

Oracle® Cloud

Administering Oracle Cloud Infrastructure Process Automation



F56095-13
September 2024



Oracle Cloud Administering Oracle Cloud Infrastructure Process Automation,
F56095-13

Copyright © 2022, 2024, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

Contents

1 Get Started

| | |
|--|-----|
| Overview of Oracle Cloud Infrastructure Process Automation | 1-1 |
| Service Types | 1-1 |
| Process Automation Roles | 1-2 |
| Administrative Interfaces | 1-4 |

2 Before You Begin

| | |
|--|-----|
| Sign In to the Oracle Cloud Infrastructure Console | 2-1 |
| Sign In to the Console in Tenancies That Use Identity Domains | 2-1 |
| Sign In to the Console in Tenancies That Do Not Use Identity Domains | 2-2 |
| Create a Compartment | 2-3 |

3 Manage Access and Assign Roles

| | |
|---|------|
| Differences Between Tenancies With and Without Identity Domains | 3-1 |
| About IAM Policies for Process Automation | 3-2 |
| Manage Access in an Identity Domain | 3-4 |
| Create an Identity Domain | 3-6 |
| Create an IAM Group in an Identity Domain | 3-6 |
| Create an IAM Policy in an Identity Domain | 3-7 |
| Create a User in an Identity Domain | 3-8 |
| Assign IDCS Application Roles to Groups in an Identity Domain | 3-8 |
| Manage Access Without an Identity Domain | 3-10 |
| Understand Federation | 3-11 |
| Create an IDCS Group | 3-12 |
| Create an IAM Group | 3-12 |
| Create an IAM Policy | 3-13 |
| Map the IDCS and IAM Groups | 3-14 |
| Create IDCS Users | 3-14 |
| Create IAM Users | 3-15 |
| Assign IDCS Application Roles to Groups | 3-15 |
| Configure Multiple Identity Stripes for Process Automation | 3-16 |
| Define a Stripe Naming Convention | 3-17 |

| | |
|--|------|
| Create an IDCS Group for Secondary Stripe Users | 3-17 |
| Create an OAuth Client in the Secondary Stripe | 3-18 |
| Create an IAM Group for Secondary Stripe Users | 3-18 |
| Create the Federation and its Group Mapping | 3-18 |
| Create an IAM Policy for Federated Users to Create Instances | 3-19 |
| Provide Access to a Federated Stripe in the IAM Group for Secondary Stripe Users | 3-20 |
| Create Process Automation Instances in the Secondary Stripe Compartments | 3-21 |

4 Provision and Manage Oracle Cloud Infrastructure Process Automation Instances

| | |
|---|------|
| Provision a Process Automation Instance | 4-1 |
| Access the Process Automation Instance | 4-2 |
| Delete a Process Automation Instance | 4-3 |
| Edit a Process Automation Instance | 4-3 |
| View Instance Details | 4-4 |
| Stop and Start a Process Automation Instance | 4-5 |
| Move an Instance to a Different Compartment | 4-6 |
| Create an Access Token to Provision an Instance | 4-7 |
| Create an Access Token in a Tenancy That Uses Identity Domain | 4-7 |
| Create an Application | 4-7 |
| Generate an Access Token | 4-8 |
| Create an Access Token in a Tenancy That Do Not Use Identity Domain | 4-9 |
| Create an Application | 4-9 |
| Generate an Access Token | 4-10 |
| Generate the Access Token from the CLI or an API | 4-10 |
| Enable Process Automation with Oracle Integration 3 | 4-11 |
| Set Up IAM Policies to Manage Process Automation Instance | 4-11 |
| Enable Process Automation | 4-12 |
| Assign IDCS Application Roles to Manage Access | 4-12 |

5 Monitor Oracle Cloud Infrastructure Process Automation

| | |
|--|-----|
| Overview of Oracle Cloud Infrastructure Process Automation Service Metrics | 5-1 |
| View Service Metrics | 5-3 |
| Monitor Service Metrics, Alarms, and Notifications | 5-3 |

A Service Limits, Quotas, and Events

| | |
|-------------------------------------|-----|
| Service Limits | A-1 |
| Set Instance Quotas on Compartments | A-4 |

Preface

This document describes how to provision, manage, and administer Oracle Cloud Infrastructure Process Automation from the Oracle Cloud Infrastructure Console.

Topics:

- [Audience](#)
- [Documentation Accessibility](#)
- [Diversity and Inclusion](#)
- [Related Resources](#)
- [Conventions](#)

Audience

Administering Oracle Cloud Infrastructure Process Automation is intended for users who want to set up, manage, and administer Oracle Cloud Infrastructure Process Automation instances in the Oracle Cloud Infrastructure Console.

Documentation Accessibility

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

Access to Oracle Support

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

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Resources

For more information, see these Oracle resources:

- Oracle Cloud Infrastructure Process Automation documentation in the Oracle Cloud Library on the Oracle Help Center.

Conventions

The following text conventions are used in this document:

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

1

Get Started

Oracle Cloud Infrastructure Process Automation helps you to rapidly design, automate, and manage business processes in the cloud.

Explore the following topics to get started with Oracle Cloud Infrastructure Process Automation.

- [Overview of Oracle Cloud Infrastructure Process Automation](#)
- [Service Types](#)
- [Process Automation Roles](#)
- [Administrative Interfaces](#)

Overview of Oracle Cloud Infrastructure Process Automation

Oracle Cloud Infrastructure Process Automation helps you to rapidly design, automate, and manage business processes in the cloud.

With Oracle Cloud Infrastructure Process Automation you can:

- Design structured and dynamic processes
- Model decisions
- Connect to other applications
- Create forms
- Track and manage user tasks

Designer and Workspace environments

The Process Automation development and runtime management environments enables you to perform iterative process automation development.

- Use **Designer**, the design-time environment, to create and edit process applications and their components. This environment is for process automation developers.
- Use **Workspace**, the runtime environment, to test, run, monitor, and administer process applications. This environment is for administrators and end users.

Want to learn more about how to use Process Automation? See *Using Oracle Cloud Infrastructure Process Automation*.

Explore REST APIs

You can use REST APIs to work with applications, processes, and user tasks. See available endpoints in *REST API for Oracle Cloud Infrastructure Process Automation*.

Service Types

Oracle Cloud Infrastructure Process Automation is available in three models - as an individual or standalone Oracle Cloud Infrastructure service, as a service paired with a Fusion-based Oracle Cloud Applications service (such as HCM Cloud or CX Cloud), and as a service enabled with Oracle Integration 3.

- **Individual Oracle Cloud Infrastructure (OCI) service:** When you order Process Automation as an individual service, you provision and set up the service instance from the OCI console.

Explore topics in this guide to set up Oracle Cloud Infrastructure Process Automation as an individual Oracle Cloud Infrastructure service.

- **Paired with Fusion-based Oracle Cloud applications:** Process Automation service instances paired with Fusion-based Oracle Cloud Applications such as Oracle Human Capital Management (HCM) Cloud or Oracle Customer Experience (CX) Cloud, are designed for you to use and extend existing out of the box features that are provided by Fusion-based Oracle Cloud Applications.

When you get Process Automation in this way, it is automatically provisioned for you. You give team members access to the instance in the Oracle Identity Cloud Service (IDCS) application of the service instance. See *Use Process Automation with Fusion-Based Oracle Cloud Applications* in *Using Oracle Cloud Infrastructure Process Automation*.

- **Enabled with Oracle Integration 3:** Process Automation service instances can be enabled and provisioned with Oracle Integration 3 Enterprise Editions. See [Enable Process Automation with Oracle Integration 3](#).

When Process Automation is provisioned in this way, and predefined IDCS application roles are assigned for managing access to the Process Automation and Oracle Integration design-time, you can use active integrations from Oracle Integration that are designed with REST triggers into your process applications. Thus, optimizing your business processes to communicate and exchange data with other applications and services in the cloud. See *Work with Integrations* in *Using Oracle Cloud Infrastructure Process Automation*.

Process Automation Roles

There are different types of roles in Oracle Cloud Infrastructure Process Automation. Understanding how they work together is essential to giving users the access they need to perform their tasks.

Cloud Account Administrator role

Cloud Account Administrators are set up when the Oracle Cloud account is created. They use their Oracle Cloud account to sign in to Oracle Cloud and access the Oracle Cloud Infrastructure Console.

Cloud Account Administrators can use the Oracle Cloud Infrastructure console to perform the following actions:

- Monitor and manage services for one or more Cloud accounts.
- Create and manage users and groups.
- Provide access to services by assigning IDCS application roles.

IDCS Application roles

There are two predefined Oracle Identity Cloud Service (IDCS) application roles in Oracle Cloud Infrastructure Process Automation: **ServiceAdministrator** and **ServiceDeveloper**. These are functional roles that determine whether or not a user has access to the Workspace Administration section and Designer user interfaces.



Note:

You *do not* require the IDCS application roles for accessing Workspace user interfaces or runtime APIs. Any authenticated user can work in Workspace or access runtime APIs.

| Role | Description |
|-----------------------------|--|
| ServiceAdministrator | <ul style="list-style-type: none"> Grants full administrative privileges within the Process Automation instance. Allows users to access the Administration section in Workspace and work on administrative tasks under it. See <i>Workspace Administration</i> in <i>Using Oracle Cloud Infrastructure Process Automation</i>. Allows users to manage process application roles in Workspace. |



Note:

Users assigned the ServiceAdministrator role are also referred to as **Process Automation Administrators** in Oracle Cloud Infrastructure Process Automation.

| | |
|-------------------------|---|
| ServiceDeveloper | <ul style="list-style-type: none"> Allows users to access Designer and create, manage and activate process applications and its components. Allows users to create and configure process application roles in Designer. |
|-------------------------|---|



Note:

Users assigned the ServiceDeveloper role are also referred to as **Process Automation Designers** in Oracle Cloud Infrastructure Process Automation.

You assign IDCS application roles to users in Oracle Identity Cloud Service.

- [Assign IDCS Application Roles to Groups in an Identity Domain](#)
- [Assign IDCS Application Roles to Groups](#)

Process Application roles

To further define data access and task permissions for users and groups, you can configure roles specific to process applications in your Process Automation instance. See *About Process Application Roles* in *Using Oracle Cloud Infrastructure Process Automation*.

Each process application role is comprised of users/groups and permissions. See *Users, Groups and Permissions* in *Using Oracle Cloud Infrastructure Process Automation*.

You can work with process application roles in Designer and Workspace Administration section.

- Create and configure process application roles in Designer. See *Work with Roles in Designer* in *Using Oracle Cloud Infrastructure Process Automation*. You have to be a Process Automation Designer (assigned the ServiceDeveloper IDCS application role) to work with process application roles in Designer.

- Manage process application roles under the Administration section in Workspace. See *Manage Roles in Workspace* in *Using Oracle Cloud Infrastructure Process Automation*. You have to be a Process Automation Administrator (assigned the ServiceAdministrator IDCS application role) to work with process application roles in Workspace.

Administrative Interfaces

There are different interfaces used to administer and manage your services.

- Oracle Cloud Infrastructure Console — Use the Oracle Cloud Infrastructure Console to create and manage your Oracle Cloud resources.
- Oracle Identity Cloud Service (IDCS) Console — Manage users and groups in IDCS.
- Administration: Workspace — Use the Workspace Administration section to:
 - Manage global and process application roles
 - Manage notifications
 - Manage global and application credentials
 - Specify data management settings
 - Register new cloud services with Process Automation

See *Workspace Administration* in *Using Oracle Cloud Infrastructure Process Automation*.

2

Before You Begin

For provisioning and administering Oracle Cloud Infrastructure Process Automation, you must sign in to the Oracle Cloud Infrastructure console and create a compartment.

Topics:

- [Sign In to the Oracle Cloud Infrastructure Console](#)
- [Create a Compartment](#)

Sign In to the Oracle Cloud Infrastructure Console

Signing into the Oracle Cloud Infrastructure Console differs depending on whether or not your tenancy uses identity domains.

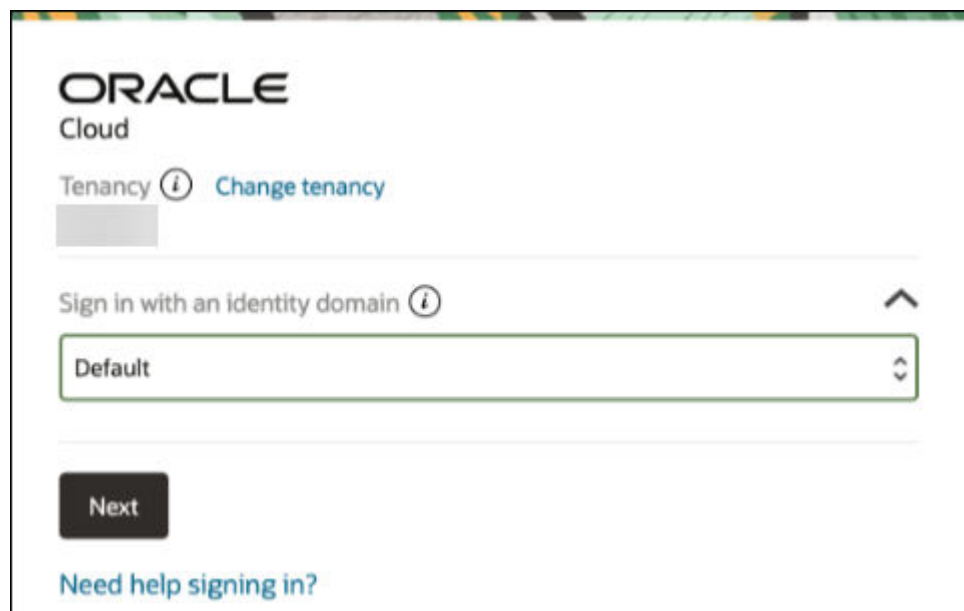
If you are not sure if your tenancy uses identity domains, see [Differences Between Tenancies With and Without Identity Domains](#).

- [Sign In to the Console in Tenancies That Use Identity Domains](#)
- [Sign In to the Console in Tenancies That Do Not Use Identity Domains](#)

Sign In to the Console in Tenancies That Use Identity Domains

If your tenancy uses identity domains, you sign in to the Oracle Cloud Infrastructure Console as a user configured in Oracle Cloud Infrastructure Identity and Access Management (IAM).

1. Go to <http://cloud.oracle.com>.
2. Enter your tenancy name and click **Next**.
3. Leave the **Default** domain selected, and click **Next**.



The screenshot shows the Oracle Cloud sign-in page. At the top left is the Oracle logo and the word "Cloud". Below that is a "Tenancy" field with an information icon and a "Change tenancy" link. A text input field is present below the tenancy field. Underneath is a "Sign in with an identity domain" section with an information icon and an upward arrow. A dropdown menu is open, showing "Default" as the selected option. At the bottom left is a dark "Next" button. At the bottom center is a link that says "Need help signing in?".

Note that you can click the **Sign in with an identity domain** drop-down list to view all available identity domains in your tenancy. If required, you can select a domain of your choice from the list instead of the default domain.

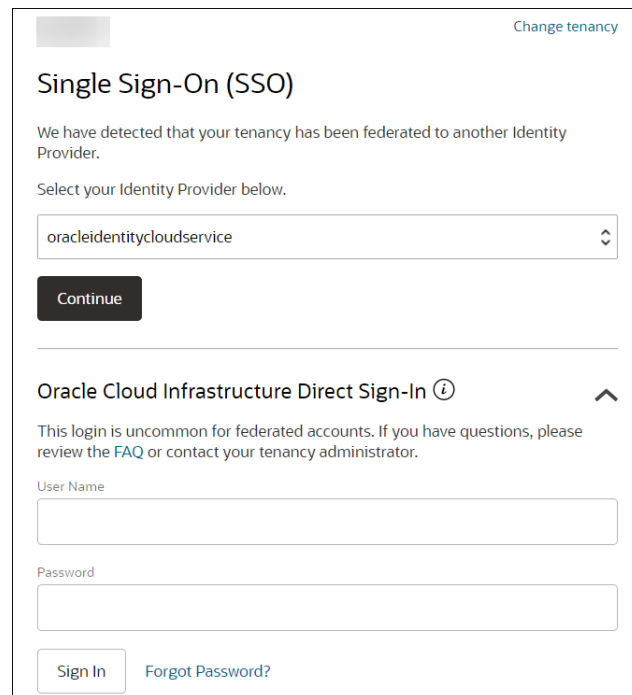
4. Enter the user name and password provided in the welcome email, and click **Sign In**.
The Oracle Cloud Infrastructure Console is displayed.
5. Explore categories and options in the navigation menu.
 - Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Process Automation**. Use this landing page to access, create, and manage Oracle Cloud Infrastructure Process Automation instances.
 - Open the navigation menu and click **Identity & Security**. Under **Identity**, click identity links to create compartments if needed, and to perform tasks related to identity management. See [Manage Access and Assign Roles](#).

Sign In to the Console in Tenancies That Do Not Use Identity Domains

If your tenancy does not use identity domains, you sign in to the Oracle Cloud Infrastructure Console as a user federated through Oracle Identity Cloud Service (IDCS). A federated environment enables business partners to integrate in the identity management realm by providing a mechanism for users to share identity information across respective security domains.

1. Go to <http://cloud.oracle.com>.
2. Enter your tenancy name and click **Next**.

Identity options are displayed.



The screenshot shows the Oracle Cloud Infrastructure console sign-in page for federated accounts. At the top right, there is a "Change tenancy" link. The main heading is "Single Sign-On (SSO)". Below this, a message states: "We have detected that your tenancy has been federated to another Identity Provider. Select your Identity Provider below." A dropdown menu is open, showing "oracleidentitycloudservice" as the selected option. Below the dropdown is a "Continue" button. A horizontal line separates this section from the "Oracle Cloud Infrastructure Direct Sign-In" section, which has an information icon. A message below the heading reads: "This login is uncommon for federated accounts. If you have questions, please review the FAQ or contact your tenancy administrator." There are two input fields: "User Name" and "Password". At the bottom, there is a "Sign In" button and a "Forgot Password?" link.

- The *upper* portion displays federated sign in (Oracle Cloud Infrastructure Process Automation is federated with Oracle Identity Cloud Service).

- The *lower* portion displays native Identity and Access Management (IAM) options standard to Oracle Cloud Infrastructure.

Under Single Sign-On (SSO) options, note the identity provider selected in the **Identity Providers** field and click **Continue**.

The Oracle Identity Cloud Service sign in screen is displayed.

3. Enter the user name and password provided in the welcome email, and click **Sign In**.

The Oracle Cloud Infrastructure Console is displayed.

4. Explore categories and options in the navigation menu.
 - Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Process Automation**. Use this landing page to access, create, and manage Oracle Cloud Infrastructure Process Automation instances.
 - Open the navigation menu and click **Identity & Security**. Under **Identity**, click identity links to create compartments if needed, and to perform tasks related to identity management. See [Manage Access and Assign Roles](#).

Create a Compartment

Compartments enable you to partition resources in Oracle Cloud Infrastructure so that you can better control access to those resources. To create an Oracle Cloud Infrastructure Process Automation instance, you must first create a compartment, unless you want to create the instance in the root compartment.

See [Managing Compartments](#).

1. In the Oracle Cloud Infrastructure Console home page, open the navigation menu, and click **Identity & Security**. Under **Identity**, click **Compartments**.

A list of the compartments in your tenancy is displayed. Note that if there are existing compartments, you can also choose to create your Process Automation instance in an existing compartment.

2. Click **Create Compartment**.
3. Enter the following details:
 - **Name:** Enter a name that is unique across all compartments in your tenancy (maximum 100 characters, including letters, numbers, periods, hyphens, and underscores). For example, enter a name such as `OCIPACompartment`.
 - **Description:** Enter a description for this compartment.
 - **Tags:** Enter tags to organize and list resources based on your business needs. See [Managing Tags and Tag Namespaces](#).
4. Click **Create Compartment**.

3

Manage Access and Assign Roles

The steps for managing access to Oracle Cloud Infrastructure Process Automation differ, depending on whether or not your region was updated to use identity domains prior to creation of your tenancy.

To give people access to Process Automation, create users, assign them to groups, and then assign preconfigured roles to the groups. Assign policies to groups to give people access to resources.

These tasks differ depending on whether your region uses identity domains.

Topics:

- [Differences Between Tenancies With and Without Identity Domains](#)
- [About IAM Policies for Process Automation](#)
- [Manage Access in an Identity Domain](#)
- [Manage Access Without an Identity Domain](#)

Differences Between Tenancies With and Without Identity Domains

Setting up users, groups, and policies for access to Oracle Cloud Infrastructure Process Automation differs depending on whether or not your tenancy uses identity domains.

Where You Manage Users and Groups

Beginning in March 2023, Oracle began a region-by-region migration of all tenancies to use identity domains. Tenancy owners will be notified two weeks prior to the migration of their tenancy. All IDCS instances in the tenancy will be converted at the same time regardless of the IDCS home region.

Your tenancy already uses identity domains if Oracle updated your region to use identity domains before you created your tenancy. However, if Oracle updated your region to use identity domains after you created your tenancy, then your tenancy will be migrated.

The migration to identity domains includes the migration of all users, groups, and roles. During the period that Oracle is migrating tenancies, you manage users, groups, and roles depending on the status of your tenancy:

- Manage users, groups, and roles in Oracle Cloud Infrastructure Identity and Access Management (IAM) if either of the following are true:
 - Oracle updated your region to use identity domains before you created your tenancy
 - Or, Oracle has migrated existing tenancies in your region to use identity domains

In either scenario, you do not use Oracle Identity Cloud Service (IDCS) or federation to manage users and groups.

- Manage users, groups, and roles in both IDCS and Oracle Cloud Infrastructure IAM, linked using federation, if both of the following are true:

- Oracle updated your region to use identity domains after you created your tenancy
- And, Oracle has not yet migrated existing tenancies in your region to use identity domains

Determine Whether a Tenancy Uses Identity Domains

To determine whether or not your tenancy uses identity domains, open the Oracle Cloud Infrastructure navigation menu and click **Identity & Security**. Under **Identity**, check for **Domains**:

- If **Domains** is listed, then your tenancy uses identity domains. See [Manage Access in an Identity Domain](#).
- If **Domains** is not listed, then your tenancy is still configured to link identities in IDCS and IAM using federation. See [Manage Access Without an Identity Domain](#).

About Identity Domains

An identity domain is a container for managing users and roles and performing other access-related tasks. Every tenancy contains a Default identity domain, and you can create additional identity domains as needed to hold different user populations.

Identity domains offer several benefits, including improved performance and scalability and a unified experience for administration. For more information, see [Managing Identity Domains](#).

Differences

The following table outlines the differences between the two configurations.

| Tenancies that use Identity Domains | Tenancies that do not use Identity Domains |
|--|---|
| Users and groups are configured in IAM. | Users and groups are configured in IAM and IDCS, linked through federation. See Understand Federation . |
| The IAM service provides a single unified console for managing users, groups, dynamic groups, and applications in <i>domains</i> . | IAM must be federated with IDCS for your tenancy. |
| Provides Single Sign-On to more applications using a single set of credentials and a unified authentication process. | Requires separate federated credentials for IDCS. |
| The Federation page does not list any IDCS entries. | The Federation page lists the primordial IDCS type that is automatically federated as part of the tenancy creation. |

About IAM Policies for Process Automation

Use Oracle Cloud Infrastructure Identity and Access Management (IAM) to control access to resources in your tenancy. For example, you can create a policy that authorizes users to create and manage Oracle Cloud Infrastructure Process Automation instances.

You create IAM policies using the Oracle Cloud Infrastructure Console. See [Managing Policies](#) in the Oracle Cloud Infrastructure documentation.

Resource Type

The resource type available for Process Automation is `process-automation-instance`.

Supported Variables

The `process-automation-instance` resource type can use the following variables.

| Supported Variables | Variable | Variable Type | Description |
|---|---|----------------|---|
| Required Variables Supplied by the Service for Every Request | <code>target.compartment.id</code> | ENTITY | The OCID of the primary resource for the request. |
| | <code>request.operation</code> | STRING | The operation ID (for example <code>GetUser</code>) for the request. |
| | <code>target.resource.kind</code> | STRING | The resource kind name of the primary resource for the request. |
| Automatic Variables Supplied by the SDK for Every Request | <code>request.user.id</code> | ENTITY | For user-initiated requests. The OCID of the calling user. |
| | <code>request.groups.id</code> | LIST (ENTITY) | For user-initiated requests. The OCIDs of the groups of <code>request.user.id</code> . |
| | <code>target.compartment.name</code> | STRING | The name of the compartment specified in <code>target.compartment.id</code> . |
| Dynamic Variables Computed Implicitly by IAM Authorization | <code>target.tenant.id</code> | ENTITY | The OCID of the target tenant id. |
| | <code>request.principal.group.tag.tagNS.tagKey</code> | STRING | The value of each tag on a group of which the principal is a member. |
| | <code>request.principal.compartment.tag.tagNS.tagKey</code> | STRING | The value of each tag on the compartment that contains the principal. |
| | <code>target.resource.tag.tagNS.tagKey</code> | STRING | The value of each tag on the target resource. (Computed based on <code>tagSlug</code> supplied by service on each request.) |
| | <code>target.resource.compartment.tag.tagNS.tagKey</code> | STRING | The value of each tag on the compartment that contains the target resource. (Computed based on <code>tagSlug</code> supplied by service on each request.) |

Details for Verb + Resource-Type Combinations

This table shows the permissions and API operations covered by each verb. The level of access is cumulative as you go from `INSPECT` to `READ` to `USE` to `MANAGE`.

| Verb | Permissions | APIs Fully Covered | APIs Partially Covered |
|----------------|--|--|------------------------|
| INSPECT | <code>PROCESS_AUTOMATION_INSTANCE_INSPECT</code> | <ul style="list-style-type: none"> <code>ListProcessInstances</code> <code>ListWorkRequests</code> | None |
| READ | Inherits from <code>INSPECT</code> : <ul style="list-style-type: none"> <code>PROCESS_AUTOMATION_INSTANCE_INSPECT</code> <code>PROCESS_AUTOMATION_INSTANCE_READ</code> | <ul style="list-style-type: none"> <code>GetProcessInstance</code> <code>GetWorkRequest</code> | None |

| Verb | Permissions | APIs Fully Covered | APIs Partially Covered |
|---------------|--|--|------------------------|
| USE | Inherits from READ: <ul style="list-style-type: none"> PROCESS_AUTOMATION_INSTANCE_INSPECT PROCESS_AUTOMATION_INSTANCE_READ PROCESS_AUTOMATION_INSTANCE_UPDATE | <ul style="list-style-type: none"> UpdateProcessInstances | None |
| MANAGE | Inherits from USE: <ul style="list-style-type: none"> PROCESS_AUTOMATION_INSTANCE_INSPECT PROCESS_AUTOMATION_INSTANCE_READ PROCESS_AUTOMATION_INSTANCE_UPDATE PROCESS_AUTOMATION_INSTANCE_CREATE PROCESS_AUTOMATION_INSTANCE_DELETE PROCESS_AUTOMATION_INSTANCE_MOVE | <ul style="list-style-type: none"> CreateProcessInstance DeleteProcessInstance ChangeProcessCompartment | None |

Permissions Required for Each API Operation

This table lists the API operations available for Process Automation and the permissions required to use each of the operations.

| API Operation | Permissions Required to Use the Operation |
|--------------------------|---|
| ListProcessInstances | PROCESS_AUTOMATION_INSTANCE_INSPECT |
| GetProcessInstance | PROCESS_AUTOMATION_INSTANCE_READ |
| CreateProcessInstance | PROCESS_AUTOMATION_INSTANCE_CREATE |
| DeleteProcessInstance | PROCESS_AUTOMATION_INSTANCE_DELETE |
| UpdateProcessInstances | PROCESS_AUTOMATION_INSTANCE_UPDATE |
| ListWorkRequests | PROCESS_AUTOMATION_INSTANCE_INSPECT |
| GetWorkRequest | PROCESS_AUTOMATION_INSTANCE_READ |
| ChangeProcessCompartment | PROCESS_AUTOMATION_INSTANCE_MOVE |

Manage Access in an Identity Domain

For a tenancy in a region updated to use identity domains prior to the creation of the cloud account, users and groups are managed in only Oracle Cloud Infrastructure Identity and Access Management (IAM).

Determine Whether You Use Identity Domains

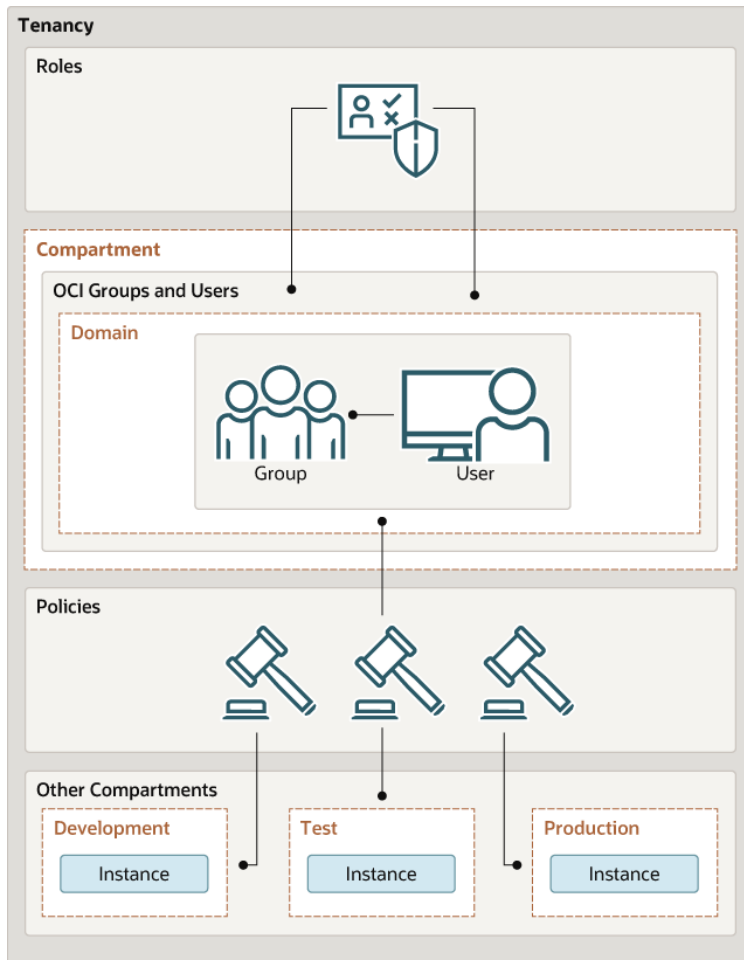
If you are not sure if your tenancy uses identity domains, see [Differences Between Tenancies With and Without Identity Domains](#).

Documentation for Identity Services

For more information about IAM, IDCS, and the documentation that provides the information you need, see *Documentation to Use for Cloud Identity* in [Overview of IAM](#) in the Oracle Cloud Infrastructure documentation.

How Roles Are Assigned in Identity Domains

With identity domains, roles are assigned to IAM groups within a domain, as illustrated in the following diagram.



Topics:

- [Create an Identity Domain](#)
- [Create an IAM Group in an Identity Domain](#)
- [Create an IAM Policy in an Identity Domain](#)
- [Create a User in an Identity Domain](#)
- [Assign IDCS Application Roles to Groups in an Identity Domain](#)

Create an Identity Domain

Create an identity domain in which to configure users, groups, and policies.

 **Note:**

This topic applies only to tenancies that use identity domains. See [Differences Between Tenancies With and Without Identity Domains](#).

For more information about identity domains, see [Managing Identity Domains](#) in the Oracle Cloud Infrastructure documentation.

In an Oracle Cloud Infrastructure tenancy (cloud account) your environment includes a root (default) compartment and possibly several other compartments, depending on how your environment is configured. To create compartments, see [Create a Compartment](#). Within each compartment, you can create users and groups. For example, as a best practice:

- In the root (default) compartment, use the default domain for administrators only.
- In another compartment (for example, named **Dev**), create a domain for users and groups in a development environment.
- In another compartment (for example, named **Prod**), create a domain for users and groups in a production environment.

You can also create multiple domains in a single compartment.

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**. The Domains page is displayed.
2. If not already selected, select the **Compartment** where you want to create the domain.
3. Click **Create domain**.
4. Enter required information in the Create domain page. See [Creating Identity Domains](#) in the Oracle Cloud Infrastructure documentation.

Create an IAM Group in an Identity Domain

Create a group, such as an instance administrator group, in an identity domain.

 **Note:**

This topic applies only to tenancies that use identity domains. See [Differences Between Tenancies With and Without Identity Domains](#).

For more information about IAM groups in identity domains, see [Managing Groups](#) in the Oracle Cloud Infrastructure documentation.

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**. The Domains page is displayed.
2. If not already selected, select the **Compartment** in which the domain where you want to create the group resides.

3. In the **Name** column, click the domain in which you want to create the group for creating and managing instances.
The domain Overview page is displayed.
4. Click **Groups**.
The Groups page for the domain is displayed.
5. Click **Create group**.
6. In the Create group window, assign a name to the group (for example, `oci-pa-admins`), and enter a description.
7. Click **Create**.

Create an IAM Policy in an Identity Domain

Create a policy to grant permissions to users in a domain group to work with Oracle Cloud Infrastructure Process Automation instances within a specified tenancy or compartment.

Note:

This topic applies only to tenancies that use identity domains. See [Differences Between Tenancies With and Without Identity Domains](#).

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Policies**.
2. Click **Create Policy**.
3. In the Create Policy window, enter a name (for example `ProcessAutomationGroupPolicy`) and a description.
4. In the Policy Builder, select **Show manual editor** and enter the required policy statements.

Syntax:

- `allow group domain-name/group_name to verb resource-type in compartment compartment-name`
- `allow group domain-name/group_name to verb resource-type in tenancy`

Example: `allow group admin/oci-pa-admins to manage process-automation-instance in compartment PACompartment`

Note:

If you omit the domain name, the default domain is assumed.

This policy statement allows the `oci-pa-admins` group in the `admin` domain to manage instance `process-automation-instance` in compartment `PACompartment`.

When defining policy statements, you can specify either verbs (as used in these steps) or permissions (typically used by power users).

Want to learn more about policies?

- See [How Policies Work](#) and [Policy Reference](#).
- See [About IAM Policies for Process Automation](#).

5. If desired, you can add a policy to allow members of the group to view service metrics as described in [View Service Metrics](#).

For example: allow group oci-pa-admins to read metrics in compartment PCompartment

6. Click **Create**.

The policy statements are validated and syntax errors (if any) are displayed.

Create a User in an Identity Domain

Create a user to assign to a group in an identity domain.

Note:

This topic applies only to tenancies that use identity domains. See [Differences Between Tenancies With and Without Identity Domains](#).

For more information about users in identity domains, see [Managing Users](#) in the Oracle Cloud Infrastructure documentation.

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**.
The Domains page is displayed.
2. If not already selected, select the **Compartment** in which the domain that contains the group to which you want to add a new user resides.
3. In the **Name** column, click the domain for the group in which you want to create the user.
The domain Overview page is displayed.
4. Click **Users**.
The Users page of the domain is displayed.
5. Click **Create user**.
6. In the Create user window, enter the user's first and last name, and their username. Then select one or more groups to which the user should be assigned.
7. Click **Create**.
The new user is added to the selected group(s) and has permissions assigned to the group by its policy statement.
8. On the user details page that is displayed, you can edit user information as needed, and reset the user's password.
9. Provide new users with the credentials they need to sign in to their tenancy. Upon signing in, they will be prompted to enter a new password.

Assign IDCS Application Roles to Groups in an Identity Domain

After an Oracle Cloud Infrastructure Process Automation instance is created, you must assign IDCS application roles to groups of users in Oracle Identity Cloud Service (IDCS) to allow them

to access the Workspace Administration and Designer user interfaces of the Process Automation instance.


 **Note:**

This topic applies only to tenancies that use identity domains. See [Differences Between Tenancies With and Without Identity Domains](#).

 **Note:**

It's a best practice to assign IDCS application roles to selected groups rather than individual users.

There are two predefined IDCS application roles in Oracle Cloud Infrastructure Process Automation: **ServiceAdministrator** and **ServiceDeveloper**. To learn more, see the IDCS Application roles section in [Process Automation Roles](#).

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**.
The Domains page is displayed.
2. If not already selected, select the **Compartment** in which the domain that contains the group to which you want to assign Process Automation roles resides.
3. In the **Name** column, click the domain for the group to which you want to assign roles.
The domain Overview page is displayed.
4. In the navigation pane, click **Oracle Cloud Services**.
The Oracle Cloud Services page is displayed.
5. In the Oracle Cloud Services page, navigate to the Process Automation service instance for which you want to assign group roles.
You can also search for the service instance by entering the prefix or string that begins the Process Automation service instance's display name.
6. Click the Process Automation service instance to open the instance details page.
7. Under **Resources**, click **Application roles**.
The available IDCS application roles are displayed.
8. In the Application roles list, locate the role(s) that you want to assign to the group. At the far right, click **Open Details** .
9. Next to **Assigned groups**, click the **Manage** link.
10. On the Manage group assignments pane, click **Show available groups**.
11. In the Available groups list, select the group to which to assign the role, and click **Assign**.

Manage Access Without an Identity Domain

For a tenancy in a region not yet updated to use identity domains prior to the creation of the tenancy, users and groups are set up in Oracle Cloud Infrastructure Identity and Access Management (IAM) and Oracle Identity Cloud Service (IDCS).

Determine Whether You Use Identity Domains

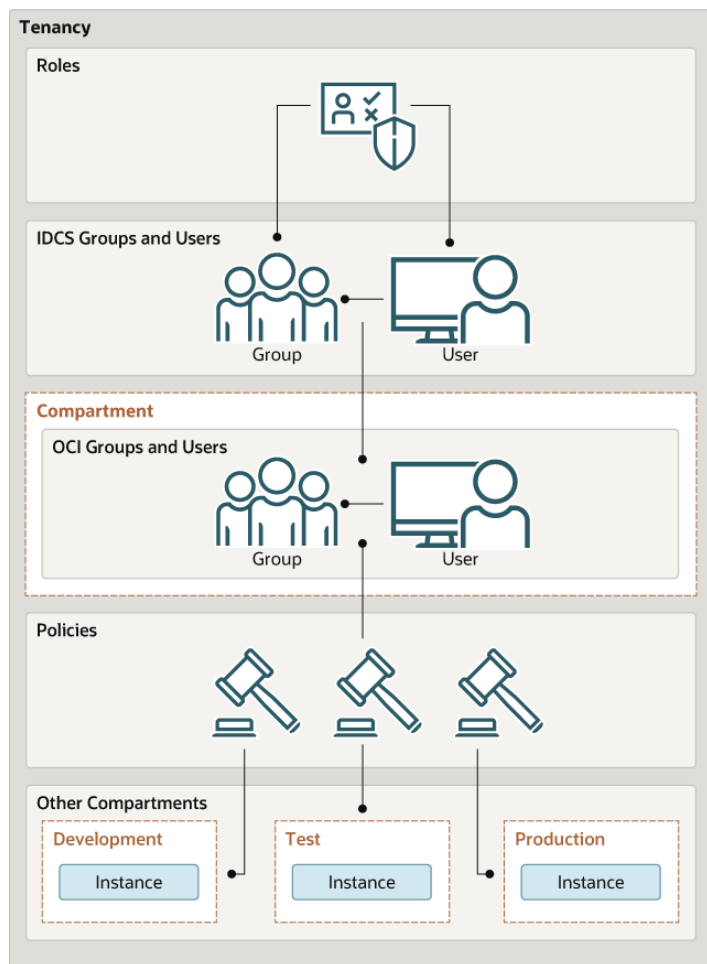
If you are not sure if your tenancy uses identity domains, see [Differences Between Tenancies With and Without Identity Domains](#).

Documentation for Identity Services

For more information about IAM, IDCS, and the documentation that provides the information you need, see *Documentation to Use for Cloud Identity* in [Overview of IAM](#) in the Oracle Cloud Infrastructure documentation.

How Roles Are Assigned in Identity Domains

Without identity domains, roles are assigned to IDCS groups, then linked to IAM groups using federation, as illustrated in the following diagram.



Topics:

- [Understand Federation](#)
- [Create an IDCS Group](#)
- [Create an IAM Group](#)
- [Create an IAM Policy](#)
- [Map the IDCS and IAM Groups](#)
- [Create IDCS Users](#)
- [Create IAM Users](#)
- [Assign IDCS Application Roles to Groups](#)
- [Configure Multiple Identity Stripes for Process Automation](#)

Understand Federation

If your tenancy does not use identity domains, Oracle Cloud Infrastructure Identity and Access Management (IAM) must be federated with Oracle Identity Cloud Service (IDCS) for your tenancy.



Note:

This topic applies only to tenancies that do not use identity domains. See [Differences Between Tenancies With and Without Identity Domains](#).

User federation refers to linking a user's identity and attributes across multiple identity management systems. Federation in Oracle Cloud Infrastructure Process Automation means that identities are linked in IDCS and IAM.

Oracle Cloud Infrastructure Process Automation uses both Oracle Identity Cloud Service (IDCS) and Oracle Cloud Infrastructure Identity and Access Management (IAM) to manage users and groups:

- Create and manage users in IDCS. By default, most tenancies are federated with IDCS. For more information, see Understanding Administrator Roles in *Administering Oracle Identity Cloud Service*.
- Manage permissions using policies in Oracle Cloud Infrastructure's IAM service.

For background information on federation with Oracle Identity Cloud Service, see [Federating with Identity Providers](#) and [Federating with Oracle Identity Cloud Service](#) in the Oracle Cloud Infrastructure documentation.

Create an IDCS Group

You can create Oracle Identity Cloud Service (IDCS) groups for later mapping them to Oracle Cloud Infrastructure Identity and Access Management (IAM) identities.



Note:

This topic applies only to tenancies that do not use identity domains. See [Differences Between Tenancies With and Without Identity Domains](#).

For more information, see [Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console](#) in the Oracle Cloud Infrastructure documentation.

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Federation**.
The Federation page is shown, and includes the identity provider, called **OracleIdentityCloudService**. This is the default federation between the IDCS stripe and the Oracle Cloud Infrastructure (OCI) tenancy in a tenancy.
2. Click the **OracleIdentityCloudService** link to view the default IDCS identity federation.
3. Click **Groups** from the **Resources** options.
4. Click **Create IDCS Group**.
5. In the Create IDCS Group dialog, enter a name (for example, `idcs-ocipa-admin`) and a description.
6. Click **Create**.

Create an IAM Group

You can create an instance administrator group in Oracle Cloud Infrastructure Identity and Access Management (IAM) and then map it to your previously created Oracle Identity Cloud Service (IDCS) group.



Note:

This topic applies only to tenancies that do not use identity domains. See [Differences Between Tenancies With and Without Identity Domains](#).

For more information about IAM groups, see [Managing Groups](#) in the Oracle Cloud Infrastructure documentation.

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Groups**.
The Groups page is displayed.
2. Click **Create Group**.
3. In the Create Group window, assign a name to the group that differentiates it from the IDCS group (for example, `oci-ocipa-admins`), and enter a description.
4. Click **Create**.

Create an IAM Policy

Create a policy to grant permission to users in a group to work with Oracle Cloud Infrastructure Process Automation instances within a specified tenancy or compartment.

Note:

This topic applies only to tenancies that do not use identity domains. See [Differences Between Tenancies With and Without Identity Domains](#).

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Policies**.
2. Click **Create Policy**.
3. In the Create Policy window, enter a name (for example, `ProcessAutomationGroupPolicy`) and a description.
4. In the **Policy Builder**, select **Show manual editor** and enter the required policy statements.

Syntax:

- `allow group group_name to verb resource-type in compartment compartment-name`
- `allow group group_name to verb resource-type in tenancy`

Example: `allow group oci-ocipa-admins to manage process-automation-instance in compartment PACompartment`

This policy statement allows the `oci-ocipa-admins` group to manage instance `process-automation-instance` in compartment `PACompartment`.

Want to learn more about policies?

- See [How Policies Work](#) and [Policy Reference](#).
 - See [About IAM Policies for Process Automation](#).
5. If desired, you can add a policy to allow members of the group to view service metrics as described in [View Service Metrics](#).

For example: `allow group oci-ocipa-admins to read metrics in compartment PACompartment`

6. Click **Create**.

The policy statements are validated and syntax errors (if any) are displayed.

Map the IDCS and IAM Groups

Map the group in Oracle Cloud Infrastructure Identity and Access Management (IAM) to the group that you created in Oracle Identity Cloud Service (IDCS).



Note:

This topic applies only to tenancies that do not use identity domains. See [Differences Between Tenancies With and Without Identity Domains](#).

For more information, see [Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console](#) in the Oracle Cloud Infrastructure documentation.

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Federation**.
2. On the Federation page, select the **OracleIdentityCloudService** link.
3. From the **Resources** options, choose **Group Mapping**.
4. Click **Add Mappings**.
5. In the Add Mappings dialog, select your IDCS group from the drop-down list in the **Identity Provider Group** field, and your IAM group in the **OCI Group** field.
6. Click **Add Mappings**.

Create IDCS Users

You can create Oracle Identity Cloud Service (IDCS) users for day to day interaction with services. These users authenticate through single sign-on and can be granted access to all services included in your Cloud account.



Note:

This topic applies only to tenancies that do not use identity domains. See [Differences Between Tenancies With and Without Identity Domains](#).

For more information, see [Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console](#) in the Oracle Cloud Infrastructure documentation.

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Federation**.
2. On the Federation page, select the **OracleIdentityCloudService** link to view the default IDCS federation.
3. Under **Resources** click **Users**.
4. In the **Users** section, click **Create User**.
5. In the Create IDCS User dialog, complete the fields to identify the user.
In the **Groups** field, select the IDCS group you want this user to belong to.
6. Click **Create**.

A message is displayed that the user was created. Optionally, click the **Email Password Instructions** button to email a change password link to the new user.

The new user is displayed in the table of users. Notice that the user's federation was automatically triggered if the user was added to a federated IDCS group, and is displayed in the **OCI Synched User** column.

Create IAM Users

You can create Oracle Cloud Infrastructure Identity and Access Management (IAM) users for less typical user scenarios, such as emergency administrator access.



Note:

This topic applies only to tenancies that do not use identity domains. See [Differences Between Tenancies With and Without Identity Domains](#).

For more information about IAM users, see [Managing Users](#) in the Oracle Cloud Infrastructure documentation.

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Users**.
2. Click **Create User**.
3. In the resulting page, select **IAM User**.
4. Fill the required fields, and click **Create**.
5. Add the user to an IAM group with specific access.
 - a. Under **Identity**, select **Groups**.
 - b. From the groups list, click the group to which you want to add the user.
 - c. Click **Add User to Group**.
 - d. In the Add User to Group dialog, select the user you created from the drop-down list in the **Users** field, and click **Add**.
6. Create the user's password.
 - a. From the Group Members table on the Group Details screen, select the user you added.
 - b. Click **Create/Reset Password**. The Create/Reset Password dialog is displayed with a one-time password listed.
 - c. Click **Copy**, then **Close**.
7. Provide read only users the information they need to sign in.
 - a. Copy the password in an email to the user.
 - b. Instruct the user to sign in using the **User Name** and **Password** fields.
 - c. Upon signing in, the user will be prompted to change the password.

Assign IDCS Application Roles to Groups

After an Oracle Cloud Infrastructure Process Automation instance is created, you must assign IDCS application roles to groups of users in Oracle Identity Cloud Service (IDCS) to allow them

to access the Workspace Administration and Designer user interfaces of the Process Automation instance.

 **Note:**

This topic applies only to tenancies that do not use identity domains. See [Differences Between Tenancies With and Without Identity Domains](#).

 **Note:**

It's a best practice to assign IDCS application roles to selected groups rather than individual users.

There are two predefined IDCS application roles in Oracle Cloud Infrastructure Process Automation: **ServiceAdministrator** and **ServiceDeveloper**. To learn more, see the IDCS Application roles section in [Process Automation Roles](#).

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Federation**.
2. On the Federation page, select the **OracleIdentityCloudService** link to view the default Oracle Identity Cloud Service identity federation.
3. On the Identity Provider Details page, select the **Identity Provider Information** tab (if not selected already) and click the **Oracle Identity Cloud Service Console** link.


The IDCS console page opens.

4. Open the IDCS navigation menu, and click **Oracle Cloud Services**.
5. In the Oracle Cloud Services page, navigate to the Process Automation service instance for which you want to assign group roles.

You can also search for the service instance by entering the prefix or string that begins the Process Automation service instance's display name.

6. Click the instance to open the instance details page.
7. Click the **Application Roles** tab.

The available IDCS application roles are displayed.

8. Select the role that you want to assign. In the tile for the role, click  and then select **Assign Groups**.
9. In the Assign Group dialog, select the group(s) to which you want to assign the role, and click **Assign**.

Configure Multiple Identity Stripes for Process Automation

For Oracle Cloud Infrastructure Process Automation, the primary (primordial) stripe is automatically federated using preconfigured groups. However, you can create separate environments for a single cloud service or application (for example, create one environment for development and one for production), where each environment has a different identity and security requirements.



Note:

This topic applies only to tenancies that do not use identity domains. See [Differences Between Tenancies With and Without Identity Domains](#).

Implementing one or more secondary stripes enables you to create and manage multiple instances of Oracle Identity Cloud Service to protect your applications and Oracle Cloud services.

You can manually federate one or more secondary stripes with Oracle Cloud Infrastructure using SAML IDP federation in which multiple Oracle Identity Cloud Service stripes are associated with the same cloud account. Note that the account owner administers both primary and secondary stripes, but identities within the stripes are isolated from each other.

First, define a naming convention for the striping, as described in [Define a Stripe Naming Convention](#). Then follow the steps below to manually federate a secondary stripe for your cloud account. You must be the account owner.

1. [Create an IDCS Group for Secondary Stripe Users](#)
2. [Create an OAuth Client in the Secondary Stripe](#)
3. [Create an IAM Group for Secondary Stripe Users](#)
4. [Create the Federation and its Group Mapping](#)
5. [Create an IAM Policy for Federated Users to Create Instances](#)
6. [Provide Access to a Federated Stripe in the IAM Group for Secondary Stripe Users](#)
7. [Create Process Automation Instances in the Secondary Stripe Compartments](#)

Define a Stripe Naming Convention

As a best practice, define a `<stripename>` for all the entities you'll create specific to the stripe. Uniquely identifying configurations associated with a stripe is important, especially when multiple stripes are configured.

In the sections that follow, you'll use `stripename` in these entities:

| Entity | Naming convention |
|-------------------|--|
| IDCS group | <code>stripename_administrators</code> |
| OCI group | <code>oci_stripename_administrators</code> |
| Compartment | <code>stripename_compartment</code> |
| Identity Provider | <code>stripename_service</code> |
| Policy | <code>stripename_adminpolicy</code> |
| Policy Statement | <code>allow group oci_stripename_administrators to manage process-automation-instance in compartment stripename_compartment</code> |

Create an IDCS Group for Secondary Stripe Users

In IDCS, create a group in the secondary stripe and add users from the secondary stripe to the group.

1. Add a group in the secondary stripe, and name it `stripename_administrators`. For example, name it as `stripe2_administrators`. Click **Finish**.

These administrators will be granted permission to create Process Automation instances. This IDCS group will be mapped with an IAM group. See [Map the IDCS and IAM Groups](#).

2. Add users from the secondary stripe to the group.

Create an OAuth Client in the Secondary Stripe

Create an IDCS confidential application that uses OAuth client credentials and is assigned the IDCS domain administrator role. You must create a confidential application per secondary stripe.

1. As an IDCS administrator, sign in to the secondary IDCS admin console.
2. Add a confidential application.
 - a. Navigate to the **Applications** tab.
 - b. Click **Add**.
 - c. Choose **Confidential Application**.
 - d. Name the application `Client_Credentials_For_SAML_Federation`.
 - e. Click **Next**.
3. Configure client settings.
 - a. Click **Configure this application as a client now**.
 - b. Under **Authorization**, select **Client Credentials**.
 - c. Under **Grant the client access to Identity Cloud Service Admin APIs**, click **Add** and select the app role **Identity Domain Administrator**.
 - d. Click **Next** twice.
4. Click **Finish**. Once the application is created, note its client ID and client secret. You'll need this information in upcoming steps for federation.
5. Click **Activate** and confirm activating the application.

Create an IAM Group for Secondary Stripe Users

This group is needed because the Oracle Cloud Infrastructure SAML IDP federation requires group mapping for federating users from the federated IDP (IDCS), and OCI native group membership is required for defining and granting Oracle Cloud Infrastructure permissions (policies) for federated users.

1. In the Oracle Cloud Infrastructure Console, open the navigation menu and click **Identity & Security**. Under **Identity**, click **Groups**.

This IAM group will be mapped with the IDCS group you created.

2. Create a group and name it `oci_stripename_administrators`. For example, name it `oci_stripe2_administrators`.

Create the Federation and its Group Mapping

Now that you have the IDCS and IAM groups created and the client information needed, create the IDCS identity provider and map the groups.

1. Sign in to the Oracle Cloud Infrastructure console. Select the identity domain of the primordial stripe (identitycloudservice) and enter its user credentials.

Keep in mind that group mapping for a secondary stripe uses the primordial stripe user sign in. This is important, since adding multiple stripes adds multiple options to this dropdown.

2. Open the navigation menu and click **Identity & Security**, then **Federation**.
3. Click **Add Identity Provider**.
4. In the resulting window, complete the fields as shown below.

| Field | Information to Enter |
|---|---|
| Name | <stripename>_service |
| Description | Federation with IDCS secondary stripe |
| Type | Oracle Identity Cloud Service |
| Oracle Identity Cloud Service Base URL | Enter the following URL using the format: https://idcs-xxxx.identity.oraclecloud.com Replace the <idcs-xxxx> domain part with your secondary IDCS stripe. |
| Client ID/Client Secret | Enter the client ID and secret that you obtained while creating an OAuth client in the secondary stripe. See Create an OAuth Client in the Secondary Stripe . |
| Force Authentication | Select this option. |

5. Click **Continue**.
6. Map the IDCS secondary stripe and OCI groups you previously created.
Map the IDCS secondary stripe group (created in [Create an IDCS Group for Secondary Stripe Users](#)) and the OCI group (created in [Create an IAM Group for Secondary Stripe Users](#)).
7. Click **Add Provider**.
The secondary stripe federation is complete. Notice that the group mapping is displayed.
8. Verify the secondary stripe, and configure visibility for secondary stripe administrators and users.
 - The tenant administrator can see all federated IDCS stripes in the OCI console.
 - The secondary stripe administrator and all other secondary stripe users will not see any stripes under federation. To resolve that, see [Provide Access to a Federated Stripe in the IAM Group for Secondary Stripe Users](#).

Create an IAM Policy for Federated Users to Create Instances

With the federation done, set up IAM policies that allow federated users from the secondary IDCS stripe to create Oracle Cloud Infrastructure Process Automation instances. As a common pattern, the policy is scoped to a compartment.

1. Create a compartment where Oracle Cloud Infrastructure Process Automation instances for the secondary IDCS stripe can be created. Name the compartment *stripename_compartment*.

For example, create a compartment named *stripe2_compartment*.

2. Create a policy that will allow federated users to create Oracle Cloud Infrastructure Process Automation instances in the compartment. Name the policy `stripename_adminpolicy` (for example, `stripe2_adminpolicy`).

Under Policy Builder, select **Show manual editor**.

- **Syntax:** `allow group stripename_administrators to verb resource-type in compartment stripename_compartment`
- **Policy:** `allow group oci_stripe2_administrators to manage process-automation-instance in compartment stripe2_compartment`

This policy allows a user who is a member of the group in the policy to create an Oracle Cloud Infrastructure Process Automation instance (**process-automation-instance**) in the compartment named **stripe2_compartment**.

Provide Access to a Federated Stripe in the IAM Group for Secondary Stripe Users

Perform additional steps to enable the secondary stripe administrator and all other secondary stripe users to see stripes under federation.

1. In Oracle Identity Cloud Service, create a group called `stripe2_federation_administrators`.
2. Add users to the group that you want to be able to see the federation and to create users and groups in the Oracle Cloud Infrastructure console in that stripe.
3. In the Oracle Cloud Infrastructure console, using the primary stripe user with the correct permission, create an IAM group called `oci_stripe2_federation_administrators`.
4. Map the `stripe2_federation_administrators` and `oci_stripe2_federation_administrators` groups.
5. Using the following statement examples, define a policy that grants access to federated stripes.

Several of the examples show how to grant access to a specific federated stripe, by using a `where` clause that identifies the secondary stripe.

You can get the federation's OCID from the federation view in the Oracle Cloud Infrastructure console.

| Allows secondary stripe administrators to... | Policy statement |
|---|---|
| Create groups (use) | <code>allow group oci_stripe2_federation_administrators to use groups in tenancy</code> |
| List the identity providers in the federation (inspect) | <code>allow group oci_stripe2_federation_administrators to inspect identity-providers in tenancy</code> Note that if the secondary stripe admins are required to create groups, this policy is required when a <code>where</code> clause is included. |
| Access a specific federated stripe (use) | <code>allow group oci_stripe2_federation_administrators to use identity-providers in tenancy where target.identity- provider.id="ocid1.saml2idp.oc1..aaaa aaaa..."</code> |

When you sign in as a user in the above IDCS group, you can create users and groups in the Oracle Cloud Infrastructure console and assign permissions as you would in a primary stripe.

Create Process Automation Instances in the Secondary Stripe Compartments

With federation and Oracle Cloud Infrastructure policies defined, federated users can sign into the Oracle Cloud Infrastructure Console and create Oracle Cloud Infrastructure Process Automation instances.

1. Sign in as a federated user from the secondary stripe.

Users will need to select the secondary stripe in the **Identity Provider** field. For example, `stripe2_administrators`.

2. Authorized administrators can create Process Automation instances in the specified compartment (for example, `stripe2_compartment`).

4

Provision and Manage Oracle Cloud Infrastructure Process Automation Instances

Provision and manage Oracle Cloud Infrastructure Process Automation instances in the Oracle Cloud Infrastructure Console.



Note:

As a tenancy administrator, you have the permissions required to create and edit Process Automation instances. To allow other users to perform these tasks, you must complete the steps to manage users and groups for access to Process Automation. These steps differ depending on whether or not your tenancy uses identity domains. See [Differences Between Tenancies With and Without Identity Domains](#).

Topics:


- [Provision a Process Automation Instance](#)
- [Access the Process Automation Instance](#)
- [Delete a Process Automation Instance](#)
- [Edit a Process Automation Instance](#)
- [View Instance Details](#)
- [Stop and Start a Process Automation Instance](#)
- [Move an Instance to a Different Compartment](#)
- [Create an Access Token to Provision an Instance](#)
- [Enable Process Automation with Oracle Integration 3](#)

Provision a Process Automation Instance

You can provision an Oracle Cloud Infrastructure Process Automation instance in a selected compartment.

1. Sign in to the Oracle Cloud Infrastructure Console.
Note your selected region. Once created, instances are visible only in the region in which they were created. For information about regions, see [Regions and Availability Domains](#).
2. Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Process Automation**.
3. From the **Compartment** drop-down list, select the compartment in which you want to create the instance.
The page is refreshed to show any existing instances in the selected compartment.
4. Click **Create**.

- In the Create instance dialog, enter the following details:

| Field | Information to Enter |
|---|--|
| Name | Enter the display name of the instance. |
| Description | Enter the description of the instance. |
| Access Token | Enter the access token. For details on how to obtain the access token, see Create an Access Token to Provision an Instance . |
| <div style="border: 1px solid #ccc; padding: 10px; background-color: #e6f2ff;"> <p> Note:</p> <p>If your tenancy uses identity domain or federated IDCS stripe, and the home region of the identity domain or IDCS stripe with which you have signed in is same as the region in which you are creating the Oracle Cloud Infrastructure Process Automation instance, then the access token is <i>prefetched</i> for you.</p> </div> | |
| Shapes | Select the instance shape: <ul style="list-style-type: none"> Development: Choose this shape for development, staging, or testing instances. Production: Choose this shape for production instances. |
| Metering model | Select a metering model: <ul style="list-style-type: none"> Execution pack: You can use this model if you're looking for usage based pricing based on transactions. A single execution pack consists of 10,000 execution activities. The first 10,000 activities are free and after that each execution pack consumed will be charged. Note that an <i>activity</i> can be any part of the process flow that is executed in runtime. For example, human tasks, notifications, service calls, start/end events and so on. Users: You can use this model if you know the number of users that you want to onboard to the service. An <i>active user</i> can be any user who accesses the service for tasks related to design, operation, development, and so on. Any user who interacts with the service through REST APIs will also be counted as an active user. Note that one or multiple interactions of a user with the service in the duration of an hour is counted as one active user. |
| Tags (optional) | Optionally, click the Show Advanced Options link to add tags to the instance. You can use tags to search for and categorize your instances in your tenancy. See Resource Tags . |

- Click **Create instance**.

Access the Process Automation Instance

After you've provisioned a Oracle Cloud Infrastructure Process Automation instance, you can access it from the Oracle Cloud Infrastructure Console.

- Sign in to the Oracle Cloud Infrastructure Console.
- Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Process Automation**.
- From the **Compartment** drop-down list, select the compartment in which you created your Process Automation instance.

The existing instances in the selected compartment are listed.

4. You can filter down further by instance states. Under Filters, select **Active** from the **State** drop-down list.
5. Click the instance to open the instance details page.
6. On the instance details page, click **Open console** to access the Process Automation instance login page.

If a message appears that access was denied, you don't have access to Process Automation Designer (design-time).

For users to access the Process Automation Designer, they have to be assigned the **ServiceDeveloper** IDCS application role. See:

- [Assign IDCS Application Roles to Groups](#)
- [Assign IDCS Application Roles to Groups in an Identity Domain](#)

Delete a Process Automation Instance


You can delete an Oracle Cloud Infrastructure Process Automation instance.



Note:

Deleting an Oracle Cloud Infrastructure Process Automation instance cannot be undone. This action permanently removes all design-time and runtime data.

You can delete an instance in either of two ways:

1. From the main Oracle Cloud Infrastructure Console page for Oracle Cloud Infrastructure Process Automation.
 - a. Identify the instance to delete.
 - b. On the far right, click  and select **Delete**.
 - c. In the Delete instance dialog, click **Delete**.

A message displays that the instance is being deleted. The state of the instance shows as *Deleting*. Once the instance is deleted, the instance state changes to *Deleted*.

2. From the Instance details page of an existing Oracle Cloud Infrastructure Process Automation instance.
 - a. Click the instance name that you want to delete in the Oracle Cloud Infrastructure Console.
 - b. Click **Delete**.
 - c. In the Delete instance dialog, click **Delete**.

A message displays that the instance is being deleted. The state of the instance shows as *Deleting*. Once the instance is deleted, the instance state changes to *Deleted*.

Edit a Process Automation Instance

You can edit the display name and description of an Oracle Cloud Infrastructure Process Automation instance.

1. From the Instance details page of an existing Oracle Cloud Infrastructure Process Automation instance, click the instance name that you want to edit.
2. Click **Edit**.
3. In the Edit instance dialog:
 - Update the instance name in the **Display name** field.
 - Optionally, update the description in the **Description** field.
4. Click **Save changes** to save your changes.

View Instance Details

You can view details about a provisioned Oracle Cloud Infrastructure Process Automation instance and perform tasks such as editing an instance, deleting an instance, moving an instance to another compartment, adding tags and so on.

1. Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Process Automation**.
2. From the list of Oracle Cloud Infrastructure Process Automation instances that display, click a specific instance.

The instance details page appears. The following table describes the key information shown on the instance details page:

| Field | Description |
|---------------------|--|
| Details tab | <ul style="list-style-type: none"> • Description of the instance. • The date and time on which the instance was created. • The date and time on which the instance was updated. • Selected consumption (billable) model. • OCID value that uniquely identifies the instance, which can be shown in full and easily copied. • Process Automation Designer URL which can be shown in full and easily copied. • Process Automation Workspace URL which can be shown in full and easily copied. • Selected instance shape. • Selected metering model. |
| Tags tab | Click to view the tags created for the instance. |
| Open console | <p>For federated users, click to access the design time environment (Designer) of the Oracle Cloud Infrastructure Process Automation instance directly.</p> <p>For non-federated users, click to open the Sign in page to access Oracle Cloud Infrastructure Process Automation.</p> |
| Edit | Click to edit the display name and description of the instance. See Edit a Process Automation Instance . |
| Move | Click to move the instance to another compartment. See Move an Instance to a Different Compartment . |

| Field | Description |
|----------------------------|---|
| Add tags | Click to add tags to the instance. You can use tags to search for and categorize your instances in your tenancy. |
| Delete | Click to delete the instance. See Delete a Process Automation Instance . |
| Metrics | Displays metrics for executed activities and active users. |
| Work Requests | Lists instance life cycle activities, such as instance creation, updates and so on. Click a work request to see log and error message metrics. |
| Associated services | Lists services that are associated with the instance. For example, if an Oracle Integration instance is associated with the Process Automation, the Oracle Integration instance will be listed on the Associated services page. |

Stop and Start a Process Automation Instance


You can stop and start any standalone Oracle Cloud Infrastructure Process Automation instances. To stop or start a child Process Automation instance, you have to perform the action on the parent Oracle Integration instance. After a stop request is initiated, the Process Automation instance goes into the inactive state. During the inactive state, no new processes are started. Inactive service instances are paused. When the processes are no longer running, the Process Automation instance goes into a completely inactive state. During this state, the workspace and designer capabilities are unavailable.



Note:

Oracle recommends the following:

- Do not stop Process Automation instances running in a production environment.

1. Start or stop a Process Automation instance in either of two ways:
 - a. On the Process Automation Instances page, go to the end of the row for the specific instance, and click .

Note that an active Process Automation instance is identified as **Active** and an inactive/stopped Process Automation instance is identified as **Inactive** in the **State** column.
 - b. On the details page of a specific Process Automation instance, click the **More Actions** menu.
2. Select the action to perform:
 - To stop your Process Automation instance, select **Stop**, then select **Stop** again when prompted to confirm your selection.

The instance state changes to **Updating** during the pausing process. When complete, the state changes to **Inactive** in the **State** column.

This action causes the following to occur:

- For execution pack and active user SKU based instances, the billing stops for the duration that the instance is paused.
- Database purging continues to run.
- REST APIs are unavailable for use. If you attempt to use the APIs while your Process Automation instance is in a paused state, you receive an error message.
- To resume your Process Automation instance, select **Start**, then select **Start** again when prompted to confirm your selection.

 **Note:**

You cannot start an Process Automation instance when maintenance and security patching are in progress.

The Process Automation instance state changes to **Updating** during the resumption. When complete, the state changes to **Active** in the **State** column.

Move an Instance to a Different Compartment

You can move an Oracle Cloud Infrastructure Process Automation instance to a different compartment.


 **Note:**

Moving an instance can potentially change who has access to the instance. For example, if a user has the manage or read permission for one compartment and you move the instance to another compartment, the user loses access. Ensure that users have necessary permissions for the compartment to which you want to move the instance.

 **Note:**

Moving an instance affects access within the Oracle Cloud Infrastructure Console only (view or manage permissions). Access to an Oracle Cloud Infrastructure Process Automation instance does not change.

You can move an instance in either of two ways.

1. From the main Oracle Cloud Infrastructure Console page for Oracle Cloud Infrastructure Process Automation.
 - a. Identify the instance to edit.
 - b. On the far right, click  and select **Move**.
 - c. In the Move to another compartment dialog, select the compartment to which you want to move the instance from the drop-down list in the **Compartment** field, and click **Move**.
2. From the Instance details page of an existing Oracle Cloud Infrastructure Process Automation instance.

- a. Click the instance name that you want to edit in the Oracle Cloud Infrastructure Console.
- b. Click **Move**.
- c. In the Move to another compartment dialog, select the compartment to which you want to move the instance from the drop-down list in the **Compartment** field, and click **Move**.

The instance is available in the compartment to which it was moved.

Create an Access Token to Provision an Instance

Generally, the access token for provisioning an Oracle Cloud Infrastructure Process Automation instance is prefetched for users that sign in to tenancies using identity domains or federated Oracle Identity Cloud Service (IDCS) stripes. However, in some cases users may need to manually create the access token for provisioning an Oracle Cloud Infrastructure Process Automation instance.

Create an access token to provision a Process Automation instance in the following scenarios:

- Your tenancy uses identity domain, but the home region of the identity domain with which you have signed in is different from the region in which you want to create the Process Automation instance. See [Create an Access Token in a Tenancy That Uses Identity Domain](#).
- Your tenancy uses federated IDCS stripe, but the home region of the federated stripe with which you have signed in is different from the region in which you want to create the Process Automation instance. See [Create an Access Token in a Tenancy That Do Not Use Identity Domain](#).
- Your tenancy does not use identity domain, and you have signed in with direct sign-in option (not with federated IDCS stripe) using Oracle Cloud Infrastructure Identity and Access Management (IAM). See [Create an Access Token in a Tenancy That Do Not Use Identity Domain](#).
- You want to create a Process Automation instance by using Process Automation control plane REST APIs.

Topics:

- [Create an Access Token in a Tenancy That Uses Identity Domain](#)
- [Create an Access Token in a Tenancy That Do Not Use Identity Domain](#)
- [Generate the Access Token from the CLI or an API](#)

Create an Access Token in a Tenancy That Uses Identity Domain

The following sections walk you through the steps required to create an application and generate an access token in a tenancy that uses identity domain.

Create an Application

1. Sign in as the tenant administrator to the Oracle Cloud Infrastructure Console.
2. Open the Oracle Cloud Infrastructure navigation menu, and click **Identity & Security**. Under **Identity** click **Domains**.
3. Select the identity domain you want to work in.

The domain Overview page is displayed.

4. From the left navigation menu, click **Applications**.
5. In the Applications page, click **Add application**.
6. In the Add application dialog, click **Confidential Application**, and click **Launch workflow**.

The Add Confidential Application wizard opens.

7. Enter a name for the app and a suitable description, and then click **Next**.
8. Click **Configure this application as a client now**.
9. Provide the following information to configure this application as a client.

- a. Under Authorization, select one or more grant types.

Process Automation supports the following grant types:

- **Resource owner**
- **JWT assertion**
- **Authorization code**
- **Implicit**

- b. If you selected **Authorization code** or **Implicit** grant types, then enter the application URL where the user is redirected after authentication in the **Redirect URL** field. Otherwise, skip this step.

 **Note:**

You don't have to configure the application as a resource server.

10. In the Token issuance policy section, configure the following.
 - a. Select **Add app roles**.
 - b. Click **Add roles**. In the Add app roles window, select the application role that you want to assign to this application, and click **Add**.

For example, select **Identity Domain Administrator** and click **Add**. All REST API tasks available to the identity domain administrator will be accessible to your application.

11. Click **Next**.
12. Select **Skip and do later**, then click **Finish**.

The application has been added in a deactivated state.
13. Note the **Client ID** and **Client secret** that appear in the Application added dialog box. To integrate with your confidential application, you can use this ID and secret as part of your connection settings.

14. Click **Close**.

The new application's detail page is displayed.

15. Click **Activate**, and confirm the activation.

Generate an Access Token

After creating the application, you can use the app to generate the access token required to create an Oracle Cloud Infrastructure Process Automation instance.

1. Sign in as the tenant administrator to the Oracle Cloud Infrastructure Console.
2. Open the Oracle Cloud Infrastructure navigation menu, and click **Identity & Security**. Under **Identity** click **Domains**.
3. Select the identity domain you want to work in.
The domain Overview page is displayed.
4. From the left navigation menu, click **Applications**.
5. On the Applications page, select the application that you created.
6. Scroll down on the app details page, and in the left under **Resources** click **Access token**.
7. Leave the default selections. In the following example, **Customized Scopes, Invokes Identity Cloud Service APIs** and **Identity Domain Administrator** are selected by default.
8. Click **Download Token** and save the file.
The `tokens.tok` file contains the access token with the attribute name `access_token`.

```
tokens.tok
{"access_token":"eyJ4NXQjUzI. . . . ."}


```

9. Provide the part of the access token between the quotes to the user to use for provisioning an instance. Do *not* provide the part labeled `access_token`.

Create an Access Token in a Tenancy That Do Not Use Identity Domain

The following sections walk you through the steps required to create an application and generate an access token in a tenancy that *do not* use identity domain.

Create an Application

1. Sign in to the Oracle Identity Cloud Service (IDCS) administrator console.
2. Click  on the upper left, and from the menu options that display, select **Applications**.
3. On the Applications page, click **+Add**.
4. In the Add Application dialog, select **Confidential Application**.
The Add Confidential Application Wizard appears.
5. Enter a name and an optional description, and click **Next**.
6. Select **Configure this application as a client now**. Then provide the following information for configuring the app as a client, and click **Next**.
 - a. Under the Authorization section, provide details for client authorization.

| Field | Information to Enter |
|----------------------------|--|
| Allowed Grant Types | Select one or more grant types. Oracle Cloud Infrastructure Process Automation supports the following grant types: <ul style="list-style-type: none"> • Resource Owner • JWT Assertion • Authorization Code • Implicit |

| Field | Information to Enter |
|---------------------------|--|
| Redirect URL | If you selected Authorization Code or Implicit grant types, enter the application URL where the user is redirected after authorization. Otherwise, leave this field blank. |
| Allowed Operations | Select Introspect . |

- b. Under **Grant the client access to Identity Cloud Service Admin APIs**, click **+ Add**.
 - i. In the Add App Role dialog, select **Identity Domain Administrator** and click **Add**.


 **Note:**

You don't have to configure the application as a resource server.

7. Select **Skip for later**, and click **Next**.
8. In the last page in the wizard, leave **Enforce Grants as Authorization** unselected, and click **Finish**.
A confirmation dialog lets you know that the application has been created.
9. Click **Activate**, then click **OK** to confirm that you want to activate the application.
The application is created and you can use it to generate the access token for users.

Generate an Access Token

After creating the application, you can use the app to generate the access token required to create an Oracle Cloud Infrastructure Process Automation instance.

1. Sign in to the Oracle Identity Cloud Service (IDCS) administrator console.
2. Click  on the upper left, and from the menu options that display, select **Applications**.
3. On the Applications page, click the application you created.
4. Click **Generate Access Token**.
5. In the Generate Token dialog, select **Customized Scopes**.

Note that the **Invokes Identity Cloud Service APIs** and **Identity Domain Administrator** are selected by default.

6. Click **Download Token** and save the file.

The `tokens.tok` file contains the access token with the attribute name `access_token`.

```
tokens.tok
{"access_token":"eyJ4NXQjUzI. . . . ."}

```

7. Provide the part of the access token between the quotes to the user to use for provisioning an instance. Do *not* provide the part labeled `access_token`.

Generate the Access Token from the CLI or an API

You can also generate the access token from the CLI or an API.

For example:

```
IDCS_AT_PWD=$(curl "${CURL_FLAGS}" -u
"$IDCS_CLIENT_ID:$IDCS_CLIENT_SECRET" $IDCS_URL/oauth2/v1/token -d
"grant_type=password&scope=urn:opc:idm:__myscopes__&username=${
IDCS_USERNAME}&password=${IDCS_PASSWORD}" | jq -r ".access_token")
```

Enable Process Automation with Oracle Integration 3

To use Process Automation with Oracle Integration, an administrator needs to enable it from an Oracle Integration service instance in the Oracle Cloud Infrastructure (OCI) Console.

When enabled, a Process Automation instance gets automatically provisioned with the Oracle Integration instance. In such a case, the two services become *associated* with each other and gets listed in each others Associated services page in the Oracle Cloud Infrastructure Console.

Key points about enabling Process Automation with Oracle Integration:

- You can enable Process Automation only with Oracle Integration 3 *Enterprise Edition*.
- You must ensure that the user who enables Process Automation with Oracle Integration must exist in the identity domain of the Oracle Integration instance and must have `MANAGE` permissions on Process Automation.
- You must ensure that you've set up the correct IAM policies to manage access to the Process Automation instance. See [Set Up IAM Policies to Manage Process Automation Instance](#).
- A Process Automation instance provisioned with Oracle Integration cannot be deleted independently. Such an instance is deleted whenever the Oracle Integration instance with which it is associated is deleted.
- A Process Automation instance provisioned with Oracle Integration must be in the same tenancy, region, and compartment as the Oracle Integration instance. You cannot move the instance to a different compartment.

Topics:

- [Set Up IAM Policies to Manage Process Automation Instance](#)
- [Enable Process Automation](#)
- [Assign IDCS Application Roles to Manage Access](#)

Set Up IAM Policies to Manage Process Automation Instance

To enable Process Automation with Oracle Integration, you need to create Oracle Cloud Infrastructure Identity and Access Management (IAM) policies that allow Oracle Integration administrators belonging to a specified IAM group to manage the Process Automation instance.

Set up the following IAM policies for Process Automation:

- **Syntax:** allow group <group_name> to manage process-automation-instances in compartment <compartment_name>

Example: allow group domain_admins to manage process-automation-instances in compartment oicpa_compartment

- **Syntax:** allow group `<group_name>` to read metrics in compartment `<compartment_name>`

Example: allow group `domain_admins` to read metrics in compartment `oicpa_compartment`

See [About IAM Policies for Process Automation](#) and [Create an IAM Policy in an Identity Domain](#).

For information on IAM policies for Oracle Integration, see [About IAM Policies for Oracle Integration](#) and [Create an IAM Policy in an Identity Domain for Oracle Integration in Provisioning and Administering Oracle Integration 3](#).

Enable Process Automation

To enable a Process Automation instance with an Oracle Integration instance:

1. Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Integration**.
2. From the **Compartment** drop-down list, select the compartment in which you want to provision and enable a Process Automation instance with an Oracle Integration instance.
The page is refreshed to show any existing service instances in the selected compartment.
3. Choose an existing instance or [create an Oracle Integration instance](#) and select it.
The Integration instance details page opens.
4. Click the **Enable** link for Process Automation on the Integration instance information tab.
5. When prompted, click **Enable** to confirm that you want to enable Process Automation.

Note the following:

- The Oracle Integration icon turns orange and its status changes to Updating.
 - It can take several minutes for the enablement to complete.
 - Once complete, that is when a Process Automation instance gets enabled and provisioned with the Oracle Integration instance, the Oracle Integration icon changes back to green with an Active status and Process Automation shows as Enabled.
6. To navigate to the Process Automation instance that just got created, click **Associated services** under **Resources**.
 7. Select the Process Automation instance and view its details.

See [View Instance Details](#).

Assign IDCS Application Roles to Manage Access

After you've enabled an Process Automation instance, assign predefined IDCS application roles to users so that they can work with the features of the Process Automation instance.

In Process Automation, there are two predefined IDCS application roles: **ServiceDeveloper** and **ServiceAdministrator**. These roles have to be assigned to users or groups in the Process Automation service instance application from the Oracle Identity Cloud Service (IDCS) admin console.

 **Note:**

The user who enables Process Automation with Oracle Integration 3 is automatically granted the ServiceAdministrator role.

- **ServiceDeveloper:** Any user who wants to access and work on Process Automation Designer has to be assigned the ServiceDeveloper role.
- **ServiceAdministrator:** Any user who wants full administrative privileges within Process Automation including administrative tasks in Workspace has to be assigned the ServiceAdministrator role.

As a best practice, it is recommended that you assign these roles to groups, rather than individual users. For example, assign the ServiceDeveloper IDCS application role to a group in both the Oracle Integration and Process Automation service instance applications from the Oracle Identity Cloud Service admin console. In this way it will be easier to manage user access, as any user who is a member of the group can access the Oracle Integration and Process Automation design-time.

For information on how to assign IDCS application roles for Process Automation and Oracle Integration, see:

- [Assign IDCS Application Roles to Groups in an Identity Domain](#)
- [Assign Oracle Integration Roles to Groups in an Identity Domain](#)

Now that a Process Automation instance is enabled and provisioned with an Oracle Integration instance, and IDCS application roles assigned, you can:

- Open the Process Automation Designer and Workspace user interfaces using the Designer and Workspace URLs displayed on the Details tab of the Process Automation instance details page.
- Open Oracle Integration by clicking the **Service Console** button from the Oracle Integration instance details page. From the navigation menu in the Oracle Integration home page, click the punch out URL for Process Automation. The Process Automation Designer opens in another browser tab and you can start designing your process applications.

5

Monitor Oracle Cloud Infrastructure Process Automation

You can monitor the health, capacity, and performance of Oracle Cloud Infrastructure Process Automation by using metrics, alarms, and notifications.

For more information, see [Monitoring Overview](#) and [Notification Overview](#).

This chapter describes the metrics emitted by the Oracle Cloud Infrastructure Process Automation service in the `oci_process_automation` metric namespace.

Topics:

- [Overview of Oracle Cloud Infrastructure Process Automation Service Metrics](#)
- [View Service Metrics](#)
- [Monitor Service Metrics, Alarms, and Notifications](#)

Overview of Oracle Cloud Infrastructure Process Automation Service Metrics

Oracle Cloud Infrastructure Process Automation service metrics help you measure the number of activities and users in Oracle Cloud Infrastructure. You can use metrics data to view and diagnose issues.

To view a default set of metrics charts in the Console, navigate to the service instance you're interested in, and then click **Metrics**. You can also use the Monitoring service to create [custom queries](#).

Prerequisites

Metrics are automatically available for any Oracle Cloud Infrastructure Process Automation service instance you create. You do not need to enable monitoring on the resource to get the metrics. However, you must meet the following prerequisites.

1. To get any metrics, at least one of the following events must happen:
 - One or more processes must run on the instance.
 - One or more users must access the instance.

Note that Oracle Cloud Infrastructure Process Automation instances with no running processes and no user activity emit no metric data.

2. To monitor resources, you must have permission to view message metrics for the compartment.
 - If you are an administrator with manage access, you can automatically view message metrics for the compartment. For manage access, you must be part of an Oracle Cloud Infrastructure group assigned a `manage` policy.

- If you are an administrator or a non-admin user with read only access, you must be part of an Oracle Cloud Infrastructure group assigned a `read metrics` policy. For example:
 - **Syntax:** `allow group group_name to verb resource-type in compartment compartment-name`
 - **Policy:** `allow group OpaMetricReaders to read metrics in compartment OCIPACompartment`

As an administrator, you can further restrict the scope of access to the specified metric namespace.

For example:

- **Syntax:** `allow group group_name to verb resource-type in compartment compartment-name where target.metrics.namespace='oci_process_automation'`
- **Policy:** `allow group OpaMetricReaders to read metrics in compartment OCIPACompartment where target.metrics.namespace='oci_process_automation'`

However, note that if you specify metric namespace in the policy, then as a non-admin user you won't be able to view namespace under **Metrics Explorer**.

See [Manage Access and Assign Roles](#).

Available Metrics: `oci_process_automation`

| Metric | Metric Display Name | Unit | Description | Emitted Information | Dimensions |
|-----------------------|--------------------------|-------|---|---|------------|
| ExecutedActivityCount | Activity Execution Count | Count | The number of activities that run per hour. | "displayName": "Executed Activity Count" "unit": "Activities" | resourceId |
| ActiveUserCount | Active User Count | Count | The number of active users per hour. | "displayName": "Active User Count" "unit": "Active Users Count" | resourceId |

Each metric includes the following dimensions:

- **RESOURCEID:** Oracle Cloud ID (OCID), which is the identifier for the service instance.
- **RESOURCENAME:** The name of the service instance, as specified when you created the instance.

Note:

Valid alarm intervals are 60 minutes or greater because of the frequency at which these metrics are emitted.

View Service Metrics

You can view the default metrics chart for a single Oracle Cloud Infrastructure Process Automation instance using the Oracle Cloud Infrastructure Console.

1. In the Oracle Cloud Infrastructure Console, open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Process Automation**.
2. From the list of Oracle Cloud Infrastructure Process Automation instances that display, click a specific instance.
3. On the left, under **Resources** click **Metrics**.

The metrics section displays a default set of charts for the instance.

- **Start Time** and **End Time** are selected at the top of the Metrics section. Change these values to select a different time period and view metrics for that time period.
- Change the **Interval** and **Statistic** fields for each chart to change the metrics displayed.
- Click **Options** on the top right of each chart to view the query in Metric Explorer, copy the chart URL, copy query, create an alarm on the query or to display the metrics in table view.

Monitor Service Metrics, Alarms, and Notifications

You can use Oracle Cloud Infrastructure monitoring and notification APIs to monitor metrics, alarms, and notifications.

- Use the [Monitoring API](#) for metrics and alarm.
- Use the [Notification API](#) for notifications (used with alarms).

A

Service Limits, Quotas, and Events

This section describes the Oracle Cloud Infrastructure Process Automation service limits, quotas, and events.

Topics:

- [Service Limits](#)
- [Set Instance Quotas on Compartments](#)
- [Automate with Events](#)

Service Limits

Review the following service limits for Oracle Cloud Infrastructure Process Automation resources. A service limit is the quota or allowance set on a resource.

Process Automation Instances Service Limits

| Resource | Service Limit |
|-----------------------------------|---|
| Process Automation instance count | 25 instances per Oracle Cloud Infrastructure (OCI) tenancy. |

Process Automation Components Service Limits

- [Applications](#)
- [Connectors](#)
- [Decisions](#)
- [Processes](#)
- [Roles](#)
- [Types](#)
- [UIs](#)

Table A-1 Applications

| Resource | Service Limit |
|--|---------------|
| Maximum number of process applications per instance | 100 |
| Maximum number of application/versions that can be activated per instance | 250 |
| Maximum number of application versions that can be created per application | 25 |
| Maximum number of <i>activated</i> application versions per application | 25 |
| Maximum number of snapshots per application | 200 |

Table A-2 Connectors

| Resource | Service Limit |
|--|---------------|
| Maximum number of connectors per application | 25 |
| Connector HTTP request read time out | 90 secs |
| Connector HTTP request connect time out | 3 secs |
| Connector request payload size | 50 KB |
| Connector response payload size | 50 KB |

Table A-3 Decisions

| Resource | Service Limit |
|---|---------------|
| Maximum number of decisions per application | 1 |
| Maximum number of concurrent executions for mutating PUT/PATCH/DELETE operations in Decision Lifecycle APIs | 1 |
| Maximum number of decision nodes per decision model | 50 |
| Maximum number of rules (rows) per decision table | 100 |
| Maximum number of input expressions (columns) per decision table | 5 |
| Maximum number of key/value pairs per context decision | 100 |
| Maximum number of conditions in if/else | 100 |
| Maximum number of entries in relation table | 100 |
| Maximum number of input data per decision | 100 |
| Maximum number of business types per decision | 100 |
| Maximum number of services per decision | 25 |
| Maximum number of levels in nested decisions | 2 |

Table A-4 Processes

| Resource | Service Limit |
|--|---------------|
| Maximum number of structured processes per application | 25 |
| Maximum number of dynamic processes per application | 25 |
| Maximum number of activities per structured process | 100 |
| Maximum number of activities per dynamic process | 100 |

Table A-5 Roles

| Resource | Service Limit |
|---|---------------|
| Maximum number of roles per application | 25 |

Table A-6 Types

| Resource | Service Limit |
|---|---------------|
| Maximum number of types per application | 100 |

Table A-7 UIs

| Resource | Service Limit |
|---|---------------|
| Maximum number of forms per application | 25 |
| Maximum number of components per form | 250 |

Other Service Limits

| Resource | Service Limit |
|--|--|
| Data plane requests | <ul style="list-style-type: none"> Number of data plane requests per sec (across all users) per service instance: 20 Number of data plane requests per sec per user per service instance: 5 |
| Attachments | <ul style="list-style-type: none"> Maximum attachment upload size: 15 MB Maximum number of native attachments per process instance: 20 Maximum number of native attachments per task instance: 10 |
| Maximum size of notification email payload | 2 MB |
| Number of execution loops in a process instance | 1000 |
| Variable size limit in a process instance | 50 KB |
| Retention period of a completed process instance before archival | 90 days |

 **Note:**

Depending on the usage of the system, archival can be triggered based on space usage thresholds also.

 **Note:**

The current service limits are set to ensure stability in your usage of the service and to prevent unintentional resource exhaustion. As the service scales up and grows, these limits may be expanded and changed to ensure best performance of the service.

Oracle Cloud Infrastructure also has service limits. See [Service Limits](#) in the Oracle Cloud Infrastructure documentation.

Set Instance Quotas on Compartments

You can set limits on the number of Oracle Cloud Infrastructure Process Automation instances that can be created in a compartment.

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Policies**.
2. Click **Create Policy**.
3. In the Create Policy window, enter a name (for example, `instanceCreationQuota`) and a description. Under Policy Builder, choose **Show manual editor**.
4. Complete the **Policy Statements** field.

For example, to set a quota limit of 10 instances for the compartment named `MyCompartment`, enter the following statement:

```
Set process-automation quota instance-count to 10 in compartment
MyCompartment
```

Where:

- `process-automation` is the family name for Oracle Cloud Infrastructure Process Automation.
 - `instance-count` is the quota name.
5. Click **Create**.

The policy statement is validated and any syntax errors are displayed.

Automate with Events

You can create automation based on state changes for your Oracle Cloud Infrastructure resources by using event types, rules, and actions.

Oracle Cloud Infrastructure services emit events, which are structured messages that indicate changes in resources. An Oracle Cloud Infrastructure Process Automation administrator can create rules to track these events, such as when instances are created, updated, or deleted, and compartments changed.

For more information, see [Overview of Events](#).

The following Oracle Cloud Infrastructure Process Automation resource emits events.

- `process-automation-instance`

Process Automation Instance Event Types

These are the event types that Process Automation instances emit.

| Friendly Name | Event Type |
|---|---|
| Create Process Automation Instance Begin | <code>com.oraclecloud.processautomation.creat eopainstance.begin</code> |
| Create Process Automation Instance End | <code>com.oraclecloud.processautomation.creat eopainstance.end</code> |

| Friendly Name | Event Type |
|--|--|
| Update Process Automation Instance Begin | com.oraclecloud.processautomation.updat eopainstance.begin |
| Update Process Automation Instance End | com.oraclecloud.processautomation.updat eopainstance.end |
| Delete Process Automation Instance Begin | com.oraclecloud.processautomation.delet eopainstance.begin |
| Delete Process Automation Instance End | com.oraclecloud.processautomation.delet eopainstance.end |
| Change Process Automation Instance Compartment Begin | com.oraclecloud.processautomation.chang eopainstancecompartment.begin |
| Change Process Automation Instance Compartment End | com.oraclecloud.processautomation.chang eopainstancecompartment.end |

Process Automation Instance Event Example

This is a reference event for Process Automation instances:

```
{
  "eventType": "com.oraclecloud.processautomation.createopainstance.begin",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "eventID": "<unique_ID>",
  "source": "process-automation",
  "eventTime": "2022-03-18T17:24:42.987Z",
  "contentType": "application/json",
  "extensions": {
    "compartmentId": "ocidl.compartment.oc1..<unique_ID>"
  },
  "data": {
    "compartmentId": "ocidl.compartment.oc1..<unique_ID>",
    "compartmentName": "example_compartment",
    "resourceName": "My test resource",
    "resourceId": "ocidl.processautomationinstance.oc1.phx.<unique_ID>",
    "availabilityDomain": "<availability_domain>",
    "freeFormTags": {
      "Department": "Finance"
    },
    "definedTags": {
      "Operations": {
        "CostCenter": "42"
      }
    },
    "additionalDetails": {
      "shape": "PRODUCTION",
      "isBreakglassEnabled": "false"
    }
  }
}
```