

Oracle® Cloud

Access Governance Cloud Service



F59550-10



Oracle Cloud Access Governance Cloud Service,

F59550-10

Copyright © 2022, Oracle and/or its affiliates.

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

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

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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

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

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

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

1 Getting Started

Overview	1-1
About Access Governance	1-1
Key Features	1-1
Access Review	1-1
Access Review Campaigns	1-2
Event-Based Access Reviews	1-2
Identity Intelligence	1-3
Workflows	1-3
Identity Orchestration	1-3
Intuitive User Interface	1-3
Reporting and Analytics	1-3
Before You Begin	1-4
Oracle Cloud Infrastructure Services	1-4
Typical Workflow for Administrators	1-5
Set Up Users	1-6
About Setting Up Users and Groups	1-7
Understanding Application Roles	1-7
Use Identity Domains to Onboard Users and Groups for Oracle Access Governance	1-8
Use Oracle Identity Cloud Service to Onboard Users and Groups for Oracle Access Governance	1-10
Assign Access Governance Application Roles to Users and Groups	1-11
Set Up Service Instance	1-12
Regions	1-12
Prerequisites	1-15
Create Service Instance	1-16
Verify Service Instance	1-17

2 Administer

System Administration	2-1
Performance Tuning	2-1
Tuning Runtime Configuration	2-1

Sizing Virtual Machine/Host	2-2
Manage Settings	2-2
Set Notification Email	2-2
Set Up Service Instance	2-3
Regions	2-3
Prerequisites	2-6
Create Service Instance	2-6
Verify Service Instance	2-8
Manage Service Instance	2-9
Review Service Instance	2-9
Launch Service Home Page	2-9
Edit Service Instance	2-10
Delete Service Instance	2-11
Service Administration	2-11
Activate/Inactivate Identities for License Management	2-11
Navigate to Manage Identities	2-11
Select Identities for Activation	2-12
View and Configure Custom Identity Attributes	2-13
Overview	2-13
View Custom Attributes	2-13
Fetch Latest Custom Attributes	2-14
Modify Attribute Settings	2-15
Access Control Administration	2-16
Create Identity Collections	2-16
Navigate to Identity Collections	2-16
Add Details	2-16
Select Identities	2-17
Review and Submit	2-18
Manage Identity Collections	2-18
View and Manage Identity Collections	2-18
Preferences	2-20
Manage Delegation Preferences	2-21
Set up Your Delegation Preferences	2-21
Edit a Delegation	2-22
Delete a Delegation	2-22

3 Integrate

Getting Started with Integration	3-1
Access Governance Integration with Connected Systems	3-1
Connected Systems Overview	3-1

Integration Concepts	3-1
Manage the Connected System	3-2
Agent Administration	3-4
Register and Download a Connected System Agent	3-4
Prerequisites	3-5
Agent Management Operations	3-5
Install Agent on Target System	3-7
Verify Agent	3-8
Agent Example Usage	3-9
Integrate with Target Systems	3-11
Integrate with Oracle Identity Governance	3-11
Register and Download the Oracle Identity Governance Agent	3-12
Integrate with Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM)	3-15
Prerequisites	3-15
Establish Connection by Adding a New Cloud Service Provider - OCI IAM	3-15

4 Review

About Reviews	4-1
Overview	4-1
Examples	4-2
Create and Configure Reviews	4-3
Create User Access Review Campaigns	4-3
Navigate to Campaigns	4-3
Selection Criteria	4-3
Assign Workflow	4-6
Add Details	4-7
Review and Submit	4-8
Create Policy Review Campaigns	4-8
Login	4-8
Selection Criteria	4-9
Assign Workflow	4-10
Add Details	4-11
Review and Submit	4-12
Enable Event-based Access Reviews	4-12
Setup Event-Based Access Review	4-12
Configure Multi-Events	4-14
View Event-Types	4-15
Manage and Monitor Access Reviews	4-15
Manage Access Review Campaign	4-16
Manage an Access Review Campaign	4-16

Monitor an Access Review Campaign	4-19
Generate Event-Based Access Reviews Report	4-21
Navigate to the Event-Based Access Reviews Report Service	4-21
Run Event-Based Access Reviews Report	4-21
View Event-Based Access Reviews Report Results	4-22
Additional Actions	4-23
Review Access and Permissions	4-23
Perform Access Review	4-23
Identity Review Tasks	4-24
Policy Review Tasks	4-25
View Access to Resources	4-27
My Directs' Access	4-27
My Access	4-28
Enterprise-wide Access	4-29

5 Related Content

Oracle Access Governance Release Notes	5-1
Access Governance REST APIs	5-1

1

Getting Started

Overview

About Access Governance

Oracle Access Governance is a cloud-native Identity Governance and Administration (IGA) solution that provides insights-based access reviews, identity analytics, and intelligence capabilities for businesses.

Oracle Access Governance provides features including:

- Visibility of enterprise compliance by providing details on who has access to what.
- Ability for reviewers to optimize user privileges through intelligent access review campaigns.
- Actionable identity intelligence by building deep insights into potential security violations that enable rapid remediation of identity and access challenges.
- Continuous compliance to meet governance and compliance requirements across many applications, workloads, infrastructures, and identity platforms.

Key Features

Key features of Oracle Access Governance include the following:

Access Review

An **Access Review** is the review of access and permissions for an entity, usually an end user, that is carried out to confirm whether the access and permissions assigned to that entity are still valid. An example use case might be when an end user moves to another department in your organization, and as a result, no longer requires access to a particular resource.

Access reviews can be carried out by the following users:

- **User** (review access assigned to me/self)
- **Manager** (review access assigned to users in my team)
- **Owner** (review access assigned to users over resources I own)
- **CloudAccessReviewer** (review access of cloud resources, such as OCI IAM Policies)
- **Custom Reviewer** (review access tasks assigned to a user other than end-user, manager, or owner. The default value is *Me*)

Access reviews enable the following features:

- User access reviews

- Policy reviews
- Event-based access reviews
- Intelligent reminders to drive action from end-users, approvers, and skip level approvers.
- Self-reviews by the end-users

Access Review Campaigns

Access review campaigns are run on-demand or can be scheduled periodically. You can run access review campaigns one-time or opt to choose a recurring pattern like **Quarterly, Monthly, Half-Yearly, or Yearly**.

Access review campaigns include:

- **User Access Reviews:** Comprises a group of access reviews for members of your enterprise population where individual access to a specific source is checked and either certified or remediated.
- **Policy Reviews:** Comprises a group of policy reviews that evaluates access control of Identity and Access Management (IAM) Policies. Access control of each cloud resource is evaluated up to the policy statement-level. The policy statements can either be accepted or revoked. The final remediation decision will be submitted per policy, and further sent to the connected system for closed-loop access remediation.

Event-Based Access Reviews

Event-Based Access Reviews are the action-oriented access reviews carried out by Oracle Access Governance when one or more predefined event types occur. Whenever events, such as job-code change, location change, and so on occur, the event-based access review feature helps the service administrators to check, certify or remediate the impacted user or application roles, permissions, or entitlements.

Once configured, a single or a multi-event access review activity may launch. This depends on the changes in the identity profile and the duration between data refreshes for those identity changes.

For example, if a department of an organization merges into another department, it results in department change, manager change, and job-code change. As a result, the impacted members of the organization require access to the resources of the new department and should not use the resources of the previous department. If the database is updated synchronously for these events, this will trigger a multi-event access review activity within Oracle Access Governance.

Whenever such predefined event types occur, and are reflected in the database, these are automatically picked up by Oracle Access Governance through the **Connected Systems** functionality that initiate the **Event-Based Access Review** activities.

Using this feature, you can:

- Control the event-type to initiate the access reviews.
- Define auto-actions for low-risk access reviews.
- Generate insights on event-based access reviews.

Identity Intelligence

Oracle Access Governance analyzes each identity and its privileges, builds insights into potential high-risk assignment and security violations, and recommends remediations. This enables access reviewers to make corrective decisions quickly. This feature enables:

- Assimilation and analysis of identity data and access privileges.
- Recognition of contextual insights and identification of security blind spots.
- Remediation recommendations enable access reviewers to make corrective decisions quickly.

Workflows

Workflows provide out-of-the-box features in Oracle Access Governance. These include:

- **Notifications:** Reviewers are notified about assigned and pending access reviews.
- **Multi-stage approvals:** Oracle Access Governance supports one-level, two-level, and three-level access review workflows.
- **Decision making:** Access reviews can be accepted or revoked.

Workflows in Oracle Access Governance enable:

- Zero coding workflow creation.
- Multi-stage approval workflows.
- Suggestions for intelligent workflow based on selected criteria.

Identity Orchestration

Identity orchestration is provided by Oracle Access Governance, enabling integration with both on-premises and Cloud-connected systems. This code-less integration of identity allows for the assimilation of identity data and access privileges from multiple connected systems and subsequent analysis in Oracle Access Governance.

Features include :

- Minimal configuration, and code-less integration with on-premises and on-cloud applications and systems.
- Improves IT efficiency and reduces operational costs through automation.

Intuitive User Interface

The Oracle Access Governance Console provides an intuitive user interface (UI) for access reviews, allowing smart tracking of access review campaigns. Intelligent dashboards are available that assist in focusing on prioritized and urgent review tasks.

Reporting and Analytics

Oracle Access Governance enables reporting and analytics in the following areas:

- 360-degree visibility into identities, accounts, and permissions usage in intuitive dashboards.
- Discover, determine risk, and monitor accounts with privileged access for anomalous behavior.
- Access Reviews outcome and fulfillment reports.

Before You Begin

Oracle Cloud Infrastructure Services

When you order Oracle Access Governance through Universal Credits, you automatically get access to Oracle Cloud Infrastructure and other required services.

Here's some information about how Oracle Access Governance uses other services and what you need to do if you're setting up Oracle Access Governance for the first time.

Table 1-1 Oracle Cloud Infrastructure Services used by Oracle Access Governance

Service	What is it for?	Do I need to do anything?
Oracle Cloud Infrastructure Identity and Access Management	<p>Compartments: You use compartments to organize resources on Oracle Cloud Infrastructure.</p> <p>Policies: You use IAM security policies to grant permissions.</p> <p>Domains: You use identity domains to manage users and groups in your organization who will be required to use Oracle Access Governance and Oracle Cloud Infrastructure Console.</p>	<p>Yes</p> <p>Before you create your first Oracle Access Governance instance, Oracle recommends that you set up one or more compartments in which you can deploy and secure your cloud resources.</p> <ul style="list-style-type: none"> • Setting Up Your Tenancy • Managing Compartments <p>Optionally, you can set up security policies that give other users permission to set up and manage Oracle Access Governance instances. See Set Up Users for further details.</p>

Table 1-1 (Cont.) Oracle Cloud Infrastructure Services used by Oracle Access Governance

Service	What is it for?	Do I need to do anything?
Oracle Identity Cloud Service	<p>If identity domains aren't available in your cloud account, you use Oracle Identity Cloud Service to manage the users and groups in your organization who will use Oracle Access Governance.</p> <p>In most cases, Oracle Access Governance is automatically federated with the <i>primary</i> Oracle Identity Cloud Service instance associated with your tenancy.</p>	<p>Yes</p> <p>You can add users and groups before you create the Oracle Access Governance instance or after; you can decide. See Set Up Users for further details.</p> <p>If you want to federate with a secondary Oracle Identity Cloud Service instance or your tenancy is a government region where federation isn't set up automatically, you must federate with Oracle Identity Cloud Service manually.</p>

Typical Workflow for Administrators

This topic outlines a typical workflow for Oracle Access Governance administrators.

If you're setting up Oracle Access Governance for the first time, follow these tasks as a guide.

Task	Description	More Information
Place an order for Oracle Access Governance or sign up for a free Oracle Cloud promotion	<p>Sign up for a free credit promotion or subscribe to Oracle Access Governance through Universal Credits.</p> <p>See Oracle Global Infrastructure Regions</p>	<p>Request and Manage Free Oracle Cloud Promotions</p> <p>Upgrade Your Free Oracle Cloud Promotion</p>
Activate your Oracle Cloud account and sign in for the first time	<p>You receive a welcome email when your account is ready. To activate your account, you must sign in with the credentials provided in the email.</p> <p>As the Cloud Account Administrator, you can complete all the setup tasks for Oracle Access Governance.</p>	Manage Service Instance
Determine your service requirements	<p>Plan your Oracle Access Governance deployment. Think about what you need before you start.</p>	<p>Service Requirements</p> <ul style="list-style-type: none"> • Users • Region
(Optional) Enable other users to set up services	<p>If you don't want to set up Oracle Access Governance yourself, give other users permissions to create services.</p>	Set Up Users

Task	Description	More Information
(Recommended) Create a compartment for your service	Create a compartment for your Oracle Access Governance deployment.	When you sign up for Oracle Cloud Infrastructure, Oracle creates your tenancy with a root compartment that holds all your cloud resources. You then create additional compartments within the tenancy (root compartment) and corresponding policies to control access to the resources in each compartment. Before you create an Oracle Access Governance instance, Oracle recommends that you set up the compartment where you want the instance to belong. You create compartments in Oracle Cloud Infrastructure Identity and Access Management. See Setting Up Your Tenancy and Managing Compartments .
Create a service	Deploy a new service with Oracle Access Governance.	Set Up Service Instance
Verify your service	When your service is ready, check that you can sign in and your service is up and running.	Set Up Service Instance
Activate Identities for License Management	Define which identities can use your Oracle Access Governance service.	
Integrate with Connected Systems	Configure integration with external systems which you want to perform access reviews and campaigns against	See <ul style="list-style-type: none"> • Integrate with Connected Systems • Integrate with Oracle Identity Governance • Integrate with Oracle Cloud Infrastructure (OCI) Identity and Access Management
Set up users and groups	Set up users and groups for Oracle Access Governance and assign them to application roles.	Set Up Users
Administer services	Monitor services and perform administrative tasks such as edit and delete. Delegate administrative responsibilities to others through security policies.	See Manage Service Instance and Set Up Users

Set Up Users

About Setting Up Users and Groups

Set up user accounts for everyone you expect to use Oracle Access Governance.

The way you manage users for Oracle Access Governance (and Oracle Cloud Infrastructure) depends on whether *identity domains* are available in your cloud account.

- **Oracle Cloud Infrastructure Identity and Access Management (IAM) Identity Domains:** Some Oracle Cloud regions have been updated to use identity domains. If you have a new cloud account in one of these regions, you use identity domains to manage the users who perform tasks in both Oracle Access Governance and Oracle Cloud Infrastructure.
- **Oracle Identity Cloud Service:** If you have an existing cloud account or you deploy Oracle Access Governance in a region that does not currently offer identity domains, you use a federated Oracle Identity Cloud Service to manage the users who perform tasks in Oracle Access Governance. In addition, you use Oracle Cloud Infrastructure Identity and Access Management to manage the users who create and manage your Oracle Access Governance deployments using the Oracle Cloud Infrastructure Console.

It is easy to determine whether or not your cloud account offers identity domains. In Oracle Cloud Infrastructure Console, navigate to **Identity & Security**. Under **Identity**, check for **Domains**.

- If you see **Domains**, you use identity domains to manage users and groups for Oracle Cloud Infrastructure and your Oracle Access Governance deployments. See [Use Identity Domains to Onboard Users and Groups for Oracle Access Governance](#).
- If **Domains** is not listed, you use a federated Oracle Identity Cloud Service to manage Oracle Access Governance users and IAM to manage Oracle Cloud Infrastructure users. See [Use Oracle Identity Cloud Service to Onboard Users and Groups for Oracle Access Governance](#).

The following table outlines the differences between the two configurations.

Cloud Accounts That Use Identity Domains	Cloud Accounts That Don't Use Identity Domains
Users and groups are configured in IAM.	Users and groups are configured in both IAM and Oracle Identity Cloud Service, and are linked through federation.
Provides a single, unified console for managing users, groups, dynamic groups, and applications in <i>domains</i> .	Oracle Cloud Infrastructure Identity and Access Management must be federated with Oracle Identity Cloud Service.
Provides Single Sign-On to more applications using a single set of credentials and a unified authentication process.	Requires separate federated credentials for Oracle Identity Cloud Service.
The Federation page doesn't list any entries for Oracle Identity Cloud Service.	The Federation page lists oracleidentitycloudservice , the primordial Oracle Identity Cloud Service automatically federated in your cloud account.

Understanding Application Roles

Oracle Access Governance users can be assigned any of the following roles depending on the access required.

Table 1-2 Oracle Access Governance Application Roles

Application Role	Entitlements
Administrator	<ul style="list-style-type: none"> Integrate target identity data systems with Access Governance Create campaigns Modify, Delete, Monitor all access review campaigns Create, Modify Security Settings Create, Modify Systems Settings Enable or Disable an event for access reviews Define auto-action for low-risk access reviews Modify, Delete, Monitor all event-based access reviews Generate Event-Based Access Report
Campaign Administrator	<ul style="list-style-type: none"> Create Campaigns Modify, Delete, Monitor self-created access review campaigns
Auditor	<ul style="list-style-type: none"> Monitor all access review campaigns
User	<ul style="list-style-type: none"> As a campaign owner - modify, delete, monitor self-owned access review campaigns. As an access reviewer - review and certify the access review tasks. As an end user - review the assigned privileges assigned to self and direct reports.

 **Note:**

Any Oracle Cloud Infrastructure user can log in to Oracle Access Governance with the **User** application role.

Use Identity Domains to Onboard Users and Groups for Oracle Access Governance

If your Oracle Access Governance instance uses *identity domains* for identity management, you use Oracle Identity Governance provisioning, an external Identity Provider (IDP), or a self-registration profile to onboard user accounts for everyone you

expect to use Oracle Access Governance. These users will be assigned to a group, which, when you have completed onboarding, you map to Oracle Access Governance *application roles*)

As an Oracle Cloud Infrastructure *Cloud Administrator*, you can use one of the following approaches to enable access for users to the Oracle Access Governance application.

Approach 1: Set Federated Authentication from an External Identity Provider (IDP)

1. Setup federation with an external IDP:
 - a. Set up a federated login between an Identity Domain and external IDP. Users can sign in and access Oracle Access Governance resources and features by using existing logins and passwords managed by the IDP.
 - b. Refer to [Managing Identity Providers](#) in the Oracle Cloud Infrastructure documentation for further details.
2. Enable SAML Just-In-Time provisioning.
 - a. This process automates user account creation when a user first tries to sign in to Oracle Cloud Infrastructure where the user does not yet exist in the Identity Domain.
 - b. Refer to [About SAML Just-In-Time Provisioning](#) in the Oracle Cloud Infrastructure documentation for further details.

Approach 2: Configure Oracle Identity Governance Provisioning with Oracle Cloud Infrastructure Identity and Access Management Using the Oracle Identity Cloud Service Application

1. Configure the Oracle Identity Cloud Service Application.
 - a. Download the connector installation package and copy the contents to the `OIG_HOME/server/ConnectorDefaultDirectory` directory. Refer to [Downloading the Connector Installation Package](#) for further details.
 - b. Log in to the Oracle Cloud Infrastructure Console and create an application with the type *Confidential*. Refer to [Creating an Application By Using the Connector](#) for further details.
 - c. Copy the *Client ID* and *Client Secret* from the created Application. This will be used in customAuthHeaders in ITResource.
 - d. Configure SSL to secure communication between Oracle Identity Governance and the target system, in this case, Oracle Access Governance. Refer to [Configuring SSL for the Connector](#) for further details.
2. Create Groups: Login to the Oracle Cloud Infrastructure Console and create groups for any Oracle Identity Governance groups you want to map to Oracle Access Governance roles.
3. Create an IDCS application in Oracle Identity Governance. Refer to [Creating an Application By Using the Connector](#) for further details.
4. Run the Group Lookup Recon Job.
5. Provision the IDCS application for those users with a membership of Access Governance groups.

Approach 3: Self Registration Profiles

Create self-registration profiles to enable users to create their accounts in Oracle Cloud Infrastructure Identity and Access Management. Refer to [Creating Self-Registration Profiles](#) for further details.

Use Oracle Identity Cloud Service to Onboard Users and Groups for Oracle Access Governance

If your Oracle Access Governance instance uses Oracle Identity Cloud Service for identity management, you use Oracle Identity Governance provisioning, an external Identity Provider (IDP), or a self-registration profile to onboard user accounts for everyone you expect to use Oracle Access Governance. These users will be assigned to a group, which, when you have completed onboarding, you map to Oracle Access Governance *application roles*.

As an Oracle Cloud Infrastructure *Cloud Administrator*, you can use one of the following approaches to enable access for users to the Oracle Access Governance application.

Approach 1: Set Federated Authentication from an External Identity Provider (IDP)

1. Setup federation with an external IDP:
 - a. Set up a federated login between an Identity Domain and external IDP. Users can sign in and access Oracle Access Governance resources and features by using existing logins and passwords managed by the IDP.
 - b. Refer to [Federating with Identity Providers](#) in the Oracle Cloud Infrastructure documentation for further details.
2. Enable SAML Just-In-Time provisioning.
 - a. This process automates user account creation when a user first tries to sign in to Oracle Cloud Infrastructure where the user does not yet exist in the Identity Domain.
 - b. Refer to [User Provisioning for Federated Users](#) in the Oracle Cloud Infrastructure documentation for further details.

Approach 2: Configure Oracle Identity Governance Provisioning with Oracle Cloud Infrastructure Identity and Access Management Using the Oracle Identity Cloud Service Application

1. Configure the Oracle Identity Cloud Service Application.
 - a. Download the connector installation package and copy the contents to the `OIG_HOME/server/ConnectorDefaultDirectory` directory. Refer to [Downloading the Connector Installation Package](#) for further details.
 - b. Log in to the Oracle Cloud Infrastructure Console and create an application with the type *Confidential*. Refer to [Creating an Application By Using the Connector](#) for further details.
 - c. Copy the *Client ID* and *Client Secret* from the created Application. This will be used in `customAuthHeaders` in `ITResource`.

- d. Configure SSL to secure communication between Oracle Identity Governance and the target system, in this case, Oracle Access Governance. Refer to [Configuring SSL for the Connector](#) for further details.
2. Create Groups: Login to the Oracle Cloud Infrastructure Console and create groups for any Oracle Identity Governance groups you want to map to Oracle Access Governance roles.
3. Create an IDCS application in Oracle Identity Governance. Refer to [Creating an Application By Using the Connector](#) for further details.
4. Run the Group Lookup Recon Job.
5. Provision the IDCS application for those users with a membership of Access Governance groups.

Approach 3: Self Registration Profiles

Create self-registration profiles to enable users to create their accounts in Oracle Cloud Infrastructure Identity and Access Management. Refer to [Creating Self-Registration Profiles](#) for further details.

Assign Access Governance Application Roles to Users and Groups


Once users are onboarded, they can log in and access the Oracle Access Governance Console. To determine what privileges they have within Oracle Access Governance, assign them the relevant predefined application roles as described in [Understanding Application Roles](#).


Assigning Oracle Access Governance depends on whether identity domains are available in your cloud account.

- If **Domains** is listed, then use the [For Identity Domain Users](#) method.
- If **Domains** is not listed, and you use the federated Oracle Identity Cloud Service (IDCS) method to manage users, then use the [For Non Identity Domain Users](#) method.

For Identity Domain Users

Here's how you can assign Oracle Access Governance application roles to Users and Groups:

1. Open your web browser and navigate to <https://cloud.oracle.com>.
2. Enter the name of your **Cloud Account Administrator** in the **Cloud Account Name** field and click **Next**.
3. On the Cloud Infrastructure sign-in page, enter your sign-in credentials under **Oracle Cloud Infrastructure Direct Sign-In**. Click **Sign In**.
4. Click the  icon in the top, left corner to display the navigation menu.
5. Click **Identity & Security** in the navigation menu.
6. Select **Domains** within the **Identity** list.
7. On the left pane, in the **Compartment** list, select the relevant compartment for Oracle Access Governance.
8. In the available domain list, select the domain link related to Oracle Access Governance. Your selected domain page is displayed.

9. From the left pane, select the **Oracle Cloud Services** tab.
10. Select the Oracle Access Governance cloud service.
11. On the left pane, in the **Resources** section, select **Application roles**.
12. In the **Application roles** section, select the  icon corresponding to the application role that you want to assign.
13. Select the **Manage** link corresponding to the **Assigned users** category. The **Manage user assignments** window is displayed.

 **Note:**



To assign application roles to user groups, select the **Manage** link corresponding to the **Assigned groups** category.

14. Select the **Show available users** link.
15. In the available list of users, select the check box corresponding to the user name, and then click **Assign**.

The application role is assigned to the selected user or group. You can verify the same by viewing the names in the **Available users** or **Available groups** list.

For Non Identity Domain Users

Here's how you can assign Oracle Access Governance application roles to Users and Groups for Non Identity Domain-based users:

- Sign in to the Oracle Identity Cloud Service console with the user assigned as the *Service Administrator* team role.
- Click the  icon in the top, left corner to display the navigation menu.
- Click **Oracle Cloud Services** and then select your Oracle Access Governance service instance.
- Click the **Application Roles** tab. All the available application roles in Oracle Access Governance are displayed.
- Click the  role menu icon corresponding to the application role that you want to assign, and then, as per your requirement, select **Assign Users** or **Assign Groups**.

Set Up Service Instance

Regions

You can create an Oracle Access Governance service instance in the following regions: US East (Ashburn) for North America, Brazil East (Sao Paulo) for South America, Germany Central (Frankfurt) or UAE Central (Abu Dhabi) for Europe, and Australia East (Sydney) for Asia-Pacific. When you login to your tenancy, depending on your home region, chose the region hosting Oracle Access Governance within your geographic region to create and manage service instances. The tables below list the

home regions that support Oracle Access Governance and which region they need to have a subscription for to access the Oracle Access Governance service.

North America

If you have an Oracle Cloud Infrastructure tenancy in one of the below home regions, you must have a subscription to the **US East (Ashburn)** region to be able to access the Oracle Access Governance service.

Region Name	Region Identifier	Region Location	Region Key	Realm Key	Availability Domains
Canada Southeast (Montreal)	ca-montreal-1	Montreal, Canada	YUL	OC1	1
Canada Southeast (Toronto)	ca-toronto-1	Toronto, Canada	YYZ	OC1	1
US East (Ashburn)	us-ashburn-1	Ashburn, VA	IAD	OC1	3
US West (Phoenix)	us-phoenix-1	Phoenix, AZ	PHX	OC1	3
US West (San Jose)	us-sanjose-1	San Jose, CA	SJC	OC1	1

South America

If you have an Oracle Cloud Infrastructure tenancy in one of the below home regions, you must have a subscription to the **Brazil East (Sao Paulo)** region to be able to access the Oracle Access Governance service.

Region Name	Region Identifier	Region Location	Region Key	Realm Key	Availability Domains
Brazil East (Sao Paulo)	sa-saopaulo-1	Sao Paulo, Brazil	GRU	OC1	1
Brazil Southeast (Vinhedo)	sa-vinhedo-1	Vinhedo, Brazil	VCP	OC1	1
Chile (Santiago)	sa-santiago-1	Santiago, Chile	SCL	OC1	1

Europe

If you have an Oracle Cloud Infrastructure tenancy in one of the below home regions, you must have a subscription to the **Germany Central (Frankfurt)** or the **UAE Central (Abu Dhabi)** region to be able to access the Oracle Access Governance service.

Region Name	Region Identifier	Region Location	Region Key	Realm Key	Availability Domains
France Central (Paris)	eu-paris-1	Paris, France	CDG	OC1	1
France South (Marseille)	eu-marseille-1	Marseille, France	MRS	OC1	1

Region Name	Region Identifier	Region Location	Region Key	Realm Key	Availability Domains
Germany Central (Frankfurt)	eu-frankfurt-1	Frankfurt, Germany	FRA	OC1	3
Israel Central (Jerusalem)	il-jerusalem-1	Jerusalem, Israel	MTZ	OC1	1
Italy Northwest (Milan)	eu-milan-1	Milan, Italy	LIN	OC1	1
Netherlands Northwest (Amsterdam)	eu-amsterdam-1	Amsterdam, Netherlands	AMS	OC1	1
Saudi Arabia West (Jeddah)	me-jeddah-1	Jeddah, Saudi Arabia	JED	OC1	1
South Africa Central (Johannesburg)	af-johannesburg-1	Johannesburg, South Africa	JNB	OC1	1
Sweden Central (Stockholm)	eu-stockholm-1	Stockholm, Sweden	ARN	OC1	1
Switzerland North (Zurich)	eu-zurich-1	Zurich, Switzerland	ZRH	OC1	1
UAE Central (Abu Dhabi)	me-abudhabi-1	Abu Dhabi, UAE	AUH	OC1	1
UAE East (Dubai)	me-dubai-1	Dubai, UAE	DXB	OC1	1
UK South (London)	uk-london-1	London, United Kingdom	LHR	OC1	3
UK West (Newport)	uk-cardiff-1	Newport, United Kingdom	CWL	OC1	1

Asia-Pacific

If you have an Oracle Cloud Infrastructure tenancy in one of the below home regions, you must have a subscription to the **Australia East (Sydney)** region to be able to access the Oracle Access Governance service.

Region Name	Region Identifier	Region Location	Region Key	Realm Key	Availability Domains
Australia East (Sydney)	ap-sydney-1	Sydney, Australia	SYD	OC1	1
Australia Southeast (Melbourne)	ap-melbourne-1	Melbourne, Australia	MEL	OC1	1
India South (Hyderabad)	ap-hyderabad-1	Hyderabad, India	HYD	OC1	1
India West (Mumbai)	ap-mumbai-1	Mumbai, India	BOM	OC1	1

Region Name	Region Identifier	Region Location	Region Key	Realm Key	Availability Domains
Japan Central (Osaka)	ap-osaka-1	Osaka, Japan	KIX	OC1	1
Japan East (Tokyo)	ap-tokyo-1	Tokyo, Japan	NRT	OC1	1
Singapore (Singapore)	ap-singapore-1	Singapore, Singapore	SIN	OC1	1
South Korea Central (Seoul)	ap-seoul-1	Seoul, South Korea	ICN	OC1	1
South Korea North (Chuncheon)	ap-chuncheon-1	Chuncheon, South Korea	YNY	OC1	1

 **Note:**

You cannot access the Oracle Access Governance service from a subscription to a region outside your geographical region. An example would be if your home region is **UK South (London)** then you cannot access the service with a subscription to **US East (Ashburn)**, you must have a subscription to **Germany Central (Frankfurt)** within your geographical region.

Prerequisites

A prerequisite for creating and setting up a service instance is to provide permissions for **agcs-instance** resources.


In order to create, update, or delete an Oracle Access Governance service instance, the Oracle Cloud Infrastructure Identity and Access Management administrator or domain administrator can create a group and allow that group permissions to manage **agcs-instance** resources for a given compartment or tenancy in a policy statement:

1. Examples for Tenancies using Identity Domain:
 - a. Allow group <domain_name>/<group_name> to manage **agcs-instance** in compartment <compartment_name>
 - b. Allow group <domain_name>/<group_name> to manage **all-resources** in compartment <compartment_name>
2. Examples for Tenancies without Identity Domain:
 - a. Allow group <group_name> to manage **agcs-instance** in compartment <compartment_name>
 - b. Allow group <group_name> to manage all-resources in in compartment <compartment_name>


Create Service Instance

Create an Oracle Access Governance instance in the Oracle Cloud Infrastructure console.

You can create an Oracle Access Governance service instance using the following steps:

1. Open your web browser and navigate to <https://cloud.oracle.com>.
2. Enter the name of your **Cloud Account Administrator** in the **Cloud Account Name** field and click **Next**.
3. On the Cloud Infrastructure sign-in page, enter your sign-in credentials under **Oracle Cloud Infrastructure Direct Sign-In**. Click **Sign In**.
4. When you have successfully logged in, select **Regions** → **[US East (Ashburn)|Brazil East (Sao Paulo)|Germany Central (Frankfurt)|Australia East (Sydney)]**, depending on your Home region location, from the top navigation menu.
5. Click the  icon in the top left corner to display the navigation menu.
6. Click **Identity and Security** in the navigation menu.
7. Select **Access Governance** from the list of products.
8. On the **Service Instances** page, click the **Create service instance** button.
9. Enter values for the service instance as detailed in the following table .


Parameter	Value	Description
Name		Name of the service instance.
Description		Description of the service instance.
Create in compartment	Compartment Name into which the service instance will be created.	Name of the OCI compartment into which the service instance will be created.

Parameter	Value	Description
License type		<p>Select from the following license types:</p> <ul style="list-style-type: none"> • Access Governance for Oracle Workloads: Governance of access privileges for Oracle Workloads running anywhere • Access Governance for Oracle Cloud Infrastructure: Governance of access privileges for OCI resources and services.
		<p> Note:</p> <p>Access Governance for OCI is the entry level license option, covering OCI in cloud environments. Access Governance for Oracle Workloads is a broader option, covering Oracle Workloads running anywhere, and includes OCI.</p>
Tagging		<p>Tags allow you to organize and track resources within your tenancy. If you want to tag resources within the service instance, add them here. Add value as described in the following rows. If you want to add additional tags, select Another Tag to create more.</p>
	TAG NAMESPACE	Namespace to which the tag applies.
	TAG KEY	Key for the tag.
	TAG VALUE	Value of the tag.

10. To create the service instance with the value you have input, select **Create service instance**. If you do not want to proceed with the service creation, select **Cancel**.

Verify Service Instance

You can verify an Oracle Access Governance service instance using the following steps:

1. Open your web browser and navigate to <https://cloud.oracle.com>.
2. Enter the name of your **Cloud Account Administrator** in the **Cloud Account Name** field and click **Next**.
3. On the Cloud Infrastructure sign-in page, enter your sign-in credentials under **Oracle Cloud Infrastructure Direct Sign-In**. Click **Sign In**.
4. Click the  icon in the top left corner to display the navigation menu.
5. Click **Identity and Security** in the navigation menu
6. Select **Access Governance** from the list of products.
7. On the **Service Instances** page, select the newly created service instance.
8. Click **Service Home Page** to access the Oracle Access Governance Console in a browser.

2

Administer

System Administration

Performance Tuning

Tuning Runtime Configuration

The table below lists the parameters for fine tuning the runtime configuration of the connected system agent, and suggests specific values for small, medium, and large scale implementations.

Details of how to configure these parameters can be found in Agent Parameters.

Parameter	Description	Small Scale	Medium Scale	Large Scale
idoConfig.sparkMaxResultSizeInGB	Limit of total size of serialized results of all partitions for each action (e.g. collect) in bytes. Should be at least 1M, or 0 for unlimited. Jobs will be aborted if the total size is above this limit. Having a high limit may cause out-of-memory errors in driver (depends on spark.driver.memory and memory overhead of objects in JVM). Setting a proper limit can protect the driver from out-of-memory errors.	2	5	7

Parameter	Description	Small Scale	Medium Scale	Large Scale
idoConfig.sparkExecutorMemoryInGB	Amount of additional memory to be allocated per executor process, in MiB unless otherwise specified. This is memory that accounts for things like VM overheads, interned strings, other native overheads, etc.	2	5	7
idoConfig.numberOfPartition	Number of partitions.	3	5	7

Sizing Virtual Machine/Host

The table below suggests values for sizing your connected system agent VM or host for small, medium, and large scale implementations.

Parameter	Description	Small Scale	Medium Scale	Large Scale
CPU Cores	Number of CPU Cores.	2	4	8
Memory	Amount of memory (GB)	16	32	64


Manage Settings

Product-wide settings for Oracle Access Governance can be managed in the Oracle Cloud Infrastructure Console.

Set Notification Email

You can set the notification email in the Oracle Cloud Infrastructure Console.

The notification email for Oracle Access Governance defines the sender email address that is used to send all notifications regarding campaigns to your users. Only one sender's email address can be active at any given point in time. The sender's email address must be verified before it becomes active. To set the notification email for Oracle Access Governance, you should perform the tasks detailed in this topic:

1. Log in to the Oracle Cloud Infrastructure Console as a user with the Oracle Access Governance *Administrator* application role.
2. Click the  in the top left corner to display the navigation menu.
3. Click **Identity and Security** in the navigation menu.
4. Select **Access Governance** from the list of products.
5. Select **Settings** menu.

6. In the **Notification email** section, enter the following details:

- **From email address:**

Enter the email address you want to appear in the From field for all email notifications.

 **Note:**

Initially, the email address defined here will show with a status of **Pending email verification**. A verification email is sent to the address defined. Once verified, the email address shows a status of **Email Verified**.

 **Note:**

To maintain the credibility of the sender domain, it is recommended that you configure Sender Policy Framework (SPF) and DomainKeys Identified Email (DKIM) for your email domain.

- **Inbox configured:**

Check this box if the email address entered has an Inbox configured to receive the verification email. If unchecked then the verification email is sent to the postmaster account of the email domain. If the postmaster account verifies the domain, any email address from that domain can be set as the sender's email address without having to perform the verification process.

- **Display name:** Optionally, enter a display name for the sender's email address.

Set Up Service Instance

Regions

You can create an Oracle Access Governance service instance in the following regions: US East (Ashburn) for North America, Brazil East (Sao Paulo) for South America, Germany Central (Frankfurt) or UAE Central (Abu Dhabi) for Europe, and Australia East (Sydney) for Asia-Pacific. When you login to your tenancy, depending on your home region, chose the region hosting Oracle Access Governance within your geographic region to create and manage service instances. The tables below list the home regions that support Oracle Access Governance and which region they need to have a subscription for to access the Oracle Access Governance service.

North America

If you have an Oracle Cloud Infrastructure tenancy in one of the below home regions, you must have a subscription to the **US East (Ashburn)** region to be able to access the Oracle Access Governance service.

Region Name	Region Identifier	Region Location	Region Key	Realm Key	Availability Domains
Canada Southeast (Montreal)	ca-montreal-1	Montreal, Canada	YUL	OC1	1
Canada Southeast (Toronto)	ca-toronto-1	Toronto, Canada	YYZ	OC1	1
US East (Ashburn)	us-ashburn-1	Ashburn, VA	IAD	OC1	3
US West (Phoenix)	us-phoenix-1	Phoenix, AZ	PHX	OC1	3
US West (San Jose)	us-sanjose-1	San Jose, CA	SJC	OC1	1

South America

If you have an Oracle Cloud Infrastructure tenancy in one of the below home regions, you must have a subscription to the **Brazil East (Sao Paulo)** region to be able to access the Oracle Access Governance service.

Region Name	Region Identifier	Region Location	Region Key	Realm Key	Availability Domains
Brazil East (Sao Paulo)	sa-saopaulo-1	Sao Paulo, Brazil	GRU	OC1	1
Brazil Southeast (Vinhedo)	sa-vinhedo-1	Vinhedo, Brazil	VCP	OC1	1
Chile (Santiago)	sa-santiago-1	Santiago, Chile	SCL	OC1	1

Europe

If you have an Oracle Cloud Infrastructure tenancy in one of the below home regions, you must have a subscription to the **Germany Central (Frankfurt)** or the **UAE Central (Abu Dhabi)** region to be able to access the Oracle Access Governance service.

Region Name	Region Identifier	Region Location	Region Key	Realm Key	Availability Domains
France Central (Paris)	eu-paris-1	Paris, France	CDG	OC1	1
France South (Marseille)	eu-marseille-1	Marseille, France	MRS	OC1	1
Germany Central (Frankfurt)	eu-frankfurt-1	Frankfurt, Germany	FRA	OC1	3
Israel Central (Jerusalem)	il-jerusalem-1	Jerusalem, Israel	MTZ	OC1	1

Region Name	Region Identifier	Region Location	Region Key	Realm Key	Availability Domains
Italy Northwest (Milan)	eu-milan-1	Milan, Italy	LIN	OC1	1
Netherlands Northwest (Amsterdam)	eu-amsterdam-1	Amsterdam, Netherlands	AMS	OC1	1
Saudi Arabia West (Jeddah)	me-jeddah-1	Jeddah, Saudi Arabia	JED	OC1	1
South Africa Central (Johannesburg)	af-johannesburg-1	Johannesburg, South Africa	JNB	OC1	1
Sweden Central (Stockholm)	eu-stockholm-1	Stockholm, Sweden	ARN	OC1	1
Switzerland North (Zurich)	eu-zurich-1	Zurich, Switzerland	ZRH	OC1	1
UAE Central (Abu Dhabi)	me-abudhabi-1	Abu Dhabi, UAE	AUH	OC1	1
UAE East (Dubai)	me-dubai-1	Dubai, UAE	DXB	OC1	1
UK South (London)	uk-london-1	London, United Kingdom	LHR	OC1	3
UK West (Newport)	uk-cardiff-1	Newport, United Kingdom	CWL	OC1	1

Asia-Pacific

If you have an Oracle Cloud Infrastructure tenancy in one of the below home regions, you must have a subscription to the **Australia East (Sydney)** region to be able to access the Oracle Access Governance service.

Region Name	Region Identifier	Region Location	Region Key	Realm Key	Availability Domains
Australia East (Sydney)	ap-sydney-1	Sydney, Australia	SYD	OC1	1
Australia Southeast (Melbourne)	ap-melbourne-1	Melbourne, Australia	MEL	OC1	1
India South (Hyderabad)	ap-hyderabad-1	Hyderabad, India	HYD	OC1	1
India West (Mumbai)	ap-mumbai-1	Mumbai, India	BOM	OC1	1
Japan Central (Osaka)	ap-osaka-1	Osaka, Japan	KIX	OC1	1

Region Name	Region Identifier	Region Location	Region Key	Realm Key	Availability Domains
Japan East (Tokyo)	ap-tokyo-1	Tokyo, Japan	NRT	OC1	1
Singapore (Singapore)	ap-singapore-1	Singapore, Singapore	SIN	OC1	1
South Korea Central (Seoul)	ap-seoul-1	Seoul, South Korea	ICN	OC1	1
South Korea North (Chuncheon)	ap-chuncheon-1	Chuncheon, South Korea	YNY	OC1	1

 **Note:**

You cannot access the Oracle Access Governance service from a subscription to a region outside your geographical region. An example would be if your home region is **UK South (London)** then you cannot access the service with a subscription to **US East (Ashburn)**, you must have a subscription to **Germany Central (Frankfurt)** within your geographical region.

Prerequisites

A prerequisite for creating and setting up a service instance is to provide permissions for **agcs-instance** resources.


In order to create, update, or delete an Oracle Access Governance service instance, the Oracle Cloud Infrastructure Identity and Access Management administrator or domain administrator can create a group and allow that group permissions to manage **agcs-instance** resources for a given compartment or tenancy in a policy statement:

1. Examples for Tenancies using Identity Domain:
 - a. Allow group <domain_name>/<group_name> to manage **agcs-instance** in compartment <compartment_name>
 - b. Allow group <domain_name>/<group_name> to manage **all-resources** in compartment <compartment_name>
2. Examples for Tenancies without Identity Domain:
 - a. Allow group <group_name> to manage **agcs-instance** in compartment <compartment_name>
 - b. Allow group <group_name> to manage all-resources in in compartment <compartment_name>


Create Service Instance

Create an Oracle Access Governance instance in the Oracle Cloud Infrastructure console.

You can create an Oracle Access Governance service instance using the following steps:

1. Open your web browser and navigate to <https://cloud.oracle.com>.
2. Enter the name of your **Cloud Account Administrator** in the **Cloud Account Name** field and click **Next**.
3. On the Cloud Infrastructure sign-in page, enter your sign-in credentials under **Oracle Cloud Infrastructure Direct Sign-In**. Click **Sign In**.
4. When you have successfully logged in, select **Regions** → [**US East (Ashburn)**]**Brazil East (Sao Paulo)**]**Germany Central (Frankfurt)**]**Australia East (Sydney)**], depending on your Home region location, from the top navigation menu.
5. Click the  icon in the top left corner to display the navigation menu.
6. Click **Identity and Security** in the navigation menu.
7. Select **Access Governance** from the list of products.
8. On the **Service Instances** page, click the **Create service instance** button.
9. Enter values for the service instance as detailed in the following table .

Parameter	Value	Description
Name		Name of the service instance.
Description		Description of the service instance.
Create in compartment	Compartment Name into which the service instance will be created.	Name of the OCI compartment into which the service instance will be created.


Parameter	Value	Description
License type		<p>Select from the following license types:</p> <ul style="list-style-type: none"> Access Governance for Oracle Workloads: Governance of access privileges for Oracle Workloads running anywhere Access Governance for Oracle Cloud Infrastructure: Governance of access privileges for OCI resources and services.
		<p> Note:</p> <p>Access Governance for OCI is the entry level license option, covering OCI in cloud environments. Access Governance for Oracle Workloads is a broader option, covering Oracle Workloads running anywhere, and includes OCI.</p>
Tagging		<p>Tags allow you to organize and track resources within your tenancy. If you want to tag resources within the service instance, add them here. Add value as described in the following rows. If you want to add additional tags, select Another Tag to create more.</p>
	TAG NAMESPACE	Namespace to which the tag applies.
	TAG KEY	Key for the tag.
	TAG VALUE	Value of the tag.

- To create the service instance with the value you have input, select **Create service instance**. If you do not want to proceed with the service creation, select **Cancel**.

Verify Service Instance

You can verify an Oracle Access Governance service instance using the following steps:

- Open your web browser and navigate to <https://cloud.oracle.com>.

2. Enter the name of your **Cloud Account Administrator** in the **Cloud Account Name** field and click **Next**.
3. On the Cloud Infrastructure sign-in page, enter your sign-in credentials under **Oracle Cloud Infrastructure Direct Sign-In**. Click **Sign In**.
4. Click the  icon in the top left corner to display the navigation menu.
5. Click **Identity and Security** in the navigation menu
6. Select **Access Governance** from the list of products.
7. On the **Service Instances** page, select the newly created service instance.
8. Click **Service Home Page** to access the Oracle Access Governance Console in a browser.



Manage Service Instance

You can manage an Oracle Access Governance instance in the Oracle Cloud Infrastructure Console. The steps below show you how to perform management tasks on your service instance using the Oracle Cloud Infrastructure Console.

Review Service Instance

As *Cloud Account Administrator*, you can review Oracle Access Governance instances in the Oracle Cloud Infrastructure Console.


To review the details of a service instance, use the tasks detailed in this section:

1. Open your web browser and navigate to <https://cloud.oracle.com>.
2. Enter the name of your **Cloud Account Administrator** in the **Cloud Account Name** field and click **Next**.
3. On the Cloud Infrastructure sign-in page, enter your sign-in credentials under **Oracle Cloud Infrastructure Direct Sign-In**. Click **Sign In**.
4. Click the  icon in the top left corner to display the navigation menu.
5. Click **Identity and Security** in the navigation menu
6. Select **Access Governance** from the list of products.
7. On the **Access Governance** page, select **Service Instances**.
8. Click the **Actions** menu  for the service instance that you want to review.
9. Select **View details**.
10. Review the information for the service instance in the **Service Instance Details** page.


Launch Service Home Page

As a *Cloud Account Administrator*, you can launch the service home page for Oracle Access Governance from the Oracle Cloud Infrastructure Console.

To launch the service home page:

1. Open your web browser and navigate to <https://cloud.oracle.com>.
2. Enter the name of your **Cloud Account Administrator** in the **Cloud Account Name** field and click **Next**.
3. On the Cloud Infrastructure sign-in page, enter your sign-in credentials under **Oracle Cloud Infrastructure Direct Sign-In**. Click **Sign In**.
4. Click the  icon in the top left corner to display the navigation menu.
5. Click **Identity and Security** in the navigation menu
6. Select **Access Governance** from the list of products.
7. On the **Access Governance** page, select **Service Instances**.




8. Click the **Actions** menu  for the service instance that you want to review.
9. Select **Service home page**.
10. Perform activities in the Oracle Access Governance Console.


Edit Service Instance

As a *Cloud Account Administrator*, you can edit an Oracle Access Governance service instance from the Oracle Cloud Infrastructure Console.

To edit a service instance:

1. Open your web browser and navigate to <https://cloud.oracle.com>.
2. Enter the name of your **Cloud Account Administrator** in the **Cloud Account Name** field and click **Next**.
3. On the Cloud Infrastructure sign-in page, enter your sign-in credentials under **Oracle Cloud Infrastructure Direct Sign-In**. Click **Sign In**.
4. Click the  icon in the top left corner to display the navigation menu.
5. Click **Identity and Security** in the navigation menu
6. Select **Access Governance** from the list of products.
7. On the **Access Governance** page, select **Service Instances**.





8. Click the **Actions** menu  for the service instance that you want to review.
9. Select **Edit**.
10. The *Cloud Account Administrator* can update the name and description of the service selected.

Delete Service Instance

As a *Cloud Account Administrator*, you can delete an Oracle Access Governance service instance from the Oracle Cloud Infrastructure Console.

To delete a service instance:


1. Open your web browser and navigate to <https://cloud.oracle.com>.
2. Enter the name of your **Cloud Account Administrator** in the **Cloud Account Name** field and click **Next**.
3. On the Cloud Infrastructure sign-in page, enter your sign-in credentials under **Oracle Cloud Infrastructure Direct Sign-In**. Click **Sign In**.
4. Click the  icon in the top left corner to display the navigation menu.
5. Click **Identity and Security** in the navigation menu
6. Select **Access Governance** from the list of products.
7. On the **Access Governance** page, select **Service Instances**.
8. Click the **Actions** menu  for the service instance that you want to review.
9. Select **Delete**.
10. The service instance is marked for deletion. The service URL to the Oracle Access Governance Console is inaccessible to all users.

Service Administration

Activate/Inactivate Identities for License Management

Navigate to Manage Identities

Here's how you can access the Manage Identities page:

1. Log in to the Oracle Access Governance Console as a user with the *Administrator* application role.
2. Click  in the top left corner to display the navigation menu.
3. Select **Service Administration** → **Manage Identities** to begin defining your identity rules.

The Manage Identities page is displayed, where you have to define which identities you want to activate.

Select Identities for Activation

In the **Manage Identities** page, an Administrator defines the identities that you want to include in the Oracle Access Governance service.

You can identify identities to include in your service by selecting criteria based on conditional statements. Either at least one (**Any**) or all (**All**) the set conditions must be satisfied. The list of available attributes is determined by the ingested data from the connected systems, and may include custom attributes.

To activate identities in your service, do the following:

1. Select **Any** if any one of the set conditions should be satisfied, or select **All** if all the set conditions must be satisfied for that identity.
2. Select the attribute name from the list
You can select both standard and/or custom attributes. The list of attributes available for selection is determined by whether the specific attribute has the **Include in manage identities** option selected in the **Identity Attributes** page. To see how to include an attribute see *Modify Attribute Settings*.
3. Select the conditional operator. Based on the data type of the attribute selected, the usage of these operators will vary.
4. Select or type the attribute value.
5. Continue to add the conditional statements or rules for more attributes.
6. Once you have defined your rules, select **Preview summary based on the rule above** to go to the *Preview Summary* popup. This will display the following information, for the top 10 in each category:
 - Total number of matches based on the rules you have entered.
 - Total number of identities in the service.
 - Breakdown of the distribution of included identities based on:
 - Organization
 - Job code
 - Location
 - Employee type
7. When you are happy with the rules configured, select **Save** to save your included identities rules.

Note:

Existing customers with identities loaded from Oracle Identity Governance should be aware that they must activate identities required, else they will not be able to see loaded identities in the system as all identities are excluded by default. Customers in this situation can either activate users, as described above, or set the following rule which will activate all identities they previously loaded from Oracle Identity Governance.

```
status=Active
```

View and Configure Custom Identity Attributes

Overview

Oracle Access Governance automatically fetches custom attributes defined in a connected system. Details of custom attributes are automatically loaded into Oracle Access Governance when data is loaded from a connected system into Oracle Access Governance and you can run a refresh load to fetch the latest custom attributes, anytime post the connection.



Note:

To view the **Identity Attributes** option, you must activate at least one identity from the Manage Identities page. See [Select Included Identities](#) for details on how to enable identities in Oracle Access Governance.

You can use these custom attributes in Oracle Access Governance to perform various functions, such as running access reviews campaigns, choosing identities for identity collections, or applying attribute conditions to enable/disable the available identity data set.

To understand this better, let's look at a couple of examples:

- While creating a campaign, a *Campaign Administrator* selects custom attributes - *Cost Center* and *Department ID* to further refine the campaign selection criteria to run access review campaigns.
- While creating an identity collection, an *Administrator* can apply membership rules using the core and custom attributes. For instance, to create a senior management list of employees for the *Accounting* organization, create an identity collection to include employees where the *Job Level* is Director and above, and the *Organization* is Accounting.


Custom attributes are governed by certain assumptions and rules. Let's see a few of them:

- **Organization, Identity Location** and **Job Code** are the core attributes in the identity data. You can extend the schema definition, and use additional attributes in Oracle Access Governance features by defining custom attributes in your schema.
- A custom attribute that is encrypted in your schema will not be available in Oracle Access Governance and won't show up on the **Identity Attributes** page.

View Custom Attributes

As an *Administrator*, you can view, search, and configure the available custom attributes to use them across various Oracle Access Governance features.

Here's how you can view the available custom attributes:

1. In the Oracle Access Governance Console, from the  navigation menu, select **Administration**, and then select **Custom Identity Attributes**. The **Custom Identity Attributes** page is displayed. You can view the available custom attributes, and when the settings for these attributes were last updated for your organization.

Search and Filter Custom Attributes


Use the **Search** field to locate the required attribute by the attribute name. You can manage a large set of attributes by applying filters based on the following Oracle Access Governance features:

- **Campaign selections:** On or Off
- **Event-based:** On or Off
- **Manage identities:** On or Off
- **Identity details:** On or Off

View Attribute Details

You can view the following attribute details:

- **Attribute name:** Original attribute name as available in the data system that is connected with Oracle Access Governance.
- **Connected system:** Connected system name in Oracle Access Governance Console.
- **Display name:** Unique attribute name that will be used within Oracle Access Governance Console for easy identification and usage.
- **Type:** Data type of the attribute.
- Flags indicating where these custom attributes have been used:
 - **Identity details:** This selection will show custom attributes in the:
 - * Who Has Access to What functionality where you can view resource details for an identity.
 - * My Access Reviews functionality where you can perform access reviews and see review insights.
 - **Campaign selection:** This selection will show custom attributes to define user access review campaigns.
 - **Event-based Setup:** This selection will show custom attributes to configure event-based triggers for identity access reviews.
 - **Manage Identities:** This selection will show custom attributes to configure activation rules to manage identities from Oracle Access Governance, and to enable custom attributes in creating an identity collection.
- **Last updated by:** Name of the administrator who last modified the settings for that identity attribute.

Use the  Edit icon to edit the settings for that custom attribute.

Fetch Latest Custom Attributes

If you don't see the latest custom attributes in the list, click the **Fetch attributes** button.

This action will run the schema discovery on the connected system, and fetch the latest schema objects to get the updated list of custom attributes, if available. If new

custom attributes are available, then the schema discovery process may take a couple of minutes to complete, and show the updated list of custom attributes.

 **Note:**

If you have an encrypted attribute in your schema, then this process won't fetch and show up that encrypted attribute on this page.

Whenever a new custom attribute is added, you first need to enable that attribute for the features where you want to use it.


 **Note:**

This action won't ingest the attribute data from the connected system but will just load the schema objects. To fetch and use the attributes' data, you either have to wait for the next upcoming scheduled data sync operation or manually run the data load operation. See the Manage the Connected System topic.

Modify Attribute Settings

You can modify the custom attribute settings to include or exclude the use of these attributes for the Oracle Access Governance features.

Perform the following steps on the **Custom Identity Attributes** page:

1. Click the  icon corresponding to the custom attribute that you want to modify.
You will see the *Change custom identity attribute settings* pop-up window displaying the custom attribute name. You can also see the *Administrator* name who last updated the settings for this custom attribute.
2. As deemed necessary, update the following:
 - a. Update the **Display name**. This unique name will be used across Oracle Access Governance for this custom attribute.
 - b. Select the check box corresponding to the Oracle Access Governance features where you want to use this custom attribute. The available options are:
 - Include in identity details

 **Note:**

You can select up to 250 attributes for this feature.

- Include in event based access reviews
 - Include in campaign selections
 - Include in manage identities
3. Once you have selected your preferences, click **Apply**. Click **Cancel** to discard your changes.

Access Control Administration

Create Identity Collections


Identity Collections are identities grouped based on shared attributes or specific identities. These identities are on boarded from connected systems in Oracle Access Governance Console.

Identity Collections simplify tasks by allowing you to configure features for a collection of identities, rather than for each individual identity. In Oracle Access Governance, you can use Identity Collections to:

- Delegate Access Review tasks to an Identity Collection.

Navigate to Identity Collections

Here's how you can access the Identity Collections page:

1. Sign in to the Oracle Access Governance Console .
2. Click the  icon, and select **Access Controls** and then **Identity Collections**. You will see the **Identity Collections** page where you can view and manage the existing identity collections.
3. To create a new identity collection, click the **Create an identity collection** button.

The **Create a new identity collection** page is displayed.

Add Details

In the **Add Details** task, you can enter specifics about your identity collection. Here, you can give a meaningful name to your identity collection and add its supporting description.



Note:

By default, for all identities enabled in the Manage Identities service, all identity data attributes including custom attributes ingested from the connected systems are available to create identity collections.

1. Enter name for your identity collection in the **What do you want to call this identity collection?** field.
2. Add a description for your identity collection in the **How would you describe this collection?** field.
3. Add or select one or more identities name in the **Who can manage this identity collection** list. The owner along with the listed identities can manage this identity collection.
4. Add one or more tags to identify or search your identity collection.

5. Once you have set your preferences, select **Next** to go to the *Select Identities* step.
6. Optional: You may click **Cancel** to cancel the current process.

Select Identities

In the **Select Identities** task, you have to select identities for your identity collection.

You can select identities based on:

- **Membership rule:** Set criteria based on certain conditional statements. Either one (**Any**) or all (**All**) the set conditions must be satisfied. The list of available attributes is determined by the ingested data from the connected systems.
- **Named identities:** Search and select one or more users by their full name that you want to include in your identity collection. The list of available users is determined by the ingested data from the connected systems.
- **Both Membership rule and Named identities:** You can have a combination of both membership rule and named identities to set criteria for your identity collection.



Note:

You can also exclude specific members from your identity collection.

Add Identities based on Membership Rule

To add identities based on conditional statements, select the **Membership rule** tab.

The identities satisfying the set criteria will automatically be included in that identity collection. For example, for an identity collection, if you set the conditional rule to **Department Equals Finance**, then all the human identities belonging to the Finance department will be included in that identity collection.

To set the conditional rule for identities, do the following:

1. Select **Any** if any one of the set conditions should be satisfied, or select **All** if all the set conditions must be satisfied for that identity.
2. Select the attribute name from the list



Note:

Based on the connected systems, you can select both core and/or custom attributes. To enable custom attributes, see [View and Configure Custom Identity Attributes](#)

3. Select the conditional operator. Based on the data type of the attribute selected, the usage of these operators will vary.
4. Type the attribute value.
5. Continue to add the conditional statements or rules for more attributes. By default all the identities matching the criteria will be included.
6. However, you can exclude certain identities from your conditional statements.

Click the **Manage Exclusions** button next to **Excluding # identity from the attribute conditions** and then select the identities that you want to exclude from the identity collection.

As you set the conditions or add identities, you can see the effect on the right-side of the screen of which identities are excluded and the applied membership rule.

7. Once you have set your preferences, select **Next** to go to the *Review and submit* step. You may select one of the additional actions:
 - **Save as draft**: To save your changes and later come back and edit the identities.
 - **Cancel**: To cancel the current process.
 - **Back**: To go back to the previous step.

Add Identities based on Named Identities

To directly add identities based on their full name, select the **Included named identities** tab.

All the available active identities (configured from the Manage Identities page) will be displayed. In the user tile, you can view user details, such as full name, email address, organization name. Search or select one or more user tile that you want to include in your identity collection. As you select the identities, you can see the effect on the right-side of the screen of which identities are included. Once you have set your preferences, select **Next** to go to the *Review and submit* step.

Review and Submit

The Review and Submit step displays the information you have added in the previous steps.

You can see the preview of your identity collection. For this, click the **preview the identity collection** link available on the right-side of the page. If you are satisfied with your identity collection preview, click **Create**. You may select addition actions:

- **Save as draft**: to save your changes and edit the identity collection later.
- **Cancel**: To cancel the process.
- **Back**: To go back to the previous step.

Manage Identity Collections


Oracle Access Governance users can view and manage identity collection from the Oracle Access Governance Console.

View and Manage Identity Collections

You can view existing identity collections and manage the ones that you created.

Follow the steps to navigate to the **Identity Collections** screen:


1. Sign in to the Oracle Access Governance Console .

- Click the  icon, and select **Access Controls** and then select **Identity Collections**. The **Identity Collections** screen is displayed where you can view and manage the existing identity collections.

Here, you can see the count of existing identity collections and the details are listed in the grid that includes:

- **Name:** Identity collection name.
- **Status: Active or Draft**
- **Owner:** Name of the owner who created this identity collection.
- **Last updated:** Date on which the identity collection was last modified.
- **Tags:** User-defined tags for quick search and easy identification of the identity collection.



Use the  *Actions* menu icon to **Edit, Delete or View Details** of the identity collection.

**Note:**

Users who own the identity collection or authorized users (selected while creating/modifying an identity collection) can edit or delete the identity collection.

Search and Filter Identity Collections

You can use the **Search** field to locate the required identity collection by its name. You can narrow down the results by applying filters:

- **Updated Last Month:** You can view all the identity collections that were updated within the last month.
- **Updated Last Week:** You can view all the identity collections that were updated within the last week.
- **Created by Me:** You can view the identity collections that you have created.
- **Status Draft:** You can view the identity collections that haven't been created and are in the draft state.
- **Status Active:** You can view the identity collections that have been created and can be used within Oracle Access Governance.


Edit an Identity Collection

The **Edit an Identity Collection** page provides the same guided tasks as you see while creating a new identity collection.

Owner of the identity collection and/or authorized users can modify its description, identity type, or added identities.

To do so:




- Click the  *Actions* menu icon corresponding to the identity collection that you want to modify, and then select **Edit**.

After updating your identity collection details, on the *Review and submit* step, select **Update** to update the campaign. Alternatively you can select **Back** to edit values, or select **Cancel** to discard your changes.

View Details for an Identity Collection



- Click the  *Actions* menu icon corresponding to the identity collection that you want to view, and then select **View Details**. You will see the *Identity Collections* page displaying the details, such as *Identities*, *Identity Type*, *Created by*, and *Last updated*.

On the left panel, you will see the following details:

- In the donut chart, you can see the total count of identities, and break up of identities in the collection that are included either through **Membership rule** or directly through **Included named identities**.
- If you have created an identity collection through **Membership rule**, you can see all the rules that helped to create the collection.
- If you have excluded an identity in the collection, you can see a list of excluded member(s).
- If you have created an identity collection directly using named identities, you can see a list included member(s).


On the rest of the page, you will see the identity names and their details in a tile format. You can search an identity using identity name.

Use the *Actions* menu to either **Edit** or **Delete** the identity collection. Owner of the identity collection and/or authorized users can edit or delete the identity collection.

Delete and Identity Collection

You can delete an identity collection as long as it is not associated with any delegation. If you are the owner of the identity collection or you have been given the rights by the identity collection creator, then you can delete the identity collection.



1. Click the  *Actions* menu icon corresponding to the identity collection that you want to delete, and then select **Delete**.
2. On the confirmation pop-up, click **Delete** to remove the identity collection or click **Cancel** to retain the identity collection.

Preferences

Manage Delegation Preferences

In Oracle Access Governance you can set up and manage preferences.

Users can delegate tasks/activities using the Oracle Access Governance. You can use the **My Preferences** setting to assign tasks/activities to another user or identity collection. You can choose when to start this delegation process and also specify the duration of the delegation. In Oracle Access Governance, you can delegate:

- **Access Reviews:** Some other user or identity collection can perform access reviews on your behalf

 **Note:**

You can access the **My Preferences** settings by clicking the user name located at the top-right corner of the Oracle Access Governance landing page.

You may want to delegate approvals or access reviews for the following reasons:

- Unavailability because of vacation, sickness, or working on other tasks.
- To have the most qualified person to make the decisions.
- Develop someone else's ability to handle additional assignments.

Set up Your Delegation Preferences

Perform the following steps to navigate to the **My Preferences** screen:

1. Log in to the Oracle Access Governance Console.
2. On the console home page, click on the username, located at the top-right corner of the screen, and then click

Perform the following steps to add a new delegation:

1. In the My Preferences screen, click the **Add a delegation** button. You will be navigated to the Add a delegation pop-up window.
2. The field **Who do you want to delegate to?** allows you to either delegate the selected task to an individual or an identity collection.
 - If **An individual** option is selected, enter the name of the delegator in the **Who?** field
 - If **An identity collection** option is selected, enter the name of the identity collection group in the **Who?** field

 **Note:**

The Identity collection can have one or more than one member in it.

3. Select the date range for the delegation from the **How long do you want the delegation to last?** field. It can be either an indefinite time or a specific time range. Selecting:
 - **Indefinitely:** Allows you to set the delegation for an indefinite time.

- **During a time range:** Allows you to select a date range for the delegation.
4. Click **Save**.

Tasks or activities created after assigning a delegate is visible on both the dashboards of the delegator (the one who delegated the task) and the delegate (the one to whom the task/activity was delegated to).

**Note:**

Tasks or activities that were created before delegation will not appear on the delegate's dashboard.

Edit a Delegation

Perform the following steps to edit a delegation:

1. In the My Preferences screen, click the **Edit** button.
You will be navigated to the Edit pop-up window.
2. The field **Who do you want to delegate to?** allows you to either modify the individual name or the identity collection name based on your selection.


**Note:**

The Identity collection can have one or more than one member in it.

3. Select the date range for the delegation from the **How long do you want the delegation to last?** field. It can be either an indefinite time or a specific time range. Selecting:
 - **Indefinitely:** Allows you to set the delegation for an indefinite time.
 - **During a time range:** Allows you to select a date range for the delegation.
4. Click **Save**.
You will be navigated to the **My Preferences** screen.

Delete a Delegation

Perform the following steps to delete a delegation:

1. In the My Preferences screen, click the  button.
2. In the Confirmation pop up, select **Delete** to remove the delegation or **Cancel** to retain the delegation.
You will navigated back to the **My Preferences** screen.

3

Integrate

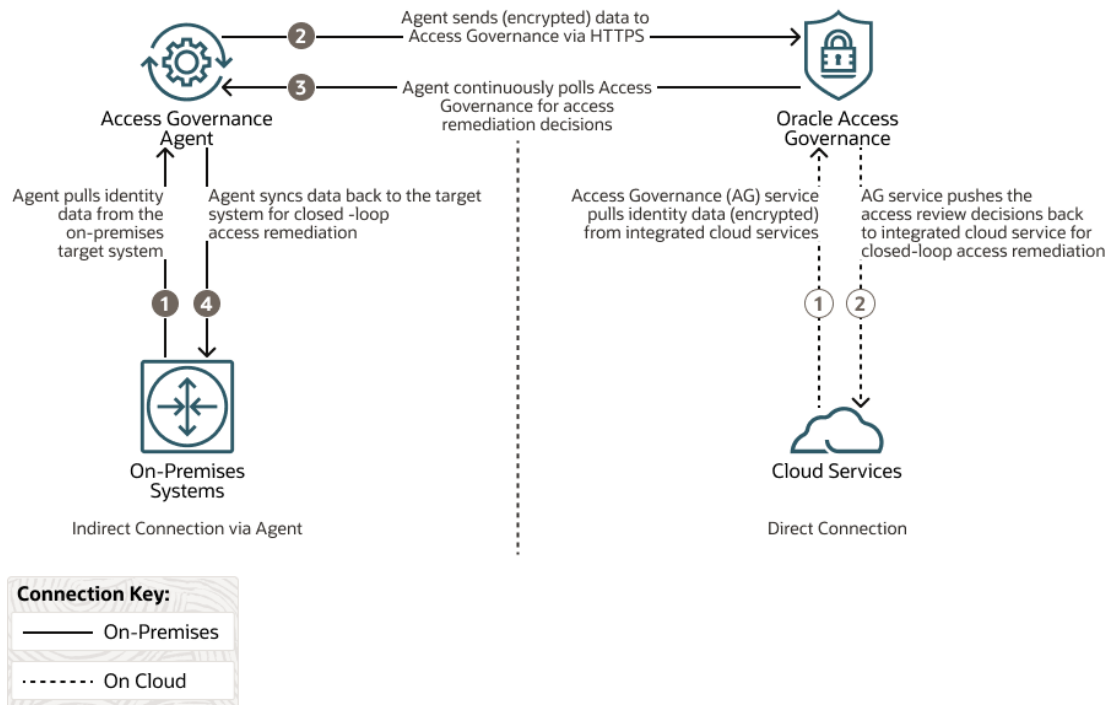
Getting Started with Integration

Access Governance Integration with Connected Systems

Connected Systems Overview

Oracle Access Governance can be integrated with target identity systems by defining a connected system.

A connected system allows you to load data from a remote target identity system into Oracle Access Governance. The connected system will define parameters such as connection details that are required to access remote identity data. Where a direct connection between Oracle Access Governance and the target identity system is not possible, an agent may be deployed to bridge between the two.



Integration Concepts

Identity Orchestration in Oracle Access Governance is made up of the following components:

- **Connected System:** A connected system is the footprint definition for a target identity system that can be integrated with and provide data to Oracle Access Governance. Once defined, the connected system enables integration and data synchronization between target identity systems and Oracle Access Governance, through either a direct connection or an agent.
- **Oracle Access Governance Console:** The Oracle Access Governance Console allows users with the *Administrators* application role, to register the connected system, download the agent docker image where connection to the target system is indirect, and configure and monitor the progress of the connected system in real-time. The Oracle Access Governance Console also supports life cycle activity such as resetting the connected system status to trigger full or incremental synchronization, or disable or enable the connected system.
- **Agent:**

The Oracle Access Governance agent is a docker image-based agent, which allows Oracle Access Governance to synchronize continuously or periodically with target identity systems where a direct connection is not available. The agent runs scheduled distributed extract-transform-load (ETL) jobs to perform full or incremental synchronization of remote identity data, such as users, roles, application instances, entitlements, and entitlement assignments, to Oracle Access Governance. Once registered and installed, the agent can be monitored via the Oracle Access Governance Console. The agent runs in a docker environment located at the customer. This environment should meet the following prerequisites:

 - Installation of Docker or Podman
 - Allow connection to the customer's target identity database
 - Allow connection to the customer's Oracle Access Governance instance hosted in Oracle Cloud.

The agent uses the configuration entered in Oracle Access Governance to connect to the connected system. The agent extracts data from the connected system, transforms it, and then pushes it to Oracle Cloud Infrastructure Object Storage over HTTPS. Once transferred to object storage, the data is then picked up by the Oracle Access Governance ingestion service and is loaded into Oracle Access Governance for consumption. On completion of access review campaigns, any permissions that have been revoked in Oracle Access Governance will be remediated by raising a revoke operation in the connected system. This revoke request will be passed to the connected system via the agent.

Agents are applicable only in cases where a direct connection cannot be established with Oracle Access Governance. Typically, you will need an agent when integrating with the on-premises target systems. The Oracle Access Governance agent acts as an arbitrator supporting synchronization of identity data between target systems and Oracle Access Governance.

Manage the Connected System

The connected system can be added and managed from the Oracle Access Governance Console.

 **Note:**

The connection details depends on the type of connected system. This section explains the Manage Connected System screen, and lists the general steps to manage the connected systems. Refer documentation on integration with target systems to connect to a specific target system.

- [Integrate with Oracle Identity Governance](#)

In the Oracle Access Governance Console, from the navigation menu, select **Service Administration** → **Connected Systems**, and then select **Add a connected system** to add a new connected system, or select **Service Administration** → **Connected Systems** to manage the existing connected systems.


On the **Manage Connected System** screen, for each connected system, you can view a list of activities, their statuses, when they were initiated, total time taken to complete each activity, and name of the user who performed that activity. You can also initiate a data load, update connection settings, and disable the connected system.

In the **Activity Log**, you can view the following activities:

- **Data load:** Initiates when the data is either run on-demand by the Administrator, or when data is auto-synced as per the system settings. Currently, the data automatically refreshes after 24 hours from the previous data load activity.
- **Full data load:** Initiates when the data is synced for the first time after the new connection is established.
- **Validate:** Initiates when a new connection is established or when you update the connection settings.
- **Revoke:** Initiates when an access reviewer revokes one or more user privileges in the access review tasks. This activity occurs to support closed-loop access remediation.
- **Schema discovery:** Initiates when a new connection is established, or when you select the Fetch attributes button in the *Custom Identity Attributes* page.


Data Load

To initiate a data load from the target connected system instance, perform the following tasks.

1. In the Oracle Access Governance Console, access the navigation menu by selecting the  icon. Select **Service Administration** → **Connected Systems**.
2. In the **Connected Systems** screen, select the **Manage** button for the Oracle Access Governance connected system you want to manage.
3. Select the **Load data now** option from the **Actions** drop-down menu in the top right-hand corner. This will initiate a data load and you can track the status in the **Activity Log**.

Update Connection Details


To update the connection details used by the connected system to connect to the target identity system perform the following tasks.

1. In the Oracle Access Governance console, access the navigation menu by selecting the  icon. Select **Service Administration** → **Connected Systems**.

2. In the **Connected Systems** screen, select the **Manage** button for the connected system you want to update.
3. Select the **Change Settings** option from the **Actions** drop-down menu in the top right-hand corner. Update connection settings and click **Save**.

Disable the Connected System


To disable the agent from running, perform the following tasks.

1. In the Oracle Access Governance Console, access the navigation menu by selecting the  icon. Select **Service Administration** → **Connected Systems**.
2. In the **Connected Systems** screen, select the **Manage** button for the connected system you want to disable.
3. Select the **Disable** button in the top right-hand corner. The agent will display a status of **Disabled** on the **Connected Systems** page.

Agent Administration

Register and Download a Connected System Agent

In some cases, a connected system does not have a direct connection to Oracle Access Governance and requires an agent to enable data transfer between Oracle Access Governance and the connected system. To enable a connected system agent to connect to Oracle Access Governance, you need to enter connection details and credentials for the target system and build an agent specific to your environment.

1. In a browser, navigate to the Oracle Access Governance service home page and log in as a user with the *Administrator* application role.
2. On the Oracle Access Governance service home page, click on the  icon and select **Service Administration** and then **Connected Systems**.
3. On the tile labeled **Would you like to connect to an Identity Governance System**, select the **Add** button.
4. Click **Close** on the information pop-up to navigate to the **Add an Identity Governance System** page and begin the configuration.
5. On the **Select System** step, select the tile for the connected system you want to configure the agent for, and then click **Next**.
6. On the **Enter Details** step, enter the following details:
 - **Name**
 - **Description**Click **Next**.
7. On the **Configure** step, enter connection details for the target system:

 **Note:**

The connection details will differ depending on the type of connected system. Refer to the documentation for the connected system type you require for details.

[Integrate with Oracle Identity Governance](#)

8. On the **Download Agent** step, select the **Download** link and download the agent zip file to the environment in which the agent will run.

The contents of the agent package will look similar to the following:

```
agent-package-<version>.zip
- config.json
- wallet
  - cwallet.sso
  - cwallet.sso.lck
- container-image
  - agent.tar.gz
```

Prerequisites

Prerequisites for installation and running of a connected system agent.

The following prerequisites should be met in order to install and run a connected system agent.

1. **Container runtime:**
The agent management script supports **docker** and **podman** as the container runtime. The agent management script auto-detects the container runtime. If both are present, **podman** is selected.
2. **Utilities:**
A connected system agent requires the following operation system utilities:
 - a. **unzip**
 - b. **sed**
 - c. **awk**
3. **JDK**
A connected system agent requires **JDK 11.0.x**.

Agent Management Operations

Lists details of the operations that the agent can perform and related parameter descriptions.

The connected system agent can be managed using the `agentManagement.sh` script. This script can be downloaded from GitHub. The script supports `docker` and `podman`, it autodetects the container runtime available. If both are available, the script uses `podman`.

Operations

Operation	Description	Additional Information
<code>--install</code>	<ul style="list-style-type: none"> Installs the downloaded agent package to the specified volume. Loads the container image. 	Use <code>--config</code> to use a custom configuration.
<code>--start</code>	<ul style="list-style-type: none"> Starts the agent container. Starts the agent daemon. 	Use <code>--newcontainer</code> to start a new container. Use <code>--config</code> to use a custom configuration.
<code>--stop</code>	<ul style="list-style-type: none"> Stops the agent daemon. Stops the agent container. 	
<code>--restart</code>	<ul style="list-style-type: none"> Stops the agent daemon. Stops the agent container. Remove the agent container if <code>newcontainer</code> flag is set to true. Starts the agent container. Starts the agent daemon. 	
<code>--uninstall</code>	<ul style="list-style-type: none"> Stops the agent daemon. Remove the agent container. Clean up the volume. 	
<code>--upgrade</code>	<ul style="list-style-type: none"> Unzips new <code>agent-package.zip</code> in a temporary location. Validates the package contents. Loads the image from the new zip file. Starts a temporary container using the new image and configuration. If the temporary container has no issues then stop the container. Stop the existing container. Copy new configuration from the temporary location to the current location. This retains any customizations. Starts the agent with the new image and configuration. Starts the agent daemon. 	<p>The following changes require an upgrade where you will need to download the new agent package from the Oracle Access Governance Console, and invoke the upgrade operation.</p> <ul style="list-style-type: none"> Change in configuration (<code>config.json</code>) Connector bundle change Change in Wallet Change of agent image <p>The following changes will trigger a reconfigure operation which is handled by the agent framework.</p> <ul style="list-style-type: none"> Connector (same template version) Connector (different template version)

Operation	Description	Additional Information
<code>--status</code>	Lists the following details of the agent: <ul style="list-style-type: none"> • Agent ID • Container runtime and version • Agent package • Agent version • Install location • Agent state 	
<code>--enableautoupgrade</code>	Enables automatic upgrade by performing the following tasks: <ul style="list-style-type: none"> • Sets up a <code>cron</code> job to detect upgrades for any changes in target connectivity parameters, or in connector bundle code. • <code>cron</code> job runs every 24 hours and upgrades the agent automatically if required. 	
<code>--disableautoupgrade</code>	Disables automatic upgrades by removing the auto-upgrade <code>cron</code> job.	

Install Agent on Target System

To install the downloaded agent into your local system, perform the following steps:

1. Unzip the downloaded agent to your local location.

Contents of the unzipped agent should be:

```
agent-package-<version>.zip
- config.json
- wallet
  - cwallet.sso
  - cwallet.sso.lck
- container-image
  - agent.tar.gz
```

2. Run the management script with the following parameters:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/OracleIdentityGovernance/samples/scripts/agentManagement.sh -o agentManagement.sh ; sh agentManagement.sh \
--volume <PERSISTENT_VOLUME_LOCATION> \
--agentpackage <PACKAGE_FULL_PATH>\
--install
```

An example with default configuration would look like the following:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/OracleIdentityGovernance/samples/scripts/agentManagement.sh -o agentManagement.sh ; sh agentManagement.sh \
--volume /access-governance/agent-management/volume \
--agentpackage /access-governance/agent-management/agent-package-  
<version>.zip \
--agentid myagent \
--install
```

An example with custom configuration would look like the following:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/OracleIdentityGovernance/samples/scripts/agentManagement.sh -o agentManagement.sh ; sh agentManagement.sh \
--volume /access-governance/agent-management/volume \
--agentpackage /access-governance/agent-management/agent-package-  
<version>.zip \
--agentid myagent \
--config /access-governance/agent-management/config.properties \
--install
```

3. Start the agent with the following command:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/OracleIdentityGovernance/samples/scripts/agentManagement.sh -o agentManagement.sh ; sh agentManagement.sh \
--volume <PERSISTENT_VOLUME_LOCATION> \
--start
```


For example:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/OracleIdentityGovernance/samples/scripts/agentManagement.sh -o agentManagement.sh ; sh agentManagement.sh \
--volume /access-governance/agent-management/volume \
--start
```

Verify Agent

Details how to verify the installation and operation of the connected system agent.

To verify the installation of the connected system agent, complete the following steps:

1. In the Oracle Access Governance Console, select the  icon to display the navigation menu.
2. In the Oracle Access Governance Console, select **Service Administration** → **Connected Systems** from the navigation menu.
3. On the **Connected Systems** screen, the tile showing the Identity Data Orchestrator created in [Install Agent on Target System](#) shows a status of **Waiting for initial connection**. Click on **Manage** → **Troubleshooting Checklist**.

4. The **Activity Log** at the bottom of the page will show the status of the Validate operation, **Pending** while the agent comes up. If the agent does not come up, check the agent install and operation logs for any issues.
5. Once the agent has come up, the status of the Validate operation will show as **Success**.

Agent Example Usage

Displays examples of usage of the agent management script.

Once you have successfully installed and verified your agent, you can start to manage the lifecycle. The `agentManagement.sh` script provides support for the start, stop, restart, uninstall, and upgrade operations.

Start the Agent

You start the agent with the following command:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/OracleIdentityGovernance/samples/scripts/agentManagement.sh -o agentManagement.sh ; sh agentManagement.sh \
--volume <PERSISTENT_VOLUME_LOCATION> \
--start
```

For example:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/OracleIdentityGovernance/samples/scripts/agentManagement.sh -o agentManagement.sh ; sh agentManagement.sh \
--volume /access-governance/agent-management/volume \
--start
```

Stop the Agent

You stop the agent with the following command:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/OracleIdentityGovernance/samples/scripts/agentManagement.sh -o agentManagement.sh ; sh agentManagement.sh \
--volume <PERSISTENT_VOLUME_LOCATION> \
--stop
```

For example:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/OracleIdentityGovernance/samples/scripts/agentManagement.sh -o agentManagement.sh ; sh agentManagement.sh \
--volume /access-governance/agent-management/volume \
--stop
```

Restart the Agent

You restart the agent with the following command:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/OracleIdentityGovernance/samples/scripts/agentManagement.sh -o agentManagement.sh ; sh agentManagement.sh \
--volume <PERSISTENT_VOLUME_LOCATION> \
--restart
```

For example:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/OracleIdentityGovernance/samples/scripts/agentManagement.sh -o agentManagement.sh ; sh agentManagement.sh \
--volume /access-governance/agent-management/volume \
--restart
```

Uninstall the Agent

You uninstall the agent with the following command:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/OracleIdentityGovernance/samples/scripts/agentManagement.sh -o agentManagement.sh ; sh agentManagement.sh \
--volume <PERSISTENT_VOLUME_LOCATION> \
--uninstall
```

For example:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/OracleIdentityGovernance/samples/scripts/agentManagement.sh -o agentManagement.sh ; sh agentManagement.sh \
--volume /access-governance/agent-management/volume \
--uninstall
```

Upgrade the Agent

You upgrade the agent with the following command:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/OracleIdentityGovernance/samples/scripts/agentManagement.sh -o agentManagement.sh ; sh agentManagement.sh \
--volume <PERSISTENT_VOLUME_LOCATION> \
--agentpackage <NEW_PACKAGE_FULL_PATH> \
--upgrade
```

For example:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/OracleIdentityGovernance/samples/scripts/agentManagement.sh -o agentManagement.sh ; sh agentManagement.sh \
```



```
--volume /access-governance/agent-management/volume \  
--agentpackage /access-governance/agent-management/agent-package-  
<version>.zip \  
--upgrade
```

Enable Auto Upgrade

Enable auto upgrade with the following command:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/  
OracleIdentityGovernance/samples/scripts/agentManagement.sh -o  
agentManagement.sh; sh agentManagement.sh \  
--volume <PERSISTENT_VOLUME_LOCATION> \  
--enableautoupgrade
```

For example:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/  
OracleIdentityGovernance/samples/scripts/agentManagement.sh -o  
agentManagement.sh; sh agentManagement.sh \  
--volume /access-governance/agent-management/volume \  
--enableautoupgrade
```

Disable Auto Upgrade

Disable auto upgrade with the following command:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/  
OracleIdentityGovernance/samples/scripts/agentManagement.sh -o  
agentManagement.sh; sh agentManagement.sh \  
--volume <PERSISTENT_VOLUME_LOCATION> \  
--disableautoupgrade
```

For example:

```
curl https://raw.githubusercontent.com/oracle/docker-images/main/  
OracleIdentityGovernance/samples/scripts/agentManagement.sh -o  
agentManagement.sh; sh agentManagement.sh \  
--volume /access-governance/agent-management/volume \  
--disableautoupgrade
```

Integrate with Target Systems

Integrate with Oracle Identity Governance

Register and Download the Oracle Identity Governance Agent


To enable the Oracle Identity Governance agent to connect to Oracle Access Governance, you need to enter connection details and credentials for the target system and build an agent specific to your environment.

Note:

Oracle Access Governance supports building an agent for Oracle Identity Governance Version 12.2.1.4 Bundle Patch Number 11 (12.2.1.4.220703). If your current version of Oracle Identity Governance is not compatible then contact [Oracle Support](#), who can arrange a patch for your Oracle Identity Governance system

Note:

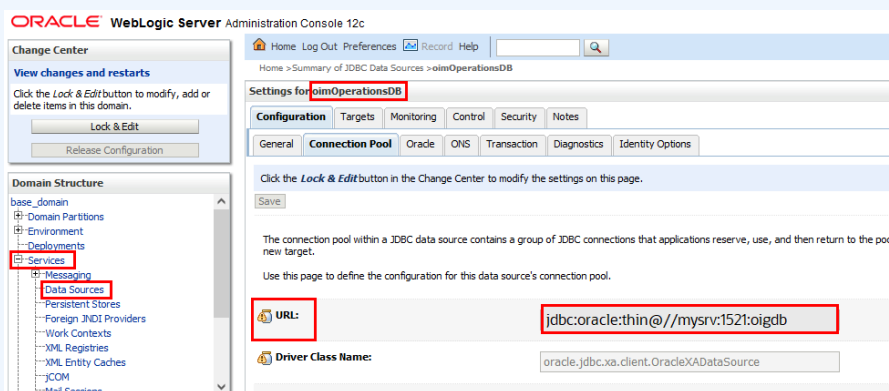
Applications in Oracle Identity Governance must be marked as **Certifiable** in order to be ingested by Oracle Access Governance. Log in to the Oracle Identity Governance Self Service application and navigate to **Request Access** → **Request for Self** → **[Search for Your App]** and click the information icon **Certifiable**.

1. In a browser, navigate to the Oracle Access Governance service home page and log in as a user with the *Administrator* application role.
2. On the Oracle Access Governance service home page, click on the  icon and select **Service Administration** and then **Connected Systems**.
3. Select **Add a connected system** to navigate to the **Add a Connected System** page and begin the configuration.
4. On the **Let's connect a system** step, select the tile for **Oracle Identity Governance** to configure the agent for a target Oracle Identity Governance connected system, and then click **Add**.
5. On the **Enter Details** step, enter the following details:
 - **Name**
 - **Description**Click **Next**.
6. On the **Configure** step, enter connection details for the target system:
 - **JDBC URL**: JDBC URL for the target OIG database.

 **Note:**

To obtain the JDBC URL:

- a. Log on to the Oracle WebLogic Server Administration Console associated with your Oracle Identity Governance instance.
- b. Navigate to **Services** → **Data Sources**.
- c. Select **oimOperationsDB** from the **Configurations** tab.
- d. Select **Connections Pool**, and copy the value from the **URL:** field to use as the JDBC URL for Oracle Identity Governance.



The screenshot shows the Oracle WebLogic Server Administration Console interface. On the left, the 'Domain Structure' tree is visible, with 'Services' and 'Data Sources' highlighted. The main area displays the 'Settings for oimOperationsDB' configuration page. The 'Configuration' tab is active, and the 'Connection Pool' sub-tab is selected. The 'URL:' field is highlighted with a red box and contains the value 'jdbc:oracle:thin://mysrv:1521:oigdb'. The 'Driver Class Name:' field contains 'oracle.jdbc.xa.client.OracleXADataSource'.

- **OIG Database User Name:** Database user to connect to the OIG database.

 **Note:**

This can be any user with read access to the OIG database.

- **Password:** Password for the OIG Database User Name.
- **Confirm Password:** Password for the OIG Database User Name.
- **OIG Server URL:** The URL of the target OIG server.

 **Note:**

To obtain the OIG Server URL:

- Log on to the Oracle Enterprise Manager Fusion Middleware Control.
- Navigate to the **System MBean Browser** and locate the **XMLConfig.DiscoveryConfig** MBean.
- Copy the value of the **OimExternalFrontEndURL** attribute and use this as the value for the Oracle Identity Governance Server URL.

4 Search Result

1 oracle.iam:Application=oim_Location=oim_server1/XMLConfig=Config,name=Discovery,type=XMLConfig.DiscoveryConfig

Application Defined MBeans: XMLConfig.DiscoveryConfig:Discovery

Information

The changes made on this mbean are not managed by the configuration session. The changes will be applied immediately. You cannot undo the changes from the Change Center.

Show MBean Information

Attributes Notifications

Name	Description	Access	Value
1 BackOfficeURL	Discovery Config back office URL	RW	
2 BIPublisherURL	Discovery Config BI publisher URL	RW	http://localhost:9704
3 ConfigMBean	If true, it indicates that this MBean is a Config MBean.	R	true
4 eventProvider	If true, it indicates that this MBean is an event provider as defin...	R	true
5 eventTypes	All the event's types emitted by this MBean.	R	jmx.attribute.change
6 objectName	The MBean's unique JMX name	R	oracle.iam.name=Discovery,type=XMLConfig.DiscoveryConfig/XMLConfig=Config,Application=oim
7 OimExternalFrontEndURL	Discovery Config OIM External front end URL	RW	http://mysrv:14000

- **OIG Server User Name:** OIG user used for remediation and schema discovery.

 **Note:**

The Oracle Identity Governance Server user can be any Oracle Identity Governance user that is a member of the **System Administrator** administration role. This role is required to perform the remediation process, and to support schema discovery for custom attributes. In the case where only remediation support is needed then user can be a member of the **OrclOAGIntegrationAdmin** administration role. With this user the schema discovery operation will fail.

 **Note:**

Information about the Oracle Identity Governance Server (URL, Username, and Password), and Oracle Identity Governance datasource (JDBC URL, Username, and Password) is required to integrate Oracle Access Governance and Oracle Identity Governance. Oracle Access Governance will use the Oracle Identity Governance data source to load the data and the Oracle Identity Governance Server URL to perform remediation operations. In case of a connection failure, the Oracle Access Governance agent automatically retries a maximum of three times to secure a connection with the Oracle Identity Governance server.

7. On the **Download Agent** step, select the **Download** link and download the agent zip file to the environment in which the agent will run.

After downloading the agent, follow the instructions explained in the [Agent Administration](#) article.

You can also follow the instructions provided in the [Set Up Identity Orchestration between Oracle Access Governance and Oracle Identity Governance \(OIG\)](#) tutorial.

Integrate with Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM)

You can establish a connection between Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) and Oracle Access Governance by entering connection details and configuring your cloud service provider environment. To achieve this, use the Connected Systems functionality available in the Oracle Access Governance Console.

Prerequisites

Before you can establish a connection, you need to create a policy in your cloud tenancy that allows the connector to access the target system.

The following prerequisites must be satisfied to integrate with Oracle Access Governance with OCI IAM:

- Your cloud account must use Identity Domains to manage identities on OCI.
- As a cloud administrator, you must be able to manage identities in the **Default** domain and manage policies in the **root compartment** of your tenancy.
- If you want to integrate an OCI tenancy to an Oracle Access Governance service instance outside the OCI tenancy's home region, your OCI tenancy must be subscribed to the region where Oracle Access Governance is running. For example, if your OCI tenancy is in Tokyo, and you want to integrate with Oracle Access Governance running in Ashburn, the Tokyo tenancy will need to be subscribed to the Ashburn region.


To allow Oracle Access Governance to connect OCI, you must set up the following policy in your cloud tenancy:

- ALLOW RESOURCE `accessgov-agent resource-scanner` to read all-resources IN TENANCY
- ALLOW RESOURCE `accessgov-agent resource-scanner resource-manager` to manage domains IN TENANCY
- ALLOW RESOURCE `accessgov-agent resource-scanner resource-manager` to manage policies IN TENANCY

Establish Connection by Adding a New Cloud Service Provider - OCI IAM

Integration with Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) is achieved by configuring a new cloud service provider with the Oracle Access Governance Console.

1. In a browser, navigate to the Oracle Access Governance service home page and log in as a user with the *Administrator* application role.

2. On the Oracle Access Governance service home page, click on the  icon and select **Administration** → **Connected Systems**. Select the **Add a connected system** button from the Connected Systems page.
3. Select **Add** from the **Would you like to connect to a cloud service provider?** tile. This will navigate you to the **Add a Cloud Service Provider** workflow, which guides you through the steps required to configure Oracle Access Governance integration with Oracle Cloud Infrastructure Identity and Access Management.
4. **Select system** is the first step of the workflow. Select the **Oracle Cloud Infrastructure** tile. Once selected, a value of *Oracle Cloud Infrastructure* is displayed on the right hand side under **What I've selected**. Click **Next**.
5. Next step is **Enter details** where you enter name and description for the cloud service provider. Enter values for the following:
 - **What do you want to call your cloud service provider?:** Enter a name for the cloud service provider. Do not add space while naming your connected system.
 - **How do you want to describe this cloud service provider?:** Optionally, enter a description for the cloud service provider.
6. Next step is **Configure** where you add connection details for your cloud service provider. Enter the following values for your cloud service provider.
 - **What is the OCI tenancy OCID?:** Enter the OCID for the target tenancy. For further information regarding OCIDs see [Oracle Cloud Identifier](#), [OCID Syntax](#), and [Where to Get the Tenancy's OCID and User's OCID](#).
 - **What is the OCI tenancy's home region?:** Enter the home region for the target OCI tenancy. For further information on home region, see [The Home Region](#), and [How do I find my tenancy home region?](#). The home region will look similar to `us-ashburn-1`.

Observe that the details you enter are added to the list of **What I've selected**. Click **Add** to create the cloud service provider. If the configuration details are correct, then the connection is validated and displays "Success" on the console. The Full Data Load operation is completed within a few minutes and displays "Success" on the console. The system automatically runs incremental data load every four hours to sync data with the connected system.

 **Note:**

You cannot create multiple connected systems using the same tenancy ID. Use unique tenancy for each system.

4

Review

About Reviews

Overview

Access Review refers to review of accesses and permissions for an identity, usually an end user, that is carried out to confirm whether the access and permissions assigned to that entity are still valid. Access Review Campaigns from Oracle Access Governance are used to review these access rights and can be created on-demand which you can choose to run either one-time or periodically from the Oracle Access Governance Console.

As an *Administrator* or *Campaign Administrator*, you can create access review campaigns. There are currently two types of access review campaigns:

- User Access Review Campaigns
- Policy Reviews Campaigns

The type is determined by the data attributes chosen when configuring the campaign. The data attributes also depend on the target systems integrated with Oracle Access Governance. Some general rules to consider while configuring a campaign are:

Campaign Types	Description	Primary Selection Criteria	Additional Selection Criteria	More Details
User Access Review Campaign	Comprises a group of access reviews for members of your enterprise population where individual access to a specific source is checked and either certified or remediated	<ul style="list-style-type: none">• Who has access• What they are accessing• Which permissions• Which roles	Which cloud provider	<ul style="list-style-type: none">• Which permissions and Which roles are mutually exclusive, that is you can select only one of the two while creating a campaign.• If you select any of the primary identity selection criteria parameters, policy criteria selection is no longer applicable and is disabled.

Campaign Types	Description	Primary Selection Criteria	Additional Selection Criteria	More Details
Policy Review Campaign	Comprises a group of policy reviews that evaluates access control of Identity and Access Management (IAM) Policies.	Which policy	Which cloud provider	If you select any of the primary policy selection criteria parameters, user criteria selection is no longer applicable and is disabled.

Examples

Let's see some of the examples to create access review campaigns.

Example 1: Identity Access Reviews for a particular cloud provider

Scenario: You need to carry out identity access reviews to check roles and applications assigned to users on one of your cloud compartments on Oracle Cloud Infrastructure (OCI).

To do so, filter your cloud provider by selecting **Which cloud provider** and refine further to select your compartment. In addition, select applications from **What are they accessing?**, and roles **Which roles?**. However, you cannot perform policy reviews for your cloud compartment within this same campaign and **Which policies?** will be disabled.

Example 2: Review Access Permissions for an Application in your Organization

Scenario: To help your organization to deter any harm against misuse of access rights, you need to create a campaign to review access rights for the users of your organization who have *update* and *terminate* permissions for an application.

To do so, filter your division from **Who has access?**, select application from **What are they accessing?**, and select appropriate permissions using **Which permissions?**. You can either create a campaign to review permissions or review roles but both cannot be selected in a single campaign. In this example, **Which roles?** will be disabled along with **Which policies?**

Example 3: Review Policies for all Cloud Resources

Scenario: You need to carry out access reviews for all the cloud policies available in your cloud compartment.

To do so, filter your cloud provider by selecting **Which cloud provider** and refine further to select your compartment. In this example, this campaign will raise all the applicable review tasks for cloud policies under the **Policy Review** tab of **My Access Reviews**.


Create and Configure Reviews

Create User Access Review Campaigns

As a user with the **Administrator** or **Campaign Administrator** application role, you can create access review campaigns from the Oracle Access Governance Console. You can define selection criteria for access reviews based on users (who has access), applications (what are they accessing), permissions (which permissions), and roles (which roles). You can also define the workflow for the review in terms of the number of review levels, duration, and who performs the review.

To create an access review campaign using Oracle Access Governance Console:

Navigate to Campaigns

1. Log in to the Oracle Access Governance Console with a user assigned either the *Administrator* or *Campaign Administrator* application role.
2. You can select one of the following options to navigate to the screen:
 - On the console home page, click the **Select** button on the **Let's create some work and define a new campaign** tile.
 - Click the  icon, and select **Access Reviews** and then **Campaigns**. Click the **Create a campaign** button.

You will be navigated to the *Create a new access review campaign* workflow screen, from which you can define and configure your user access review campaign.

Selection Criteria

By default, all identity data ingested from the connected system is available to the access review campaign. This may be a large amount of data, so *selection criteria* allow you to narrow the criteria available for the campaign:

Criteria for user access reviews can be filtered based on:

- **Who has access:** Selecting review criteria to filter users based on standard (Organization, Job, Location), or custom attributes.
- **What they are accessing:** Selecting review criteria to filter users based on resources they have access to
- **Which permissions:** Selecting review criteria to filter users based on permissions such as *create*, *update*, *terminate*, *approve*, and so on.
- **Which roles:** Selecting review criteria to filter users based on application roles.

Additionally, depending on the connected system integrated with Oracle Access Governance, you can also add the following filter in combination with those listed above:

- Which cloud providers

 **Note:**

- The selection criteria vary based on the ingested data from the connected system and a few tiles listed above may not be available for selection. For example, if no roles are available in the connected system schema definition, then you won't see the **Which roles** tile.
- If you select any of the identity parameters above, policy criteria selection (**which policies?**) is no longer applicable and is disabled.

These criteria can be chosen and edited in any order before moving on to the next step. If you do not need to update each dimension, you can select any number from those above, and leave the remaining unchanged. If you do not need to narrow the criteria for your enterprise, then you can choose to move to the next step without adding any selection criteria. All criteria can be searched by *name*

 **Note:**

The following combinations are not supported and are mutually exclusive, that is you can select only one of the two while creating a campaign:

- **Which permissions** and **Which roles**

For example, you can create a campaign by selecting **Who has access?**, **What are they accessing?**, and **Which roles?** but you cannot create a campaign with the combination of **Who has access?**, **Which roles?**, and **Which permissions?**

1. Select the **Who has access?** tile to set criteria based on users.
 - a. After selecting the tile, select criteria from the following standard parameters:
 - i. Organization
 - ii. Job Code
 - iii. Location
 - b. To add one or more additional parameters, from the **Additional selection attributes** drop-down list, select one or more custom attributes and then click **Add**. For example, you may want to add users specific to certain *Cost Center* or *Project Code* in your access reviews.

 **Note:**

- Based on the number of selected custom attributes, you will see additional tabs to make your selection.
- You can only select up to five (5) additional custom attributes
- Contact Oracle Access Governance Administrator if you don't see the option for selecting custom attributes. You first need to enable it from the Administration settings within Oracle Access Governance Console. See View and Configure Custom Identity Attributes

Make your selections and when finished, click on **Apply my selections** or **Cancel** as appropriate. You are returned to the *Create a new access review campaign* step.

2. Select the **What are they accessing?** tile to define criteria based on the resources users have access to.

This allows you to narrow criteria based on the resources and applications users have access to.

Make your selections and when finished, click on **Apply my selections** or **Cancel** as appropriate. You are returned to the *Create a new access review campaign* step.


3. Select the **Which permissions?** tile to specify criteria based on permissions such as *create*, *update*, *terminate*, *approve*, and so on. Actual values for permissions will depend on the connected system identity data.

Make your selections and when finished, click on **Apply my selections** or **Cancel** as appropriate. You are returned to the *Create a new access review campaign* step.

4. Select the **Which roles?** tile to specify criteria based on roles. Actual values for roles will depend on the connected system identity data.

Make your selections and when finished, click **Apply my selections** or **Cancel** as appropriate. You are returned to the *Create a new access review campaign* step.



If you want to restrict the values further, click the  *Actions* menu icon, and select **Refine further**. In the **Cloud provider** pop-up, you can further refine your criteria by specifying one or more compartments, and/or one or more domains from the cloud provider you have selected in the main step.

As you make selections of the various criteria, you can see the effect that your selections make and an estimate of the number of review items that your access review campaign will generate. This information is displayed in the section on the right-hand of the page.

 **Note:**

If you need to make changes to your selections before moving on to workflows, select the **Modify** button on the relevant tile and amend as described in the steps above.

When you are happy with your selection criteria, click **I'm good, go to workflows** button to proceed to the *Assign workflow* dimension to select the guided workflow.

5. Select the **Which cloud providers?** tile to specify criteria based on a specific cloud provider. Actual values for this parameter will depend on the connected system integrated with Oracle Access Governance.


Assign Workflow

The *Assign Workflow* step is where the approval workflow for your access reviews is defined. Oracle Access Governance will provide a suggested optimal workflow based on your selection criteria.

If you wish to define your workflow, click the **I'll choose my own workflow** button.

1. Select how many levels of approval you want for your reviews. Choose from the following values:
 - One-level approval workflow
 - Two-level approval workflow
 - Three-level approval workflow
2. For each review level, select how you want the review level to be handled. Choose from the following values:

Parameter	Value
Who is the first second third reviewer?	<ul style="list-style-type: none"> • Owner • User manager • User • Custom reviewer
How many days do they have to review?	Number of days for each review
Who gets the notification?	<ul style="list-style-type: none"> • Only reviewer • Reviewer and manager
Who do you want to send reminders to?	<ul style="list-style-type: none"> • Only reviewer • Reviewer and manager
How many days between reminders	Duration (in days) before the next notification reminder.

 **Note:**

You can only assign a reviewer type to a single review level. If you assign **User** to Level 1, you cannot then assign **User** to Level 2 or 3, and so on.

3. Select where review decisions require a justification. Choose from the following values:
 - Required for all review decisions
 - Required only for revoke decisions

- Optional for all review decisions
4. Select the completion rule for the review. This gives a default action for all un-reviewed tasks at the end of each approval workflow level. Choose from the following values:
 - Approve all un-reviewed tasks
 - Revoke all un-reviewed tasks
 5. Select **Save** to save your workflow definition or **Cancel** to discard your changes.
 6. When you are happy with your workflow definitions, select **Save draft** to save your campaign for work later on or select **Next** to proceed to the *Add details* page.

Add Details

With the *Add Details* step, you can define the frequency (one-time or periodic) at which to run an access review campaign, give a meaningful name to your campaign, add a supporting description, and assign values to additional attributes, such as who owns it and when the campaign should start or end.

To add details :

1. Add values for the following parameters for your campaign:
 - **How often do you want this to run?:** Select **One time** to run a single occurrence of this campaign, or select a recurring pattern like **Quarterly**, **Monthly**, **Half-Yearly**, or **Yearly** to run this access review campaign periodically.
 - **What do you want to call this campaign?:** Add a name for your campaign.
 - **How do you want to describe this campaign?:** Add a description for your campaign.
 - **Who owns this campaign?:** Add the name of the campaign owner.
 - **How would you like to schedule your campaign?:** You can view this field only if you have selected to run your campaign one time. Select either **Run now** or **Schedule Later**. By default, the campaign is set to begin at the top of the next hour, the following day of campaign creation.
 - **When do you want to Begin?:** If you have set a recurring pattern, then select the start date of when you want to begin the campaign series. By default, the campaign is set to begin at the top of the next hour, the following day of campaign creation. If you want to change this, select the **Select Date Time** icon and add a new date/time.
 - **When do you want to End?:** If you have set a recurring pattern, then select the end date of when you want to end the campaign series.
2. Once you have set your preferences, select **Next** to go to the *Review and submit* step.
3. Optional: You may select one of the additional actions:
 - **Save Draft:** To save your changes and later come back and edit the workflow or details.
 - **Cancel:** To cancel the current process.
 - **Back:** To go back to the previous step.

Review and Submit

The *Review and submit* step displays the information you have added in the previous steps.

To review and submit your campaign :

- Select **Save draft** to save your campaign for work later on or select **Create** to create the campaign.

Note:


Oracle Access Governance supports permissions, accounts, and roles that are assigned through a request or direct provisioning mechanism. Some access assignments cannot have the Accept or Revoke operations performed on them and are not included in the access review campaign. These include:

- permission or account assigned to a user by a role
- role assigned to a user by a membership rule

Create Policy Review Campaigns

As an *Administrator* or *Campaign Administrator* of Oracle Access Governance, you can create one-time or periodic access review campaigns from the Oracle Access Governance Console. In this article we will look at how you can create on-demand policy reviews, where you define the selection criteria based on the policies associated with users. You can also define the approval workflow to select the number of review levels, review duration, and reviewer details.

Login

1. Sign in to the Oracle Access Governance Console with a user assigned either the *Administrator* or *Campaign Administrator* application role.
2. You can select one of the following options to navigate to the **Campaigns** screen:
 - On the console home page, click the **Select** button on the **Let's create some work and define a new campaign** tile.
 - Click the  icon, and select **Access Reviews**, and then **Campaigns**, then click the **Create a campaign** button.

You will be navigated to the *Create a new access review campaign* workflow screen, from which you can define and configure your policy review campaign.

Selection Criteria

By default, all identity data ingested from the connected system is available to the access review campaign. This may be a large amount of data, so *selection criteria* allows you to narrow the criteria available for the campaign:

Criteria for policy reviews can be filtered based on:

- Which Policy



Note:

If you select the policy criteria, user criteria selection is no longer applicable and is disabled.

Additionally, you can also add the following filter in combination with those listed above:

- Which cloud providers

These criteria can be chosen and edited in any order before moving on to the next step. If you do not need to update each dimension, you can select any number from those above, and leave the remaining unchanged. If you do not need to narrow the criteria for your enterprise, then you can choose to move to the next step without adding any selection criteria.




Note:

All criteria can be searched by *name*

1. Select the **Which cloud providers?** tile to specify criteria based on a specific cloud provider. Actual values for this parameter will depend on the target system you select.



- If you want to restrict the values further, click on the  menu icon, and select **Refine further**. In the **Cloud provider** pop-up, you can further refine your criteria by specifying one or more compartments, and/or one or more domains from the cloud provider you have select in the main step.
2. Select the **Which Policy?** tile to set criteria for policies.
 3. On selecting this tile, you can select criteria for the following parameters:
 - Policy name
 - Policies created since a given date
 4. Make your selections and when finished, click on **Apply my selections** or **Cancel** as appropriate. You are returned to the *Create a new access review campaign* step.

 **Note:**

As you make selections of the various criteria, you can see the effect that your selections make and an estimate of the number of review items that your access review campaign will generate. This information is displayed in the section on the right-hand of the page.

 **Note:**

If you need to make changes to your selections before moving on to workflows, select the **Modify** button on the relevant tile and amend as described in the steps above.

- When you are happy with your selection criteria, click **I'm good, go to workflows** button to proceed to the *Assign workflow* dimension to select the guided workflow.

Assign Workflow

The *Assign Workflow* step is where the approval workflow for your access reviews are defined. Oracle Access Governance will provide a suggested optimal workflow based on your selection criteria.

If you wish to define your workflow, click the **I'll choose my own workflow** button.

- Policy reviews have only one level of approval workflow. The following value is selected for you:
 - One-level approval workflow
- Select how you want the review to be handled. Choose from the following values:

Parameter	Value
Who is the first reviewer?	Defaults to the following value: <ul style="list-style-type: none"> Cloud provider custom reviewer
Whom do you want to be the reviewer?	If the current reviewer has the correct permissions then this value defaults to Me . If not then the value will default to the first reviewer with either Administrator or CloudAccessReviewer permissions.
How many days do they have to review?	Number of days for each review
Who gets the notification?	<ul style="list-style-type: none"> Only reviewer Reviewer and manager
Who do you want to send reminders to?	<ul style="list-style-type: none"> Only reviewer Reviewer and manager
How many days between reminders	Number of days for the gap between reminders

- Select where review decisions require a justification. Choose from the following values:
 - Required for all review decisions
 - Required only for revoke decisions

- Optional for all review decisions
4. Select the completion rule for the review. This auto performs a default action for all un-reviewed tasks at the end of each approval workflow level. Choose from the following values:
 - Approve all un-reviewed tasks
 - Revoke all un-reviewed tasks
 5. Select **Save** to save your workflow definition or **Cancel** to discard your changes.
 6. When you are happy with your workflow definitions, select **Save draft** to save your campaign for work later on or select **Next** to proceed to the *Add details* page.

Add Details

With the *Add Details* step, you can define the frequency (one-time or periodic) at which to run an access review campaign, give a meaningful name to your campaign, add a supporting description, and assign values to additional attributes, such as who owns it and when the campaign should start or end.

To add details :

1. Add values for the following parameters for your campaign:
 - **How often do you want this to run?:** Select **One time** to run a single occurrence of this campaign, or select a recurring pattern like **Quarterly**, **Monthly**, **Half-Yearly**, or **Yearly** to run this access review campaign periodically.
 - **What do you want to call this campaign?:** Add a name for your campaign.
 - **How do you want to describe this campaign?:** Add a description for your campaign.
 - **Who owns this campaign?:** Add the name of the campaign owner.
 - **How would you like to schedule your campaign?:** You can view this field only if you have selected to run your campaign one time. Select either **Run now** or **Schedule Later**. By default, the campaign is set to begin at the top of the next hour, the following day of campaign creation.
 - **When do you want to Begin?:** If you have set a recurring pattern, then select the start date of when you want to begin the campaign series. By default, the campaign is set to begin at the top of the next hour, the following day of campaign creation. If you want to change this, select the **Select Date Time** icon and add a new date/time.
 - **When do you want to End?:** If you have set a recurring pattern, then select the end date of when you want to end the campaign series.
2. Once you have set your preferences, select **Next** to go to the *Review and submit* step.
3. Optional: You may select one of the additional actions:
 - **Save Draft:** To save your changes and later come back and edit the workflow or details.
 - **Cancel:** To cancel the current process.
 - **Back:** To go back to the previous step.

Review and Submit

The *Review and submit* step displays the information you have added in the previous steps.

To review and submit your campaign :

- Select **Save draft** to save your campaign for work later on or select **Create** to create the campaign.

Enable Event-based Access Reviews

Setup Event-Based Access Review

To manage event-based access reviews using the Oracle Access Governance Console:

Event-based access reviews can be enabled and configured for the following event-types:

- **Identity Enabled**
- **Identity Disabled**
- **Department Change**
- **Manager Change**
- **Organization Change**
- **Location Change**
- **Job Code Change**
- **Custom Attribute**


Display name of the custom attribute is displayed in a tile format. You may see one or more custom attributes' tiles which depends on attribute's selection to enable the event-based functionality.

 **Note:**

If you don't see the option for selecting custom attributes, contact the Oracle Access Governance Administrator. You first need to enable it from the Administration settings within Oracle Access Governance Console. See [View and Configure Custom Identity Attributes](#).


- **Multiple Event Changes**

To enable event-based access reviews:

1. Log in to the Oracle Access Governance Console with a user assigned the *Administrator* application role.
2. Select from the  navigation menu. Click **Access Reviews** and then **Event-Based Setup**. The **Event-Based Setup** landing page is displayed.

3. Each event type is displayed as a tile with a status of **Enabled** or **Disabled** and an **Actions** drop-down menu, providing the option to **Edit** or **View details**. Select **Edit** for the event-type you want to enable.
4. On the **Configure the event type** screen:
 - a. Use the radio button to **Enable** or **Disable** the event-type.
 - b. If you want to auto-approve low risk task for this event type, select **Yes**.
5. The Oracle Access Governance service provides a suggested optimal workflow for the event-type. You can select **Save** to accept the suggested workflow, **Cancel** to abandon the setup, or **I'll choose my own workflow** to configure the workflow. If you choose **I'll choose my own workflow** then follow the subsequent steps.
6. Select how many levels of approval you want for your reviews.
 - One-level approval workflow
 - Two-level approval workflow
 - Three-level approval workflow
7. For each review level, select how you want the review to be handled.

Parameter	Value
Who is the first second third reviewer?	<ul style="list-style-type: none"> • Owner • User manager • User • Custom reviewer
How many days do they have to review?	Number of days for each review
Who gets the notification?	<ul style="list-style-type: none"> • Only reviewer • Reviewer and manager
Who do you want to send reminders to?	<ul style="list-style-type: none"> • Only reviewer • Reviewer and manager
How many days between reminders	Number of days for the gap between reminders

 **Note:**

You can only assign a reviewer type to a single review level. If you assign **User** to Level 1, you cannot then assign **User** to Level 2 or 3, and so on.


8. Select where review decisions require a justification.
 - Required for all review decisions
 - Required only for revoke decisions
 - Optional for all review decisions
9. Select the completion rule for the review. This gives a default action for all un-reviewed tasks at the end of each approval workflow level. Choose from the following values:
 - Approve all un-reviewed tasks
 - Revoke all un-reviewed tasks

10. Select **Save** to save your workflow definition or **Cancel** to discard your changes.
11. You return to the **Configure the event type** screen. Select **Save** to keep the changes to your event-type configuration, or **Cancel** to abandon the changes.

Configure Multi-Events

Multi-events occur when Oracle Access Governance receives changes for more than one event-type, that is associated with a single identity.

Users with the *Administrator* application role can configure a shared workflow which is applied when multi-events are identified. To configure the shared workflow:

1. Log in to the Oracle Access Governance Console with a user assigned the *Administrator* application role.
2. Select **Event-Based Administration** → **Event-Based Setup** from the  navigation menu.
3. Select **Edit shared workflow**.
4. On the **How do you want multi-event reviews to proceed?** screen:
 - a. Confirm if you want to auto-approve low risk task for this event type by selecting **Yes** or **No**.
 - b. Select how many levels of approval you want for your reviews.
 - One-level approval workflow
 - Two-level approval workflow
 - Three-level approval workflow
 - c. For each review level, select how you want the review to be handled.

Parameter	Value
Who is the first second third reviewer?	<ul style="list-style-type: none"> • Owner • User manager • User • Custom reviewer
How many days do they have to review?	Number of days for each review
Who gets the notification?	<ul style="list-style-type: none"> • Only reviewer • Reviewer and manager
Who do you want to send reminders to?	<ul style="list-style-type: none"> • Only reviewer • Reviewer and manager

 **Note:**

You can only assign a reviewer type to a single review level. If you assign **User** to Level 1, you cannot then assign **User** to Level 2 or 3, and so on.


Parameter	Value
How many days between reminders	Number of days for the gap between reminders

- d. Select where review decisions require a justification.
 - Required for all review decisions
 - Required only for revoke decisions
 - Optional for all review decisions
- e. Select the completion rule for the review. This gives a default action for all un-reviewed tasks at the end of each approval workflow level.
 - Approve all un-reviewed tasks
 - Revoke all un-reviewed tasks
- f. Enter a name for the default access review owner.
- g. Select **Save** to update the shared workflow configuration, or **Cancel** to discard the changes.

View Event-Types

As an *Administrator* you can view the details of each event-type in the Oracle Access Governance Console.

To view event-based settings:

1. Select **Event-Based Administration** → **Event-Based Setup** from the  navigation menu.
2. Select **View details** from the **Actions** drop-down menu for the event-type you want to view.
3. The **Event - <event type name>** screen is displayed, allowing you to view the following details:
 - Status of the event type (Disabled or Enabled), and the date when the status was last changed.
 - Whether the low-risk tasks for this event-based access review will be auto-approved or not.
 - Details of the approval workflow.
 - Details of when justification is required.
 - Details of the completion rule.
 - Default owner of the access review.

Manage and Monitor Access Reviews

Manage Access Review Campaign

Users with the **Administrator** or **Campaign Administrator** application role and campaign owners can monitor and manage access review campaigns using the Oracle Access Governance Console.

Manage an Access Review Campaign

Management tasks are performed in the Oracle Access Governance Console.

To manage an access review campaign:

View and Manage Campaigns

1. Log on to the Oracle Access Governance Console either with an Administrator, Campaign Administrator, or a user with the campaign owner application role.
2. You can select one of the following options to navigate to the **Campaigns** screen:
 - On the console home page, click the **Select** button on the **Show me my ongoing campaigns** tile.
 - Click the **Select** button on the **You're making progress** tile.
 - Click the **Select** button on the **Show me all campaigns** tile.

- Click the  icon, and then **Access Reviews**, and then **Campaigns**.

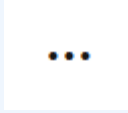
Whichever option you will choose, you will be navigated to the **Campaigns** screen to manage all campaign access reviews.

In the **Campaigns** screen, you can see your campaigns listed in the tabular form that includes campaign attributes, such as campaign name, status, campaign frequency, recurring pattern, campaign owner, and campaign duration (start date and due date).

You can use the **Search** field to locate the required campaigns. By default, you see **your ongoing campaigns** in the list, but you can filter the campaigns by using the drop-down menu in the top, right corner of the application page based on the following categories:


- **My ongoing campaigns:** Displays current campaigns with a **Status** of *In progress* or *Ready for approval*.
 - **My upcoming campaigns:** Displays upcoming scheduled campaigns with a **Status** of *Scheduled* or *Draft*.
 - **My previous campaigns:** Displays closed campaigns with a **Status** of *Approved*, *System ended* or *Terminated*.
 - **All campaigns:** Displays all campaigns with all the available statuses.
3. To perform tasks on the campaign, you can select the campaign link and then select the **Actions** menu. The tasks that you can perform are dependent on the **Status** of the campaign. The tasks that can be performed for each **Status** are detailed in the table below:

 **Note:**

Tasks can also be accessed by navigating the **Menu**  corresponding to each campaign on the **Campaigns** page.

Status	Available Actions
Draft	<ul style="list-style-type: none"> • View campaign details • Edit • Delete
Scheduled	<ul style="list-style-type: none"> • View campaign details • Edit • Clone • Terminate • Terminate Series
In progress	<ul style="list-style-type: none"> • Clone • Terminate • Terminate Series • View report • Download CSV data
Ready for approval	<ul style="list-style-type: none"> • Approve • Clone • Terminate • Terminate Series • View report • Download CSV data
Approved	<ul style="list-style-type: none"> • Clone • View report • Download CSV data
System ended	<ul style="list-style-type: none"> • Clone • View report • Download CSV data
Terminated	<ul style="list-style-type: none"> • Clone • View report • Download CSV data



4. Select tasks either from the **Menu**  on the main **Campaigns** page or from the **Actions** menu on the campaign detail page. Perform tasks as follows:

Clone

1. Select the **Clone** task to make a clone of the current access review campaign. You are taken to the **Clone campaign** page.
2. On the **Clone campaign** page, enter values for the following parameters, which will apply to the cloned campaign.

- **How often do you want this to run?** : Select **One time** to run a single occurrence of this campaign, or select a recurring pattern like **Quarterly**, **Monthly**, **Half-Yearly**, or **Yearly** to run this access review campaign periodically.
 - **What do you want to call this campaign?:** Provide a name for the cloned campaign.
 - **How do you want to describe this campaign?:** Provide a description for the cloned campaign.
 - **Who owns this campaign?:** Provide details of the owner of the cloned campaign.
 - **How would you like to schedule your campaign?:** You can view this field only if you have selected to run your campaign one time. Select either **Run now** or **Schedule Later**. By default, the campaign is set to begin at the upcoming next hour, the following day of campaign creation.
 - **When do you want to Begin?:** If you have set a recurring pattern, then select the start date of when you want to begin the campaign series. By default, the campaign is set to begin at the top of the next hour, the following day of campaign creation. If you want to change this, select the **Select Date Time** icon and add a new date/time.
 - **When do you want to End?:** If you have set a recurring pattern, then select the end date of when you want to end the campaign series.
3. When you have set your clone preferences, select **Create** to clone the current campaign.
 4. You may select one of the additional actions:
 - **Save Draft:** To save your changes and later come back and edit the workflow or details.
 - **Cancel:** To cancel the current process.

Edit

Select the **Edit** task to make changes to the upcoming or scheduled access review campaign. You are taken to the **Edit campaign** page.

The **Edit campaign** page provides the same guided workflow for entering your campaign parameters as the *Create* campaign page. You can edit the selection criteria, workflow and reviewer details, campaign details, and schedule of campaign.

After updating your campaign details, on the **Review and submit** step, select **Update** to update the campaign. Alternatively you can select **Back** to edit values, or **Cancel** to discard your changes.

Delete

1. Select the **Delete** task to remove the current access review campaign.
2. On the **Confirmation** pop up, select **Cancel** to retain the campaign, or **Delete** to remove the campaign.

Terminate

1. Select the **Terminate** task to terminate the current access review campaign.

2. On the **Confirmation** pop up dialog, select **Cancel** to retain the campaign or **Terminate** to end the campaign.

Terminate Series

This option is available only if your access review campaign has a recurring pattern and its frequency is other than a one-time campaign. With this option, you can cancel all the ongoing (currently running) and upcoming (scheduled in future dates) access reviews for that campaign series. This option won't change the closed campaigns available in the **My Previous Campaigns**.

1. Select the **Terminate Series** task to terminate the series of the access review campaign.
2. On the **Confirmation** pop-up dialog window, select **Terminate Series** to end the campaign series or select **Cancel** to retain the campaign series.

You will get the confirmation message after the termination of the series.

Approve

Select **Approve** to approve a campaign. You will see a confirmation message stating that the campaign has been approved.

Monitor an Access Review Campaign

Monitor the state and progress of campaigns using the Oracle Access Governance Console.

Users with the *Administrator*, *Auditor*, or *Campaign Administrator* application role or the campaign owner can monitor the state and progress of campaigns.

- **Administrator/Auditor**: Can monitor all campaigns in Oracle Access Governance.
- **Campaign Administrator**: Can monitor campaigns that they have created.
- **Campaign Owner (User)**: Can monitor campaigns that they own.

To monitor access review campaigns using Oracle Access Governance Console:

Login and Search for Campaigns

1. Log in to the Oracle Access Governance Console with a user assigned either the *Administrator* or *Campaign Administrator* application role. Click the **Select** button on the **Show me my ongoing campaigns**, the **You're making progress**, or the **Show me all campaigns** tiles.

Whichever tile you select, you will be navigated to the **Campaigns** page, from which you can monitor access review campaigns.


In the **Campaigns** page you can either search for campaigns using the selections under the **Search** field or use the drop-down menu in the top-right corner to select one from the following:

- **My ongoing campaigns**: Displays campaigns with a **Status** of *In progress* or *Ready for approval*.
- **My upcoming campaigns**: Displays campaigns with a **Status** of *Scheduled* or *Draft*.
- **My previous campaigns**: Displays campaigns with a **Status** of *Approved*, *System ended* or *Terminated*.
- **All campaigns**: Displays all campaigns.

View Campaign Details

1. To view details of a particular campaign, select either the campaign **Name** or



select **View campaign details** from the  Navigation Menu icon.

2. The Campaign details page shows the details of the campaign you have selected including:
 - **Progress so far:** Graphic showing the number of reviews and status for the campaign.
 - **Reviewers:** Details of the reviewers for this campaign, their review level, and progress.

Note:

The reviewers displayed on this page can be filtered based on the **Reviewer level** in the **Search** field.

3. Select the **Additional details** menu to display more information about the campaign, including *Owner*, *Start date*, *Due date*, and *Review process*. Select **Close** to return to the Campaign details page.

View report

1. Select **View report** to view a report showing the details of the selected campaign. The report is displayed on another page, showing the information on access reviews and a number of bar charts showing details of:
 - **User accounts review decision**
 - **Role membership review decision**
 - **Permission assignments review decision**
 - **Group by user organization- Top 5**
 - **Group by applications- Top 5**
 - **Group by roles- Top 5**
 - **Group by cloud account - Top 5**

Note:

The report details will vary based on connected systems and campaign selection criteria.

2. If you want to retain a copy of the report, select **Download PDF**, else select **Close** to return to the campaign.

Download CSV data

1. Select **Download CSV data** to generate a comma-separated values file with data for the campaign.

2. On the **Download CSV data** confirmation pop-up dialog, select **Download** to download the CSV file or else **Cancel** to discard.

Generate Event-Based Access Reviews Report

As an *Administrator* of Oracle Access Governance, you can analyze information on event-based access reviews by generating reports using the Event-Based Report capability of Oracle Access Governance.

Navigate to the Event-Based Access Reviews Report Service


You can run, view, and save the event-based access review report.

You must have *Administrator* rights to view and run this service. Find out more about application roles in the [Understanding Application Roles](#) topic

Here's how you can open the event-based access review report service on Oracle Access Governance Console:

1. From your browser, go to Oracle Access Governance. On the OCI console, you can open it using the **Service Home Page** link.
2. In the **Username** field, enter either your *Administrator* user name.
3. In the **Password** field, enter your password and select **Sign In**.

You will be navigated to the home page of your Oracle Access Governance Console.

4. Click  icon on the top, left corner of the application page to display the navigation menu.
5. Select **Access Reviews**, and then **Event-Based Setup**
The **Event-Based Setup** landing page is displayed.
6. Click the **View access review report** button

The **Event-Based Access Reviews Report** landing page is displayed.

Run Event-Based Access Reviews Report

As an Administrator, you can generate a monthly report on event-based access reviews by selecting appropriate reporting criteria.

You can generate the report based on date range and event types (predefined identity changes to perform access reviews). For example, you can generate a report on the access reviews initiated or implemented for all the new identities added or removed in your organization in the last month.

Here's how you can run an event-based access reviews report by selecting the appropriate report selection criteria:

1. In the **From** field, select the start date from which you want to run a report.
2. In the **To** field, select the end date up to which you want to run a report.

To generate a report, you must take care of the following date range rules:

- You can select only the first day of the month.

- You can generate a report only for a maximum of a 12-month period, i.e. the difference between the From date and the To date cannot be more than 12 months.

If you started implementing event-based access reviews from the 10th of this month and want to generate report till the present day, then in the **From** field, select the first day of this month, and in the **To** field, select the first day of the next month. However, the results will include records only from the date of implementation of the event-based access reviews up to the current day.

- Select one or more predefined actions or triggered scenarios for your report. The available options are:
 - Identity Enabled** (Default)
 - Department Change**
 - Job Code Change**
 - Location Change**
 - Manager Change**
 - Organization Change**
 - Multi Event Change**

 **Note:**

The **Enabled** and **Disabled** event-types are based on the **Event-Based Setup** activity.

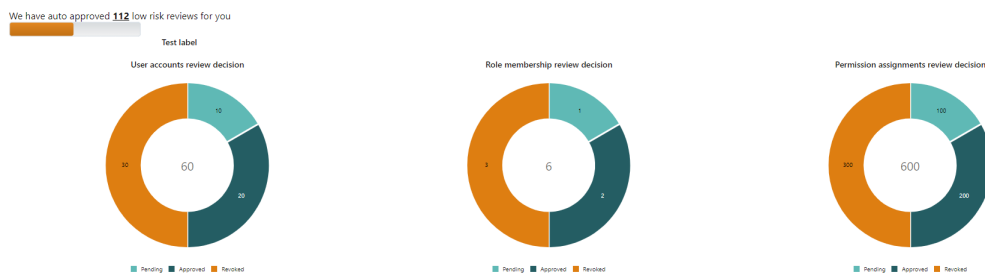
- Select **Apply**.

As per the selected criteria, you can view the graphical charts on the same application page.

View Event-Based Access Reviews Report Results

After you generate an event-based access review report, you can see a set of graphical charts (donut charts, stacked bar charts, and chart legends) displaying the report details on the same application page.

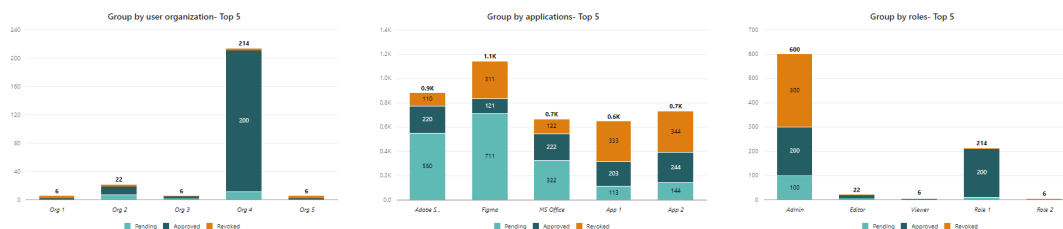
The donut charts display the following information:



- User accounts review decision:** Shows the number of impacted user accounts after running the event-based access reviews. The decision statuses are categorized based on *Pending*, *Approved*, or *Revoked* access reviews.

- **Role membership review decision:** Shows the number of impacted user roles and group roles after running the event-based access reviews. The decision statuses are categorized based on *Pending*, *Approved*, or *Revoked* access reviews.
- **Permission assignments review decision:** Shows the number of impacted user permissions or entitlements after running the event-based access reviews. The decision statuses are categorized based on *Pending*, *Approved*, or *Revoked* access reviews.
- **Auto action of low risk:** Shows the number of approved low-risk review tasks after running the event-based access review. These low-risks review tasks are categorized based on **Auto**, which are automatically approved by Oracle Access Governance, or **Manual**, which are manually approved by the assigned reviewer.

The stacked bar charts display the following group information:



- **Group by user organization - Top 5:** Shows which top five organizations are affected after the running the event-based access reviews. The decision statuses are categorized based on *Pending*, *Approved*, or *Revoked* access reviews.
- **Group by applications - Top 5:** Shows which top five applications are affected after the running the event-based access reviews. The decision statuses are categorized based on *Pending*, *Approved*, or *Revoked* access reviews.
- **Group by Roles - Top 5:** Shows which top five roles are affected after the running the event-based access reviews. The decision statuses are categorized based on *Pending*, *Approved*, or *Revoked* access reviews.

Additional Actions

In addition to viewing report, you can also save the event-based access reviews report offline in the PDF format or download the CSV data for further analysis, audit, or anything else you usually do with offline reports.

Download PDF: Select the **Download PDF** button, which is available at the top, right corner of the application page, to save the report results offline in PDF format. Your PDF file will be saved to your downloads directory.

Download CSV Data: Select the **Download CSV Data** button, which is available at the top, right corner of the application page, to export the data in the CSV format.

Review Access and Permissions

Perform Access Review

Access reviews can be carried out from the Oracle Access Governance Console by users with the following roles, which are based on data attributes derived from the connected system:

Users can review identity and policy review tasks. They can bulk approve low-risk items, check the AI/ML-equipped prescriptive analytic insights, review high-risks items, and make informed decisions based on AI/ML-driven recommendations provided by Oracle Access Governance.


Identity Review Tasks

Identity Review Tasks include audit of user access rights carried out by campaigns that are run periodically, on-demand, or are initiated on occurrence of some identity events. These access reviews tasks help organizations to evaluate user account, entitlements and roles, make informed decision based on the AI/ML driven recommendations, and deter any harm that could be caused due to misuse of access rights.

Identity access review tasks can be carried out by users with the following roles:

- **User** (review access assigned to me/self)
- **Manager** (review access assigned to users in my team)
- **Owner** (review access assigned to users over resources I own)
- **Custom Reviewer** (review access tasks assigned to a user other than end-user, manager, or owner. The default value is *Me*)

To perform an identity access review:

1. In the Oracle Access Governance Console, select **Access Reviews**, and then **My Access Reviews** from the  navigation menu.

You navigate to the **My Access Reviews** page. You can search a specific access review task by identity name or policy name, or apply the given filters to narrow down the search results. You can also view the count of total identity and policy review tasks assigned to you as a reviewer. By default, you will see the **Identity review tasks** tab. Select the **policy review tasks** tab to view and take appropriate actions on the IAM policies.

On the **Identity review tasks** tab, you see all user and event-based review tasks assigned to you as a reviewer. The following information is displayed for each review item:

- **Identity name**
- **Manager Name**
- **Assignment name**
- **Assignment type**
- **Due days**
- **Review source**
- **Recommendation**
- **Insights**
- **Actions**

The **Insights** column has a link for each review item which, when clicked, takes you to the **Insights** page. The insights are based on our in-house AI/ML-equipped prescriptive analytic-based Identity Intelligence system. On a high-level, analysis of the permission is based on the following factors:

- Comparison with peers reporting to the same manager

- Comparison with peers with the same job code
- Comparison with peers in the same organization
- Recent changes in a user profile

On the **Insights** page, based on the analysis, you can view recommendation for the access review task. On the left-panel, you can view the access rights information for that identity. On the page, you can view the graphical insights based on the analysis factors, series of access review tasks initiated for that identity since the time the specific permission was granted, and recent change events related to that identity.

To make a review decision:

2. You can either revoke or accept a review item. This can be done either from the **Insights** page or by selecting the relevant option in the **Actions** column on the **My Access Reviews** page.
3. To revoke a review item, select **Revoke**. In the confirmation pop-up dialogue, add a **Justification** and select **Submit**. You will be taken back to the **My Access Reviews** page and a confirmation that the decision has been saved will display.

 **Note:**

- To approve an access privilege, all the reviewers must approve a review item. However, to revoke an access privilege, first revoke done by any-level reviewer is considered final.
 - If you revoke an **Account** task, then it will auto action to revoke all the related entitlement tasks.
 - If you accept an entitlement (**Role** or **Permission**) task, then it will auto action to accept the related **Account** tasks.
 - When you revoke a review item, the item is remediated automatically. A request is sent back to the connected system to revoke the item in the back-end system. No manual steps are required.
4. To accept a review item, select **Accept**. In the confirmation pop-up dialogue, add a **Justification** and select **Submit**. You will be taken back to the **My Access Reviews** page and a confirmation that the decision has been saved will display.


Policy Review Tasks

Policy Review tasks include audit of Identity and Access Management (IAM) policies initiated by policy access review campaigns that are run periodically or on-demand. These access review tasks help organizations to evaluate access control of cloud resources up to the statement level, review high-risk policies, make informed decision based on the AI/ML driven recommendations, and deter any harm that could be caused due to misuse of policy permissions.

Policy access review tasks can be carried out by users with the following roles:

- **CloudAccessReviewer** (review cloud resources such as OCI IAM Policies)
- **Administrator** (modify, delete, monitor all access review campaigns)

To perform a policy access review task:

1. In the Oracle Access Governance Console, select **My Access Reviews** from the  navigation menu. You navigate to the **My Access Reviews** page.

By default, you will see the **Identity review tasks** tab. Select the **Policy review tasks** tab to view and take appropriate actions on the IAM policies. You can search a specific access review task by a policy name, or apply the given filters to narrow down the search results. You can also view the count of total identity and policy review tasks assigned to you as a reviewer.

On the **Policy review tasks** tab, you will see all policy access review tasks assigned to you as a reviewer. The following information is displayed for each review item:

- **Policy name**
- **Connected system**
- **Policy Provider**
- **Due days**
- **Review source**
- **Recommendation**
- **Insights**

 **Note:**

If you have modified the IAM policy after the policy review tasks have been generated, these updated policies would not be considered for review, either wait for the next periodic campaign to run, or create a fresh campaign after the incremental data load operation.

The **Insights** column has an *Actions* link for each policy review item, which when clicked, takes you to the **Insights** page. The insights are based on our in-house AI/ML-equipped prescriptive analytic-based Identity Intelligence system.

On the **Insights** page, you can view our recommendation for the policy review task. On the left-panel, you can view the policy information. On the right, you can view a complete list of actionable and non actionable policy statements, view policy details to see who and what the policy statement is granting access to, and make appropriate decisions on each statement.

You can also view a series of access review tasks initiated for that policy since the time it was granted. The non actionable statements provide no access rights, therefore no action can be taken on those policy statements. For example, any rule statement that forms a construct which can further be used in other policy statements to provide access rights.

To make a review decision, you can either revoke all or accept all actionable statements in that policy at once, or make decision individually on each policy statement and then select **Apply**. By default, all the actionable policy statements are selected with a tick icon. The final remediation decision will be submitted per policy, and further sent to the connected system for closed-loop access remediation.

2. From the **Insights** page, to accept or to revoke policy statement(s):
 - To revoke all policy statements at once, select **Revoke all**.

- To revoke an individual policy statement, select the cross icon to revoke access for that policy statement. Repeat this action on each policy statement that you want to revoke.
- To accept all policy statements at once, select **Accept all**.
- To accept an individual policy statement, select the tick or check mark icon to accept the policy statement. Repeat this action on each policy statement that you want to accept.

 **Note:**

- To approve a policy, all the reviewers must approve a review item. However, to revoke an access privilege, first revoke done by any-level reviewer is considered final.
- When you revoke a policy, the policy is remediated automatically. A request is sent back to the connected system to revoke the item in the back-end system. No manual steps are required.

3. After you have finalized the decision on all the policy statements, select **Apply** .

The confirmation pop-up dialogue is displayed. The count for policy statements that you selected to accept and revoke is displayed. Add your comments in the **Justification** field, and then select **Submit**. You will be taken back to the **My Access Reviews** page and a confirmation that the decision has been saved will display.

View Access to Resources

Users can check what access they have for themselves or for their direct reports.


My Directs' Access

Managers can view details of the applications, cloud resources, permissions, and roles assigned to their direct reports.

 **Note:**

This feature is not available if you have integrated only OCI IAM, as your target system, with Oracle Access Governance.

To review team access:

1. In the Oracle Access Governance Console, select **Who Has Access to What** , and then **My Directs' Access** from the  navigation menu.

You navigate to the **My Directs' Access** page. A list of your direct reports is displayed with the following details:

- **Username**
- **First name**

- **Last name**
- **Email ID**
- **Applications**
- **Permissions**
- **Roles**

You can use **Advanced filters** to limit the search results of users specific to user attributes, such as an application, a job code, or a location.


2. To view access privileges assigned to a user, select the **Username**.

Details of all permissions assigned to the selected user are displayed, grouped by **Roles, Cloud resources, or Application**.

My Access

Users can view details of the application, cloud resources, permissions, and roles assigned to themselves.

To review your access:

- In the Oracle Access Governance Console, select **Who Has Access to What**, and then **My Access** from the  navigation menu.

You navigate to the **My Access** page. The count of applications, cloud resources, and roles assigned to you are displayed.

Details of all permissions assigned to you are displayed, grouped by **Role, Cloud resources, or Application**. Select a specific option from the **Group by** drop-down to view access details specific to cloud resources, applications, or roles assigned to you.

You can search across the list and improve your search results. For example, you can search specific to application, cloud resource, or role attributes, such as grant type, application permission, account name, policy name, privilege, and so on.

For **Applications**, you can view the following details:

- **Accounts:** User account name or user ID
- **Permission:** Application permission to perform operations, such as Admin, Viewer, and so on.
- **Grant type:** Method of granting access to application. For example, through *Access Policy, Direct Provision, Request*, or through *Role* assignment.
- **Date granted:** Date on which the application access was granted
- **Granted until:** End date, if any, for application access.

For **Cloud resources**, you can view the following details:

- **Resource name:** Name of that resource as defined in the cloud system.
- **Resource type:** Individual or family resource type, such as VCNs, subnets, instances, volumes, and so on.
- **Compartment:** Compartment name on which that resource is located and access is granted.
- **Policy name:** Name of the policy as defined in the cloud system.

- **Privilege:** Level of access to perform operations on that resource. For example, *Inspect*, *Read*, *Write*, or *Manage*

For **Roles**, you can view the following details:


- **Role name:** Logical role name granted for applications along with relevant permissions. For example, **Users** role granted for JIRA, Confluence, and Figma applications, with *Read* permissions.
- **Grant type:** Method of granting role, such as *Direct* or through *Request*.
- **Date granted:** Date on which the role was granted.
- **Granted until:** End date, if any, for that role.

Enterprise-wide Access

Users with an *Administrator* role can get a 360-degree view of all the resources and assigned permissions for those resources from the Oracle Access Governance Console.

From the **Enterprise-wide Access** page, you can view a list of the entire organization's resources and resource types across various systems connected with Oracle Access Governance. You can also fetch which identities are currently assigned to that resource, at what permission level, and how those permissions are assigned or granted (manually or through some policy).

To view a list of available resources:

1. In the Oracle Access Governance Console, from the  navigation menu, select **Who Has Access to What**, and then **Enterprise-wide Access**. The *Enterprise-wide Access* page is displayed. You can view the count of resources and resource types available in Oracle Access Governance for your organization.

Search and Sort Resources

Use the **Search** field to locate the required resources by resource name. You can manage a large set of resources by applying sorting techniques. Use the **Sort by** drop-down to sort resources by **Resource Name** or **Resource Type** and/or use the **Sort Direction** drop-down to arrange resources alphabetically either in ascending (A-Z) or descending (Z-A) order.

View Resource Details

You can view resource details, such as:

- Resource Name
- Resource Type
- Count of Identities who have access to that resource

Click the resource name to view identity details.

At the top, the resource details page displays the count of identities who can access that resource. Based on the available data ingested into Oracle Access Governance, you can view a complete list of identities and their details, such as identity name, email address, organization, job code, location, manager details, permission level, and how that permission is assigned to the resource.

The pie charts show you the break down of identities having access to the resource based on organization, job-code, or location. Use the **Sort by** drop-down to sort identities by **First**

Name or **Last Name**, and/or use the **Sort Direction** drop-down to arrange identities alphabetically either in ascending (A-Z) or descending (Z-A) order.

Click the **CSV** icon to export the data in the CSV format.

5

Related Content

Use the listed resources to explore more about Access Governance capabilities, refer to OAG REST APIs to create, manage, and view *GovernanceInstances*, and read OAG Rel Notes to learn about new features and enhancements added recently to improve your experience.

- [Oracle Access Governance Release Notes](#)
- [Access Governance REST APIs](#)

Oracle Access Governance Release Notes

Oracle Access Governance Release Notes allow you to keep informed about new features and enhancements added to enhance your experience.

To view release notes for Access Governance, refer to the following:

- [Oracle Access Governance Release Notes](#)

Access Governance REST APIs

Oracle Access Governance REST APIs are available to create, view, and manage *GovernanceInstances*.

To view REST API reference and endpoints for Access Governance, refer to the following:

- [Access Governance REST APIs](#)