updated by	Extracted from the author element of the XML metadata file.
Total Rows	Total number of rows in the table.

Plug-in Details

Plug-in Details section reflects configuration details for the selected plug-in the table. The following table describes the elements in the Plug-in Details section of the Authentication Plug-ins page.

Element	Description
Configuration Parameters	Depending on your Plug-in selection, various configuration details are extracted from the configuration element of the XML metadata file to populate Configuration Parameters.
Save	Click **Save** to save your changes to the configuration parameters.
Activation Status	The Activation Status is maintained by the AdminServer.

Related Topics

Managing Authentication and Shared Policy Components in *Administrator's Guide for Oracle Access Management*.

Part II

Federation Help

This part contains online help for the console sections on the Federation Launch Pad.

- Federation Help

7 Federation Help

Identity Federation enables organizations to securely link accounts and identities across security boundaries without a central user repository or the need to synchronize data stores. It provides an interoperable way to implement cross-domain single sign-on without the overhead of managing, maintaining, and administering their identities and credentials.

The following topics are covered:

- Create Service Provider Partner
- Create SP Partner Attribute Profile
- Create Identity Provider Partner
- Create IDP Partner Attribute Profile
- Identity Provider Administration
- Service Provider Administration

7.1 Create Service Provider Partner

Use the Create Service Provider Partner page to define a partner profile when Identity Federation is configured as an Identity Provider (IdP). You can specify service details manually or load them from a metadata file.

General

Following table describes elements in the General section of the Create Service Provider Partner page:

Element	Description
Name	Type a provider name.
Enable Partner	Select whether this partner is currently participating in the federation.
Description	Type a short description that will help you or another Administrator identify this provider in the future.

Service Information

Following table describes elements in the Service Information section of the Create Service Provider Partner page:

Element	Description
Protocol	Choose from the following menu options in the drop-down: • **SAML 1.1** • **SAML 2.0** • **OpenID 2.0**

Element	Description
Service Details	Select any of the following: - **Load from Provider Metadata** - You can specify service details by loading an XML metadata file. - **Enter Manually**- You can specify service details by entering values manually. Applies to SAML 2.0 only.
Metadata File	Click **Browse** and select a file to use. This field appears only if **Load from Provider Metadata** option is selected. Applies to SAML 2.0 only.
Provider ID	The Provider ID of the remote Service Provider. Applies to SAML 2.0 and SAML 1.1 only.
Assertion Consumer URL	Type the URL to which Assertion responses will be sent. Applies to SAML 2.0 and SAML 1.1 only.
Load Signing Certificate	Click **Browse** and select a file to upload the signing certificate used by this SP. Only visible when **Enter Manually** is selected. Applies to SAML 2.0 and SAML 1.1 only.
Logout Request URL	Type the URL to which logout requests will be sent. Applies to SAML 2.0 only.
Logout Response URL	Type the URL to which responses to logout requests will be sent. Applies to SAML 2.0 only.
Load Encryption Certificate	Click **Browse** and select a file to upload the encryption certificate used by this SP. Only visible when **Enter Manually** is selected. Applies to SAML 2.0 only.
Realm	This is the URL identifying an OpenID SP. Applies to OpenID 2.0 only.
Endpoint URL	Type the URL to which the IdP will redirect the user with the OpenID Assertion. Applies to OpenID 2.0 only.

NameID Format

Following table describes the elements in the NameID Format section of the Create Service Provider Partner page:

Element	Description
NameID Format	Indicates which NameID format should be used for this SP. Applies to SAML 2.0 and SAML 1.1 only.
Custom NameID Format URI	Only visible when **Custom** option is selected from the **NameID Format** menu. Applies to SAML 2.0 and SAML 1.1 only.
NameID Value	Indicates how to populate the NameID value. - If **User ID Store Attribute** is selected, specify the user attribute to be used. - If **Expression** is selected, enter the expression to be used.

Mapping Options

Following table describes elements in the Mapping Options section of the Create Service Provider Partner page:

Element	Description
Attribute Profile	Indicates the attribute mapping profile to which the partner is bound. Click the search icon to open a Search window from which you can search for one or more previously configured Attribute Profiles. Select the profile and click **OK** to select or click **Cancel** to cancel the selection.
Save	Click **Save** to create the remote SP partner profile.

Related Topics

Managing Identity Federation Partners in *Administrator's Guide for Oracle Access Management*.

7.2 Create SP Partner Attribute Profile

Create SP Partner Attribute Profile page is used to define which message attributes map to which Access Manager Session Attributes.

General

Following table describes elements in the General section of the Create SP Partner Attribute Profile page:

Element	Description
Name	Type a SP Partner Attribute Profile Name.
Description	Type a short description that will help you or another Administrator identify this partner in the future.
Default SP Partner Attribute Profile	The `sp-attribute-profile` is the default Attribute Mapping Profile. Select to use the default attribute Profile.

Attribute Mapping

The following table describes the elements in the Attribute Mapping section of the Create SP Partner Attribute Profile page:

Element	Description
Actions	Choose from the following options: • **Create**- Select to create a new Partner Attribute Profile using the Create Attribute Mapping dialog box. • **Edit** - Select a row in the table and choose **Edit** to open the Attribute Mapping dialog box.After edit, click **OK** to save the changes, or **Cancel** to cancel the changes. • **Delete** - To delete a row from the table, select the row and choose **Delete**.

Element	Description
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Create	Click to create a new Partner Attribute Profile using the Create Attribute Mapping dialog box.
Edit	Select a row in the table and click **Edit** to open the Attribute Mapping dialog box. After edit, click **OK** to save the changes, or **Cancel** to cancel the changes.
Delete	To delete a row from the table, select the row and click on **Delete**.
Detach	Click to open the table in a larger window.
Row	Displays the row number.
Message Attribute Name	Lists the added Message Attribute Names.
Value	Lists the added values for the Message Attributes.
Always Send	Displays **true** if selected and **false** if not selected.
Number of Rows	Displays the number of rows in the table.
Save	Click **Save** to create SP Partner Attribute Profile.

Create Attribute Mapping dialog box

The following table describes the elements in the Attribute Mapping dialog box of the Attribute Mapping section:

Element	Description
Message Attribute Name	This is the name for the attribute in the incoming/outgoing Federation messages.
Value	This is the response expression, set as a variable. The following variable types are to enable single sign-on: • **Request**- Information on the requested resource, the client making the request, and the policy matched during evaluation. • **Session**- User session details. • **User**- User details (user ID, group, and attribute information). **Note**: More than one message attribute can have the same value expression.
Always Send	Indicates if the attribute should be sent even when it has not been specifically requested. If selected, the attribute has to be included in an outgoing Assertion irrespective of whether it has been requested. If not selected, the attribute will not be included in the Assertion unless requested.
OK	Click **OK** to populate the created data in Attribute Mapping table.
Cancel	Click **Cancel** to cancel the changes made in the window.

Element	Description
✕	Click to close the window.

Related Topics

Managing Identity Federation Partners in *Administrator's Guide for Oracle Access Management*.

7.3 Create Identity Provider Partner

Create Identity Provider Pattern page is used to define an identity provider (IdP) partner record for Access Manager. You can specify service details manually or load them from a metadata file.

General

Following table describes the elements in General section of the Create Identity Provider Partner page:

Element	Description
Name	Type a Provider Name.
Description	Type a short description that will help you or another Administrator identify this provider in the future.
Enable Partner	Select whether this partner is currently participating in the federation.
Default Identity Provider Partner	Select to use the default Provider Partner.

Service Information

Following table describes the elements in the Service Information section of the Create Identity Provider Partner page:

Element	Description
Protocol	Choose from the following menu options in the drop-down: • **SAML 1.1** • **SAML 2.0** • **OpenID 2.0**
Provider ID	This is the Provider ID of the provider. Applies to SAML 1.1 and SAML 2.0 only.
Succinct ID	This is the succinct ID of the provider. This element is required if using the artifact profile. Applies to SAML 1.1 and SAML 2.0 only.
SSO Service URL	This is the URL address to which the SSO requests are sent. Applies to SAML 1.1 and SAML 2.0 only.
SOAP Service URL	This is the URL address to which SOAP service request is sent. This element is required if using artifact profile. Applies to SAML 1.1 and SAML 2.0 only.

Element	Description
Load Signing Certificate	Upload the signing certificate. Click on Browse and select the file that needs to be uploaded. You can specify it in `pem` and `der` formats. Applies to SAML 1.1 and SAML 2.0 only.
Service Details	Choose from the following options: • **Load from provider metadata**- You can specify service details by loading an XML metadata file. • **Enter Manually**- You can specify service details by entering values manually. Applies to SAML 2.0 only.
Metadata File	Click **Browse** and select a file to use. This field appears only if **Load from Provider Metadata** option is selected. Applies to SAML 2.0 only.
Logout Request Service URL	This is the URL to which logout requests are sent. Applies to SAML 2.0 only.
Logout Response URL	This is the URL to which responses to logout requests are sent. Applies to SAML 2.0 only.
Load Encryption Certificate	Click **Browse** and select a file to upload the Encryption certificate. Only visible when **Enter Manually** is selected. Applies to SAML 2.0 only.
Service Details	Select an option from the drop-down menu. Indicates which of the following options Identity Federation (the RP) uses to perform Federation SSO with the Idp. • By discovering the Idp SSO URLs via the Idp XRDS metadata available at the Discovery Service URL. • By using the specified static OpenID login endpoint which is the IDP SSO service URL. Applies to OpenID 2.0 only.
Discovery URL	Defines the location where the IdP publishes its XRDS metadata. Applies to OpenID 2.0 only.
Endpoint URL	Defines the Idp SSO Service location. Applies to OpenID 2.0 only.

Mapping Options

This setting indicates how an incoming assertion is mapped to a user in the identity store. The following table describes the elements in the User Mapping section of the Create Identity Provider Partner page:

Element	Description
User Identity Store	Choose an option from the drop-down menu. This is the identity store in which the IdP's users will be located and mapped. Identity Federation supports multiple identity stores, defined on a per-partner basis. Optionally, if no user identity is selected, the default Access Manager store is used.
User Search Base DN	This is the base search DN used when looking up user records. If omitted, the default user search base DN configured for the selected user identity store is used.

Element	Description
Map assertion Name ID to User ID Store attribute	This setting indicates how an incoming assertion is mapped to a user in the identity store. Choose this option to indicate a map assertion Name ID to User ID store attribute.
Map assertion Name ID to User ID Store attribute	Enter the identity store attribute to which the assertion NameID will be mapped.
Map assertion attribute to User ID Store attribute	This setting indicates how an incoming assertion is mapped to a user in the identity store. Choose this option to indicate a map assertion attribute to User ID store attribute.
Assertion Attribute	Enter assertion attribute to which it will be mapped.
User ID Store Attribute	Enter Identity Store Attribute to which it will be mapped.
Map assertion to user record using LDAP query	This setting indicates how an incoming assertion is mapped to a user in the identity store. Choose this option to indicate a map assertion to user record using LDAP query.
LDAP Query	Enter an LDAP query with placeholders for incoming data. You may use any of the following: • An attribute from the SAML assertions `Attribute Statement` element, referenced by its name prefixed and suffixed with the % character. • The SAML assertion subject's `NameID` referenced by `%fed.nameidvalue%`. • The identity provider's partner name, referenced by `%fed.partner%`. For example, an LDAP query to map an incoming assertion based on two assertion attributes (lastname and email) would be `(&(sn=%lastname%)(mail=%email%))`.

Attribute Mapping

Following table describes the elements in the Attribute Mapping section of the Create Identity Provider Partner page:

Element	Description
Attribute Profile	Indicates the attribute mapping profile to which the partner is bound. Click the search icon to open a Search window from which you can search for one or more previously configured Attribute Profiles. Select the profile and click **OK** to select, or click **Cancel** to cancel the selection.
Save	Click **Save** to create the identity provider definition.

Related Topics

Managing Identity Federation Partners in *Administrator's Guide for Oracle Access Management*.

7.4 Create IDP Partner Attribute Profile

Create IDP Partner Attribute Profile page is used to allow the administrator to define which attributes map to which Access Manager session attributes.

General

Following tale describes the elements in the General section of the Create IDP Partner Attribute Profile page:

Element	Description
Name	Type a Partner Name.
Description	Type a short description that will help you or another Administrator identify this partner in the future.
Ignore Unmapped Attribute	Indicates how to deal with Assertion Attributes not present or that are present but have no value in the Access Manager Session Attribute column. • If selected, any Assertion Attribute not present in the table or with no value mapped to Access Manager will be ignored and not added to the Access Manager session. • If not selected, all Assertion Attribute that are not present in the table or don't have a value mapped to Access Manager will be stored in the Access Manager session with the same attribute name it had in the Assertion.
Default IDP Partner Attribute Profile	The`idp-attribute-profile` is the default Attribute Mapping Profile. Select to use the default attribute profile.

Attribute Mapping

Following table describes elements in the Attribute Mapping section of the Create IDP Partner Attribute Profile page:

Element	Description
Actions	Choose from the following options: • **Create** - Click to create a new Partner Attribute Profile using the Create Attribute Mapping dialog box. • **Edit** - Select a row in the table and choose **Edit** to open the Attribute Mapping dialog box. After edit, click **Ok** to save the changes or **Cancel** to cancel the changes. • **Delete** - To delete a row from the table, select the row and choose **Delete**.
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Create	Click to create a new Partner Attribute Profile using the Create Attribute Mapping dialog box.
Edit	Select a row in the table and click **Edit** to open the Attribute Mapping dialog box. After edit, click **OK** to save the changes, or **Cancel** to cancel the changes.
Delete	To delete a row from the table, select the row and click on **Delete**.
Detach	Click to open the table in a larger window.
Row	Displays the row number.

Element	Description
Message Attribute Name	Lists the added Message Attribute Names.
OAM Session Attribute Name	Lists the added OAM Session Attribute Names.
Request Form Partner	Displays **true** if selected or **false** if not selected.
Number of Rows	Displays the number of rows in the table.
Save	Click **Save** to save the changes made to the page.

Create Attribute Mapping dialog box

The following table describes the elements in the Attribute Mapping dialog box of the Attribute Mapping section:

Element	Description
Message Attribute Name	This is the name for the attribute in the incoming/outgoing Federation messages.
OAM Session Attribute Name	This is the name by which the attributes is known to the local Access Manager server.
Request Form Partner	If selected, it indicates if this attribute is sent in the Request made to the IdP (a value for this attribute is requested by the SP).
OK	Click **OK** to populate the created data in Attribute Mapping table.
Cancel	Click **Cancel** to cancel the changes made in the window.
✕	Click to close the window.

Related Topics

Managing Identity Federation Partners in *Administrator's Guide for Oracle Access Management*

7.5 Identity Provider Administration

Use the Identity Provider Administration page to manage an existing IdP for Identity Federation.

Search Service Provider Partners

Use the Search section of the Service Provider partner page to perform an advanced search for specific sessions. User can create query based on filter conditions and add fields to the query to further refine the search. The following table describes the elements in the Search area of the Search Service Provider Partners page:

Element	Description
Partner Name	Searches for a specific partner name.
Provider ID	Searches by provider ID.
Status	Searches providers matching a status.

Element	Description
Protocol	Searches for providers that use a specified protocol.
Description	Searches by provider description.
Search	Click Search to display search results in the table.
Reset	Click Reset to reset the search criteria.
Create Service Provider Partner	Click **Create Service Provider Partner**: Use the Create Service Provider Partner page to create a new service provider partner.

Search Results

Search results returned are the service provider partner that met the conditions specified in the search fields. The following table describes the elements in the Search Results section of the Search Service Provider Partners page:

Element	Description
Actions	Choose from the following options: • **Create**- Select **Create** to create a new service provider partner. • **Edit** - Select a row in the table and choose **Edit** to open the record in edit mode. After edit, click **Ok** to save the changes, or **Cancel** to cancel the changes. • **Delete** - To delete a row from the table, select the row and choose **Delete**.
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Create	Click **Create**. Use the **Create Service Provider Partner** page to create a new service provider partner.
Duplicate	Click to create a copy of the existing record. Select a row and click **Duplicate** to open the existing record in edit mode. User can make changes and save the record.
Edit	Select a row in the table and click **Edit** to open the record in edit mode. After edit, click **OK** to save the changes, or **Cancel** to cancel the changes.
Delete	Select a row in the table and click **Delete**. In the confirm pop-up click **Yes** to remove the row, or click **No** to retain the row.
Detach	Click to open the table in a larger window.
Row	Displays the Row number.
Partner Name	Displays the searched Partner Name.
Status	Displays the searched Status.
Provider ID	Displays the searched Provider ID.
Protocol	Displays the searched Protocol.
Description	Displays the searched provider description.

Element	Description
Number of Rows	Displays the number of rows in the table.
▲	Click to sort the items in the column in ascending order.
▼	Click to sort the items in the column in descending order.

Search Service Provider Attribute Profiles

Use the Search section of the Service Provider Attribute Profiles to perform an advanced search for specific sessions. User can create query based on filter conditions and add fields to the query to further refine the search. The following table describes the elements in the Search area of the Service Provider Attribute Profiles page:

Element	Description
Name	Search by SP Attribute Profile Name.
Description	Search by SP Attribute Description.
Search	Click Search to populate Search results in the table.
Reset	Click Reset to reset the Search criteria.
Create SP Attribute Profile	Click **Create SP Attribute Profile**. Use the Create SP Partner Attribute Profile page to create a new partner attribute profile.

Search Results

Search results returned are the partner attribute profile that met the conditions specified in the search fields. The following table describes the elements in the Search Results section of the Service Provider Attribute Profiles page:

Element	Description
Actions	Choose from the following options: • **Create** - Select **Create** to create a new partner attribute profile. • **Edit** - Select a row in the table and choose **Edit** to open the record in edit mode. After edit, click **OK** to save the changes or **Cancel** to cancel the changes. • **Delete** - To delete a row from the table, select the row and choose **Delete**.
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Create	Click **Create**. Use the **Create SP Partner Attribute Profile** page to create a new partner attribute profile.

Element	Description
Duplicate	Click to create a copy of the existing record. Select a row and click **Duplicate** to open the existing record in edit mode. User can make changes and save the record.
Edit	Select a row in the table and click **Edit** to open the record in edit mode. After edit, click **OK** to save the changes, or **Cancel** to cancel the changes.
Delete	Select a row in the table and click **Delete**. In the confirm pop-up click **Yes** to remove the row, or click **No** to retain the row.
Detach	Click to open the table in a larger window.
Row	Displays the row number.
Name	Displays the searched Attribute Profile Name.
Description	Displays the searched Attribute Profile description.
Number of Rows	Displays the number of rows in the table.

Related Topics

Managing Identity Federation Partners in *Administrator's Guide for Oracle Access Management*.

7.6 Service Provider Administration

Use the Service Provider Administration page to edit and manage the profiles of remote SP partners, search for the profile and make changes to the attribute values.

Search Identity Provider Partners

Use the Search section of the Identity Provider partner page to perform an advanced search for specific sessions. User can create query based on filter conditions and add fields to the query to further refine the search. The following table describes the elements in the Search area of the Identity Provider Partners tab:

Element	Description
Partner Name	Searches for a specific partner name.
Provider ID	Searches by provider ID.
Status	Searches providers matching a status.
Protocol	Searches for providers that use a specified protocol.
Description	Searches by provider description.
Search	Click **Search** to display search results in the table.
Reset	Click **Reset** to reset the search criteria.
Create Identity Provider Partner	Click **Create Identity Provider Partner**. Use the Create Identity Provider Partner page to create a new provider partner.

Search Results

Search results are the provider partner that met the conditions specified in the search fields. The following table describes the elements in the Search Results section of the Identity Provider partner page:

Element	Description
Actions	Choose from the following options: • **Create** - Select **Create**to create a new provider partner. • **Edit**- Select a row in the table and choose **Edit**to open the record in edit mode. After edit, click **Ok** to save the changes, or **Cancel**to cancel the changes. • **Delete** - To delete a row from the table, select the row and choose **Delete**.
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Create	Click **Create**. Use the Create Identity Provider Partner page to create a new provider partner.
Duplicate	Click to create a copy of the existing record. Select a row and click **Duplicate** to open the existing record in edit mode. User can make changes and save the record.
Edit	Select a row in the table and click **Edit** to open the record in edit mode. After edit, click **OK** to save the changes or **Cancel** to cancel the changes.
Delete	Select a row in the table and click **Delete**. In the confirm pop-up click **Yes** to remove the row or click **No** to retain the row.
Detach	Click to open the table in a larger window.
Row	Displays the row number.
Partner Name	Displays the searched Partner Name.
Status	Displays the searched Status.
Provider ID	Displays the searched Provider ID.
Protocol	Displays the searched Protocol.
Description	Displays the searched provider description.
Number of Rows	Displays the number of rows in the table.
▲	Click to sort the items in the column in ascending order.
▼	Click to sort the items in the column in descending order.

Search Identity Provider Attribute Profiles

Use the Search section of the Identity Provider attribute profile page to perform an advanced search for specific sessions. User can create query based on filter conditions and add fields to the query to further refine the search. The following table describes the elements in the Search area of the Identity Provider Attribute Profiles page:

Element	Description
Name	Searches for a specific Provider Name.
Description	Searches by Provider Description.
Search	Click **Search** to display search results in the table.
Reset	Click**Reset** to reset the search criteria.
Create IDP Attribute Profile	Click **Create IDP Attribute Profile**. Use the Create IDP Partner Attribute Profile page to create a new partner attribute profile.

Search Results

The following table describes the elements in the Search Results section of the Identity Provider Attribute Profiles tab:

Element	Description
Actions	Choose from the following options: • **Create** - Select **Create** to create a new partner attribute profile. • **Edit** - Select a row in the table and choose **Edit** to open the record in edit mode. After edit, click **OK** to save the changes or **Cancel** to cancel the changes. • **Delete** - To delete a row from the table, select the row and choose **Delete**.
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Create	Click **Create.** Use the Create IDP Partner Attribute Profile page to create a new partner attribute profile.
Duplicate	Click to create a copy of the existing record. Select a row and click **Duplicate** to open the existing record in edit mode. User can make changes and save the record.
Edit	Select a row in the table and click **Edit** to open the record in edit mode. After edit, click **OK** to save the changes or **Cancel** to cancel the changes.
Delete	Select a row in the table and click **Delete**. In the confirm pop-up click **Yes** to remove the row or click **No** to retain the row.
Detach	Click to open the table in a larger window.
Row	Displays the Row number.
Name	Lists the Provider name.
Description	Lists the Provider description.
Number of Rows	Lists the total number of rows in the table.

Related Topics

Managing Identity Federation Partners in *Administrator's Guide for Oracle Access Management*

Part III
Configuration Help

This part contains online help for the console sections on the Configuration Launch Pad.

8

Available Services Help

The Available Services page provides the status of services, and controls to enable or disable a service. It provides the user with configuration options. The page is arranged in the following sections:

- Available Services

8.1 Available Services

The Available Service page displays the Configuration options.

Enabling or Disabling Available Services

The following table describes the Enabling or Disabling Available Services elements of the Available Services page:

Element	Description
Enable Service	Click **Enable Service** beside the desired service name and confirm that the Status check mark is green ✅
Disable Service	Click **Disable Service** beside the desired service name and confirm that the status check mark is red ❌
✅	Indicates that the corresponding service is enabled.
❌	Indicates that the corresponding service is disabled.

Application Security

The following table describes the elements in the Application Security section of the Available Services page:

Element	Description
Access Manager	Access Manager functionality is enabled by default. Access Manager Service is required to set SSO policies, configure Access Manager, as well as Common Configuration, and when REST Services are enabled. **Default:** Enabled.

Element	Description
Adaptive Authentication Service	Required for adaptive authentication functionality. **Default:** Enabled.
OAuth Service	OAuth enables a third-party application to obtain limited access to resources from web, mobile and desktop applications based on standard tokens. **Default:** Disabled.

Federation

The following table describes the elements in the Federation section of the Available Services page:

Element	Description
Identity Federation	Must be enabled to manage the federation partners. **Default:** Disabled. **Note:** The Access Manager service must also be enabled because Identity Federation is another authentication module.
Access Portal Service	Must be enabled to manage the Access Portal Service. **Note:** By default, the Enable Services button will be disabled. The service cannot be enabled until the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files are available. **Default:** Disabled.

Related Topics

Managing Common Services and Certificate Validation in *Administrator's Guide for Oracle Access Management*

9

User Identity Stores Help

User Identity Store is a centralized LDAP repository in which an aggregation of Administrator and user-oriented data is stored and maintained in an organized way. Use this page to register and manage user identity store.

The User Identity Stores page is arranged in the following sections:

- User Identity Stores
- Create User Identity Store

9.1 User Identity Stores

Default and System Store

The following table describes the elements in the Default and System Store section of the User Identity Stores page:

Element	Description
Default Store	Select a default store from the drop-down menu. It is the automatic choice for use by LDAP authentication modules unless you configure use of a different store for the module or plug-in.
System Store	Select a system store from the drop-down menu. Only one User Identity Store can be designated as the System Store. This is used to authenticate Administrators signing in to use the Oracle Access Management Console, remote registration tools, and custom administrative commands in WLST.
Apply	Click **Apply** to submit the changes.

Access System Administrators

This table appears only while changing System Store. All Administrator roles, users, and groups must be stored in the System Store. If the System Store changes, appropriate Administrator roles must be added to the new System Store.

The following table describes the elements in the Access System Administrators section of the User Identity Stores page:

Element	Description
Name	Displays the name added using Add System Administrators Roles dialog box.
Type	Displays the type of the added name.
▲	Click to sort the items in the column in ascending order.
▼	Click to sort the items in the column in descending order.
Add	Click to open Add System Administrators Roles dialog box.

Element	Description
Delete	Select a row in the table and click **Delete** to remove the row.

Add System Administrators Roles dialog box

Click Add button in Access System Administrators section to open this dialog box.

Search

In this section, user can search the System Store to find configured administrators.

The following table describes the elements in the Add System Administrator Roles dialog box of the Access System Administrators section:

Element	Description
Name	Type a name that needs to be searched.
Type	Select a Type from the list.
Search	Click **Search** to initiate the search and populate results in the search results table.
Reset	Click **Reset** to reset the search criteria.

Search Results

This section lists the records matching the search criteria.

The following table describes the elements in the Add System Administrator Roles dialog box of the Access System Administrators section:

Element	Description
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Detach	Click to expand the table to a full page.
Name	Displays the searched names.
Type	Displays the Type of the searched names.
Add selected	Select the desired user from the table, then click **Add Selected** to add the selected rows to **Access System Administrators** table.
Cancel	Click **Cancel** to cancel your selections.
✕	Click to close the dialog box.

OAM ID Stores

The following table describes the elements in the OAM ID Stores section of the User Identity Stores page:

Element	Description
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Create	Click to create a new user identity store using the Create User Identity Store page.
Duplicate	Click to create a copy of the existing record. Select a row and click **Duplicate** to open the existing record in edit mode, user can make changes and save the record.
Edit	Select a row in the table and click **Edit** to open the record in edit mode. Modify values as needed and click **Apply** to update the registration or close the tab without applying changes.
Delete	Select a row in the table and click **Delete**, in the confirm pop-up click **Delete** to remove the row or click **Cancel** to retain the row.
Name	Lists all the created Store Names.
Directory Type	Lists the type of directory server software hosting the repository. If the type is not selected, this field will be empty.
Host Information	Lists the information about the host computer on which the Identity Directory Service Repository is located.
Description	Lists the description added while creating the Identity Store.
Synched IDS Profiles	Lists the IDS profiles that are synched.
▲	Click to sort the items in the column in ascending order.
▼	Click to sort the items in the column in descending order.
Sync IDS Profiles	Click to make common Identity Directory Service Profiles accessible to Oracle Access Management as local Identity Stores.

Identity Directory Service

Identity Directory Service is a common service used by Oracle Identity Management products to access and manage Identity Directory. The IDS Profiles can be used within Oracle Access Management after they are synchronized.

IDS Profiles

The following table describes the elements in the IDS Profiles section of the User Identity Stores page:

Element	Description
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Create	Click to create a new identity directory service profile using the Create Identity Store Profile page.
Edit	Select a row in the table and click **Edit** to open the record in edit mode. Modify values as needed and click **Apply** to update the registration or close the tab without applying changes.
Delete	Select a row in the table and click **Delete**, in the confirm pop-up click **Delete** to remove the row, or click **Cancel** to retain the row.
Name	Lists all the created User Profile Service Provider names.
Description	Lists all the descriptions added for the Service Provider names.
Repository Name	Lists all the Repository Names added for the Service Provider names.
Created By	Displays the name of the user who created the IDS profile.
▲	Click to sort the items in the column in ascending order.
▼	Click to sort the items in the column in descending order.

Create Identity Store Profile

Use this page to create an Identity Service Profile. Click **Create** under IDS Profiles section to access this page.

The following table describes the elements in the Create Identity Store Profile page:

Element	Description
Name	Type a unique name for this User Profile Service Provider.
Description	Type a short description that will help you or another Administrator identify this service in the future.

Repository

The following table describes the elements in the Repository section of the Create Identity Store Profile page:

Element	Description
Repository Options	Select any of the following options: • **Create New** - Defines a new Repository object for the Identity Directory Service connection. • **Use Existing** - Allows you to choose a previously defined Repository object selecting it from the drop down menu.

Element	Description
Name	Enter a unique name to create, or choose an existing one from the menu. After entering a new name, configure properties for the Identity Directory Service connection.
Directory Type	Select the type of directory server software hosting the Repository. **For Example:** Microsoft Active Directory or Oracle Internet Directory. If your directory is not listed, leave this field empty. **Note:** If you are not defining a new Identity Directory Service connection or creating a new repository, this field is read-only.
Hosts	Contains information about the host computer on which the Identity Directory Service Repository is located. Add multiple hosts if the directory server is part of a cluster.
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Add	Click to add a new host to the table.
Remove	Select a row in the table and click **Remove**to delete the row.
Host Name	Type either the IP address or the name of the computer on which the Directory server is running.
Port	Type the port number that the directory server is configured to use.
Load Distribution (%)	Type the load amount as a percentage that should be directed to each host. For multiple hosts, the amount should add up to 100%.
Availability	Choose from the following: • **Failover** - Choose if the cluster is configured for failover operation. • **Load balanced** - Choose if the cluster distributes the load across multiple hosts. **Note:** This field is read-only if you are using an existing repository.
SSL	Select **Enabled** if the connection is configured for SSL.
Bind DN	Type the distinguished name (DN) of the LDAP Administrator used to authenticate to the Directory server.
Bind Password	Type the Bind DN password used to authenticate to the Directory server.
Base DN	Type the base distinguished name (DN) where User and Group data is located.
Password Management	Select **Enabled** to enable password policy enforcement against attribute values. Refer Password Management for attribute values and to configure the corresponding options in the password policy.
Use Native ID Store Settings	This enables getting the authentication code for natively locked/disabled/ pw_must_change code in the LDAP authentication module.
Use Oblix User schema	Click to check this box to Enable the use of OBLIX schema instead of standard Oracle schema.
Create	Click to create this identity profile, the profile is displayed in the IDS Profiles table.
Cancel	Click to cancel this identity profile.
Test Connection	Click to confirm connectivity, then close the confirmation window.

Form-Fill Application IDS Profile

Use this page to create an Identity Directory Service Profile for a Form-fill Application, click the **Create Form-Fill Application IDS Profile** button on the left of the IDS Profile section to access this page.

This page is arranged in the following sections:

- Repository
- Entity Search Bases

The following table describes the elements in the Form-Fill Application IDS Profile page:

Element	Description
Name	Type a unique name for this User Profile Service Provider.
Description	Type a short description that will help you or another Administrator identify this service in the future.

Repository

The following table describes the elements in the Repository section of the Form-Fill Application IDS Profile page:

Element	Description
Repository Options	Select any of the following options: • **Create New** - Defines a new Repository object for the Identity Directory Service connection. • **Use Existing** - Allows you to choose a previously defined Repository object selecting it from the drop down menu.
Name	Enter a unique name to create, or choose an existing one from the menu. After entering a new name, configure properties for the Identity Directory Service connection.
Directory Type	Select the type of directory server software hosting the Repository. **For Example:** Microsoft Active Directory or Oracle Internet Directory. If your directory is not listed, leave this field empty. **Note:**If you are not defining a new Identity Directory Service connection or creating a new repository, this field is read-only.
Hosts	Contains information about the host computer on which the Identity Directory Service Repository is located. Add multiple hosts if the directory server is part of a cluster.
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Add	Click to add a new host to the table.
Remove	Select a row from the table and click **Remove** to delete the row.
Host Name	Type either the IP address or the name of the computer on which the Directory server is running.

Element	Description
Port	Type the port number that the directory server is configured to use.
Load Distribution (%)	Type the load amount as a percentage that should be directed to each host. For multiple hosts, the amount should add up to 100%.
Availability	Choose from the following: • **Failover** - Choose if the cluster is configured for failover operation. • **Load balanced** - Choose if the cluster distributes the load across multiple hosts. **Note:** This field is read-only if you are using an existing repository.
SSL	Select **Enabled** if the connection is configured for SSL.
Bind DN	Type the distinguished name (DN) of the LDAP Administrator used to authenticate to the Directory server.
Bind Password	Type the Bind DN password used to authenticate to the Directory server.
Base DN	Type the base distinguished name (DN) where User and Group data is located.
Password Management	Select **Enabled** to enable password policy enforcement against attribute values. Refer Password Management for attribute values and to configure the corresponding options in the password policy.
Use Native ID Store Settings	This enables getting the authentication code for natively locked/disabled/pw_must_change code in the LDAP authentication module.
Use Oblix User schema	Click to check this box to Enable the use of OBLIX schema instead of standard Oracle schema.

Entity Search Bases

The following table describes the elements in the Entity Search Bases section of the Form-Fill Application IDS Profile page:

Element	Description
User Base DN	Full DN for the node at which enterprise users are stored in the directory. **For Example:** cn=Users,realm_DN.
Group Base DN	Full DN for the node at which enterprise groups are stored in the directory. **For Example:** ou=demo.
Application Template Base DN	Full DN for the node from which searches for the Application Templates will begin.
Top Search Base DN	Full DN for the node from which searches will begin. **For Example:** cn=realm_DN.
Create	Click to create this identity profile, the profile is displayed in the IDS Profiles table.
Cancel	Click to cancel this identity profile.
Test Connection	Click to confirm connectivity, then close the confirmation window.

IDS Repositories Elements

The following table describes the elements in the IDS Repositories section of the User Identity Stores page:

Element	Description
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Create	Click to create a new IDS Repository using the Create IDS Repositories page.
Edit	Select a row in the table and click **Edit** to open the record in edit mode. Modify values as needed and click **Apply** to update the repository, or close the tab without applying changes.
Delete	Select a row in the table and click **Delete**, in the confirm pop-up click **Delete** to remove the row, or click **Cancel** to retain the row.
Name	Lists the created IDS Repository names.
Directory Type	Lists the Directory Type added for the Repositories.
Host Information	Lists the Host Information added.
▲	Click to sort the items in the column in ascending order.
▼	Click to sort the items in the column in descending order.

Create IDS Repositories/Create LDAP Repository

Use this page to create an Identity Directory Service Repository, click **Create** under IDS Repository to access this page.

The following table describes the elements in the Create IDS Repositories page:

Element	Description
Name	Type a unique name to create, or choose an existing one from the menu. After entering a new name, configure properties for the Identity Directory Service connection.
Directory Type	Select the type of directory server software hosting the Repository. **For example:** Microsoft Active Directory or Oracle Internet Directory. If your directory is not listed, leave this field empty. **Note:** If you are not defining a new Identity Directory Service connection or creating a new repository, this field is read-only.
Hosts	Contains information about the host computer on which the Identity Directory Service Repository is located. Add multiple hosts if the directory server is part of a cluster.
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Add	Click to add a new host to the table.

Element	Description
Remove	Select a row from the table and click **Remove** to delete the row.
Host Name	Type either the IP address or the name of the computer on which the Directory server is running.
Port	Type the port number that the directory server is configured to use.
Load Distribution (%)	Type the load amount as a percentage that should be directed to each host. For multiple hosts, the amount should add up to 100%.
Availability	Choose from the following: • **Failover** - Choose if the cluster is configured for failover operation. • **Load balanced** - Choose if the cluster distributes the load across multiple hosts. **Note:** This field is read-only if you are using an existing repository.
SSL	Select **Enabled** if the connection is configured for SSL.
Bind DN	Type the distinguished name (DN) of the LDAP Administrator used to authenticate to the Directory server.
Bind Password	Type the Bind DN password used to authenticate to the Directory server.
Base DN	Type the base distinguished name (DN) where User and Group data is located.
Password Management	Select **Enabled** to enable password policy enforcement against attribute values. Refer Password Management for attribute values and to configure the corresponding options in the password policy.
Use Native ID Store Settings	This enables getting the authentication code for natively locked/disabled/ pw_must_change code in the LDAP authentication module.
Use Oblix User Schema	Click to check this box to Enable the use of OBLIX schema instead of standard Oracle schema.
Test Connection	Click to confirm if the values are correct.
Create	Click to create this IDS Repository, the repository is displayed in the IDS Repositories table.
Cancel	Click to cancel this IDS Repository.

Related Topics

Managing Data Sources in *Administrator's Guide for Oracle Access Management*.

9.2 Create User Identity Store

This page provides fields where you enter details for your store and default settings that you can edit for your environment. Click **Create** under OAM ID Stores to access this page.

The Create User Identity Store page is arranged in the following sections:

- Location and Credentials
- Users and Groups
- Connection Details
- Password Management

The following table describes the elements in the Create User Identity Store page:

Element	Description
Store Name	Type a unique name for this registration, you can type up to 30 characters.
Store Type	Choose from the list of all supported LDAP providers.
Description	Type a short description for this Store Name.
Enable SSL	Select this box to enable SSL between the directory server and OAM Server.
Use Native ID Store Settings	Select this box to enable getting the authentication code for natively locked/ disabled/pw_must_changecode in the LDAP authentication module.
Prefetched Attributes	List of comma-separated user attributes. **For Example:** e-mail, phone, mobile. **Note:** • The OAM server will cache the list of user attributes in memory while it authenticates the user against the identity store.The cached values will be used to compute the Authentication policy conditions. • Pre-fetched attributes provide huge performance improvements by avoiding a round trip to the user identity store. The OAM Administrator has to make sure all the user attributes used in Authentication and Authorization policy response headers and Authorization conditions are defined as prefetched attributes in the user identity store profile.

Location and Credentials

The following table describes the elements in the Location and Credentials section of the Create User Identity Store page:

Element	Description
Location	Provide the URL for the LDAP host, including the port number. Enter one (or more) LDAP URIs in `host:port` format, Multiple URIs must be separated by a space or new line (Oracle Access Management supports multiple LDAP URIs with failover capability. The Identity Assertion Provider fails over to the next LDAP URL based on the order in which these appear). **Note:** The number of characters a supported URL can have is based on the browser version. Ensure that your applications do not use URIs that exceed the length that Oracle Access Management and the browser can handle.
Bind DN	Provide the user DN for the connection pool over which all other BINDs occur. Oracle recommends a non administrator user with appropriate Read and Search privileges for the user and group base DNs. **For Example:** `uid=amldapuser,ou=people,o=org`.
Password	Type a password for the Principal, this is encrypted for security.

Users and Groups

The following table describes the elements in the Users and Groups section of the Create User Identity Store page:

Element	Description
Login ID Attribute	Enter the attribute that identifies the login ID (user name). **For Example:**`uid`.

Element	Description
User Password Attribute	Enter the attribute in the user identity store (LDAP directory) which stores the user's password. This is made configurable for added flexibility.
User Search Base	Provide the node in the directory information tree (DIT) under which user data is stored, this is the highest possible base for all user data searches. **For example:** `ou=people,ou=myrealm,dc=base_domain`.
User Filter Object Classes	Enter the object classes to be included in search results for users, in a comma separated list of user object class names. **For example:** `user,person`.
Group Name Attribute	Enter the attribute that identifies the group name. **Default:** cn.
Group Search Base	Provide the node in the directory information tree (DIT) under which group data is stored, this is the highest possible base for all group data searches. **For Example:** `ou=groups,ou=myrealm, dc=base_doamin`.
Group Filter Classes	Enter the object classes to be included in the search results for groups, in a comma-separated list of group object classes. **For Example:** groups, groupOfNames.
Enable Group Membership Cache	Check this box to set the value for group cache to true. Do not check to set the value for group cache to false. **Default:**true.
Group Membership Cache Maximum Size	Enter a integer for the group cache size. **Default:**10000
Group Membership Cache Time to Live (in seconds)	Enter a integer (in seconds) for Time to Live for group cache elements. **Default:** 0

Connection Details

The following table describes the elements in the Connection Details section of the Create User Identity Store page:

Element	Description
Minimum Pool Size	Set the smallest size for the connection pool. **Default:** 10
Maximum Pool Size	Set the greatest size for the connection pool. **Default:** 50
Wait Timeout (in seconds)	Set the number (in seconds) that connection requests can wait before timing out in the event of a fully utilized pool. **Default:** 120
Inactivity Timeout (in seconds)	Set the number (in seconds) that connection requests can be inactive before timing out in the event of a fully utilized pool.
Results time limit (in seconds)	Set the time limit (in seconds) for LDAP searches and bind operations on the connection pool. **Default:** 0

Element	Description
Retry Count	Enter a integer to set the number of times the connection can be retried when there is a connection failure. **Default:** 3
Referral Policy	Choose from the following options in the drop-down menu: • **follow** - Follows referrals during an LDAP search (Default). • **ignore** - Ignores referral entries during an LDAP search. • **throw** - Results in a Referral Exception, which can be caught by the component user.

Password Management

The following table describes the elements in the Password Management section of the Create User Identity Store page:

Element	Description
Enable Password Management	Select to enable password policy enforcement against the attribute values. The corresponding options in the password policy must be configured as well.
Use Oblix User Schema	Select to enable the use of OBLIX schema instead of standard Oracle schema.
Global Common ID Attribute	Specify the User ID attribute name, this attribute will be used as part of the password policy to check that the user ID is not part of the password.
First Name Attribute	Specify the First Name attribute, this attribute will be used as part of the password policy to check that the user's first name is not part of the password.
Last Name Attribute	Specify the Last Name attribute, this attribute will be used as part of the password policy to check that the user's last name is not part of the password.
Email Address Attribute	Currently not supported.
Test Connection	Click to confirm connectivity, then close the confirmation window.
Apply	Click **Apply** to submit the registration.

Related Topics

Managing Data Sources in *Administrator's Guide for Oracle Access Management*.

10
Administration Help

The Administration page is used to add or remove an administrator role from the system store. All Administrator roles, users, and groups must be stored in the System Store. If the system store changes, appropriate Administrator roles must be added to the new System Store.

The Administration page is described in the following sections:

- Administration

10.1 Administration

The following table describes the elements in the Administration page:

Element	Description
System Store	Displays the registered System Store, this field is read-only.
Search	Use this section to search the System Store to find configured administrators.
Search Results	Displays the search results.

Search

The following table describes the elements in the Search section of the Administration page:

Element	Description
Name	Type a name that needs to be searched.
Role	Select a Role from the drop-down menu.
Type	Select a Type from the drop-down menu.
Search	Click **Search** to initiate the search and populate results in the search results table.
Reset	Click **Reset** to reset the search criteria.

Search Results

The following table describes the elements in the Search Results section of the Administration page:

Element	Description
Actions	Choose from the following options: • **Grant** - Choose **Grant** to add a user/group using the Add Users and Group dialog box. • **Revoke** - Select a row from the table and choose **Revoke** to remove the row.

Element	Description
View	Choose commands from the View menu to control how the columns are displayed: - **Columns** - Click a column header name to quickly show or hide a single column. - **Detach** - Click to open the table in a larger window. - **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns.
Grant	Click to open Add Users and Groups dialog box and grant specific roles to users and groups.
Revoke	Select a row from the table and click **Revoke** to remove the roles for that user and group.
Detach	Click to open the table in a larger window.
Row	Displays the row number.
Name	Displays the searched names.
Type	Displays the type of the searched names.
Role	Displays the roles of the searched names.
▲	Click to sort the items in the column in ascending order.
▼	Click to sort the items in the column in descending order.
Total Rows	Displays the total number of rows in the table.

Add Users and Groups dialog box

Click **Grant** to open this dialog box.

This dialog box is arranged in the following sections:

- Search
- Roles

Search

The following table describes the elements in the Search section of the Add Users and Groups dialog box:

Element	Description
Name	Type a name that needs to be searched.
Type	Select any of the following options from the drop-down menu: - **User** - Select User to add User Roles. - **Group** - Select Group to add Group Roles. - **All** - Select All to add both User and Group Roles.
Search	Click **Search** to initiate the search and populate results in the search results table.
Reset	Click **Reset** to reset the search criteria.

Search Results

The following table describes the elements in the Search Results section of the Add Users and Groups dialog box:

Element	Description
Name	Displays the searched names.
Type	Displays the type of the searched names.

Roles

The following table describes the elements in the Roles section of the Add Users and Groups dialog box:

Element	Description
Role	Select a role from the drop-down menu to be assigned to the selected users and groups.
Add Selected	In the search results table, select the desired User/Group and then click the **Add Selected** button to add the Users/Groups to the system store.
Cancel	Click **Cancel** to cancel the selections.
✕	Click to close the pop-up window.

Related Topics

Managing Data Sources in *Administrator's Guide for Oracle Access Management*

11
Certificate Validation Help

The Certification Validation module is used by the Security Token Service to validate X.509 tokens and to verify whether or not the certificates have been revoked.

The Certificate Validation page is described in the following section:

- Certificate Validation

11.1 Certificate Validation

The Certification Validation module is used by the Security Token Service to validate X.509 tokens and to verify whether or not the certificates have been revoked.

Certificate Revocation List

The Certificate Revocation List (CRL) page lists certificates that can be revoked. Revoked certificates are listed with a reason, an issue date, and the issuing entity. When a potential user attempts to access a server, the server allows or denies access based on the CRL entry for the particular user.

The following table describes the elements in the Certificate Revocation List section of the Certificate Validation page:

Element	Description
Actions	Choose options from the menu to perform the following operations: • **Add** - Click the **Add** button, in **Add CA CRL** dialog box, browse for the CRL file, select it, and click **Import**. • **Delete** - Select a row in the table and choose **Delete**, in the confirm pop-up click **Yes** to remove the row or click **No** to retain the row.
View	Choose commands from the menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Reorder Columns** - Click to open a dialog that lets you change the order of the table columns. • **Query By Example**- Click to show or hide the filter row that is displayed above the column headers to query on the columns.
Add	Click the **Add** button, in **Add CA CRL** dialog box, browse for the CRL file, select it, and click **Import**.
Delete	Select a row in the table and click **Delete**, in the confirm pop-up click **Yes** to remove the row or click **No** to retain the row.
⧩	Click to show or hide the filter row that is displayed above the column headers to query on the columns.
✎	Click to clear all the entries in the filter row.
Row	Displays the row number.

Element	Description
Issuer	Displays the entity name that issued the certificate.
Date Issued	Displays the certificate issue date.
Renewal Date	Displays the proposed date for renewal.
Enabled	Select to enable the Certificate Revocation List functionality.
Apply	Click **Apply** to save the configuration.
Revert	Click **Revert** to revert back the changes.

OCSP/CDP

The Online Certificate Status Protocol (OCSP) was developed as an alternative to CRLs. OCSP specified how the client application that requests information on a certificate's status will obtain it from the server that responds to the request. An OCSP responder can return a signed response signifying that the certificate specified in the request is either good, revoked or unknown. If the OCSP cannot process the request, it returns an error code.

The CRL Distribution Point extension (CDP) contains information regarding the location of the CRLs and OCSP servers.

The following table describes the elements in the OCSP/CDP section of the Certificate Validation page:

Element	Description
OCSP Enabled	Select to enable OCSP.
OCSP URL	Enter the URL of the OCSP Service.
OCSP Certificate Subject	Enter the Subject DN of the OCSP Service.
CDP Enabled	Select to Enable CDP.
Apply	Click to save this configuration.
Revert	Click to revert back the changes.

Related Topics

Managing Common Services and Certificate Validation in *Administrator's Guide for Oracle Access Management*

12
Server Instances Help

The Server Instances page is used to manage and monitor OAM server instances.

The following topics are covered:

- Server Instances
- Create OAM Server

12.1 Server Instances

Use the Server Instances page to, search for the existing OAM Servers.

Search

The following table describes the elements in the Search section of the Server Instances page:

Element	Description
Name	Type the name of the server that needs to be searched.
Search	Click **Search** to initiate the search and populate results in the Search Results table.
Reset	Click **Reset** to reset the search criteria.
Create OAM Server	Click to create a new OAM Server using the Create OAM Server page.

Search Results

The following table describes the elements in the Search Results section of the Server Instances page:

Element	Description
Actions	Choose from the following options: • **Create**- Select to create a new OAM server using the Create OAM Server page. • **Edit** - Select a row in the table and choose **Edit** to open the Create OAM Server page. After edit, click **OK** to save the changes or **Cancel** to cancel the changes. • **Delete** - To delete a row from the table, select the row and choose **Delete**. • **Monitor** - Select a server instance and choose **Monitor** to monitor the performance for the selected server instance.
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column. • **Detach** - Click to open the table in a larger window.

Element	Description
Create	Click to create a new OAM server using the Create OAM Server page.
Duplicate	Click to create a copy of the existing record. Select a row and click **Duplicate** to open the existing record in edit mode. User can make changes and save the record.
Edit	Select a row in the table and click **Edit** to open the record in edit mode. After edit, click **OK** to save the changes, or **Cancel** to cancel the changes.
Delete	Select a row in the table and click **Delete**. In the confirm pop-up click **Yes** to remove the row, or click **No** to retain the row.
Monitor	Select a server instance from the table and click **Monitor** to monitor the performance of the selected server instance. On the monitor page, click any of the following sub tab to view results for the server instance: • **Server Processes Overview** • **Session Operations** • **Server Operations** • **WebGates**
Detach	Click to open the table in a larger window.
Row	Displays the Row number.
Name	Displays the searched server names.
▲	Click to sort the items in the column in ascending order.
▼	Click to sort the items in the column in descending order.

Related Topics

Managing Server Registration in *Administrator's Guide for Oracle Access Management*.

12.2 Create OAM Server

Use the Create OAM Server page to:

- Register a freshly installed OAM Server instance.
- Modify an existing OAM Server registration.

The following table describes the elements in the Create OAM Server page:

Element	Description
Server Name	The identifying name for this server instance, which was defined during initial deployment in the WebLogic Server domain.
Host	Type the full DNS name (or IP address) of the computer hosting the server instance. **For Example:** *host2.domain.com*

Element	Description
Port	Provide the port on which this server communicates (listens and responds). **Default:**5575. **Note:**If both the SSL and Open ports of the Managed Server are enabled, then the Managed Server is set to the SSL port by default. If you must use the non-SSL port, the credential collector URL of the authentication scheme must be sent to the absolute URL which points to `http` as the protocol and non-SSL port.
Apply	Click **Apply** to submit your changes.

OAM Proxy

Use this section to configure OAM Proxy for OAM Servers.

The following table describes the elements in the OAM Proxy section of the Create OAM Server page:

Element	Description
Proxy Server Id	Type any valid and relevant string, DNS hostname is preferred. This is the identifier of the computer on which the OAM Proxy (and this OAM Server instance) resides.
Port	The unique port on which this OAM Proxy instance is listening. On a default installation, the port is 5575.
Mode	OAM channel transport security for the OAM Proxy can be one of the following (the agent mode must match during registartion and can be higher after registration). Choose any of the following from the drop-down menu: • **Open** - No encryption. • **Simple** - The data passed between the OAM Agent and OAM Server is encrypted using OAM self-signed certificates. **Note:** Before specifying Simple mode, you must specify the global passphrase. • **Cert** - The data between the OAM Agent and OAM Server is encrypted using Certificate Authority (CA) signed X.509 certificates. **Note:** Before specifying Cert mode, you must acquire signed certificates from a trusted third party Certificate Authority. On a default installation, the mode is Open.

Related Topics

Managing Server Registration in *Administrator's Guide for Oracle Access Management*.

13 Settings Help

The Settings page is used to manage configuration of access components.

The following topics are covered:

- Common Settings
- Access Manager Settings
- Federation Settings

13.1 Common Settings

Use the Common Settings page to Provide access to configurable settings that are global and common to all OAM Servers in your environment.

Session

In this section, you can configure Session life cycles.

The following table describes the elements in the Session section of the Common Settings page:

Element	Description
Session Lifetime (minutes)	Specify the amount of time that a user's authentication session remains active. When the lifetime is reached, the session expires. • Default value is 1440 minutes. • A value of zero (0) disables this setting. • Any value between 0(zero) and 2147483647 is allowed. **Note:** An expired session is automatically deleted from the in-memory caches (or database).
Idle Timeout (minutes)	Specify the amount of time that a user's authentication session remains active without accessing any Access Manager protected resources. When the user is idle for a longer period, they are asked to re-authenticate. • Default value is 15 minutes. • A value of zero (0) disables the setting. • Any value between 0(zero) and 2147483647 is allowed. **Note:** Timed-out sessions are not deleted from the session manager. Session data could be removed from the memory but will still be available in the persistent store (database). After re-authentication, the same session will be re-activated.
(Management) Maximum Search Results	Specify the maximum number of sessions that can be fetched by default for a session query if the result set is large.

Element	Description
Maximum Number of Sessions per User	Specify the exact number of sessions each user can have at one time. Use this setting to configure multiple session restrictions for all users. • Any positive integer is allowed. • Specifying the count as 1 (one) activates a special mode. If a user already has a session then he authenticates using another device (thereby creating a new session), then their existing session is deleted. No error is reported and no warning is given. **Note:**Too high a number impacts performance and results in a security risk. Oracle recommends less than 20 as a reasonable limit per user. Otherwise there can be performance impact.

Audit Configuration

In this section, you can manage Audit Configuration.

The following table describes the elements in the Audit Configuration section of the Common Settings page:

Element	Description
Maximum Directory Size (MB)	Specify the maximum size for the directory that contains audit output files. **For Example:** • Assuming that the maximum file size is 10, a value of 100 for this parameter implies that the directory allows a maximum of 10 files. Once the maximum directory size is reached, the audit logging stops. • A value of 100 specifies a maximum of 10 files if the file size is 10 MB. If the size exceeds this, the creation of audit logs stops.
Maximum File Size (MB)	Specify the maximum size for the audit log file. Once the size of the file reaches the maximum size, a new log file is created. **For Example:** Specifying 10 directs file rotation when the file size reaches 10 MB.
Filter Enabled	Check this box to enable event filtering.
Filter Preset	Defines the amount and type of information that is logged when the filter is enabled. Choose any option from the following drop-down menu: • **All** - Captures and records all auditable OAM events. • **Low** - Captures and records a specific set of auditable OAM events. • **Medium** - Captures and records events covered by the Low setting plus a number of other auditable OAM events. • **None** - no OAM events are captured and recorded. The default value is **None**. **Note:** Events for each filter are fixed in the read-only component_events.xml file. Editing or customizing this file is not supported for Oracle Access Management. Only items that are configured for auditing at the specified filter preset can be audited.
Audit Configuration	Administrators can add, remove, or edit special users using Audit Configuration table. The actions of the users specified in the table are included only when the filter is enabled. All actions of the special users are audited regardless of the filter preset.

Audit Configuration table

This table is displayed when Filter option is enabled.

The following table describes the elements in the Audit Configuration section of the Common Settings page:

Element	Description
View	Choose commands from the View menu to control how the columns are displayed: • **Columns** - Click a column header name to quickly show or hide a single column.
Add	Click to add a new row to the table.
Delete	Select a row and click **Delete** to remove the row.
Users	Add the users whose actions are to be audited.

Default and System Stores

In this section, you can define Default and System Identity Stores.

The following table describes the elements in the Default and System Identity Stores section of the Common Settings page:

Element	Description
Default Store	Click the name of the default store to display the configuration page.
System Store	Click the name of the system store to display the configuration page.

Related Topics

Managing Common Services and Certificate Validation in *Administrator's Guide for Oracle Access Management*.

13.2 Access Manager Settings

Load Balancing

The following table describes the elements in the Load Balancing section of the Access Manager Settings page:

Element	Description
OAM Server Host	Type the virtual host name that represents the OAM Server Cluster, which might be exposed by a load balancer in front of an OAM Server Cluster.
OAM Server Port	Provide the virtual host port associated with the OAM Server Cluster. Values between 1 and 65535 are supported.
OAM Server Protocol	Choose either HTTP or HTTPS from the drop-down menu, this is used to access the virtual host that represents the OAM Server Cluster.
Server Error Mode	Choose from the following options in the drop-down menu to configure error messages with varying degrees of security for your custom login pages: • **Internal** - Least secure level. • **External** - Recommended level. • **Secure** - Most secure. Provides generic error messages that barely give any hint of the internal reason for the error.

SSO

The following table describes the elements in the SSO section of the Access Manager Settings page:

Element	Description
IP Validation	Check the box to enable IP Validation, clear the box to disable IP validation. Specific to WebGates and is used to determine whether a client's IP address is same as the IP address stored in the ObSSOCookie generated for single sign-on.
SSO Token Version	Select your SSO token version from the drop-down menu.

Access Protocol

Access Protocol provides configuration options for Simple mode and Cert Mode Transport security.

The following table describes the elements in the Access Protocol section of the Access Manager Settings page:

Element	Description
Simple Mode Configuration	Add data to **Global Passphrase** field, for communication if you are using OAM-signed X.509 certificates. **Note:** This is set during initial OAM Server installation.Administrators can edit this passphrase and then reconfigure all existing OAM agents to use it.
Cert Mode Configuration	Specify details in the following fields, which is required for the Key Store where the Cert mode X.509 certificates signed by an outside Certificate Authority reside: • **PEM Keystore Alias** • **PEM Keystore Alias Password** **Note:** These are set during initial OAM Server installation. The certificates can be imported using the import certificate utility or the keytool shipped with JDK.

Policy

The following table describes the elements in the Policy section of the Access Manager Settings page:

Element	Description
Resource Matching Cache	Caches mapping between the requested URL and the policy holding the resource pattern that applies to the URL. Configure the following fields: • **Maximum Size** - Default value is 100000. Zero disables the cache. • **Time to Live** - Default value is 3600. Zero disables Time to Live.

Related Topics

Configuring Access Manager Settings in *Administrator's Guide for Oracle Access Management*.

13.3 Federation Settings

Use the Federation Settings page to:

- Configure the settings for use by Oracle Access Management Identity Federation.
- Configure to enable the Identity Federation functionality available from the Oracle Access Management Console.

The following table describes the elements in the Federation Settings page:

Element	Description
General	General federation settings include basic information about the provider and the keys used to send assertions.
Proxy	Proxy settings enable you to set up a proxy server for federation.
Keystore	Keystore settings enable you to create aliases (a short hand notation) for keys in the keystore.
Apply	Click **Apply** to submit your changes.

General

This section of the Federation Settings page, you can view and manage general federation properties. The following table describes the elements in the General section of the Federation Settings page:

Element	Description
Provider ID	Specify the provider ID of this federation server. **For example**: `http://foo.example.com/fed`
Succinct ID	This is the succinct ID of the provider.
Signing Key	Select a key from the drop-down menu, this key is used to sign assertions.
Encryption Key	Select a key from the drop-down menu, this key is used to decrypt incoming messages.
Custom Trust Anchor File	Specify a keystore that contains trusted root certificates used in federation. The default trust store is, `DOMAIN_HOME/config/fmwconfig/amtruststore` In most cases, the default trust anchor should be enough. If necessary, specify the location of an alternate keystore to use. **Note:** When you use a custom trust anc,hor keystore, it will not be replicated automatically across the cluster. You must manage the replication of this keystore.
Export SAML 2.0 Metadata	Click **Export SAML 2.0 Metadata**, a dialog box appears where you must specify the file for the exported metadata, Click **Save** to save your new metadata file.

Proxy

In this section of the Federation Settings page, you can view and manage a proxy configured for use with federation partners. The following table describes the elements in the Proxy section of the Federation Settings page:

Element	Description
Enable Proxy	Check this box to enable the proxy server. Clear this box to disable the proxy function and related fields will be inaccessible for editing.
Host	Specify a proxy host name.
Port	Specify the proxy port number.
Non-Proxy Hosts	Specify a list of hosts for which the proxy should not be used. Use ';' to separate multiple hosts.
Username	Enter the proxy user name to use when connecting to the proxy.
Password	Enter the proxy password to use when connecting to the proxy.

Keystore

In this section of the Federation Settings page, you can view and manage keystores configured for use with federation partners. The following table describes the elements in the Keystore section of the Federation Settings page:

Element	Description
Keystore Location	This element specifies the keystore path.
Add	Click on **Add** to add a new row to the table.
Delete	Select a row from the table and click on **Delete** to remove the row from the table.
Row	Displays the row number.
Key ID	Specify the unique key ID.
Alias	Choose the key alias from the drop-down menu. **Note:** You can choose one of the aliases that is available in the keystore using the drop-down.
Password	Specify the key password.
Description	Provide a brief description of the key, such as its usage type.

Related Topics

Managing Settings for Identity Federation in *Administrator's Guide for Oracle Access Management*.

13.4 Access Portal Service Settings

The following table describes the elements in the Access Portal Service Settings page:

Element	Description
IDS Profile	Choose a IDS Profile from the drop-down list that you created earlier.
OPAM URL	Points to the instance of OPAM.
Apply	Click to submit the changes.