# Oracle® Cloud

# Using Oracle Integration 3 on Oracle Cloud Infrastructure US Government Cloud

F45536-21
March 2025

Oracle Cloud Using Oracle Integration 3 on Oracle Cloud Infrastructure US Government Cloud,

F45536-21



Primary Author: Oracle Corporation

# Contents


## 1 Get Started with Oracle Integration

How to Use This Guide 1-1
About Oracle Integration 3 on Oracle Cloud Infrastructure US Government Cloud 1-1
- Feature Availability 1-2
- Useful Resources 1-3

Restrictions 1-4

## 2 Set Up Users and Groups

Configure Access to Create and Manage Instances 2-1
- Create an Oracle Cloud Infrastructure Compartment 2-1
- Create an Identity Domain 2-2
- Create an IAM Group 2-2
- Create an IAM Policy 2-3
- Create a User in an IAM Group 2-4
- Assign Oracle Integration Roles to Groups in an Identity Domain 2-5
  - Oracle Integration Service Roles 2-6

## 3 Work with Instances

Create an Oracle Integration Instance 3-1
Use Supported Formats for Key Pairs in SFTP 3-3
View Instance Details 3-4

# Preface

This guide describes how to use Oracle Integration 3 in Oracle Cloud Infrastructure US Government environments.

**Topics:**


- Audience
- Documentation Accessibility
- Diversity and Inclusion
- Related Resources
- Conventions


## Audience

This guide is intended for administrators who want to use Oracle Integration 3 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 3 in a commercial, UK government, or commercial US government environment, see Overview of Oracle Integration 3 in *Provisioning and Administering Oracle Integration 3*.

## Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `https://www.oracle.com/corporate/accessibility/`.

**Access to Oracle Support**

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `https://support.oracle.com/portal/` or visit `Oracle Accessibility Learning and Support` 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.
- Oracle Cloud at `http://cloud.oracle.com`.

# 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

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

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 3 on Oracle Cloud Infrastructure US Government Cloud
- Restrictions


## How to Use This Guide

This guide is intended for administrators using Oracle Integration 3 in an Oracle Cloud Infrastructure US Government Cloud region.

This guide is intended to complement the documentation available in the Oracle Integration 3 documentation library. Use this guide to learn about:

- Oracle Integration 3 feature availability and restrictions in an Oracle Cloud Infrastructure US Government Cloud region.
- Tasks for setting up users and groups, provisioning an Oracle Integration 3 instance, and viewing instance details in an Oracle Cloud Infrastructure US Government Cloud region.

## About Oracle Integration 3 on Oracle Cloud Infrastructure US Government Cloud

Oracle Integration 3 supports several levels of government operators.

### Audience for This Guide

This guide is intended for administrators using Oracle Integration 3 in the Oracle Cloud Infrastructure US Government Cloud regions listed below. To use Oracle Integration 3 in a commercial or United Kingdom Government region, see the Oracle Integration documentation on the Oracle Help Center.

### Supported Realms and Region Locations

| Supported realm | Description | Region locations and available shapes |
|---|---|---|
| Oracle US Government Cloud<br>Realm key: OC2 | Oracle Cloud Infrastructure US Government Cloud with FedRAMP Authorization<br>For more information, see Oracle Cloud Infrastructure US Government Cloud with FedRAMP Authorization. | • US Gov East (Ashburn): Development or Production<br>• US Gov West (Phoenix): Production |
| Oracle US Defense Cloud<br>Realm key: OC3 | Oracle Cloud Infrastructure US Federal Cloud with DISA Impact Level 5 Authorization<br>For more information, see Oracle Cloud Infrastructure US Federal Cloud with DISA Impact Level 5 Authorization. | • US DoD East (Ashburn): Production<br>• US DoD North (Chicago): Production<br>• US DoD West (Phoenix): Production |

### Key Points

- The instances that you can provision in Oracle US Defense Cloud depend upon whether your tenancy uses identity domains:
  - If your tenancy uses identity domains, you can provision only Oracle Integration 3 instances in Oracle US Defense Cloud.
  - If your tenancy doesn't use identity domains, you can provision only Oracle Integration Generation 2 instances in Oracle US Defense Cloud.
- B2B for Oracle Integration is supported.

### Topics

- Feature Availability
- Useful Resources

# Feature Availability

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 |
|---|---|
| Adapters | All Oracle Integration Adapters available. |
| 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. |
| Authentication | Client credentials is the only authorization grant flow supported for OAuth authentication in Oracle Cloud Infrastructure in government environments. |
| B2B for Oracle Integration | Available. |

| Oracle Integration Features | Notes |
|---|---|
| Development shapes for instances | Available in some regions. See About Oracle Integration 3 on Oracle Cloud Infrastructure US Government Cloud. |
| File Server | Available. |
| Integrations | Available, except for the following:<br>• Accept mapping recommendations with the recommendations engine.<br>• Invoke a process from an integration.<br>• Create an event integration:<br>– Available in Oracle US Government Cloud (realm key: OC2), US Gov East (Ashburn).<br>Region identifier: us-langley-1<br>– Not available in Oracle US Government Cloud (realm key: OC2), US Gov West (Phoenix).<br>Region identifier: us-luke-1<br>– Not available in Oracle US Defense Cloud (realm key: OC3). |
| Oracle Assistant for Oracle Integration | Not available. |
| Oracle Integration for Healthcare | Not available. |
| Private endpoints | Available in Oracle US Government Cloud (realm key: OC2).<br>Not available in Oracle US Defense Cloud (realm key: OC3). |
| Process Automation | Available. |
| Robots | Not available. |
| Upgrading from Oracle Integration Generation 2 to Oracle Integration 3 | Available. See Upgrade in an Oracle Cloud Infrastructure US Government Cloud Region in *Provisioning and Administering Oracle Integration 3*. |
| Visual Builder | Available. |
| Oracle-managed disaster recovery | Not available. |

# Useful Resources

Review the following documentation resources.

| Documentation | Notes and Main Differences in US Government Cloud |
|---|---|
| *What's New for Oracle Integration 3*<br>*Known Issues for Oracle Integration 3*<br>*Getting Started with Oracle Integration 3*<br>*Using Integrations in Oracle Integration 3*<br>Oracle Integration Adapters<br>*Provisioning and Administering Oracle Integration 3* | 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 Feature Availability. Also ignore references to Oracle Identity Cloud Service. In Oracle Cloud Infrastructure US Government Cloud environments, you use IAM to manage users and groups. |

| Documentation | Notes and Main Differences in US Government Cloud |
|---|---|
| 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. |

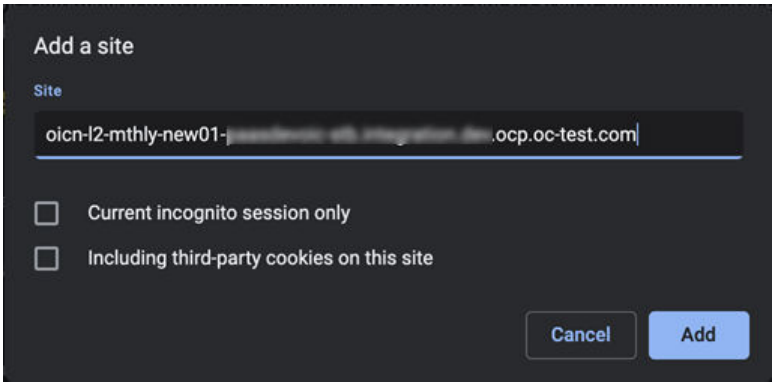
# Restrictions

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

- US Government Cloud does not support creating events to publish and subscribe to in integrations.
- 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 3*), 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 and project deployments.
- In US Government Cloud realm (realm key: OC2) 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 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.
- 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.
- The Oracle Autonomous Transaction Processing Adapter, Oracle Autonomous Data Warehouse Adapter, and Oracle Database Cloud Service Adapter do not support using the JDBC Basic Authentication security policy (also known as Username Password Token) with direct connectivity. You must use a wallet security policy (JDBC Over SSL or JDBC With OCI Signature) if you want to directly connect to database endpoints.
- **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 check boxes deselected, and click **Add**.




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

2

# Set Up Users and Groups

Configure users and groups and grant them the right level of access on Oracle Cloud Infrastructure US Government Cloud.

**Topics:**


- Configure Access to Create and Manage Instances


## Configure Access to Create and Manage Instances

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

In Oracle Integration 3 government regions, users and groups are managed in identity domains in Oracle Cloud Infrastructure Identity and Access Management (IAM).

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 Compartment
- Create an Identity Domain
- Create an IAM Group
- Create an IAM Policy
- Create a User in an IAM Group
- Assign Oracle Integration Roles to Groups in an Identity Domain


### Create an Oracle Cloud Infrastructure Compartment

Oracle Integration instances use the Oracle Cloud Infrastructure as their underlying infrastructure. To create an Oracle Integration instance, you must first create a compartment, unless you want to create the instance in the root compartment.

See Managing Compartments.

You can create a new compartment or use an existing compartment. You must have permission to create and delete compartments.

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Compartments**.
   A list of the compartments in your tenancy is displayed.

2. Select the compartment in which you want to create your instance or create a new compartment.
   To create a new compartment:
   a. Click **Create Compartment** to create the compartment to use for creating an instance.
   b. Enter the following:
      - **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 `OICCompartment`.
      - **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.
   c. Click **Create Compartment**.

      Return to the navigation pane.

## Create an Identity Domain

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

For more information about identity domains, see Managing Identity Domains in the Oracle Cloud Infrastructure documentation.

In an Oracle Cloud Infrastructure tenancy, your environment includes a root (default) compartment and possibly several other compartments, depending on how your environment is configured. To create compartments, see Create an Oracle Cloud Infrastructure 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

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

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. Click **Groups**.

   The Groups page for the domain is displayed.
4. Click **Create group**.
5. In the Create group screen, assign a name to the group (for example, `oci-integration-admins`), and enter a description.
6. Click **Create**.

## Create an IAM Policy

Create a policy to grant permissions to users in a domain group to work with Oracle Integration instances within a specified tenancy or 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, `IntegrationGroupPolicy`) 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-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`.

**Notes:**

- If you omit the domain name, the default domain is assumed.
- When defining policy statements, you can specify either verbs (as used in these steps) or permissions (typically used by power users).
- You can create separate groups for different permissions, such as a group with `read` permission only.
- 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. |

To learn more about policies, see:

- How Policies Work and Policy Reference in the Oracle Cloud Infrastructure documentation

5. Click **Create**.

   The policy statements are validated and syntax errors are displayed.

## Create a User in an IAM Group

Create a user to assign to a group in an Oracle Cloud Infrastructure identity domain.

For more information about users, 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 for the domain is displayed.

5. Click **Create user**.
6. In the Create user screen, enter the user's first and last name, and their username, then select the 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.
    - **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.
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 Oracle Integration Roles to Groups in an Identity Domain

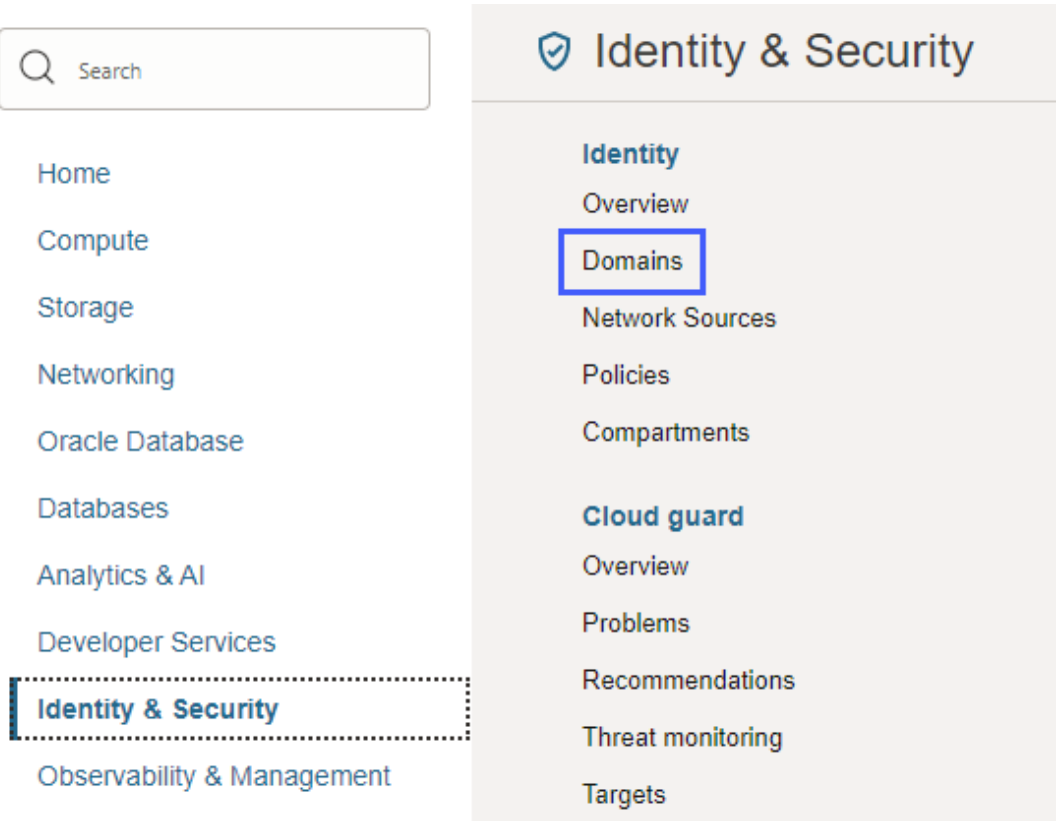
After an Oracle Integration instance has been created, assign Oracle Integration roles to groups of users to allow them to work with the features of the Oracle Integration instance.

> **Note:**
>
> It's a best practice to assign Oracle Integration roles to selected groups rather than individual users.

Oracle Integration provides a standard set of roles, which govern access to features. See Oracle Integration Service Roles. Depending on the Oracle Integration features your organization uses, you may choose to create groups named for the role they are granted. 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

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 Oracle Integration roles resides.
3. Open 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 **Name** column, click the Oracle Integration instance for which you want to assign group roles.

   The instance details page is displayed.
6. In the navigation pane, click **Application roles**.
7. In the **Application roles** list, locate the role(s) you want to assign to the group. At the far right, click **Open Details** ⌄.
8. Next to **Assigned groups**, click **Manage**.
9. On the Manage group assignment panel, click **Show available groups**.
10. In the **Available groups** list, select the group to which to assign the role, and click **Assign**.

## 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. |
| `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.

3

# Work with Instances

Create and edit Oracle Integration 3 instances in the Oracle Cloud Infrastructure Console on Oracle Cloud Infrastructure US Government Cloud.

**Topics:**

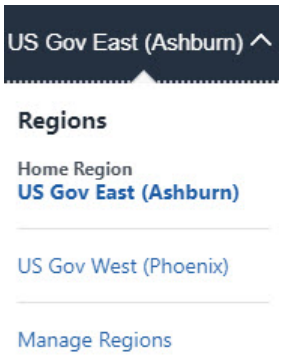

- Create an Oracle Integration Instance
- Use Supported Formats for Key Pairs in SFTP
- View Instance Details


## Create an Oracle Integration Instance

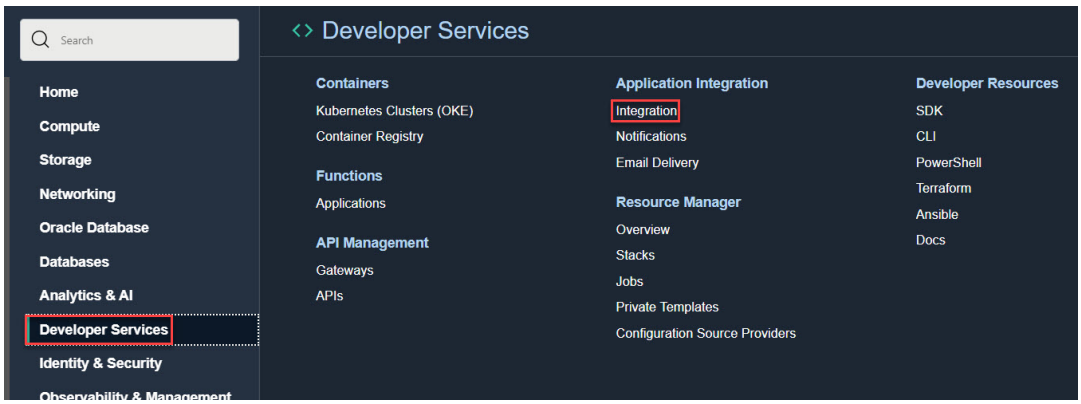
To create an Oracle Integration instance in a selected compartment:

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

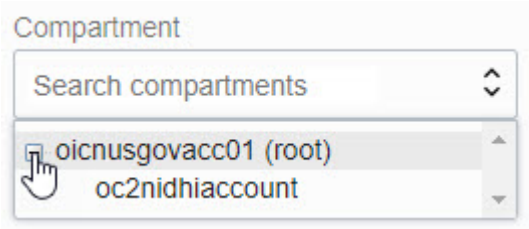
   Once created, instances are visible only in the region in which they were created.




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

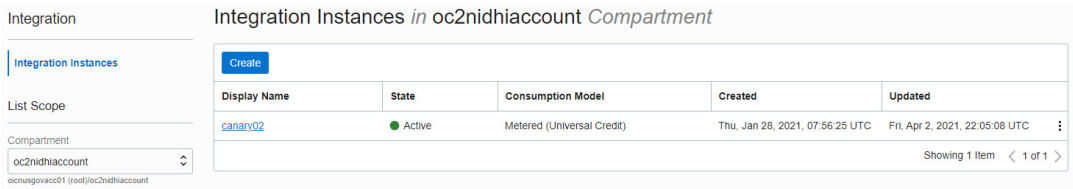


3. From the **Compartment** list, click through the hierarchy of compartments and select the one in which to create the instance. You may need to expand the **+** icon to find the compartment to use. Compartments can contain other compartments. It may take several minutes for the new compartment to appear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




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. |
| 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><br>**Note:**<br>*Oracle Integration Government* is a license and doesn't specify the realm. |

| Field | Description |
|---|---|
| Shape | Choose a shape for the instance. The shape determines when the instance receives updates, which happen every other month.<br>Only some regions allow you to choose a shape. If you don't see the option to choose a shape, your instance is created in the **Production** shape. For details about the shapes that each region supports, see About Oracle Integration 3 on Oracle Cloud Infrastructure US Government Cloud.<br>• **Development:** Instances with this shape receive updates two weeks before instances with a Production shape.<br>• **Production:** Instances with this shape receive updates two weeks after instances with a Development shape.<br>**Note:** You can't change the shape after you create the instance. However, you can move data to another instance using the export and import features. |
| 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.

# Use Supported Formats for Key Pairs in SFTP

If you want to use public key authentication with SFTP servers for service instances in government realms, you must use SSH keys in OpenSSH format. PEM format does not work.

Perform the following task based on your scenario.

| If... | Then... |
|---|---|
| You need to create a new key pair | Enter the following command:<br>`ssh-keygen -t rsa -m RFC4716` |

| If... | Then... |
| --- | --- |
| You already have a PEM-formatted key pair | Enter the following command to convert from PEM to OpenSSH format<br><br>`ssh-keygen -p -f your_PEM_formatted_private_key -m RFC4716` |

Once the private key is generated, upload it to the Connections page for the FTP Adapter. If you open the OpenSSH-formatted key, the header must look similar to the following:

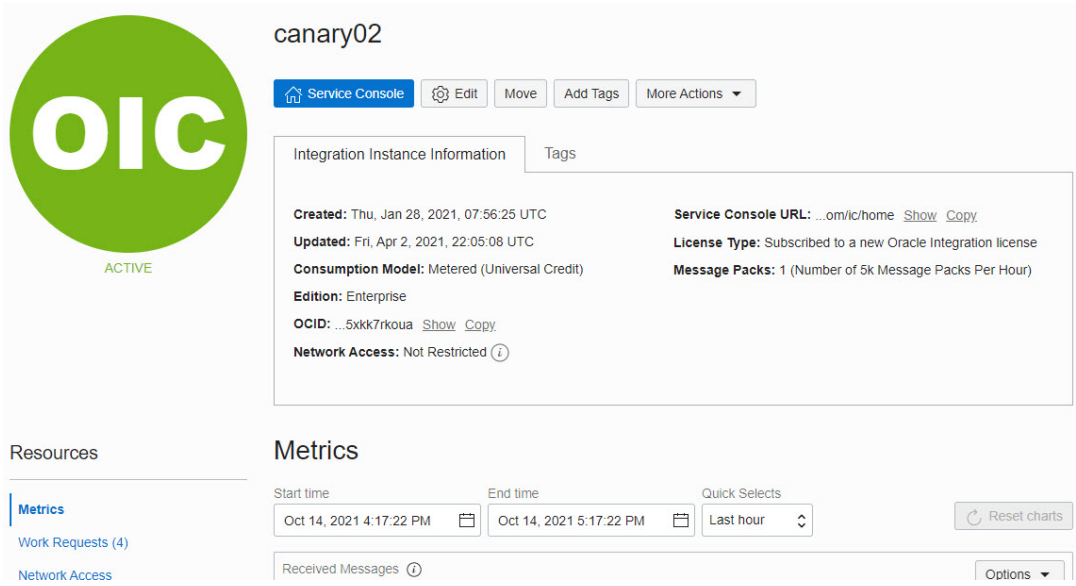
```
----BEGIN OPENSSH PRIVATE KEY----
```

If the key shows anything else, authentication fails.

# 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.




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 3*. |
| **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 3*. |
| **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 3*:<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 3*. |

| Field | Description |
| --- | --- |
| **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. |