

Oracle® Cloud

Administering Oracle Analytics Cloud on Oracle Cloud Infrastructure (Gen 2)



G50143-02
February 2026



Oracle Cloud Administering Oracle Analytics Cloud on Oracle Cloud Infrastructure (Gen 2),

G50143-02

Copyright © 2019, 2026, Oracle and/or its affiliates.

Primary Author: Rosie Harvey

Contributors: Oracle Analytics Cloud development, product management, and quality assurance teams

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

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

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

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

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

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

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

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

Contents

Preface

Audience	i
Related Documents	i
Conventions	i

1 Get Started with Administration

About Oracle Analytics Cloud on Gen 2	1
Region Availability	1
Service Limits	2
Service Quotas	2
Service Events	3
Supported TLS Ciphers	5
Typical Workflow for Administrators	5
Before You Begin with Oracle Analytics Cloud on Gen 2	6
Signing In to the Oracle Cloud Infrastructure Console	7
Sign In to a Cloud Account That Uses Identity Domains	8
Sign In to a Cloud Account That Does Not Use Identity Domains	10

2 Set Up Users

About Setting Up Users and Groups	1
Use Identity Domains to Set Up Users and Groups for Oracle Analytics Cloud	2
Use Oracle Identity Cloud Service to Set Up Users and Groups for Oracle Analytics Cloud	3

3 Create Services with Oracle Analytics Cloud

Typical Workflow to Create a Service	1
Before You Create a Service	2
Plan Your Service	2
Which Edition Do You Need?	2
Where Do You Want to Deploy Your Service?	3
Which Identity Provider and Administrator Do You Want for Your Service?	3
Do You Need a Public or Private Endpoint?	4

What Sizing Options Are Available to You?	4
What Name Do You Want for Your Service?	10
Do You Want Early Access to Updates?	11
Give Another User Permission to Set Up Oracle Analytics Cloud	11
Create a Compartment	12
Create a Service	13
Create a Service using the Console	14
Create a Service using the REST API	18
Create a Service using the Command Line	19
Generate IDCS Access Tokens for the REST API and CLI	19
Create a Confidential Application to Generate Access Tokens (Identity Domains)	20
Generate and Use Access Tokens in REST API and CLI Payloads (Identity Domains)	22
Create a Confidential Application to Generate Access Tokens (IDCS)	24
Generate and Use Access Tokens in REST API and CLI Payloads (IDCS)	26
After You Create a Service	28
Verify Your Service and Sign In	28
Configure Options for Your Service	30
Migrate to Oracle Analytics Cloud from Other Environments	30

4 Administer Services

About Oracle Analytics Cloud Administration Pages	1
Typical Workflow to Administer a Service	7
View or Update a Service	7
View or Update a Service using the Console	8
View or Update a Service using the REST API	9
View or Update a Service using the Command Line	9
Scale a Service	10
About Scaling	10
Scale Up or Down using the Console	11
Scale Up or Down using the REST API	13
Scale Up or Down using the Command Line	13
Pause and Resume a Service	13
Pause and Resume using the Console	14
Pause and Resume a Service using the REST API	14
Pause and Resume using the Command Line	14
Delete a Service	15
Delete a Service using the Console	15
Delete a Service using the REST API	15
Delete a Service using the Command Line	16
Monitor Status	16

Monitor Status using the Console	16
Monitor Status using the REST API	18
Monitor Status using the Command Line	18
Monitor Metrics	19
About Metrics for Oracle Analytics Cloud	20
Access Metrics for Oracle Analytics Cloud Using the Console (Instance Details)	21
Access Metrics for Oracle Analytics Cloud Using the Console (Metrics Explorer)	22
Access Metrics Using the REST API	23
Access Metrics Using the Command Line	23
Monitor Logs	24
Monitor Usage and Diagnostic Logs	24
About Audit and Diagnostic Logs for Oracle Analytics Cloud	25
Access Audit and Diagnostic Logs for Oracle Analytics Cloud Using the Console	33
Monitor Instance Event Logs	36
Find Oracle Analytics Cloud Resources	37
Read Cost Reports	39
Analyze Costs for Oracle Analytics Cloud	39
Verify Update Cycle	41

5 Manage Service Access and Security

Give Users Permissions to Manage Analytics Cloud Instances	1
About Permissions to Manage Oracle Analytics Cloud Instances	1
Example Policy Statements to Manage Analytics Cloud Instances	4
Set Up Polices (Identity Domains)	7
Typical Workflow for Setting Up Policies to Manage Analytics Cloud Instances (Identity Domains)	7
Give a User Permissions to Manage Analytics Cloud Instances (Identity Domains)	8
Set Up Policies (Federated Oracle Identity Cloud Service)	8
Typical Workflow to Set Up Policies to Manage Analytics Cloud Instances (Oracle Identity Cloud Service)	9
Give a User in Oracle Identity Cloud Service Permissions to Manage Analytics Cloud Instances	9
Give Data Sources Access to Analytics Cloud Instances	10
Find the IP Address or Host Name of Your Oracle Analytics Cloud Instance	11
Add the IP Address of Your Oracle Analytics Cloud Instance to Allowlists	12
Public IP Ranges and Gateway IPs for Oracle Analytics Cloud Instances	14
Restrict Access to Oracle Analytics Cloud Deployed with a Public Endpoint	16
About Public Endpoints and Access Control Rules	16
Prerequisites for a Public Endpoint	18
Typical Workflow to Restrict Public Access using Rules	19
Create Oracle Analytics Cloud with a Public Endpoint	20
Control Incoming Traffic for a Public Endpoint (Ingress)	20

Manage Ingress Access Rules for a Public Endpoint using the Console	21
Manage Ingress Access Rules for a Public Endpoint using the REST API	22
Manage Ingress Access Rules for a Public Endpoint using the Command Line	22
Control Outgoing Traffic for a Public Endpoint (Egress)	23
Deploy Oracle Analytics Cloud with a Private Endpoint	23
About Private Endpoints	24
Prerequisites for a Private Endpoint	25
Typical Workflow to Deploy Oracle Analytics Cloud with a Private Endpoint	26
Create Oracle Analytics Cloud with a Private Endpoint	27
Connect to Your On-premise Network using FastConnect or VPN Connect	28
Change the VCN or Subnet Used to Access a Private Endpoint	29
Change a Private Endpoint using the Console	29
Change a Private Endpoint using the REST API	31
Change a Private Endpoint using the Command Line	31
Control Incoming and Outgoing Traffic for a Private Endpoint (Ingress and Egress)	31
Connect to Private Sources Through a Private Access Channel	32
About Private Access Channels	33
About Private Sources	34
About Connecting to Private Sources	34
Supported Private Data Sources	35
Private Source Limitations - SCAN	35
Private Source Limitations - Canonical Host Names	36
Top FAQs for Private Sources	36
Prerequisites for a Private Access Channel	40
Typical Workflow to Set Up a Private Access Channel	44
Configure a Private Access Channel	45
Configure a Private Access Channel using the Console	46
Configure a Private Access Channel using the REST API	48
Configure a Private Access Channel using the Command Line	49
Edit a Private Access Channel	49
Edit Network Details for a Private Access Channel using the Console	49
Manage the Private Sources You Can Access on a Private Access Channel Using the Console	51
Edit a Private Access Channel using the REST API	53
Edit a Private Access Channel using the Command Line	53
Delete a Private Access Channel	54
Delete a Private Access Channel using the Console	54
Delete a Private Access Channel using the REST API	55
Delete a Private Access Channel using the Command Line	55
Use Network Security Groups to Control Access	55
About Network Security Groups and Security Lists	55
About Using Network Security Groups with Oracle Analytics Cloud	56

Manage Egress Access Rules for a Public Endpoint using the Console	57
Prerequisites for Network Security Groups	59
Manage Ingress and Egress Access Rules for a Private Endpoint using the Console	60
Federate with Oracle Identity Cloud Service Manually	61
Set Up a Custom Vanity URL	62
About Vanity URLs	63
Typical Workflow to Set Up a Vanity URL	63
Prerequisites for a Vanity URL	64
Configure a Vanity URL	64
Configure a Vanity URL using the Console	64
Configure a Vanity URL using the REST API	66
Configure a Vanity URL using the Command Line	66
Update Certificates for a Vanity URL	66
Update Certificates for a Vanity URL using the Console	67
Update Certificates for a Vanity URL using the REST API	67
Update Certificates for a Vanity URL using the Command Line	67
Delete a Vanity URL	68
Delete a Vanity URL using the Console	68
Delete a Vanity URL using the REST API	68
Delete a Vanity URL using the Command Line	69
Encrypt Sensitive Information	69
About Encryption in Oracle Analytics Cloud	69
Typical Workflow to Manage Encryption	70
Prerequisites for Custom Encryption	71
Assign a Custom Encryption Key	72
Assign a Custom Encryption Key using the Console	72
Assign a Custom Encryption Key using the REST API	74
Assign a Custom Encryption Key using the Command Line	74
Rotate or Change the Custom Encryption Key	74
Rotate or Change the Custom Encryption Key using the Console	75
Rotate or Change the Custom Encryption Key using the REST API	76
Rotate or Change the Custom Encryption Key using the Command Line	76
Remove a Custom Encryption Key	77
Remove a Custom Encryption Key using the Console	77
Remove a Custom Encryption Key using the REST API	78
Remove a Custom Encryption Key using the Command Line	78

6 Frequently Asked Questions

Top FAQs for Administration	3
Top FAQs For Backup and Restore User Content (Snapshots)	7
Top FAQs For Disaster Recovery	9

Top FAQs for Public or Private Endpoint Security	9
Top FAQs for Network Security Groups	11
Top FAQs for Private Sources	12
Top FAQs for Vanity URLs	16
Top FAQs for Data Encryption	17

7 Troubleshoot

Troubleshoot Instance Creation Issues	1
Troubleshoot Data Source Connectivity Issues	3
Troubleshoot Connectivity Issues Using Network Path Analyzer	3
Example: Oracle Analytics Cloud Connection to an On-premises Database	5
Troubleshoot Other Issues	7

Preface

Learn how to create and manage services with Oracle Analytics Cloud on Oracle Cloud Infrastructure.

Topics:

- [Audience](#)
- [Related Documents](#)
- [Conventions](#)

Audience

Administering Oracle Analytics Cloud on Oracle Cloud Infrastructure (Gen 2) is intended for administrators who set up Oracle Analytics Cloud on Oracle Cloud Infrastructure.

- **Administrators** set up services with Oracle Analytics Cloud and manage access to those services.
- **Analysts** load and model data and create reports and data visualizations for consumers. Data integration options range from self-service import to operational ETL updates. Analysts can select interactive visualizations and create advanced calculations to reveal insights in the data.
- **Consumers** customize dashboard pages and work with their favorite reports and data visualizations. Dashboards allow consumers to quickly analyze and manage activity across their system.

Related Documents

These related Oracle resources provide more information.

- [Getting Started with Oracle Analytics Cloud](#)
- [Visualizing Data and Building Reports in Oracle Analytics Cloud](#)
- [Configuring Oracle Analytics Cloud](#)

Conventions

Conventions used in this document are described in this topic.

Text Conventions

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.

Convention	Meaning
<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.

Videos and Images

Your company can use skins and styles to customize the look of the Oracle Analytics Cloud, dashboards, reports, and other objects. It is possible that the videos and images included in the product documentation look different than the skins and styles your company uses.

Even if your skins and styles are different than those shown in the videos and images, the product behavior and techniques shown and demonstrated are the same.

1

Get Started with Administration

Let's explore Oracle Analytics Cloud and what you need to know to get started with deployment and administration on Oracle Cloud Infrastructure Gen 2.

Note

If your Oracle Analytics Cloud subscription started before Oracle Analytics Cloud was available on Oracle Cloud Infrastructure Gen 2, read these topics to find out what's new and different:

- **North America:** See [Get Started with Oracle Analytics Cloud \(North America\) - Accounts Started Before 14th February 2020](#).
- **EMEA:** See [Get Started with Oracle Analytics Cloud \(EMEA\) - Accounts Started Before 2nd March 2020](#).

Topics

- [About Oracle Analytics Cloud on Gen 2](#)
- [Typical Workflow for Administrators](#)
- [Before You Begin with Oracle Analytics Cloud on Gen 2](#)

About Oracle Analytics Cloud on Gen 2

Oracle Analytics Cloud is a scalable and secure public cloud service that provides capabilities to explore and perform collaborative analytics for you, your workgroup, and your enterprise.

Oracle Analytics Cloud is available on Oracle Cloud Infrastructure Gen 2 in several regions in North America, EMEA, APAC, and LAD when you subscribe through Universal Credits. You can subscribe to Professional Edition or Enterprise Edition.

When you deploy Oracle Analytics Cloud on Gen 2, you complete some initial setup steps, and then Oracle takes care of most service management, patching, backup and restore, and other maintenance tasks. You determine the size of your service when you set up the service and you can increase or decrease capacity if your requirements change. Oracle Analytics Cloud offers two sizing options, you can specify the number of Oracle Compute Units (OCPU) you want to deploy or how many people you expect to use the service.

Region Availability

Oracle Analytics Cloud is currently available on several data regions in North America, Europe, the Middle East and Africa (EMEA), Asia-Pacific (APAC), and Latin American (LAD). Thereafter, Oracle Analytics Cloud will expand to other regions.

For the latest information on availability in regions, see [Data Regions for Platform and Infrastructure Services](#).

Service Limits

Oracle Analytics Cloud has various default limits. Whenever you create an Oracle Analytics Cloud instance or scale up, the system ensures that your request is within the bounds of your limit. The limit that applies to you depends on which edition you subscribe to: Professional Edition or Enterprise Edition.

Resource Limit	Limit Short Name	Default Value (Universal Credits)	Default Value (Pay As You Go or Trials)	Description
Professional Edition OCPUs	se-ocpu-count	4	4	Maximum number of OCPUs available with Oracle Analytics Cloud Professional Edition.
Enterprise Edition OCPUs	ee-ocpu-count	40	4	Maximum number of OCPUs available with Oracle Analytics Cloud Enterprise Edition.
Professional Edition Users	se-user-count	200	-	Maximum number of users available with Oracle Analytics Cloud Professional Edition.
Enterprise Edition Users	ee-user-count	200	-	Maximum number of users available with Oracle Analytics Cloud Enterprise Edition.

You can submit a request to increase your limits from **Limits, Quotas, and Usage** page in Oracle Cloud Infrastructure Console.

See [About Service Limits and Usage](#).

Service Quotas

You can use quotas to determine how other users allocate Oracle Analytics Cloud resources across compartments in Oracle Cloud Infrastructure. Whenever you create an Oracle Analytics Cloud instance or scale up, the system ensures that your request is within the bounds of the quota for that compartment.

The quota that you use to allocate Oracle Analytics Cloud resources depends on which edition you subscribe to: Professional Edition or Enterprise Edition.

Quota Name	Scope	Description
se-ocpu-count	Regional	Number of Professional Edition OCPUs.
ee-ocpu-count	Regional	Number of Enterprise Edition OCPUs.

Quota Name	Scope	Description
se-user-count	Regional	Number of Professional Edition users.
ee-user-count	Regional	Number of Enterprise Edition users.

Example Quota Statements for Oracle Analytics Cloud

- Limit the number of OCPUs that users can allocate to self-service analytics services they create in MyDVCompartment to 2.**

```
set analytics quota se-ocpu-count to 2 in compartment MyDVCompartment
```
- Limit the number of OCPUs that users can allocate to enterprise analytics services they create in MyEnterpriseCompartment to 10.**

```
set analytics quota ee-ocpu-count to 10 in compartment MyEnterpriseCompartment
```
- Limit the user count for enterprise analytics services that users create in MyEnterpriseCompartment to 100.**

```
set analytics quota ee-user-count to 100 in compartment MyEnterpriseCompartment
```
- Don't allow users to allocate any OCPUs to enterprise analytics services in MyTestCompartment.**

```
zero analytics quota ee-ocpu-count in compartment MyTestCompartment
```

See [About Compartment Quotas](#).

Service Events

Actions that you perform on Oracle Analytics Cloud instances emit events.

You can define rules that trigger a specific action when an event occurs. For example, you might define a rule that sends a notification to administrators when someone deletes an instance. See [Overview of Events](#) and [Get Started with Events](#).

This table lists the Oracle Analytics Cloud events that you can reference.

Event Name	Event Type
Analytics - Instance - Create Instance	com.oraclecloud.analytics.createanalyticsinstance
Analytics - Instance - Update Instance	com.oraclecloud.analytics.updateanalyticsinstance
Analytics - Instance - Delete Instance	com.oraclecloud.analytics.deleteanalyticsinstance
Analytics - Instance - Scale Instance Up or Down Begin	com.oraclecloud.analytics.scaleanalyticsinstance.begin
Analytics - Instance - Scale Instance Up or Down End	com.oraclecloud.analytics.scaleanalyticsinstance.end
Analytics - Instance - Start Instance Begin	com.oraclecloud.analytics.startanalyticsinstance.begin
Analytics - Instance - Start Instance End	com.oraclecloud.analytics.startanalyticsinstance.end
Analytics - Instance - Stop Instance Begin	com.oraclecloud.analytics.stopanalyticsinstance.begin
Analytics - Instance - Stop Instance End	com.oraclecloud.analytics.stopanalyticsinstance.end

Event Name	Event Type
Analytics - Instance - Change Compartment Begin	com.oraclecloud.analytics.changeanalyticsinstance.compartment.begin
Analytics - Instance - Change Compartment End	com.oraclecloud.analytics.changeanalyticsinstance.compartment.end
Analytics - Instance - Change Network Endpoint Begin	com.oraclecloud.analytics.changeanalyticsinstance.networkendpoint.begin
Analytics - Instance - Change Network Endpoint End	com.oraclecloud.analytics.changeanalyticsinstance.networkendpoint.end
Analytics - Instance - Create Vanity URL Begin	com.oraclecloud.analytics.createvanityurl.begin
Analytics - Instance - Create Vanity URL End	com.oraclecloud.analytics.createvanityurl.end
Analytics - Instance - Update Vanity URL Begin	com.oraclecloud.analytics.updatevanityurl.begin
Analytics - Instance - Update Vanity URL End	com.oraclecloud.analytics.updatevanityurl.end
Analytics - Instance - Delete Vanity URL Begin	com.oraclecloud.analytics.deletevanityurl.begin
Analytics - Instance - Delete Vanity URL End	com.oraclecloud.analytics.deletevanityurl.end
Analytics - Instance - Update Custom Encryption Key Begin	com.oraclecloud.analytics.updateinstancekmskeyid.begin
Analytics - Instance - Update Custom Encryption Key End	com.oraclecloud.analytics.updateinstancekmskeyid.end
Analytics - Instance - Create Private Access Channel Begin	com.oraclecloud.analytics.createprivateaccesschannel.begin
Analytics - Instance - Create Private Access Channel End	com.oraclecloud.analytics.createprivateaccesschannel.end
Analytics - Instance - Update Private Access Channel Begin	com.oraclecloud.analytics.updateprivateaccesschannel.begin
Analytics - Instance - Update Private Access Channel End	com.oraclecloud.analytics.updateprivateaccesschannel.end
Analytics - Instance - Delete Private Access Channel Begin	com.oraclecloud.analytics.deleteprivateaccesschannel.begin
Analytics - Instance - Delete Private Access Channel End	com.oraclecloud.analytics.deleteprivateaccesschannel.end

Example

This example shows information associated with the event **Analytics - Instance - Create Instance**:

```
{
  "cloudEventsVersion": "0.1",
  "contentType": "application/json",
  "source": "analytics",
  "eventID": "<unique_ID>",
  "eventType": "com.oraclecloud.analytics.createanalyticsinstance",
  "eventTypeVersion": "<version>",
  "eventTime": "2019-10-19T00:53:04.126Z",
  "data": {
    "additionalDetails": {},
    "availabilityDomain": "<availability_domain>",
    "compartmentId": "ocidl.compartment.oc1..<unique_ID>",
    "compartmentName": "my_compartment",
    "freeformTags": {},
    "resourceId": "ocidl.analyticsinstance.oc1..<unique_ID>",
    "resourceName": "my_analytics_cloud"
  }
}
```

```

    },
    "extensions": {
      "compartmentId": "ocidl.compartment.ocl1.<unique_ID>"
    }
  }

```

Supported TLS Ciphers

Oracle Analytics Cloud supports the following ciphers with TLS 1.3 and TLS 1.2.

Supported Ciphers

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-CCM
- ECDHE-ECDSA-AES128-CCM

Deprecated Ciphers

The following ciphers are not supported as of December 2024. If you use any of these ciphers, replace them with a supported cipher.

- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384

Typical Workflow for Administrators

If you're setting up Oracle Analytics Cloud on Gen 2 for the first time, follow these tasks as a guide.

Task	Description	More Information
Place an order for Oracle Analytics Cloud or sign up for a free Oracle Cloud promotion	Sign up for a free credit promotion or subscribe to Oracle Analytics Cloud through Universal Credits. See Data Regions for Platform and Infrastructure Services .	Request and Manage Free Oracle Cloud Promotions Upgrade to a Paid Account
Activate your Oracle Cloud account and sign in for the first time	You receive a welcome email when your account is ready. To activate your account, you must sign in with the credentials provided in the email. As the Cloud Account Administrator, you can complete all the setup tasks for Oracle Analytics Cloud.	Signing in for the First Time
Determine your service requirements	Plan your Oracle Analytics Cloud deployment. Think about what you need before you start.	Plan Your Service
(Optional) Enable other users to set up services	If you don't want to set up Oracle Analytics Cloud yourself, give other users permissions to create services.	Give Another User Permission to Set Up Oracle Analytics Cloud

Task	Description	More Information
(Recommended) Create a compartment for your service	Create a compartment for your Oracle Analytics Cloud deployment.	Create a Compartment
Create a service	Deploy a new service with Oracle Analytics Cloud.	Create a Service
Verify your service	When your service is ready, check that you can sign in and your service is up and running.	Verify Your Service and Sign In
Set up users and groups	Set up users and groups for Oracle Analytics Cloud and assign them to application roles.	Set Up Users
Schedule regular backups of your data (snapshots)	As part of your business continuity plan, take a snapshot before people start using the system and again at suitable intervals so you can restore the environment if something goes wrong.	Schedule Regular Snapshots
Set service-level options	Configure service-level options for everyone using your service.	Configure Options for Your Service
Migrate content	Leverage your existing content in Oracle Analytics Cloud.	Migrate to Oracle Analytics Cloud from Other Environments
Administer services	Monitor services and perform administrative tasks such as pause, resume, scale, delete, and so on. Delegate administrative responsibilities to others through security policies.	Administer Services Give Users Permissions to Manage Analytics Cloud Instances

Before You Begin with Oracle Analytics Cloud on Gen 2

When you order Oracle Analytics Cloud through Universal Credits, you automatically get access to Oracle Cloud Infrastructure Gen 2 and other required services.

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

Service	What is it for?	Do I need to do anything?
Oracle Cloud Infrastructure Identity and Access Management (IAM)	<p>Compartments: You use compartments to organize resources on Oracle Cloud Infrastructure.</p> <p>Policies: You use IAM security policies to grant permissions.</p> <p>Domains: If available in your cloud account, you use identity domains to manage users and groups in your organization who will use Oracle Analytics Cloud and Oracle Cloud Infrastructure Console.</p>	<p>Yes.</p> <p>Before you create your first Oracle Analytics Cloud instance, Oracle recommends that you set up one or more compartments in which you can deploy and secure your cloud resources.</p> <ul style="list-style-type: none"> • Setting Up Your Tenancy • Managing Compartments <p>Optionally, you can set up security policies that give other users permission to set up and manage Oracle Analytics Cloud instances. See Give Users Permissions to Manage Analytics Cloud Instances.</p> <p>If identity domains are available, you can add Oracle Analytics Cloud users and groups before you create the Oracle Analytics Cloud instance or after; you can decide. See Use Identity Domains to Set Up Users and Groups for Oracle Analytics Cloud.</p>
Oracle Identity Cloud Service	<p>If identity domains aren't available in your cloud account, you use Oracle Identity Cloud Service to manage the users and groups in your organization who will use Oracle Analytics Cloud.</p> <p>In most cases, Oracle Analytics Cloud is automatically federated with the <i>primary</i> Oracle Identity Cloud Service instance associated with your tenancy.</p>	<p>Yes.</p> <p>You can add users and groups before you create the Oracle Analytics Cloud instance or after; you can decide. See Use Oracle Identity Cloud Service to Set Up Users and Groups for Oracle Analytics Cloud.</p> <p>Note: If you want to federate with a <i>secondary</i> Oracle Identity Cloud Service instance or your tenancy is a government region where federation isn't set up automatically, you must federate with Oracle Identity Cloud Service manually. See Federate with Oracle Identity Cloud Service Manually.</p>

Signing In to the Oracle Cloud Infrastructure Console

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

If you are not sure if your cloud account uses identity domains, see [Set Up Users](#).

Topics:

- [Sign In to a Cloud Account That Uses Identity Domains](#)
- [Sign In to a Cloud Account That Does Not Use Identity Domains](#)

Sign In to a Cloud Account That Uses Identity Domains

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

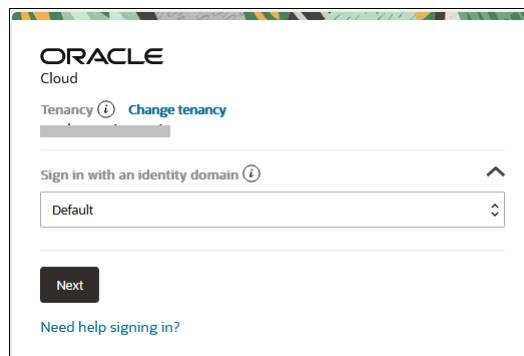


This topic applies only to cloud accounts that use identity domains. See [Set Up Users](#).

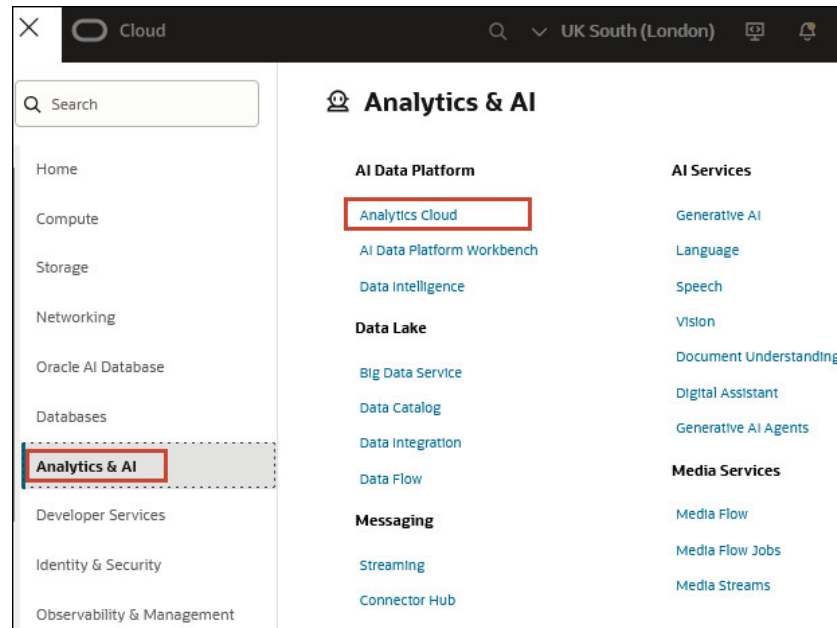
1. Go to <http://cloud.oracle.com>.
2. Enter your cloud account name and click **Next**.
3. Select the **Default** domain.


Every cloud account includes a **Default** identity domain.

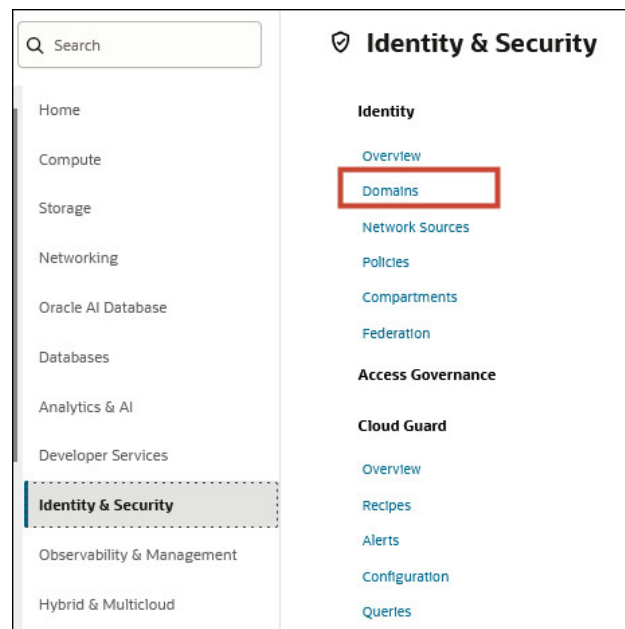
You can create and manage multiple identity domains in your cloud account. For example, you might want one for development and one for production. If multiple identity domains are available, select the domain you want.



4. Enter the user name and password provided in the welcome email, and click **Sign In**.
The Oracle Cloud Infrastructure Console is displayed.
Take some time to explore categories and options in the navigation menu.
5. Navigate to the **Oracle Analytics Cloud** landing page where you access, create, and manage Oracle Analytics Cloud instances.
 - a. Open the navigation menu and click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.



- b. Click **pin**  to save the selection under the **Pinned** category on the Home page.
6. Navigate to the **Oracle Cloud Infrastructure Identity and Access Management** landing page where you create and manage compartments, identity domains, users, groups, and more.
 - a. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains, Compartments, Policies**, and so on.



- b. Click **pin**  to save the selection under the **Pinned** category on the Home page.

Sign In to a Cloud Account That Does Not Use Identity Domains

If your cloud account doesn't use identity domains, you sign in to the Oracle Cloud Infrastructure Console as a user federated through Oracle Identity Cloud Service.



This topic applies only to cloud accounts that don't use identity domains. See [Set Up Users](#).

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

myanalytics Change tenancy

Single Sign-On (SSO)

We have detected that your tenancy has been federated to another Identity Provider.

Select your Identity Provider below.

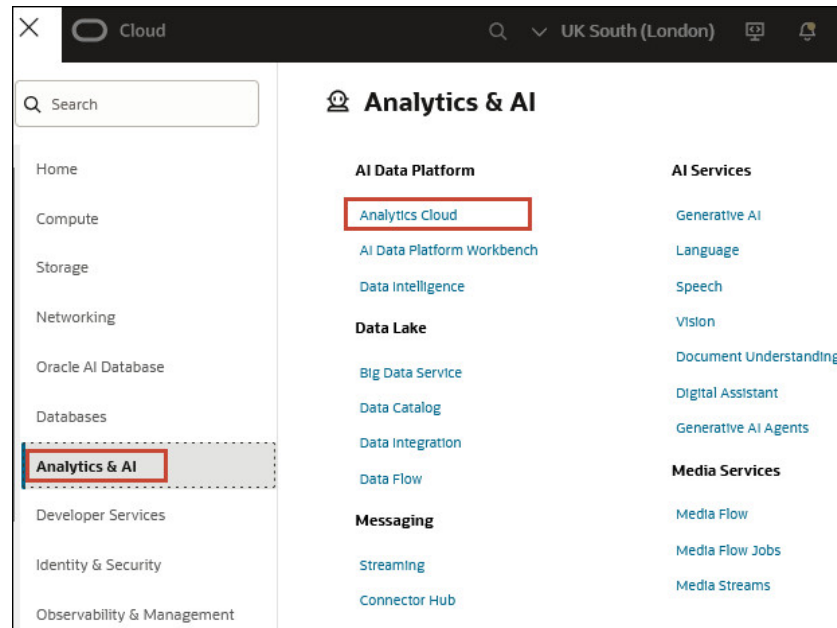
oracleidentitycloudservice


Continue

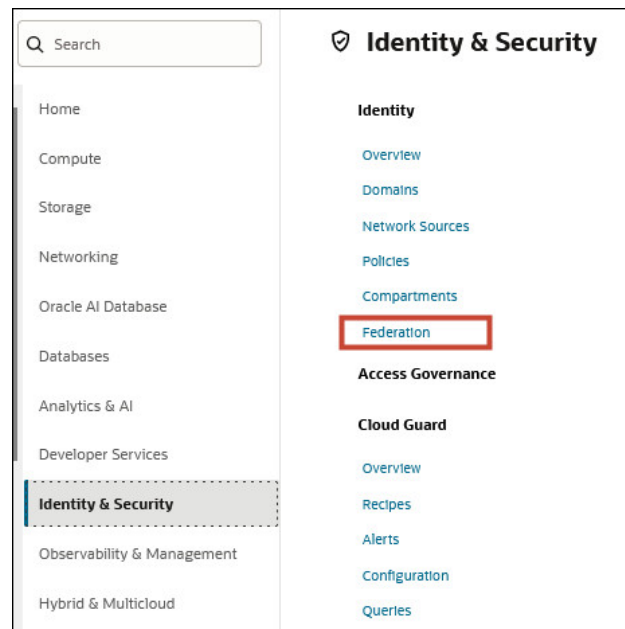
Oracle Cloud Infrastructure Direct Sign-In ⓘ


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

3. Enter the user name and password provided in the welcome email, and click **Sign In**.
The Oracle Cloud Infrastructure Console is displayed.
Take some time to explore categories and options in the navigation menu.
4. Navigate to the **Oracle Analytics Cloud** landing page where you access, create, and manage Oracle Analytics Cloud instances.
 - a. Open the navigation menu and click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.



- b. Click **pin**  to save the selection under the **Pinned** category on the Home page.
5. Navigate to the Oracle Identity Cloud Service Console to manage end users for Oracle Analytics Cloud.
 - a. Open the navigation menu and click **Identity & Security**.



- b. Under **Identity**, click **Federation**, select **oracleidentitycloudservice**, and then click the **Oracle Identity Cloud Service Console URL** to access the landing page for Oracle Identity Cloud Service.
- c. Click **pin**  to save the selection under the **Pinned** category on the Home page.

6. Navigate to the **Oracle Cloud Infrastructure Identity and Access Management (IAM)** landing page where you create and manage resources on Oracle Cloud Infrastructure (compartments, policies, users, groups, and more).
 - a. Open the navigation menu and click **Identity & Security**.
 - b. Under **Identity**, click **Users** and **Groups** to set up other users to manage resources on Oracle Cloud Infrastructure and map your groups in Oracle Identity Cloud Service to groups in IAM.
 - c. Click **Compartments** to set up compartments for the resources you want to create on Oracle Cloud Infrastructure.
 - d. Click **Policies** to set up security policies that allow users to manage resources on Oracle Cloud Infrastructure.

2

Set Up Users

You can set up user accounts for everyone you expect to use Oracle Analytics Cloud before or after you create your Oracle Analytics Cloud instances.

Topics

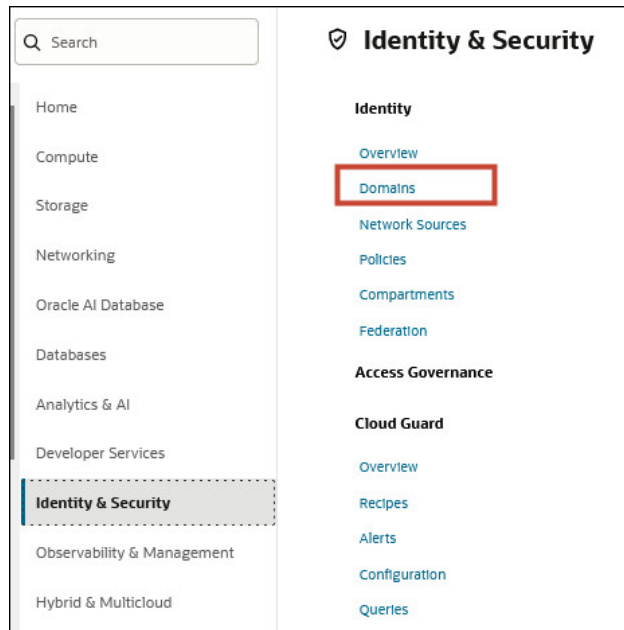
- [About Setting Up Users and Groups](#)
- [Use Identity Domains to Set Up Users and Groups for Oracle Analytics Cloud](#)
- [Use Oracle Identity Cloud Service to Set Up Users and Groups for Oracle Analytics Cloud](#)

About Setting Up Users and Groups

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

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

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



- If you see **Domains**, you use identity domains to manage users and groups for Oracle Cloud Infrastructure and your Oracle Analytics Cloud deployments. See [Use Identity Domains to Set Up Users and Groups for Oracle Analytics Cloud](#).
- If **Domains** isn't listed, you use a federated Oracle Identity Cloud Service to manage Oracle Analytics Cloud users and IAM to manage Oracle Cloud Infrastructure users. See [Use Oracle Identity Cloud Service to Set Up Users and Groups for Oracle Analytics Cloud](#).

The following table outlines the differences between the two configurations.

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

Use Identity Domains to Set Up Users and Groups for Oracle Analytics Cloud

If your Oracle Analytics Cloud instance uses *identity domains* for identity management, you use Oracle Cloud Infrastructure Console to set up and manage user accounts for everyone you expect to use Oracle Analytics Cloud. After setting up the users and groups, you use the

Console in Oracle Analytics Cloud to assign them suitable permissions (also known as *application roles*)

If you're not sure whether your Oracle Analytics Cloud instance uses identity domains, see [About Setting Up Users and Groups](#).

1. **Use the Identity Domain page in Oracle Cloud Infrastructure Console to add users and groups.**

See [Managing Users](#) and [Managing Groups](#) in *Oracle Cloud Infrastructure* documentation.

2. **Use Oracle Analytics Cloud to assign permissions to users and groups through application roles.**

See Manage What Users Can See and Do in *Configuring Oracle Analytics Cloud*.

Use Oracle Identity Cloud Service to Set Up Users and Groups for Oracle Analytics Cloud

If your Oracle Analytics Cloud instance uses Oracle Identity Cloud Service for identity management, you use the Console in Oracle Identity Cloud Service to set up and manage user accounts for everyone you expect to use Oracle Analytics Cloud. After setting up the users and groups, you use the Console in Oracle Analytics Cloud to assign them suitable permissions (also known as *application roles*).

If you're not sure whether your Oracle Analytics Cloud instance uses Oracle Identity Cloud Service, see [About Setting Up Users and Groups](#).

1. **Use Oracle Identity Cloud Service to add users and groups.**

See Manage Users and Groups in Oracle Identity Cloud Service in *Administering Oracle Identity Cloud Service*.

2. **Use Oracle Analytics Cloud to assign permissions to users and groups through application roles.**

See Manage What Users Can See and Do in *Configuring Oracle Analytics Cloud*.

3

Create Services with Oracle Analytics Cloud

As Cloud Account Administrator, you can create and set up services in Oracle Analytics Cloud for your organization.



Topics

- [Typical Workflow to Create a Service](#)
- [Before You Create a Service](#)
- [Create a Service](#)
- [After You Create a Service](#)

Typical Workflow to Create a Service

If you're about to create an Oracle Analytics Cloud instance on Oracle Cloud Infrastructure and you're using Oracle Cloud Infrastructure Console for the first time, follow these tasks as a guide.

Task	Description	More Information
Before you start		
Activate your order and sign in to your Oracle Cloud account	As the Cloud Account Administrator, you can complete all setup tasks for Oracle Analytics Cloud.	Request and Manage Free Oracle Cloud Promotions Upgrade to a Paid Account
Determine your service requirements	Plan your Oracle Analytics Cloud deployment. Think about what you need before you start.	Plan Your Service
(Optional) Enable other users to set up services	If you don't want to set up Oracle Analytics Cloud yourself, give other users permissions to create services.	Give Another User Permission to Set Up Oracle Analytics Cloud
(Recommended) Create a compartment for your service	Create a compartment for your Oracle Analytics Cloud deployment.	Create a Compartment
Create the service		
Create a service	Use Oracle Cloud Infrastructure Console to deploy a new service.	Create a Service
Verify your service	When your service is ready, check that you can sign in and your service is up and running.	Verify Your Service and Sign In
Complete the setup		
Set up users and groups	Set up users and groups for Oracle Analytics Cloud and assign them to application roles.	Set Up Users

Task	Description	More Information
Schedule regular backups of your data (snapshots)	As part of your business continuity plan, take a snapshot before people start using the system and again at suitable intervals so you can restore the environment if something goes wrong.	Schedule Regular Snapshots
Set service-level options	Configure service-level options for everyone using the service.	Configure Options for Your Service
Migrate content	Leverage your existing content in Oracle Analytics Cloud.	Migrate to Oracle Analytics Cloud from Other Environments

Before You Create a Service

Before you set up Oracle Analytics Cloud on Oracle Cloud Infrastructure using Oracle Cloud Infrastructure Console, Oracle recommends that you take some time to plan your service.

- [Plan Your Service](#)
- [Give Another User Permission to Set Up Oracle Analytics Cloud](#) (Optional)
- [Create a Compartment](#) (Recommended)

Plan Your Service

Take some time to plan your Oracle Analytics Cloud service before you create it. Think about the questions outlined here and decide what you want to do, before you start.

- [Which Edition Do You Need?](#)
- [Where Do You Want to Deploy Your Service?](#)
- [Which Identity Provider and Administrator Do You Want for Your Service?](#)
- [Do You Need a Public or Private Endpoint?](#)
- [What Sizing Options Are Available to You?](#)
- [What Name Do You Want for Your Service?](#)
- [Do You Want Early Access to Updates?](#)

Which Edition Do You Need?

When you set up a service you specify the edition you subscribe to and this determines which features are deployed.

Edition	Description
Professional Edition	Enables you to deploy an instance with data visualization.
Enterprise Edition	Enables you to deploy an instance with enterprise modeling, reporting, and data visualization.

For more information about the features available with each edition, see Editions: Enterprise and Professional .

Where Do You Want to Deploy Your Service?

Oracle Cloud Infrastructure (Gen 2) is hosted in several different geographic areas, called regions. When you sign up for Oracle Analytics Cloud, Oracle creates a tenancy for your company with access to one or more regions. If multiple regions are available to you, decide where you want to deploy your Oracle Analytics Cloud instance.

To find out more, see [Region Availability](#).

Note

The way you deploy and manage Oracle Analytics Cloud depends on the region, type, and start date of your subscription. If your Oracle Analytics Cloud subscription started before Oracle Analytics Cloud was available on Oracle Cloud Infrastructure (Gen 2), the deployment process is different. See:

- **North America:** See [Get Started with Oracle Analytics Cloud \(North America\) - Accounts Started Before 14th February 2020](#).
- **EMEA:** See [Get Started with Oracle Analytics Cloud \(EMEA\) - Accounts Started Before 2nd March 2020](#).

Which Identity Provider and Administrator Do You Want for Your Service?

If your tenancy supports identity domains, you can select which identity domain you want the service to use when you create an Oracle Analytics Cloud instance. You can also select an administrator for the service.

Note

If your tenancy doesn't support identity domains you can't customize the identity provider. Any Oracle Analytics Cloud instance that you create uses the Oracle Identity Cloud Service you're logged into.

By default, new Oracle Analytics Cloud instances use the identity domain you're logged into, with you as the administrator. If other identity domains are available in your tenancy and you have read access to them, you can select a different identity domain for your service. You can also specify a different user to be the administrator.

Note

Oracle recommends that you use an identity domain in the same region as your Oracle Analytics Cloud instance (or users that predominantly use it) to minimize latency and ensure seamless performance across services. Some regions automatically enforce this recommendation, specifically those regions that became available from May 2025 such as Batam.

You can't switch to a different identity domain after you've created the Oracle Analytics Cloud instance. So it's important to decide which identity domain your organization needs and ensure you have read permissions on that domain before you start. For example, ensure that you (or

whoever plans to create the Oracle Analytics Cloud instance) have the required IAM policy to read the identity domain through a policy statement similar to these samples:

- ```
#Let users in the MyOACAdminGroup read identity domains in the tenancy
allow group MyOACAdminGroup to read domains in tenancy
```
- ```
#Let users in the MyOACAdminGroup read identity domains in the compartment  
MyOracleAnalytics  
allow group MyOACAdminGroup to read domains in compartment MyOracleAnalytics
```

The identity domain you select is displayed on the **Details** tab for your Oracle Analytics Cloud. See [How can I find information about the identity provider my Oracle Analytics Cloud uses?](#)

Do You Need a Public or Private Endpoint?

When you create an Oracle Analytics Cloud instance, you specify how you want to access your service: through a *public internet accessible endpoint* or a *private endpoint*.

After you've created Oracle Analytics Cloud, you can't switch from a public endpoint to a private endpoint (or the other way around). So it's important to decide what type of access your organization needs and complete the required prerequisites before you start. See [Prerequisites for a Public Endpoint](#) and [Prerequisites for a Private Endpoint](#).

If you're not sure, see [About Public Endpoints and Access Control Rules](#) and [About Private Endpoints](#).

What Sizing Options Are Available to You?

When you create an Oracle Analytics Cloud instance for your production or non-production environment, you either specify the number of Oracle Compute Units (OCPU) you want to deploy or the number of people you expect to use the service.

- [How Many OCPUs Do You Think You'll Need?](#)
- [How Many People Do You Expect to Use the Service?](#)
- [What's the Difference Between Production and Non-Production Environments](#)

How Many OCPUs Do You Think You'll Need?

Oracle Analytics Cloud offers a range of compute sizes (OCPU) to suit different scenarios and environments. The larger the compute size, the greater the processing power. If you're not sure which size to use, contact your sales team to discuss sizing guidelines.

The compute size you select also determines some configuration limits for the different types of content that users can create:

- Data visualizations
- Classic analyses and dashboards
- Classic pixel-perfect reports

For example, limits such as the maximum number of input rows you can return from a data source query or the maximum number of rows you can download from a report to a file (for example, when you export to a CSV file).

- [Limits Querying Data \(Data Visualization Workbooks, Classic Analyses and Dashboards\)](#)
- [Limits Displaying Data \(Data Visualization Workbooks, Classic Analyses and Dashboards\)](#)
- [Limits Exporting Data \(Data Visualization Workbooks\)](#)

- [Limits Exporting Data \(Classic Analyses and Dashboards\)](#)
- [Limits Delivering by Email \(Classic Analyses and Dashboards\)](#)
- [Data Size Limits \(Classic Pixel-Perfect Reports\)](#)
- [Processing Limits \(Classic Pixel-Perfect Reports\)](#)

Limits Querying Data (Data Visualization Workbooks, Classic Analyses and Dashboards)

When you query a data source for visualizations or classic analyses and dashboards, the compute size determines the maximum number of rows that are returned from the data source.

Which compute size do you think you'll need?	Limits when querying data for visualizations, analyses, and dashboards	
	Max input rows returned from any data source query	Query timeout (seconds)
1 OCPU (non-production only)	125,000	660
2 OCPU	2,000,000	660
4 OCPU	2,000,000	660
6 OCPU	2,000,000	660
8 OCPU	2,000,000	660
10 OCPU	2,000,000	660
12 OCPU	2,000,000	660
16 OCPU	4,000,000	660
24 OCPU	4,000,000	660
36 OCPU	4,000,000	660
52 OCPU	4,000,000	660

Limits Displaying Data (Data Visualization Workbooks, Classic Analyses and Dashboards)

When you display data in visualizations or classic analyses and dashboards, the compute size determines the maximum number of summarized rows returned from the data source that are displayed.

Which compute size do you think you'll need?	Limits when displaying data in visualizations, analyses, and dashboards
	Max summarized rows returned from any data source query
1 OCPU (non-production only)	125,000
2 OCPU	500,000
4 OCPU	500,000
6 OCPU	500,000
8 OCPU	500,000
10 OCPU	500,000
12 OCPU	500,000

Which compute size do you think you'll need?	Limits when displaying data in visualizations, analyses, and dashboards
	Max summarized rows returned from any data source query
16 OCPU	1,000,000
24 OCPU	1,000,000
36 OCPU	1,000,000
52 OCPU	1,000,000

Limits Exporting Data (Data Visualization Workbooks)

When you export data from a data visualization workbook, the compute size determines the maximum number of rows you can export, number of parallel exports, and queue size for incoming export requests. If you regularly exceed export limits, you can scale up to a larger compute size or reduce the number of parallel export requests.

There are different row limits for formatted and unformatted data.

- **Unformatted data limit:** Comma Separated Values (CSV)
- **Formatted data limit:** Microsoft Excel (XLSX)

*The maximum row limits shown in the table are based on exports that contain up to 40 columns. Additional columns will impact the maximum number of rows you can export.

Note

Data exports are expensive operations and have a direct impact on the overall system performance. The impact on system performance increases with the number of rows and columns that you export. Oracle recommends that you export large amounts of data during non-peak hours to reduce any performance impact.

Which compute size do you think you'll need?	Limits when exporting data from data visualization workbooks	
	Maximum number of rows exported to CSV*	Maximum number of rows exported to Microsoft Excel (XLSX)*
1 OCPU (non-production only)	125,000	25,000
2 OCPU	2,000,000	50,000
4 OCPU	2,000,000	50,000
6 OCPU	2,000,000	50,000
8 OCPU	2,000,000	50,000
10 OCPU	2,000,000	50,000
12 OCPU	2,000,000	100,000
16 OCPU	4,000,000	100,000
24 OCPU	4,000,000	100,000
36 OCPU	4,000,000	100,000
52 OCPU	4,000,000	100,000

Limits Exporting Data (Classic Analyses and Dashboards)

When you export data from analyses and dashboards, the compute size determines the maximum number of rows you can export, number of parallel exports, and queue size for incoming export requests. If you regularly exceed export limits, you can scale up to a larger compute size or reduce the number of parallel export requests.

There are different limits for formatted reports and unformatted reports.

- **Unformatted report limits:** formats such as CSV, Excel, XML, and Tab Delimited.
- **Formatted report limits:** formats such as PDF, Excel, Powerpoint, and Web Archive/HTML.

When two pivot views are laid out side by side in a union the *formatted* export limit will be 20,000 rows.

*The maximum row limits shown in the table are based on exports that contain up to 40 columns. Additional columns will impact the maximum number of rows you can export.

Note

Data exports are expensive operations and have a direct impact on the overall system performance. The impact on system performance increases with the number of rows and columns that you export and the output format. Oracle recommends that you export large amounts of data during non-peak hours or export unformatted data to reduce any performance impact.

Which compute size do you think you'll need?	Limits when exporting data from analyses and dashboards	
	Maximum number of rows exported to unformatted reports*	Maximum number of rows exported to formatted reports*
1 OCPU (non-production only)	125,000	1,000
2 OCPU	2,000,000	200,000
4 OCPU	2,000,000	200,000
6 OCPU	2,000,000	200,000
8 OCPU	2,000,000	200,000
10 OCPU	2,000,000	200,000
12 OCPU	2,000,000	200,000
16 OCPU	4,000,000	400,000
24 OCPU	4,000,000	400,000
36 OCPU	4,000,000	400,000
52 OCPU	4,000,000	400,000

Limits Delivering by Email (Classic Analyses and Dashboards)

When you send analyses and dashboards by email, the compute size determines the maximum number of rows you can deliver in a single email. There are different limits for delivering formatted reports and unformatted reports.

- **Unformatted report limits:** formats such as CSV, XML, and Tab Delimited.

- **Formatted report limits:** formats such as PDF, Excel, Powerpoint, and Web Archive/HTML.

Note

Content delivery by email is an expensive operation and has a direct impact on the overall system performance. The impact on system performance increases with the number of recipients, the number of rows and columns that you send, and the delivery format. Oracle recommends that you schedule deliveries during non-peak hours or change the delivery format to reduce any performance impact.

Which compute size do you think you'll need?	Limits when delivering analyses and dashboards by email	
	Max rows in unformatted reports delivered by email	Max rows in formatted reports delivered by email
1 OCPU (non-production only)	2,000	1,000
2 OCPU	200,000	50,000
4 OCPU	200,000	50,000
6 OCPU	200,000	50,000
8 OCPU	200,000	50,000
10 OCPU	200,000	50,000
12 OCPU	200,000	50,000
16 OCPU	300,000	100,000
24 OCPU	300,000	100,000
36 OCPU	300,000	100,000
52 OCPU	300,000	100,000

Data Size Limits (Classic Pixel-Perfect Reports)

The compute size determines several limits associated with generating reports.

Which compute size do you think you'll need?	Report data size limits when generating pixel-perfect reports			
	Max data size for online reports	Max data size for offline (scheduled) reports	Max data size for bursting reports	Max data size for data generation
1 OCPU (non-production only)	200MB	500MB	2GB	500MB
2 OCPU	500MB	2GB	4GB	2GB
4 OCPU	500MB	2GB	4GB	2GB
6 OCPU	500MB	2GB	4GB	2GB
8 OCPU	500MB	2GB	4GB	2GB
10 OCPU	500MB	2GB	4GB	2GB
12 OCPU	500MB	2GB	4GB	2GB
16 OCPU	800MB	4GB	8GB	4GB
24 OCPU	800MB	4GB	8GB	4GB

Which compute size do you think you'll need?	Report data size limits when generating pixel-perfect reports			
	Max data size for online reports	Max data size for offline (scheduled) reports	Max data size for bursting reports	Max data size for data generation
36 OCPU	800MB	4GB	8GB	4GB
52 OCPU	800MB	4GB	8GB	4GB

Processing Limits (Classic Pixel-Perfect Reports)

The compute size determines several limits associated with processing reports.

Which compute size do you think you'll need?	Data model and report processing limits when generating pixel-perfect reports				
	SQL Query timeout for scheduled reports (seconds)	Max rows for CSV output	Max number of in-memory rows in XPT layout	Max number of concurrent scheduled jobs	Max number of concurrent online reports
1 OCPU (non-production only)	1,800	1,000,000	100,000	1	2
2 OCPU	1,800	4,000,000	200,000	4	16
4 OCPU	1,800	4,000,000	200,000	4	32
6 OCPU	1,800	4,000,000	200,000	4	48
8 OCPU	1,800	4,000,000	200,000	4	64
10 OCPU	1,800	4,000,000	200,000	4	80
12 OCPU	1,800	4,000,000	200,000	4	96
16 OCPU	3,600	6,000,000	300,000	10	320
24 OCPU	3,600	6,000,000	300,000	10	480
36 OCPU	3,600	6,000,000	300,000	10	720
52 OCPU	3,600	6,000,000	300,000	10	1040

How Many People Do You Expect to Use the Service?

With Oracle Analytics Cloud, you can opt to specify how many people you expect to use the service. Typically, services have between 10 and 3000 users. Configuration limits for user-based subscriptions are equivalent to those shown here.

Configuration Limits for User-based Subscriptions: Data Visualization Workbooks, Classic Analyses and Dashboards

Limit Description	Limit Value
Limits when querying data for visualizations, analyses, and dashboards	
Max input rows returned from any data source query	2,000,000 rows
Query timeout (seconds)	660 seconds
Limits when displaying data in visualizations, analyses, and dashboards	
Max summarized rows returned from any data source query	500,000 rows

Limit Description	Limit Value
Limits when exporting data from data visualization workbooks	
Maximum number of rows exported to CSV	2,000,000 rows
Maximum number of rows exported to Microsoft Excel (XLSX)	25,000 rows
Limits when exporting data from analyses and dashboards	
Max rows exported to unformatted reports	2,000,000 rows
Max rows exported to formatted reports	200,000 rows
Limits when delivering analyses and dashboards by email	
Max rows in unformatted reports delivered by email	200,000 rows
Max rows in formatted reports delivered by email	50,000 rows

Configuration Limits for User-based Subscriptions: Classic Pixel-Perfect Reports

Limit Description	Limit Value
Report data size limits when generating pixel-perfect reports	
Max data size for online reports	500MB
Max data size for offline (scheduled) reports	2GB
Max data size for bursting reports	4GB
Max data size for data generation	2GB
Data model and report processing limits when generating pixel-perfect reports	
SQL Query timeout for scheduled reports (seconds)	1,800 seconds
Max rows for CSV output	4,000,000 rows
Max number of in-memory rows in XPT layout	200,000 rows
Max number of concurrent scheduled jobs	4 jobs
Max number of concurrent online reports	32 reports

What's the Difference Between Production and Non-Production Environments

- Non-production environment:** Oracle enables you to deploy a non-production environment with 1 OCPU. A non-production environment is specifically sized and designed for test, development and training purposes. Non-production services aren't intended for daily use, multiple concurrent users, or complex business scenarios.

If you decide you want to keep the content that you create during testing, you can save it to a snapshot and copy it to a production service (minimum 2 OCPU or 10 users). See [Migrate Oracle Analytics Cloud Using Snapshots](#). Alternatively, you can scale up your 1 OCPU environment to between 2 and 8 OCPUs.
- Production environment:** A production environment is designed for daily commercial use. You can scale some production environments up and down. For example, you can scale between 2 and 8 OCPUs and 10 and 12 OCPUs. You can also scale between various user ranges such as 10 - 400 users and 401 - 601 users. See [About Scaling](#).

What Name Do You Want for Your Service?

Think about a suitable name for your service. The name that you specify is displayed in Oracle Cloud Infrastructure Console and the URL for your service.

Name restrictions:

- Must contain between 1 and 25 characters.

- Must start with an ASCII letter: a to z or A to Z.
- Must contain only ASCII letters or numbers.
- Mustn't contain any other special characters.
- Must be unique within the identity domain.

Do You Want Early Access to Updates?

When you set up a new service you can opt to receive product updates early or on the regular schedule.

Oracle delivers innovative product updates on a regular basis, with zero customer downtime. If early access to new features is important to you, you can opt to receive updates immediately when they become available. If you manage multiple Oracle Analytics Cloud environments, early access gives you the flexibility to explore new features and stagger updates between environments.

After creating your Oracle Analytics Cloud environment and opting for either the regular or early update cycle, your selection is locked. You can't switch from the early rollout cycle to the regular rollout cycle (or the other way around). So, it's important to consider whether early updates are suitable for your environment from the start. If your needs change, you must create a new service instance with the desired update schedule and migrate your content to the new service.

Update Cycle	Description
Early	Oracle delivers updates as soon as they're available. If you manage multiple Oracle Analytics Cloud environments, early access gives you the flexibility to explore new features and stagger updates between environments.
Regular	(Default) Oracle delivers updates a few weeks after completing the early update cycle. If you manage multiple Oracle Analytics Cloud environments on the regular update cycle, Oracle will share the <i>actual date</i> of software updates for each environment in your software update notification.

Note

Update cycle options are available in commercial, US government, US defense, UK government, and EU sovereign realms.

Oracle sends notifications to communicate actual dates for software updates for each Oracle Analytics Cloud environment that you manage. See [Does Oracle send notifications for all service updates?](#)

The update cycle you select takes effect from January 2025 onwards.

Give Another User Permission to Set Up Oracle Analytics Cloud

When you activate your order for Oracle Analytics Cloud, you get the Cloud Account Administrator role. This role gives you *full* administration privileges in Oracle Cloud Infrastructure so you can complete all aspects of Oracle Analytics Cloud setup and much more. There's no need to delegate this responsibility but, if you want to, you can give someone

else privileges to create and manage Oracle Analytics Cloud instances through the `manage analytics-instances` permission.

In Oracle Cloud Infrastructure you use IAM security policies to grant permissions. First, you must add the user to a group, and then you create a security policy that grants the group the `manage analytics-instances` permission on a specific compartment or the tenancy (any compartment in the tenancy). For example, you might create a policy statement that looks like one of these:

- `allow group MyAdminGroup to manage analytics-instances in tenancy`
- `allow group MyAdminGroup to manage analytics-instances in compartment MyOracleAnalytics`

To find out how to create security policy statements specifically for Oracle Analytics Cloud, see [Give Users Permissions to Manage Analytics Cloud Instances](#).

Create a Compartment

When you sign up for Oracle Cloud Infrastructure, Oracle creates your tenancy with a root compartment that holds all your cloud resources. You then create additional compartments within the tenancy (root compartment) and corresponding policies to control access to the resources in each compartment. Before you create an Oracle Analytics Cloud instance, Oracle recommends that you set up the compartment where you want the instance to belong.

You create compartments in Oracle Cloud Infrastructure Identity and Access Management (IAM). See [Setting Up Your Tenancy](#) and [Managing Compartments](#).

Create a Service

You can create an Oracle Analytics Cloud instance using the Console, API, or command line.

Note

Required IAM Policy

Verb: manage

Resource Type: analytics-instance, analytics-instances

Custom Permission: ANALYTICS_INSTANCE_CREATE

See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

Additional IAM Policy Required to Select an Alternative Identity Domain

Verb: read

Resource Type: domains

Additional IAM Policy Required to Create a Public Endpoint

Verb: read

Resource Type: virtual-network-family, compartment, compartments

See [Prerequisites for a Public Endpoint](#).

Additional IAM Policy Required to Create a Private Endpoint

Verb: manage

Resource Type: virtual-network-family

Verb: read

Resource Type: compartment, compartments

Required only for network security groups:

Verb: use

Resource Type: network-security-groups

To learn about other, more detailed access policy options, see [Prerequisites for a Private Endpoint](#).

Topics

- [Create a Service using the Console](#)
- [Create a Service using the REST API](#)
- [Create a Service using the Command Line](#)


Create a Service using the Console

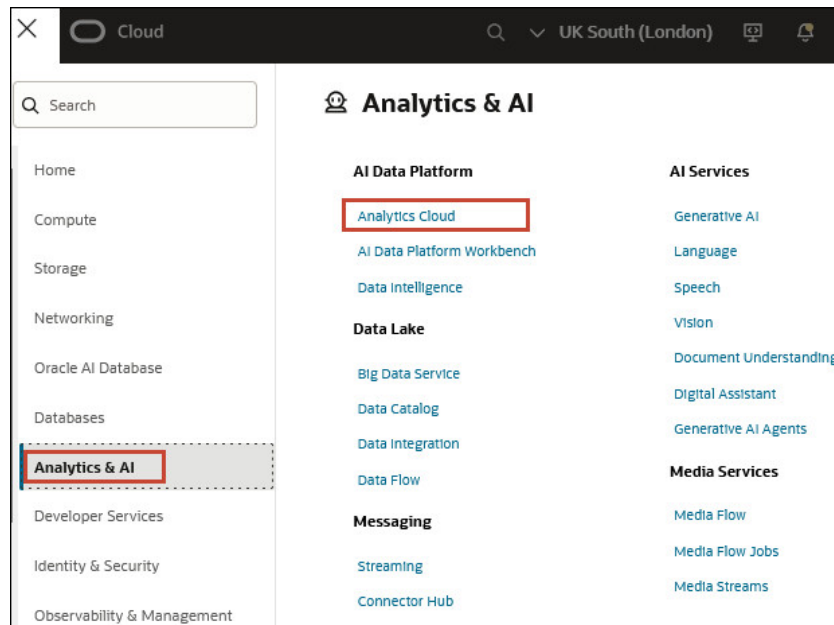
You can use Oracle Cloud Infrastructure Console to set up a service instance with Oracle Analytics Cloud.

You must belong to an OCI group that is granted the required policies to create an Analytics instance. See [Give Users Permissions to Manage Analytics Cloud Instances](#).

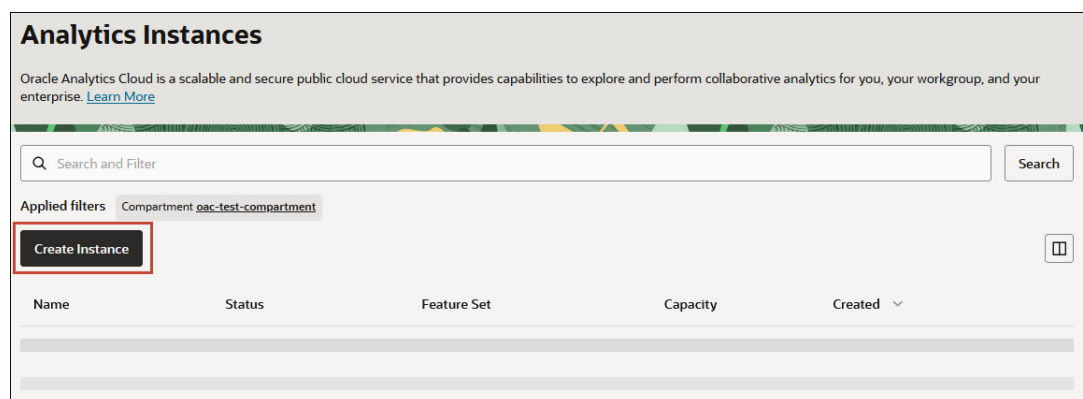
1. Sign in to your Oracle Cloud account.

The way you sign in depends whether your cloud account uses identity domains or federates with Oracle Identity Cloud Service. See [Signing In to the Oracle Cloud Infrastructure Console](#).

2. In Console, click  in the top left corner.
3. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.



4. From the **Compartment** list, select the compartment in which you want to create the service.
5. Click **Create Instance**.



6. In the **Create Analytics Instance** pane, enter a name and brief description to identify your instance.

Name must start with a letter and can contain only letters and numbers.

Create Analytics Instance

Name
myanalytics
Must be unique, start with a letter and contain only alphanumeric characters.

Description
Enterprise analytics for MyCompany in London

Create in Compartment
oac-test-compartment

Feature Set

Edition

Enterprise Edition
Deploy an instance with enterprise modeling, reporting, and data visualization. [Learn More](#)

Professional Edition
Deploy an instance with data visualization. [Learn More](#)

Capacity

Capacity Type

OCPU
Number of OCPUs you want to deploy for your service.

Users
Number of users expected to use this service.

OCPU Count
4

7. Select the **Edition** that matches your subscription.
- **Enterprise Edition:** Deploys an instance with enterprise modeling, reporting, and data visualization.
 - **Professional Edition:** Deploys an instance with data visualization.
8. For **Capacity**, select the size of your deployment.

Configure the capacity type that matches your subscription, that is, either *OCPUs per hour* or *Users per month*.

- **OCPU:** Select the number of OCPUs you want to deploy.
 - **Production environment:** Select between 2 and 52 OCPUs.
 - **Non-Production environment:** Select 1 OCPU if you want to create an instance for test purposes.

See [What's the Difference Between Production and Non-Production Environments](#).

You must select the **OCPU** option if you plan to use your Oracle Middleware on-premise license with Oracle Analytics Cloud (BYOL).

- **Users:** Enter the number of users you expect to use this service.

You can split your capacity over multiple services. For example, if you subscribe to 100 users per month, you might deploy a test instance for 10 users and a production instance with the remaining 90 users.

- For **License**, select **License Included** to subscribe to an Oracle Cloud license for Oracle Analytics Cloud or **Bring Your Own License (BYOL)** to use your Oracle Middleware on-premise license with Oracle Analytics Cloud and be charged the Bring Your Own License (BYOL) rate.

The **Bring Your Own License (BYOL)** option is available when you select **OCPU** for Capacity.

If you select **Users**, you must have an Oracle Cloud license for Oracle Analytics Cloud.

The screenshot shows a configuration interface with two main sections: **Licensing** and **Software Updates**.

Licensing section:

- License**
 - License Included**: Subscribe to a new Analytics Cloud software license and the Analytics Cloud service.
 - Bring Your Own License (BYOL)**: Bring my organization's middleware software license to the Analytics Cloud service. [Learn More](#)

Software Updates section:

Select the timing of Oracle Analytics Cloud instance updates within the rollout window. Two cycles, separated by a few weeks, provide flexibility for customers with multiple instances to stagger updates between environments. The selection is permanent and you can't change to a different update cycle later.

Update Cycle

- Early**: First rollout cycle, be the first to explore new features and stagger updates between your environments.
- Regular**: Second rollout cycle, scheduled a few weeks after the first rollout.

- For **Update Cycle**, select **Early** to receive updates early or keep the default (**Regular**).

The selection you make is permanent. You can't switch from the regular update cycle to the early cycle later on (or the other way around). So, it's important to consider whether early updates are suitable for your environment from the start. See [Do You Want Early Access to Updates?](#)

Note

The **Update Cycle** option is available only in commercial, US government, US defense, UK government, and EU sovereign realms.

- Optional: Click **Show Advanced Options** to configure identity management, network access, or data encryption options.

The screenshot displays three configuration sections in the Oracle Cloud console:

- Identity Management:** Contains three dropdown menus. The first is 'Domain compartment' with the value 'oac-test-compartment'. The second is 'Identity Domain' with the value 'OracleIdentityCloudProvider'. The third is 'Admin User' with the value 'oacserviceadmin'.
- Network Access:** Shows 'Access Type' with two options: 'Public' (Access your instance from anywhere) and 'Private' (Access your instance from a Virtual Cloud Network only). Below this is a 'Configure Access Control' toggle switch, which is currently turned off.
- Data Encryption:** Shows 'Data Encryption' with two options: 'Encrypt using Oracle-managed Keys' (Leave all encryption to Oracle.) and 'Encrypt using Customer-managed Keys' (Requires a valid key from a vault that you have access to. [Learn More](#)).

12. Optional: In **Identity Management**, select a different identity domain or administrator for Oracle Analytics Cloud or keep the default.
- **Domain Compartment:** If the identity domain you want to use isn't in the same compartment as Oracle Analytics Cloud, select the appropriate compartment.
 - **Identity Domain:** Select the identity domain you want Oracle Analytics Cloud to use. You must have read permissions for domains in the selected compartment. See [Which Identity Provider and Administrator Do You Want for Your Service?](#)
 - **Admin User:** Select a user from the selected identity domain to be the administrator for Oracle Analytics Cloud.

If identity domains aren't available in your tenancy, the **Identity Management** section doesn't display.

13. In **Network Access**, configure how you want users to access Oracle Analytics Cloud: over the public internet or through a private network.
- **Public:** Enable access over the public internet.
The Public option deploys Oracle Analytics Cloud with a public internet accessible endpoint. If required, you can configure access control rules to restrict access by public IP address, public CIDR block range, VCN, and Oracle services. See [Restrict Access to Oracle Analytics Cloud Deployed with a Public Endpoint](#).
 - **Private:** Enable private access from an on-premise network or hosts on a virtual cloud network (VCN). Private access means that traffic doesn't go over the internet.

The Private option deploys Oracle Analytics Cloud with a private endpoint. Before you configure this option, you must set up the Oracle Cloud Infrastructure VCN that you plan to use with a subnet for Oracle Analytics Cloud. If required, you can restrict access to private endpoints through network security groups. If your network security groups aren't set up yet, you can save this task for later. See [Deploy Oracle Analytics Cloud with a Private Endpoint](#).

You can configure access control rules for a public endpoint or change the VCN, subnet, and network security group access for a private endpoint, later on as required. However, you *can't change* your network access selection from public to private (or private to public).

14. Optional: In **Data Encryption**, customize how Oracle Analytics Cloud encrypts customer data.

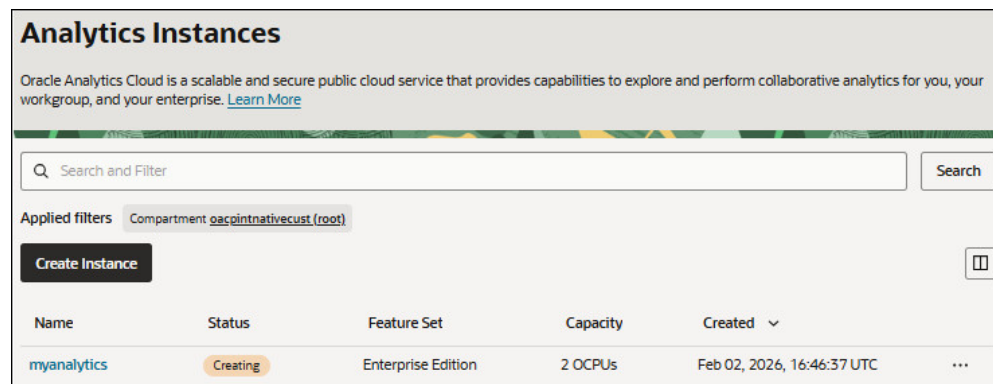
- **Encrypt using Oracle-managed Keys:** Leave all data encryption to Oracle.
- **Encrypt using Customer-managed Keys:** Specify the custom encryption key you want to use.

You can configure data encryption now or later. If you haven't created a master encryption key yet, leave this task for later. See [Encrypt Sensitive Information](#).

Your Oracle Analytics Cloud instance must be deployed with **Enterprise Edition**. Custom encryption isn't available on Oracle Analytics Cloud instances deployed with **Professional Edition**.

15. Verify that the details are correct, and click **Create**.

It takes about 20 minutes to create the service. Display the Instance page to check the current status.



Analytics Instances

Oracle Analytics Cloud is a scalable and secure public cloud service that provides capabilities to explore and perform collaborative analytics for you, your workgroup, and your enterprise. [Learn More](#)

Search and Filter Search

Applied filters: [Compartment oacpintnativecust \(root\)](#)

Create Instance

Name	Status	Feature Set	Capacity	Created	
myanalytics	Creating	Enterprise Edition	2 OCPUs	Feb 02, 2026, 16:46:37 UTC	...

Create a Service using the REST API

You can use the `CreateAnalyticsInstance` operation to set up a service instance with Oracle Analytics Cloud.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use this operation:

- [CreateAnalyticsInstance](#)

Note

(Oracle Identity Cloud Service only) If *identity domains* aren't available in your cloud account, you use Oracle Identity Cloud Service for identity management. To use the REST API with Oracle Identity Cloud Service, you must generate an access token and specify the token value in the parameter `idcsAccessToken`. See [Generate IDCS Access Tokens for the REST API and CLI](#).

Create a Service using the Command Line

You can use the `analytics-instance create` command to set up a service instance with Oracle Analytics Cloud.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- [analytics-instance create](#)

Note

(Oracle Identity Cloud Service only) If *identity domains* aren't available in your cloud account, you use Oracle Identity Cloud Service for identity management. To use the CLI with Oracle Identity Cloud Service, you must generate an access token, copy the token value to a file, and specify the name of the file in the CLI parameter `--idcs-access-token-file [filename]`. See [Generate IDCS Access Tokens for the REST API and CLI](#).

Generate IDCS Access Tokens for the REST API and CLI

(Oracle Identity Cloud Service only) If *identity domains* aren't available in your cloud account, you use Oracle Identity Cloud Service for identity management. In this case, you need an *access token* to create an Oracle Analytics Cloud instance using the command line interface (CLI) or REST API.

This section describes how to set up a confidential application to generate the required access tokens, and how to specify the tokens in CLI and REST API payloads.

Note

The instructions are different for *identity domains* and *Oracle Identity Cloud Service*. Follow the correct instructions for your tenancy. If you're not sure, see [How can I find information about the identity provider my Oracle Analytics Cloud uses?](#)

For tenancies offering Oracle Identity Cloud Service:

- [Create a Confidential Application to Generate Access Tokens \(IDCS\)](#)
- [Generate and Use Access Tokens in REST API and CLI Payloads \(IDCS\)](#)

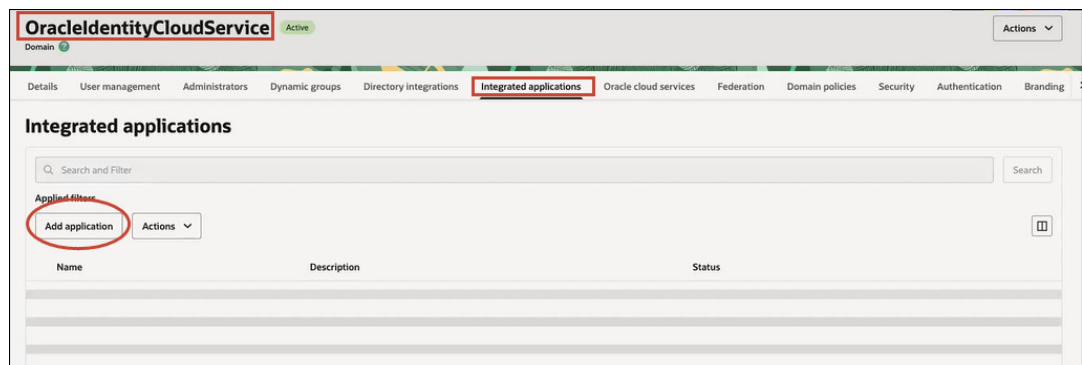
Create a Confidential Application to Generate Access Tokens (Identity Domains)

Create a confidential application that enables you to generate the access token required to create an Analytics instance using CLI or REST API.

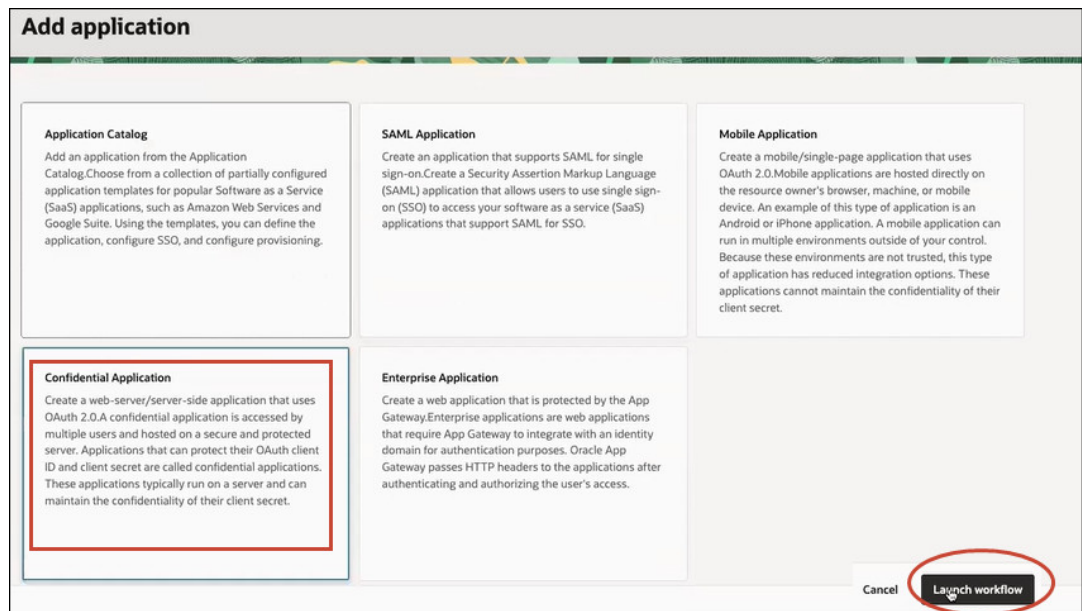
Note

These instructions are for tenancies that use *identity domains*. If your tenancy uses Oracle Identity Cloud Service (IDCS), see [Create a Confidential Application to Generate Access Tokens \(IDCS\)](#).

1. Sign in to your Oracle Cloud account as an administrator.
2. In Oracle Cloud Infrastructure Console, navigate to **Identity & Security**, and click **Domains**.
3. Click the name of the identity domain where you plan to create an Analytics instance, and click **Integrated applications**.

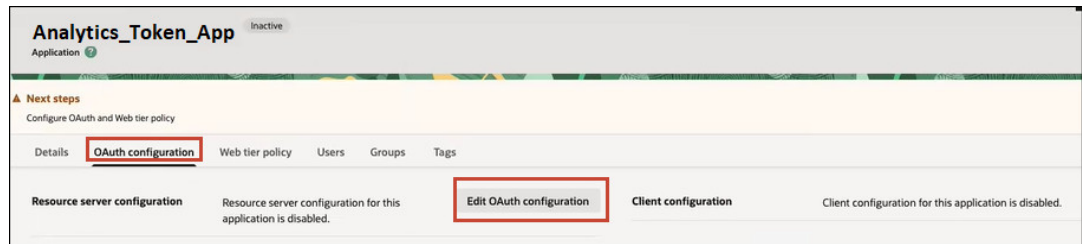


4. Click **Add application**, select **Confidential Application**, and then click **Launch workflow**.

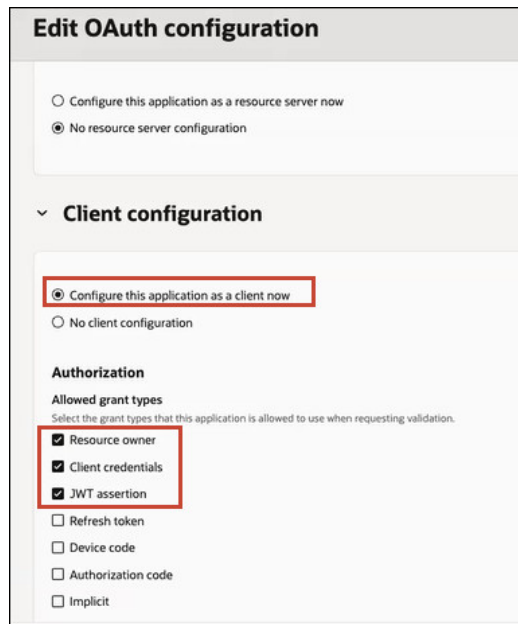


5. Enter a name for the application (for example, `Analytics_Token_App`), and click **Submit**.

- Click the **OAuth configuration** tab for the application, and then click **Edit OAuth configuration**.



- In the **Client Configuration** section, select **Configure this application as a client now**.
- Under **Authorization**, select the allowed grant types: **Resource owner**, **Client credentials**, and **JWT assertion**.



- Under the **Token issuance policy** section, select **Add app roles**, and click **Add roles**

Edit OAuth configuration

Token issuance policy

Authorized resources
Choose which authorized resources a client application can access. Select 'All' to access any resource within a domain. Select 'Specific' to access only those resources where an explicit association between the client and the resource exists.

All

Specific

Add resources

Add resources if you want your application to access the APIs of other applications.

Add app roles

Add the application roles to assign to this application. For example, add the Identity Domain Administrator role so that all REST API tasks available to the identity domain administrator will be available to the application.

App roles

Search and Filter

App roles	Protected
No items to display	

Create new items or search again using different filters or search terms.

10. Select **Me**.

Add app roles

Search and Filter

Name
<input type="checkbox"/> Reset Password
<input type="checkbox"/> Self Registration
<input type="checkbox"/> Forgot Password
<input type="checkbox"/> Verify Email
<input checked="" type="checkbox"/> Me
<input type="checkbox"/> Cloud Gate
<input type="checkbox"/> Kerberos Administrator
<input type="checkbox"/> DB Administrator
<input type="checkbox"/> MFA Client
<input type="checkbox"/> Authenticator Client

11. Click **Add**, then **Submit**.

12. On the application page, click the **Actions** menu, select **Activate**, then **Activate Application**.

Now you can use the confidential application to generate access tokens that you can include in REST API and CLI payloads. See [Generate and Use Access Tokens in REST API and CLI Payloads \(Identity Domains\)](#).

Generate and Use Access Tokens in REST API and CLI Payloads (Identity Domains)

If you want to create an Oracle Analytics Cloud instance programmatically, you must generate an access token that you can include in the payload for REST API or CLI create operations. Access tokens are set to expire after a certain time period so you might need to repeat this

task for subsequent create operations. By default, access tokens are valid for one hour (3600 seconds).

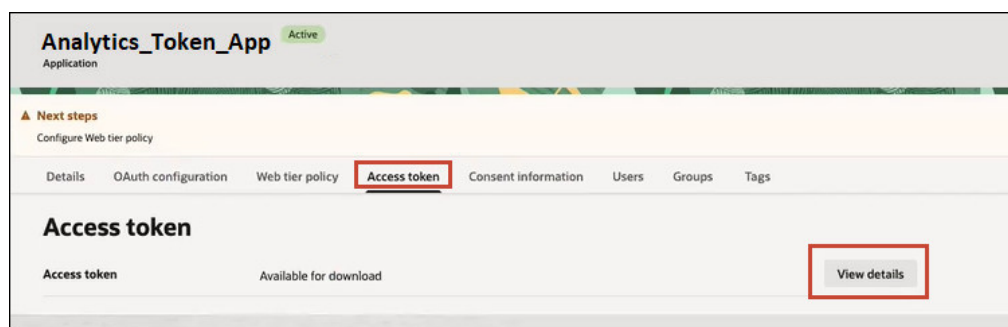
Note

These instructions are for tenancies that use *identity domains*. If your tenancy uses Oracle Identity Cloud Service (IDCS), see [Generate and Use Access Tokens in REST API and CLI Payloads \(IDCS\)](#).

You can generate access tokens using the Console or programmatically (using CLI or an API).

To generate access tokens from the Console:

1. Sign in to your Oracle Cloud account as an administrator.
2. In Oracle Cloud Infrastructure Console, navigate to **Identity & Security**, and click **Domains**.
3. Click the name of the identity domain where you plan to create an Analytics instance, and click **Integrated applications**.
4. Navigate to the application that you previously created to generate tokens. For example, `Analytics_Token_App`.
5. Click the **Access Token** tab, then click **View Details**.



6. Select **Customized cscopes**.
7. Select **Invokes identity domain APIs**, and specify **Me**.
8. Click **Download token** and save the `tokens.tok` file.
`tokens.tok` contains the access token with the attribute name **app_access_token**.
9. Open `tokens.tok`.
For example:

```

{"app_access_token": "eyJ4NXQjUzI...0jxcCw5oR0ajaNw"}

```
10. Copy the access token value *between* the quotes. For example, the value `eyJ4NXQjUzI...0jxcCw5oR0ajaNw`.
11. To create an Oracle Analytics Cloud instance with this access token, do one of the following:
 - REST API [CreateAnalyticsInstance](#): Specify the token value in the parameter `idcsAccessToken`.

- CLI [analytics-instance create](#): Copy the token value to a file and specify the name of the file in the CLI parameter `--idcs-access-token-file [filename]`.

To generate access tokens using an API or CLI:

1. Generate the access token using an API or from the CLI. For example:

```
curl
-X POST
-u "<client_id>:<client_secret>"
-H 'content-type: application/x-www-form-urlencoded;charset=UTF-8'
-d "grant_type=password"
-d "username=<user>"
-d "password=<password>"
-d 'scope=urn:opc:idm:t.user.me'
"https://<stripe>.identity.oraclecloud.com:443/oauth2/v1/token"
```

Note

Navigate to your domain's information page to obtain the `stripe` associated with your domain. Click **Show** next to the **Domain URL** property to discover the `stripe` value.

The command returns a JSON response similar to this:

```
{"access_token": "eyJ4NXQjUzI...0jxcCw5oR0ajaNw", "token_type": "Bearer", "expires_in": 3600}
```

2. Copy the access token from the JSON. For example, `eyJ4NXQjUzI...0jxcCw5oR0ajaNw`.
3. To create an Oracle Analytics Cloud instance with this access token, do one of the following:
 - REST API [CreateAnalyticsInstance](#): Specify the token value in the parameter `idcsAccessToken`.
 - CLI [analytics-instance create](#): Copy the token value to a file and specify the name of the file in the CLI parameter `--idcs-access-token-file [filename]`.

Create a Confidential Application to Generate Access Tokens (IDCS)

(Oracle Identity Cloud Service only) Create a confidential application that enables you to generate the access token required to create an Analytics instance using CLI or REST API.

Note

These instructions are for tenancies that use *Oracle Identity Cloud Service* (IDCS). If your tenancy uses *identity domains* you don't need to generate an access token to use the CLI or REST API.

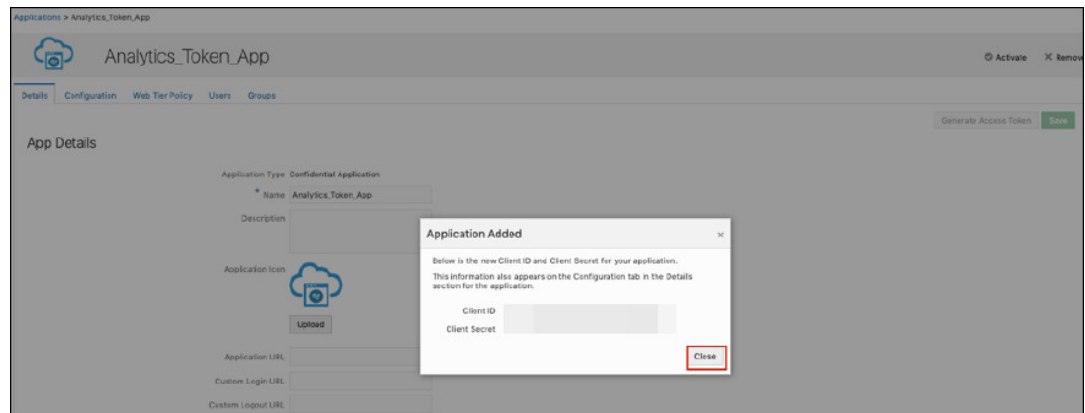
1. Sign in to your Oracle Cloud account as an administrator.

2. In Oracle Cloud Infrastructure Console, navigate to **Identity & Security**, click **Federation**, select **OracleIdentityCloudService**, and then click the **Oracle Identity Cloud Service Console URL**.
3. Navigate to the **Applications** tab, and click **Add**.
4. Select **Confidential Application**.
5. Enter a name for the application (for example, `Analytics_Token_App`), and click **Next**.

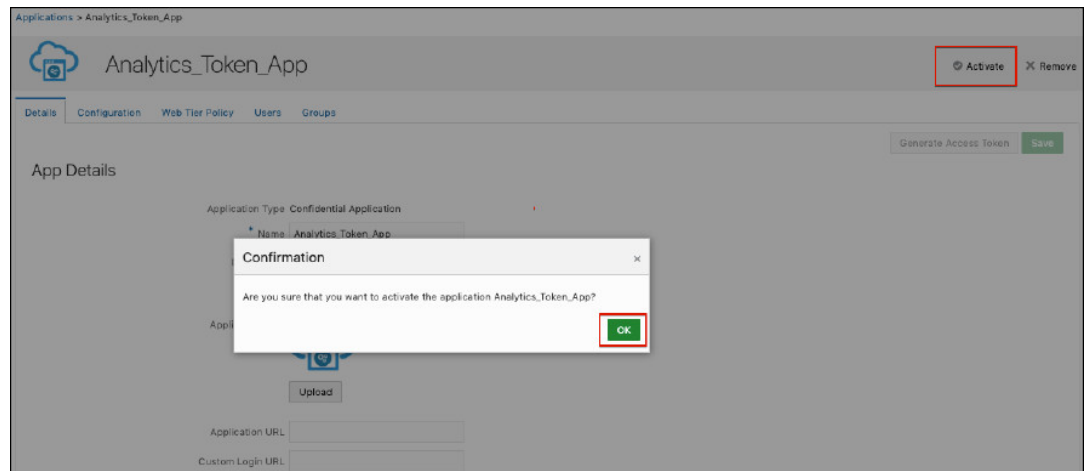
6. Select **Configure this application as a client now** and provide the following **Allowed Grant Types** for client authorization:
 - **Resource Owner**
 - **Client Credentials**
 - **JWT Assertion**
7. Under **Grant the client access to Identity Cloud Service Admin APIs**, click **Add**.
8. Select **Me**, then click **Add**.

9. Click **Next** to go to the Resources tab.
10. Click **Next** to go to the Web Tier Policy tab.
11. Click **Next** to go to navigate to the Authorization tab.

12. Click **Finish**.
13. Copy and save the **Client ID** and **Client Secret**.



14. Click **Activate**, then click to confirm that you want to activate the application.



Now you can use the confidential application to generate access tokens that you can include in REST API and CLI payloads. See [Generate and Use Access Tokens in REST API and CLI Payloads \(IDCS\)](#)

Generate and Use Access Tokens in REST API and CLI Payloads (IDCS)

(Oracle Identity Cloud Service only) If you want to create an Oracle Analytics Cloud instance programmatically, you must generate an access token that you can include in the payload for REST API and CLI create operation. Access tokens are set to expire after a certain time period so you might need to repeat this task for subsequent create operations. By default, access tokens are valid for one hour (3600 seconds).

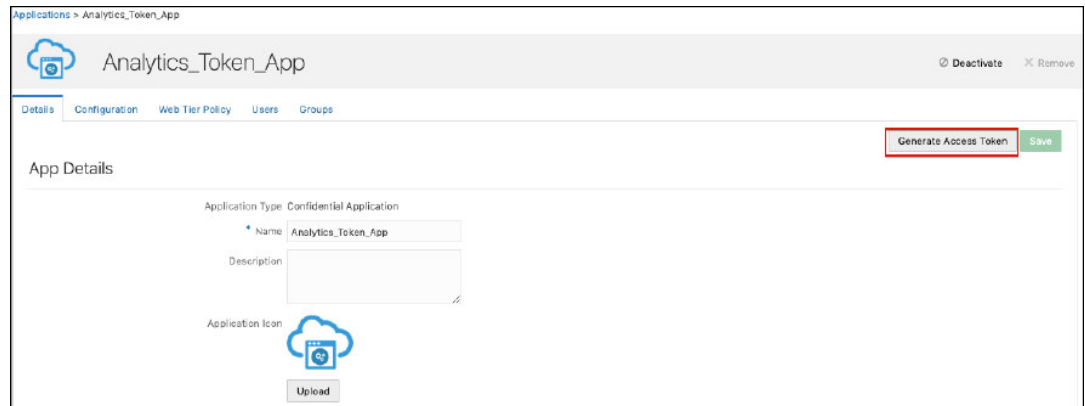
Note

These instructions are for tenancies that use *Oracle Identity Cloud Service (IDCS)*. If your tenancy uses *identity domains* you don't need to generate an access token to use the CLI or REST API.

You can generate access tokens using the Console or programmatically (using CLI or an API).

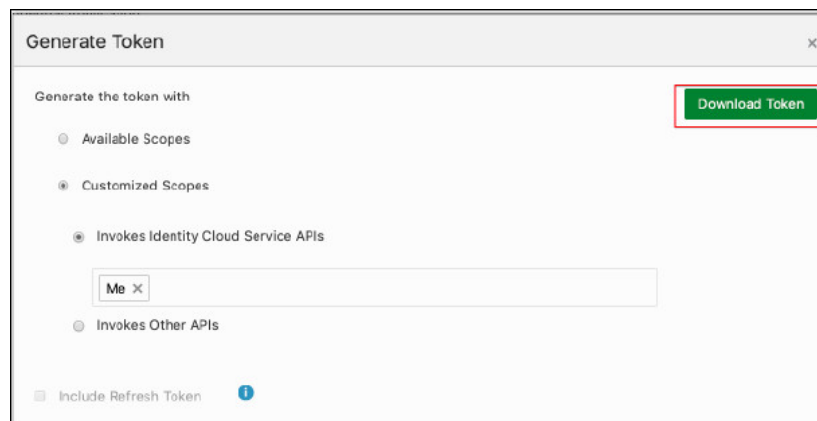
To generate access tokens from the Console:

1. Sign in to your Oracle Cloud account as an administrator.
2. In Oracle Cloud Infrastructure Console, navigate to **Identity & Security**, click **Federation**, select **OracleIdentityCloudService**, and then click the **Oracle Identity Cloud Service Console URL**.
3. Navigate to the **Applications** tab, and click the application that you previously created to generate tokens. For example, `Analytics_Token_App`.
4. Click **Generate Access Token**.



5. Select **Customized Scopes**.
6. Select **Invokes Identity Cloud Service APIs**, and specify **Me**.
7. Click **Download Token** and save the `tokens.tok` file.

`tokens.tok` contains the access token with the attribute name **app_access_token**.



8. Open `tokens.tok`.

For example:

```
{"app_access_token": "eyJ4NXQjUzI...0jxcCw5oR0ajaNw" }
```

9. Copy the access token value *between* the quotes. For example, the value `eyJ4NXQjUzI...0jxcCw5oR0ajaNw`.
10. To create an Oracle Analytics Cloud instance with this access token, do one of the following:
 - REST API [CreateAnalyticsInstance](#): Specify the token value in the parameter `idcsAccessToken`.

- CLI [analytics-instance create](#): Copy the token value to a file and specify the name of the file in the CLI parameter `--idcs-access-token-file [filename]`.

To generate access tokens using an API or CLI:

1. Generate the access token using an API or from the CLI. For example:

```
curl
-X POST
-u "<client_id>:<client_secret>"
-H 'content-type: application/x-www-form-urlencoded;charset=UTF-8'
-d "grant_type=password"
-d "username=<user>"
-d "password=<password>"
-d 'scope=urn:opc:idm:t.user.me'
"https://<stripe>.identity.oraclecloud.com:443/oauth2/v1/token"
```

The command returns a JSON response similar to this:

```
{"access_token": "eyJ4NXQjUzI...0jxcCw5oR0ajaNw", "token_type": "Bearer", "expires_in": 3600}
```

2. Copy the access token from the JSON. For example, `eyJ4NXQjUzI...0jxcCw5oR0ajaNw`.
3. To create an Oracle Analytics Cloud instance with this access token, do one of the following:
 - REST API [CreateAnalyticsInstance](#): Specify the token value in the parameter `idcsAccessToken`.
 - CLI [analytics-instance create](#): Copy the token value to a file and specify the name of the file in the CLI parameter `--idcs-access-token-file [filename]`.

After You Create a Service

After creating and verifying a service with Oracle Analytics Cloud, you must set up your users and configure additional options for your service. If you're migrating to Oracle Analytics Cloud from on-premises or another cloud service you might want to migrate your existing content now.

- [Verify Your Service and Sign In](#)
- [Set Up Users](#)
- [Configure Options for Your Service](#)
- [Migrate to Oracle Analytics Cloud from Other Environments](#)

Verify Your Service and Sign In

Oracle sends an email to the designated email address when your Oracle Analytics Cloud service is ready. Navigate to your service in Oracle Cloud Infrastructure Console, click the

Analytics Home Page button, and then sign in to verify your Oracle Analytics Cloud service is up and running.

Note


Required IAM Policy

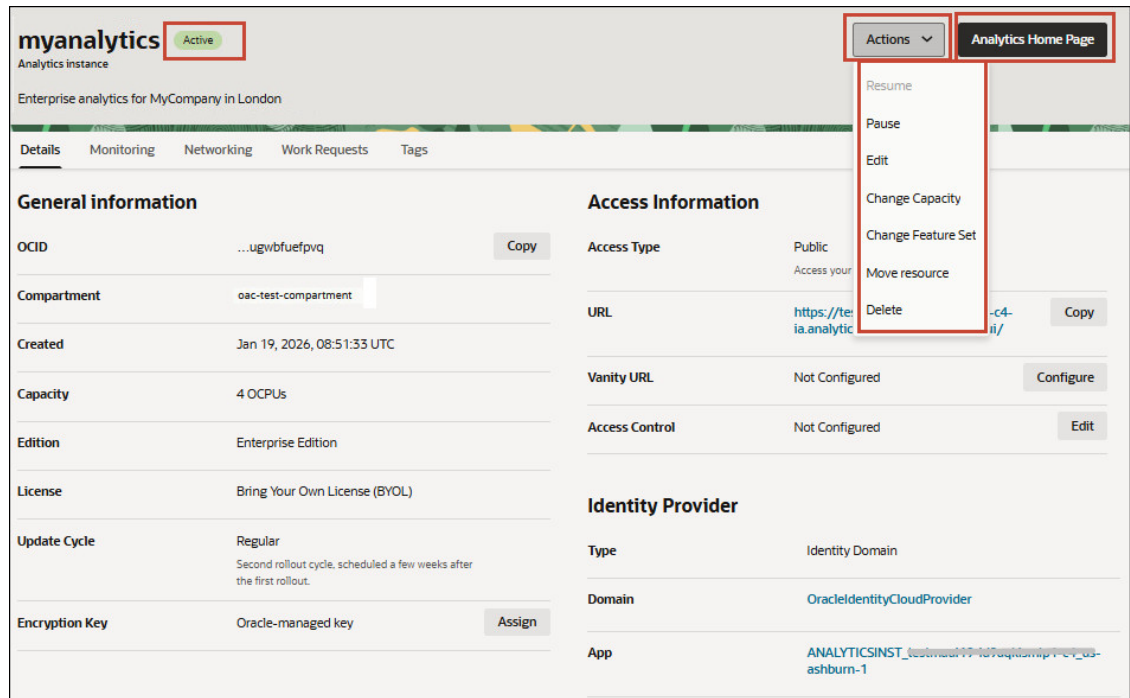
Verb: read

Resource Types: analytics-instance, analytics-instances

Permission: ANALYTICS_INSTANCE_READ

See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

1. In Console, click  in the top left corner.
2. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.
3. Select the compartment in which you created the instance.
4. Click the name of the new instance.
5. Take some time to familiarize yourself with the information and actions available for your instance.
 - **Actions** button: Instance-level actions that enable you to pause, resume, change capacity (scale) and change the feature set (edition). You can also change the license type, edit the description, move your instance to a different compartment, and delete your service.
 - **Instance Details** tab: Information such as OCID, compartment, current capacity, edition deployed, license used, update cycle, public or private access, and identity provider (the Identity and Access Management (IAM) domain or Oracle Identity Cloud Service instance (stripe). Access to encryption key configuration, access control rules for public endpoints, VCN and subnet configuration for private endpoints, the service URL, and vanity URL configuration.
 - **Monitoring** tab: Access to key usage metrics.
 - **Networking** tab: Network configuration information such as your service's host name, IP address, and gateway IP address. Access to private access channel configuration.
 - **Work Requests** tab: Status and activity logs. Drill down for detailed information, log messages, error messages, and associated resources.
 - Tags:
6. Verify and explore your service.
 - a. Click **Analytics Home Page**.
 - b. Sign into Oracle Analytics Cloud service with your administrator credentials.



Configure Options for Your Service

Administrators perform many critical duties; they control user permissions and amend accounts, set up database connections for data modelers, manage data storage to avoid exceeding storage limits, take regular snapshots so users don't risk losing their work, authorize access to external content by registering safe domains, troubleshoot user queries, and much more. After setting up a service with Oracle Analytics Cloud, you can review typical administrator tasks for your service.

See Administrator Task List in *Configuring Oracle Analytics Cloud*.

Migrate to Oracle Analytics Cloud from Other Environments

Do you have content in an existing on-premise system or another cloud service that you want to leverage in Oracle Analytics Cloud? After setting up your service, you can migrate the content to the new environment.

Migrate From...	More Information
Other Oracle Analytics Cloud deployments on Oracle Cloud Infrastructure	Migrate Oracle Analytics Cloud Using Snapshots
Oracle Analytics Cloud - Classic deployed on Oracle Cloud Infrastructure Classic	Migrating Oracle Analytics Cloud - Classic Instances to Oracle Cloud Infrastructure
Oracle Analytics Server	In Oracle Analytics Server: Take a Snapshot and Export the Snapshot In Oracle Analytics Cloud: Import the Snapshot and Restore from the Snapshot
Oracle BI Enterprise Edition 12c (Oracle BI EE 12.2.1.4 or later)	Migrating Oracle Business Intelligence Enterprise Edition to Oracle Analytics Cloud

4

Administer Services

You administer Oracle Analytics Cloud for your organization through Oracle Cloud Infrastructure Console.

Topics

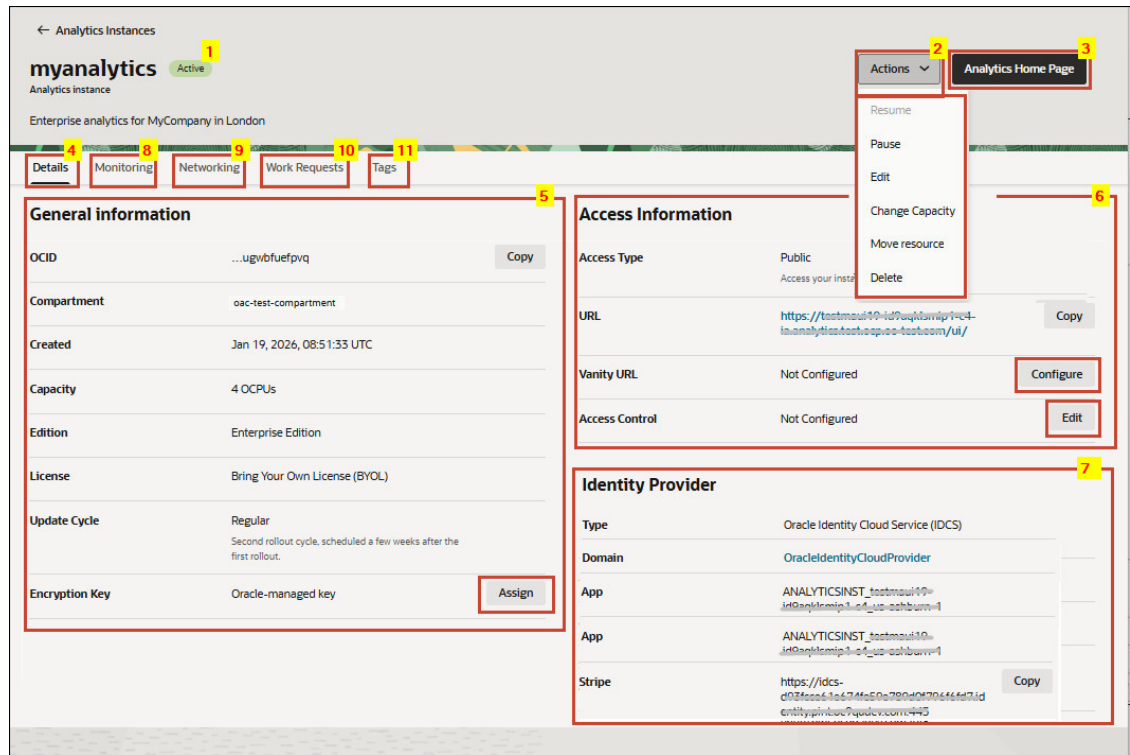
- [About Oracle Analytics Cloud Administration Pages](#)
- [Typical Workflow to Administer a Service](#)
- [View or Update a Service](#)
- [Scale a Service](#)
- [Pause and Resume a Service](#)
- [Delete a Service](#)
- [Monitor Status](#)
- [Monitor Metrics](#)
- [Monitor Logs](#)
- [Find Oracle Analytics Cloud Resources](#)
- [Read Cost Reports](#)
- [Analyze Costs for Oracle Analytics Cloud](#)

About Oracle Analytics Cloud Administration Pages

You can perform most administration tasks for your Oracle Analytics Cloud deployment from the Instance Details page in Oracle Cloud Infrastructure Console. This topic describes the information available and actions you can perform from the Instance Details page and provides links to more detailed documentation.

- [Instance Details page](#)
- [Monitoring tab](#)
- [Networking tab](#)
- [Work Requests tab](#)
- [Tags tab](#)

Oracle Analytics Cloud - Instance Details



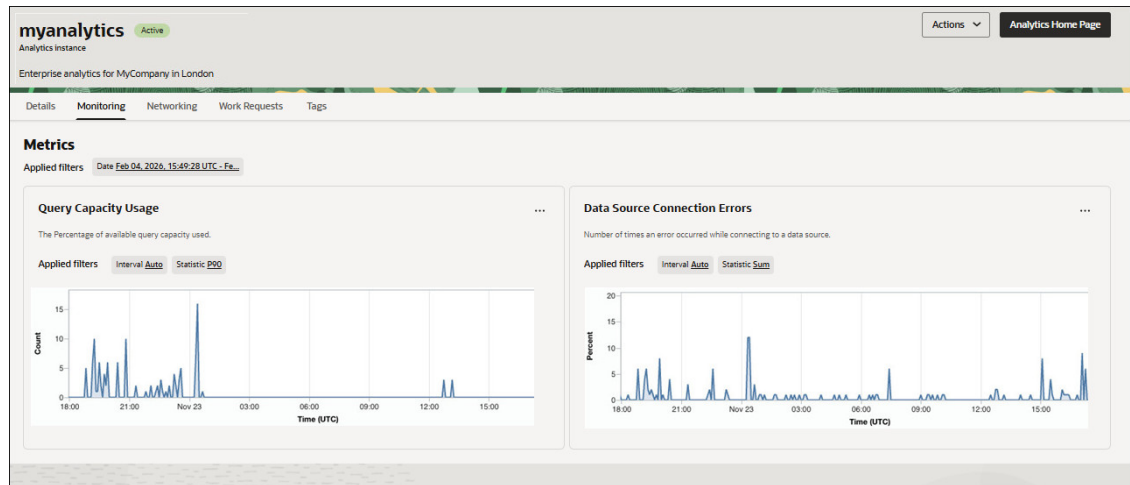
Nu **Description**
mbe
r

- 1 The status of your Oracle Analytics Cloud. For example, **Active**, **Failed**, **Updating**, and so on.
- 2 Click **Actions** to access additional menu options:
 - **Resume** - Re-enable access to your Oracle Analytics Cloud after pausing it.
 - **Pause** - Temporarily disable access to your Oracle Analytics Cloud. See [Pause and Resume a Service](#).
 - **Edit** - Change the description of your Oracle Analytics Cloud or the license type (Oracle Cloud or BYOL). See [View or Update a Service](#).
 - **Change Capacity** - Scale your Oracle Analytics Cloud deployment up or down. See [Scale a Service](#).
 - **Move resource** - Move your Oracle Analytics Cloud to a different compartment. This action can take some time to complete. See [About Compartments](#).
 - **Delete** - Delete your Oracle Analytics Cloud. See [Delete a Service](#).
 - Move these....
 - **Add tags** - Add or edit tags. You can use tags to search for and categorize your instances in your tenancy. See [About Tagging](#).
 - **Update vanity URL certificate** - Update security certificates associated with your vanity URL, if you configured one. See [Update Certificates for a Vanity URL](#).
 - **Remove vanity URL** - Delete your vanity URL, if you configured one. See [Delete a Vanity URL](#).
- 3 Click **Analytics Home Page** to navigate to the home page of your Oracle Analytics Cloud. See [Verify Your Service and Sign In](#).
- 4 Click **Details** to access general information about your Oracle Analytics Cloud deployment.

Number	Description
5	<p>The General Information section displays the following information:</p> <ul style="list-style-type: none"> • OCID - Shows the Oracle Cloud identifier that uniquely identifies your Oracle Analytics Cloud instance. Click Show to see the full OCID. Click Copy to copy it. • Compartment - Shows the compartment in which the Oracle Analytics Cloud instance is stored. • Created - Shows the date the Oracle Analytics Cloud instance was created. • Capacity - Shows the number of OCPUs or users allocated to the Oracle Analytics Cloud instance. See What Sizing Options Are Available to You? To increase or decrease capacity, click the Change Capacity action button. See Scale a Service. • Edition - Shows the edition you selected for the Oracle Analytics Cloud instance. Either Professional or Enterprise. See Which Edition Do You Need? • License - Shows the type of license the Oracle Analytics Cloud instance uses. Either an Oracle Cloud license or an existing license brought over from Oracle Middleware (BYOL). • Update Cycle - Shows the update cycle you selected for the Oracle Analytics Cloud instance. Either Regular or Early. See Do You Want Early Access to Updates? • Encryption Key - Shows the master encryption key your Oracle Analytics Cloud instance uses. Either an Oracle-managed key or a custom encryption key. Click Assign to configure a custom encryption key. Click Edit to rotate or change the current encryption key. See Encrypt Sensitive Information.
6	<p>The Access Information section displays the following information:</p> <ul style="list-style-type: none"> • Access Type - Shows whether your Oracle Analytics Cloud is accessible through a public or private endpoint. • URL - Shows the default URL for your Oracle Analytics Cloud instance. Click Copy to copy it. • Vanity URL - If not yet configured, click Configure to set up a vanity URL. See Set Up a Custom Vanity URL. If configured, shows the vanity URL for your Oracle Analytics Cloud instance. Click Copy to copy it. To update security certificates associated with your vanity URL, click More Actions and then select Update Vanity URL Certificate. See Update Certificates for a Vanity URL. To delete a vanity URL, click More Actions and then select Remove Vanity URL. See Delete a Vanity URL. <p>Public endpoint</p> <ul style="list-style-type: none"> • Access Control - Enables you to configure access control rules for a public Oracle Analytics Cloud instance. Click Edit to add, change, or delete rules. See Restrict Access to Oracle Analytics Cloud Deployed with a Public Endpoint. <p>Private endpoint</p> <ul style="list-style-type: none"> • Virtual Cloud Network - Shows the VCN where you deployed Oracle Analytics Cloud. • Subnet - Shows the subnet where you deployed Oracle Analytics Cloud. Click Edit to select a different VCN or subnet, and configure network security groups that restrict traffic through ingress and egress rules. See Change the VCN or Subnet Used to Access a Private Endpoint and Control Incoming and Outgoing Traffic for a Private Endpoint (Ingress and Egress).
7	<p>The Identity Provider section displays the following information</p> <ul style="list-style-type: none"> • Type - Displays the type of identity provider that your Oracle Analytics Cloud uses. Either Identity Domain or Oracle Identity Cloud Service (IDCS). See How can I find information about the identity provider my Oracle Analytics Cloud uses? <p>Identity domain</p> <ul style="list-style-type: none"> – Domain - The identity domain your Oracle Analytics Cloud uses. Click the link to navigate to the administration pages for the identity domain. – Domain URL - The identity domain URL. Click Copy to copy it. <p>Oracle Identity Cloud Service (IDCS)</p> <ul style="list-style-type: none"> – Stripe - The Oracle Identity Cloud Service instance your Oracle Analytics Cloud uses (also referred to as the stripe). Click Copy to copy it. <ul style="list-style-type: none"> • App - The application associated with the identity provider.
8	<p>Click Monitoring to access key usage metrics. For example, you can view charts that report how many errors occur connecting to your data sources and how much available query capacity you're using. See Access Metrics for Oracle Analytics Cloud Using the Console (Instance Details).</p>
9	<p>Click Networking to access networking and identity management information. See below for details.</p>

Number	Description
10	Click Work Requests to access a list of activities related to your Oracle Analytics Cloud and the current status of each activity. You can use the activity log to track the history, progress, and error for operations such as create, pause, resume, scale, and so on. See Monitor Status .
11	Click Tags to view and edit tags assigned to Oracle Analytics Cloud resources.

Oracle Analytics Cloud - Monitoring



Number	Description
12	Query Capacity Usage - The percentage of available query capacity that your Oracle Analytics Cloud instance uses. See About Metrics for Oracle Analytics Cloud .
13	Data Source Connection Errors - The number of times a connection error occurs. See About Metrics for Oracle Analytics Cloud .

Oracle Analytics Cloud - Networking

The screenshot shows the Oracle Analytics Cloud Administration interface. At the top, there is a header with the instance name 'myanalytics' (Active), an 'Actions' dropdown, and a link to 'Analytics Home Page'. Below the header, there are navigation tabs: 'Details', 'Monitoring', 'Networking' (highlighted with a red box), 'Work Requests', and 'Tags'. The main content area is divided into two sections:

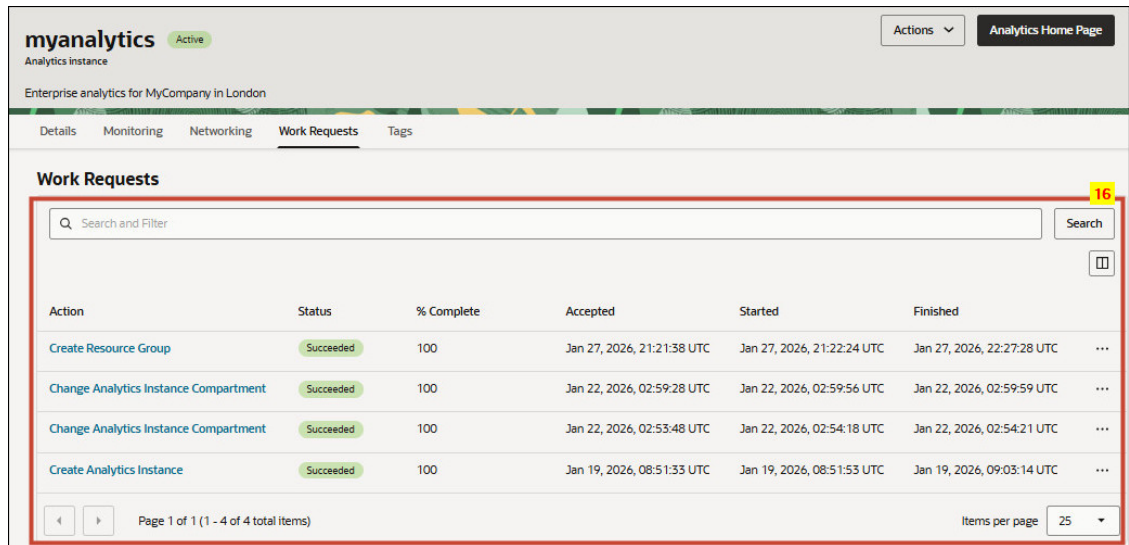
- Networking Information (12):** This section displays three rows of information:

Hostname	myanalyticsinstance2-f07uqtdanip1-v0-l0analytics-testocpoc-test.com	Copy
IP Address	150.3.65.117	Copy
Gateway IP Address	150.3.65.32	Copy
- Private Access Channel (13):** This section contains a search bar with the placeholder text 'Search and Filter' and a 'Search' button. Below the search bar is a button labeled 'Configure Private Access Channel' (highlighted with a red box). Underneath is a table with columns: 'Name', 'Virtual Cloud Network', 'Subnet', and 'Private Sources'. The table is currently empty, displaying the message 'No items to display' and a note: 'Create new items or search again using different filters or search terms.'

Number	Description
--------	-------------

- | | |
|----|--|
| 14 | <p>The Networking Information section displays the following information:</p> <ul style="list-style-type: none"> • Hostname - Shows the host name of your Oracle Analytics Cloud deployment. Click Copy to copy it. • IP Address - Shows the IP address of your Oracle Analytics Cloud deployment. If you set up a vanity URL, you must add a DNS entry that maps the custom domain name you want to use to the IP Address of your Oracle Analytics Cloud instance. Click Copy to copy it. • Gateway IP Address - Shows the Gateway IP address of your Oracle Analytics Cloud deployment. Some data sources use an allowlist to control access to their data. To include your Oracle Analytics Cloud instance in an allowlist, copy the Gateway IP Address and add it to the allowlist so that Oracle Analytics Cloud can connect and access the data. Click Copy to copy it. <p>See Find the IP Address or Host Name of Your Oracle Analytics Cloud Instance.</p> |
| 15 | <p>The Private Access Channel section enables you to configure a private access channel so your Oracle Analytics Cloud can access data on private hosts. See Connect to Private Sources Through a Private Access Channel.</p> |

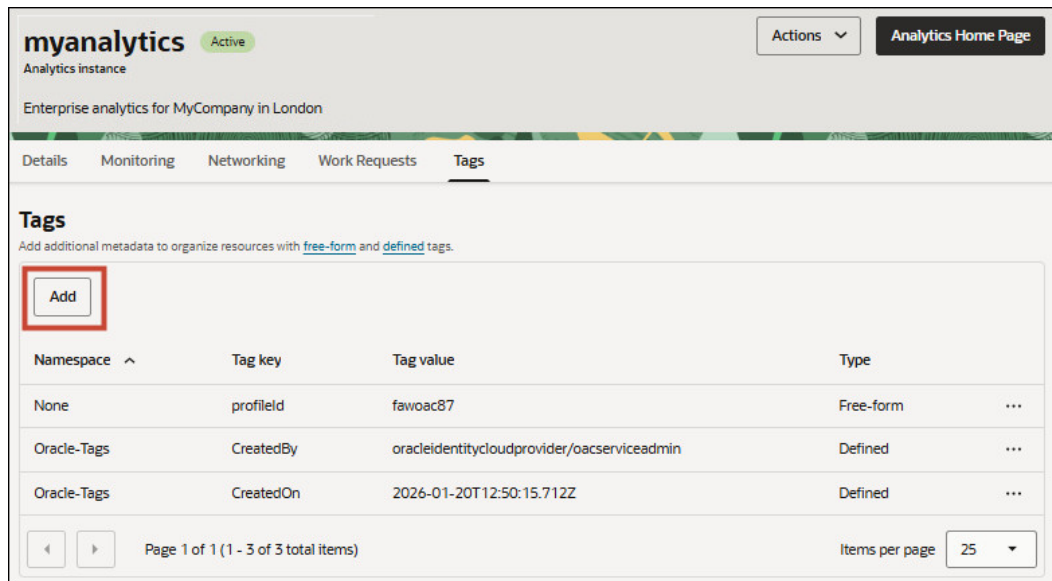
Oracle Analytics Cloud - Work Requests



Number **Description**

16 Lists activities related to your Oracle Analytics Cloud and the current status of each activity. You can drill down the activity log to track the history, progress, and error for operations such as create, pause, resume, scale, and so on. See [Monitor Status](#).

Oracle Analytics Cloud - Tags



List tags associated with your Oracle Analytics Cloud instance. Click **Add** to create a tag (free-form or defined).

- Defined tags are tags that your tag administrator applied to resources associated with the Oracle Analytics Cloud instance. See [Resource Tags](#).
- Free-form tags are tags that you assign to your Oracle Analytics Cloud instance to help your search for and categorize instances and other resources in your tenancy. See [Understanding Free-form Tags](#).

Typical Workflow to Administer a Service

After you create an Oracle Analytics Cloud instance with Oracle Cloud Infrastructure for the first time, follow these tasks as a guide.

Task	Description	More Information
View and update service details	View instances, edit details, move your instance to a different compartment, and more. Use the search facility to find instances across compartments.	About Oracle Analytics Cloud Administration Pages View or Update a Service using the Console Find Oracle Analytics Cloud Resources
Scale a service up or down	Increase or decrease the number of Oracle Compute Units (OCPU) allocated to your service.	Scale a Service
Pause or resume a service	Pause a service to temporarily prevent users from accessing the service.	Pause and Resume a Service
Delete a service	Delete services that you don't want anymore.	Delete a Service
Monitor services	Monitor the status of your service.	Monitor Status Monitor Instance Event Logs
Track usage and billing	Track costs associated with your services.	Read Cost Reports Analyze Costs for Oracle Analytics Cloud

View or Update a Service

You can access services and update instance details using the Console, API, or command line. You can edit details such as the description, license type, or tags.

Note

Required IAM Policy

Verb: `inspect` (to view), `manage` (to update)

Resource Types: `analytics-instance`, `analytics-instances`

Permission: `ANALYTICS_INSTANCE_INSPECT` (to view), `ANALYTICS_INSTANCE_UPDATE` (to update)


See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

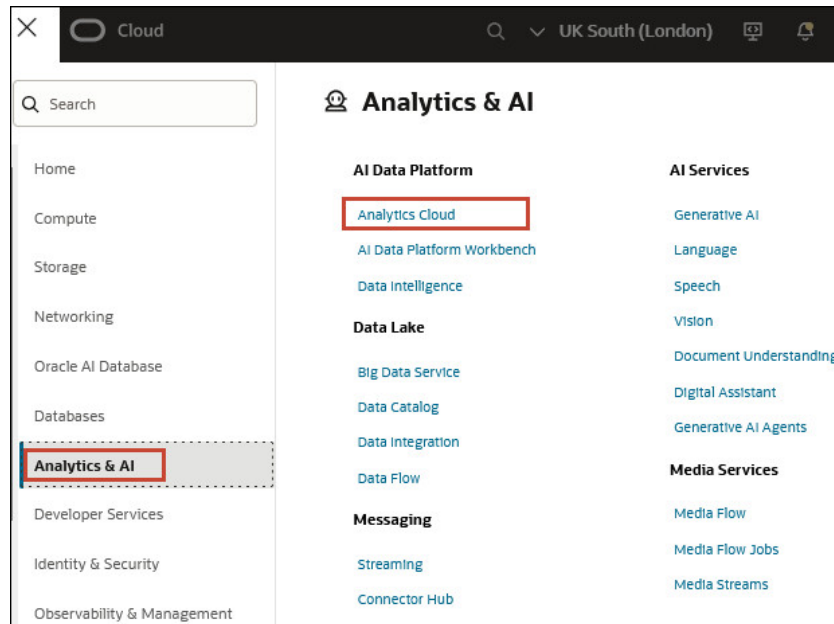
Topics


- [View or Update a Service using the Console](#)
- [View or Update a Service using the REST API](#)
- [View or Update a Service using the Command Line](#)

View or Update a Service using the Console

You can use Oracle Cloud Infrastructure Console to view and edit Oracle Analytics Cloud instances.

1. Sign in to your Oracle Cloud account.
2. In Oracle Cloud Infrastructure Console, click  in the top left corner.
3. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.



4. Select the compartment that contains the Oracle Analytics Cloud instances you're looking for.
5. To change the description or the license type, click  for the instance, and select **Edit**.

Analytics Instances

Oracle Analytics Cloud is a scalable and secure public cloud service that provides capabilities to explore and perform collaborative analytics for you, your workgroup, and your enterprise. [Learn More](#)

Search and Filter Search

Applied filters: Compartment analytics-instances

Create Instance ☰

Name	Status	Feature Set	Capacity	Created
analyticsinstance01	Active	Enterprise Edition	2 OCPUs	Feb 06, 2026, 16:21:13 UTC

Page 1 of 1 (1 - 1 of 1 total items)

Analytics Home Page
Edit
Resume
Pause
Delete
Move resource
Copy OCID

- To edit or add tags, click the name of your instance to show the details page, and then click the **Tags** tab.

View or Update a Service using the REST API

You use the `GetAnalyticsInstance` and `UpdateAnalyticsInstance` operations to return and edit Oracle Analytics Cloud instances. If you want to move the instance to a different container you use `ChangeAnalyticsInstanceCompartment`.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use these operations:

- [GetAnalyticsInstance](#)
- [UpdateAnalyticsInstance](#)
- [ChangeAnalyticsInstanceCompartment](#)

View or Update a Service using the Command Line

You can use the `analytics-instance list`, `analytics-instance get`, `analytics-instance update`, and `analytics-instance change-compartment` commands to return and update Oracle Analytics Cloud instances.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use these commands:

- [analytics-instance list](#)
- [analytics-instance get](#)
- [analytics-instance update](#)
- [analytics-instance change-compartment](#)

Scale a Service

You can scale the number of Oracle Compute Units (OCPU) or users that your service uses as your needs change.

Note

Required IAM Policy

Verb: manage

Resource Types: analytics-instance, analytics-instances

Custom Permission: ANALYTICS_INSTANCE_MANAGE

See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

Topics:

- [About Scaling](#)
- [Scale Up or Down using the Console](#)
- [Scale Up or Down using the REST API](#)
- [Scale Up or Down using the Command Line](#)

About Scaling

If you subscribe to Oracle Analytics Cloud through Universal Credits and your service performs poorly, you can scale up the number of Oracle Compute Units (OCPU) allocated to the service to improve performance. To save costs or if your workload is reduced, you might scale down. Similarly, if you set up Oracle Analytics Cloud to support a specific number of users and your user requirements change, you can scale the number of users up or down.

[LiveLabs Sprint](#)

You can scale your Oracle Analytics Cloud environment up and down within the OCPU range (or user range) available to your service (see table) and within the overall service limit for your tenancy (see [Service Limits](#)). Users don't experience any downtime when you scale a service up or down; the service stays up and running. Users might experience a reduction in performance for about 60 minutes during scale operations.

- **Scale the Number of OCPUs**

With Universal Credits, you can scale up and down between 1 and 16 OCPUs.

Current OCPUs	OCPU Range	Scale Up within Range?	Scale Down within Range?
		(Incremental + increase)	(Incremental - decrease)
1 (non-production)	1 - 16	Yes (+1, +3, +5, +7, +9, +11, +15)	No (minimum for this range)
2	1 - 16	Yes (+2, +4, +6, +8, +10, +14)	Yes (-1)
4	1 - 16	Yes (+2, +4, +6, +8, +12)	Yes (-2, -3)

Current OCPUs	OCPU Range	Scale Up within Range?	Scale Down within Range?
		(Incremental + increase)	(Incremental - decrease)
6	1 - 16	Yes (+2, +4, +6, +10)	Yes (-2, -4, -5)
8	1 - 16	Yes (+2, +4, +8)	Yes (-2, -4, -6, -7)
10*	1 - 16	Yes (+2, +4)	Yes (-2, -4, -6, -8, -9)
12*	1 - 16	Yes (+4)	Yes (-2, -4, -6, -8, -10, -11)
16	1 - 16	No (maximum for this range)	Yes (-4, -6, -8, -10, -12, -14, -15)
24	24	No	No
36	36	No	No
52	52	No	No

* If you created your Oracle Analytics Cloud instance with 10 - 12 OCPUs *before* August 2024, you can only scale between 10 – 12 OCPUs. In this case, if you want to scale between 1 – 16 OCPUS, you must create a service instance with the OCPUs that you want and migrate your content to the new service. See [Migrate Oracle Analytics Cloud Using Snapshots](#).

- **Scale the Number of Users**


With Universal Credits, you can size your service based on the number of users you expect to use Oracle Analytics Cloud. If your user requirements increase or decrease, you can scale within specific user ranges.

Minimum Users	Maximum Users
10	400
401	600
601	900
901	1400
1401	2200
2201	3000

For example, if you currently subscribe with 200 users, you can increase to 400 or decrease to 10. If you want to scale across these ranges (for example, scale up from 300 to 500 or scale down from 500 to 300), you must create a service instance with the number of users that you want and migrate your content to the new service.

Scale Up or Down using the Console

You can use the Console to scale up or scale down the number of OCPUs or users allocated to your service.

1. In Oracle Cloud Infrastructure Console, click  in the top left corner.
2. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to scale.
5. Note how many OCPUs or users your service currently uses.

The current **Capacity** is displayed on the **Details** tab.

6. Click **Actions**, then **Change Capacity**.

You can't scale up or down while your service is being backed up, restored, or undergoing similar administrative operations. If you see the message `System is not in a READY state. Current state is CONFIGURING`, wait a few minutes for the current operation to complete and try again.

7. Select the number of **OCPUs** or **Users** you want.

The values available to you depend on how many OCPUs (or users) your service currently uses. Remember that you can add or remove capacity within the OCPU range (or user range) of your service.

- Change the number of OCPUs:

Change Capacity

OCPU Count
2

1 (Non-production)

2

4

6

8

10

12

16

- Change the number of users:

Change Capacity

User Count

310

10 - 400

Save Changes Cancel

You see a message if scale options aren't available for your environment. For example, you can't scale an environment with 24 OCPUs.

8. Click **Update** to save your changes.

The scale up (or down) operation can take up to 60 minutes to complete. The status of the service changes to **Updating**. Users don't experience any downtime while the operation is in progress; the service remains available.

Scale Up or Down using the REST API

You can use the `ScaleAnalyticsInstance` operation to scale up or scale down an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use this operation:

- [ScaleAnalyticsInstance](#)

Scale Up or Down using the Command Line

You can use the `analytics-instance scale` command to scale up or scale down an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- [analytics-instance scale](#)

Pause and Resume a Service

When you subscribe to Oracle Analytics Cloud through Universal Credits, you can pause a service if you want to temporarily prevent anyone accessing the service and reduce costs. You can pause and resume an Oracle Analytics Cloud instance using the Console, API, or command line.

Note

Pause disables access, and resume enables access to your instance. Pause and resume *doesn't* restart your instance.

Note

Required IAM Policy

Verb: use

Resource Types: `analytics-instance`, `analytics-instances`

Permission: `ANALYTICS_INSTANCE_USE`


See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

For information about metering and billing implications when you pause a service, see [Oracle PaaS and IaaS Universal Credits Service Descriptions \(PDF\)](#).

- [Pause and Resume using the Console](#)
- [Pause and Resume a Service using the REST API](#)
- [Pause and Resume using the Command Line](#)

Pause and Resume using the Console

You can use the Console to pause a service if you want to temporarily prevent anyone accessing the service and reduce costs.

1. In Oracle Cloud Infrastructure Console, click  in the top left corner.
2. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to pause or resume.
5. To temporarily pause a service, click **Actions**, and select **Pause**.
While in progress, the status of the service changes to **Updating**.
After a few minutes, the service status changes to **Inactive**.
6. To resume the service, click **Actions**, and select **Resume**.
While in progress, the status of the service changes to **Updating**.
After a few minutes, the service status changes to **Active**.
When complete, users can sign in to the service and normal billing resumes.

Pause and Resume a Service using the REST API

You use the `StopAnalyticsInstance` and `StartAnalyticsInstance` operations to pause and resume an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use these operations:

- [StopAnalyticsInstance](#)
- [StartAnalyticsInstance](#)

Pause and Resume using the Command Line

You can use the `analytics-instance stop` and `analytics-instance start` commands to pause and resume an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use these commands:

- [analytics-instance stop](#)
- [analytics-instance start](#)

Delete a Service

You can delete an Oracle Analytics Cloud instance using the Console, API, or command line.

Note

Required IAM Policy

Verb: manage

Resource Types: analytics-instance, analytics-instances

Permission: ANALYTICS_INSTANCE_DELETE

See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

Topics



- [Delete a Service using the Console](#)
- [Delete a Service using the REST API](#)
- [Delete a Service using the Command Line](#)

Delete a Service using the Console

You can use the Console to delete services you created but don't need anymore.

1. In Oracle Analytics Cloud, take a snapshot of your content and download the snapshot to your local system in case you want to restore the content in the future.

See [Take a Snapshot and Download a Snapshot](#).

2. In Oracle Cloud Infrastructure Console, click  in the top left corner.
3. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.
4. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
5. Click  for the instance you want to delete, and then select **Delete**.
6. Click **Delete** to confirm.

The Status of the instance changes to **Deleting**. After a few moments, the status changes to **Deleted**.

Delete a Service using the REST API

You can use the `DeleteAnalyticsInstance` operation to delete an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use this operation:

- [DeleteAnalyticsInstance](#)

Delete a Service using the Command Line

You can use the `analytics-instance delete` command to delete an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- [analytics-instance delete](#)

Monitor Status

You can monitor the current status and progress of operations for an Oracle Analytics Cloud instance using the Console, API, or command line.

Note

Required IAM Policy

Verb: read

Resource Types: analytics-instance, analytics-instances

Permission: ANALYTICS_INSTANCE_READ


See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

Topics

- [Monitor Status using the Console](#)
- [Monitor Status using the REST API](#)
- [Monitor Status using the Command Line](#)

Monitor Status using the Console

You can use Oracle Cloud Infrastructure Console to check the status of your Oracle Analytics Cloud instances and any operations that are in progress.

1. In Oracle Cloud Infrastructure Console, click  in the top left corner.
2. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.
3. Select the compartment that contains the Oracle Analytics Cloud instances you're looking for.

A list of all the instances in the compartment are displayed.

4. Check the **Status** column to determine the current status of your instance.
 - **Creating:** Instance is in the process of being created.
 - **Active:** Instance is running normally.
 - **Updating:** Instance is being updated. For example, in the process of scaling up or down, being paused or resumed, or undergoing maintenance. Lifecycle operations

such as pause, resume, and scale are temporarily unavailable while the status is **Updating**.

- **Inactive:** Instance has been temporarily stopped or is stopping.
- **Failed:** Instance isn't running due to an error.
- **Deleting:** Instance is in the process of being deleted.
- **Deleted:** Instance has been deleted and resources released.

Analytics Instances

Oracle Analytics Cloud is a scalable and secure public cloud service that provides capabilities to explore and perform collaborative analytics for you, your workgroup, and your enterprise. [Learn More](#)

Search and Filter Search

Applied filters Compartment analytics-instances

Create Instance

Name	Status	Feature Set	Capacity	Created
Temp	Creating	Professional Edition	10 Users	Feb 11, 2026, 19:25:25 UTC
analyticsinstance01	Active	Enterprise Edition	2 OCPUs	Feb 06, 2026, 16:21:13 UTC

Page 1 of 1 (1 - 2 of 2 total items) Items per page 25

5. Click the name of your service to access activity details.
6. Click the **Work Requests** tab to view the history and status of activities related to the instance. For example, work requests such as create, start, stop, scale, and so on.
 - **ACCEPTED:** The request is in the queue to be processed.
 - **IN PROGRESS:** The work request started but isn't complete.
 - **SUCCEEDED:** A work request record exists for this request and an associated WORK_COMPLETED record is in the state SUCCEEDED.
 - **FAILED:** A work request record exists for this request and an associated WORK_COMPLETED record is in the state FAILED.
 - **CANCELING:** The work request is in the process of canceling.
 - **CANCELED:** The work request has been canceled.

Action	Status	% Complete	Accepted	Started	Finished
Create Vanity URL	Succeeded	100	Feb 07, 2026, 01:05:41 UTC	Feb 07, 2026, 01:06:05 UTC	Feb 07, 2026, 01:11:29 ...
Edit Private Access Channel	Succeeded	100	Feb 07, 2026, 00:51:21 UTC	Feb 07, 2026, 00:51:34 UTC	Feb 07, 2026, 00:57:48 ...
Create Private Access Channel	Succeeded	100	Feb 07, 2026, 00:37:17 UTC	Feb 07, 2026, 00:37:29 UTC	Feb 07, 2026, 00:49:14 ...
Create Analytics Instance	Succeeded	100	Feb 06, 2026, 16:21:13 UTC	Feb 06, 2026, 16:21:24 UTC	Feb 06, 2026, 16:30:40 ...

Monitor Status using the REST API

You use `GetWorkRequest` to get the current status of operations you perform on Oracle Analytics Cloud instances. If you want to cancel an operation, you use `DeleteWorkRequest`. To check errors and access logs, you use `ListWorkRequestErrors` and `ListWorkRequestLogs`.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use these operations:

- [GetWorkRequest](#)
- [DeleteWorkRequest](#)
- [ListWorkRequestErrors](#)
- [ListWorkRequestLogs](#)

Monitor Status using the Command Line

You use the `work-request list` and `work-request get` commands to get the current status of operations you perform on Oracle Analytics Cloud instances. If you want to cancel an operation, you use `work-request delete`. To check errors and access logs, you use `work-request-error list` and `work-request-log list`.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- [work-request list](#)
- [work-request get](#)
- [work-request delete](#)
- [work-request-error list](#)
- [work-request-log list](#)

Monitor Metrics

You can monitor metrics that track usage and errors in your Oracle Analytics Cloud instance using the Console, API, or command line.



Oracle Cloud Infrastructure Console displays metrics in two places.

- **Analytics Instance Details page.** You need manage access to see metric information here.
- **Metrics Explorer**

Note

Required IAM Policy - Analytics Instance Details page

If you're an administrator with manage access, you can automatically view metrics on the Analytics Instance Details page.

Verb: manage

Resource Types: analytics-instance, analytics-instances

Permission: ANALYTICS_INSTANCE_MANAGE

See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

Note

Required IAM Policy - Metrics Explorer

If you're a user with read-only access, you must belong to a group with the `read metrics` permission on the compartment containing the instance and use Metrics Explorer to view the metrics.

Verb: read

Resource Types: metrics

For example:

```
#Let users in the analytics_users group view metrics for any Analytics instance in myOACProduction compartment
```

```
allow group analytics_users to read metrics in compartment myOACProduction
```

Topics

- [About Metrics for Oracle Analytics Cloud](#)
- [Access Metrics for Oracle Analytics Cloud Using the Console \(Instance Details\)](#)
- [Access Metrics for Oracle Analytics Cloud Using the Console \(Metrics Explorer\)](#)

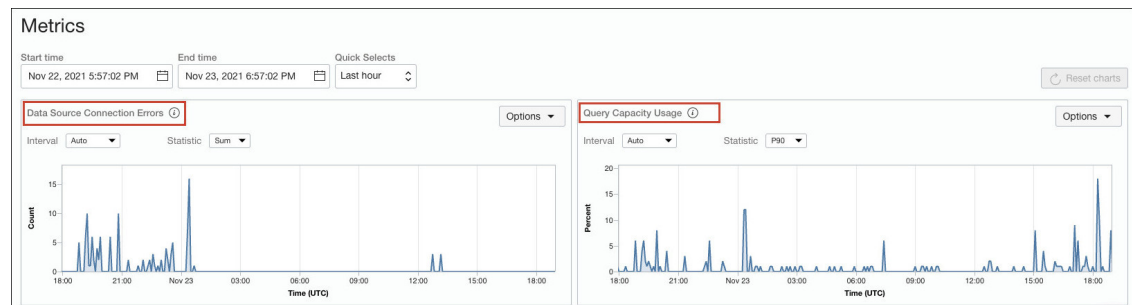
- [Access Metrics Using the REST API](#)
- [Access Metrics Using the Command Line](#)

About Metrics for Oracle Analytics Cloud

You can use charts to monitor key usage and error metrics for Oracle Analytics Cloud. Monitoring these metrics can help you detect anomalies, bottlenecks, and issues with Oracle Analytics Cloud and any data sources that Oracle Analytics Cloud connects to.

Note

Oracle Analytics Cloud offers metrics through the Oracle Cloud Infrastructure Monitoring service. The Oracle Cloud Infrastructure Monitoring service enables you to actively and passively monitor all your cloud resources using the metrics and alarms features. See [Monitoring Overview](#).



Oracle Analytics Cloud Metrics

This table describes the metrics you can monitor for Oracle Analytics Cloud and offers guidance on possible causes and actions to metric trends. You can use the Monitoring service to set up alarms that notify you when these metrics meet certain criteria. For example, you might want to trigger an alarm when query capacity usage reaches 90%. See [Managing Alarms](#).


Metric Name	Description	Action
Query Capacity Usage	<p>The percentage of available query capacity that your Oracle Analytics Cloud instance uses.</p> <p>Query capacity indicates the overall usage of resources required to process analytics workloads.</p>	<p>If the query usage is consistently high (for example, above 80%), your organization's usage is consuming a significant amount of resources. This might be due to high concurrent user activity or application design. Review and tune both the size of your deployment and application design.</p>

Metric Name	Description	Action
Data Source Connection Errors	The number of times a connection error occurs when Oracle Analytics Cloud tries to access data sources through a semantic model connection. Self-service connection errors aren't captured at this time.	<p>Connection errors might occur for several reasons.</p> <ul style="list-style-type: none"> • Connection details are incorrect or no longer valid. • The data source is temporarily unavailable. • Network connectivity issues exist between Oracle Analytics Cloud and the data source. <p>Work with the administrators responsible for the network and the data source to investigate further.</p>

Access Metrics for Oracle Analytics Cloud Using the Console (Instance Details)

If you're an administrator with manage access, you'll see a **Metrics** tab on the Oracle Analytics Cloud instance details page. From the Metrics tab, you can view charts that report how many errors occur connecting to your data sources and how much available query capacity you're using.

If you check these metrics regularly, you'll learn to recognize trends as they develop and prevent problems in the future.

1. In Oracle Cloud Infrastructure Console, click  in the top left corner.
2. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.
3. Select the compartment that contains the Oracle Analytics Cloud instances you're looking for.
4. Click the name of the instance you want to view metrics for.
5. Click the **Monitoring** tab.

6. Click the **Date** filter above the charts to monitor metrics over a different time period such as **Last 24 hours**.

Alternatively, you can change the **Start Date**, **Start Time**, **End Date**, and **End Time** to select a custom range.

7. Change the **Interval** and **Statistic** fields to change the metrics displayed.


The metric count occurs every five minutes.

8. Click the **Actions** menu to navigate to the Metrics Explorer where you can create custom metric dashboards and alarms. For general information about monitoring in Oracle Cloud Infrastructure, see [Monitoring](#).

Access Metrics for Oracle Analytics Cloud Using the Console (Metrics Explorer)

You can use the Metrics Explorer in Oracle Cloud Infrastructure Console to monitor metrics for Oracle Analytics Cloud, and other resource types such as Oracle Cloud Database, virtual cloud network, and so on.

For Oracle Analytics Cloud, you can view charts that report how many errors occur connecting to your data sources and how much available query capacity you're using. If you check these metrics regularly, you'll learn to recognize trends as they develop and prevent problems in the future.

1. In Oracle Cloud Infrastructure Console, click  in the top left corner.
2. Click **Observability & Management**. Under **Monitoring**, click **Metrics Explorer**.
3. In **Compartment**, select the compartment that contains the Oracle Analytics Cloud instance you're looking for.

4. In **Metrics namespace**, select **oci_analytics**.
5. In **Metric name**, select the metric you want to monitor.
 - Query Capacity Usage (%) (PercentQueryCapacityUsed)
 - Data Source Connection Errors (DataSourceConnectionErrors)

If required, edit the **Interval** and **Statistic** fields to change the aggregation window and aggregation function.

6. In **Dimension name** and **Dimension value**, select **resourceName** and then select the name of the instance you want to view metrics for.
7. Click **Update Chart**.

The screenshot displays the Oracle Cloud Monitoring Metrics Explorer. The top section shows a line chart for the metric 'PercentQueryCapacityUsed' over a time range from Feb 5, 2020, 12:22:37 PM UTC to Feb 12, 2020, 12:22:37 PM UTC. The chart shows a fluctuating line around a value of 3. Below the chart is a query editor with the following configuration:

- Compartment: analytics-instances
- Metric namespace: oci_analytics
- Metric name: percentquerycapacityused
- Interval: 1 minute
- Statistic: P90
- Dimension name: resourceName
- Dimension value: analyticsinstance01

The 'Update Chart' button is highlighted in the bottom right corner of the query editor.

8. Optionally, change the **Start time** and **End time** to view the metrics over a specific time range.

For general information about monitoring in Oracle Cloud Infrastructure, see [Monitoring](#).

Access Metrics Using the REST API

You can access metrics and metric alarms through the *Monitoring API*.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use this API:

- [Monitoring API](#)

Access Metrics Using the Command Line

You can access metrics and metric alarms using the *Monitoring CLI*.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use the Monitoring commands.

- [Monitoring CLI](#)

Monitor Logs

Oracle Cloud Infrastructure offers log and audit services that you can use to track usage, diagnostic information, and changes to your Oracle Cloud Infrastructure resources (including Oracle Analytics Cloud).

Topics

- [Monitor Usage and Diagnostic Logs](#)
- [Monitor Instance Event Logs](#)

Monitor Usage and Diagnostic Logs

You can use the *Logging service* in Oracle Cloud Infrastructure to view and manage all the logs in your tenancy, and this includes audit and diagnostic logs from Oracle Analytics Cloud. These logs include important usage information and diagnostic logs that you can use to troubleshoot issues and understand how Oracle Analytics Cloud resources are used.



Note

Required IAM Policy - Enable Service Logs and Create Log Groups

Verb: manage

Resource Types: log-groups

Permission: LOG_GROUP_CREATE

For example:

```
#Let users in the analytics_admin group enable logging for Oracle Analytics Cloud instances and set up log groups.
```

```
allow group analytics_admins to manage log-groups in compartment myOACProduction
```

Required IAM Policy - Read Oracle Analytics Cloud logs

Verb: read

Resource Types: log-content

Permission: LOG_CONTENT_READ

For example:

```
#Let users in the analytics_users group read logs for Oracle Analytics Cloud instances.
```

```
allow group analytics_users to read log-content in compartment myOACProduction
```

See [Permissions for Working with Logging](#).

Topics

- [About Audit and Diagnostic Logs for Oracle Analytics Cloud](#)
- [Access Audit and Diagnostic Logs for Oracle Analytics Cloud Using the Console](#)

About Audit and Diagnostic Logs for Oracle Analytics Cloud

You can monitor Oracle Analytics Cloud activity using various audit and diagnostic logs. Analyzing logs can help you understand how Oracle Analytics Cloud resources are used and troubleshoot issues.

Note

Oracle Analytics Cloud offers logs through the Oracle Cloud Infrastructure (OCI) Logging service. The Logging service provides a highly scalable and fully managed single interface for logs in your tenancy. You can use Logging to access logs from many Oracle Cloud Infrastructure resources, including Oracle Analytics Cloud. See [Logging](#).

Log Categories

Oracle Analytics Cloud offers two types of log: *audit* and *diagnostic*.

API value (ID):	Console (Display Name)	Description
audit	Audit logs	<p>Logs activity in Oracle Analytics Cloud.</p> <ul style="list-style-type: none"> Catalog objects: Create, update, delete, and permission change operations on all catalog objects, such as classic analyses, dashboards, workbooks, pixel-perfect reports, folders, datasets, self-service connections, data flows, sequences, scripts, and so on. Includes the activity of catalog objects in shared folders and personal folders. <p>"category": "catalog"</p> Data export : Data export operations for reports and dashboards to all formats (CSV, Excel, Powerpoint, PDF, and so on). Data export operations for workbooks to CSV format only. <p>Note: Workbook data exports to all other formats are recorded in the <i>diagnostic</i> log.</p> <p>"category": "data"</p> Data Gateway: Invalid key authentication attempts from Data Gateway clients. <p>"category": "data"</p> Publisher: Administration and configuration activity for pixel-perfect reports, such as connections, run-time properties, delivery channels, file uploads and downloads, delivery scheduling, and so on. <p>"category": "publisher"</p> Security: Create and delete operations for user-defined application roles. User role assignments, and policy store changes. <p>"category": "security"</p> Semantic models: Upload and download of semantic models (RPD files), updates to connection pools and variables. <p>"category": "semanticModel"</p> Settings: Changes to system settings, and configuration activities for mail server, virus scanner, social channels, Data Gateway, console connections, deliveries, search crawls, safe domains, plug-in custom visualization types, map layers, map backgrounds, and so on. <p>"category": "settings"</p> Snapshots: Lifecycle management operations such as create, delete, and restore snapshots, import and export snapshots. Registration and deregistration of snapshots in customer-owned object storage using REST APIs. <p>"category": "snapshot"</p> Workbooks: Export and import workbooks as DVA packages. <p>"category": "DVA"</p>

API value (ID):	Console (Display Name)	Description
diagnostic	Diagnostic logs	<p>Logs diagnostic information.</p> <ul style="list-style-type: none"> Data export : Data export operations for workbooks to all formats <i>except</i> CSV. That is, Powerpoint, PDF, and so on. Note: Workbook data exports to CSV format are recorded in the <i>audit</i> log. "category": "data" Data load: Data reload (or refresh) operations for datasets and data flows. "category": "dataLoad" GenAI: Generative AI operations for AI Assistant and AI agents. "category": "GenAI" Queries: Data query details. "category": "query"

Contents of an Oracle Analytics Cloud Log

Oracle Analytics Cloud logs contain the following fields.

Field	Description	Example
data	<p>JSON object that contains:</p> <ul style="list-style-type: none"> userid ipAddress category message ecid logLevel additionalDetails 	<p>The data field logs details about each event, including the user who initiated the event. See examples:</p> <ul style="list-style-type: none"> Sample Analytics Cloud Diagnostic Log - Query Detail Sample Analytics Cloud Diagnostic Log - Physical Query Summary
<ul style="list-style-type: none"> userid 	<p>User performing the action or activity. Either:</p> <ul style="list-style-type: none"> GUID of the user in Oracle Identity Cloud (default). Name of the user in Oracle Identity Cloud. <p>To record user names rather than GUIDs in audit and diagnostic logs, go to the System Settings page in your Oracle Analytics Cloud instance and enable the setting User Names as the User Identifier in Service Logs. See Usage Tracking Options and Configure System Settings.</p>	<p>"userId": "aa11bb22cc33dd44ee55ff66gg77hh88"</p> <p>"userId": "john.smith@mycompany.com"</p>

Field	Description	Example
• ipAddress	Client IP address of the user's computer or device performing the action or activity. This field provides the first recorded IP address in the web request associated with the user action.	"ipAddress": "192.168.1.1"
• category	One of the following log categories: <ul style="list-style-type: none"> • catalog • data • dataLoad • DVA • publisher • query • security • semanticModel • settings • snapshot 	snapshot
• message	Summary of the log event.	Snapshot 'MyFirstSnapshot' created."
• ecid	Execution context ID associated with the log event.	1122a3b3-c440-5566-7788-99d001ef1223-34455aa6
• logLevel	Type of message. Only one possible value: <ul style="list-style-type: none"> • info (information) 	info
• additionalDetails	(Optional) JSON object that contains additional details applicable to a particular log in the format: "additionalDetails": { "propertyName": "foo", "propertyValue": "bar", }	"additionalDetails": { "snapshotSizeInBytes": "948999", "source": "console" },
id	Unique ID for each log entry.	38c5cc58-f9f6-11eb-bee4-0200170046fa
GenAI	JSON object that contains: <ul style="list-style-type: none"> • message • feedback • feedback_category • feedback_details • datamodel_name • utterance 	"category": "GenAI"
• message	Description of the user-feedback action. For example, AI Assistant feedback marked as positive or negative.	"message": "GenAI:Assistant - Negative Feedback"

Field	Description	Example
• feedback	Type of user feedback for an AI generated response. Either positive or negative.	"feedback" : "negative"
• feedback_category	Reason for negative feedback. For example, incorrect answer, incomplete response, or unclear result.	"feedback_category" : "incorrect_answer"
• feedback_details	Free-text comment entered by the user to explain their feedback choice.	"feedback_details" : "wanted a map visualization"
• datamodel_name	Dataset or semantic model used by the AI request.	"datamodel_name" : "US Wind Turbines"
• utterance	Exact natural-language question or instruction entered by the user.	"utterance" : "show me the total number of turbines"
oracle	JSON object that contains: <ul style="list-style-type: none"> • compartmentid • ingestedtime • loggroupid • logid • tenantid 	See examples: <ul style="list-style-type: none"> • Sample Analytics Cloud Audit Log - Create Snapshot (MyFirstSnapshot) • Sample Analytics Cloud Audit Log - Update Workbook (Worklife Balance)
• compartmentid	OCID of the compartment that the log group belongs to in the format <code>ocid1.compartment.oc1.<unique_ID></code> .	<code>ocid1.compartment.oc1..aaaaaa111111bbbbbb222222cccc333333ddddd444444eeeeee555555</code>
• ingestedtime	The time the log was captured by Oracle Cloud Infrastructure Logging, in RFC 3339 timestamp format.	<code>2022-08-16T11:01:01.507Z</code>
• loggroupid	OCID of the log group that contains the log in the format <code>ocid1.loggroup.oc1.<region_ID>.<unique_ID></code> .	<code>ocid1.loggroup.oc1.me-dubai-1.aaaa1111bbbb3333cccc4444ddd5555eeee6666fff7777gggg8888hhhh</code>
• logid	OCID of the service log object in the format <code>ocid1.log.oc1.<region_ID>.<unique_ID></code> .	<code>ocid1.log.oc1.me-dubai-1.aaaa1111bbbb3333jjjj4444kkkk555511116666mmmm7777nnnn8888oooo</code>
• tenantid	OCID of the tenancy in the format <code>ocid1.tenancy.oc1.<region_ID>.<unique_ID></code> .	<code>ocid1.tenancy.oc1..aaaaaaaa1111111111111111bbbbbbbbb222222222222cccccccc3333333333</code>

Field	Description	Example
source	Display name for the Oracle Analytics Cloud instance.	oacdemo1
specversion	OCI logging schema version.	1.0
time	The time the log was created at the source, in RFC 3339 timestamp format.	2021-07-10T16:15:59.469Z
type	The log category type (audit or diagnostic). Possible values: <ul style="list-style-type: none"> audit diagnostic 	com.oraclecloud.analytics.analyticsinstance.audit OR com.oraclecloud.analytics.analyticsinstance.diagnostic

Sample Audit and Diagnostic Logs

Here are some examples of audit and diagnostic logs generated by Oracle Analytics Cloud.

- Audit Log - Create Snapshot (MyFirstSnapshot)
- Audit Log - Update Workbook (Worklife Balance)
- Diagnostic Log - Query Detail
- Diagnostic Log - Physical Query Summary

Sample Analytics Cloud Audit Log - Create Snapshot (MyFirstSnapshot)

```
{
  "datetime": 1660647631611,
  "logContent": {
    "data": {
      "additionalDetails": {
        "snapshotSizeInBytes": "948999",
        "source": "console"
      },
      "category": "snapshot",
      "ecid": "aaaaaaaa-1111-bbbb-2222-cccccc333333-ddddd4444",
      "logLevel": "info",
      "message": "Snapshot 'MyFirstSnapshot' created.",
      "userId": "aa11bb22cc33dd44ee55ff66gg77hh88",
      "ipAddress": "192.168.1.1"
    },
    "id": "11111111-aaaa-2222-bbbb-333333cccccc",
    "oracle": {
      "compartmentid":
"ocid1.tenancy.oc1..aaaaa111111bbbbbb222222cccccc333333dddddd444444eeeeee5555"
```

```

55",
    "ingestedtime": "2022-08-16T11:01:01.507Z",
    "loggroupid": "ocid1.loggroup.oc1.me-
dubai-1.aaaa1111bbbb3333cccc4444dddd5555eeee6666ffff7777gggg8888hhhh",
    "logid": "ocid1.log.oc1.me-
dubai-1.aaaa1111bbbb3333jjjj4444kkkk555511116666mmmm7777nnnn8888oooo",
    "tenantid":
"ocid1.tenancy.oc1..aaaaaaaaa1111111111bbbbbbbbb2222222222cccccccccc33333333
33"
  },
  "source": "MyOACInstance",
  "specversion": "1.0",
  "time": "2022-08-16T11:00:31.611Z",
  "type": "com.oraclecloud.analytics.analyticsinstance.audit"
}
}

```

Sample Analytics Cloud Audit Log - Update Workbook (Worklife Balance)

```

{
  "datetime": 1661186013000,
  "logContent": {
    "data": {
      "additionalDetails": {
        "path": "/users/john.smith@example.com/Worklife Balance",
        "type": "data visualization workbook"
      },
      "category": "catalog",
      "ecid": "aaaaaaaa-1111-bbbb-2222-cccccc333333-dddd4444",
      "logLevel": "info",
      "message": "Data Visualization Workbook (Worklife Balance) properties
updated.",
      "userId": "aa11bb22cc33dd44ee55ff66gg77hh88",
      "ipAddress": "192.168.1.1"
    },
    "id": "11111111-aaaa-2222-bbbb-333333cccc",
    "oracle": {
      "compartmentid":
"ocid1.tenancy.oc1..aaaaa1111111111bbbbbbbbb2222222222cccccc3333333333ddddd44444444eeeeee5555
55",
      "ingestedtime": "2022-08-16T11:01:01.507Z",
      "loggroupid": "ocid1.loggroup.oc1.me-
dubai-1.aaaa1111bbbb3333cccc4444dddd5555eeee6666ffff7777gggg8888hhhh",
      "logid": "ocid1.log.oc1.me-
dubai-1.aaaa1111bbbb3333jjjj4444kkkk555511116666mmmm7777nnnn8888oooo",
      "tenantid":
"ocid1.tenancy.oc1..aaaaaaaaa1111111111bbbbbbbbb2222222222cccccccccc33333333
33"
    },
    "source": "MyOACInstance",
    "specversion": "1.0",
    "time": "2022-08-16T11:00:31.611Z",
    "type": "com.oraclecloud.analytics.analyticsinstance.audit"
  }
}
}

```


- **Resource Compartment:** Select the compartment containing the Oracle Analytics Cloud instance you want to collect logs for.
- **Service:** Select **Analytics Cloud**.
- **Resource:** Select the Oracle Analytics Cloud instance.
- **Log Category:** Select either **Audit Logs** or **Diagnostic Logs**.
- **Log Name:** Enter a name for the log.

Enable resource log

For more information about service logs, see [documentation](#).

Select resource

Resource compartment
analytics-instances

Service
Analytics Cloud

Resource
analyticsinstance01

Configure log

Log category
Audit Logs

Log name
MyOACLogs

Enable auto archiving to object storage (legacy)

> **Advanced options**

- Optional: Click **Show Advanced Options** to change the default log location and retention period.

By default, logs are retained for 1 month.

▼ **Advanced options**

Log location

Compartment
analytics-instances

Log group
MyOACLogs

Log retention

Log retention
1 month (default) (30 days)

- Click **Enable Log**.

The **Status** field changes from **Creating** to **Active** when the log set up is complete.

You can explore, search, and monitor log events in the Explore Log panel.

- Click the **Explore log** tab, then select **Edit** to specify the time range you want to display event logs for and click **Update**. For example, **Past hour**.

Monitor Instance Event Logs

Oracle Cloud Infrastructure logs API operations on Oracle Analytics Cloud instances for audit purposes. You can view the audit logs for Oracle Analytics Cloud API operations from the **Audit** page.

Note

Required IAM Policy - Audit page

You must be assigned to a security policy that allows you to read audit events.

Verb: read

Resource Types: audit-events

Example: For example, if you have an IAM user group called `AnalyticsServiceAdmins`, you might want to allow this group to view audit logs for the whole tenancy or for a particular compartment.

```
allow group AnalyticsServiceAdmins to read audit-events in tenancy
```

```
allow group AnalyticsServiceAdmins to read audit-events in compartment  
MyEnterpriseAnalytics
```

To learn more, see [Overview of Audit](#).

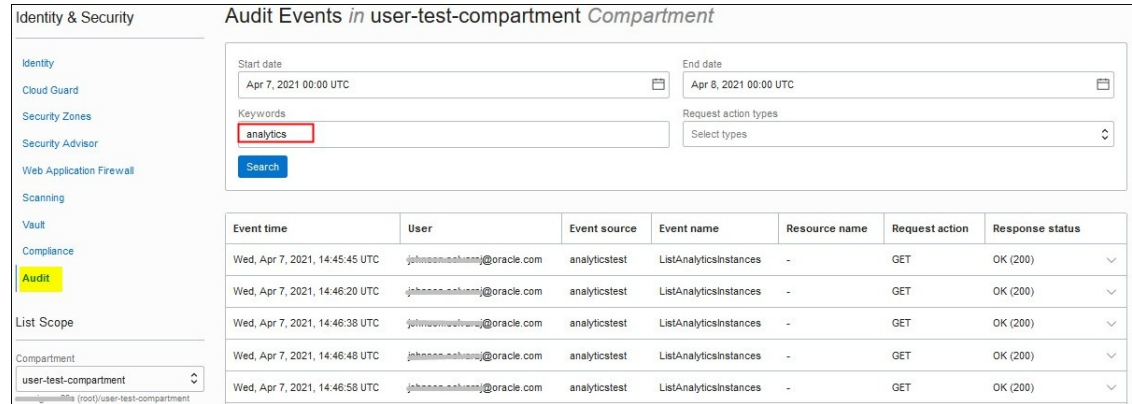
About Oracle Analytics Cloud Instance Events

From the **Audit** page, you can view audit logs such as:

- ListAnalyticsInstances
- CreateAnalyticsInstance
- GetAnalyticsInstance
- UpdateAnalyticsInstance
- DeleteAnalyticsInstance
- StartAnalyticsInstance
- StopAnalyticsInstance
- ScaleAnalyticsInstance
- ChangeAnalyticsInstanceCompartment
- ListWorkRequests
- GetWorkRequest
- DeleteWorkRequest
- ListWorkRequestErrors
- ListWorkRequestLogs

Access Oracle Analytics Cloud Instance Event Logs

To open the Audit page, navigate to **Identity & Security**, click **Audit**, and select the compartment you want. You can filter the log to audit a particular Oracle Analytics Cloud operation, such as `ListAnalyticsInstances` or `StopAnalyticsInstance`, by entering the name of the operation in the **Keyword** field. You can also filter by date or API operation (POST, DELETE, PUT, and so on).



Event time	User	Event source	Event name	Resource name	Request action	Response status
Wed, Apr 7, 2021, 14:45:45 UTC	johnsonjohnson@oracle.com	analyticstest	ListAnalyticsInstances	-	GET	OK (200)
Wed, Apr 7, 2021, 14:46:20 UTC	johnsonjohnson@oracle.com	analyticstest	ListAnalyticsInstances	-	GET	OK (200)
Wed, Apr 7, 2021, 14:46:38 UTC	johnsonjohnson@oracle.com	analyticstest	ListAnalyticsInstances	-	GET	OK (200)
Wed, Apr 7, 2021, 14:46:48 UTC	johnsonjohnson@oracle.com	analyticstest	ListAnalyticsInstances	-	GET	OK (200)
Wed, Apr 7, 2021, 14:46:58 UTC	johnsonjohnson@oracle.com	analyticstest	ListAnalyticsInstances	-	GET	OK (200)

Find Oracle Analytics Cloud Resources

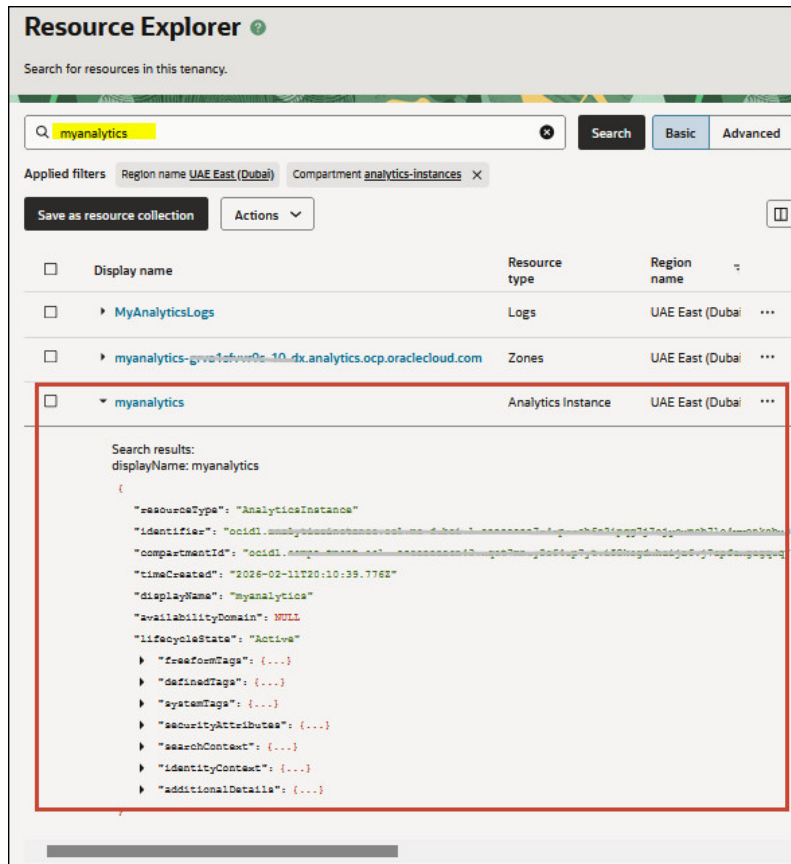
You can use the simple and advanced search features in Oracle Cloud Infrastructure Console to find Oracle Analytics Cloud instances across compartments in your tenancy.

Simple Search

If you know the name of the resource you're looking for, enter all or part of the name in the search bar. For example, `myanalytics`.

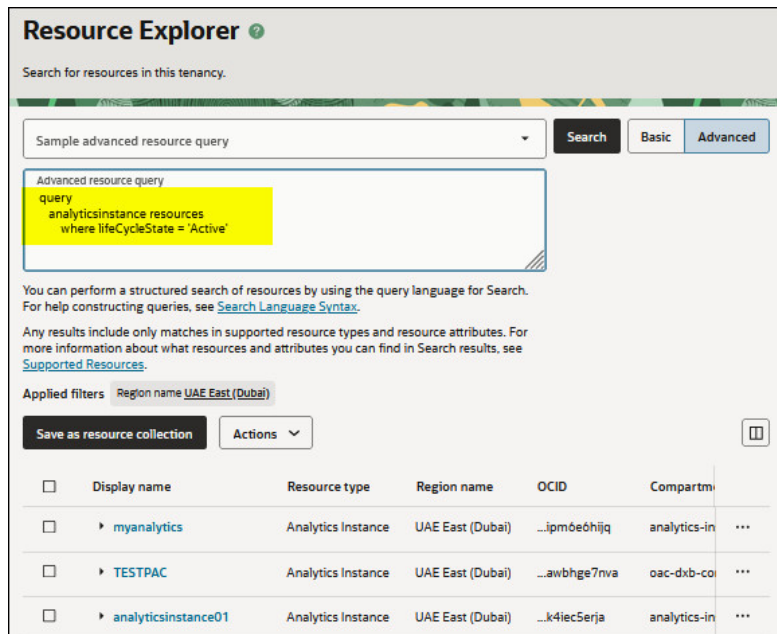


Results matching your search display. If you don't find what you're looking for, or you want to perform more sophisticated searches, click **Advanced resource query**.



Advanced Search

You can enter advanced search queries to search for Oracle Analytics Cloud instances. Click **Advanced Search**, then either select one of the predefined, sample queries or enter one of your own.



For example:

- To find all the Oracle Analytics Cloud instances in your tenancy:

```
query
  analyticsinstance resources
```

- To find all the Oracle Analytics Cloud instances that are tagged with the term "test":

```
query
  analyticsinstance resources
  where
    (freeformTags.key = 'Environment' && freeformTags.value = 'test')
```

- To find all the Oracle Analytics Cloud instances that are currently up and running normally (active):

```
query
  analyticsinstance resources
  where lifeCycleState = 'ACTIVE'
```

To learn more, see [Overview of Search](#).

Read Cost Reports

A cost report is a comma-separated value (CSV) file that gives you a detailed breakdown of the Oracle Analytics Cloud resources that you use in Oracle Cloud Infrastructure, for audit or invoice reconciliation. You can use the information in your cost reports to help you optimize your Oracle Cloud Infrastructure spending and make more informed cloud spending decisions. You must be assigned to a security policy that allows you to read cost reports.

For example, if you have an OCI user group called `AnalyticsServiceAdmins`, you might want to allow this group to read cost reports.

The policy statement will look like this:

```
define tenancy usage-report as
ocid1.tenancy.oc1..aaaaaaaaned4fkpkisbwjlr56u7cj631f3wffbilvqknstgtvzub7vhqkkgg
q
endorse group AnalyticsServiceAdmins to read objects in tenancy usage-report
```

To learn more, see [How Cost Reports Work](#) and [Accessing Cost Reports](#).

Analyze Costs for Oracle Analytics Cloud

You can analyze the cost of the Oracle Analytics Cloud instances you're using in the **Cost Analysis** page. Cost Analysis is an easy-to-use visualization tool to help you track and optimize your Oracle Cloud Infrastructure spending.

The way you're billed for a particular instance depends which edition you subscribe to (Professional or Enterprise) and whether you have an Oracle Cloud subscription or a Bring Your Own License (BYOL) subscription:

- Oracle Analytics Cloud - Professional - OCPU Per Hour
- Oracle Analytics Cloud - Professional - Users Per Month
- Oracle Analytics Cloud - Professional - BYOL - OCPU Per Hour

- Oracle Analytics Cloud - Enterprise - OCPU Per Hour
- Oracle Analytics Cloud - Enterprise - Users Per Month
- Oracle Analytics Cloud - Enterprise - BYOL - OCPU Per Hour

Note

You might incur additional costs if you decide to use other Oracle Cloud Infrastructure services with Oracle Analytics Cloud. For example, services such as Object Storage (to store snapshots, pixel-perfect reports, OCI Vision artifacts, and so on), Email Delivery (to send emails), Logging (to store usage and diagnostic logs). See <https://www.oracle.com/cloud/price-list>.

You must be assigned to a security policy that allows you to read cost information. For example, if you have an Oracle Cloud Infrastructure user group called `AnalyticsServiceAdmins`, you might want to allow this group to see cost information.

The policy statement will look like this:

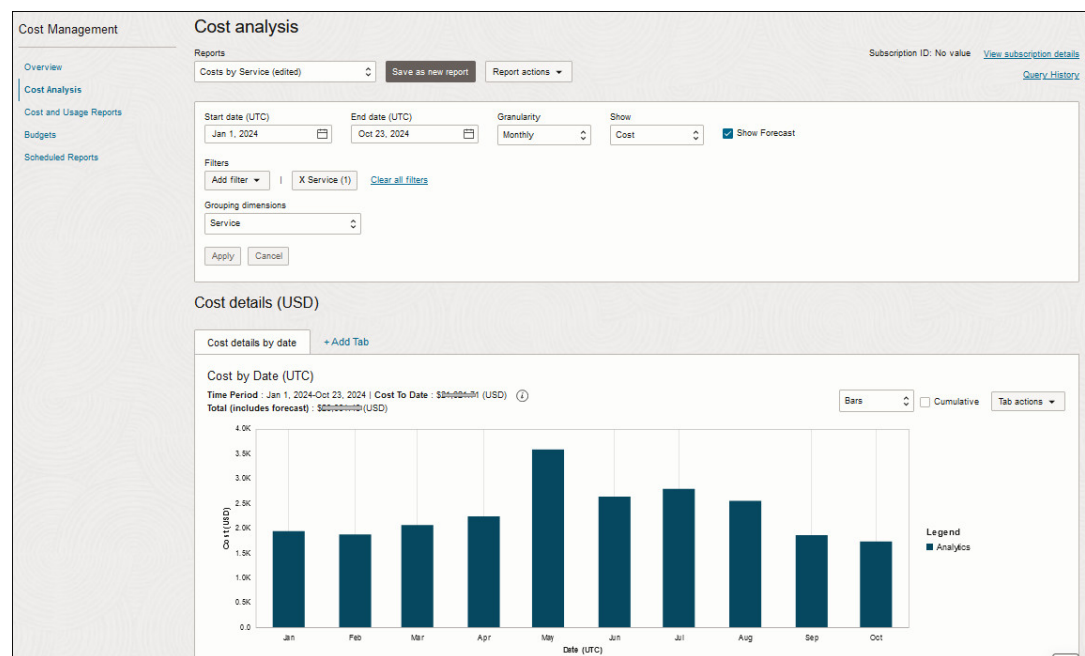
```
allow group AnalyticsServiceAdmins to read usage-reports in tenancy
```

To open the **Cost Analysis** page:

1. In Oracle Cloud Infrastructure Console, navigate to **Billing and Cost Management**, and click **Cost Analysis**.

By default, costs for all the services you use are displayed.

2. To view only costs for Oracle Analytics Cloud, click **Add filter**, select **Service**, and then **ANALYTICS_CLOUD**.



3. Customize dates, filters, and other settings as required.

To learn more, see [Checking Your Expenses and Usage](#).


Verify Update Cycle

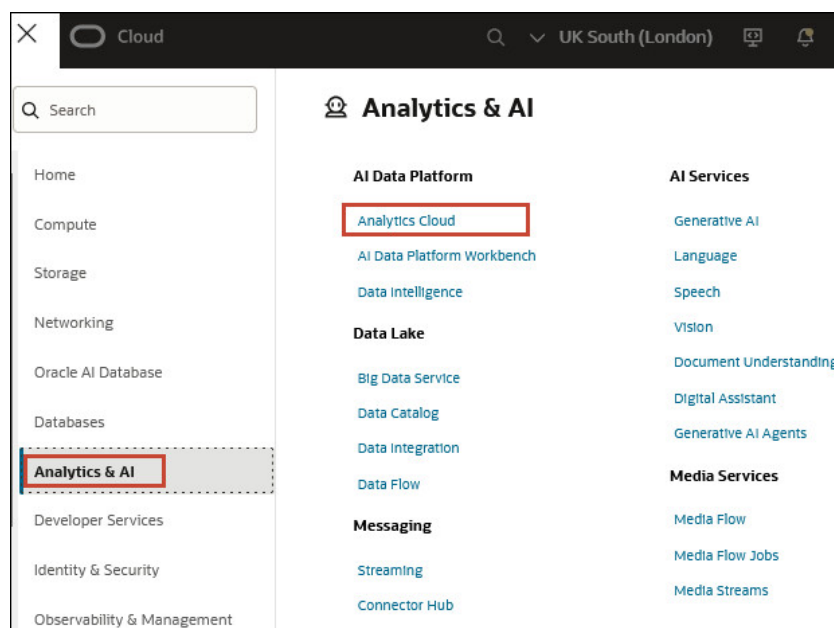
When you set up Oracle Analytics Cloud, you select an update cycle that's appropriate for your environment (either **Early** or **Regular**). You can review your selection from the Instance Details page.

Update Cycle	Description
Early	Oracle delivers updates as soon as they're available. If you manage multiple Oracle Analytics Cloud environments, early access gives you the flexibility to explore new features and stagger updates between environments.
Regular	(Default) Oracle delivers updates a few weeks after completing the early update cycle. If you manage multiple Oracle Analytics Cloud environments on the regular update cycle, Oracle will share the <i>actual date</i> of software updates for each environment in your software update notification.

Note

You can't switch from the early rollout cycle to the regular rollout cycle (or the other way around). The update cycle you select is permanent and you can't change it. If your needs change, you must create a new service instance with the desired update cycle and migrate your content to the new service.

1. Sign in to your Oracle Cloud account.
2. In Oracle Cloud Infrastructure Console, click  in the top left corner.
3. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.



4. Select the compartment that contains your Oracle Analytics Cloud instance.
5. Click the name of the instance you want to review update cycle details for.
The **Update Cycle** is displayed on the Details page.

The screenshot displays the 'Details' page for an Oracle Analytics Cloud instance. The instance is named 'myanalytics' and is in an 'Active' state. The page is titled 'My Analytics Instance in London' and has a navigation bar with tabs for 'Details', 'Monitoring', 'Networking', 'Work Requests', and 'Tags'. The 'Details' tab is selected. The page content is organized into a 'General information' section with the following fields:

OCID	...vipm0e6hijq	Copy
Compartment	analytics-instances	
Created	Feb 11, 2026, 20:10:39 UTC	
Capacity	2 OCPUs	
Edition	Enterprise Edition	
License	Bring Your Own License (BYOL)	
Update Cycle	Regular Second rollout cycle, scheduled a few weeks after the first rollout.	
Encryption Key	Oracle-managed key	Assign

5

Manage Service Access and Security

As administrator, you manage access to your Oracle Analytics Cloud environment for your organization using security features in Oracle Cloud Infrastructure and Oracle Identity Cloud Service.

Topics

- [Give Users Permissions to Manage Analytics Cloud Instances](#)
- [Give Data Sources Access to Analytics Cloud Instances](#)
- [Deploy Oracle Analytics Cloud with a Private Endpoint](#)
- [Connect to Private Sources Through a Private Access Channel](#)
- [Use Network Security Groups to Control Access](#)
- [Federate with Oracle Identity Cloud Service Manually](#)
- [Set Up a Custom Vanity URL](#)
- [Encrypt Sensitive Information](#)

Give Users Permissions to Manage Analytics Cloud Instances

You can give other users permissions to manage Oracle Analytics Cloud instances through security policies.

Topics

- [About Permissions to Manage Oracle Analytics Cloud Instances](#)
- [Example Policy Statements to Manage Analytics Cloud Instances](#)
- [Set Up Policies \(Identity Domains\)](#)
- [Set Up Policies \(Federated Oracle Identity Cloud Service\)](#)

About Permissions to Manage Oracle Analytics Cloud Instances

You use authorization policies to control access to resources in your tenancy. For example, you can create a policy that authorizes users to create and manage Oracle Analytics Cloud instances.

You create policies using the Oracle Cloud Infrastructure Console. For detailed information, see [Managing Policies](#).

Resource Types for Oracle Analytics Cloud

Resource Types	Description
analytics-instance	A single Oracle Analytics Cloud instance.
analytics-instances	One or more Oracle Analytics Cloud instances.

Resource Types	Description
analytics-instance-work-request	A single work request for Oracle Analytics Cloud. Each operation you perform on an Oracle Analytics Cloud instance, creates a work request. For example, operations such as create, start, stop, and so on.
analytics-instance-work-requests	One or more work requests.

Supported Variables

The values of these variables are supplied by Oracle Analytics Cloud. In addition, other general variables are supported. See [General Variables for All Requests](#).

Variable	Type	Description	Sample Value
target.analytics-instance.id	ocid	OCID for the Analytics Cloud instance.	target.analytics-instance.id = 'oci1.analyticsinstance.oc1..abc123'
target.analytics-instance.name	string	Name of the Analytics Cloud instance.	target.analytics-instance.name = 'myanalytics_1'
target.analytics-instance.source-compartment.id	ocid	OCID of the source compartment, in a "move compartment" operation.	target.analytics-instance.source-compartment.id = 'ocid1.compartment.oc1..aaa100'
target.analytics-instance.destination-compartment.id	ocid	OCID of the destination compartment in a "move compartment" operation.	target.analytics-instance.destination-compartment.id = 'ocid1.compartment.oc1..aaa200'

Details for Verb and Resource-Type Combinations

Oracle Cloud Infrastructure offers a standard set of verbs to define permissions across Oracle Cloud Infrastructure resources (**Inspect**, **Read**, **Use**, **Manage**). These tables list the Oracle Analytics Cloud permissions associated with each verb. The level of access is cumulative as you go from **Inspect** to **Read** to **Use** to **Manage**.

INSPECT

Resource- Type	INSPECT Permission
<ul style="list-style-type: none"> analytics-instance analytics-instances 	<ul style="list-style-type: none"> ANALYTICS_INSTANCE_INSPECT
<ul style="list-style-type: none"> analytics-instance-work-request analytics-instance-work-requests 	<ul style="list-style-type: none"> ANALYTICS_INSTANCE_WR_INSPECT

READ

Resource- Type	READ Permission
<ul style="list-style-type: none"> analytics-instance analytics-instances 	<ul style="list-style-type: none"> ANALYTICS_INSTANCE_INSPECT ANALYTICS_INSTANCE_READ

Resource- Type	READ Permission
<ul style="list-style-type: none"> analytics-instance-work-request analytics-instance-work-requests 	<ul style="list-style-type: none"> ANALYTICS_INSTANCE_WR_INSPECT ANALYTICS_INSTANCE_WR_READ

USE

Resource- Type	USE Permission
<ul style="list-style-type: none"> analytics-instance analytics-instances 	<ul style="list-style-type: none"> ANALYTICS_INSTANCE_INSPECT ANALYTICS_INSTANCE_READ ANALYTICS_INSTANCE_USE
<ul style="list-style-type: none"> analytics-instance-work-request analytics-instance-work-requests 	<ul style="list-style-type: none"> N/A

MANAGE

Resource- Type	MANAGE Permission
<ul style="list-style-type: none"> analytics-instance analytics-instances 	<ul style="list-style-type: none"> ANALYTICS_INSTANCE_INSPECT ANALYTICS_INSTANCE_READ ANALYTICS_INSTANCE_USE ANALYTICS_INSTANCE_CREATE ANALYTICS_INSTANCE_DELETE ANALYTICS_INSTANCE_UPDATE ANALYTICS_INSTANCE_MOVE ANALYTICS_INSTANCE_MANAGE
<ul style="list-style-type: none"> analytics-instance-work-request analytics-instance-work-requests 	<ul style="list-style-type: none"> ANALYTICS_INSTANCE_WR_INSPECT ANALYTICS_INSTANCE_WR_READ ANALYTICS_INSTANCE_WR_DELETE

Permissions Required for Each API Operation

This table shows the API operations available for Oracle Analytics Cloud, grouped by resource type.

REST API Operation	CLI Command Operation	Permission Required to Use the Operation
ListAnalyticsInstances	analytics-instance list	ANALYTICS_INSTANCE_INSPECT
CreateAnalyticsInstance	analytics-instance create	ANALYTICS_INSTANCE_CREATE
GetAnalyticsInstance	analytics-instance get	ANALYTICS_INSTANCE_READ
UpdateAnalyticsInstance	analytics-instance update	ANALYTICS_INSTANCE_UPDATE
DeleteAnalyticsInstance	analytics-instance delete	ANALYTICS_INSTANCE_DELETE
StartAnalyticsInstance	analytics-instance start	ANALYTICS_INSTANCE_USE
StopAnalyticsInstance	analytics-instance stop	ANALYTICS_INSTANCE_USE
ScaleAnalyticsInstance	analytics-instance scale	ANALYTICS_INSTANCE_MANAGE
ChangeAnalyticsInstanceCompartment	analytics-instance change-compartment	ANALYTICS_INSTANCE_MOVE

REST API Operation	CLI Command Operation	Permission Required to Use the Operation
ChangeAnalyticsInstanceNetworkEndpoint	analytics-instance change-network-endpoint	ANALYTICS_INSTANCE_MANAGE
GetPrivateAccessChannel	analytics-instance get-private-access-channel	ANALYTICS_INSTANCE_MANAGE
CreatePrivateAccessChannel	analytics-instance create-private-access-channel	ANALYTICS_INSTANCE_MANAGE
UpdatePrivateAccessChannel	analytics-instance update-private-access-channel	ANALYTICS_INSTANCE_MANAGE
DeletePrivateAccessChannel	analytics-instance delete-private-access-channel	ANALYTICS_INSTANCE_MANAGE
CreateVanityUrl	analytics-instance create-vanity-url	ANALYTICS_INSTANCE_MANAGE
UpdateVanityUrl	analytics-instance update-vanity-url	ANALYTICS_INSTANCE_MANAGE
DeleteVanityUrl	analytics-instance delete-vanity-url	ANALYTICS_INSTANCE_MANAGE
SetKmsKey	analytics-instance set-kms-key	ANALYTICS_INSTANCE_MANAGE
ListWorkRequests	work-request list	ANALYTICS_INSTANCE_WR_INSPECT
GetWorkRequest	work-request get	ANALYTICS_INSTANCE_WR_READ
DeleteWorkRequest	work-request delete	ANALYTICS_INSTANCE_WR_DELETE
ListWorkRequestErrors	work-request-error list	ANALYTICS_INSTANCE_WR_INSPECT
ListWorkRequestLogs	work-request-log list	ANALYTICS_INSTANCE_WR_INSPECT

Example Policy Statements to Manage Analytics Cloud Instances

Here are typical policy statements that you might use to authorize access to Oracle Analytics Cloud instances.

When you create a policy for your tenancy, you grant users access to all compartments by way of [policy inheritance](#). Alternatively, you can restrict access to individual Oracle Analytics Cloud instances or compartments.

Let users in the Administrators group fully manage any Analytics instance

```
# Full manage permissions (Create, View, Update, Delete, Scale, Start, Stop...)
allow group Administrators to manage analytics-instances in tenancy
allow group Administrators to manage analytics-instance-work-requests in tenancy
```

Let users in the analytics_power_users group read, start, and stop all Analytics instances in compartment MyOACProduction

```
# Use permissions (List, Get, Start, Stop)
allow group analytics_power_users to use analytics-instances in compartment
MyOACProduction
```

Let users in the analytics_test_users group create and manage a single Analytics instance (myanalytics_1) in compartment MyOACTest

```
# Full manage permissions on a single instance
allow group analytics_test_users to manage analytics-instances in compartment
MyOACTest where target.analytics-instances.name = 'myanalytics_1'
```

Let users in the analytics_power_users group move Analytics instances between two named compartments

```
# Custom permissions to move instances between two specific compartments.
allow group analytics_power_users to {ANALYTICS_INSTANCE_INSPECT,
ANALYTICS_INSTANCE_READ, ANALYTICS_INSTANCE_MOVE} in tenancy
where all {
    target.analytics-instance.source-compartment.id =
    'ocidl.compartment.oc1..aaa100',
    target.analytics-instance.destination-compartment.id =
    'ocidl.compartment.oc1..aaa200'
}
```

Let users in the analytics_users group inspect any Analytics instance and their associated work requests

```
# Inspect permissions (list analytics instances and work requests) using
metaverbs.
allow group analytics_users to inspect analytics-instances in tenancy
allow group analytics_users to inspect analytics-instance-work-requests in
tenancy
```

```
# Inspect permissions (list analytics instances and work requests) using
permission names.
allow group analytics_users to {ANALYTICS_INSTANCE_INSPECT} in tenancy
allow group analytics_users to {ANALYTICS_INSTANCE_WR_INSPECT} in tenancy
```

Let users in the analytics_users2 group read details about any Analytics instance and their associated work requests

```
# Read permissions (read complete analytics instance and work request
metadata) using metaverbs.
allow group analytics_users2 to read analytics-instances in tenancy
```

```
allow group analytics_users2 to read analytics-instance-work-requests in
tenancy
```

```
# Read permissions (read complete analytics instance and work request
metadata) using permission names.
allow group analytics_users2 to {ANALYTICS_INSTANCE_INSPECT,
ANALYTICS_INSTANCE_READ} in tenancy
allow group analytics_users2 to {ANALYTICS_INSTANCE_WR_INSPECT,
ANALYTICS_INSTANCE_WR_READ} in tenancy
```

Let users in the analytics_users2 group view performance metrics for any Analytics instance in a named compartment

```
# View performance metrics permissions
allow group analytics_users2 to read metrics in compartment myOACProduction
```

Let users in the analytics_power_users2 group read, start, and stop all Analytics instances and read their associated work requests

```
# Use permissions (read, stop, start on analytics instance, read on work
request) using metaverbs.
allow group analytics_power_users2 to use analytics-instances in tenancy
allow group analytics_power_users2 to read analytics-instance-work-requests
in tenancy
```

```
# Use permissions (read, stop, start on analytics instance, read on work
request) using permission names.
```

```
allow group
    analytics_power_users2 to {ANALYTICS_INSTANCE_INSPECT,
ANALYTICS_INSTANCE_READ, ANALYTICS_INSTANCE_USE} in
    tenancy
allow group
    analytics_power_users2 to {ANALYTICS_INSTANCE_WR_INSPECT,
ANALYTICS_INSTANCE_WR_READ} in
    tenancy
```

Let users in the Administrators2 group manage any Analytics instance and their associated work requests

```
# Full manage permissions (use, scale, delete on analytics instance, read and
cancel on work request) using metaverbs.
allow group Administrators2 to manage analytics-instances in tenancy
```

```

allow group Administrators2 to manage analytics-instance-work-requests in
tenancy

# Full manage permissions (use, create, scale, delete on analytics instance,
read and cancel on work request) using permission names.

allow group
  Administrators2 to
    {ANALYTICS_INSTANCE_INSPECT, ANALYTICS_INSTANCE_READ,
ANALYTICS_INSTANCE_USE,
    ANALYTICS_INSTANCE_CREATE, ANALYTICS_INSTANCE_DELETE,
ANALYTICS_INSTANCE_UPDATE,
    ANALYTICS_INSTANCE_MOVE, ANALYTICS_INSTANCE_MANAGE} in
  tenancy

allow group
  Administrators2 to
    {ANALYTICS_INSTANCE_WR_INSPECT, ANALYTICS_INSTANCE_WR_READ,
ANALYTICS_INSTANCE_WR_DELETE} in
  tenancy

```

Set Up Polices (Identity Domains)

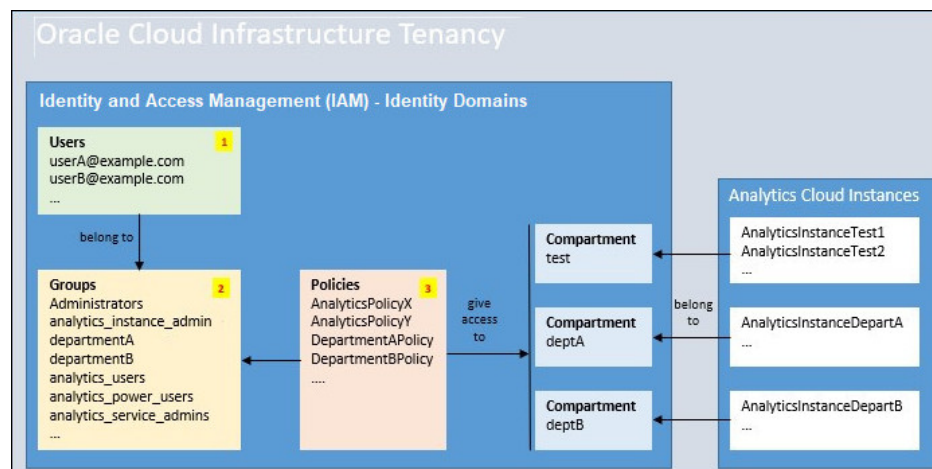
If your cloud account offers identity domains, use Oracle Cloud Infrastructure Identity and Access Management (IAM) to set up users and groups before you set up security policies in Oracle Cloud Infrastructure.

Topics

- [Typical Workflow for Setting Up Policies to Manage Analytics Cloud Instances \(Identity Domains\)](#)
- [Give a User Permissions to Manage Analytics Cloud Instances \(Identity Domains\)](#)

Typical Workflow for Setting Up Policies to Manage Analytics Cloud Instances (Identity Domains)

If you're setting up policies for the first time, take some time to understand what's required before you start.



High-level steps:

1. Use Oracle Cloud Infrastructure Identity and Access Management Identity Domains to create users.
2. Create one or more groups and assign users to each group, as required. Give the groups suitable names. For example, prefix them with `analytics` and use a meaningful naming convention such as: `analytics_instance_admin`, `analytics_service_admins`, `analytics_power_users`, `analytics_users`, and so on.
3. Create one or more policies, as required. Give users in the IAM groups suitable access permissions on compartments and Oracle Analytics Cloud instances.

For more detailed steps, see the next topic.

Give a User Permissions to Manage Analytics Cloud Instances (Identity Domains)

You can create security policies to give users in your IAM identity domain suitable access to Oracle Analytics Cloud instances in Oracle Cloud Infrastructure Console.

1. Sign-in to your cloud account as Cloud Account Administrator.
2. In Oracle Cloud Infrastructure Console, navigate to **Identity & Security**. Under **Identity**, click **Domains** to add one or more users. See [Managing Users](#).
3. In **Domains**, add one or more groups. See [Managing Groups](#).

For example, if you're creating a policy that gives another user permissions to fully manage Oracle Analytics Cloud instances you might name the group `analytics_instance_admin` (or similar) and include a short description such as *"Users with permissions to set up and manage Oracle Analytics Cloud instances"* (or similar).

4. In **Domains**, assign users to one or more groups. See [Adding Users to a Group](#).
5. Create a policy that gives users belonging to group, specific access permissions to Oracle Analytics Cloud instances or compartments.
 - a. Navigate to **Identity & Security**. Under **Identity**, click **Policies**.
 - b. Select a compartment, and click **Create Policy**.

For details and examples, see [About Permissions to Manage Oracle Analytics Cloud Instances](#) and [Example Policy Statements to Manage Analytics Cloud Instances](#).

Users belonging to any groups mentioned in the policy statement get their new permission when they next sign in to the Console.

Set Up Policies (Federated Oracle Identity Cloud Service)

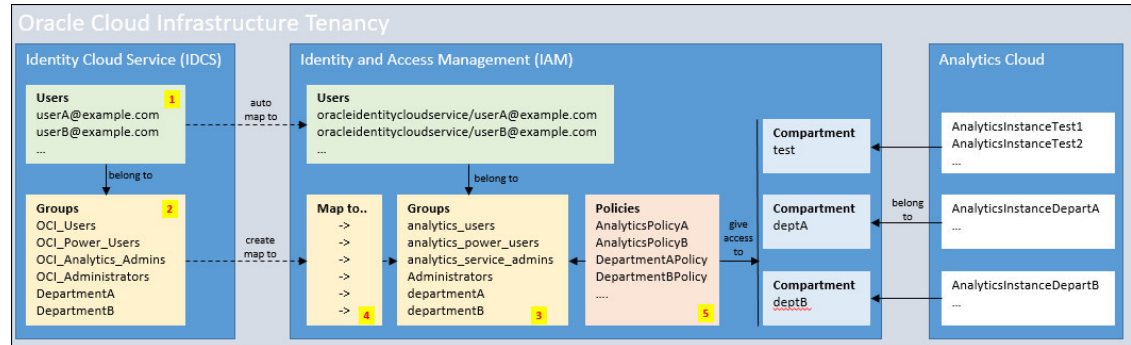
If your cloud account federates with Oracle Identity Cloud Service, you need to map your users and groups in Oracle Identity Cloud Service to users and groups in Oracle Cloud Infrastructure Identity and Access Management (IAM) before you set up policies in Oracle Cloud Infrastructure.

Topics

- [Typical Workflow to Set Up Policies to Manage Analytics Cloud Instances \(Oracle Identity Cloud Service\)](#)
- [Give a User Permissions to Manage Analytics Cloud Instances \(Identity Domains\)](#)

Typical Workflow to Set Up Policies to Manage Analytics Cloud Instances (Oracle Identity Cloud Service)

If your cloud account federates with Oracle Identity Cloud Service and you're setting up policies for the first time, take some time to understand what's required before you start.



High-level steps:

1. Create users in the federated Oracle Identity Cloud Service (IDCS).
2. Create one or more groups and assign users to each group, as required. Give the groups suitable names and include only those users that you want to manage Oracle Analytics Cloud instances in Oracle Cloud Infrastructure (Gen 2). For example, prefix them with `OCI` and indicate the level of access for users in the group: `OCI_Users`, `OCI_Power_Users`, `OCI_Analytics_Admins`, and so on.
3. Create groups in Oracle Cloud Infrastructure (OCI). Give the groups suitable names. For example, prefix them with `analytics` and mirror the naming convention that you used in Oracle Identity Cloud Service: `analytics_users`, `analytics_power_users`, `analytics_service_admins`, and so on.
4. Map the groups you created in OCI to the groups in Oracle Identity Cloud Service.
5. Create one or more policies, as required. Give users in OCI groups suitable access permissions to compartments and Oracle Analytics Cloud instances.

For more detailed steps, see the next topic.

Give a User in Oracle Identity Cloud Service Permissions to Manage Analytics Cloud Instances

You can create security policies to give users in Oracle Identity Cloud Service suitable access to Oracle Analytics Cloud instances in Oracle Cloud Infrastructure Console.

1. Sign-in to your cloud account as Cloud Account Administrator.
2. Navigate to the federated Oracle Identity Cloud Service.
 - a. Click **Identity & Security**. Under **Identity**, click **Federation**.
 - b. Click the link to your **Oracle Identity Cloud Service Console**.
3. In Oracle Identity Cloud Service, add one or more users.
 - a. In the **Users** section, click **Add a User**.
 - b. Enter details about the user, and click **Finish**.

4. In Oracle Identity Cloud Service, create one or more groups and assign users to the appropriate group.
 - a. Click **Groups** in the Navigator, and then click **Add**.
 - b. Enter details about the group, and click **Next**.

For example, if you're creating a policy that gives users permissions to fully manage Oracle Analytics Cloud instances you might name the group *OCI_Analytics_Admins* (or similar) and include a short description such as "Users with permissions to set up and manage Oracle Analytics Cloud instances on Oracle Cloud Infrastructure" (or similar).
 - c. Add one or more users to the group.
5. In Oracle Cloud Infrastructure Console, create an OCI group that corresponds to each of the groups you created in Oracle Identity Cloud Service.
 - a. Click **Identity & Security**. Under **Identity**, click **Groups**.
 - b. Click **Create Group**.
 - c. Enter details about the group.

For example, if you're creating a policy that gives users permissions to fully manage Oracle Analytics Cloud instances you might name the group *analytics_service_admin* (or similar) and include a short description such as "Users with permissions to set up and manage Oracle Analytics Cloud instances on Oracle Cloud Infrastructure" (or similar).
6. Map OCI groups to the corresponding groups in Oracle Identity Cloud Service.
 - a. Click **Identity & Security**. Under **Identity**, click **Federation**.
 - b. Navigate to your Oracle Identity Cloud Service federation.

For most tenancies, the federation is named *OracleIdentityCloudService*.
 - c. Click **Add Mapping** and select the name of a group you created in Oracle Identity Cloud Service. For example, *OCI_Analytics_Admins*.
 - d. Select the OCI group you want to map to. For example, *analytics_service_admin*.
7. Create a policy that gives users belonging to an OCI group, specific access permissions to Oracle Analytics Cloud instances or compartments.
 - a. Click **Identity & Security**. Under **Identity**, click **Policies**.
 - b. Select a compartment, and click **Create Policy**.

For details and examples, see [About Permissions to Manage Oracle Analytics Cloud Instances](#) and [Example Policy Statements to Manage Analytics Cloud Instances](#) .

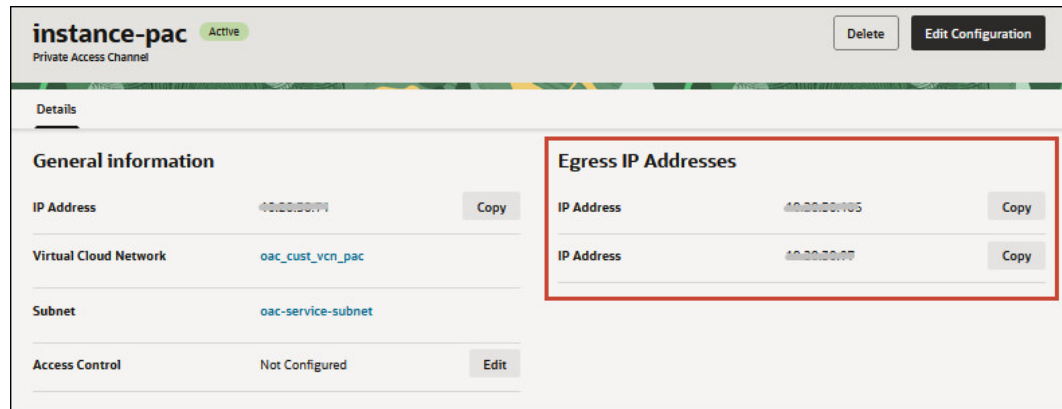
Users belonging to any groups mentioned in the policy statement get their new permission when they next sign in to the Console.

Give Data Sources Access to Analytics Cloud Instances

You can connect Oracle Analytics Cloud to a wide range of data sources. Some data sources, such as Oracle Autonomous AI Lakehouse, require you to include the IP address of your Oracle Analytics Cloud instance in their allowlist.

Topics:

- [Find the IP Address or Host Name of Your Oracle Analytics Cloud Instance](#)



Add the IP Address of Your Oracle Analytics Cloud Instance to Allowlists

Before you try to connect Oracle Analytics Cloud to an Oracle Cloud database, ask the database administrator to add the **Gateway IP Address** (or address range) for your Oracle Analytics Cloud instance to the target database's allowlist. The database administrator must add a security rule on the target Oracle Cloud database that allows TCP/IP traffic from Oracle Analytics Cloud on a specific database port.

This topic describes how to add Oracle Analytics Cloud to the allowlist for an Oracle Cloud database. If you want to connect to other data sources, follow similar steps, as required.

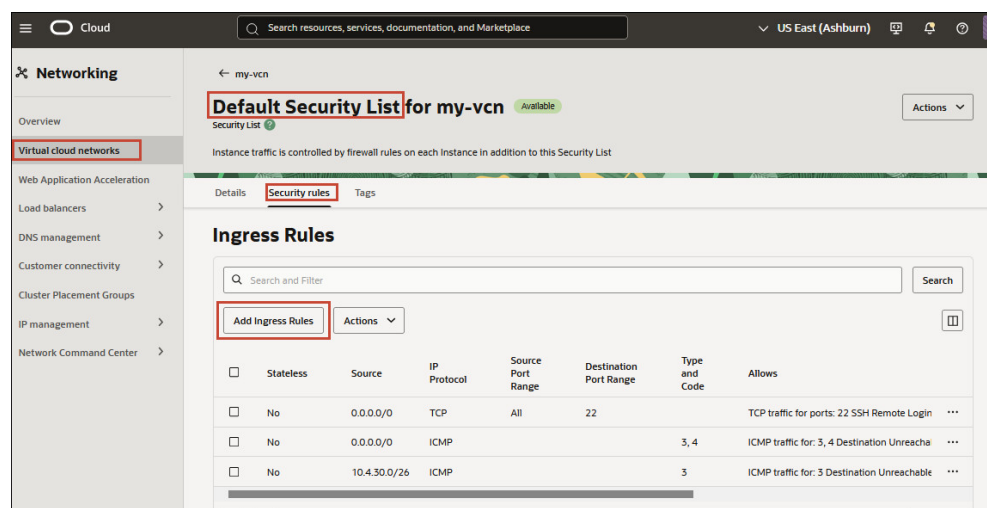
1. Make a note of the Gateway IP Address of your Oracle Analytics Cloud instance or the Egress IP address of the private access channel that you or your database administrator must allow access to.

See Find the IP Address or Host Name of Your Oracle Analytics Cloud Instance.

2. Include the Gateway IP Address that you made a note of in Step 1 in the security list for your Oracle Cloud database.

The way you register the IP address of your Oracle Analytics Cloud instance depends on whether the database you're trying to connect to is deployed on Oracle Cloud Infrastructure or Oracle Cloud Infrastructure Classic:

- **Database on Oracle Cloud Infrastructure**
 - a. Add an ingress rule.



- b. Specify the IP address in the **SOURCE CIDR** field.

- **Database on Oracle Cloud Infrastructure Classic**

- a. Add an access rule.

Status	Rule Name	Source	Destination	Ports	Protocol	Description	Rule Type	Actions
	TestPortASH	130.35.0.0/16	DB_1	1521	TCP		USER	
	TestPortPHX1	130.35.128.0/17	DB_1	1521	TCP		USER	
	TestPortPHX2	138.1.128.0/17	DB_1	1521	TCP		USER	

- b. Specify the IP address in the field below the **Source** field

Public IP Ranges and Gateway IPs for Oracle Analytics Cloud Instances

If you want to connect Oracle Analytics Cloud with a *public endpoint* to a database in Oracle Cloud, you must add the public gateway IP Address (or IP address range) where your Oracle Analytics Cloud instance is located on Oracle Cloud Infrastructure to the database's allowlist.

The public IP address information that you provide depends on the type of database you want to connect to and whether or not your Oracle Analytics Cloud instance is deployed in the same region as the database.

Database	Oracle Autonomous AI Lakehouse	Oracle Autonomous AI Transaction Processing	Any Other Oracle Cloud Database
Same region as Oracle Analytics Cloud	Allow 240.0.0.0/4	Allow 240.0.0.0/4	Allow the region-specific IP address.
Different region to Oracle Analytics Cloud	Allow the region-specific IP address.	Allow the region-specific IP address.	Allow the region-specific IP address.

Region-Specific Public IP Address Information for Oracle Analytics Cloud

Use Oracle Cloud Infrastructure Console to find the public gateway IP address (or IP address range) of your Oracle Analytics Cloud instance that you or your database administrator must add to the database's allowlist. See [Find the IP Address or Host Name of Your Oracle Analytics Cloud Instance](#).

Alternatively, if you know the region where you deployed your Oracle Analytics Cloud instance, find that region in the table below and make a note of the public IP address information listed in the **IP Address Range** column or the **Gateway IP Address** column.

The security policy enforced by your company or organization determines whether you must provide the IP address ranges or Gateway IP address. If you're not sure, check with your network administrator.

For example, if you deployed your Oracle Analytics Cloud instance in Tokyo, Japan East (ap-tokyo-1) and your company's security policy requires you to provide an IP address range, you add 192.29.39.56/29. Alternatively, if you're required to provide a Gateway IP address, you add 192.29.39.59.

Region Where Oracle Analytics Cloud Deployed	Region Identifier	IP Address Range	Gateway IP Address
Asia Pacific (APAC)			
Australia Southeast (Melbourne)	ap-melbourne-1	192.29.211.152/29	192.29.211.154
Australia East (Sydney)	ap-sydney-1	192.29.144.152/29	192.29.144.154
India South (Hyderabad)	ap-hyderabad-1	129.148.128.56/29	129.148.128.61
India West (Mumbai)	ap-mumbai-1	192.29.48.240/29	192.29.48.246
Indonesia (Batam)	ap-batam-1	168.110.254.168/29	168.110.254.175
Japan Central (Osaka)	ap-osaka-1	192.29.242.208/29	192.29.242.211
Japan East (Tokyo)	ap-tokyo-1	192.29.39.56/29	192.29.39.59
Malaysia (Kulai)	ap-kulai-2	149.118.162.112/29	149.118.162.115
Singapore (Singapore)	ap-singapore-1	129.148.178.96/29	129.148.178.102

Region Where Oracle Analytics Cloud Deployed	Region Identifier	IP Address Range	Gateway IP Address
Singapore West (Singapore)	ap-singapore-2	159.13.3.8/29	159.13.3.9
South Korea Central (Seoul)	ap-seoul-1	192.29.20.96/29	192.29.20.98
South Korea North (Chuncheon)	ap-chuncheon-1	129.148.144.24/29	129.148.144.31
Europe, the Middle East and Africa (EMEA)			
France Central (Paris)	eu-paris-1	155.248.129.232/29	155.248.129.237
France South (Marseille)	eu-marseille-1	129.149.99.160/29	129.149.99.166
Germany Central (Frankfurt)	eu-frankfurt-1	147.154.148.0/29	147.154.148.171
		138.1.64.32/29	138.1.64.33
		147.154.131.128/29	147.154.131.133
Israel 1 (Jerusalem)	il-jerusalem-1	129.149.121.32/29	129.149.121.32
Italy Northwest (Milan)	eu-milan-1	129.149.113.56/29	129.149.113.56
Italy Northwest (Turin)	eu-turin-1	84.8.227.40/29	84.8.227.40
Netherlands Northwest (Amsterdam)	eu-amsterdam-1	192.29.193.72/29	192.29.193.76
Saudi Arabia West (Jeddah)	me-jeddah-1	192.29.225.72/29	192.29.225.78
Saudi Arabia (Riyadh)	me-riyadh-1	84.8.65.88/29	158.247.99.174
Serbia (Jovanovac)	eu-jovanovac-1	207.127.84.72/29	207.127.84.75
South Africa Central (Johannesburg)	af-johannesburg-1	129.149.67.184/29	129.149.67.187
Spain Central (Madrid)	eu-madrid-1	155.248.138.136/29	155.248.138.140
Spain Central (Madrid)	eu-madrid-3	80.225.167.72/29	80.225.167.73
Sweden Central (Stockholm)	eu-stockholm-1	129.149.80.152/29	129.149.80.153
Switzerland North (Zurich)	eu-zurich-1	192.29.60.112/29	192.29.60.112
UAE Central (Abu Dhabi)	me-abudhabi-1	129.149.50.80/29	129.149.50.84
UAE East (Dubai)	me-dubai-1	129.148.214.184/29	129.148.214.189
UK South (London)	uk-london-1	147.154.229.168/29	147.154.229.170
		147.154.232.168/29	147.154.232.175
UK West (Newport)	uk-cardiff-1	129.149.20.112/29	129.149.20.118
Latin America			
Brazil East (Sao Paulo)	sa-saopaulo-1	192.29.128.232/29	192.29.128.238
Brazil Southeast (Vinhedo)	sa-vinhedo-1	129.149.2.208/29	129.149.2.208
Chile Central (Santiago)	sa-santiago-1	129.148.152.208/29	129.148.152.214
Chile Central (Valparaiso)	sa-valparaiso-1	10.23.0.0/16	165.1.96.225
Colombia (Bogota)	sa-bogota-1	10.24.0.0/16	158.247.99.174
Mexico Central (Monterrey)	mx-monterrey-1	139.177.105.88/29	139.177.105.94
Mexico Central (Queretaro)	mx-queretaro-1	155.248.146.152/29	155.248.146.152
North America			

Region Where Oracle Analytics Cloud Deployed	Region Identifier	IP Address Range	Gateway IP Address
Canada Southeast (Montreal)	ca-montreal-1	192.29.82.176/29	192.29.82.176
Canada Southeast (Toronto)	ca-toronto-1	192.29.13.0/29	192.29.13.6
		192.29.14.104/29	192.29.14.106
US East (Ashburn)	us-ashburn-1	147.154.20.0/29	147.154.20.1
		147.154.3.184/29	147.154.3.185
		147.154.0.0/29	147.154.0.3
		147.154.3.8/29	147.154.3.13
		130.35.99.216/29	130.35.99.221
US East (Columbus)	us-columbus-1	147.154.16.168/29	147.154.16.169
		157.137.103.104/29	157.137.103.109
US North (Chicago)	us-chicago-1	131.186.10.104/29	131.186.10.109
US West (Boardman)	us-boardman-1	192.22.100.184/29	192.22.100.184
US West (Phoenix)	us-phoenix-1	147.154.104.160/29	147.154.104.165
		138.1.32.24/29	138.1.32.29
		147.154.120.80/29	147.154.120.84
US West (San Jose)	us-sanjose-1	129.148.161.112/29	129.148.161.117

Restrict Access to Oracle Analytics Cloud Deployed with a Public Endpoint

If you deploy Oracle Analytics Cloud with a public internet accessible endpoint, you can restrict access through one or more rules.

Topics:

- [About Public Endpoints and Access Control Rules](#)
- [Prerequisites for a Public Endpoint](#)
- [Typical Workflow to Restrict Public Access using Rules](#)
- [Create Oracle Analytics Cloud with a Public Endpoint](#)
- [Manage Ingress Access Rules for a Public Endpoint using the Console](#)

About Public Endpoints and Access Control Rules

When you set up an Oracle Analytics Cloud instance you have the option to deploy Oracle Analytics Cloud with a *public internet accessible endpoint*.

For security reasons, you might want to restrict incoming traffic (ingress) through one or more access control rules. Similarly, if you use a private access channel to connect to private data sources, you might want to restrict outgoing traffic (egress) through one or more network security group rules.

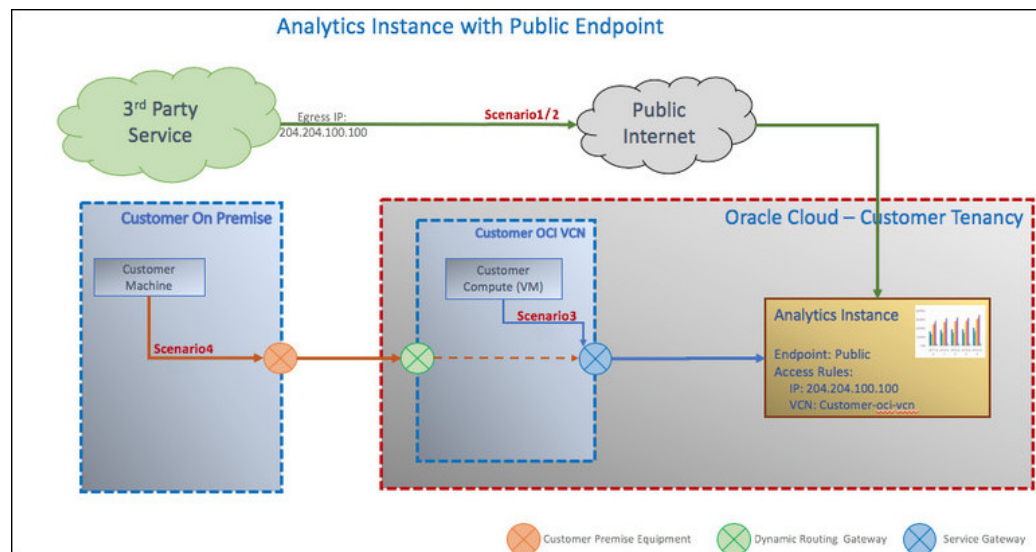
Ingress Access Control Rules

You can add and edit incoming access control rules whenever you want, and manage access in several ways. You can manage access from:

- A specific set of IP addresses
- CIDR block ranges (Classless Inter-Domain Routing)
- One or more Oracle Cloud Infrastructure VCNs (Virtual Cloud Network)
- Oracle services in the same region through a service gateway
- Any combination of the above, that is, IP addresses, CIDR ranges, VCNs, Oracle services.

For example:

- **Scenario 1** - Allow access to Oracle Analytics Cloud over the public internet. Restrict access to a fixed set of IP addresses.
- **Scenario 2** - Allow access to Oracle Analytics Cloud over the public internet. Restrict access to hosts within a fixed CIDR block range.
- **Scenario 3** - Allow access to Oracle Analytics Cloud from an Oracle Cloud Infrastructure VCN that's deployed in the same region as Oracle Analytics Cloud, without going over the public internet. At the same time, allow other third-party cloud services or users to access Oracle Analytics Cloud over the public internet.
- **Scenario 4** - Allow access to Oracle Analytics Cloud from your on-premise network without going through the public internet. At the same time, allow other third-party cloud services or users to access Oracle Analytics Cloud over the public internet.
- **Scenario 6** - Allow access to Oracle Analytics Cloud from your on-premise network without going through the public internet. At the same time, allow Oracle Services in the same region to access Oracle Analytics Cloud.



The sample diagram shows Oracle Analytics Cloud deployed with a public endpoint and two access control rules. The first rule allows access from the IP address 204.204.100.100 and the second rule allows access from the Oracle Cloud Infrastructure VCN `customer-oci-vcn`. The VCN is peered to an on-premise network, and access to Oracle Analytics Cloud is routed through the VCN's service gateway.

While Oracle Analytics Cloud is accessible from the public internet, you can implement your own access control rules to provide any additional security that you need. In this example, only

the third-party service with the egress gateway IP address 204.204.100.100 accesses Oracle Analytics Cloud over the public internet. Traffic from the on-premise network never uses the public internet, instead it uses the service gateway configured inside the VCN.

Egress Network Security Group Rules

if your Oracle Analytics Cloud instance uses a private access channel to connect to private data sources, you can restrict outgoing traffic (egress) through one or more network security group rules. You can specify up to five network security group rules for the private channel and edit them whenever you want.

Prerequisites for a Public Endpoint

Before you create an Oracle Analytics Cloud instance that's accessible from the public internet, consider whether or not your organization wants to restrict incoming traffic (ingress).

No Restrictions

No prerequisites. If you want Oracle Analytics Cloud to be accessible from anywhere, you can create the Oracle Analytics Cloud instance with no access control.

Restrict Access to a Specific IP Address or CIDR Block Range

If you plan to limit incoming traffic (ingress) from a specific IP address or CIDR block range, record all the IP addresses or CIDR ranges that you want to allow. When you create your Oracle Analytics Cloud instance, you use this information to define one or more access control rules for Oracle Analytics Cloud.

Restrict Access to a Specific VCN

If you plan to limit access to traffic from a specific Oracle Cloud Infrastructure VCN, ensure that the VCN exists and you have the required policies to access the VCN.

1. Set up an Oracle Cloud Infrastructure VCN in the same region as the Oracle Analytics Cloud instance you plan to create.
See [Set up the VCN and subnets](#).
2. Set up a service gateway in your VCN, and a route table to send traffic to Oracle Analytics Cloud through the service gateway.
See [Setting Up a Service Gateway in the Console](#).
3. Ensure that you (or whoever plans to create the Oracle Analytics Cloud instance) have the required policies to access the VCN.

- **READ** policy for the **compartment**:

```
ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ compartments IN TENANCY
```

- **READ** policy for the **VCN**:

```
ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ virtual-network-family IN TENANCY
```

Restrict Access to Oracle Services

No prerequisites. After creating your instance, you can add a single access control rule that allows all trusted Oracle Services in your region to access your Oracle Analytics Cloud instance.

Typical Workflow to Restrict Public Access using Rules

If you want to deploy an Oracle Analytics Cloud instance with a public endpoint for the first time with one or more access control rules, follow these tasks as a guide.

Task	Description	More Information
Understand prerequisites for a public endpoint	Consider whether or not your organization plans to restrict access for incoming traffic. If required, record the IP addresses, CIDR ranges, and VCNs that you plan to <i>allow</i> access to.	Prerequisites for a Public Endpoint
Create Oracle Analytics Cloud with a public endpoint	Use Oracle Cloud Infrastructure Console to deploy a new service.	Create Oracle Analytics Cloud with a Public Endpoint
Allow access by IP address, CIDR range, VCN, and to Oracle services	Add one or more access control rules for incoming traffic. You can allow access to Oracle Analytics Cloud by public IP address, public CIDR block range, VCN, and to Oracle services.	Control Incoming Traffic for a Public Endpoint (Ingress)
(Optional) Set up private access from your on-premise network	<p>Set up an Oracle Cloud Infrastructure VCN that connects to your on-premise network using FastConnect private peering or VPN Connect. The VCN must be deployed in the same region as Oracle Analytics Cloud.</p> <p>Set up a service gateway in your VCN, and a route table to send traffic to Oracle Analytics Cloud through the service gateway.</p> <p>Add an access control rule in your Oracle Analytics Cloud instance that allows access from your VCN.</p> <p>Configure VCN peering to your on-premise network through FastConnect or VPN Connect to enable access from your on-premise network.</p> <p>Configure transit routing with the VCN to give your on-premise network private access to Oracle Analytics Cloud.</p>	Working with VCNs and Subnets Setting Up a Service Gateway in the Console Control Incoming Traffic for a Public Endpoint (Ingress) Access to Your On-Premises Network Setting Up Private Access to Oracle Services
(Optional) Set up private access from hosts on your VCN	<p>Set up an Oracle Cloud Infrastructure VCN in the same region as Oracle Analytics Cloud.</p> <p>Set up a service gateway in your VCN, and a route table to send traffic to Oracle Analytics Cloud through the service gateway.</p> <p>Add an access control rule in your Oracle Analytics Cloud instance that allows access from your VCN.</p>	Working with VCNs and Subnets Setting Up a Service Gateway in the Console Control Incoming Traffic for a Public Endpoint (Ingress)
(Optional) Set up a private access channel	<p>Set up a private access channel and register the domain names or SCAN host names of the data sources that require private access.</p> <p>Use network security group rules to restrict access to your private data sources.</p>	Connect to Private Sources Through a Private Access Channel Control Outgoing Traffic for a Public Endpoint (Egress)

Create Oracle Analytics Cloud with a Public Endpoint

You can use Oracle Cloud Infrastructure Console, API, or command line to deploy Oracle Analytics Cloud with a public endpoint.

This topic highlights the information you must configure to enable access over the public internet and define any access control rules that you require.

Create Analytics Instance

Network Access

Access Type

Public
Access your instance from anywhere

Private
Access your instance from a Virtual Cloud Network only

Configure Access Control

Access Control Rules

Rule Type IP Address	IP Address 137.254.16.112	×
Rule Type CIDR Block	CIDR Block 137.254.16.112/28	×
Rule Type Virtual Cloud Network	Virtual Cloud Ne... oac-dxb-compartn	Virtual Cloud ... ×
Rule Type Service	Service All services on the Oracle Services Network in this region	×

Add Access Control Rule

1. Specify a name, select an edition, license, size, and update cycle for your service, and then click **Show Advanced Options**.
If you're new to Oracle Analytics Cloud, see [Create a Service](#) for all the steps.
2. In **Network Access**, select **Public**.
3. Optional: To restrict incoming traffic (ingress), select **Configure Access Control**, and then add one or more rules that allowlist specific public IP addresses, public CIDR block ranges, VCNs, and Oracle Services.

You can add, edit, and delete access control rules at any time. So if you prefer, you can configure your rules later.

Control Incoming Traffic for a Public Endpoint (Ingress)

If you deployed Oracle Analytics Cloud with a public internet accessible endpoint, you can restrict incoming traffic to your service through an access control list (ACL) that contains one or more rules. You can add and edit access control rules whenever you want and allow access by public IP address, public CIDR block range, VCN, or other Oracle services using the Console, API, or command line.

Oracle Analytics Cloud enables you to specify up to 20 access rules.

Alternatively, if you're able to route traffic through a VCN, you can specify a single access rule in Oracle Analytics Cloud for the VCN and define all your access restrictions in the VCN instead.

Note

Required IAM Policy to Edit Analytics Instance

Verb: manage

Resource Types: analytics-instance, analytics-instances

Permission: ANALYTICS_INSTANCE_MANAGE

See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

Additional IAM Policy Required to Edit a Public Endpoint

Verb: read

Resource Type: virtual-network-family, compartment, compartments


See [Prerequisites for a Public Endpoint](#).

Topics

- [Manage Ingress Access Rules for a Public Endpoint using the Console](#)
- [Manage Ingress Access Rules for a Public Endpoint using the REST API](#)
- [Manage Ingress Access Rules for a Public Endpoint using the Command Line](#)

Manage Ingress Access Rules for a Public Endpoint using the Console

If you deployed Oracle Analytics Cloud with a public internet accessible endpoint, you can restrict incoming traffic to your service through an access control list (ACL) that contains one or more ingress rules. You can add and edit access control rules whenever you want and allow access to a public IP address, a public CIDR block range, a VCN or Oracle services.

1. In Oracle Cloud Infrastructure Console, click  in the top left corner.
2. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to control access to.
5. On the Details tab under **Network Access**, click the **Edit** link next to the **Access Control** option.

6. Add or edit access control rules as required.

You can specify the following types of rule:

- **IP Address:** Select **IP Address** to a specific public IP address.
- **CIDR Block:** Select **CIDR Block** to specify a range of public IP addresses using CIDR notation.
- **Service:** Select **Service** to allow Oracle services to access your Oracle Analytics Cloud instance.
- **Virtual Cloud Network:** Select **Virtual Cloud Network** to specify an existing Oracle Cloud Infrastructure VCN. The drop-down list shows all the VCNs in the current compartment that you have access to. If you can't see the VCN or subnet you want, check you have the required permissions. See [About Public Endpoints and Access Control Rules](#).

Click **Virtual Cloud Network Compartment** to select a VCN from a different compartment.

Manage Ingress Access Rules for a Public Endpoint using the REST API

You can use the `ChangeAnalyticsInstanceNetworkEndpoint` operation to change access control rules for incoming traffic to an Oracle Analytics Cloud instance with a public endpoint.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use this operation:

- [ChangeAnalyticsInstanceNetworkEndpoint](#)

Manage Ingress Access Rules for a Public Endpoint using the Command Line

You can use the `change-network-endpoint` command to change access control rules for incoming traffic to an Oracle Analytics Cloud instance with a public endpoint.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- [change-network-endpoint](#)

Control Outgoing Traffic for a Public Endpoint (Egress)

If you deployed Oracle Analytics Cloud with a public internet accessible endpoint and you have private data sources that Oracle Analytics Cloud connects to over a private access channel, you can use egress rules that you define in *network security groups* to restrict outgoing traffic through the channel. You can add up to five network security groups using the Console, REST API, and CLI.

Note

Required IAM Policy

Verb: manage

Resource Type: analytics-instance, analytics-instances

Custom Permission: ANALYTICS_INSTANCE_MANAGE

See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

Verb: manage

Resource Type: virtual-network-family

Verb: read

Resource Type: compartment, compartments

Verb: use

Resource Type: network-security-groups

To learn about other, more detailed access policy options, see [Prerequisites for a Private Access Channel](#).

Topics

- [Edit Network Details for a Private Access Channel using the Console](#)
- [Edit a Private Access Channel using the REST API](#)
- [Edit a Private Access Channel using the Command Line](#)

Deploy Oracle Analytics Cloud with a Private Endpoint

If you want only hosts within your virtual cloud network (VCN) or your on-premise network to have access to Oracle Analytics Cloud, you can deploy your Oracle Analytics Cloud instance with a *private endpoint*.

Topics:

- [About Private Endpoints](#)
- [Prerequisites for a Private Endpoint](#)
- [Typical Workflow to Deploy Oracle Analytics Cloud with a Private Endpoint](#)
- [Create Oracle Analytics Cloud with a Private Endpoint](#)

- [Change a Private Endpoint using the Console](#)
- [Connect to Your On-premise Network using FastConnect or VPN Connect](#)

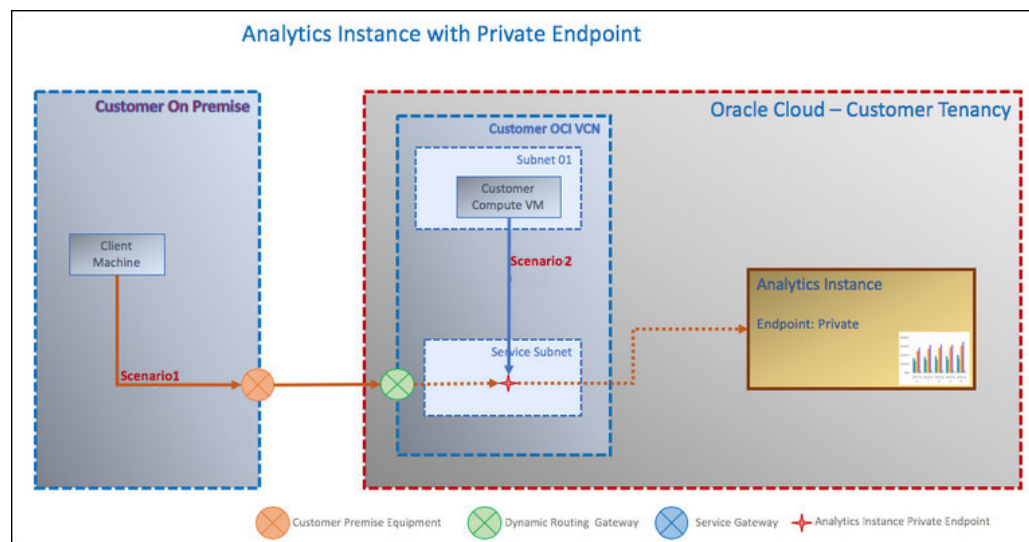
About Private Endpoints

When you set up an Oracle Analytics Cloud instance you have the option to restrict access through a *private endpoint*. Private access means that traffic doesn't go over the internet. Private access can be from hosts within your virtual cloud network (VCN) or your on-premise network.

For example:

- **Scenario 1** - Allow access to Oracle Analytics Cloud from an on-premise (corporate) network. Don't allow access to anyone outside the corporate network.
- **Scenario 2** - Allow access to Oracle Analytics Cloud from an Oracle Cloud Infrastructure VCN that's deployed in the same region as Oracle Analytics Cloud. Don't allow access to anyone outside the virtual cloud network.

When you deploy an Oracle Analytics Cloud instance with a private endpoint, the Oracle Analytics Cloud URL is only accessible from a browser if the client machine supports host name resolution. This means you must configure Domain Name Server (DNS) resolution on your private network to access the private endpoint. For example, you might use a DNS resolution strategy similar to that described in the article [Hybrid DNS Configuration using DNS VM in VCN](#).



The diagram shows Oracle Analytics Cloud deployed with a private endpoint. The private Oracle Analytics Cloud is only accessible through an Oracle Cloud Infrastructure VCN in your tenancy; you can't access Oracle Analytics Cloud from the public internet.

You must peer the VCN to your on-premise network. To enable access to Oracle Analytics Cloud, the on-premise network DNS must provide host name resolution for Oracle Analytics Cloud.

Ingress and Egress Access Control Rules

If you deploy Oracle Analytics Cloud with a private endpoint, you can restrict incoming traffic (ingress) to your service through predefined network security groups that contain one or more access rules.

If the Oracle Analytics Cloud uses a private access channel to connect to private data sources, you can also use network security groups to restrict outgoing traffic (egress) on the private access channel.

You can specify up to five network security group rules for incoming traffic and for outgoing traffic on the private access channel, and you can edit the rules whenever you want.

Prerequisites for a Private Endpoint

Before you create an Oracle Analytics Cloud instance with a private endpoint, complete the required prerequisites.

The prerequisites are the same for both scenarios:

- Private access from an on-premise network through an Oracle Cloud Infrastructure VCN
- Private access from hosts in an Oracle Cloud Infrastructure VCN
- 1. Set up the Oracle Cloud Infrastructure VCN with a subnet for Oracle Analytics Cloud.

The VCN must be in the region where you plan to deploy Oracle Analytics Cloud. See [Working with VCNs and Subnets](#).

Note

If you plan to access Oracle Analytics Cloud from an on-premise network, keep some address space available in the VCN for additional subnets in case you need them for host name resolution.

2. Ensure that you (or whoever plans to create the Oracle Analytics Cloud instance) have the required policies to access the VCN.

Several options are available. Choose the most appropriate level for you:

Broad Resource Access Policy

- `ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ compartments IN TENANCY`
- `ALLOW GROUP <ANALYTICS ADMIN GROUP> TO MANAGE virtual-network-family IN TENANCY`

Limited Resource Access Policy

- `ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ compartments IN TENANCY`
- `ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ virtual-network-family IN compartment <compartment name of VCN>`
- `ALLOW GROUP <ANALYTICS ADMIN GROUP> TO USE subnets IN compartment <compartment name of subnet>`
- `ALLOW GROUP <ANALYTICS ADMIN GROUP> TO MANAGE vnics IN compartment <compartment name of AnalyticsInstance>`

Moderate Resource Access Policy - Option 1

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ compartments IN TENANCY
- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ virtual-network-family IN TENANCY
- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO USE subnets IN TENANCY
- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO MANAGE vnics IN TENANCY

Moderate Resource Access Policy - Option 2

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ compartments IN TENANCY
 - ALLOW GROUP <ANALYTICS ADMIN GROUP> TO USE virtual-network-family IN compartment <compartment name of VCN>
 - ALLOW GROUP <ANALYTICS ADMIN GROUP> TO MANAGE virtual-network-family IN compartment <compartment name of AnalyticsInstance>
3. Optional: If you plan to restrict incoming traffic (ingress) using network security group rules, you can do so when you create your Oracle Analytics Cloud instance or you can save the task for later.

If you want to configure network security groups when you create your Oracle Analytics Cloud instance, make sure the network security groups exist in the same VCN as your Oracle Analytics Cloud and you have the required policies to use network security groups.

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO USE network-security-groups IN TENANCY

Typical Workflow to Deploy Oracle Analytics Cloud with a Private Endpoint

If you want to deploy an Oracle Analytics Cloud instance with a private endpoint for the first time, follow these tasks as a guide.

Task	Description	More Information
Understand prerequisites for a private endpoint	Set up an Oracle Cloud Infrastructure virtual cloud network (VCN) with a subnet for Oracle Analytics Cloud. The VCN must be in the region where you plan to deploy Oracle Analytics Cloud.	Prerequisites for a Private Endpoint
Create Oracle Analytics Cloud with a private endpoint	Use Oracle Cloud Infrastructure Console to deploy a new service.	Create Oracle Analytics Cloud with a Private Endpoint
Configure the connection to your on-premise network using FastConnect or VPN Connect.	(Only required if you want to access Oracle Analytics Cloud from an on-premise network) Use FastConnect or VPN to peer your on-premise network with the Oracle Cloud Infrastructure VCN through which you plan to access Oracle Analytics Cloud.	Connect to Your On-premise Network using FastConnect or VPN Connect
Change the VCN or subnet used to access Oracle Analytics Cloud	If you want to access Oracle Analytics Cloud through a different VCN or subnet, you can edit the configuration at any time.	Change a Private Endpoint using the Console

Task	Description	More Information
(Optional) Control incoming traffic (ingress) and outgoing traffic (egress) using network security group rules	Use one or more network security groups to control access to and from Oracle Analytics Cloud.	Control Incoming and Outgoing Traffic for a Private Endpoint (Ingress and Egress)
(Optional) Set up a private access channel	Set up a private access channel and register the domain names or SCAN host names of the data sources that require private access. Optionally, use network security group rules to restrict traffic to and from your private data sources.	Connect to Private Sources Through a Private Access Channel Control Incoming and Outgoing Traffic for a Private Endpoint (Ingress and Egress)

Create Oracle Analytics Cloud with a Private Endpoint

You can use Oracle Cloud Infrastructure Console, API, or command line to deploy Oracle Analytics Cloud with a private endpoint.

This topic highlights the information you must configure to enable private access through a private endpoint.

Network Access

Access Type

Public
Access your instance from anywhere

Private
Access your instance from a Virtual Cloud Network only

Virtual Cloud Network compartment
oac-dxb-compartment

Virtual Cloud Network
oac_cust_vcn_pac

Subnet compartment
oac-dxb-compartment

Subnet
oac-service-subnet

Configure Access Control

Network Security Groups

Network security group compartment
oac-dxb-compartment

Network security group
adw-nsg

Add Network Security Group

1. Specify a name, select an edition, license, size, and update cycle for your service, and then click **Show Advanced Options**.
If you're new to Oracle Analytics Cloud, see [Create a Service](#) for all the steps.
2. In **Network Access**, select **Private**.
3. Select the **Virtual Cloud Network** and the **Subnet** that you want to use to access Oracle Analytics Cloud.
4. Optional: To restrict incoming traffic (ingress), select **Configure Access Control**, and then select one or more network security groups that you want to allow access to.

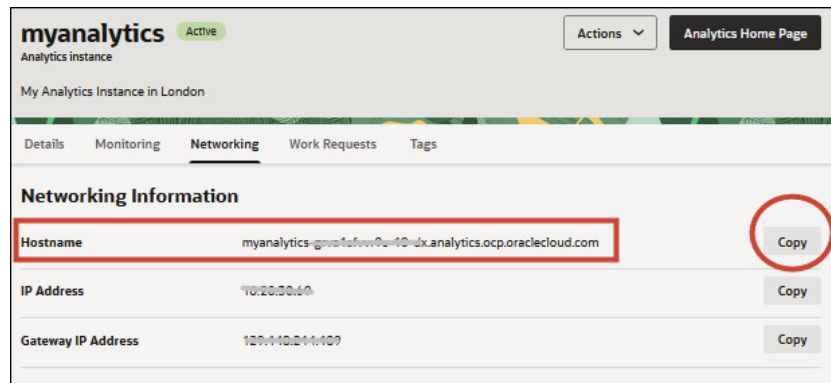
You can add, edit, and delete network security groups at any time. So if you prefer, you can configure these later.

Connect to Your On-premise Network using FastConnect or VPN Connect

If you want to access an Oracle Analytics Cloud instance that is deployed with a private endpoint in an Oracle Cloud Infrastructure VCN from your on-premise network, you must peer your on-premise network with the Oracle Cloud Infrastructure VCN. You can use FastConnect or VPN to peer your on-premise network with a VCN on Oracle Cloud Infrastructure.

Typically, these tasks are performed by the network administrator responsible for the on-premise network and the Oracle Cloud Infrastructure network. You can complete these steps before or after you create your Oracle Analytics Cloud instance.

1. In Oracle Cloud Infrastructure Console, navigate to the **Networking** tab to determine the **Hostname** of your Oracle Analytics Cloud instance.



See [Find the IP Address or Host Name of Your Oracle Analytics Cloud Instance](#).

2. Peer your on-premise network with the Oracle Cloud Infrastructure VCN through FastConnect or VPN Connect.

See [Access to Your On-Premises Network](#).

3. In your on-premise network, configure a suitable host name resolution solution for Oracle Analytics Cloud.

Several options are available to you:

- (Testing purposes only) From a client machine in your on-premise network, add a host name entry in the `/etc/hosts` file for Oracle Analytics Cloud.

For example, add a new line in the format: `<IP_address> <hostname>`. Enter the hostname and IP address that you copied in Step 1. For example: `192.0.2.1 oac-xxxxxxxxxxxxm-ia.analytics.ocp.oraclecloud.com`

- Add a DNS record in your on-premise intranet DNS server (Domain Name System) for Oracle Analytics Cloud, that is, specify the host name for Oracle Analytics Cloud and its private IP address.
- Set up a hybrid DNS solution. For example, see [Hybrid DNS configuration using DNS VM in OCI VCN](#).
 - a. Configure your on-premise intranet DNS server with conditional DNS forwarding to the DNS server configured in the VCN, and specify the host name for Oracle Analytics Cloud.
 - b. Configure your on-premise intranet DNS server with DNS forwarding to the DNS server configured in the VCN, and specify the entire Oracle Analytics Cloud hostname that you copied in Step 1.

4. Test that you can access Oracle Analytics Cloud from your on-premise network.

If required, use Network Path Analyzer to troubleshoot connectivity issues. See [Troubleshoot Connectivity Issues Using Network Path Analyzer](#).

Change the VCN or Subnet Used to Access a Private Endpoint

If you want to access Oracle Analytics Cloud through a different VCN or subnet, you can edit the configuration using the Console, API, or command line.

Note

Required IAM Policy to Edit Analytics Instance

Verb: `manage`

Resource Types: `analytics-instance, analytics-instances`

Permission: `ANALYTICS_INSTANCE_MANAGE`

See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

IAM Policy Required to Change a Private Endpoint

Verb: `manage`

Resource Type: `virtual-network-family`

Verb: `read`

Resource Type: `compartment, compartments`

To learn about other, more detailed access policy options, see [Prerequisites for a Private Endpoint](#).

Topics

- [Change a Private Endpoint using the Console](#)
- [Change a Private Endpoint using the REST API](#)
- [Change a Private Endpoint using the Command Line](#)

Change a Private Endpoint using the Console

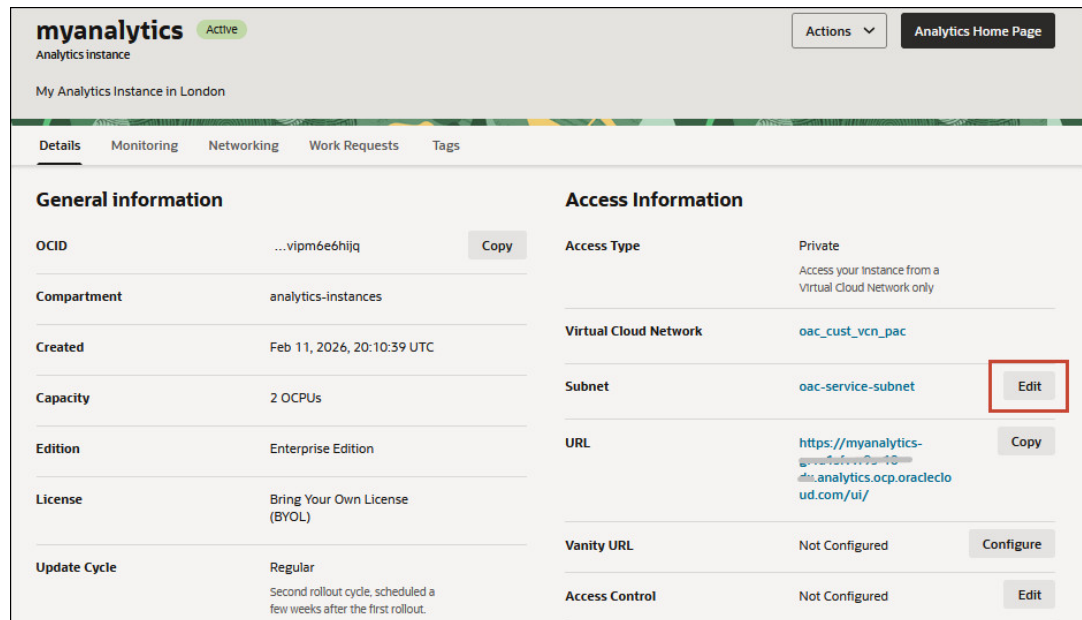
If you want to access Oracle Analytics Cloud through a different VCN or subnet you can edit the configuration. You can also configure the network security groups used to control ingress and egress.

Note

If you change the VCN you must reconfigure the network security groups.

1. In Oracle Cloud Infrastructure Console, click  in the top left corner.
2. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.

3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to change access to.
5. On the Details page, click the **Edit** link next to **Subnet**.

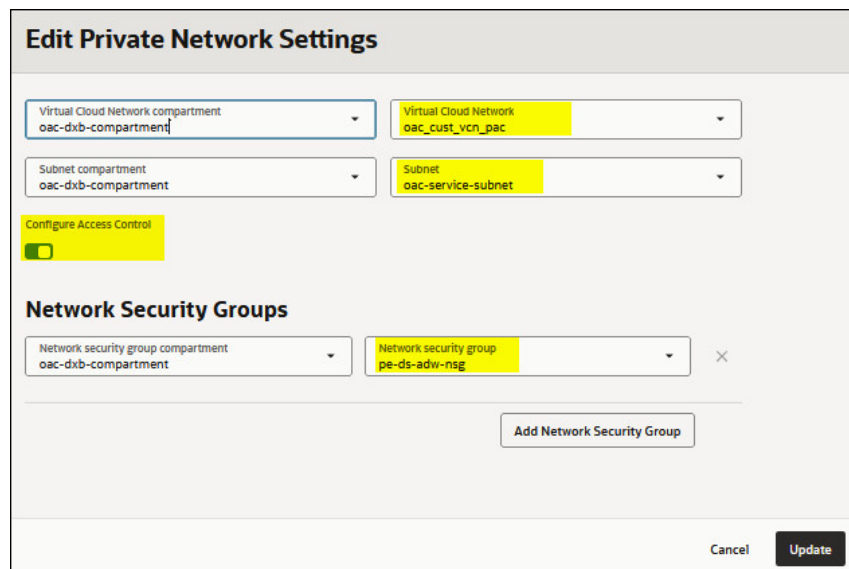


The screenshot shows the 'myanalytics' instance details page. The 'Access Information' section contains the following data:

Field	Value	Action
Access Type	Private	
Virtual Cloud Network	oac_cust_vcn_pac	
Subnet	oac-service-subnet	Edit
URL	https://myanalytics-...analytics.ocp.oraclecloud.com/ui/	Copy
Vanity URL	Not Configured	Configure
Access Control	Not Configured	Edit

6. Select a different **Virtual Cloud Network**, **Subnet**, or both.

Click **Virtual Cloud Network Compartment** or **Subnet Compartment** to select resources from a different compartment. If you can't see the VCN or subnet you want, check you have the required permissions. See [Prerequisites for a Private Endpoint](#).



The 'Edit Private Network Settings' dialog box contains the following configuration:

- Virtual Cloud Network compartment: oac-dxb-compartment
- Virtual Cloud Network: oac_cust_vcn_pac
- Subnet compartment: oac-dxb-compartment
- Subnet: oac-service-subnet
- Configure Access Control:
- Network Security Group compartment: oac-dxb-compartment
- Network Security Group: pe-ds-adw-nsg
- Buttons: Add Network Security Group, Cancel, Update

7. Click **Add Network Security Group** and then select the name of the network security group you want to give access to.

Click **Network Security Group Compartment** if the network security group you're looking for is located in a different compartment.

8. Click **Add Network Security Group** to give access to other network security groups.

You can add up to five network security groups.

Change a Private Endpoint using the REST API

You can use the `ChangeAnalyticsInstanceNetworkEndpoint` operation to command to change the VCN or subnet used to access an Oracle Analytics Cloud instance with a private endpoint.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use this operation:

- [ChangeAnalyticsInstanceNetworkEndpoint](#)

Change a Private Endpoint using the Command Line

You can use the `change-network-endpoint` command to change the VCN or subnet used to access an Oracle Analytics Cloud instance with a private endpoint.

For example:

```
oci \
  analytics analytics-instance change-network-endpoint \
  --analytics-instance-id ocid1.analyticsinstance.oc1.us-
ashburn-1.aaaaaaa5pynfxr2e6wpshkhkoa joiqizwmhc6x7ogp4aw66whyq76fdk32q \
  --network-endpoint-details '{
"networkEndpointType": "PRIVATE", "vcnId" :
"ocid1.vcn.oc1.us-
ashburn-1.amaaaaaarfop2rqav4x2wox6dt72o57jmnevpguq63gcsdtrbk42bvz446sa",
"subnetId": "ocid1.subnet.oc1.us-
ashburn-1.aaaaaaa15xb6vodov35nbcqhsnwoypeieowgy44vambmnozpwv22pvjxoq"
}'
```

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- [change-network-endpoint](#)

Control Incoming and Outgoing Traffic for a Private Endpoint (Ingress and Egress)

If you deployed Oracle Analytics Cloud with a private endpoint, you can restrict incoming and outgoing traffic to your service through ingress and egress rules that you define in network security groups.

Oracle Analytics Cloud enables you to specify up to 5 network security groups and you can configure these network security groups at any time.

Note**Required IAM Policy to Edit Analytics Instance****Verb:** manage**Resource Types:** analytics-instance, analytics-instances**Permission:** ANALYTICS_INSTANCE_MANAGESee [About Permissions to Manage Oracle Analytics Cloud Instances](#).**Additional IAM Policy Required to Edit a Private Endpoint****Verb:** manage**Resource Type:** virtual-network-family**Verb:** read**Resource Type:** compartment, compartments**Verb:** use**Resource Type:** network-security-groupsSee [Prerequisites for a Public Endpoint](#).**Topics**

- [Change a Private Endpoint using the Console](#)
- [Change a Private Endpoint using the REST API](#)
- [Change a Private Endpoint using the Command Line](#)

Connect to Private Sources Through a Private Access Channel

If the data you want to analyze is stored on a private host or you want to use a private Git repository to store semantic model development files, you can set up a private access channel between your Oracle Analytics Cloud instance and your private source.

Topics:

- [About Private Access Channels](#)
- [About Private Sources](#)
- [Top FAQs for Private Sources](#)
- [Prerequisites for a Private Access Channel](#)
- [Typical Workflow to Set Up a Private Access Channel](#)
- [Configure a Private Access Channel](#)
- [Edit a Private Access Channel](#)
- [Delete a Private Access Channel](#)

About Private Access Channels

If you want Oracle Analytics Cloud to access a private host, you can set up a private access channel. A private access channel can give Oracle Analytics Cloud access to private data sources or private Git repositories within your virtual cloud network (VCN) on Oracle Cloud Infrastructure or other networks peered to the VCN such as your corporate network.

You can set up a private access channel for Oracle Analytics Cloud instances deployed with **Enterprise Edition**. Private access channels aren't available to Oracle Analytics Cloud instances with **Professional Edition**.

It doesn't matter whether your Oracle Analytics Cloud instance has a public endpoint or a private endpoint. Oracle Analytics Cloud can access private data sources or private Git repositories through a private access channel for both network scenarios.

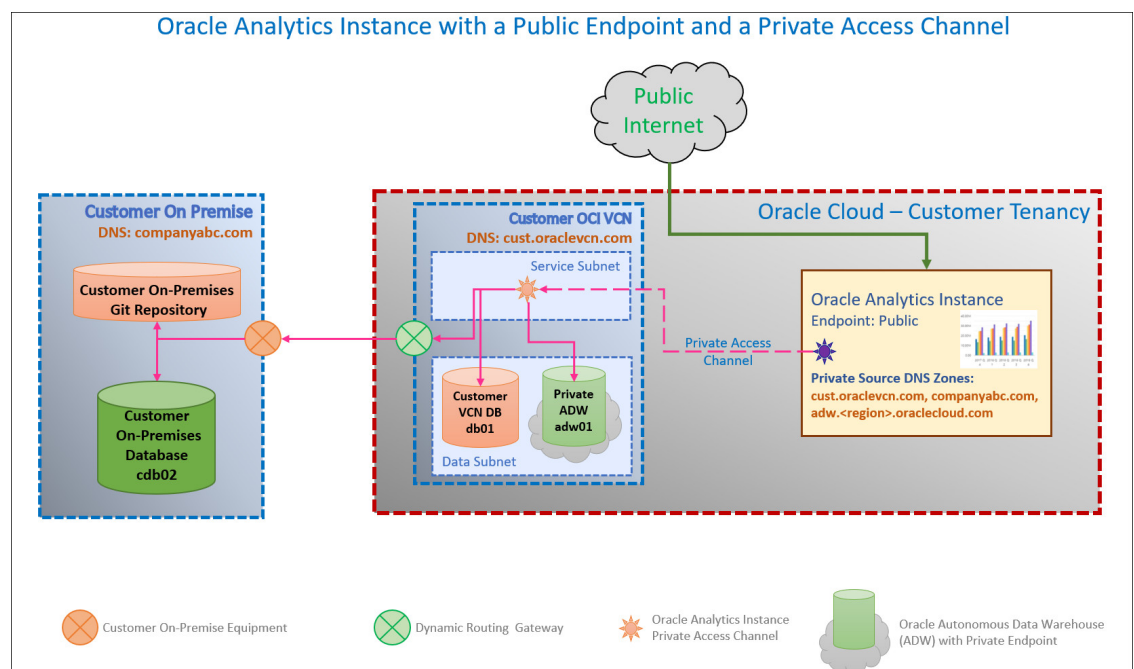
Note

Private access channels enable you to connect to hosts that represent private *data sources* and private *Git repositories*. You can't use a private access channel to access any other type of private host. For example, you can't use private access channels to access private hosts that represent FTP servers, SMTP servers, printers, MapViewer configuration, or any other type of private host you might use.

Private Access Channel for Oracle Analytics Cloud Instances with Public Endpoint

If Oracle Analytics Cloud has a public endpoint you must specify the VCN and subnet you want the private access channel to use.

If you want to restrict outgoing traffic (egress) over the private access channel, you can configure network security groups for your Oracle Analytics Cloud instance that contain one or more egress rules.

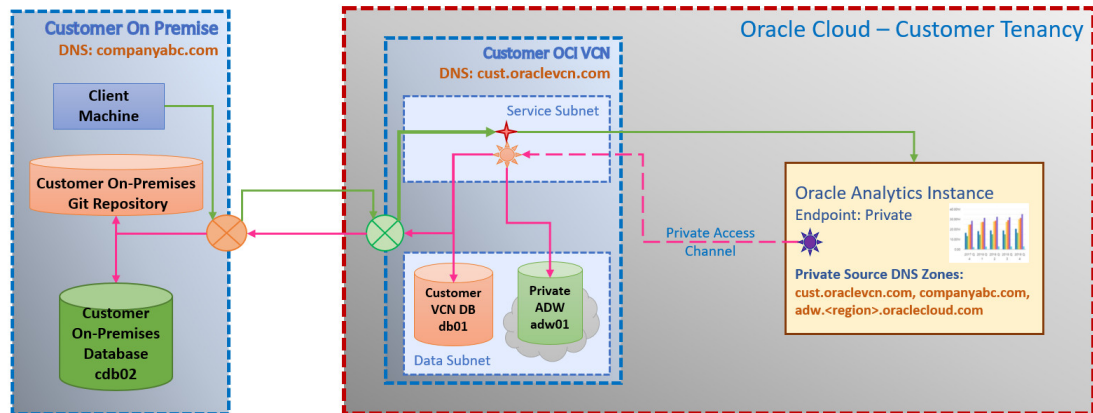


Private Access Channel for Oracle Analytics Cloud Instances with Private Endpoint

If Oracle Analytics Cloud has a private endpoint, the private access channel uses the same VCN and subnet as the private endpoint.

If you want to restrict incoming traffic (ingress) or outgoing traffic (egress) over the private access channel, you can configure network security groups for your Oracle Analytics Cloud instance that contain one or more ingress or egress rules.

Oracle Analytics Instance with a Private Endpoint and a Private Access Channel



About Private Sources

Oracle Analytics Cloud can access private data sources and private Git repositories with a Fully Qualified Domain Name (FQDN) that resolves through the Domain Name System (DNS) in your tenancy. Oracle Analytics Cloud can also access private Oracle Databases configured with a Single Client Access Name (SCAN).

- **DNS Zone:** Specify domain names such as `companyabc.com`, `example.com`, `myoacvcn.oraclevcn.com`, and so on.
- **SCAN Host and Port:** Specify host names such as `db01-scan.corp.example.com`, `prd-db01-scan.mycompany.com`, and the port where the SCAN protocol connects, for example 1521.

Topics

- [About Connecting to Private Sources](#)
- [Supported Private Data Sources](#)
- [Private Source Limitations - SCAN](#)
- [Private Source Limitations - Canonical Host Names](#)
- [Top FAQs for Private Sources](#)

About Connecting to Private Sources

In Oracle Analytics Cloud, you configure access to private data sources in two stages.

- **Stage 1)** In Oracle Cloud Infrastructure Console, you set up a private access channel and register the data sources or Git repositories that require private access using their DNS domain name or SCAN host name and port.

When you set up (or edit) a private access channel you alter the configuration of your Oracle Analytics Cloud instance. Some users might experience a temporary disruption in service during the configuration process so Oracle recommends that you plan private access channel configuration on critical instances accordingly.

- **Stage 2)** In Oracle Analytics Cloud, you connect to the data source and analyze the data in the usual way. In Semantic Modeler, you must create an SSH or HTTPS connection to access the Git repository.

For detailed guidance, see [Typical Workflow to Set Up a Private Access Channel](#).

Supported Private Data Sources

In Oracle Analytics Cloud, you can use a private access channel to connect to a range of certified data sources. To check whether you can use a private access change to connect to your data source, see Supported Data Sources.

Note

Private access channels enable you to connect to private *data source* hosts. You can't use a private access channel to access any other type of private host. For example, you can't use private access channels to access private hosts that represent FTP servers, SMTP servers, printers, MapViewer configuration, or any other type of private host you might use.

Private Source Limitations - SCAN

Oracle Analytics Cloud can't access private data sources on an Oracle Database that uses a Single Client Access Name (SCAN) with the TCP/IP with SSL protocol (TCPS). If you want to use TCPS to access an Oracle Database that uses a SCAN, use one of the following methods to set up the connection in Oracle Analytics Cloud:

- Configure the data source connection using the **Advanced Connection String** option and connect directly to the Oracle Database nodes, instead of SCAN.
For example:

```
(DESCRIPTION=(ENABLE=BROKEN)
 (ADDRESS_LIST=(LOAD_BALANCE=on)(FAILOVER=ON)
 (ADDRESS=(PROTOCOL=tcps)(HOST=<DB Node 1 FQDN Host Name>)(PORT=2484))
 (ADDRESS=(PROTOCOL=tcps)(HOST=<DB Node 2 FQDN Host Name>)(PORT=2484)))
 (CONNECT_DATA=
 (SERVICE_NAME=<DB Service Name>))
 (SECURITY=(SSL_SERVER_CERT_DN="CN=<DB Server Certificate DN>"))))
```

Where the distinguished name (DN) might look something like:

```
(SECURITY=(SSL_SERVER_CERT_DN="CN=host-example-
scan.mysubnet.exadatainfrastr.oraclevcn.com"))
```

The way you configure this connection string depends how many database hosts are active at the *same* time:

- If *more than one* database host is active at the same time, set `(LOAD_BALANCE=on)` in the connection string above.

- If *only one* database host is active at a time, set (`LOAD_BALANCE=off`) in the connection string. To optimize performance, include the `ADDRESS` of the active database host *first* in the `ADDRESS_LIST`.

To find out which database host is active at any given time, refer to the documentation for your database. For example, for Oracle Database you can use [V\\$INSTANCE](#).
- Configure an Oracle Connection Manager in front of SCAN and then configure a data source connection in Oracle Analytics Cloud that connects to the Oracle Connection Manager endpoint.

Private Source Limitations - Canonical Host Names

You can't use canonical host names to connect to private data sources over a private access channel. This means that if you want to connect to private data sources such as Snowflake that use AWS PrivateLink, you must create a private DNS zone (in the same VCN as the private access channel) with A records to map the private data source host names to private IP addresses. Then, you must add this private DNS zone to the private access channel.

- **DNS Zone:** Specify domain names such as `companyabc.com`, `example.com`, `myoacvcn.oraclevcn.com`, and so on.
- **SCAN Host and Port:** Specify host names such as `db01-scan.corp.example.com`, `prd-db01-scan.mycompany.com`, and the port where the SCAN protocol connects, for example 1521.

Top FAQs for Private Sources

The top FAQs when setting up a private access channel for Oracle Analytics Cloud are identified in this topic.

What data sources can I connect to over a private access channel?

To find out which data sources you can connect to through a private access channel, see Supported Data Sources. Look for the data sources with the connectivity option *private access channel* in the "Use in Datasets" and "Use in Semantic Modeler" columns.

Note

Private access channels enable you to connect to private *data source* hosts. You can't use a private access channel to access any other type of private host. For example, you can't use private access channels to access private hosts that represent FTP servers, SMTP servers, printers, MapViewer configuration, or any other type of private host you might use.

When I connect to my private source in Oracle Analytics Cloud, do I specify the domain name or the IP address of my private source?

You must specify the Fully Qualified Domain Name (FQDN) of your private source in the connect dialog. This is the same FQDN that's registered in the private access channel. For example, domain names such as `companyabc.com`, `example.com`, `myadw.adb.us-ashburn-1.oraclecloud.com`, and so on. See [About Private Sources](#).

You can't use IP addresses to connect to private sources.

My private Oracle Database has a Single Client Access Name (SCAN). Can I use the SCAN host name to connect to my private data source?

Yes. Register the SCAN host name and the SCAN port in private access channel. For example, SCAN host names such as `db01-scan.corp.example.com`, `prd-db01-scan.mycompany.com`, and the port where the SCAN protocol connects, for example 1521. See [About Private Sources](#).

Note

At least one DNS Zone is required on the private access channel. Select **Virtual Cloud Network's domain name as DNS zone** to add the default domain.

I have several private data sources and private Git repositories. Do I access all of them over a single private access channel?

Yes. Your Oracle Analytics Cloud instance supports a single private access channel. You can connect to multiple data sources and Git repositories through the same channel.

- DNS Zones: You can add up to 30 DNS zone entries.
- SCAN Hosts: You can add up to 15 SCAN host entries.

How long does it take to create, update, or delete private sources?

It takes between 7 and 30 minutes to add or modify DNS zone and SCAN host entries.

How do I control access to the private sources on my private access channel?

You can use egress rules defined in network security groups to restrict access to your private data sources and private Git repositories. The way you configure network security groups depends whether the endpoint of your Oracle Analytics Cloud instance is public or private. See [Manage Egress Access Rules for a Public Endpoint using the Console](#) or [Manage Ingress and Egress Access Rules for a Private Endpoint using the Console](#).

Can I add and remove private sources or edit the private access channel?

Yes. You can manage the DNS zones and SCAN hosts accessible through the private access channel. If your Oracle Analytics Cloud has a public endpoint, you can also change the VCN and subnet that the private access channel uses to access the private sources and control access with one or more network security groups. See [Edit a Private Access Channel](#).

You can monitor the progress of **Edit Private Access Channel** operations in the activity log. In the unlikely event an edit operation fails, Oracle recommends that you delete the private access channel and recreate it. See [Monitor Status](#).

Can I use both a private access channel and Remote Data Gateway?

Yes. You can use both these methods to connect to your remote data sources and Git repositories.

Can I set up a private access channel with Oracle Analytics Cloud Classic or Oracle Analytics Cloud Gen 1?

No. The private access channel feature is available only with Oracle Analytics Cloud Gen 2.

Can I use the private access channel to access a private source on a different OCI region?

No. Oracle Analytics Cloud and the Oracle Cloud Infrastructure VCN that's hosting the private source must be in the same region. See [Prerequisites for a Private Access Channel](#).

Note

If you need to connect to a private Oracle Autonomous AI Lakehouse in a different region, you can set up a custom domain for Oracle Autonomous AI Lakehouse with a custom private zone.

If my private Oracle Analytics Cloud and my private source are in the same subnet, do I need a private access channel?

Yes. You must configure a private access channel to connect to your private source even when it's in the same subnet as your Oracle Analytics Cloud.

Can I use a private access channel to access Oracle-specific DNS zones?

In most cases, no. Access to most Oracle-specific DNS zones is restricted, for example `oracle.com` and `oraclecloud.com`. You can't register these DNS zones as private sources and connect to them over a private access channel.

The only Oracle-specific DNS zones you can register as a private source in a private access channel is `<adb-name>.adb.<region>.<realm public domain>`. For example, `myadw.adb.us-ashburn-1.oraclecloud.com` or `myadw.adb.uk-gov-cardiff-1.oraclegovcloud.uk`. You can use this format to access private Oracle Autonomous AI Lakehouse and Oracle Autonomous AI Transaction Processing databases.

How do I connect to a private Oracle Autonomous AI Lakehouse in a customer VCN?

1. In Oracle Cloud Infrastructure Console, configure a private access channel for the Analytics instance that uses a subnet in the virtual cloud network (VCN) where the private Oracle Autonomous AI Lakehouse is deployed. See [Configure a Private Access Channel using the Console](#).
2. Ensure that the subnet the private access channel uses has an egress rule to communicate with the private Oracle Autonomous AI Lakehouse on port 1522. See [Working with Security Lists](#).
3. Register the private Oracle Autonomous AI Lakehouse as a private source in the private access channel using the FQDN hostname in the format `<adb-name>.adb.<region>.oraclecloud.com`. For example, `myadw.adb.us-ashburn-1.oraclecloud.com`. See [Manage the Private Sources You Can Access on a Private Access Channel Using the Console](#).
4. Obtain the *regional wallet* for the private Oracle Autonomous AI Lakehouse. See [Download Client Credentials \(Wallets\)](#).
5. In Oracle Analytics Cloud, create a connection to Oracle Autonomous AI Lakehouse that uses the regional wallet and select the service name of the private Oracle Autonomous AI Lakehouse instance you want to connect to from the list. See [Connect to Oracle Autonomous AI Lakehouse](#).

How do I connect to a private source in my Oracle Cloud Infrastructure VCN?

1. In Oracle Cloud Infrastructure Console, configure a private access channel for the Analytics instance that uses a subnet in the virtual cloud network (VCN) where the private data source is deployed. See [Configure a Private Access Channel using the Console](#).

In the **Configure Private Access Channel** page, select the checkbox **VIRTUAL CLOUD NETWORK's DOMAIN NAME as DNS ZONE**.
2. Ensure that the subnet the private access channel uses has an egress rule to communicate with the private source on its port. See [Working with Security Lists](#).
3. If you didn't select the checkbox in step 1, register the DNS zone of your VCN in the format `<VCN DNS label>.oraclevcn.com`. For example, `example.oraclevcn.com`. See [Manage the Private Sources You Can Access on a Private Access Channel Using the Console](#).
4. In Oracle Analytics Cloud, create a connection that specifies the hostname of the VCN where the private data source is deployed. See [Connect to Data for Visualizations and Analyses and Manage Data Source Connections for Semantic Models](#).

How do I connect to a private source in my corporate network peered to an Oracle Cloud Infrastructure VCN?

1. Set up a direct connection between your corporate network and Oracle Cloud Infrastructure VCN. See [Access to Your On-Premises Network](#).
2. Set up a private DNS resolver in the Oracle Cloud Infrastructure VCN. Configure a DNS forwarder in the private DNS resolver to forward corporate hostname resolution to your company's DNS server. See [Private DNS](#).
3. In Oracle Cloud Infrastructure Console, configure a private access channel for the Analytics instance that uses the subnet in the virtual cloud network (VCN) that is connected to the corporate network. See [Configure a Private Access Channel using the Console](#).
4. Ensure that the subnet the private access channel uses has an egress rule to communicate with IP address and port of the private source. See [Working with Security Lists](#).
5. Register the DNS zone of the private source in the format `<domain name>`. For example, if the data source FQDN hostname is `data-source-ds01.example.com`, add the DNS Zone as `example.com`. See [Manage the Private Sources You Can Access on a Private Access Channel Using the Console](#).
6. In Oracle Analytics Cloud, create a data source connection using the FQDN hostname `data-source-ds01.example.com`. See [Connect to Data for Visualizations and Analyses and Manage Data Source Connections for Semantic Models](#).

For private Git repositories, sign-in to Oracle Analytics Cloud, open a semantic model in Semantic Modeler, click **Toggle Git Panel** to open the Git pane and connect to the private Git repository.

How do I connect to a private source using an IP address in my corporate network peered to an Oracle Cloud Infrastructure VCN?

1. Set up a direct connection between your corporate network and Oracle Cloud Infrastructure VCN. See [Access to Your On-Premises Network](#).

2. Create a private DNS view and then add a zone (in the view) for your custom domain. For example, `ocivcn.example.com`. See [Private DNS](#).
3. In the zone you just created, add a DNS record type A, and map the IP address to the fully qualified hostname. For example, `datasource-ds-01.ocivcn.example.com`.
4. Navigate to the DNS Resolver option for your VCN and associate the private DNS VCN you created in step 2. See [Private DNS Resolver](#).
Configure one of the following:
 - DNS forwarder: Configure a DNS forwarder in the private DNS resolver to forward corporate hostname resolution to your company's DNS server. See [Private DNS](#).
 - Hostname to IP address mapping: Add a custom record type A entry for the private source IP address mapping to an FQDN hostname under a unique DNS domain. For example, if the private source IP address in your corporate network is `10.40.100.55` and your corporate DNS Zone domain is `example.com`, add a DNS record type A that maps `datasource-ds-01.ocivcn.example.com` to `10.40.100.55`.
5. In Oracle Cloud Infrastructure Console, configure a private access channel for the Analytics instance that uses the subnet in the virtual cloud network (VCN) that is connected to the corporate network. See [Configure a Private Access Channel using the Console](#).
6. Register the DNS zone of the private source in the format `ocivcn.<domain name>`. For example, if the private source DNS record is `datasource-ds-01.ocivcn.example.com`, add the DNS Zone as `ocivcn.example.com`. See [Manage the Private Sources You Can Access on a Private Access Channel Using the Console](#).
7. In Oracle Analytics Cloud, create a data source connection using the hostname `datasource-ds-01.ocivn.example.com`. See [Connect to Data for Visualizations and Analyses and Manage Data Source Connections for Semantic Models](#).

For private Git repositories, sign-in to Oracle Analytics Cloud, open a semantic model in Semantic Modeler, click **Toggle Git Panel** to open the Git pane and connect to the private Git repository.

Do I have any tools to troubleshoot connection issues to my private data sources?

Yes. You can use the *Network Path Analyzer* that's available in Oracle Cloud Infrastructure Console to troubleshoot connectivity issues. See [Troubleshoot Connectivity Issues Using Network Path Analyzer](#).

Prerequisites for a Private Access Channel

Before you configure a private access channel, you need to know the domain names of the private DNS zones or SCAN host names you want Oracle Analytics Cloud to access, check that you deployed Oracle Analytics Cloud with **Enterprise Edition**, and verify you have the correct permissions.

If your Oracle Analytics Cloud is deployed with a public endpoint, you also need to know the VCN and subnet on Oracle Cloud Infrastructure that you want Oracle Analytics Cloud to use to access the private sources. If you deployed Oracle Analytics Cloud instance with a *private endpoint*, the private access channel automatically uses the same VCN and subnet you configured for the instance so you don't need to do step 3.

1. Verify that your Oracle Analytics Cloud deployment includes **Enterprise Edition**.
Edition information is displayed on the Instance Details page. See [Verify Your Service](#).

Private access channels aren't available on Oracle Analytics Cloud instances deployed with **Professional Edition**.

2. Record the domain name of each private source (DNS zone) you want Oracle Analytics Cloud to access through the private channel.

For example, domain names such as `example.com`, `companyabc.com`, and so on.

- **Private data source in a corporate network peered to an Oracle Cloud Infrastructure VCN**

Register a DNS zone in the format: `<domain name>`

For example:

- If the data source FQDN hostname is `data-source-ds01.companyabc.com`, add the DNS Zone as `companyabc.com`.
- If the data source FQDN hostname is `db01.dbdomain.companyabc.com`, add the DNS Zone as `dbdomain.companyabc.com` to only give Oracle Analytics Cloud access to hosts under `dbdomain.companyabc.com`.

- **Private data source in an Oracle Cloud Infrastructure VCN**

Register a DNS zone in the format: `<VCN DNS label>.oraclevcn.com`

For example: `companyabc.oraclevcn.com`

Tip: If you want to connect to a private source on the same VCN as the private access channel, select the checkbox **Virtual Cloud Network's Domain Name as DNS Zone** on the Configure Private Access Channel page to auto-fill the domain name value.

- **Private Oracle Autonomous AI Lakehouse or Oracle Autonomous AI Transaction Processing in an Oracle Cloud Infrastructure VCN**

The private FQDN hostname is in the format `<adb-name>.adb.<region>.<realm-public domain>`. Register a DNS zone in the same format: `<adb-name>.adb.<region>.<realm-public-domain>`

For example:

- `myadw.adb.ap-sydney-1.oraclecloud.com`
- `myadw.adb.uk-gov-cardiff-1.oraclegovcloud.uk`

3. Record the SCAN host name and SCAN port for each private Oracle Database configured with a Single Client Access Name (SCAN) that you want Oracle Analytics Cloud to access through the private channel. For example, SCAN host names such as `db01-scan.corp.example.com` or `prd-db01-scan.mycompany.com` might use port 1521.

If you want to connect to a private DB System on Oracle Cloud Infrastructure, you can find SCAN details on the **DB System Information** page (**SCAN DNS Name** and **Port**).

Overview - Bare Metal, VM and Exadata - DB Systems - DB System Details

pac-scan-test-dbs

Scale Storage Up Change Shape Clone Add SSH Keys More Actions

DB System Information Tags

General Information

Lifecycle State: Available
 Availability Domain: akTo:US-ASHBURN-AD-2
 OCID: ...pdggjq Show Copy
 Shape: VM.Standard2.2
 Created: Fri, Mar 25, 2022, 23:11:17 UTC
 Time Zone: UTC ⓘ
 Compartment: [REDACTED]

Oracle Database Software Edition: Enterprise Edition Extreme Performance
 Storage Management Software: Oracle Grid Infrastructure
 Available Data Storage: 256 GB
 Recovery Area Storage: 256 GB
 Total Storage Size: 912 GB
 License Type: Bring Your Own License (BYOL)
 Node Maintenance Reboot: Nothing Scheduled

Network

VCN: [REDACTED]
 Client subnet: pe-tenant-data-sources-subnet
 Cluster Name: None
 Port: 1521
 Hostname Prefix: pac-rac-db
 Host Domain Name: petenantds...oraclevcn.com Hide Copy
 SCAN DNS Name: pac-rac-db-scan.petenantds...oraclevcn.com Hide Copy
 SCAN IP Address: [REDACTED]
 Network Security Groups: None Edit

- Determine the Oracle Cloud Infrastructure VCN and subnet that you want Oracle Analytics Cloud to use for the private channel.

VCN Prerequisites

- Region:** The VCN must be in the same region as Oracle Analytics Cloud.

Subnet Prerequisites

- Size:** Each private access channel requires at least four IP addresses. Two IP addresses are required for network traffic egress, one IP address for the private access channel, and one reserved for future use. This means that the minimum subnet size for a single private access channel is "/29". For example, subnet CIDR 10.0.0.0/29.

If you have more than one Oracle Analytics Cloud instance, you might need to configure multiple private access channels. If you want to use a single subnet for multiple channels, you must ensure that the subnet is sized accordingly. Alternatively, use a dedicated subnet for each private access channel.

- Egress Rule:** The subnet must include an egress rule that enables communication to the private data source (IP address and port).
- Ingress Rule:** The subnet must include an ingress rule that enables communication from the private data source.

If you're not sure, ask your network administrator.

VCN and subnet configuration tasks are typically performed by the network administrator responsible for the Oracle Cloud Infrastructure network. More information is available in *Task 1 Set up the VCN and subnet* at [Scenario B: Private Subnet with a VPN](#) or [Scenario C: Public and Private Subnets with a VPN](#).

- Ensure that you (or whoever plans to configure the private access channel for Oracle Analytics Cloud) belongs to a group that is granted the required policies to access the VCN.

Several options are available. Choose the most appropriate level for you:

Broad Resource Access Policy

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ compartments IN TENANCY

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO MANAGE virtual-network-family IN TENANCY

Limited Resource Access Policy

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ compartments IN TENANCY
- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ virtual-network-family IN compartment <compartment name of VCN>
- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO USE subnets IN compartment <compartment name of subnet>
- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO MANAGE vnics IN compartment <compartment name of Analytics instance>
- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO USE private-ips IN compartment <compartment name of Analytics instance>

Moderate Resource Access Policy - Option 1

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ compartments IN TENANCY
- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ virtual-network-family IN TENANCY
- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO USE subnets IN TENANCY
- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO MANAGE vnics IN TENANCY
- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO MANAGE private-ips IN compartment <compartment name of Analytics instance>

Moderate Resource Access Policy - Option 2

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ compartments IN TENANCY
- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO USE virtual-network-family IN compartment <compartment name of VCN>
- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO MANAGE virtual-network-family IN compartment <compartment name of Analytics instance>

6. If you plan to enable access to a data source with SCAN host and port details, ensure that you (or whoever plans to configure the private access channel for Oracle Analytics Cloud) belongs to a group that is granted the required policy to access work requests.

Choose the most appropriate level for you:

Broad Resource Access Policy

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ work-requests IN TENANCY

Limited Resource Access Policy

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ work-requests IN compartment <compartment name of Analytics instance>
7. Optional: If you plan to restrict traffic over the private access channel using *network security group rules*, you can do so when you create the channel or you can save the task for later.

If you want to configure network security groups when you create the private access channel, make sure the network security groups exist and you have the required policies to use network security groups.

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO USE network-security-groups IN TENANCY

Typical Workflow to Set Up a Private Access Channel

If you want to set up a private access channel for an Oracle Analytics Cloud instance for the first time, follow these tasks as a guide.

Task	Description	More Information
Understand prerequisites for a private access channel	Make a list of the private data sources (DNS zones and SCAN host names) or private Git repositories (DNS zones names) that you want Oracle Analytics Cloud to access through the private access channel and ensure you have the required permissions to set up the private access channel in Oracle Cloud Infrastructure.	Prerequisites for a Private Access Channel
Create an Oracle Analytics Cloud instance	Deploy Oracle Analytics Cloud with Enterprise Edition .	Create a Service
Configure a private access channel	Use Oracle Cloud Infrastructure Console to configure a private access channel and list any data sources or Git repositories that Oracle Analytics Cloud must connect to privately (DNS zones and SCAN host names). Optionally, restrict outgoing traffic (egress) on the private access channel using one or more network security groups.	Configure a Private Access Channel
Create connections to private data sources	Use Oracle Analytics Cloud to create a connection to the private data source. The way you create the connection depends on how you want to use the data source, that is, whether you want to build a visualization, analysis, pixel-perfect report, or semantic model.	Connect to Data for Visualizations and Analyses Manage Data Source Connections for Semantic Models Connect to Data for Pixel-Perfect Reports
Connect to Git repositories for collaborative semantic model development	Use Oracle Analytics Cloud Semantic Modeler to connect to Git repositories on your private network. You can connect to a Git repository with an SSH or HTTPS connection.	Upload a Semantic Model to a Git Repository Using SSH Upload a Semantic Model to a Git Repository Using HTTPS

Task	Description	More Information
Manage private sources available through a private access channel	Add, edit, or delete the private sources that Oracle Analytics Cloud can access through the private access channel. Use the DNS zone or SCAN host name to identify your private sources.	Manage the Private Sources You Can Access on a Private Access Channel Using the Console Edit a Private Access Channel using the REST API Edit a Private Access Channel using the Command Line
Edit network details for a private access channel	Change the VCN or subnet on Oracle Cloud Infrastructure that Oracle Analytics Cloud uses to access private data sources or private Git repositories. Optionally, restrict traffic over the private access channel using network security groups.	Edit Network Details for a Private Access Channel using the Console Edit a Private Access Channel using the REST API Edit a Private Access Channel using the Command Line
Delete a private access channel	Delete a private access channel that you configured for Oracle Analytics Cloud but don't need anymore.	Delete a Private Access Channel

Configure a Private Access Channel

You can configure a private access channel using the Console, API, or command line.

① Note

Required IAM Policy

Verb: manage

Resource Type: analytics-instance, analytics-instances

Custom Permission: ANALYTICS_INSTANCE_MANAGE

See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

Verb: manage

Resource Type: virtual-network-family

Verb: read

Resource Type: compartment, compartments

Resource Type: work-requests (required for SCAN host configuration)

To learn about other, more detailed access policy options, see [Prerequisites for a Private Access Channel](#).


Topics

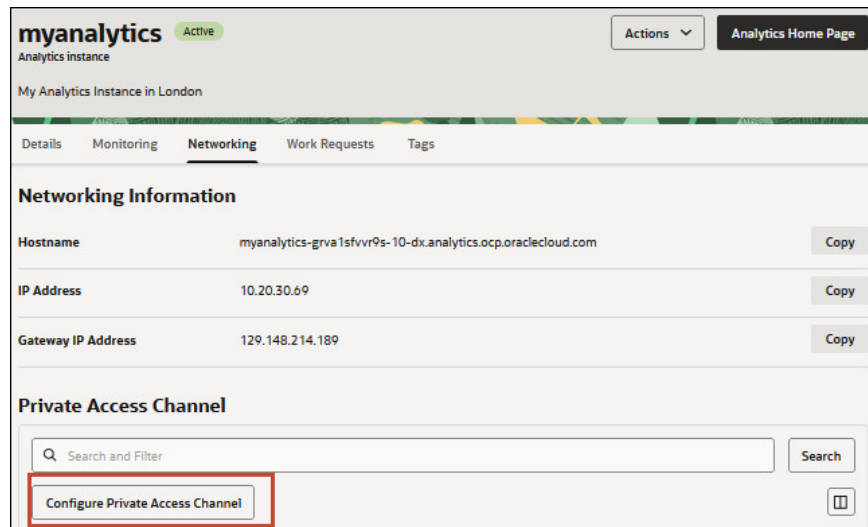
- [Configure a Private Access Channel using the Console](#)
- [Edit a Private Access Channel using the REST API](#)
- [Configure a Private Access Channel using the Command Line](#)

Configure a Private Access Channel using the Console

You can use Oracle Cloud Infrastructure Console to configure a private access channel for your Oracle Analytics Cloud instance.

When you set up a private access channel you alter the configuration of your Oracle Analytics Cloud instance. Some users might experience a temporary disruption in service during the configuration process so Oracle recommends that you plan private access channel configuration activities on critical instances accordingly.

1. In Oracle Cloud Infrastructure Console, click  in the top left corner.
2. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to configure a private access channel for.
The instance must be deployed with **Enterprise Edition**.
5. Click the **Networking** tab, navigate to the **Private Access Channel** section, and then click **Configure Private Access Channel**.



6. For **Name**, enter any name to identify the private access channel.
7. If your Oracle Analytics Cloud instance has a *public endpoint*:
 - a. Select the **Virtual Cloud Network** and the **Subnet** that you want Oracle Analytics Cloud to use to access private data sources or private Git.
 - b. Optional: If you want to restrict outgoing traffic to the private data source or private Git using egress rules in predefined network security groups, select **Configure Access Control** and then click **Add Network Security Group** to select one or more network security groups.

Click **Virtual Cloud Network Compartment** or **Subnet Compartment** to select resources from a different compartment. If you can't see the VCN, subnet, or network security group you want, check you have the required permissions.

If your Oracle Analytics Cloud instance has a *private endpoint*, the private access channel automatically uses the same VCN, subnet, and network security groups as the private endpoint. See [Create Oracle Analytics Cloud with a Private Endpoint](#).

8. Enable access to at least one private data source or to private Git:
 - a. Optional. To add the domain name associated with the selected VCN as a private source, select **Virtual Cloud Network's domain name as DNS zone**.
 - b. In **DNS Zone**, enter the name of a domain you want to give access to.

For example: `companyabc.com`

- **Private data source in a corporate network peered to an Oracle Cloud Infrastructure VCN**

Register a DNS zone in the format: `<domain name>`

For example:

- If the data source FQDN hostname is `data-source-ds01.companyabc.com`, add the DNS Zone as `companyabc.com`.
- If the data source FQDN hostname is `db01.dbdomain.companyabc.com`, add the DNS Zone as `dbdomain.companyabc.com` to only give Oracle Analytics Cloud access to hosts under `dbdomain.companyabc.com`.

- **Private data source in an Oracle Cloud Infrastructure VCN**

Register a DNS zone in the format: `<VCN DNS label>.oraclevcn.com`

For example: `companyabc.oraclevcn.com`

Tip: If you want to connect to a private source on the same VCN as the private access channel, select the checkbox **Virtual Cloud Network's Domain Name as DNS Zone** on the Configure Private Access Channel page to auto-fill the domain name value.

- **Private Oracle Autonomous AI Lakehouse or Oracle Autonomous AI Transaction Processing in an Oracle Cloud Infrastructure VCN**

The private FQDN hostname is in the format `<adb-name>.adb.<region>.<realm-public domain>`. Register a DNS zone in the same format: `<adb-name>.adb.<region>.<realm-public-domain>`

For example:

- `myadw.adb.ap-sydney-1.oraclecloud.com`
- `myadw.adb.uk-gov-cardiff-1.oraclegovcloud.uk`

- c. In **SCAN Hosts**, click **Add SCAN host** and enter the name of a SCAN host and the SCAN port you want to give access to.

For example, SCAN host names such as `db01-scan.corp.example.com` or `prd-db01-scan.mycompany.com` might use port 1521.

- d. Enter a useful description for the DNS zone or SCAN host.
- e. To add additional private sources, click **Add DNS Zone** or **Add SCAN host**.

9. Click **Configure**.

On the Analytics Instances page, the status changes to **Active** when the configuration process is complete.

10. For private data sources, to test that the private access channel is working, connect Oracle Analytics Cloud to one or more private data sources you configured and verify you can access the data in Oracle Analytics Cloud.

Note

If you're migrating to a private access channel from Remote Data Gateway, Oracle recommends that you add DNS zones for *all* connections you plan to re-route through the private access channel, and modify all their associated connections. This way, you'll avoid connection errors when you stop Remote Data Gateway to verify your connections work through the private channel.

- a. Sign-in to Oracle Analytics Cloud.
 - b. Create a connection to the private data source.

For example, if you registered the domain `companyabc.com` as a private source, set up a connection that includes this domain name.

The way you create the connection depends on how you plan to use the data source, that is, whether you want to build a visualization, analysis, pixel-perfect report, or semantic model.
 - Connect to Data for Visualizations and Analyses
 - Manage Data Source Connections for Semantic Models
 - Connect to Data for Pixel-Perfect Reports
 - c. Create a visualization, analysis, pixel-perfect report, or semantic model that uses the connection and verify you can access to the data.
11. For private Git repositories, to test that the private access channel is working, connect Oracle Analytics Cloud Semantic Modeler to the private Git repository and verify you can initialize and upload SMML development files for your semantic model.
 - a. Sign-in to Oracle Analytics Cloud.
 - b. Open a semantic model in Semantic Modeler, click **Toggle Git Panel** to open the Git pane to connect to the private Git repository.

For example, if you registered the domain `companyabc.com` for the private Git repository, set up a connection that includes this domain name.

Use SSH or HTTPS to connect to private Git. See [Upload a Semantic Model to a Git Repository Using SSH](#) or [Upload a Semantic Model to a Git Repository Using HTTPS](#).

Configure a Private Access Channel using the REST API

You can use the `CreatePrivateAccessChannel` operation to set up a private access channel for an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use this operation:

- [CreatePrivateAccessChannel](#)

Configure a Private Access Channel using the Command Line

You can use the `analytics-instance create-private-access-channel` command to set up a private access channel for an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- [analytics-instance create-private-access-channel](#)

Edit a Private Access Channel

You can edit a private access channel using the Console, API, or command line.

Note

Required IAM Policy

Verb: `manage`

Resource Type: `analytics-instance, analytics-instances`

Custom Permission: `ANALYTICS_INSTANCE_MANAGE`

See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

Verb: `manage`

Resource Type: `virtual-network-family`

Verb: `read`

Resource Type: `compartment, compartments`

Resource Type: `work-requests` (required for SCAN host configuration)

To learn about other, more detailed access policy options, see [Prerequisites for a Private Access Channel](#).

Topics

- [Edit Network Details for a Private Access Channel using the Console](#)
- [Manage the Private Sources You Can Access on a Private Access Channel Using the Console](#)
- [Edit a Private Access Channel using the REST API](#)
- [Edit a Private Access Channel using the Command Line](#)

Edit Network Details for a Private Access Channel using the Console


If you deployed your Oracle Analytics Cloud instance with a public endpoint, you can change the VCN, subnet and network security groups on Oracle Cloud Infrastructure that Oracle Analytics Cloud uses to access private sources.

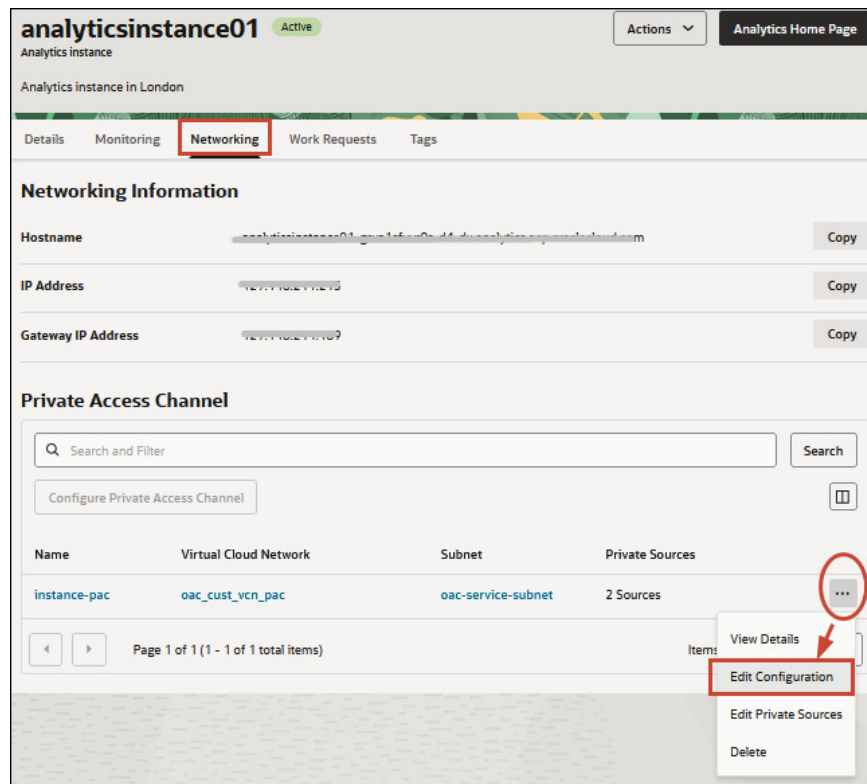
When you deploy Oracle Analytics Cloud with a private endpoint, the private access channel uses the same VCN, subnet, and network security groups you configured for the private

endpoint. To edit network settings for both the private endpoint and private network channel, see [Change the VCN or Subnet Used to Access a Private Endpoint](#).

Note

Changing the VCN or subnet impacts any private data sources or private Git repositories that you configured for this private access channel. You must ensure that the new network configuration provides a network route to these sources.

1. In Oracle Cloud Infrastructure Console, click  in the top left corner.
2. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to configure private sources for.
5. Click the **Networking** tab, and navigate to the **Private Access Channel** section.
6. Click the **Actions** menu for the private access channel you want to edit.
7. Click **Edit Configuration** to change the VCN or subnet the private channel uses or network security groups.



The screenshot shows the Oracle Cloud Infrastructure console interface for an analytics instance named 'analyticsinstance01'. The 'Networking' tab is selected, and the 'Private Access Channel' section is visible. A table lists the private access channels, with one channel named 'instance-pac' using the 'oac_cust_vcn_pac' VCN and 'oac-service-subnet' subnet. A red box highlights the 'Edit Configuration' button in the actions menu for this channel.

Name	Virtual Cloud Network	Subnet	Private Sources
instance-pac	oac_cust_vcn_pac	oac-service-subnet	2 Sources

8. Select the new **Virtual Cloud Network** or **Subnet** that you want Oracle Analytics Cloud to use to access private sources.

The private access channel and all the private sources that are associated with it inherit these changes.

You can select a VCN and subnet if your Oracle Analytics Cloud instance has a *public endpoint*. If you set up your Oracle Analytics Cloud instance for private access, the private access channel automatically uses the same VCN and subnet as the private endpoint.

Click **Virtual Cloud Network Compartment** or **Subnet Compartment** to select resources from a different compartment. If you can't see the VCN or subnet you want, check you have the required permissions.

9. If you want to restrict traffic on the private channel, click **Add Network Security Group**.

If your Oracle Analytics Cloud instance has a *public endpoint*, you can select one or more network security groups available in the same compartment as the VCN.

If your Oracle Analytics Cloud instance has a *private endpoint*, the private access channel automatically uses the same network security groups as the private endpoint.

10. Click **Update**.

You can monitor the progress of **Edit Private Access Channel** operations in the activity log. In the unlikely event an edit operation fails, Oracle recommends that you delete the private access channel and recreate it. See [Monitor Status](#).

On the Analytics Instances page, the status changes to **Active** when the configuration is complete. Some users might experience a temporary disruption in service during the configuration process.


11. Test that you can access the resources from Oracle Analytics Cloud.

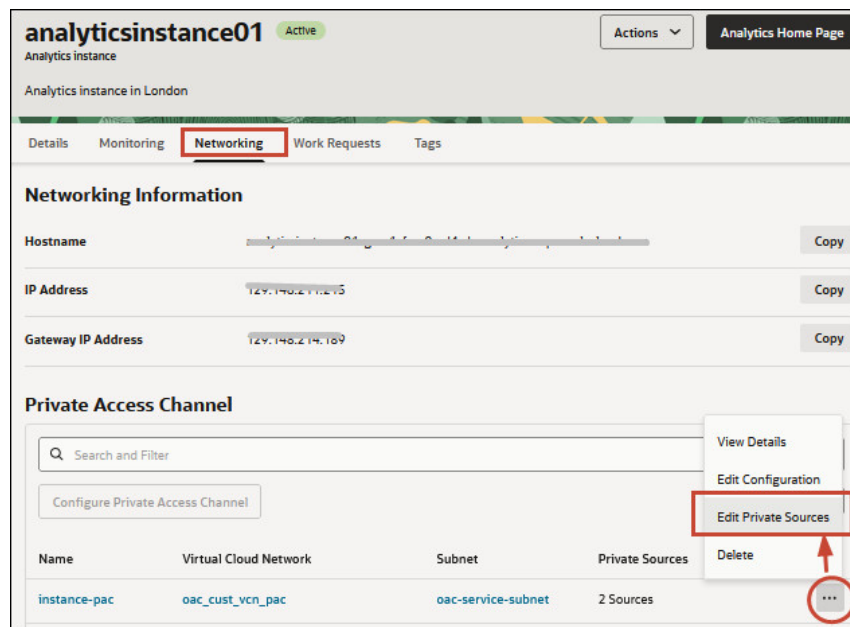
For private data sources, sign-in to Oracle Analytics Cloud, connect to one of the private data sources that you listed, and verify you have access.

For private Git repositories, sign-in to Oracle Analytics Cloud, open a semantic model in Semantic Modeler, click **Toggle Git Panel** to open the Git pane and verify that you have access.

Manage the Private Sources You Can Access on a Private Access Channel Using the Console

You can add, edit, or delete the DNS zones and SCAN hosts of private sources available through the private channel at any time.

1. In Oracle Cloud Infrastructure Console, click  in the top left corner.
2. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to configure private sources for.
5. Click the **Networking** tab, and navigate to the **Private Access Channel** section.
6. Click the **Actions** menu for the private access channel you want to edit.
7. Click **Edit Private Sources**.



8. To enable access to an additional DNS zone:
 - a. Click **Add DNS zone**.
 - b. Enter the name of the domain you want to give access to.
For example: `companyabc.com`
 - c. Enter a useful description for the domain.
9. To enable access to an additional SCAN host:
 - a. Click **Add SCAN host**.
 - b. Enter the name of the SCAN host and the SCAN port you want to give access to.
For example: `companyabc.com` on port 1521.
 - c. Enter a useful description for the domain.
10. To edit an existing DNS zone or SCAN host:
 - a. Edit the name of the private source.

Note

If your Oracle Analytics Cloud instance has working data source or Git repository connections that reference the current domain name or SCAN host name, the connections won't work after you edit the name.

- b. Edit the description.
11. To revoke access to a DNS zone or SCAN host you configured earlier, click the **X** icon for the DNS zone or SCAN host.
12. Click **Update**.

You can monitor the progress of **Edit Private Access Channel** operations in the activity log. In the unlikely event an edit operation fails, Oracle recommends that you delete the private access channel and recreate it. See [Monitor Status](#).

On the Analytics Instances page, the status changes to **Active** when the configuration is complete. Some users might experience a temporary disruption in service during the configuration process.

13. Test that you can access the resources from Oracle Analytics Cloud.

For private data sources, sign-in to Oracle Analytics Cloud, connect to one of the private data sources that you listed, and verify you have access.

For private Git repositories, sign-in to Oracle Analytics Cloud, open a semantic model in Semantic Modeler, click **Toggle Git Panel** to open the Git pane and verify that you have access.

Edit a Private Access Channel using the REST API

You can use the `UpdatePrivateAccessChannel` operation to edit a private access channel that you configured for an Oracle Analytics Cloud instance.

You can manage the DNS zones and SCAN hosts accessible through the private access channel and, if your Oracle Analytics Cloud has a public endpoint, you can change the VCN, subnet, and network security groups that the private access channel uses to access the private sources.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use this operation:

- [UpdatePrivateAccessChannel](#)

Edit a Private Access Channel using the Command Line

You can use the `analytics-instance update-private-access-channel` command to edit a private access channel that you configured for an Oracle Analytics Cloud instance.

You can manage the DNS zones and SCAN hosts accessible through the private access channel and, if your Oracle Analytics Cloud has a public endpoint, you can change the VCN, subnet, and network security groups that the private access channel uses to access the private data sources or private Git.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- [analytics-instance update-private-access-channel](#)

Delete a Private Access Channel

You can delete a private access channel using the Console, API, or command line.

Note

Required IAM Policy

Verb: manage

Resource Type: analytics-instance, analytics-instances

Custom Permission: ANALYTICS_INSTANCE_MANAGE

See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

Verb: manage

Resource Type: virtual-network-family

Verb: read

Resource Type: compartment, compartments


To learn about other, more detailed access policy options, see [Prerequisites for a Private Access Channel](#).

Topics

- [Delete a Private Access Channel using the Console](#)
- [Delete a Private Access Channel using the REST API](#)
- [Delete a Private Access Channel using the Command Line](#)

Delete a Private Access Channel using the Console

You can delete a private access channel that you configured for Oracle Analytics Cloud but don't need anymore.

1. In Oracle Cloud Infrastructure Console, click  in the top left corner.
2. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to edit.
5. Click the **Networking** tab and navigate to the **Private Access Channel** section.
6. Click the **Actions** menu for the private access channel you want to delete.
7. Click **Delete**, and then click **Delete** again to confirm.

On the Analytics Instances page, the status changes to **Active** when the deletion is complete. Some users might experience a temporary disruption in service during the configuration process.

Delete a Private Access Channel using the REST API

You can use the `DeletePrivateAccessChannel` operation to delete a private access channel for an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use this operation:

- [DeletePrivateAccessChannel](#)

Delete a Private Access Channel using the Command Line

You can use the `analytics-instance delete-private-access-channel` command to delete a private access channel for an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- [analytics-instance delete-private-access-channel](#)

Use Network Security Groups to Control Access

You can restrict incoming and outgoing traffic to Oracle Analytics Cloud through ingress and egress rules that you define in network security groups.

Topics

- [About Network Security Groups and Security Lists](#)
- [About Using Network Security Groups with Oracle Analytics Cloud](#)
- [Prerequisites for Network Security Groups](#)
- [Manage Egress Access Rules for a Public Endpoint using the Console](#)
- [Manage Ingress and Egress Access Rules for a Private Endpoint using the Console](#)
- [Top FAQs for Network Security Groups](#)

About Network Security Groups and Security Lists

The Networking service in Oracle Cloud Infrastructure (OCI) offers two virtual firewall features to control traffic at the packet level: *network security groups* and *security lists*.

- **Network security groups (NSGs):** Act as a virtual firewall for OCI resources such as Oracle Analytics Cloud. An NSG consists of a set of ingress and egress security rules that apply only to a set of VNICs of your choice in a single VCN. To learn more about NSGs and how to manage ingress and egress security rules, see [Network Security Groups](#).
- **Security lists:** The original type of virtual firewall offered by the Networking service. See [Security Lists](#).

Either option or a combination of these two features can be used. See [Comparison of Security Lists and Network Security Groups](#).

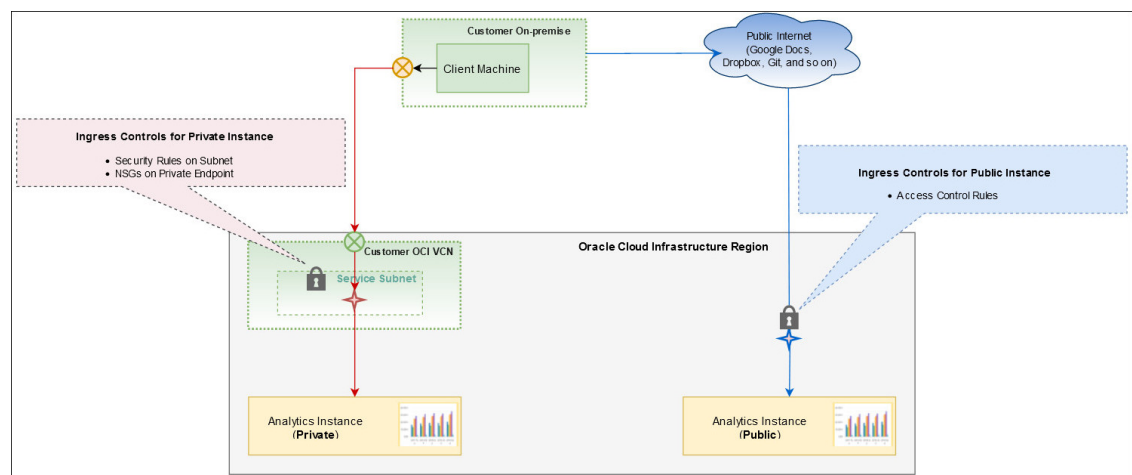
About Using Network Security Groups with Oracle Analytics Cloud

You can use network security groups (NSGs) to define ingress and egress security rules that restrict traffic to and from Oracle Analytics Cloud. This topic describes ingress and egress scenarios for Oracle Analytics Cloud.

About Ingress Scenarios for Oracle Analytics Cloud

The way you manage ingress depends whether your Oracle Analytics Cloud instance has a public or private endpoint.

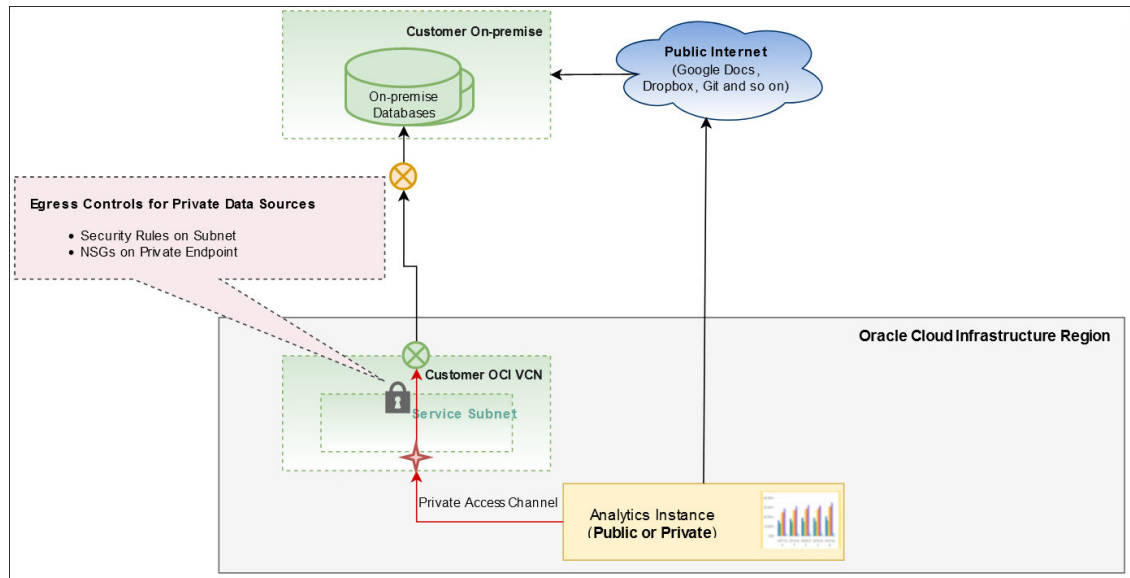
- **Public endpoint:** Use access control rules to control incoming traffic. See [Control Incoming Traffic to Public Endpoint \(Ingress\)](#).
- **Private endpoint:** Use a union of ingress rules to control incoming traffic from:
 - NSGs for the private Oracle Analytics Cloud instance. See [Control Incoming Traffic to Private Endpoint \(Ingress\)](#).
 - Security lists for the subnet.



About Egress Scenarios for Oracle Analytics Cloud

The way you manage egress depends on the data source you want to access from Oracle Analytics Cloud.

- **Publicly accessible data sources:** Oracle Analytics Cloud can egress to any data source accessible on the public internet.
- **Private data sources accessible through a private access channel:** Use a union of egress rules to control outgoing traffic from:
 - NSGs for the private access channel. See [Control Outgoing Traffic to Private Endpoint \(Egress\)](#).
 - Security lists for the private access channel subnet.




Manage Egress Access Rules for a Public Endpoint using the Console

If you deployed Oracle Analytics Cloud with a public internet accessible endpoint and you have private data sources that Oracle Analytics Cloud connects to over a private access channel, you can use egress rules that you define in *network security groups* to restrict outgoing traffic through the channel. You can add up to five network security groups.

Note

Any network security groups that you want to use must be in the same VCN as the private access channel.

1. If you haven't done so already, set up the network security groups that you want to use, and ensure you're assigned the correct policies to access to them.
2. In Oracle Cloud Infrastructure Console, click  in the top left corner.
3. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.
4. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
5. Click the name of the instance you want to control access from.
6. Click the **Networking** tab, and navigate to the **Private Access Channel** section.

If you haven't done so already, configure the private access channel, the private data sources you want this instance to connect to, and the network security groups you want the channel to use. See [Configure a Private Access Channel](#).

7. Under **Name**, click the name of the private access channel you want to edit.
8. Under **General Information**, click the **Edit** link next to **Access Control**.

instance-pac Active Delete Edit Configuration

Private Access Channel

Details

General information

IP Address 10.0.0.0/24 Copy

Subnet oac-service-subnet

Access Control Not Configured Edit

Egress IP Addresses

IP Address 10.0.0.100 Copy

IP Address 10.0.0.101 Copy

Private Sources

Search and Filter Search

Edit Private Sources +

Source Type	Allowed Destination	Description
DNS Zone	adb-...oraclecloud.com	ADW ...
SCAN Host	dx-...oraclevcn.com:1521	Scan DB ...

Page 1 of 1 (1 - 2 of 2 total items) Items per page 25

- Click **Add Network Security Group**, and then select the name of the network security group you want to give access to.

Click **Virtual Cloud Network Compartment** or **Subnet Compartment** if the network security group you're looking for is located in a different compartment.

- Click **Add Network Security Group** to give access to other network security groups. You can add up to five network security groups.

Prerequisites for Network Security Groups

Before you configure network security groups (NSGs) for your Oracle Analytics Cloud instances, complete the required prerequisites.

VCN and Subnet Configuration

Configure the VCN you want to use with or without public access. See [OCI VCN with Public and Private Subnet](#) or [OCI VCN with Only Private Subnet](#).

Ensure there's at least 4 IP addresses available in the subnet that you want Oracle Analytics Cloud to use.

Network Security Group Configuration

Configure all the NSGs you want to use in the same VCN as your Oracle Analytics Cloud instance. See [Working with Network Security Groups](#).

Add ingress rules to the NSG to control inbound traffic to a *private* Oracle Analytics Cloud instance.

Add egress rules to the NSG to control outbound traffic from a *public* or *private* Oracle Analytics Cloud instance going to private data sources (through a private access channel).

Additional Policy Requirements

You or whoever plans to configure NSGs for your Oracle Analytics Cloud instance must have the required policy to use NSGs at the tenancy level or individual compartment level:

- ALLOW GROUP <ANALYTICS ADMIN> TO USE network-security-groups in TENANCY


Manage Ingress and Egress Access Rules for a Private Endpoint using the Console

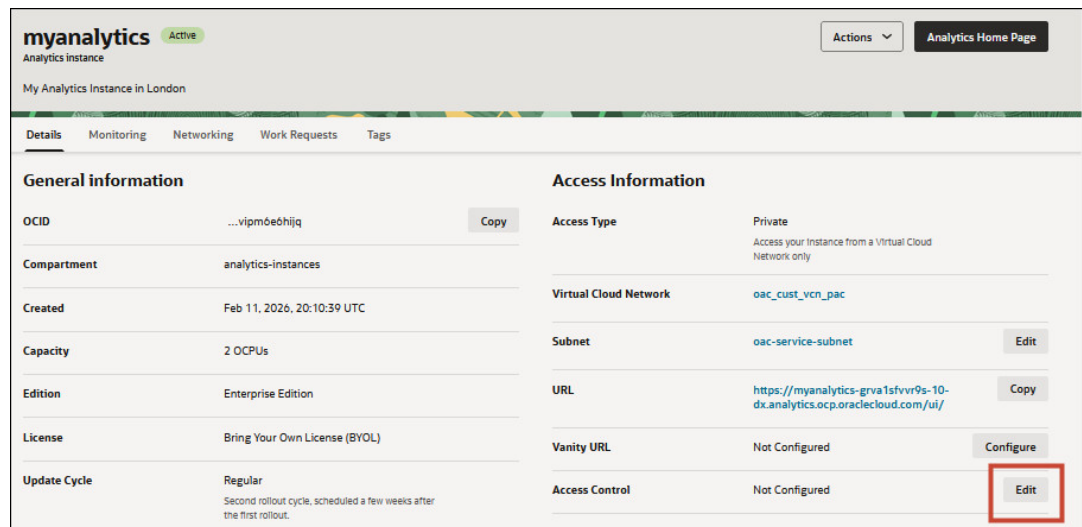
If you deployed Oracle Analytics Cloud with a private endpoint, you can restrict incoming traffic (ingress) and outgoing traffic through private access channels (egress) using predefined network security groups that contain one or more ingress or egress rules.

You define the network security groups that you want your Oracle Analytics Cloud instance to use on the Instance Details page. Ingress rules defined in the network security groups are applied to incoming traffic. If you use a private access channel to connect to private data sources, egress rules in the network security groups are applied to outgoing traffic on this private access channel.

Note

Any network security groups you want to use must be in the same VCN as your Oracle Analytics Cloud instance (and the private access channel).

1. In Oracle Cloud Infrastructure Console, click  in the top left corner.
2. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to control access to or from.
5. On the Details page, click the **Edit** link next to **Access Control**.

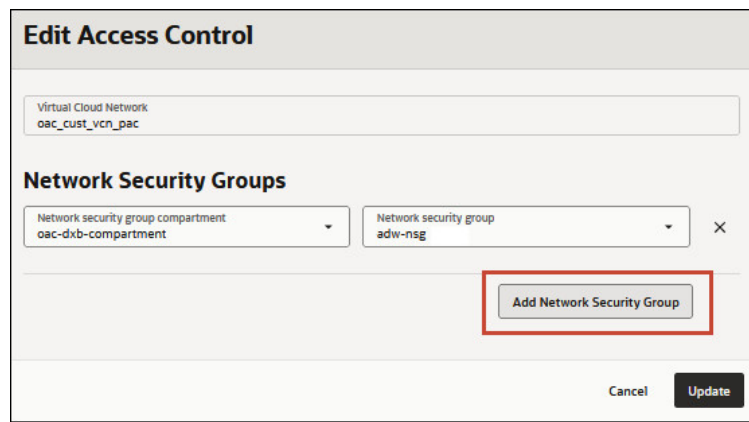


The screenshot shows the Oracle Analytics Cloud console interface. At the top, there's a header with 'myanalytics Active' and 'Analytics Home Page'. Below that, there's a navigation bar with 'Details', 'Monitoring', 'Networking', 'Work Requests', and 'Tags'. The main content area is divided into two columns: 'General information' and 'Access Information'. The 'Access Information' column has an 'Edit' button next to the 'Access Control' field, which is highlighted with a red box. The 'Access Control' field is currently set to 'Not Configured'.

General information		Access Information	
OCID	...vipm0e6hijq Copy	Access Type	Private Access your instance from a Virtual Cloud Network only
Compartment	analytics-instances	Virtual Cloud Network	oac_cust_vcn_pac
Created	Feb 11, 2026, 20:10:39 UTC	Subnet	oac-service-subnet Edit
Capacity	2 OCPUs	URL	https://myanalytics-grva1sfvr9s-10-dx.analytics.ocp.oraclecloud.com/ui/ Copy
Edition	Enterprise Edition	Vanity URL	Not Configured Configure
License	Bring Your Own License (BYOL)	Access Control	Not Configured Edit
Update Cycle	Regular Second rollout cycle, scheduled a few weeks after the first rollout.		

6. Click **Add Network Security Group**, and then select the name of the network security group you want Oracle Analytics Cloud to use for ingress and egress.

Click **Virtual Cloud Network Compartment** or **Subnet Compartment** if the network security group you're looking for is located in a different compartment.



7. Click **Add Network Security Group** to give access to other network security groups.

Federate with Oracle Identity Cloud Service Manually

In most cases, Oracle Analytics Cloud is automatically federated with the *primary* Oracle Identity Cloud Service instance associated with your tenancy. If you want to federate Oracle Analytics Cloud with a *secondary* Oracle Identity Cloud Service instance or your tenancy is a government region where federation isn't set up automatically, you must federate with Oracle Identity Cloud Service manually.



This topic applies only to cloud accounts that don't use identity domains. See [Set Up Users](#).

The way you do this depends whether your Oracle Identity Cloud Service includes the COMPUTEBAREMETAL application. If a COMPUTEBAREMETAL application doesn't exist in your tenancy, you must perform some additional steps to set up a trusted application that you can use.

Once set up, select the new Oracle Identity Cloud Service provider *before* you sign-in to Oracle Cloud and then create your Oracle Analytics Cloud instance. The new Oracle Analytics Cloud instance will use the federated Oracle Identity Cloud Service that you're signed-in with. You can't reconfigure Oracle Analytics Cloud to use a different Oracle Identity Cloud Service later on.

1. Sign-in to your Oracle Identity Cloud Service console with administrator privileges.
2. In the Oracle Identity Cloud Service console, click **Applications**.
3. Determine whether the COMPUTEBAREMETAL application is available.
 - **COMPUTEBAREMETAL application in the list**
 - a. Open the application, and click the **Configuration** tab.
 - b. Expand **General Information** and make a note of the **Client ID**.
 - c. Click **Show Secret** to display and then copy the **Client Secret**.
 - d. Skip Step 4 and go to Step 5.
 - **No COMPUTEBAREMETAL application in the list**
Continue with Step 4 to set up a trusted application.
4. Set up a trusted application.
 - a. In the Applications tab, click **Add Application**.

- b. Click **Confidential Application**.
 - c. Enter a suitable **Name** (for example, `OCI_Federation`) and **Description** (for example, Confidential application to enable federation with OCI), and then click **Next**.
 - d. In **Allowed Grant Types**, select **Resource Owner**, **Client Credentials**, and **JWT Assertion**.
 - e. In the App Roles table, add the role **Security Administrator**.
 - f. Click **Next**, and then click **Finish**.
 - g. When the Application Added dialog is displayed, make a note of the **Client ID** and **Client Secret**.
 - h. Click **Activate** and then **OK** to confirm that you want to activate the application.
5. Create a group named `OCI Administrators`.
 - a. Click the **Groups** tab.
 - b. Create a group called **OCI Administrators**, and add one or more users to the group.
6. Federate your Oracle Identity Cloud Service in Oracle Cloud Infrastructure.
 - a. Sign-in to your Oracle Cloud Infrastructure Console.
 - b. Click **Identity & Security**. Under **Identity**, click **Federation**.
 - c. Click **Add identity provider**.
 - d. Enter details about the Oracle Identity Cloud Service instance you want to use.

Enter a **Name** (for example, `MyOracleIdentityCloudProvider`), **Description**, and for Type select **Oracle Identity Cloud Service**.

Enter the Base URL for the Oracle Identity Cloud Service instance you want to use (primary or secondary), and then enter the **Client ID** and **Client Secret** values that you recorded earlier.
 - e. Click **Continue**.
 - f. Map the Oracle Identity Cloud Service group you created in Step 5 (`OCI Administrators`) to the **Administrators** group in Oracle Cloud Infrastructure.
 - g. Click **Add Provider**.

The identity provider is displayed with the status **Active**.
7. Sign out of your tenancy.

The Sign In page displays the new federated identity provider. For example `myoracleidentitycloudprovider`.

Oracle Identity Cloud Service users who sign in through the federated identity provider inherit permissions based on their Oracle Identity Cloud Service to Oracle Cloud Infrastructure group mappings. This means that users who belong to the Oracle Identity Cloud Service group `OCI Administrators` have all the permissions granted to the Oracle Cloud Infrastructure group `Administrators`.
8. In the Sign-in page, select the new federated identity provider, click **Continue**, and sign in.

Any new Oracle Analytics Cloud instances that you create will use the federated Oracle Identity Cloud Service you signed-in with.

Set Up a Custom Vanity URL

You can configure a custom vanity URL for your Oracle Analytics Cloud instance.

Topics:

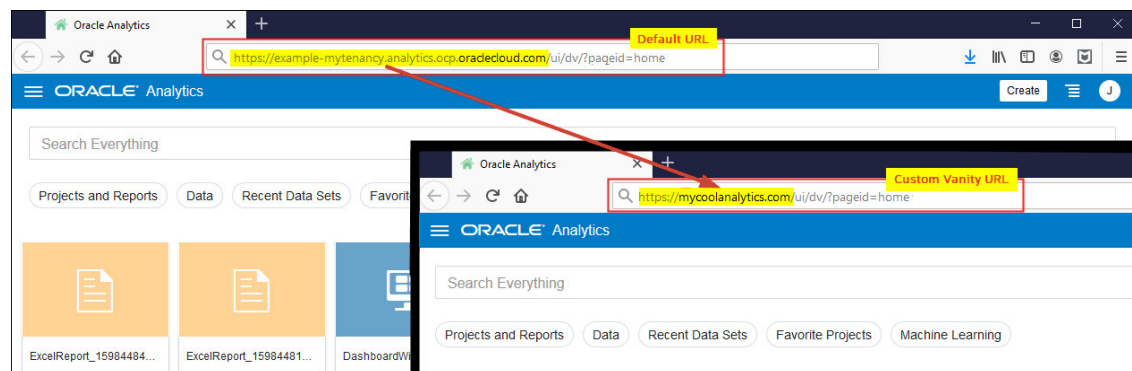
- [About Vanity URLs](#)
- [Prerequisites for a Vanity URL](#)
- [Typical Workflow to Set Up a Vanity URL](#)
- [Configure a Vanity URL](#)
- [Update Certificates for a Vanity URL](#)
- [Delete a Vanity URL](#)

About Vanity URLs

A vanity URL is a unique, customized web address that's branded for marketing purposes and helps users remember and find your web site. If you want to customize the user login experience for Oracle Analytics Cloud, you can use your own vanity URL instead of the default URL that Oracle provides.

These examples show standard URL formats for Oracle Analytics Cloud and a sample vanity URL that you might use instead:

- Standard URLs:
 - `https://example-mytenancy-<regionid>.analytics.ocp.oraclecloud.com/ui`
 - `https://example-mytenancy.analytics.<regionid>.ocp.oraclecloud.com/ui`
- Vanity URL: `https://mycoolanalytics.com/ui`



Typical Workflow to Set Up a Vanity URL

If you want to set up a vanity URL for an Oracle Analytics Cloud instance for the first time, follow these tasks as a guide.

Task	Description	More Information
Understand prerequisites for a vanity URL	Obtain the custom domain name and the required security certificates before you start.	Prerequisites for a Vanity URL
Deploy Oracle Analytics Cloud	Deploy Oracle Analytics Cloud with a public or private endpoint.	Create a Service
Configure a vanity URL	Use Oracle Cloud Infrastructure Console to configure a vanity URL.	Configure a Vanity URL
Update security certificates for the vanity domain	If the security certificate, private key file, or certificate chain associated with your vanity domain expires or changes you can upload new details.	Update Certificates for a Vanity URL

Task	Description	More Information
Delete a vanity URL	Delete a vanity URL that you configured for Oracle Analytics Cloud but don't need anymore.	Delete a Vanity URL

Prerequisites for a Vanity URL

Before you configure a vanity URL for an Oracle Analytics Cloud instance you need to know the custom domain name and valid certificate for the domain.

1. Obtain the custom domain name you want to use from a web service provider or use the domain name of your company.
2. Add a DNS entry that maps your custom domain name to the *IP address* of your Oracle Analytics Cloud instance.
See [Find the IP Address or Host Name of Your Oracle Analytics Cloud Instance](#).
3. Obtain a public digital X.509 certificate (.pem) for your vanity domain name from a Certificate Authority.
4. Obtain a private key file (.pem) that matches the certificate's public key.
5. Obtain a certificate chain for multiple certificates (.pem).

Configure a Vanity URL

You can configure a vanity URL using the Console, API, or command line.

Note

Required IAM Policy

Verb: manage

Resource Type: analytics-instance, analytics-instances

Custom Permission: ANALYTICS_INSTANCE_MANAGE


See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

Topics

- [Configure a Vanity URL using the Console](#)
- [Configure a Vanity URL using the REST API](#)
- [Configure a Vanity URL using the Command Line](#)

Configure a Vanity URL using the Console

You can use Oracle Cloud Infrastructure Console to configure a vanity URL for your Oracle Analytics Cloud instance.

1. In Oracle Cloud Infrastructure Console, click  in the top left corner.
2. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.

3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to configure a vanity URL for.
5. On the Details page, locate **Vanity URL** and click **Configure**.

The screenshot shows the Oracle Analytics Cloud console interface. At the top, there's a header with 'myanalytics Active' and 'Analytics Instance'. Below that, there's a navigation bar with 'Details', 'Monitoring', 'Networking', 'Work Requests', and 'Tags'. The 'Details' tab is selected. The main content area is divided into two columns: 'General information' and 'Access Information'. The 'Vanity URL' field in the 'Access Information' section is highlighted with a red box, and the 'Configure' button next to it is also highlighted with a red box.

General information		Access Information	
OCID	...vipm0e6hijq Copy	Access Type	Private Access your Instance from a Virtual Cloud Network only
Compartment	analytics-instances	Virtual Cloud Network	oac_cust_vcn_pac
Created	Feb 11, 2026, 20:10:39 UTC	Subnet	oac-service-subnet Edit
Capacity	2 OCPUs	URL	https://myanalytics-grva1sfvvr9s-10-dx.analytics.ocp.oraclecloud.com/ui/ Copy
Edition	Enterprise Edition	Vanity URL	Not Configured Configure
License	Bring Your Own License (BYOL)	Access Control	Not Configured Edit
Update Cycle	Regular Second rollout cycle, scheduled a few weeks after the first rollout.		

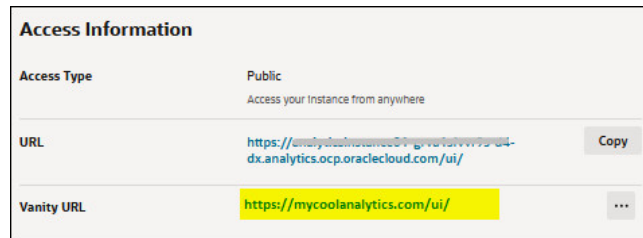
6. For **Hostname**, enter the fully qualified, custom domain name that you want to appear in the URL.

For example, enter `mycoolanalytics.com`.

A preview of the HTTPS URL is displayed. For example: `https://mycoolanalytics.com/ui/`

7. In the **Certificate** section, specify the digital X.509 (public key) certificate for your vanity domain.
 - Upload a valid certificate file in PEM format (.pem .cer .cn).
 - Paste the valid X.509 certificate text.
8. Specify the private key for this certificate.
 - Upload the private key file (.pem).
 - Paste the private key text.
9. Optional: In **Private Key passphrase**, enter the password for the private key.
10. Optional: If your certificate requires a certificate authority chain:
 - a. Select **Custom Certificate Authority Chain**.
 - b. Enter the authority chain.
 - Upload the certificate authority chain file (.pem .cer .cn).
 - Paste the authority chain text.
11. Click **Configure**.

You'll know when the vanity URL is ready to use because the URL becomes a live link in the **Access Information** section.



12. Click the link or enter the vanity URL in a browser to test you can access Oracle Analytics Cloud.

Configure a Vanity URL using the REST API

You can use the `CreateVanityUrl` operation to set up a vanity URL for an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use this operation:

- [CreateVanityUrl](#)

Configure a Vanity URL using the Command Line

You can use the `analytics-instance create-vanity-url` command to set up a vanity URL for an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- [analytics-instance create-vanity-url](#)

Update Certificates for a Vanity URL

You can update the security certificates associated with your vanity URL using the Console, API, or command line.

📘 Note

Required IAM Policy

Verb: `manage`

Resource Type: `analytics-instance`, `analytics-instances`

Custom Permission: `ANALYTICS_INSTANCE_MANAGE`


See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

Topics

- [Update Certificates for a Vanity URL using the Console](#)
- [Update Certificates for a Vanity URL using the REST API](#)
- [Update Certificates for a Vanity URL using the Command Line](#)

Update Certificates for a Vanity URL using the Console

If the security certificate, private key file, or certificate chain associated with your vanity domain expires or changes you can upload new details using the Console.

1. In Oracle Cloud Infrastructure Console, click  in the top left corner.
2. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to configure a vanity URL for.
5. On the Details page, navigate to the vanity URL, click the **Actions** icon and then select **Update**.
6. Update the digital X.509 (public key) certificate for your vanity domain.
 - Upload a valid certificate file in PEM format (.pem .cer .crt).
 - Paste the valid X.509 certificate text.
7. Update the private key for this certificate.
 - Upload the private key file (.pem .key).
 - Paste the private key text.
8. Optional: In **Private Key passphrase**, enter the password for the private key.
9. Optional: If your certificate requires a new certificate authority chain:
 - a. Select **Custom Certificate Authority Chain**.
 - b. Update the authority chain.
 - Upload the certificate authority chain file (.pem .cer .crt).
 - Paste the authority chain text.
10. Click **Update**.
11. Wait a few moments for the update to complete and then click the vanity URL link that displays in the **Access Information** section to verify you can access Oracle Analytics Cloud.

Update Certificates for a Vanity URL using the REST API

You can use the `UpdateVanityUrl` operation to update security certificates for the vanity URL that you configured for an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use this operation:

- [UpdateVanityUrl](#)

Update Certificates for a Vanity URL using the Command Line

You can use the `analytics-instance update-vanity-url` command to update security certificates for the vanity URL that you configured for an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- [analytics-instance update-vanity-url](#)

Delete a Vanity URL

You can delete a vanity URL using the Console, API, or command line.

Note


Required IAM Policy**Verb:** `manage`**Resource Type:** `analytics-instance`, `analytics-instances`**Custom Permission:** `ANALYTICS_INSTANCE_MANAGE`See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

Topics

- [Delete a Vanity URL using the Console](#)
- [Delete a Vanity URL using the REST API](#)
- [Delete a Vanity URL using the Command Line](#)

Delete a Vanity URL using the Console

You can delete a vanity URL that you configured for Oracle Analytics Cloud but don't need anymore.

1. In Oracle Cloud Infrastructure Console, click  in the top left corner.
2. Click **Analytics & AI**. Under **AI Data Platform**, click **Analytics Cloud**.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to edit.
5. On the Details page, navigate to the vanity URL, click the **Actions** icon, and then select **Remove**.
6. Click **Remove** to confirm.

Delete a Vanity URL using the REST API

You can use the `DeleteVanityUrl` operation to delete the vanity URL configured for an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use this operation:

- [DeleteVanityUrl](#)

Delete a Vanity URL using the Command Line

You can use the `analytics-instance delete-vanity-url` command to delete the vanity URL configured for an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- [analytics-instance delete-vanity-url](#)

Encrypt Sensitive Information

You can configure custom encryption keys for your Oracle Analytics Cloud instances or let Oracle manage data encryption for you.

Topics:

- [About Encryption in Oracle Analytics Cloud](#)
- [Prerequisites for Custom Encryption](#)
- [Typical Workflow to Manage Encryption](#)
- [Assign a Custom Encryption Key](#)
- [Rotate or Change the Custom Encryption Key](#)
- [Remove a Custom Encryption Key](#)

About Encryption in Oracle Analytics Cloud

Oracle Analytics Cloud provides two data encryption options:

- Oracle-managed encryption keys
- Customer-managed encryption keys

About Oracle-managed Encryption Keys

By default, Oracle manages encryption of data within Oracle Analytics Cloud using Oracle-managed keys. This doesn't include data in other platforms under your direct control. For example, data stored in cloud databases or on-premises databases that Oracle Analytics Cloud connects to.

About Customer-managed Encryption Keys

Optionally, you can use Vault services in Oracle Cloud Infrastructure to create and manage your own encryption keys for Oracle Analytics Cloud. Your customer-managed keys are used to encrypt Oracle Analytics Cloud data such as file-based datasets, any data in datasets that's configured for caching, and credentials used to connect to your data sources.

First, you create your customer-managed keys in Oracle Cloud Infrastructure Vault. Once set up, you can assign a custom encryption key to your Oracle Analytics Cloud instance. You can either specify the customer-managed key when you create your Oracle Analytics Cloud instance or assign the customer-managed key to an existing instance.

Note

To use custom encryption, your Oracle Analytics Cloud instance must be deployed with **Enterprise Edition**. Custom encryption isn't available on Oracle Analytics Cloud instances deployed with **Professional Edition**.

To configure custom encryption, you must have permissions to manage the Oracle Analytics Cloud instance, create and assign encryption keys, and access Oracle Cloud Infrastructure Object Storage. See [Prerequisites for Custom Encryption](#).

Caution

The customer-managed encryption key is stored in Oracle Cloud Infrastructure Vault, external to your Oracle Analytics Cloud instance. Deleting or disabling a customer-managed key makes your content within Oracle Analytics Cloud unreadable for everyone, including Oracle, and your Oracle Analytics Cloud instance will be inaccessible.

About Rotating Customer-managed Encryption Keys

Oracle recommends that you rotate your custom encryption key from time-to-time to maintain security compliance. After rotating your custom encryption key in Oracle Cloud Infrastructure Vault, you must assign the new key version to your Oracle Analytics Cloud instance.

1. In Oracle Cloud Infrastructure Vault, rotate the key. See [Rotate a master encryption key](#).
2. In your Oracle Analytics Cloud instance, assign the new key version. See [Rotate the custom encryption key](#).

Typical Workflow to Manage Encryption

If you want Oracle Analytics Cloud to use a custom encryption key, follow these tasks as a guide.

Task	Description	More Information
Understand prerequisites for custom data encryption	Set up a vault and create one or more master encryption keys before you start.	Prerequisites for Custom Encryption
Assign a custom encryption key to your Oracle Analytics Cloud instance	Use Oracle Cloud Infrastructure Console to assign the custom encryption key to your Oracle Analytics Cloud instance. If the Oracle Analytics Cloud instance doesn't exist yet and your custom encryption key is ready, you can create the instance with custom encryption from the start. See Create a Service .	Assign a Custom Encryption Key
Rotate a custom encryption key and update your Oracle Analytics Cloud instance	Rotate your existing encryption keys periodically to maintain security compliance, and then update your Oracle Analytics Cloud instance to use the latest version. If necessary, you can change to a different encryption key.	Rotate or Change the Custom Encryption Key

Task	Description	More Information
Remove a custom encryption key from your Oracle Analytics Cloud instance	Remove an encryption key that you configured for Oracle Analytics Cloud but don't need anymore. Use Oracle-managed keys instead.	Remove a Custom Encryption Key

Prerequisites for Custom Encryption

Before you configure custom encryption for your Oracle Analytics Cloud instance, you must set up a vault with one or more master encryption keys, and ensure that you have all the required permissions.

1. Verify that your Oracle Analytics Cloud deployment includes **Enterprise Edition**.
Custom encryption isn't available on Oracle Analytics Cloud instances deployed with **Professional Edition**. Edition information is displayed on the Instance Details page. See [Verify Your Service](#).
2. Familiarize yourself with the Vault service in Oracle Cloud Infrastructure and ensure you have permissions to manage vaults, encryption keys, and secrets. See [Overview of Vault](#) and [Let security admins manage vaults, keys, and secrets](#).
3. Set up a vault. See [Create a new vault](#).
4. Add one or more custom encryption keys. See [Create a new master encryption key](#).
5. Check you have permissions to manage the Oracle Analytics Cloud instance and assign encryption keys.

Specifically, you must belong to group that's granted permissions to:

- Create Oracle Analytics Cloud instances.
- Browse vaults and keys to enable key selection.
- Assign a key to an Oracle Analytics Cloud instance. This is required in addition to the permission to browse keys. The ability to assign keys to resources in Oracle Cloud Infrastructure requires an additional, separate permission.

For example, grant the following permissions to a user in the group `OACAdmins`. Where `<OAC-compartment-name>` is the compartment where the Analytics instance resides. `<KEY-compartment-name>` is the compartment where the key resides.

```
# Allow users in the Oracle Analytics Cloud Admins group (OACAdmins) to manage Analytics instances located in <OAC-compartment-name>. For example, MyOACCompartment.
```

```
allow group OACAdmins to manage analytics-instances in compartment <OAC-compartment-name>
```

```
# Allow users in the Oracle Analytics Cloud Admins group (OACAdmins) to browse and select vaults and keys located in <KEY-compartment-name>. For example, MyKeyCompartment.
```

```
allow group OACAdmins to read vaults in compartment <KEY-compartment-name>
```

```
allow group OACAdmins to read keys in compartment <KEY-compartment-name>
```

```
# Allow users in the Oracle Analytics Cloud Admins group (OACAdmins) to assign encryption key MyKey1 located in <KEY-compartment-name>. For example, MyKeyCompartment.
```

```
allow group OACAdmins to use key-delegate in compartment <KEY-compartment-name> where target.key.id = '<MyKey1_ocid>'
```

```
# Allow Analytics instances located in MyOACCompartment to encrypt/decrypt with MyKey1 located in MyKeyCompartment
```

```
allow any-user to use keys in compartment MyKeyCompartment where all  
{ request.principal.type='analyticsinstance',  
  request.principal.compartment.id='<MyOACCompartment_ocid>',  
  target.key.id='<MyKey1_ocid>' }
```

```
# Allow the Object Storage service to encrypt and decrypt Oracle Analytics Cloud private buckets with MyKey1 located in MyKeyCompartment (add one statement for each subscribed region)
```

```
allow service objectstorage-<region_name> to use keys in compartment MyKeyCompartment where target.key.id = '<MyKey1_ocid>'
```

Assign a Custom Encryption Key

You can assign a custom encryption key to an existing Oracle Analytics Cloud instance using the Console, API, or command line.

Note

Required IAM Policy

Verb: manage

Resource Type: analytics-instance, analytics-instances

Custom Permission: ANALYTICS_INSTANCE_MANAGE

See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

Verb: use

Resource Type: key-delegate

Verb: read

Resource Type: vaults, keys

See [Prerequisites for Custom Encryption](#).

Topics


- [Assign a Custom Encryption Key using the Console](#)
- [Assign a Custom Encryption Key using the REST API](#)
- [Assign a Custom Encryption Key using the Command Line](#)

Assign a Custom Encryption Key using the Console

You can use Oracle Cloud Infrastructure Console to assign a custom encryption key for your Oracle Analytics Cloud instance.

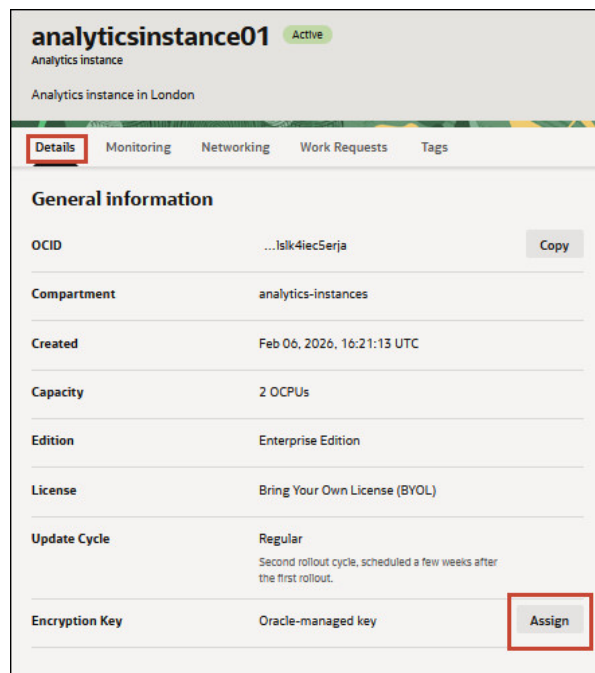
1. If you haven't done so already, create a master encryption key for your Oracle Analytics Cloud instance.

See [Create new master encryption key](#).

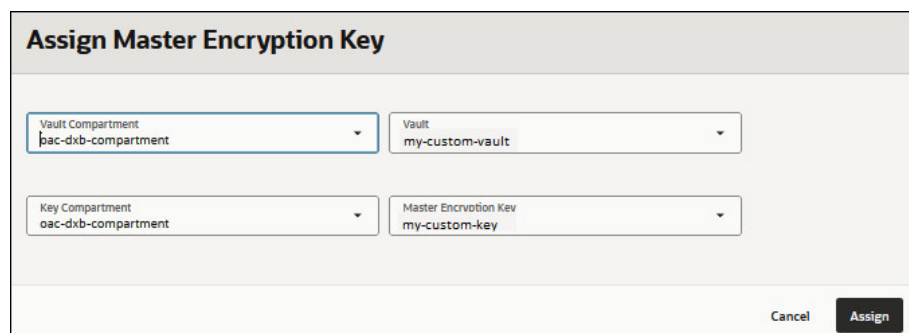
2. In Oracle Cloud Infrastructure Console, click  in the top left corner.
3. Under **Solutions and Platform**, select **AI Data Platform**, then **Analytics Cloud**.
4. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
5. Click the name of the instance that you want to use custom encryption.

The Oracle Analytics Cloud instance must be deployed with **Enterprise Edition**. Custom encryption isn't available on Oracle Analytics Cloud instances deployed with **Professional Edition**.

6. On the Details page, navigate to **Encryption Key** and click **Assign**.



7. In **Vault**, select the vault where the master encryption key is stored.
If the vault you're looking for isn't in the current compartment, click **Vault Compartment**.



8. In **Master Encryption Key**, select the name of the key you want to use for data encryption.
If the key you're looking for isn't in the current compartment, click **Key Compartment**.

9. Click **Assign**.

The Activity Log shows UPDATE_INSTANCE_ENCRYPTION_KEY in progress. The new encryption key is ready to use when you see the message `Successfully assigned Master Encryption Key`. The key update might take some time to complete; the length of time depends on the system load and the amount of data that requires re-encryption.

Assign a Custom Encryption Key using the REST API

You can use the `SetKmsKey` operation to assign a custom encryption key for an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use this operation:

- [SetKmsKey](#)

Assign a Custom Encryption Key using the Command Line

You can use the `analytics-instance set-kms-key` command to assign a custom encryption key for an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- [analytics-instance set-kms-key](#)

Rotate or Change the Custom Encryption Key

Each time you rotate your custom encryption key (or have to change to a different custom encryption key), you must update your Oracle Analytics Cloud instance. You can update the custom encryption key for an Oracle Analytics Cloud instance using the Console, API, or command line.

Each master encryption key is automatically assigned a key version. When you rotate a key, the Vault service generates a new key version. Periodically rotating keys limits the amount of data encrypted or signed by a single key version. If a key is ever compromised, key rotation reduces the risk. Each key's unique identifier (OCID), remains the same across rotations, but the key version lets the Vault service seamlessly rotate keys to meet any security compliance requirements you might have. Although Oracle Analytics Cloud doesn't use an older key version for encryption after you rotate a key, older key versions remain available to decrypt any Oracle Analytics Cloud data that it previously encrypted.

Note**Required IAM Policy****Verb:** manage**Resource Type:** analytics-instance, analytics-instances**Custom Permission:** ANALYTICS_INSTANCE_MANAGESee [About Permissions to Manage Oracle Analytics Cloud Instances](#).**Verb:** use**Resource Type:** key-delegate**Verb:** read**Resource Type:** vaults, keysSee [Prerequisites for Custom Encryption](#).**Topics**

- [Rotate or Change the Custom Encryption Key using the Console](#)
- [Rotate or Change the Custom Encryption Key using the REST API](#)
- [Rotate or Change the Custom Encryption Key using the Command Line](#)


Rotate or Change the Custom Encryption Key using the Console

Oracle recommends that you rotate your custom encryption key from time-to-time to maintain security compliance. After rotating your encryption key, you can use the Console to assign the new key version to your Oracle Analytics Cloud instance.

If for any reason you need to change to a different encryption key, you can do this from the Console too.

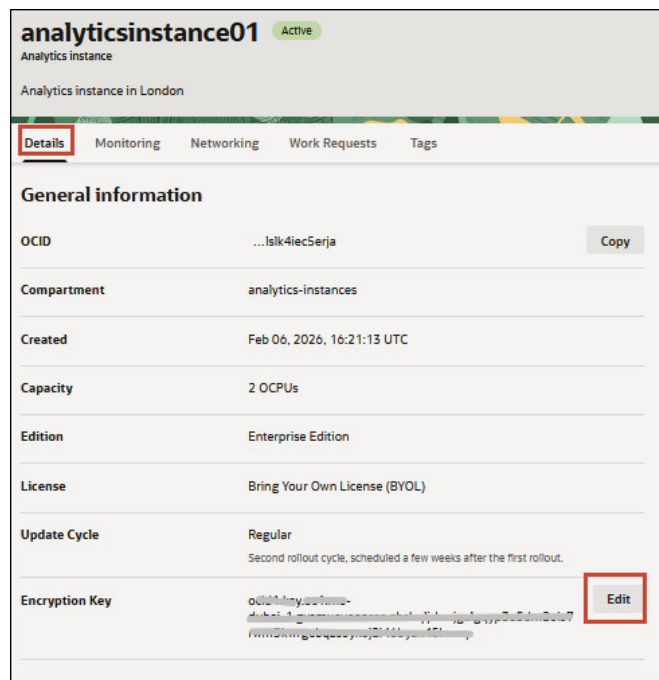
1. In Oracle Cloud Infrastructure Console, rotate the existing encryption key or set up a new one.

See [Rotate a master encryption key](#) or [Create new master encryption key](#).

2. In Console, click  in the top left corner.
3. Under **Solutions and Platform**, select **AI Data Platform**, then **Analytics Cloud**.
4. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
5. Click the name of the instance you want to update data encryption details for.

The Oracle Analytics Cloud instance must be deployed with **Enterprise Edition**. Custom encryption isn't available on Oracle Analytics Cloud instances deployed with **Professional Edition**.

6. On the Details page, navigate to **Encryption Key** and click **Edit**.



7. Do one of the following:

- **Rotate the existing master encryption key:** You don't need to select new values for **Vault** or **Master Encryption Key**. When you click **Update**, the latest version of the key will be used to encrypt data.
- **Change the master encryption key:** Use **Vault** and **Master Encryption Key** to select a different encryption key.
If the vault or key you're looking for isn't in the current compartment, click **Vault Compartment** or **Key Compartment**.

8. Click **Update**.

The Activity Log shows UPDATE_INSTANCE_ENCRYPTION_KEY in progress. The encryption key is ready to use when you see the message *Successfully changed the Master Encryption Key*. The key update might take some time to complete; the length of time depends on the system load and the amount of data that requires re-encryption.

Rotate or Change the Custom Encryption Key using the REST API

You can use the `SetKmsKey` operation to rotate an existing encryption key (refresh the same key OCID) or change the encryption key (configure a new key OCID) for an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use this operation:

- [SetKmsKey](#)

Rotate or Change the Custom Encryption Key using the Command Line

You can use the `analytics-instance set-kms-key` command to rotate an existing encryption key (refresh the same key OCID) or change the encryption key (configure a new key OCID) for an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- [analytics-instance set-kms-key](#)

Remove a Custom Encryption Key

You can remove a custom encryption key at any time and let Oracle manage data encryption for you. You can remove the key using the Console, API, or command line.

Note

Required IAM Policy

Verb: manage

Resource Type: analytics-instance, analytics-instances

Custom Permission: ANALYTICS_INSTANCE_MANAGE

See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

Verb: use

Resource Type: key-delegate

Verb: read

Resource Type: vaults, keys


See [Prerequisites for Custom Encryption](#).

Topics

- [Remove a Custom Encryption Key using the Console](#)
- [Remove a Custom Encryption Key using the REST API](#)
- [Remove a Custom Encryption Key using the Command Line](#)

Remove a Custom Encryption Key using the Console

You can remove a custom encryption key that you configured for Oracle Analytics Cloud but don't need anymore.

1. In Console, click  in the top left corner.
2. Under **Solutions and Platform**, select **AI Data Platform**, then **Analytics Cloud**.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to update data encryption details for.
5. On the Details page, navigate to **Encryption Key**, click the **Actions** icon, then click **Remove**.
6. Click **Remove** to confirm.

Key removal might take some time to complete. The length of time depends on the system load and the amount of data that requires re-encryption.

Remove a Custom Encryption Key using the REST API

You can use the `SetKmsKey` operation to remove a custom encryption key configured for an Oracle Analytics Cloud instance. To remove the current key, specify an *empty string* for the `kmsKeyId`.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use this operation:

- [SetKmsKey](#)

Remove a Custom Encryption Key using the Command Line

You can use the `analytics-instance set-kms-key` command to remove a custom encryption key configured for an Oracle Analytics Cloud instance. To remove the current key, specify an *empty string* for the `kmsKeyId`.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- [analytics-instance set-kms-key](#)

6

Frequently Asked Questions

Here are answers to common questions asked by administrators creating and managing services for Oracle Analytics Cloud.

Topics

- [Top FAQs for Administration](#)
 - [When do I use the Oracle Cloud Infrastructure Console? Is this the same as the Console available in my service?](#)
 - [How do I access Oracle Analytics Cloud pages in Oracle Cloud Infrastructure Console?](#)
 - [What is an OCPU?](#)
 - [How can I determine the right compute size for my initial deployment?](#)
 - [How do I access my service once it's created?](#)
 - [How do I patch \(or upgrade\) my service?](#)
 - [Does Oracle send notifications for all service updates?](#)
 - [Can I postpone or reschedule service updates?](#)
 - [Why does the status of my service show as "Updating"?](#)
 - [How do I increase the processing capacity of my service?](#)
 - [I want to connect to the database where my organization's analytics data is stored. Do I do this from Oracle Cloud Infrastructure Console?](#)
 - [What network options can I use to manage access into and out from my service?](#)
 - [How do I configure VPN connectivity for my service to my network?](#)
 - [Is IPv6 supported?](#)
 - [How can I find information about the identity provider my Oracle Analytics Cloud uses?](#)
 - [Can I change the identity provider that Oracle Analytics Cloud uses?](#)
 - [How can I tell my Oracle Analytics Cloud service is deployed on Gen 2?](#)
 - [Where do I manage usage and costs?](#)
 - [How do I get support for Oracle Analytics Cloud?](#)
 - [Is there a charge for Oracle Support in addition to my subscription fee?](#)
 - [Do I have direct access to the file system associated with my service?](#)
- [Top FAQs For Backup and Restore User Content \(Snapshots\)](#)
 - [What do I need to back up?](#)
 - [How often should I take snapshots?](#)
 - [When should I export snapshots?](#)
 - [Can I use APIs to automate snapshot operations?](#)

- [Can Oracle help to restore lost content?](#)
- [Top FAQs For Disaster Recovery](#)
 - [What capabilities in Oracle Analytics Cloud can I use to implement a disaster recovery plan?](#)
 - [Where can I find information about disaster recovery?](#)
- [Top FAQs for Public or Private Endpoint Security](#)
 - [In which regions is this feature available?](#)
 - [Can I use REST API or Command Line Interface \(CLI\) to create my Oracle Analytics Cloud instance with a public or private endpoint?](#)
 - [Why can't I see the VCN I want to use in the Create Instance dialog?](#)
 - [My Oracle Analytics Cloud instance has a public endpoint. Can I change this to a private endpoint?](#)
 - [How can I control access to my public endpoint?](#)
 - [I created an Oracle Analytics Cloud instance with a public endpoint and defined access rules but I'm unable to access the Oracle Analytics Cloud URL from my browser?](#)
 - [How many different access rules can I define for a public endpoint?](#)
 - [I created an Oracle Analytics Cloud instance with a private endpoint but I'm unable to access the Oracle Analytics Cloud URL from my browser?](#)
 - [How can I control access to my private endpoint?](#)
 - [Where can I find the IP address for my Oracle Analytics Cloud instance?](#)
 - [Do I have any tools to test or debug network issues from my corporate network?](#)
- [Top FAQs for Network Security Groups](#)
 - [What is a network security group or NSG?](#)
 - [Can I use NSGs in Oracle Analytics Cloud?](#)
 - [Can I use NSG ingress rules to restrict access into my public Oracle Analytics Cloud instance?](#)
 - [I applied a NSG to my Oracle Analytics Cloud instance and now I need to update the rules. Can I update or add new rules to the NSG?](#)
 - [I applied a NSG with both ingress and egress rules to my Oracle Analytics Cloud instance. What's the impact on access to and from Oracle Analytics Cloud?](#)
 - [How many NSGs can I apply to my Oracle Analytics Cloud instance?](#)
 - [If I apply multiple NSGs to my Oracle Analytics Cloud instance, what happens?](#)
 - [Can I use one set of NSGs to control access to my private Oracle Analytics Cloud instance and a different set of NSGs to control access to my private data sources?](#)
- [Top FAQs for Private Sources](#)
 - [What data sources can I connect to over a private access channel?](#)
 - [When I connect to my private source in Oracle Analytics Cloud, do I specify the domain name or the IP address of my private source?](#)
 - [My private Oracle Database has a Single Client Access Name \(SCAN\). Can I use the SCAN host name to connect to my private data source?](#)

- [I have several private data sources and private Git repositories. Do I access all of them over a single private access channel?](#)
- [How long does it take to create, update, or delete private sources?](#)
- [Can I add and remove private sources or edit the private access channel?](#)
- [How do I control access to the private sources on my private access channel?](#)
- [Can I use both a private access channel and Remote Data Gateway?](#)
- [Can I set up a private access channel with Oracle Analytics Cloud Classic or Oracle Analytics Cloud Gen 1?](#)
- [Can I use the private access channel to access a private source on a different OCI region?](#)
- [If my private Oracle Analytics Cloud and my private source are in the same subnet, do I need a private access channel?](#)
- [Can I use a private access channel to access Oracle-specific DNS zones?](#)
- [How do I connect to a private Oracle Autonomous AI Lakehouse in a customer VCN?](#)
- [How do I connect to a private source in my Oracle Cloud Infrastructure VCN?](#)
- [How do I connect to a private source in my corporate network peered to an Oracle Cloud Infrastructure VCN?](#)
- [How do I connect to a private source using an IP address in my corporate network peered to an Oracle Cloud Infrastructure VCN?](#)
- [Do I have any tools to troubleshoot connection issues to my private data sources?](#)
- [Top FAQs for Vanity URLs](#)
 - [How many vanity URLs can I create for my Oracle Analytics Cloud instance?](#)
 - [Does the standard URL continue to work?](#)
 - [Can I use a self-signed certificate when defining a vanity URL?](#)
 - [Are wildcard certificates supported?](#)
 - [Can I try this feature without registering a public DNS entry?](#)
 - [Users accessing the vanity URL report the error "400 Bad Request - Request Header Or Cookie Too Large". How do I resolve this?](#)
- [Top FAQs for Data Encryption](#)
 - [What is the difference between Oracle-managed and customer-managed encryption?](#)
 - [Why can't I see the vault or encryption key I want to use for my Oracle Analytics Cloud instance?](#)
 - [What happens if the custom encryption key my Oracle Analytics Cloud instance uses is deleted or disabled?](#)

Top FAQs for Administration

The top FAQs for Oracle Analytics Cloud administration are identified in this topic.

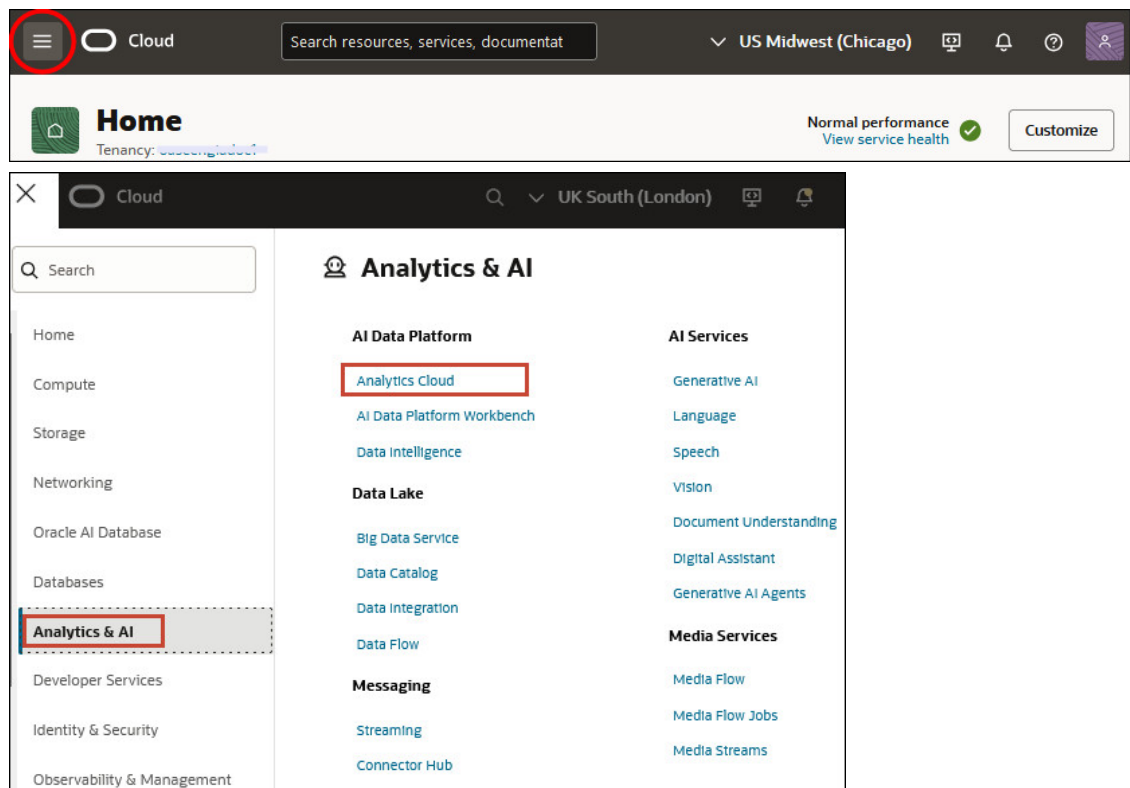
When do I use the Oracle Cloud Infrastructure Console? Is this the same as the Console available in my service?

- **Oracle Cloud Infrastructure Console** — You use the Oracle Cloud Infrastructure Console to create your Oracle Analytics Cloud instance and perform instance-level operations such as delete, scale, pause, and resume.
- **Console in Oracle Analytics Cloud** — When you sign in to a particular service, you see a different administrative console where you can customize and manage the environment for that service only.

To access the Console for a service, sign in to the service, open the **Navigator**, and then click **Console**.

How do I access Oracle Analytics Cloud pages in Oracle Cloud Infrastructure Console?

You create and manage Oracle Analytics Cloud environments through the **Analytics Cloud** menu (under **Analytics and AI**). Click the navigation menu on the home page to access the **Analytics and AI** menu.



What is an OCPU?

An Oracle Compute Unit (OCPU) is the processing unit that Oracle uses to build your service. The larger the compute size, the greater the processing power. When you create a service with Oracle Analytics Cloud, you specify the number of OCPUs you want to deploy. For more information, see [What Sizing Options Are Available to You?](#)

See also, [Oracle PaaS and IaaS Universal Credits Service Descriptions](#).

How can I determine the right compute size for my initial deployment?

A good starting point, is a size that closely matches your on-premises hardware for business intelligence.

If you're not sure which size to use, contact your Oracle representative to discuss sizing guidelines.

How do I access my service once it's created?

It's accessible from the Oracle Cloud Infrastructure Console. Navigate to **Analytics Cloud**, click the name of the service instance you want to access, and then click **Analytics Home Page**.

How do I patch (or upgrade) my service?

You don't need to patch your service. Oracle takes care of patching for you.

Does Oracle send notifications for all service updates?

Oracle notifies customers 2 weeks in advance about service updates that introduce new product capabilities to help users take advantage of new product features. Oracle sends a notification for each Oracle Analytics Cloud environment that you manage which details the *actual date* the service update will be applied.

Oracle doesn't send notifications for maintenance updates that contain stability improvements to existing product features.

Oracle automatically applies the latest update (if available) to new Oracle Analytics Cloud instances within 72 hours of their creation.

All updates to Oracle Analytics Cloud have zero customer downtime.

Can I postpone or reschedule service updates?

No. Oracle delivers innovative product updates on a regular basis, with zero customer downtime.

From November 2024, you can't reschedule service updates through service requests with Oracle Support. Instead, you can formally categorize the update cycle for your Oracle Analytics Cloud instances as either Early or Regular so that software updates can be applied on a sequence. You can be the first to explore new features and stagger updates between your environments. See [Do You Want Early Access to Updates?](#)

Why does the status of my service show as "Updating"?

In Oracle Cloud Infrastructure Console, the **Updating** status indicates that your Analytics Instance is undergoing maintenance or in the process of scaling up or down, paused or resumed. You can't perform other lifecycle operations (such as pause, resume, and scale) while the status is **Updating**. When the status changes to **Active**, the operations become available. See .

How do I increase the processing capacity of my service?

If your needs change, you can scale the number of Oracle Compute Units (OCPU) or users that your service uses. See [About Scaling](#).

 [LiveLabs Sprint](#)

I want to connect to the database where my organization's analytics data is stored. Do I do this from Oracle Cloud Infrastructure Console?

No. You connect to the data you want to analyze within a given service that you created. See [How do I access my service once it's created?](#)

What network options can I use to manage access into and out from my service?

Oracle Analytics Cloud provides options to restrict access when deployed with a public endpoint or a private endpoint. See [Restrict Access to Oracle Analytics Cloud Deployed with a Public Endpoint](#) and [Deploy Oracle Analytics Cloud with a Private Endpoint](#).

How do I add the IP address of my Oracle Analytics Cloud instance to my database allowlist?

See [Add the IP Address of Your Oracle Analytics Cloud Instance to Allowlists](#).

How do I configure VPN connectivity for my service to my network?

VPN is a separate feature from your service and is available to use with some Oracle Cloud services. Contact your Oracle representative for more information.

Is IPv6 supported?

No, not currently.

How can I find information about the identity provider my Oracle Analytics Cloud uses?

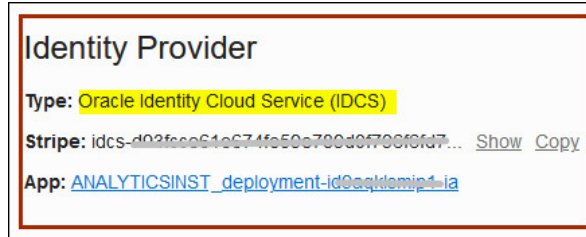
If your cloud account offers *identity domains*, your Oracle Analytics Cloud uses identity domains to manage users and groups. You can access information about the identity domain your Oracle Analytics Cloud uses on the **Details** tab in the Oracle Cloud Infrastructure (Domain name, Domain URL, associated identity application).

The screenshot displays the Oracle Cloud Infrastructure console for an Oracle Analytics Cloud instance named 'analyticsinstance01'. The 'Details' tab is selected, showing various configuration parameters. The 'Identity Provider' section is highlighted with a red box, indicating the identity provider used for user and group management.

General information		Access Information	
OCID	...lsk4iec5erja	Access Type	Public Access your instance from anywhere
Compartment	analytics-instances	URL	https://analyticsinstances01-grva1stvv9s-d4-me-dubai-1.oraclecloud.com/ui/
Created	Feb 06, 2026, 16:21:13 UTC	Vanity URL	https://analyticsinstances01-grva1stvv9s-d4-me-dubai-1.oraclecloud.com/ui/
Capacity	2 OCPUs	Access Control	Not Configured
Edition	Enterprise Edition	Identity Provider	
License	Bring Your Own License (BYOL)	Type	Identity Domain
Update Cycle	Regular Second rollout cycle, scheduled a few weeks after the first rollout.	Domain	OracleIdentityCloudService
Encryption Key	Oracle-managed key	App	ANALYTICSINST_analyticsinstance01-grva1stvv9s-d4_me-dubai-1

If identity domains aren't available in your cloud account, your Oracle Analytics Cloud uses Oracle Identity Cloud Service for identity management. In this case, the **Details** tab displays information about Oracle Identity Cloud Service instance (also referred to as the *stripe*) your

Oracle Analytics Cloud uses (Stripe name, associated identity application).



Can I change the identity provider that Oracle Analytics Cloud uses?

No. You can't switch to a different identity provider after you've created the Oracle Analytics Cloud instance. See [Which Identity Provider and Administrator Do You Want for Your Service?](#)

How can I tell my Oracle Analytics Cloud service is deployed on Gen 2?

You can tell your service is deployed on Oracle Cloud Infrastructure Gen 2 as its URL contains a *region identifier*. For example:

- <https://myoacservice-idabcd0efghj-ia.analytics.ocp.oraclecloud.com/ui/>

This Gen 2 URL includes the region identifier `-ia`, which indicates that the service is deployed in the Ashburn region.

For data regions available after 5th August 2022, such as Queretaro (Mexico), the region identifier appears slightly differently. For example, the Gen 2 URL might look something like this:

- <https://myoacservice-idabcd0efghj.analytics.mx-queretaro-1.opc.oraclecloud.com/ui/>

Where do I manage usage and costs?

When you start to deploy services on Oracle Cloud Infrastructure Gen 2, Oracle recommends that you start to view your service usage costs from the **Cost Analysis** page in Oracle Cloud Infrastructure Console. From here, you can view usage information for the new services you deploy on Oracle Cloud Infrastructure Gen 2, alongside your existing services. See [Analyze Costs for Oracle Analytics Cloud](#) and [Checking Your Balance and Usage](#) in Oracle Cloud Infrastructure documentation.

How do I get support for Oracle Analytics Cloud?

Go to [My Oracle Support](#) and create a service request.

Is there a charge for Oracle Support in addition to my subscription fee?

No. Support is included in your subscription fee.

Do I have direct access to the file system associated with my service?

No. You can't access the file system for your service. Your service is managed by Oracle.

Top FAQs For Backup and Restore User Content (Snapshots)

The [Oracle Cloud Hosting and Delivery Policy](#) describes the backup strategy for Oracle Cloud Services. In addition, customers using Oracle Analytics Cloud must take their own regular backups of their content.

The top FAQs for Oracle Analytics Cloud backup and restore are identified in this topic.

What do I need to back up?

Oracle recommends that you regularly back up all the content that users create to a file called a *snapshot*. User content includes catalog content such as reports, dashboards, data visualization workbooks, pixel perfect reports, datasets, data flows, semantic models, security roles, service settings, and so on.

If something goes wrong with your content or service, you can revert to the content you saved in a snapshot. Snapshots are also useful if you want to move or share content from one service to another.

To back up user content, see [Take a Snapshot](#).

To restore user content, see [Restore from a Snapshot](#).

How often should I take snapshots?

Oracle recommends that you take snapshots at significant checkpoints, for example, before you make a major change to your content or environment. In addition, Oracle recommends that you take regular weekly snapshots or at your own defined frequency based on the rate of change of your environment and rollback requirements.

You can keep up to 40 snapshots online and export as many as you want offline (that is, to your local file system or to your own Oracle Cloud storage).

When should I export snapshots?

Oracle recommends that you adopt a regular practice of exporting snapshots to offline storage. You can export snapshots to your own file system and store them locally. Or, you can export snapshots to your own Oracle Cloud storage. See [Export Snapshots](#).

If you regularly export large snapshots (over 5GB or larger than the download limit of your browser), Oracle recommends that you set up a storage bucket on Oracle Cloud and save your snapshots to cloud storage. This way, you can avoid export errors due to size limitations and timeouts that can sometimes occur when you export snapshots on your local file system. See [Set Up a Oracle Cloud Storage Bucket for Snapshots](#).

Can I use APIs to automate snapshot operations?

Yes. See [Manage Snapshots Using REST APIs](#).

Can Oracle help to restore lost content?

No. Customer data backup, retention, and recovery or restoration is the sole responsibility of the customer using snapshots (BAR files), catalog archives (CATALOG files), and export archives (DVA files). Oracle-managed infrastructure backups are created to maintain the service in the event of an infrastructure incident. Oracle-maintained backups aren't provided for user-created data management. See [Oracle PaaS and IaaS Public Cloud Services - Pillar document](#).

Oracle recommends that you use the Logging service in Oracle Cloud Infrastructure to track and troubleshoot content changes between snapshots. When you enable usage and diagnostic logs, you can monitor create, update, delete, and permission change operations on all catalog objects, such as classic analyses, dashboards, workbooks, pixel-perfect reports, folders, datasets, self-service connections, data flows, sequences, scripts, and so on. See [Monitor Usage and Diagnostic Logs](#).

Top FAQs For Disaster Recovery

The [Oracle PaaS and IaaS Public Cloud Services - Pillar document](#) provides information about Oracle Cloud Service continuity policy and service level agreements. In addition, your organization must adopt a well-architected business continuity plan that enables you to recover as quickly as possible and continue to provide services to your Oracle Analytics Cloud users.

What capabilities in Oracle Analytics Cloud can I use to implement a disaster recovery plan?

Oracle Analytics Cloud offers several features that you can implement to minimize disruption for users:

- **Snapshots:** Oracle recommends that you back up user content regularly to a snapshot. If required, you can restore the content in your snapshot to a redundant Oracle Analytics Cloud environment. See [Take Snapshots and Restore](#).
- **Pause and resume:** You can deploy a passive backup Oracle Analytics Cloud environment, and use the pause and resume feature to control metering and minimize costs. See [Pause and Resume a Service](#).
- **Diverse regional availability:** Oracle Analytics Cloud is available in several global regions. You can deploy a redundant Oracle Analytics Cloud environment in a different region to mitigate the risk of region-wide events. See [Data Regions for Platform and Infrastructure Services](#).

Where can I find information about disaster recovery?

See [Technical Papers](#). For additional help or assistance, engage consulting resources (Oracle or a third party) or reach out to [Oracle Analytics Community](#).

Top FAQs for Public or Private Endpoint Security

The top FAQs for securing access to Oracle Analytics Cloud through a public or private endpoint are identified in this topic.

In which regions is this feature available?

All regions.

Can I use REST API or Command Line Interface (CLI) to create my Oracle Analytics Cloud instance with a public or private endpoint?

Yes. You can use the Console, REST API or CLI commands. See [Create a Service](#).

Why can't I see the VCN I want to use in the Create Instance dialog?

You must select the compartment in which the VCN was created and you must have the required permissions. See [Prerequisites for a Public Endpoint](#) and [Prerequisites for a Private Endpoint](#).

My Oracle Analytics Cloud instance has a public endpoint. Can I change this to a private endpoint?

No. You can create an instance with a public endpoint or a private endpoint. You can't switch between the two.

If you want to protect your public endpoint, you can add very specific access control rules to control incoming traffic (ingress). See [Manage Ingress Access Rules for a Public Endpoint using the Console](#).

How can I control access to my public endpoint?

If you want to protect your public endpoint, you can add very specific access control rules to control the incoming traffic (ingress). See [Manage Ingress Access Rules for a Public Endpoint using the Console](#).

I created an Oracle Analytics Cloud instance with a public endpoint and defined access rules but I'm unable to access the Oracle Analytics Cloud URL from my browser?

Check that the machine from which you're trying to access Oracle Analytics Cloud is included in the access control list. You can review the current access rules to check whether it's missing using the console. See [Manage Ingress Access Rules for a Public Endpoint using the Console](#).

How many different access rules can I define for a public endpoint?

Oracle Analytics Cloud enables you to add up to 20 access control rules. See [Manage Ingress Access Rules for a Public Endpoint using the Console](#).

How can I control access to my private endpoint?

If you want to protect your private endpoint, you can use predefined network security groups to control the incoming traffic (ingress). See [Manage Ingress and Egress Access Rules for a Private Endpoint using the Console](#).

I created an Oracle Analytics Cloud instance with a private endpoint but I'm unable to access the Oracle Analytics Cloud URL from my browser?

After creating your Oracle Analytics Cloud instance, you must configure Domain Name Server (DNS) resolution on your private network to access the private endpoint. See [Typical Workflow to Deploy Oracle Analytics Cloud with a Private Endpoint](#).

Where can I find the IP address for my Oracle Analytics Cloud instance?

You can find the IP address, Gateway IP address, and other useful information on the Details tab in the Oracle Cloud Infrastructure Console. See [Find the IP Address or Host Name of Your Oracle Analytics Cloud Instance](#).

Do I have any tools to test or debug network issues from my corporate network?

You can use `nslookup` to find IP address information for your Oracle Analytics Cloud instance.

```
# Use nslookup
nslookup <OAC hostname> <DNS server IP address>
```

You can use `netcat` or `cURL` to check whether your Oracle Analytics Cloud instance is accessible:

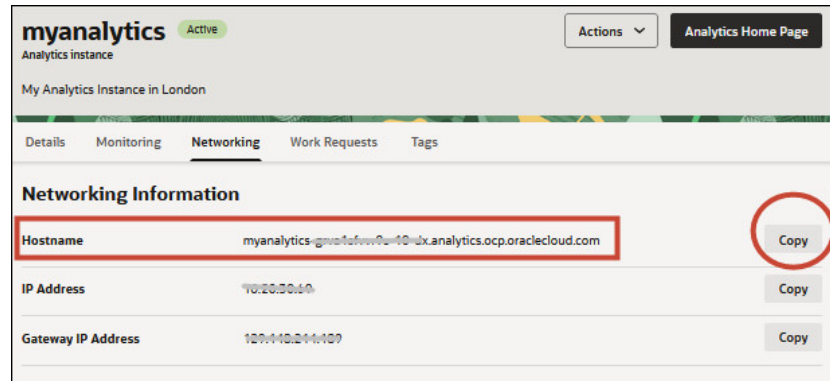
```
# Use Netcat
nc -zv <OAC hostname> 443
```

```
# Use cURL
curl -v https://<OAC hostname>/public/dv/ping
```

When you ping Oracle Analytics Cloud you can expect the following responses:

- Accessible and working as expected, returns {"serverUp": true}
- Accessible but paused, returns {"serverUp": true}
- Inaccessible or network outage, returns no reply or response

In Oracle Cloud Infrastructure Console, navigate to the **Networking** tab for your Oracle Analytics Cloud instance to determine the **Hostname**.



Top FAQs for Network Security Groups

The top FAQs when configuring network security groups (NSGs) for Oracle Analytics Cloud are identified in this topic.

What is a network security group or NSG?

Network security groups act as a virtual firewall for Oracle Cloud Infrastructure resources such as Oracle Analytics Cloud. An NSG consists of a set of ingress and egress security rules that apply only to a set of VNICs of your choice in a single VCN. To learn more about NSGs and how to manage ingress and egress security rules, see [Network Security Groups](#).

Can I use NSGs in Oracle Analytics Cloud?

Yes.

- Private Oracle Analytics Cloud instances: If you have a private Oracle Analytics Cloud instance, you can manage ingress rules through NSGs. See [Manage Ingress Access Rules for a Private Endpoint](#).
- Private data sources: If your Oracle Analytics Cloud connects to private data sources through a private access channel, you can use NSGs to manage egress rules from Oracle Analytics Cloud to the private data sources. See [Manage the Private Data Sources You Can Access on a Private Access Channel](#).

Can I use NSG ingress rules to restrict access into my public Oracle Analytics Cloud instance?

No. To restrict incoming traffic (ingress) to your public Oracle Analytics Cloud instance, use access control rules. See [Control Incoming Traffic for a Public Endpoint \(Ingress\)](#).

I applied a NSG to my Oracle Analytics Cloud instance and now I need to update the rules. Can I update or add new rules to the NSG?

Yes. Oracle Analytics Cloud applies the latest NSG rules for access to and from Oracle Analytics Cloud.

I applied a NSG with both ingress and egress rules to my Oracle Analytics Cloud instance. What's the impact on access to and from Oracle Analytics Cloud?

- Private Oracle Analytics Cloud instance: Ingress rules defined in the NSG control incoming traffic (ingress) to Oracle Analytics Cloud.
- Private data sources: Egress rules defined in the NSG control outgoing traffic.

How many NSGs can I apply to my Oracle Analytics Cloud instance?

Five.

If I apply multiple NSGs to my Oracle Analytics Cloud instance, what happens?

The set of rules applied is the union of the rules from all the NSGs.

Can I use one set of NSGs to control access to my private Oracle Analytics Cloud instance and a different set of NSGs to control access to my private data sources?

No. You must apply a single set of NSGs. The ingress rules in these NSGs control the incoming traffic and the egress rules in the NSGs control access to the private data sources.

Top FAQs for Private Sources

The top FAQs when setting up a private access channel for Oracle Analytics Cloud are identified in this topic.

What data sources can I connect to over a private access channel?

To find out which data sources you can connect to through a private access channel, see Supported Data Sources. Look for the data sources with the connectivity option *private access channel* in the "Use in Datasets" and "Use in Semantic Modeler" columns.

Note

Private access channels enable you to connect to private *data source* hosts. You can't use a private access channel to access any other type of private host. For example, you can't use private access channels to access private hosts that represent FTP servers, SMTP servers, printers, MapViewer configuration, or any other type of private host you might use.

When I connect to my private source in Oracle Analytics Cloud, do I specify the domain name or the IP address of my private source?

You must specify the Fully Qualified Domain Name (FQDN) of your private source in the connect dialog. This is the same FQDN that's registered in the private access channel. For example, domain names such as `companyabc.com`, `example.com`, `myadw.adb.us-ashburn-1.oraclecloud.com`, and so on. See [About Private Sources](#).

You can't use IP addresses to connect to private sources.

My private Oracle Database has a Single Client Access Name (SCAN). Can I use the SCAN host name to connect to my private data source?

Yes. Register the SCAN host name and the SCAN port in private access channel. For example, SCAN host names such as `db01-scan.corp.example.com`, `prd-db01-`

scan.mycompany.com, and the port where the SCAN protocol connects, for example 1521. See [About Private Sources](#).

Note

At least one DNS Zone is required on the private access channel. Select **Virtual Cloud Network's domain name as DNS zone** to add the default domain.

I have several private data sources and private Git repositories. Do I access all of them over a single private access channel?

Yes. Your Oracle Analytics Cloud instance supports a single private access channel. You can connect to multiple data sources and Git repositories through the same channel.

- DNS Zones: You can add up to 30 DNS zone entries.
- SCAN Hosts: You can add up to 15 SCAN host entries.

How long does it take to create, update, or delete private sources?

It takes between 7 and 30 minutes to add or modify DNS zone and SCAN host entries.

How do I control access to the private sources on my private access channel?

You can use egress rules defined in network security groups to restrict access to your private data sources and private Git repositories. The way you configure network security groups depends whether the endpoint of your Oracle Analytics Cloud instance is public or private. See [Manage Egress Access Rules for a Public Endpoint using the Console](#) or [Manage Ingress and Egress Access Rules for a Private Endpoint using the Console](#).

Can I add and remove private sources or edit the private access channel?

Yes. You can manage the DNS zones and SCAN hosts accessible through the private access channel. If your Oracle Analytics Cloud has a public endpoint, you can also change the VCN and subnet that the private access channel uses to access the private sources and control access with one or more network security groups. See [Edit a Private Access Channel](#).

You can monitor the progress of **Edit Private Access Channel** operations in the activity log. In the unlikely event an edit operation fails, Oracle recommends that you delete the private access channel and recreate it. See [Monitor Status](#).

Can I use both a private access channel and Remote Data Gateway?

Yes. You can use both these methods to connect to your remote data sources and Git repositories.

Can I set up a private access channel with Oracle Analytics Cloud Classic or Oracle Analytics Cloud Gen 1?

No. The private access channel feature is available only with Oracle Analytics Cloud Gen 2.

Can I use the private access channel to access a private source on a different OCI region?

No. Oracle Analytics Cloud and the Oracle Cloud Infrastructure VCN that's hosting the private source must be in the same region. See [Prerequisites for a Private Access Channel](#).

Note

If you need to connect to a private Oracle Autonomous AI Lakehouse in a different region, you can set up a custom domain for Oracle Autonomous AI Lakehouse with a custom private zone.

If my private Oracle Analytics Cloud and my private source are in the same subnet, do I need a private access channel?

Yes. You must configure a private access channel to connect to your private source even when it's in the same subnet as your Oracle Analytics Cloud.

Can I use a private access channel to access Oracle-specific DNS zones?

In most cases, no. Access to most Oracle-specific DNS zones is restricted, for example `oracle.com` and `oraclecloud.com`. You can't register these DNS zones as private sources and connect to them over a private access channel.

The only Oracle-specific DNS zones you can register as a private source in a private access channel is `<adb-name>.adb.<region>.<realm public domain>`. For example, `myadw.adb.us-ashburn-1.oraclecloud.com` or `myadw.adb.uk-gov-cardiff-1.oraclegovcloud.uk`. You can use this format to access private Oracle Autonomous AI Lakehouse and Oracle Autonomous AI Transaction Processing databases.

How do I connect to a private Oracle Autonomous AI Lakehouse in a customer VCN?

1. In Oracle Cloud Infrastructure Console, configure a private access channel for the Analytics instance that uses a subnet in the virtual cloud network (VCN) where the private Oracle Autonomous AI Lakehouse is deployed. See [Configure a Private Access Channel using the Console](#).
2. Ensure that the subnet the private access channel uses has an egress rule to communicate with the private Oracle Autonomous AI Lakehouse on port 1522. See [Working with Security Lists](#).
3. Register the private Oracle Autonomous AI Lakehouse as a private source in the private access channel using the FQDN hostname in the format `<adb-name>.adb.<region>.oraclecloud.com`. For example, `myadw.adb.us-ashburn-1.oraclecloud.com`. See [Manage the Private Sources You Can Access on a Private Access Channel Using the Console](#).
4. Obtain the *regional wallet* for the private Oracle Autonomous AI Lakehouse. See [Download Client Credentials \(Wallets\)](#).
5. In Oracle Analytics Cloud, create a connection to Oracle Autonomous AI Lakehouse that uses the regional wallet and select the service name of the private Oracle Autonomous AI Lakehouse instance you want to connect to from the list. See [Connect to Oracle Autonomous AI Lakehouse](#).

How do I connect to a private source in my Oracle Cloud Infrastructure VCN?

1. In Oracle Cloud Infrastructure Console, configure a private access channel for the Analytics instance that uses a subnet in the virtual cloud network (VCN) where the private data source is deployed. See [Configure a Private Access Channel using the Console](#).

In the **Configure Private Access Channel** page, select the checkbox **VIRTUAL CLOUD NETWORK'S DOMAIN NAME as DNS ZONE**.

2. Ensure that the subnet the private access channel uses has an egress rule to communicate with the private source on its port. See [Working with Security Lists](#).
3. If you didn't select the checkbox in step 1, register the DNS zone of your VCN in the format `<VCN DNS label>.oraclevcn.com`. For example, `example.oraclevcn.com`. See [Manage the Private Sources You Can Access on a Private Access Channel Using the Console](#).
4. In Oracle Analytics Cloud, create a connection that specifies the hostname of the VCN where the private data source is deployed. See

Connect to Data for Visualizations and Analyses and Manage Data Source Connections for Semantic Models.

How do I connect to a private source in my corporate network peered to an Oracle Cloud Infrastructure VCN?

1. Set up a direct connection between your corporate network and Oracle Cloud Infrastructure VCN. See [Access to Your On-Premises Network](#).
2. Set up a private DNS resolver in the Oracle Cloud Infrastructure VCN. Configure a DNS forwarder in the private DNS resolver to forward corporate hostname resolution to your company's DNS server. See [Private DNS](#).
3. In Oracle Cloud Infrastructure Console, configure a private access channel for the Analytics instance that uses the subnet in the virtual cloud network (VCN) that is connected to the corporate network. See [Configure a Private Access Channel using the Console](#).
4. Ensure that the subnet the private access channel uses has an egress rule to communicate with IP address and port of the private source. See [Working with Security Lists](#).
5. Register the DNS zone of the private source in the format `<domain name>`. For example, if the data source FQDN hostname is `data-source-ds01.example.com`, add the DNS Zone as `example.com`. See [Manage the Private Sources You Can Access on a Private Access Channel Using the Console](#).
6. In Oracle Analytics Cloud, create a data source connection using the FQDN hostname `data-source-ds01.example.com`. See

Connect to Data for Visualizations and Analyses and Manage Data Source Connections for Semantic Models.

For private Git repositories, sign-in to Oracle Analytics Cloud, open a semantic model in Semantic Modeler, click **Toggle Git Panel** to open the Git pane and connect to the private Git repository.

How do I connect to a private source using an IP address in my corporate network peered to an Oracle Cloud Infrastructure VCN?

1. Set up a direct connection between your corporate network and Oracle Cloud Infrastructure VCN. See [Access to Your On-Premises Network](#).
2. Create a private DNS view and then add a zone (in the view) for your custom domain. For example, `ocivcn.example.com`. See [Private DNS](#).
3. In the zone you just created, add a DNS record type A, and map the IP address to the fully qualified hostname. For example, `datasource-ds-01.ocivcn.example.com`.
4. Navigate to the DNS Resolver option for your VCN and associate the private DNS VCN you created in step 2. See [Private DNS Resolver](#).
Configure one of the following:

- DNS forwarder: Configure a DNS forwarder in the private DNS resolver to forward corporate hostname resolution to your company's DNS server. See [Private DNS](#) .
 - Hostname to IP address mapping: Add a custom record type A entry for the private source IP address mapping to an FQDN hostname under a unique DNS domain. For example, if the private source IP address in your corporate network is 10.40.100.55 and your corporate DNS Zone domain is example.com, add a DNS record type A that maps datasource-ds-01.ocivn.example.com to 10.40.100.55.
5. In Oracle Cloud Infrastructure Console, configure a private access channel for the Analytics instance that uses the subnet in the virtual cloud network (VCN) that is connected to the corporate network . See [Configure a Private Access Channel using the Console](#).
 6. Register the DNS zone of the private source in the format ocivn.<domain name>. For example, if the private source DNS record is datasource-ds-01.ocivn.example.com, add the DNS Zone as ocivn.example.com. See [Manage the Private Sources You Can Access on a Private Access Channel Using the Console](#).
 7. In Oracle Analytics Cloud, create a data source connection using the hostname datasource-ds-01.ocivn.example.com. See [Connect to Data for Visualizations and Analyses and Manage Data Source Connections for Semantic Models](#).

For private Git repositories, sign-in to Oracle Analytics Cloud, open a semantic model in Semantic Modeler, click **Toggle Git Panel** to open the Git pane and connect to the private Git repository.

Do I have any tools to troubleshoot connection issues to my private data sources?

Yes. You can use the *Network Path Analyzer* that's available in Oracle Cloud Infrastructure Console to troubleshoot connectivity issues. See [Troubleshoot Connectivity Issues Using Network Path Analyzer](#).

Top FAQs for Vanity URLs

The top FAQs when setting up a vanity URL for Oracle Analytics Cloud are identified in this topic.

How many vanity URLs can I create for my Oracle Analytics Cloud instance?

One. See [Set Up a Custom Vanity URL](#).

Does the standard URL continue to work?

Yes.

Can I use a self-signed certificate when defining a vanity URL?

No. Self-signed certificates aren't supported. However, you can create your own root signing certificate and use that to sign a certificate that you generate yourself. See [Prerequisites for a Vanity URL](#).

Are wildcard certificates supported?

Yes.

Can I try this feature without registering a public DNS entry?

Yes. In the `/etc/hosts` file on your client machine, add an entry for the vanity host name you plan to use that points to the IP address of your Oracle Analytics Cloud instance. The vanity URL works on that machine.

Users accessing the vanity URL report the error "400 Bad Request - Request Header Or Cookie Too Large". How do I resolve this?

- Ask users to clear their browser cache and cookies, and then try to access the Oracle Analytics Cloud vanity URL again.
- Work with your organization to verify the `Domain` attribute setting in the `Set-Cookie` header. Check that the `Set-Cookie` header that's being sent by other applications isn't configuring unnecessary cookies for all subdomains under your company domain.

For general information about HTTP cookies, refer to [Define where cookies are sent](#).

Top FAQs for Data Encryption

The top FAQs when using custom data encryption in Oracle Analytics Cloud are identified in this topic.

What is the difference between Oracle-managed and customer-managed encryption?

Oracle-managed is the default encryption for Oracle Analytics Cloud and many other services in Oracle Cloud Infrastructure. Oracle-managed means sensitive data in Oracle Analytics Cloud will be encrypted with an encryption key whose lifecycle management is controlled by Oracle. Customers who don't want to manage or access their encryption keys and are looking for the easiest way to protect all their data stored in Oracle Analytics Cloud can choose Oracle-managed encryption.

Customer-managed encryption is offered by the Vault service in Oracle Cloud Infrastructure. With customer-managed encryption, you control and manage the keys that protect your data.

Why can't I see the vault or encryption key I want to use for my Oracle Analytics Cloud instance?

You must have access to the compartment where the vault and master encryption key is stored, and you must have the required permissions to read and manage keys. See [Prerequisites for Custom Encryption](#).

What happens if the custom encryption key my Oracle Analytics Cloud instance uses is deleted or disabled?

Disabling or deleting a customer-managed key makes your content within Oracle Analytics Cloud unreadable for everyone (including Oracle) and anyone who tries to access Oracle Analytics Cloud sees a 403 error (forbidden).

Your Oracle Analytics Cloud instance is unavailable (403 error) when the state of the master encryption key is any of the following: `DISABLING`, `DISABLED`, `DELETING`, `DELETED`, `SCHEDULING_DELETION`, `PENDING_DELETION`.

If the key is disabled and you decide to enable the key, Oracle Analytics Cloud becomes accessible. See [Enable a key](#).

If the key was deleted, you might be able to cancel the delete operation. See [Cancel the deletion of a key](#).

7

Troubleshoot

This topic describes common problems that you might encounter administering services in Oracle Analytics Cloud and explains how to solve them.

Creating Analytics instances

- [I see an error message when I try to create a service](#)
- [I see a subscription error message in the Create Instance dialog](#)
- [I'm having problems creating a service](#)

Accessing Analytics instances

- [I see an insufficient permissions message when I try to access the service](#)

Connecting to data sources

- [I'm having issues connecting to my data sources](#)

Diagnosing other issues

- [How do I diagnose issues with Oracle Analytics Cloud?](#)
- [Where do I find the OCID for my service?](#)
- [When do I contact Oracle Support?](#)

Troubleshoot Instance Creation Issues

This topic describes common problems that you might encounter creating an Oracle Analytics Cloud instance and explains how to solve them.

Topics

- [I see an error message when I try to create a service](#)
- [I see a subscription error message in the Create Instance dialog](#)
- [I'm having problems creating a service](#)
- [I see an insufficient permissions message when I try to access the service](#)

I see an error message when I try to create a service

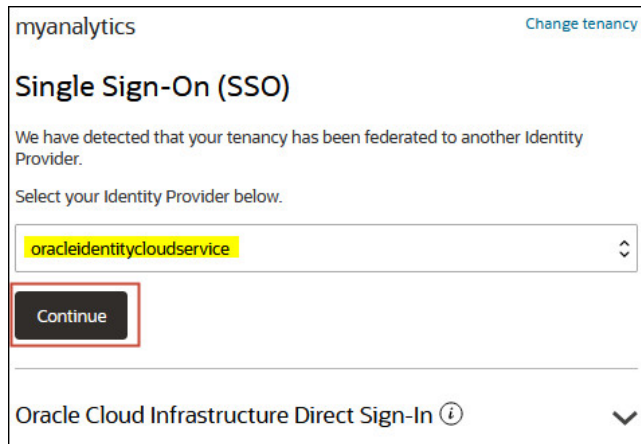
You must sign in to your Oracle Cloud account as a user with permissions to set up Oracle Analytics Cloud. See [Give Users Permissions to Manage Analytics Cloud Instances](#).

If you don't, you see an error message similar to this one when you try to create a service with Oracle Analytics Cloud:

```
Please ensure that you are logged into the console with an IDCS identity provider when creating an Analytics Instance
```

Ask your administrator to give you the required permissions and then sign back in.

Note: If your cloud account federates with Oracle Identity Cloud Service, you must sign in as a federated user.



I see a subscription error message in the Create Instance dialog

If you activated your Cloud Account in North America, EMEA, Asia Pacific (APAC) or Latin America (LAD) before Oracle Analytics Cloud was available on Oracle Cloud Infrastructure (Gen 2) in these regions, you might see this message:

```
Error: OAC-DAL-001031: Unable to verify the Analytics Cloud subscription for
your tenancy.
```

```
Please contact Oracle support.
```

If you see this message when you try to create an Analytics instance, contact Oracle Support for assistance. Provide the name of your Oracle Cloud account, your identity domain ID, and the region where you want to deploy the new Oracle Analytics Cloud service.

I'm having problems creating a service

In the Oracle Cloud Infrastructure Console, navigate to the Analytics Cloud page. Check the Status to see why provisioning failed. If you're not sure what to do, contact Oracle Support for assistance.

I see an insufficient permissions message when I try to access the service

If you're not yet assigned to any application role, you see this message:

```
Oracle Analytics
Insufficient Permissions
You do not have sufficient permissions to use this application.
```

Ask an administrator for the Analytics instance to grant you an application role. In most cases, administrators grant application roles through the **Users and Roles** page in Oracle Analytics Cloud. See [Manage What Users Can See and Do](#).

Identity domain administrators who use Oracle Cloud Infrastructure Console to add users for Oracle Analytics Cloud (through Oracle IAM Identity Domain or Oracle Identity Cloud Service), can also use this console to grant users basic permissions in Oracle Analytics Cloud through these application roles: **ServiceAdministrator**, **ServiceUser**, **ServiceViewer**. See [Add a User or a Group](#).

Troubleshoot Data Source Connectivity Issues

You can use the *Network Path Analyzer* that's available in Oracle Cloud Infrastructure Console to troubleshoot connectivity issues in Oracle Analytics Cloud. For example:

- Connectivity issues between Oracle Analytics Cloud (public or private) and any private data source that you connect to through a private access channel.
- Connectivity issue between a compute instance (on Oracle Cloud Infrastructure or on-premises) and Oracle Analytics Cloud (public or private).

Topics


- [Troubleshoot Connectivity Issues Using Network Path Analyzer](#)
- [Example: Oracle Analytics Cloud Connection to an On-premises Database](#)

Troubleshoot Connectivity Issues Using Network Path Analyzer

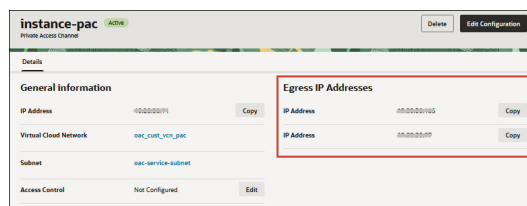
Use *Network Path Analyzer* to troubleshoot connectivity issues in Oracle Analytics Cloud.

Prerequisites

You must have the policies required to use Network Path Analyzer. See [Network Path Analyzer - Required Permissions](#).

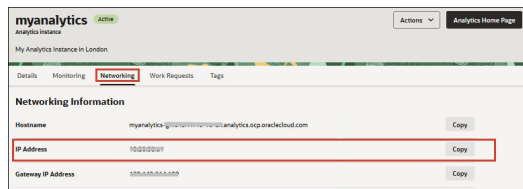
1. In Oracle Cloud Infrastructure Console, click  in the top left corner.
2. Click **Networking**. Under **Network Command Center**, click **Network Path Analyzer**.
3. Click **Create Network Path Analysis**.
4. For **Name** and **Compartment**, enter a name for the analysis and select the compartment where you want to create the analysis.
5. For **Protocol**, select the network protocol the connection uses. For example, **TCP**.
6. Enter the source and destination IP address of the connection you want to analyze. Do one of the following:
 - **Option 1 - Source:** Oracle Analytics Cloud (public or private) **Destination:** Private data source accessible through a private channel

- a. In **Source**, select **Enter IP address** and enter the egress IP address that Oracle Analytics Cloud uses to access your private data sources over a private access channel. For example, enter 10.20.30.100. A port value isn't required. If your private channel has multiple egress IPs, choose any one of these to test connectivity. See [Find the Egress IP Address of Your Private Access Channel](#).

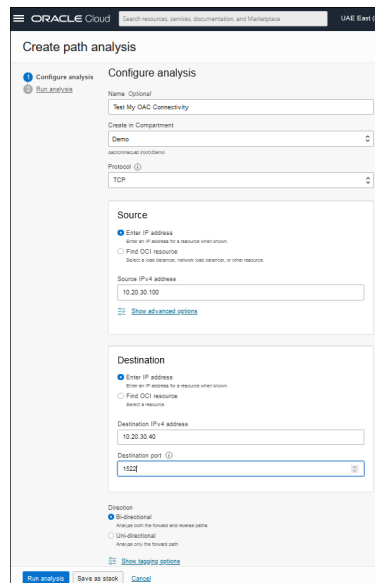


- b. In **Destination**, select **Enter IP address** and enter the IP address of the private data source (on Oracle Cloud Infrastructure or on-premises) and the destination port. For example, 10.20.30.40 and 1522.

- **Option 2 - Source:** Compute instance (on Oracle Cloud Infrastructure or on-premises)
Destination: Oracle Analytics Cloud (public or private)
 - a. In **Source**, select **Enter IP address** and enter the IP address that the compute instance uses to access Oracle Analytics Cloud. For example, enter 192.123.456.1. A port value isn't required.
 - b. In **Destination**, select **Enter IP address** and enter the IP address of Oracle Analytics Cloud and the destination port 443. For example, enter 129.123.123.123 and 443.
 See [Find the IP Address of Your Analytics Instance](#).



7. For **Direction**, we recommend you select **Bi-directional**.



8. Click **Run analysis** and wait for the results.

For example, if there's a connectivity issue in the forward traffic path, the results might look like this.

Discovered paths

Often there is more than one available path for traffic between two points. Network Path Analyzer can present up to 8 paths between the selected source and destination, but it is possible more could exist. If no complete path is found, the path with the most successful hops is shown.

Path 1

Forward path

Status: ● Unreachable Successful hops: 0

Analysis performed: Tue, Nov 1, 2022, 19:08:31 UTC

10.20.30.94
IP

View diagram information

Path hop	From	To	Routing status	Security status	Traffic
Segment	10.20.30.94		● No route	● Denied	TCP: 10.20.30.94:49152 to 10.20.30.37:1522

Showing 1 item

To find out what's missing, click the **Down** arrow to reveal more information. Network Path Analyzer tells you when a route is missing from the route table or a security policy is missing from a network security group or a security list.

View diagram information

Path hop	From	To	Routing status	Security status	Traffic
Segment	10.20.30.94		● No route	● Denied	TCP: 10.20.30.94:49152 to 10.20.30.37:1522

No route

Routing status: ● No route

Routing action: We don't have information about the routing for this segment of the path. There could be multiple hops, or it could be completely unroutable.

Security denied

Egress access control status: ● Denied

Egress access control action: We couldn't find a matching security rule for the traffic in the following security resources:

- [oac-egress-access-control-group-ns-egress](#)
- [ns-egress](#)

Ingress access control status: ● Not applicable

Ingress access control action: Security information is not applicable

Segment from

VNIC: 10.20.30.94

VCN: [oac-egress-vcn](#)

Subnet: [oac-egress-subnet](#)

Segment to

VNIC: [...nwisq5raxq](#) Show Copy

VCN: [oac-egress-vcn](#)

Subnet: [oac-egress-subnet](#)

To learn more, watch [Oracle's Network Path Analyzer video](#) or read the [Network Path Analyzer documentation](#).

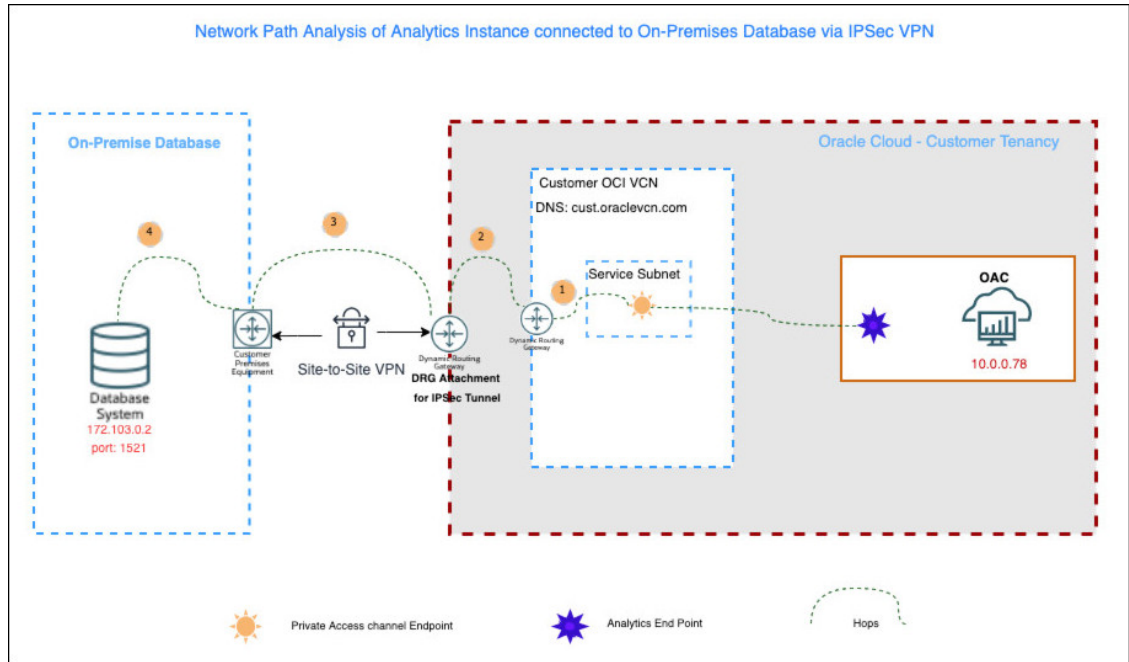
Example: Oracle Analytics Cloud Connection to an On-premises Database

The Network Path Analyzer discovers forward and return paths in your network. You can use the results to check the logical network paths match your intent and verify that the virtual network connectivity setup works as you expect before you start to send traffic or to troubleshoot issues.

Here's a sample network path analysis for an Oracle Analytics Cloud connection:

- **Source:** Oracle Analytics Cloud with a private access channel (PAC), with PAC Egress IP address 10.0.0.78
- **Destination:** On-premises database with IP address 172.103.0.2 and port 1521

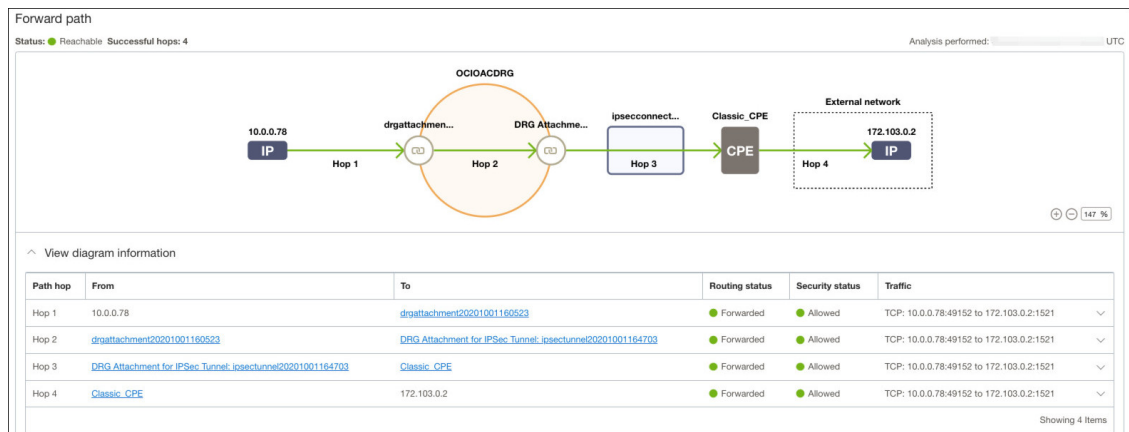
Oracle Analytics Cloud connects to the on-premises database through an IPsec VPN.



Forward Path

In this example, the forward path shows four successful, reachable network hops.

- **Hop 1:** Oracle Analytics Cloud with IP address 10.0.0.78 to the OCI VCN dynamic routing gateway
- **Hop 2:** OCI VCN dynamic routing gateway to the IPsec dynamic routing gateway
- **Hop 3:** IPsec dynamic routing gateway to the customer on-premises equipment, over site-to-site VPN
- **Hop 4:** Customer on-premises equipment to the database with IP address 172.103.0.2

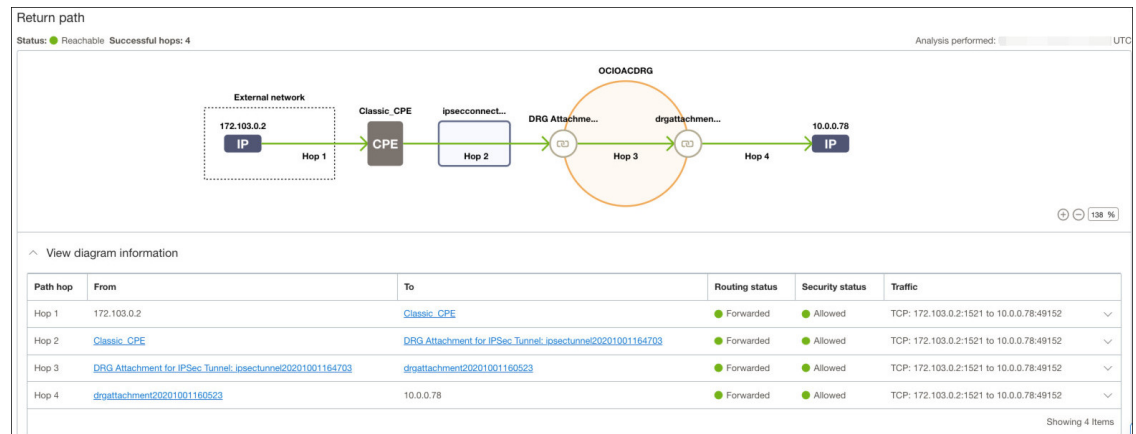


Return Path

In this example, the return path shows four successful, reachable network hops.

- **Hop 1:** Customer database with IP address 172.103.0.2 to the customer on-premises equipment
- **Hop 2:** Customer on-premises equipment to the OCI tenancy, over site-to-site VPN
- **Hop 3:** IPsec dynamic routing gateway to the OCI VCN dynamic routing gateway

- **Hop 4:** OCI VCN dynamic routing gateway to Oracle Analytics Cloud with IP address 10.0.0.78, over a private access channel



Troubleshoot Other Issues

This topic describes common problems that you might encounter with Oracle Analytics Cloud and explains how to solve them.

Topics

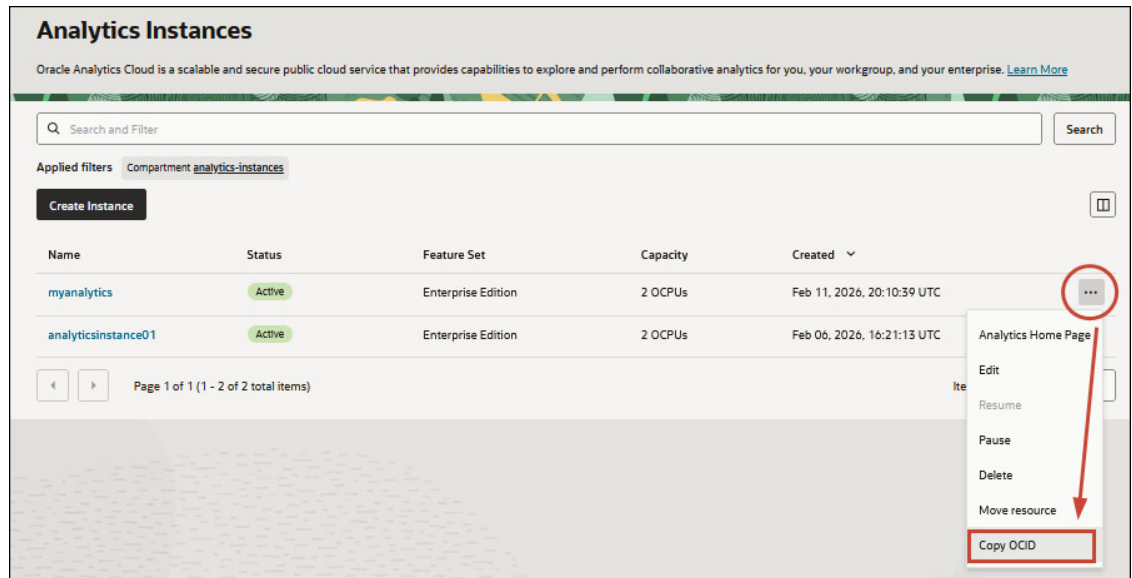
- [How do I diagnose issues with Oracle Analytics Cloud?](#)
- [Where do I find the OCID for my service?](#)
- [When do I contact Oracle Support?](#)

How do I diagnose issues with Oracle Analytics Cloud?

If you experience issues with your service, make a note of the Oracle Cloud ID (OCID) allocated to the service and contact Oracle Support for assistance.

Where do I find the OCID for my service?

In the Oracle Cloud Infrastructure Console, navigate to the Analytics Cloud page. Click the action menu for your instance and select **Copy OCID**.



The screenshot shows the Oracle Analytics Instances page. At the top, there is a search bar and a 'Search' button. Below that, there are 'Applied filters' and a 'Create Instance' button. The main content is a table with the following columns: Name, Status, Feature Set, Capacity, and Created. Two instances are listed: 'myanalytics' and 'analyticsinstance01', both with a status of 'Active'. A context menu is open over the second instance, with 'Copy OCID' highlighted. A red circle and arrow point to the menu icon and the 'Copy OCID' option.

Name	Status	Feature Set	Capacity	Created
myanalytics	Active	Enterprise Edition	2 OCPUs	Feb 11, 2026, 20:10:39 UTC
analyticsinstance01	Active	Enterprise Edition	2 OCPUs	Feb 06, 2026, 16:21:13 UTC

When do I contact Oracle Support?

If you encounter a problem creating a service, record any error messages you see in the user interface, and contact Oracle Support for assistance.

Contact Oracle Support if you want help with your service:

- You experience performance issues.
- Your service isn't available.