Oracle® Cloud

# Using Oracle Integration Generation 2 on Oracle Cloud Infrastructure US Government Cloud

F31941-14
November 2024

Oracle Cloud Using Oracle Integration Generation 2 on Oracle Cloud Infrastructure US Government Cloud,

F31941-14

Primary Author: Oracle Corporation

# Contents

# Preface

This guide describes how to use Oracle Integration Generation 2 in Oracle Cloud Infrastructure US Government environments.

**Topics:**

## Audience

This guide is intended for administrators who want to use Oracle Integration Generation 2 in an Oracle Cloud Infrastructure *US Government Cloud with FedRAMP* or *US Federal Cloud with DISA Impact Level 5 Authorization* environment. To use Oracle Integration Generation 2 in a commercial, UK government, or commercial US government environment, see Overview of Oracle Integration Generation 2 in *Provisioning and Administering Oracle Integration Generation 2*.

## 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 Integration documentation 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. |
| *italic* | Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values. |
| `monospace` | Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter. |

1

# Get Started with Oracle Integration on Oracle Cloud Infrastructure US Government Cloud

Oracle Integration is a fully managed service that allows you to integrate your cloud and on-premises applications.

With Oracle Integration, you can design integrations to monitor and manage connections between your applications, selecting from our portfolio of hundreds of prebuilt adapters and recipes to connect with Oracle and third-party applications.

**Topics:**

- How to Use This Guide
- About Oracle Integration Generation 2 on Oracle Cloud Infrastructure US Government Cloud
- Restrictions

## How to Use This Guide

This guide is intended for administrators using Oracle Integration Generation 2 in an Oracle Cloud Infrastructure US Government Cloud region.

This guide is intended to complement the documentation available in the Oracle Integration Generation 2 documentation library. Use this guide to learn about:

- Oracle Integration Generation 2 feature availability and restrictions in an Oracle Cloud Infrastructure US Government Cloud region.
- Tasks for setting up users and groups, provisioning an Oracle Integration Generation 2 instance, and viewing instance details in an Oracle Cloud Infrastructure US Government Cloud region.

## About Oracle Integration Generation 2 on Oracle Cloud Infrastructure US Government Cloud

Oracle Integration Generation 2 supports the following two levels of government operators:

- OC2 realm (Oracle Cloud Infrastructure US Government Cloud with FedRAMP Authorization) in the US Gov East (Ashburn) and West (Phoenix) regions
- OC3 realm (Oracle Cloud Infrastructure US Federal Cloud with DISA Impact Level 5 Authorization) in the US DoD East (Ashburn), North (Chicago), and West (Phoenix) regions

**Notes:**

- This guide is intended for administrators using Oracle Integration Generation 2 in the Oracle Cloud Infrastructure US Government Cloud regions listed above. To use Oracle Integration Generation 2 in a commercial or United Kingdom Government region, see the Oracle Integration documentation on the Oracle Help Center.
- In the OC2 realm, you can provision a new Oracle Integration Generation 2 instance only if your tenancy was created *before* 1 January 2023. After this date, Oracle updated regions in OC2 to use identity domains, and Oracle Integration Generation 2 instances do not support identity domains in OC2.

  If your tenancy was created *after* 1 January 2023, contact your Oracle Customer Success Manager or sales representative for assistance with provisioning a new Oracle Integration Generation 2 instance.
- In the OC3 realm, you can provision a new Oracle Integration Generation 2 instance regardless of when your tenancy was created, as regions in OC3 have not yet been updated to use identity domains.

For more information, see:

- Oracle Cloud Infrastructure US Government Cloud with FedRAMP Authorization
- Oracle Cloud Infrastructure US Federal Cloud with DISA Impact Level 5 Authorization

**Topics:**

- Oracle Integration Feature Availability on Oracle Cloud Infrastructure US Government Cloud
- Useful Resources for Oracle Integration on Oracle Cloud Infrastructure US Government Cloud

# Oracle Integration Feature Availability on Oracle Cloud Infrastructure US Government Cloud

Oracle Integration on Oracle Cloud Infrastructure US Government Cloud is available in both Standard and Enterprise editions, but not all features are available in US government realms. Review the following table for an overview of feature availability in Oracle Integration instances on Oracle Cloud Infrastructure US Government Cloud environments.

| Oracle Integration Features | Notes |
|---|---|
| Integrations | Available, except for the following:<br>• Accept mapping recommendations with the recommendations engine.<br>• Invoke a process from an integration.<br>• Map Insight milestones to integration actions. |
| Processes | Not available. |
| Visual Builder | Not available. |
| Insight | Not available. |
| File Server | Not available. |

| Oracle Integration Features | Notes |
|---|---|
| B2B | Not available. |
| Adapters | All Oracle Integration Adapters available. |
| Authentication | Client credentials is the only authorization grant flow supported for OAuth authentication in Oracle Cloud Infrastructure in government environments. |
| Announcements feature | Not available in Oracle Integration.<br>Note that Oracle Cloud Infrastructure announcements are available to Oracle Cloud Infrastructure administrators in the Oracle Cloud Infrastructure Console. |
| Oracle Assistant for Oracle Integration | Not available. |
| Upgrading from Oracle Integration Generation 2 to Oracle Integration 3 | Not available. |

## Useful Resources for Oracle Integration on Oracle Cloud Infrastructure US Government Cloud

Review the following documentation resources.

| Documentation | Notes and Main Differences in US Government Cloud |
|---|---|
| *What's New for Oracle Integration Generation 2*<br>*Known Issues for Oracle Integration Generation 2*<br>*Getting Started with Oracle Integration Generation 2*<br>*Using Integrations in Oracle Integration Generation 2*<br>Oracle Integration Adapters<br>*Provisioning and Administering Oracle Integration Generation 2* | When reviewing the Oracle Integration documentation, ignore references to features that are not currently supported in Oracle Cloud Infrastructure US Government Cloud, as listed in Oracle Integration Feature Availability on Oracle Cloud Infrastructure US Government Cloud. Also ignore references to Oracle Identity Cloud Service. In Oracle Cloud Infrastructure US Government Cloud environments, you use IAM to manage users and groups. |
| Oracle Cloud Infrastructure US Government Cloud with FedRAMP Authorization | Provides information specific to Oracle Cloud Infrastructure US Government Cloud with the FedRAMP High Joint Authorization Board. |
| Oracle Cloud Infrastructure US Federal Cloud with DISA Impact Level 5 Authorization | Provides information specific to Oracle Cloud Infrastructure US Federal Cloud with DISA Impact Level 5 authorization. |

# Restrictions

Note the following current restrictions when creating Oracle Integration instances and using them in Oracle Cloud Infrastructure US Government Cloud environments.

- **New Oracle Integration Generation 2 instances**

  You cannot provision a new Oracle Integration Generation 2 instance in the Oracle US Defense Cloud (realm key: OC3). Additionally, most organizations cannot provision a new Oracle Integration Generation 2 instance in the Oracle US Government Cloud (realm key: OC2). The only organization that can provision a new Oracle Integration Generation 2 instance in the Oracle US Government Cloud are tenancies that do not use identity domains. To create an Oracle Integration 3 instance, see Create an Oracle Integration Instance in *Using Oracle Integration 3 on Oracle Cloud Infrastructure US Government Cloud*.

- **Export and import of design-time metadata**

  US Government Cloud environments currently don't support export and import of design-time metadata between instances (see Import and Export Instances in *Provisioning and Administering Oracle Integration Generation 2*), whether you use the Import/Export page or the REST API Clone command in US Government Cloud environments. Note that you can import and export packages.

- **Credentials for API invocations**

  In US Government Cloud realm (OC2 and OC3) accounts, you can use login credentials (username and password) for console-based login flows. However, you can't use these login credentials for programmatic API invocations. To use a user account for Basic Auth authentication to invoke programmatic APIs, you must create an OAuth 2.0 client credential under that user account and use that credential as a Basic Auth credential. See Configure Basic Authentication Using Client Credentials.

- **Use of FTP Adapter with private keys**

  If you use the FTP Adapter with private keys (with a passphrase) in government environments, only OpenSSH-formatted keys are supported. RSA keys are not supported if the private key is associated with a passphrase.

- **Account for running scheduled integrations**

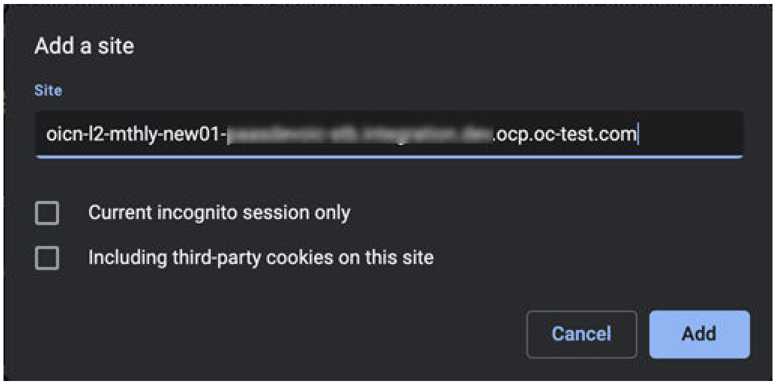
  To run a scheduled integration in an Oracle Cloud Infrastructure US Government Cloud environment, you must use a non-federated account. The user should ideally be a service account user profile, and not an actual in-person user account profile.

  If you use a federated account, the scheduler cannot trigger jobs and intermittently errors out with a `Schedule request submitted` message.

- **Logging out in an incognito browser**

  **For users working in Chrome incognito mode**: Add your Oracle Integration service instance application domain for third-party cookies as shown below. This workaround ensures users are logged out of their sessions after signing out.

  1. From an incognito browser window, click ⋮, then **Settings**.
  2. Select **Privacy and Security** from the left pane, then **Cookies and other site data**.
  3. Click **Add** next to **Sites that can always use cookies**.
  4. In the Add a site dialog that appears, enter your service instance application domain, leave the two checkboxes deselected, and click **Add**.



Add a site

Site

oicn-l2-mthly-new01-[redacted].ocp.oc-test.com

□ Current incognito session only

□ Including third-party cookies on this site

This ensures users are logged out of their sessions after signing out.

2

# Set Up Users and Groups on Oracle Cloud Infrastructure US Government Cloud

Configure users and groups in Oracle Cloud Infrastructure and grant them the right level of access.

**Topics:**

- Configure Access to Create and Manage Instances
- Configure OAuth Authentication in Oracle Cloud Infrastructure US Government Cloud Environments

## Configure Access to Create and Manage Instances

Create users and grant them permission to create and manage Oracle Integration instances.

A user's permissions to access Oracle Cloud Infrastructure services comes from the groups to which they belong. The permissions for a group are defined by policies. Policies define what actions members of a group can perform, and in which compartments. Users can then access services and perform operations based on the policies set for the groups in which they are members.

Extend Oracle Integration permissions to Oracle Cloud Infrastructure users by creating groups for key Oracle Integration roles, adding users to the groups, then creating policies that grant access to specified resources and permissions to users in those groups.

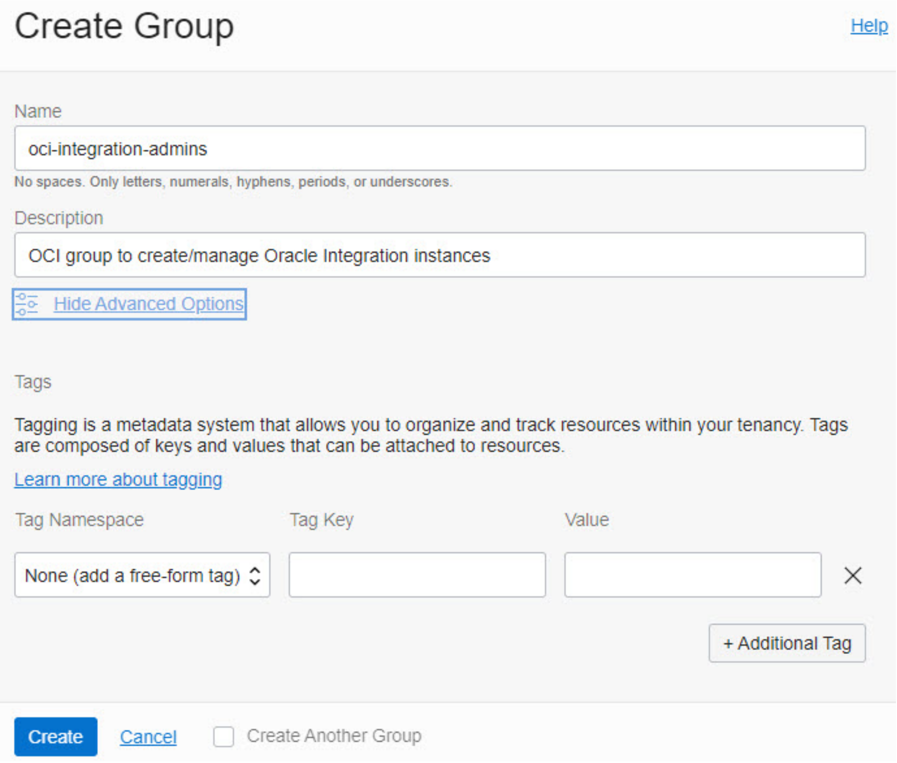
As an administrator, follow these main steps:

- Create an Oracle Cloud Infrastructure Group and Users
- Create an Oracle Cloud Infrastructure Policy
- Assign Policies to Oracle Integration Service Role Groups

### Create an Oracle Cloud Infrastructure Group and Users

To create an instance administrator group in Oracle Cloud Infrastructure IAM and add users to it:

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Groups**.
2. Click **Create Group**.
3. In the Create Group screen, assign a name to the group (for example, `oci-integration-admins`), and enter a description.



Create Group

Name

oci-integration-admins

No spaces. Only letters, numerals, hyphens, periods, or underscores.

Description

OCI group to create/manage Oracle Integration instances

Tags

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.

| Tag Namespace | Tag Key | Value |
|---|---|---|
| None (add a free-form tag) | | |

4. Click **Create**.
5. Add users to your new group so they can create and manage Oracle Integration instances.
   a. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Users**.
   b. Click **Create User**.
   c. Complete the following entries and click **Create**.
      - **Name:** A unique name or email address for the user. The name must be unique across all users in your tenancy. You cannot change this value later. The name must meet the following requirements: no spaces, only Basic Latin letters (ASCII), numerals, hyphens, periods, underscores, +, and @.
      - **Description:** This value could be the user's full name, a nickname, or other descriptive information. You can change this value later.
      - **Email:** Enter an email address for the user. This email address is used for password recovery. The email address must be unique in the tenancy. If the user forgets their password, they can click **Forgot Password** on the sign on page, and a temporary password is generated and sent to the email address provided here. The user or an administrator can also update the email address later.
   d. On the user details page, add users to the group.

> **Note:**
>
> For more information, see Managing Users in the Oracle Cloud Infrastructure Documentation.

- Click **Groups**.

- Click **Add User to Group**.
- Select the group from the drop-down list, and then click **Add**.

## Create an Oracle Cloud Infrastructure Policy

Create a policy to grant permission to the users in a group to work with Oracle Integration instances within a specified tenancy or compartment.

To create and assign a policy to the Oracle Cloud Infrastructure group:

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, `IntegrationGroupPolicy`) 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-integration-admins to manage integration-instance in compartment OICCompartment`

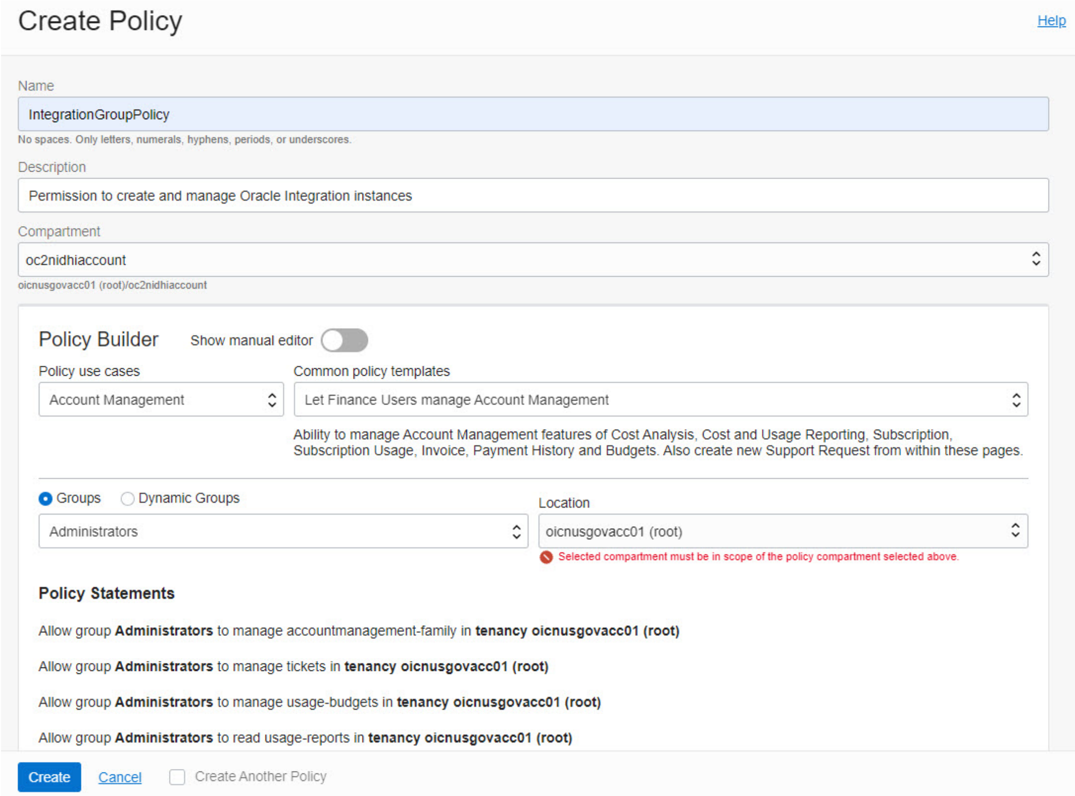
   This policy statement allows the `oci-integration-admins` group in the `admin` domain to `manage` instance `integration-instance` in compartment `OICCompartment`.

   You can create separate groups for different permissions, such as a group with `read` permission only.

   Want to learn more about policies? See How Policies Work and Policy Reference, or click **Help** in the window.

   - When defining policy statements, you can specify either verbs (as used in these steps) or permissions (typically used by power users).
   - The `read` and `manage` verbs are most applicable to Oracle Integration. The `manage` verb has the most permissions (`create`, `delete`, `edit`, `move`, and `view`).

| Verb | Access |
|---|---|
| `read` | Includes permission to view Oracle Integration instances and their details. |
| `manage` | Includes all permissions for Oracle Integration instances. |



Create Policy

Name

IntegrationGroupPolicy

No spaces. Only letters, numerals, hyphens, periods, or underscores.

Description

Permission to create and manage Oracle Integration instances

Compartment

oc2nidhiaccount

oicnusgovacc01 (root)/oc2nidhiaccount

Policy Builder

Show manual editor

Policy use cases: Account Management

Common policy templates: Let Finance Users manage Account Management

Ability to manage Account Management features of Cost Analysis, Cost and Usage Reporting, Subscription, Subscription Usage, Invoice, Payment History and Budgets. Also create new Support Request from within these pages.

● Groups ○ Dynamic Groups

Administrators

Location: oicnusgovacc01 (root)

Selected compartment must be in scope of the policy compartment selected above.

Policy Statements

Allow group **Administrators** to manage accountmanagement-family in **tenancy oicnusgovacc01 (root)**

Allow group **Administrators** to manage tickets in **tenancy oicnusgovacc01 (root)**

Allow group **Administrators** to manage usage-budgets in **tenancy oicnusgovacc01 (root)**

Allow group **Administrators** to read usage-reports in **tenancy oicnusgovacc01 (root)**

5. Click **Create**.

   The policy statements are validated and syntax errors are displayed.

# Assign Policies to Oracle Integration Service Role Groups

After an Oracle Integration instance has been created, create and assign a policy for each Oracle Integration service role and scope needed.

Extend Oracle Integration permissions to Oracle Cloud Infrastructure users by creating groups for key Oracle Integration roles, adding users to the groups, then creating policies that grant access to specified resources and permissions to users in those groups.

Oracle Integration provides a standard set of service roles, which govern access to features. See Oracle Integration Service Roles.

To assign policies to Oracle Integration service role groups:

1. Create the appropriate groups and users. See Create an Oracle Cloud Infrastructure Group and Users.

   Depending on the Oracle Integration features your organization uses, you may need to create groups for some or all of the roles. For example, you might create and name groups as follows:

   - `OICServiceAdministrators` to grant admin permissions in service instances
   - `OICServiceDevelopers` to grant developer permissions in service instances
   - `OICServiceInvokers` to grant service invoke only permission to one instance
   - `OICServiceMonitors` to grant monitor only permission to one or more instances

2. Create the appropriate policies. See Create an Oracle Cloud Infrastructure Policy.

**Syntax:** `allow group` *`group_name`* `to be` *`service_role`* `for` *`resource-type`* `in compartment` *`compartment-name`*

> **Note:**
>
> You can also restrict access to a specified instance by including an optional `where` clause.

| Description | Example Policy |
|---|---|
| Grant the `ServiceAdministrator` role for a compartment | `allow group OICAdminGroup to be ServiceAdministrator for integration-instances in compartment OICCompartment` |
| Grant the `ServiceDeveloper` role for a compartment | `allow group OICDeveloperGroup to be ServiceDeveloper for integration-instances in compartment OICCompartment` |
| Grant the `ServiceInvoker` role for an Oracle Integration instance | `allow group OICInvokerGroup to be ServiceInvoker for integration-instances in compartment OICCompartment`<br>`where all {target.app.name='test-instance1', target.app.type='integration-instances'}`<br>Here the `where` clause grants users assigned to group `OICInvokerGroup` the `ServiceInvoker` role to one Oracle Integration instance identified by its instance name and created in `OICCompartment`. |
| Grant the `ServiceMonitor` role for two Oracle Integration instances | `allow group OICMonitorGroup to be ServiceMonitor for integration-instances in compartment OICCompartment`<br>`where any {target.app.name='test-instance1', target.app.name='instance-prod-1'}`<br>This policy grants the `ServiceMonitor` Role to the `OICMonitorGroup` group over two instances identified by their respective names in `OICCompartment`. |

## Oracle Integration Service Roles

Oracle Integration predefined roles govern access to various Oracle Integration features.

The following table lists the predefined roles available in Oracle Integration, and the general tasks that users assigned the roles can perform. You can assign one or more of the predefined roles to Oracle Integration users and groups.

| Oracle Integration | Description |
|---|---|
| `ServiceAdministrator` | A super user who can manage and administer the features provisioned in an Oracle Integration instance. |
| `ServiceDeveloper` | Develops the artifacts specific to the features provisioned in an Oracle Integration instance. A developer can create integrations. |
| `ServiceMonitor` | Monitors the features provisioned in an Oracle Integration instance. For example, a user assigned this roled can view instances and metrics, find out response times, and track whether instance creation completed successfully or failed.<br>This role provides privileges for users with limited knowledge of Oracle Integration, but with high-level knowledge of monitoring it. This user role does not grant permissions to change anything. |
| `ServiceDeployer` | Publishes the artifacts developed in a feature.<br>This role is not applicable for the Integrations feature. |

| Oracle Integration | Description |
|---|---|
| `ServiceUser` | Privileges to utilize only the basic functionality of a feature such as access to the staged and published applications.<br>For example, in Integrations the user can navigate to resource pages (such as integrations and connections) and view details, but can't edit or modify anything. The user can also run integrations. |
| `ServiceInvoker` | Invokes any integration flow in an Oracle Integration instance that is exposed through SOAP/REST APIs or a scheduled integration. A user with `ServiceInvoker` role cannot:<br>• Navigate to the Oracle Integration user interface or perform any administrative actions in the user interface.<br>• Invoke any of the documented Oracle Integration REST APIs. |
| `ServiceViewer` | Navigates to all Oracle Integration resource pages (for example, integrations, connections, lookups, libraries, and so on) and view details. The user cannot edit any resources or navigate to the administrative setting pages. |

In Oracle Integration, when you assign a role to a user, the user is granted that role for all Oracle Integration features provisioned on an instance. Further, each role grants different privileges for different features to the same user. Note that not all Oracle Integration predefined roles are available in all features.

# Configure OAuth Authentication in Oracle Cloud Infrastructure US Government Cloud Environments

Configure OAuth 2.0 or Basic Authentication using client credentials, and configure a connectivity agent.

**Topics:**

- Configure OAuth 2.0 Authentication Using Client Credentials
- Configure Basic Authentication Using Client Credentials
- Configure the Connectivity Agent

## Configure OAuth 2.0 Authentication Using Client Credentials

To configure OAuth 2.0 authentication for invoking Oracle Integration APIs, configure and use client credentials.

For OAuth authentication in Oracle Cloud Infrastructure in government environments, client credentials is the only authorization grant flow supported. OAuth client credentials grant flow semantics are built into Oracle Cloud Infrastructure's IAM and scoped to an IAM user profile. Any user can create an OAuth 2.0 client credentials user for their user account using the Oracle Cloud Infrastructure Console.

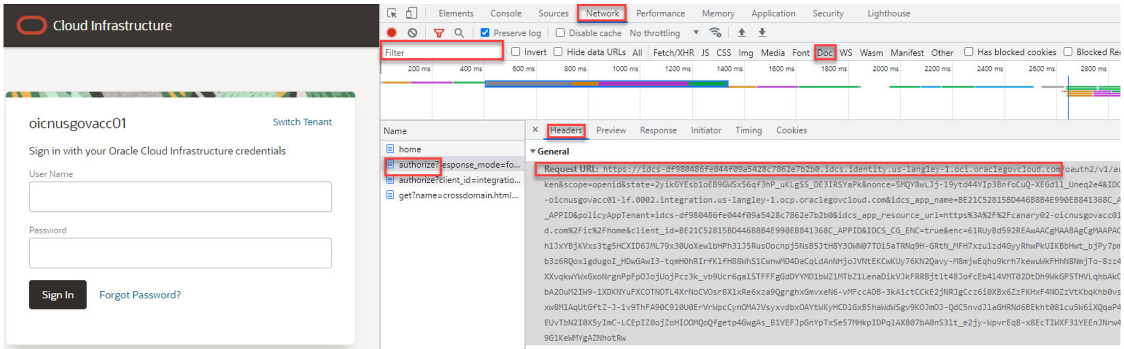
To configure OAuth client credentials, follow these main steps:

- Gather Needed Information
- Generate the Client Credentials
- Obtain an OAuth Bearer Token
- Use the Bearer Token to Invoke Oracle Integration APIs

## Gather Needed Information

Ensure you have the information described in the following table available.

| Field | Description | Example Value |
|---|---|---|
| Instance (friendly URL) | The friendly URL of your Oracle Integration instance.<br>On the Integration Instance Details page, this is the value of the **Service Console URL**. | `https://canary02-oicnusgovacc01-lf.0002.integration.us-langley-1.ocp.oraclegovcloud.com/ic/home` |
| Audience (permanent URL) | The unique URL of the Oracle Integration resource this client is allowed to access.<br>This value is automatically populated by the OAuth resource selector. | `https://1403FE2A654445B7AAC83480F67E8C48.0001.integration.dev.ocp.oc-test.com:443` |
| Scope | The applications you want this client to invoke or the APIs of the service instances you want to invoke. Scopes relevant for Oracle Integration are listed. You can use either one.<br>This value is automatically populated by the OAuth resource selector. | • `urn:opc:resource:consumer::all`<br>• `/ic/api/` |
| Associated UPI stripe | The associated UPI stripe for the Oracle Integration instance, along with its admin user and admin password. This is used to obtain an OAuth 2.0 token.<br>To find the UPI stripe:<br>1. On the Integration Instance Details page, copy the **Service Console URL**.<br>For example: `https://canary02-oicnusgovacc01-lf.0002.integration.us-langley-1.ocp.oraclegovcloud.com/ic/home`<br>2. Open a browser window, then right-click on the browser and select **Inspect** to open the developer tools pane.<br>3. In the developer tools pane, click the **Network** tab, then click **Doc**. Make sure that the **Filter** field is empty.<br>4. Paste the service console URL from step 1 into your browser address bar.<br>5. In the developer tools pane, in the **Name** column, click the `authorize?` call, then click **Headers**.<br>The first part of the **Request URL** specifies the UPI stripe. For example:<br>`https://idcs-df980486fe044f09a5428c7862e7b2b0.idcs.identity.us-langley-1.oci.oraclegovcloud.com` | • UPI stripe: `https://idcs-df980486fe044f09a5428c7862e7b2b0.idcs.identity.us-langley-1.oci.oraclegovcloud.com`<br>• Admin user: `upi-test-admin-user`<br>• Admin password: `Welcome@123456` |

| Field | Description | Example Value |
|---|---|---|
| | <br>Cloud Infrastructure<br>oicnusgovacc01 Switch Tenant<br>Sign in with your Oracle Cloud Infrastructure credentials<br>User Name<br>Password<br>Sign In Forgot Password?<br>Request URL: https://idcs-df980486fe044f09a5428c7862e7b2b0.idcs.identity.us-langley-1.oci.oraclegovcloud.com/oauth2/v1/au<br>ken&scope=openid&state=2yikGYEsb1oEB9GWSx56qf3hP_uKLgSS_DE3IRSYaPk&nonce=5MQY8wLJj-19ytd44YIp3BnfoCuQ-XEGd1l_Uneq2e4&IDC<br>-oicnusgovacc01-1f.0002.integration.us-langley-1.ocp.oraclegovcloud.com&idcs_app_name=BE21C52815BD446B8B4E990EB841368C_A<br>_APPID&policyAppTenant=idcs-df980486fe044f09a5428c7862e7b2b0&idcs_app_resource_url=https%3A%2F%2Fcanary02-oicnusgovacc01<br>d.com%2Fic%2Fhome&client_id=BE21C52815BD446B8B4E990EB841368C_APPID&IDCS_CG_ENC=true&enc=61RUyBd592REAwAACgMAABAgCgMAAPAC<br>h1JxYBjKVxs3tg5HCXID6JML79x30UoXew1bHPh31J5RusOocnpj5NsB5JtH8Y3OWN07TOi5aTRNq9H-GRtN_MFH7xzu1zd4GyyRhwPkUIKBbHwt_bjPy7pm<br>b3z6RQox1gdugoI_HDwGAwI3-tqmH0hRIrfK1fH88WhS1CwnwMD4DaCqLdAnNHjoJVNtEKCwKUy76KN2Qavy-M8mjwEqhu9krh7kewuWkFHhN8NmjTo-8zz4<br>XXvqkwYWxGxoNrgnPpFpOJojUojPcz3k_vb9Ucr6qa1STFFFgGdDYYMD1bWZ1MTbZ1LenaDikVJkFRRBjt1t48JofcEb414VMT02DtDh9WkGP5THVLqhbAkC<br>bA2OuM2IW9-1XDKNYuFXCOTNOTL4XrNoCVOsr8X1xRe6xza9QgrghxGmvxeN6-vMFccADB-3kA1ctCCkE2jNRJgCcz6i0XBx6ZzFKHxF4NOZzVtKbqKhb0vs<br>xw8M1AqUtGftZ-J-1v9ThFA90C910U0ErVrWpcCynOMAJVsyxvdbxOAYtWKyHCD1GxB5haWdWSgv9KOJmOJ-QdC5nvdJ1aGHRNd6BEkht081cu5W6iXQqaP4<br>EUvTbN2I0X5yImC-LCEpIZ0ojZoHIOOMQoQfgetp4GwgAs_B1VEFJpGnYpTxSe57MHkpIDPq1AX807bA0nS31t_e2jy-WpvrEq8-x8EcTIWXF31YEEnJNrw4<br>9G1KeWMYgAZNhotRw | |
| Client ID | The OCID of the generated OAuth 2.0 client credentials and can be retrieved from the UI next to the client credentials on the client credentials page. | `ocid1.credential.oc1..aaaaaaaaulplph33maqltcttppjoyb56jlm5asx5ikcojntvzj5mnvp25qnq` |
| Client Secret | The secret generated when you generate the OAuth 2.0 client credential. Copy it when it appears once. It isn't shown again; the only option is to regenerate another secret. | `i7BKNOG:1z1A)bqaY(]F` |

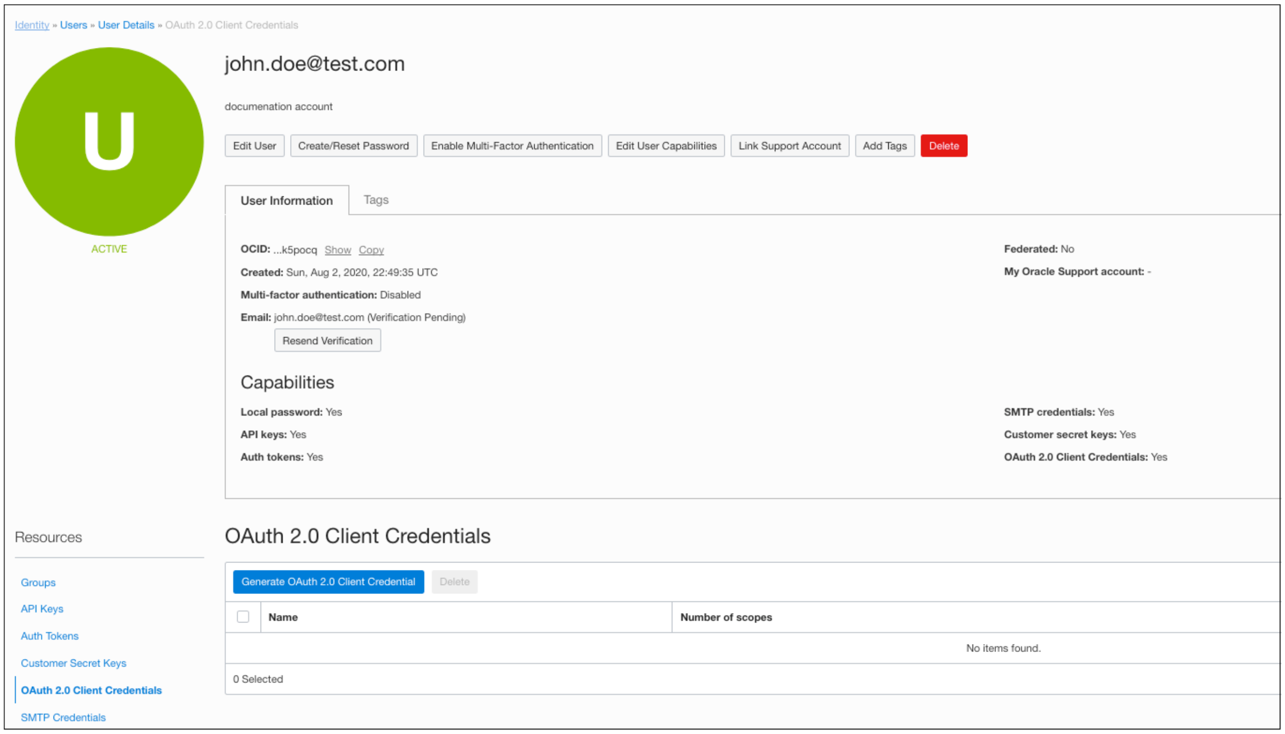
## Generate the Client Credentials

To generate the client credentials:

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Users**. In the **Name** column, click the user name that you want to update. The User Details screen is displayed.

   To programmatically invoke an API, you typically create a client credential under a service account user. The credential must be created at the user level, not a group level.

2. Under **Resources**, select **OAuth 2.0 Client Credentials**.



john.doe@test.com

documenation account

**OCID:** ...k5pocq Show Copy

**Created:** Sun, Aug 2, 2020, 22:49:35 UTC

**Multi-factor authentication:** Disabled

**Email:** john.doe@test.com (Verification Pending)

**Federated:** No

**My Oracle Support account:** -

Capabilities

**Local password:** Yes

**API keys:** Yes

**Auth tokens:** Yes

**SMTP credentials:** Yes

**Customer secret keys:** Yes

**OAuth 2.0 Client Credentials:** Yes

OAuth 2.0 Client Credentials

| ☐ | Name | Number of scopes |
|---|---|---|
| | | No items found. |

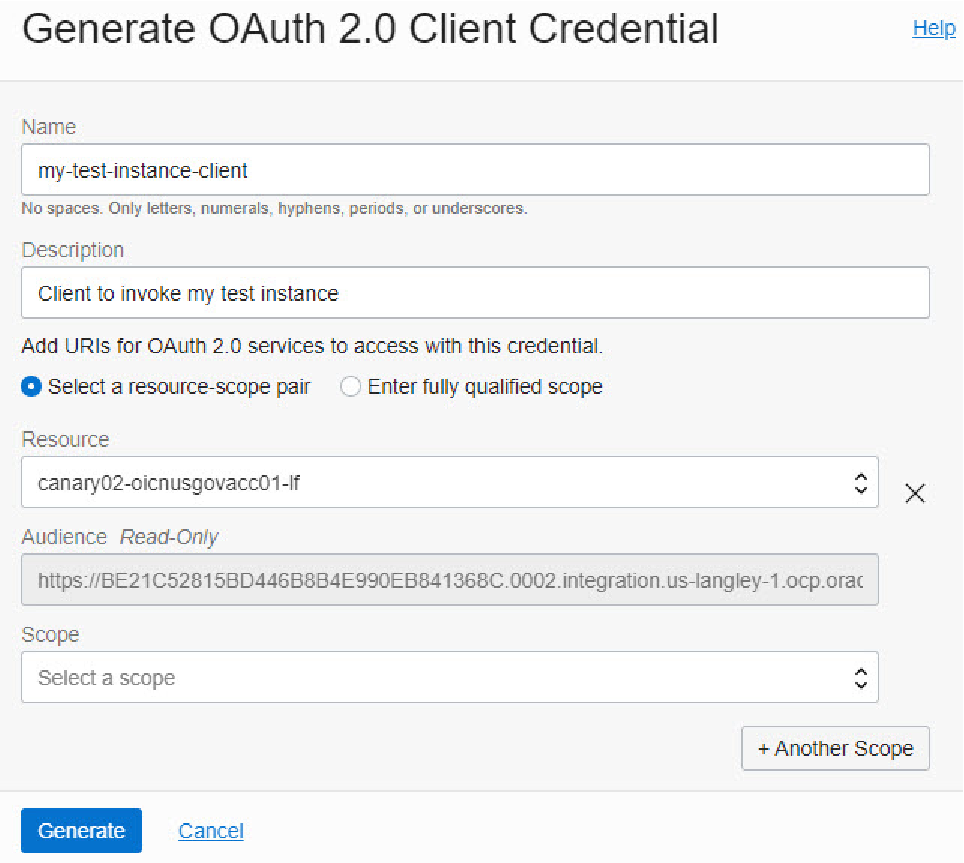
0 Selected

3. Click **Generate OAuth 2.0 Client Credential**.

   The Generate OAuth 2.0 Client Credential dialog is displayed.

4. Use the resource selector to select an Oracle Integration instance and populate audience and scope fields.

   The resource selector dropdown lists all Oracle Integration instances across all subscribed regions in your Oracle Cloud Infrastructure tenancy. The list is further filtered by the compartments to which you have access. This view enables you to select the Oracle Integration instance that the client needs to invoke, and doing so automatically populates the audience and scope values, as shown below. Note that IAM users and by extension OAuth 2.0 client credentials are global, whereas Oracle Integration instances are created in a region and so are regional.



Generate OAuth 2.0 Client Credential

Name: my-test-instance-client

No spaces. Only letters, numerals, hyphens, periods, or underscores.

Description: Client to invoke my test instance

Add URIs for OAuth 2.0 services to access with this credential.

● Select a resource-scope pair ○ Enter fully qualified scope

Resource: canary02-oicnusgovacc01-lf

Audience *Read-Only*: https://BE21C52815BD446B8B4E990EB841368C.0002.integration.us-langley-1.ocp.orac

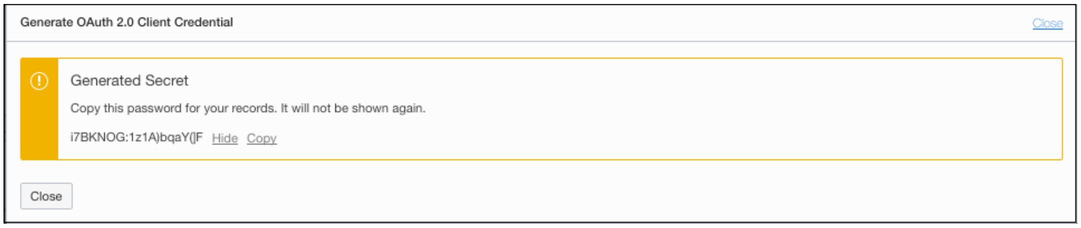
Scope: Select a scope

5. Complete additional entries in the Generate OAuth 2.0 Client Credential dialog.

   For more information, refer to the table in Gather Needed Information .

6. Click **Generate**.

   The generated credential is displayed. The client credential includes the client credential's OCID and a one-time password.



Generate OAuth 2.0 Client Credential

Generated Secret

Copy this password for your records. It will not be shown again.

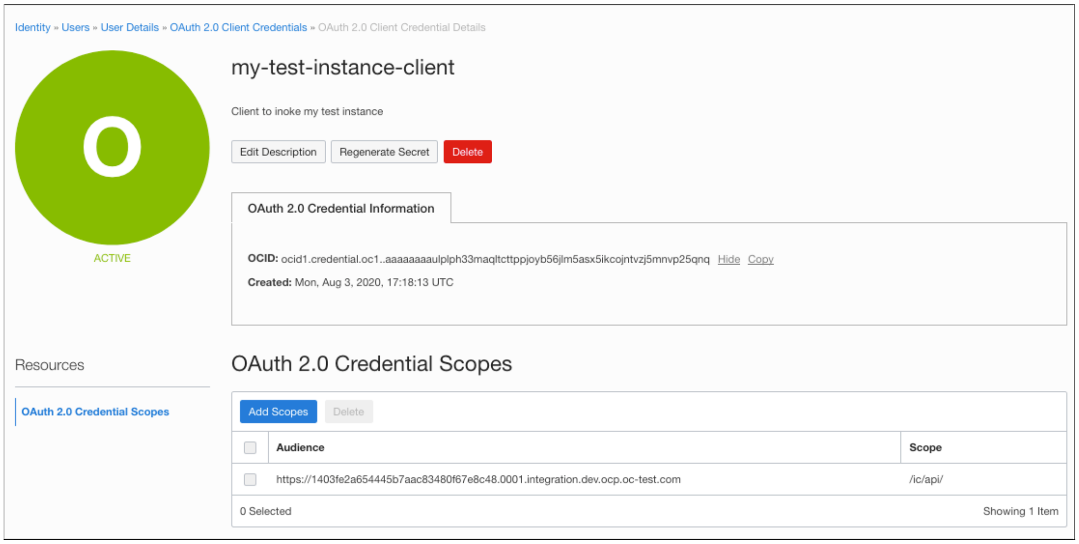
i7BKNOG:1z1A)bqaY(]F

7. Note the password, then click **Close**.

   The credential password appears here just once. There is no way to retrieve a password; if you lose it, you must regenerate the credential.

8. If needed, edit the client credential.

   The generated client credential is listed under **OAuth 2.0 Client Credentials**. You can view or change its attributes and regenerate the client secret if needed on the credential details screen.



Identity » Users » User Details » OAuth 2.0 Client Credentials » OAuth 2.0 Client Credential Details

my-test-instance-client

Client to inoke my test instance

OAuth 2.0 Credential Information

**OCID:** ocid1.credential.oc1..aaaaaaaaulplph33maqltcttppjoyb56jlm5asx5ikcojntvzj5mnvp25qnq Hide Copy

**Created:** Mon, Aug 3, 2020, 17:18:13 UTC

OAuth 2.0 Credential Scopes

| □ | Audience | Scope |
|---|---|---|
| □ | https://1403fe2a654445b7aac83480f67e8c48.0001.integration.dev.ocp.oc-test.com | /ic/api/ |

0 Selected    Showing 1 Item

## Obtain an OAuth Bearer Token

Once you have the OAuth client credential configured, you can get an OAuth bearer token based on the generated values.

To obtain an OAuth bearer token, enter the following values in your API request, using either POSTMAN or curl:

1. Client ID and secret:
   - **Client ID:** `ocid1.credential.oc1..aaaaaaaaulplph33maqltcttppjoyb56jlm5asx5ikcojntvzj5mnvp25qnq`
   - **Client Secret:** `i7BKNOG:1z1A)bqaY(]F`
2. UPI stripe token request endpoint (POST):

   ```
   https://idcs-364c06d3202948828edee2b8ba4dbc16.idcs.identity.us-phoenix-1.oci.oraclecloud.com/oauth2/v1/token
   ```
3. Scope definition in the POST request payload:

   For this instance the scope definition is a concatenation of the audience and scope (exactly) as defined in the client credentials creation step above.

   ```
   'grant_type=client_credentials'
   'scope=https://
   1403FE2A654445B7AAC83480F67E8C48.0001.integration.dev.ocp.oc-
   test.com:443urn:opc:resource:consumer::all https://
   1403FE2A654445B7AAC83480F67E8C48.0001.integration.dev.ocp.oc-
   test.com:443/ic/api'
   ```
4. Request:

   ```
   curl -X POST \
     https://idcs-364c06d3202948828edee2b8ba4dbc16.idcs.identity.us-
   phoenix-1.oci.oraclecloud.com/oauth2/v1/token \
     -H 'Accept: application/json'\
     -H 'Authorization:  Basic
   ```

```
b2NpZDEuY3JlZGVudGlhbC5vYzEuLmFhYWFhYWFhdWxwbHBoMzNtYXFsdGN0dHBwam95YjU2amx
tNWFzeDVpa2Nvam50dnpqNW1udnAyNXFucTppN0JLTk9HOjF6MUEpYnFhWShdRg=='\
  -H 'Cache-Control: no-cache' \
  -H 'Content-Type: application/x-www-form-urlencoded' \
  -H 'cache-control: no-cache' \
  -d 'grant_type=client_credentials&scope=https://
1403FE2A654445B7AAC83480F67E8C48.0001.integration.dev.ocp.oc-
test.com:443urn:opc:resource:consumer::all https://
1403FE2A654445B7AAC83480F67E8C48.0001.integration.dev.ocp.oc-
test.com:443/ic/api'
```

5. Response:

```
{
 "access_token":
"eyJ4NXQjUzI1NiI6Ijc3NmdPRkNZZUxSZ0J2Q2JFcHE4dkg3OVc1UUxhWG91Q1c1QkN0U0xEek
EiLCJ4NXQiOiJtejFrdVE4TEJudUF1VEs3S3EwQ3lRUlpCMmsiLCJraWQiOiJhc3ctb2F1dGhfb
2MxXzY1MmI4YjI5IiwiYWxnIjoiUlMyNTYifQ.eyJ1c2VyX3R6IjoiTVNUIiwic3ViIjoiam9ob
i5kb2VAdGVzdC5jb20iLCJ1c2VyX2xvY2FsZSI6IkVOIiwidXNlcl9kaXNwbGF5bmFtZSI6Impv
aG4uZG9lQHRlc3QuY29tIiwic3ViX21hcHBpbmdhdHRyIjoidXNlck5hbWUiLCJpc3MiOiJhdXR
oU2VydmljZS5vcmFjbGUuY29tIiwidG9rX3R5cGUiOiJBVCIsInB0eXBlIjoidXNlciIsInVzZX
JfdGVuYW50bmFtZSI6ImlkY3MtMzY0YzA2ZDMyMDI5NDg4MjhlZGVlMmI4YmE0ZGJjMTYiLCJjb
GllbnRfaWQiOiJvY2lkMS5jcmVkZW50aWFsLm9jMS4uYWFhYWFhYWF1bHBscGgzM21hcWx0Y3R0
cHBqb3liNTZqbG01YXN4NWlrY29qbnR2emo1bW52cDI1cW5xIiwiYXVkIjpbImh0dHBzOlwvXC9
0ZXN0ZG5zdXBpNnVzaW5nbWlnbGFiLWlkYWF0MzFkanZpcy1jcGkuMDAwMS5pbnRlZ3JhdGlvbi
5kZXYub2NwLm9jLXRlc3QuY29tOjQ0MyIsImh0dHBzOlwvXC8xNDAzRkUyQTY1NDQ0NUI3QUFDO
DM0ODBGNjdFOEM0OC4wMDAxLmludGVncmF0aW9uLmRldi5vY3Aub2MtdGVzdC5jb206NDQzIiwi
dXJuOm9wYzpsYmFhczpsb2dpY2FsZ3VpZD0xNDAzRkUyQTY1NDQ0NUI3QUFDODM0ODBGNjdFOEM
0OCJdLCJ1c2VyX2lkIjoib2NpZDEudXNlci5vYzEuLmFhYWFhYWFhMjdqZW1vcmZ3YXp2ZDVtc2
JiNzJxM2hlN3Frd2JzeXlkNzd0bWxvbmVoYzU0aGs1cG9jcSIsInN1Yl90eXBlIjoidXNlciIsI
nNjb3BlIjoidXJuOm9wYzpyZXNvdXJjZTpjb25zdW1lcjo6YWxsIFwvaWNcL2FwaSIsImNsaWVu
dF90ZW5hbnRuYW1lIjoiaWRjcy0zNjRjMDZkMzIwMjk0ODgyOGVkZWUyYjhiYTRkYmMxNiIsInV
zZXJfbGFuZyI6IkVOIiwiZXhwIjoxNTk2NTYzNzcwLCJpYXQiOjE1OTY1NjAxNzAsImNsaWVudF
9ndWlkIjoib2NpZDEuY3JlZGVudGlhbC5vYzEuLmFhYWFhYWFhdWxwbHBoMzNtYXFsdGN0dHBwa
m95YjU2amxtNWFzeDVpa2Nvam50dnpqNW1udnAyNXFucSIsImNsaWVudF9uYW1lIjoibXktdGVz
dC1pbnN0YW5jZS1jbGllbnQiLCJ0ZW5hbnRfaXNzIjoiaHR0cHM6XC9cL2lkY3MtYmEyZDI0NDg
0MmJhNGZiYWJlNmIzM2VlMGIxM2MwYzEuaWRjcy5pZGVudGl0eS51cy1hc2hidXJuLTEub2NpLm
9yYWNsZWNsb3VkLmNvbSIsImp0aSI6IjkyZGNkMDQzLTc0MDYtNGJhZi1hZTMxLTVmY2JmZTk4Y
zRiNSIsInRlbmFudCI6ImlkY3MtMzY0YzA2ZDMyMDI5NDg4MjhlZGVlMmI4YmE0ZGJjMTYifQ.J
8atPO-RjSsplzzzTYkT5_NCYo33gfHQJgZomJ3dZvrSpGdPDJ6Xxtb-UrLMLFGOZEaw-b4-
JaY_z4KWETjlicseeMTBIgnpeiqf0QppqS0vJeMzy3kA_EIJrtcX_NQglOUYpGtyNq5-
HTix6fPULYMf_ZMhLm7XAh551QAwL_TP_gz1QAXRsbYkzN_19Hs_kgJZ-
KlZ2cwYLl2H3o36x2d2V3ESZNejPwSwutky8nT0bLBT78kwfc3YRzkhThb613XD3r4oLyYLGbTi
e9wHbufHjkAbcZRX7JR_hPjSxhm_ijVlOlEvFCy5Smn5-vss3dDBKJocGIIpbSfFyffxHQ",
 "token_type": "Bearer",
 "expires_in": "3600"
}
```

## Use the Bearer Token to Invoke Oracle Integration APIs

Using the bearer token obtained in Obtain an OAuth Bearer Token, you can now invoke Oracle Integration APIs. See REST API for Oracle Integration.

For example:

```
curl -X GET \
  https://testdnsupi6usingmiglab-idaat31djvis-cpi.0001.integration.dev.ocp.oc-
test.com:443/ic/api/integration/v1/integrations
      \
  -H 'Authorization: Bearer eyJ4NXQjUz........'\
  -H 'cache-control:
    no-cache'
```

## Configure Basic Authentication Using Client Credentials

To configure Basic Authentication for invoking Oracle Integration APIs in an Oracle Cloud Infrastructure US Government Cloud environment, use the client ID and secret from an OAuth 2.0 client credential as the Basic Authentication credentials.

As a general Oracle Cloud Infrastructure security rule, Basic Authentication is not recommended as an authentication method, due to its inherent flaws.

Oracle Cloud Infrastructure's IAM model doesn't allow user login credentials to be used as Basic Authentication credentials. This means that login credentials (to log into the Oracle Cloud Infrastructure Console or to the Oracle Integration functional console) can't be used when invoking Oracle Integration APIs as a Basic Authentication credential. Instead, use the ID and secret from OAuth 2.0 client credentials as the Basic Authentication credentials (user name and password).

To configure OAuth client credentials as Basic Authentication credentials:

1. Create OAuth client credentials.

   Follow the steps in Configure OAuth 2.0 Authentication Using Client Credentials on generating the client credential. Note the client ID and client secret that are generated.

   Example values:

   - Client ID: `ocid1.credential.oc1..aaaaaaaaulplph33maqltcttppjoyb56jlm5asx5ikcojntvzj5mnvp25qnq`
   - Client Secret: `i7BKNOG:1z1A)bqaY(]F`

2. Use the OAuth credentials as the Basic Auth credentials directly in a command.

   See these examples that use values from above.

   - Using base64 encoding:

     ```
     # echo
     'ocid1.credential.oc1..aaaaaaaaulplph33maqltcttppjoyb56jlm5asx5ikcojntvz
     j5mnvp25qnq:i7BKNOG:1z1A)bqaY(]F' | base64
     b2NpZDEuY3JlZGVudGlhbC5vYzEuLmFhYWFhYWFhdWxwbHBoMzNtYXFsdGN0dHBwam95YjU2
     amxtNWFzeDVpa2Nvam50dnpqNW1udnAyNXFucTppN0JLTk9HOjF6MUEpYnFhWShdRgo=
     ```

   - Returned base64 string in the Authorization header:

     ```
     curl -X GET \
       testdnsupi6usingmiglab-idaat31djvis-cpi.0001.integration.dev.ocp.oc-
     test.com:443/ic/api/integration/v1/connections \
       -H 'Authorization: Basic
     ```

```
b2NpZDEuY3JlZGVudGlhbC5vYzEuLmFhYWFhYWFhdWxwbHBoMzNtYXFsdGN0dHBwam95YjU2
amxtNWFzeDVpa2Nvam50dnpqNW1udnAyNXFucTppN0JLTk9HOjF6MUEpYnFhWShdRgo=' \
  -H 'cache-control: no-cache'
```

## Configure the Connectivity Agent

The Connectivity Agent is required to connect Oracle Integration with an on-premises database. To use the Connectivity Agent in an Oracle Cloud Infrastructure US Government Cloud environment, it needs a non-federated account with the `ServiceAdministrator` role.

If you try to run the Connectivity Agent installation as a federated user, it fails. To prevent this issue, follow the steps below to configure a nonfederated (IAM) user to install the agent. This user enables the agent to communicate with Oracle Integration.

1. Configure a user with permissions to install the agent, by adding an IAM policy that assigns the `ServiceAdministrator` role for the compartment.

   **Syntax:** `allow group OICAdminGroup to be ServiceAdministrator for integration-instances in compartment OICCompartment`

   **Example:** `allow group OICServiceDevelopers to be ServiceAdministrator for integration-instances in compartment OrganizationCompartment`

2. In the Connectivity Agent, configure Basic Authentication using client credentials.

   Use the client ID and secret instead of a username and password for the authentication.

   a. Generate the OAuth client credentials. See Generate the Client Credentials.

   b. Use the client credentials in Basic Authentication in the Connectivity Agent configuration. See Configure Basic Authentication Using Client Credentials.

3. If you need to restart the Connectivity Agent at some point, ensure that the username and password credentials for the user you configured above are still valid.

# 3 Work with Oracle Integration Generation 2 Instances on Oracle Cloud Infrastructure US Government Cloud

Create and edit Oracle Integration Generation 2 instances in the Oracle Cloud Infrastructure Console.

**Topics:**

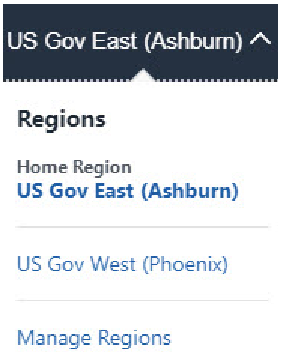
## Create an Oracle Integration Instance

> **Note:**
>
> You cannot provision a new Oracle Integration Generation 2 instance in the Oracle US Defense Cloud (realm key: OC3). Additionally, most organizations cannot provision a new Oracle Integration Generation 2 instance in the Oracle US Government Cloud (realm key: OC2). The only organization that can provision a new Oracle Integration Generation 2 instance in the Oracle US Government Cloud are tenancies that do not use identity domains. To create an Oracle Integration 3 instance, see Create an Oracle Integration Instance in *Using Oracle Integration 3 on Oracle Cloud Infrastructure US Government Cloud*.

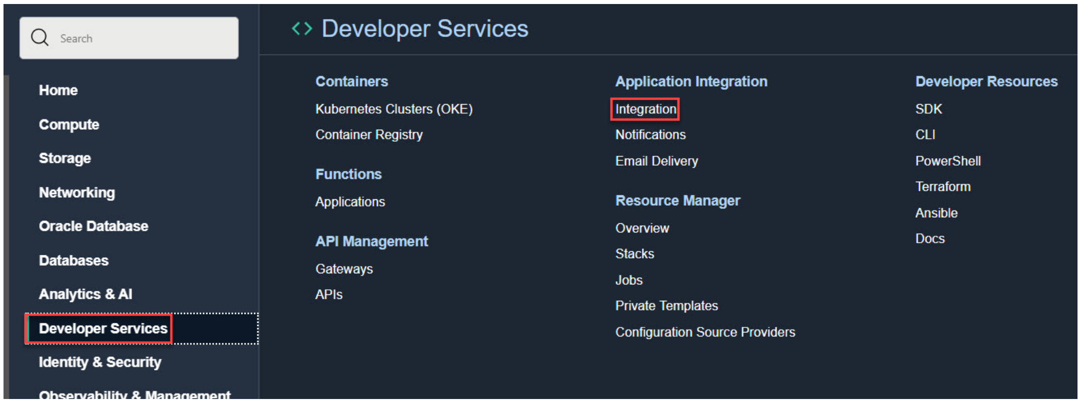
To create an Oracle Integration instance in a selected compartment:

1. In the upper corner, note your selected region.

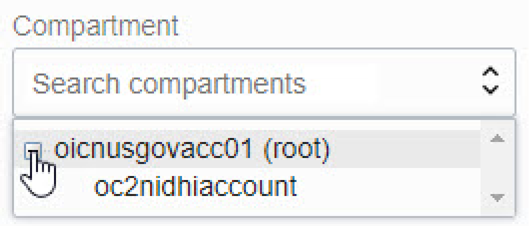
   Once created, instances are visible only in the region in which they were created.



2. Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Integration**.

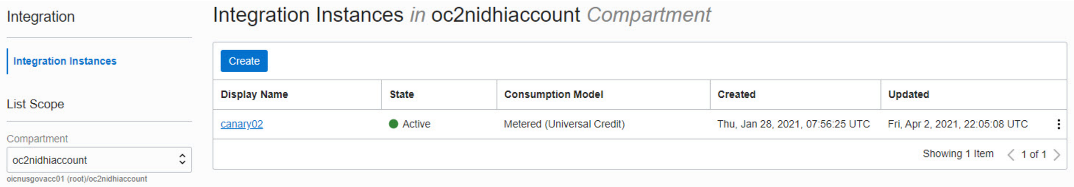


3. From the **Compartment** list, click through the hierarchy of compartments and select the one in which to create the instance. You may need to expand the **+** icon to find the compartment to use. Compartments can contain other compartments. It may take several minutes for the new compartment to appear after the policy has been created.



> **Note:**
>
> Do NOT select the `root` or `ManagedCompartmentForPaaS` compartment in which to create your instance.

The page is refreshed to show any existing instances in that compartment.



Integration Instances *in* oc2nidhiaccount *Compartment*

| Display Name | State | Consumption Model | Created | Updated |
|---|---|---|---|---|
| canary02 | ● Active | Metered (Universal Credit) | Thu, Jan 28, 2021, 07:56:25 UTC | Fri, Apr 2, 2021, 22:05:08 UTC |

Showing 1 Item 1 of 1

4. Click **Create**.

5. Enter the following details and click **Create**:

| Field | Description |
|---|---|
| **Display Name** | Enter the display name for the instance. Note that the display name becomes part of the URL for accessing the instance. |

| Field | Description |
|---|---|
| **Consumption Model** | Lists consumption models available in this tenancy. Typically, one model is displayed, but multiple consumption models are listed if your tenancy is enabled for more than one. Available models include:<br>• Metered (Universal Credit)<br>• Oracle Integration Government<br>**Note:**<br>*Oracle Integration Government* is a license and doesn't specify the realm. |
| **License Type** | • Select to create a new Oracle Integration license in the cloud. This provides you with packages of 5K messages per hour.<br>• Select to bring an existing Oracle Fusion Middleware license to the cloud for use with Oracle Integration. This provides you with packages of 20K messages per hour. This option is also known as bring your own license (BYOL). |
| **Message Packs** | The message pack options available for selection are based on the version of Oracle Integration instance you are creating. Select the number of message packs. The total number of messages available per pack is based on the **License Type** option you selected. You can select up to 3 message packs if you bring an existing Oracle Fusion Middleware license to the cloud. You can select up to 12 message packs if you create a new Oracle Integration license in the cloud. |

Typically, the selected model is displayed after **Consumption Model**. If multiple consumption models are listed, choose the model you'd like used for this instance.

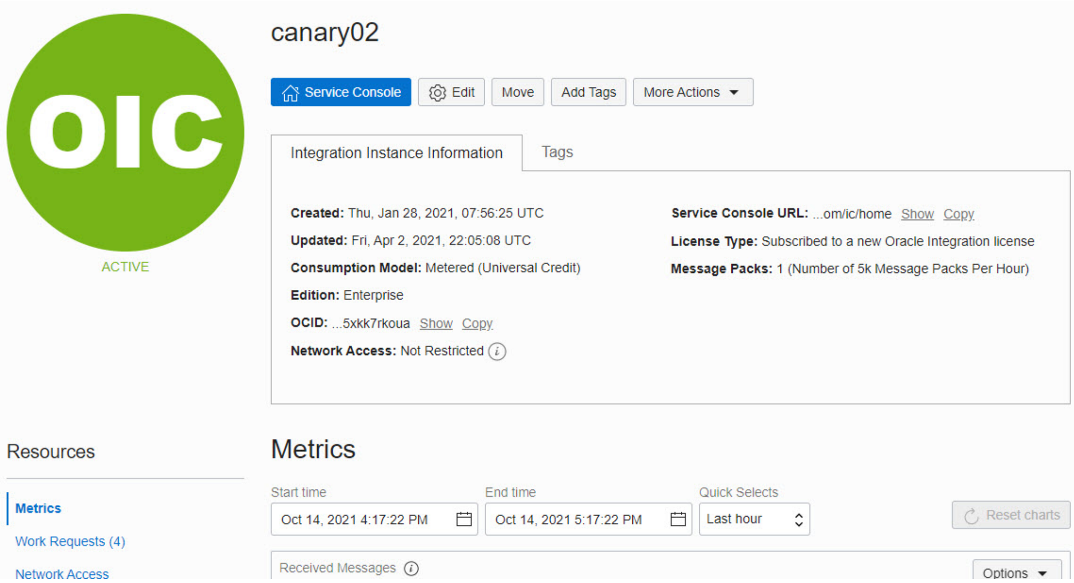
Instance creation takes some time. If you attempt to click the instance name and receive a `401: Authorization failed` or a `404: Not Found` error, but followed all the correct steps, instance creation has not completed. Wait a few more minutes.

6. When instance creation completes successfully, the instance shows as **Active** in the **State** column.

## View Instance Details

You can view details about a provisioned instance and perform tasks such as accessing the instance login page to design integrations, viewing custom endpoint details, editing an instance, adding tags, and deleting instances.

1. Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Integration**.
2. In the **Display Name** column, click a specific instance name. The Details page is displayed. The word **Active** is displayed beneath the green circle to indicate that this instance is running.



**Created:** Thu, Jan 28, 2021, 07:56:25 UTC
**Updated:** Fri, Apr 2, 2021, 22:05:08 UTC
**Consumption Model:** Metered (Universal Credit)
**Edition:** Enterprise
**OCID:** ...5xkk7rkoua Show Copy
**Network Access:** Not Restricted

**Service Console URL:** ...om/ic/home Show Copy
**License Type:** Subscribed to a new Oracle Integration license
**Message Packs:** 1 (Number of 5k Message Packs Per Hour)

Start time: Oct 14, 2021 4:17:22 PM
End time: Oct 14, 2021 5:17:22 PM
Quick Selects: Last hour

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

| Field | Description |
|---|---|
| **Integration Instance Information** tab | • Creation date<br>• Last updated date (for example, the last time started)<br>• Selected consumption (billable) model<br>• Edition (standard or enterprise)<br>• OCID value that uniquely identifies the instance, which can be shown in full and easily copied<br>• Network access setting, which you can change by clicking **Network Access** under **Resources**.<br>• Service Console URL, which can be shown in full and easily copied<br>• License type (either a new cloud license or an existing license brought over from Oracle Fusion Middleware). If you are viewing an Oracle Integration for SaaS instance, the **License Type** field is not displayed.<br>• Number of message packs and the quantity of messages in each pack |
| **Service Console** | Click to access the login page. See the Oracle Integration Help Center.<br>**Note**: You can also access the login page from the main Oracle Cloud Infrastructure Console page for Oracle Integration. At the far right, click ⋮ for the specific instance, and select **Service Console**. |
| **Edit** | Click to edit your settings.<br>See Editing the Edition, License Type, Message Packs, and Custom Endpoint of an Instance in *Provisioning and Administering Oracle Integration Generation 2*. |

| Field | Description |
|---|---|
| **Move** | Click to move the instance to a different compartment. This action can take some time to complete.<br>See Moving an Instance to a Different Compartment in *Provisioning and Administering Oracle Integration Generation 2*. |
| **Add Tags** | Click to add tags to the instance. You can use tags to search for and categorize your instances in your tenancy.<br>See Resource Tags in the Oracle Cloud Infrastructure Documentation. |
| **More Actions** | Contains options to stop, start, or delete the instance.<br>See in *Provisioning and Administering Oracle Integration Generation 2*:<br>• Stopping and Starting an Oracle Integration Instance<br>• Deleting an Instance |
| **Metrics** | Displays message metrics.<br>See Viewing Message Metrics in *Provisioning and Administering Oracle Integration Generation 2*. |
| **Work Requests** | Lists instance life cycle activity, such as instance creation time, instance stop and start times, and so on. |
| **Network Access** | Click **Edit** to change the Network Access setting. Select **Restrict Network Access** to disallow inbound traffic from external networks. |