Oracle® Cloud

Provisioning and Administering Oracle Integration 3

F45532-87
May 2024

Oracle Cloud Provisioning and Administering Oracle Integration 3,

F45532-87

Primary Author: Oracle Corporation

Contents

4 Create and Edit Oracle Integration 3 Instances

5 Manage Oracle Integration 3 Instances

6 Upgrade from Oracle Integration Generation 2 to Oracle Integration 3

A Oracle Integration 3 Reference

B Oracle Integration Roles and Privileges

Preface

Provisioning and Administering Oracle Integration 3 describes how to create and administer Oracle Integration from the Oracle Cloud Infrastructure Console.

Topics:

Audience

Provisioning and Administering Oracle Integration 3 is intended for users who want to create and manage Oracle Integration instances in the Oracle Cloud Infrastructure Console.

Documentation Accessibility

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

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `https://support.oracle.com/portal/` or visit `Oracle Accessibility Learning and Support` if you are hearing impaired.

Diversity and Inclusion

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

Related Resources

For more information, see these Oracle resources:

- Oracle Integration documentation on the Oracle Help Center.
- Oracle Cloud at `http://cloud.oracle.com`.

Conventions

The following text conventions are used in this document.

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

1
Overview of Oracle Integration 3

Oracle Integration 3 is a fully managed, preconfigured environment that gives you the power to integrate your cloud and on-premises applications, automate business processes, develop visual applications, use an SFTP-compliant file server to store and retrieve files, and exchange business documents with a B2B trading partner.

Capabilities

With Oracle Integration 3, you can:

- Design integrations to monitor and manage connections between your applications, selecting from our portfolio of hundreds of prebuilt adapters and recipes to connect with Oracle and third-party applications.
- Create process applications to automate and manage your business work flows, whether structured or dynamic.
- Develop visual applications using the embedded Visual Builder feature.
- Store and retrieve files in Oracle Integration using the embedded SFTP-compliant file server.
- Create integrations that use B2B e-commerce to extend business processes to reach trading partners.

Editions

Oracle Integration is available in two editions: Standard or Enterprise. See Oracle Integration Editions.

Oracle SaaS customers can use Oracle Integration for SaaS, which gives you the features and benefits of Oracle Integration with a focus on SaaS. See Oracle Integration for Oracle SaaS.

Instances and Updates

See Updates to Your Instance.

Topics:

Availability

Oracle Integration 3 is here and is available for provisioning.

If you want to run both Oracle Integration Generation 2 and Oracle Integration 3 side by side, file a service request. See this blog.

Questions about availability?

- See Can I Create an Oracle Integration 3 Instance?
- For Oracle Integration for SaaS administrators, see Can I Create an Oracle Integration for Oracle SaaS Instance?.
- For information about Oracle Integration 3 on US Government Cloud region availability, see *Using Oracle Integration 3 on Oracle Cloud Infrastructure US Government Cloud*.

Geography	Region Location	Region Key
APAC	Australia East (Sydney)	SYD
APAC	Australia Southeast (Melbourne)	MEL
APAC	India South (Hyderabad)	HYD
APAC	India West (Mumbai)	BOM
APAC	Japan Central (Osaka)	KIX
APAC	Japan East (Tokyo)	NRT
APAC	Singapore	SIN
APAC	South Korea Central (Seoul)	ICN
APAC	South Korea North (Chuncheon)	YNY
EMEA	Abu Dhabi	AUH
EMEA	France Central (Paris)	CDG
EMEA	France South (Marseille)	MRS
EMEA	Germany Central (Frankfurt)	FRA
EMEA	Israel (Jerusalem)	MTZ
EMEA	Italy (Milan)	LIN
EMEA	Netherlands Northwest (Amsterdam)	AMS
EMEA	Saudi Arabia West (Jeddah)	JED
EMEA	South Africa Central (Johannesburg)	JNB
EMEA	Spain Central (Madrid)	MAD
EMEA	Sweden (Stockholm)	ARN
EMEA	Switzerland North (Zurich)	ZRH
EMEA	UAE East (Dubai)	DBX
EMEA	UK Gov South (London)	LTN
EMEA	UK Gov West (Newport)	BRS
EMEA	UK West (Cardiff)	CWL
EMEA	UK South (London)	LHR
LAD	Brazil East (Sao Paulo)	GRU
LAD	Brazil Southeast (Vinhedo)	VCP

Geography	Region Location	Region Key
LAD	Chile Central (Santiago)	SCL
LAD	Chile West (Valparaiso)	VAP
LAD	Colombia Central (Bogota)	BOG
LAD	Mexico Central (Queretaro)	QRO
LAD	Mexico Northeast (Monterrey)	MTY
North America	Canada Southeast (Montreal)	YUL
North America	Canada Southeast (Toronto)	YYZ
North America	US DoD East (Ashburn)	ric
North America	US DoD North (Chicago)	pia
North America	US DoD West (Phoenix)	tus
North America	US East (Ashburn)	IAD
North America	US Gov East (Ashburn)	LFI
North America	US Gov West (Phoenix)	LUF
North America	US Midwest (Chicago)	ORD
North America	US West (Phoenix)	PHX
North America	US West (San Jose)	SJC

Restrictions

Note the following current restrictions when creating Oracle Integration instances.

- You can create Oracle Integration for SaaS instances in any Oracle data region if you created a new Oracle Cloud account on or after February 11, 2020.
- Only some customers with Oracle Integration Generation 2 instances can create Oracle Integration 3 instances. See Can I Create an Oracle Integration 3 Instance?
  To run Oracle Integration Generation 2 and Oracle Integration 3 side by side, file a service request. See this blog.
- The version, region, and use of identity domains determine where you can create an instance:
  - You can create an Oracle Integration Generation 2 instance in any region, regardless of whether your tenancy uses identity domains. First, you must subscribe to the region in the Oracle Cloud Infrastructure Console.
  - For tenancies that use identity domains, you must create the Oracle Integration 3 instance in the same region as your domain stripe. You can create a domain stripe in any region.
  - For tenancies that do not use identity domains, you can create the Oracle Integration 3 instance in a different region than your IDCS stripes.

> **Note:**
>
> Features that are available in prior versions of Oracle Integration may not be available in Oracle Integration 3. These features may be permanently removed, replaced, enhanced, or not currently supported in Oracle Integration 3. See Differences from Prior Versions of Oracle Integration in *What's New for Oracle Integration 3*.

Service Limits

Review the following service limits for Oracle Integration 3 resources. A service limit is the quota or allowance set on a resource. You cannot change the service limits configured for your tenancy.

- Oracle Cloud Infrastructure Console Service Limits
- Component: Adapters
- Component: Integrations
- Component: File Server
- Other Service Limits

Oracle Cloud Infrastructure Console Service Limits

Resource	Service Limit
Integration service instance count	200 instances per region. **Note**: This value is the number of service instances you provision per region, and *not* the number of integration instances (for example, application and schedule) that you activate and monitor under the **Observability** tab in Oracle Integration.
Instance creation	The ability to create instances outside your home region depends on several factors. See Restrictions.
Private endpoint limits	• 1 private endpoint per instance • 1 subnet per private endpoint

Component: Adapters

Resource	Service Limit
For structured payloads delivered on trigger connections or as a response from invoke connections	100 MB limit for cloud endpoints (not using the connectivity agent). The limit is 100 MB if the endpoint is enabled with a private endpoint.
For binary (unstructured) payloads (for example, attachments, MTOM)	1 GB limit for trigger connections and responses from invoke connections.
For connectivity agent-based adapters, the payload limits for structured payload (JSON, XML).	50 MB limit for SOAP and REST. For file and FTP with the connectivity agent, the limit for an invoke response is 50 MB for structured payloads. For any other protocol (for example, database, JMS, MQ, Kafka, and others), the payload limit is 10 MB for structured payloads.

Resource	Service Limit
File Adapter - file size	Read File operation: • 1 GB when used without a schema (with the connectivity agent) • 50 MB when using a schema for transformation • 50 MB for a read operation with structured payload (The File Adapter is only available with connectivity agent.) Polling with the connectivity agent: 50 MB Download File operation: 1 GB **Note:** The size of CSV files increases when translated into a message. Therefore, the file size must be less than 50 MB, so that the after-translation message size does not exceed 50 MB.
FTP Adapter - file size	**For invoke configurations** Read File operation: • 1 GB when used without a schema (when used both with or without a connectivity agent). • 100 MB for cloud-based endpoints when using a schema for transformation. • 50 MB for agent-based endpoints when using a schema for transformation. • 100 MB for public internet-based endpoints. • 100 MB for private endpoints. Download File operation: 1 GB (when used both with or without a connectivity agent).

Resource	Service Limit
REST Adapter	**For trigger configurations** • XML document size for schema generation: 3 MB. See REST Adapter Capabilities. • Messages with attachments size (for example, multipart/form-data): 1 GB • Incoming structured message payload size (any content-type header containing JSON, XML, HTML, YAML, or YML): 100 MB. • Incoming content as raw bytes (application/octet-stream as content type): 1 GB. • Specifying the response payload format in the Adapter Endpoint Configuration Wizard: JSON sample files of up to 100 KB in size are supported. **For invoke configurations** • XML document size for data definition generation: 3 MB. See REST Adapter Capabilities. • Specifying the request payload format in the Adapter Endpoint Configuration Wizard: JSON sample files of up to 100 KB in size are supported. • Agent-based endpoints: 50 MB • Private endpoints: 100 MB • Public internet-based endpoints:100 MB
REST-Based Adapters (Adapters that expose REST endpoints on the inbound or adapters invoking external REST endpoints. For example, Oracle Commerce Cloud Adapter, Oracle Field Service Cloud Adapter, and so on.)	**For trigger configurations (wherever applicable)** • XML document size for schema generation: 3 MB. See REST Adapter Capabilities. • Messages with attachments size (for example, multipart/mixed and multipart/form-data): 1 GB • Incoming structured message payload size (any content-type header containing JSON, XML, HTML, YAML, or YML): 100 MB. • Incoming content as raw bytes (application/octet-stream as content type): 1 GB. • Specifying the response payload format: JSON sample files of up to 100 KB in size are supported. **For invoke configurations (wherever applicable)** • XML document size for data definition generation: 3 MB. See REST Adapter Capabilities. • Attachment size in outbound requests: 1 GB. • Specifying the request payload format: JSON sample files of up to 100 KB in size are supported. • Agent-based endpoints: 50 MB • Private endpoints: 100 MB • Public internet-based endpoints: 100 MB
SOAP Adapter	**For trigger configurations** • Structured payload (XML) size in Request and Response: 100 MB. **For invoke configurations** • Structured payload (XML) size in Request and Response: 100 MB. • Agent-based endpoints: 50 MB • Public internet-based endpoints: 100 MB

Resource	Service Limit
SOAP-Based Adapters (Adapters that expose SOAP endpoints on the inbound or adapters invoking external SOAP endpoints. For example, Oracle Logistics Adapter.)	**For trigger configurations (wherever applicable)** • Structured payload (XML) size in request and response: 100 MB. **For invoke configurations (wherever applicable)** • Structured payload (XML) size in response: 100 MB. • Agent-based endpoints: 50 MB
Database Adapters (Oracle Database Adapter, IBM DB2 Adapter, Microsoft SQL Server Adapter, MySQL Adapter, Netezza Adapter, PostgreSQL Adapter, Oracle Autonomous Data Warehouse Adapter, Oracle Autonomous Transaction Processing Adapter, Oracle Database Cloud Service Adapter, and SAP ASE (Sybase) Adapter)	**For trigger configurations** • Polling operation for Oracle Autonomous Data Warehouse Adapter, Oracle Autonomous Transaction Processing Adapter, and Oracle Database Cloud Service Adapter: – 50 MB with schema transformation for agent-based endpoints. – 100 MB with schema transformation through private endpoints • Polling for other database adapters: – 10 MB with schema transformation for all other database adapters. **For invoke configurations** • Stored Procedure/Operation on Table/Run PureSQL Statement Operations: 10 MB with schema transformation for all the outbound operations. • Database select operation for Oracle Autonomous Data Warehouse Adapter, Oracle Autonomous Transaction Processing Adapter, and Oracle Database Cloud Service Adapter: – 100 MB for public internet-based endpoints – 100 MB for private endpoints – 50 MB for agent-based endpoints
JMS Adapters (Oracle WebLogic JMS Adapter and IBM MQ Series JMS Adapter)	**For trigger configurations** • Consume Message Operation: 10 MB with schema transformation. **For invoke configurations** • Produce Message Operation: 10 MB with schema transformation.
Apache Kafka Adapter	**For invoke configurations** • Produce/Consume Message Operations: 10 MB with schema transformation for all the outbound operations.
Oracle E-Business Suite Adapter	• 100 MB (for public internet-based endpoints) • 50 MB (for agent-based endpoints)
SAP Adapter	50 MB For the SAP Adapter as a trigger connection, the limit is 50 MB for all document types. .
Oracle CPQ Adapter - response payload	50 MB.
AS2 Adapter file size limit	10 MB.
Timeouts for all connectivity agent-based outbound adapter invocations	Connection timeout is set to 4 minutes.
Timeouts for all outbound adapter invocations	The following values are set and cannot be changed: • READ timeout is set to 5 minutes. • Connection timeout is set to 5 minutes.

Resource	Service Limit
Oracle Autonomous Data Warehouse Adapter, Oracle Autonomous Transaction Processing Adapter, Oracle Database Cloud Service Adapter, MySQL Adapter, Microsoft SQL Server Adapter, Oracle Database Adapter, and IBM DB2 Adapter	Starting with the August 2021 release, all *new* integrations that include stored procedure or PureSQL database operations must finish within 240 seconds. Otherwise, the query times out.
Salesforce Adapter - batch file size	8 MB (10,000 records). See Process Large Data Sets Asynchronously with Different Bulk Operations.
SAP Ariba Adapter	See SAP Ariba Adapter Restrictions.
Connectivity agent - memory	A minimum of 8 GB memory with 4 GB of heap size dedicated to the on-premise agent's Java Virtual Machine (JVM). To include any other processes on the host besides the agent, increase the physical memory to a value greater than 8 GB.
Connectivity agent - message payload	10 MB, through the use of compression. **All connectivity-agent-enabled adapters** • 50 MB as request. • 50 MB as response. **SOAP and REST adapters configured with connectivity agent** • 50 MB (structured XML/JSON document) as response from SOAP/REST endpoints. • 1 GB for attachments as part of a response from SOAP/REST endpoints.

Component: Integrations

Resource	Service Limit
Active integrations limit	700. This limit is enforced. See Activate an Integration in *Using Integrations in Oracle Integration 3*.
Integration invocation depth	16 invocations. For example, a parent integration (schedule integration) invokes a child integration (application integration), which in turn recursively invokes the parent integration. Integration entry points along the request execution path are counted towards the limit. When 16 is exceeded, it results in an error.
String size limit	Restricted to 10,000 characters. The limit is applicable to all variables of type string, including global variables. The limit is also applicable to all functions, including a concat function used inside an assign, stitch, or mapper.
Parallel action concurrency limits	Parallel action branches independent of the integration type (synchronous, asynchronous, and so on) count towards the concurrency limits on synchronous requests. For example. a parallel action with three branches needs two extra concurrency slots for the duration of the parallel action; one branch is counted towards the original flow already obtained.

Resource	Service Limit
Triggers (maximum number of concurrent requests)	• Synchronous: 100. • Asynchronous: No limit (50 at a time can execute, the rest are queued).
Maximum number of integrations that can subscribe to events	20 integrations can subscribe to events per service instance.
Maximum number of tracking events per instance	• 20,000 for non-error events • 30,000 for error events (extra 10,000 if events are associated with errors) • 2000 max error recorded After those limits are reached, events are no longer recorded in OpenSearch, but they continue to be processed and the instance overall state is calculated. This ensures that the instance state is updated in all scenarios.
Maximum OpenSearch payload sizes	The total payload size stored per instance in OpenSearch is limited to 25 MB. There is no limit for payloads stored in the Object Store. Only payloads under 32k are stored in OpenSearch.
Maximum duration for integration flows	• Asynchronous: Six hours (The instance is marked as aborted due to deadline timeout.) • Scheduled: Six hours (The instance is marked as aborted due to deadline timeout.) • Synchronous: Five minutes (An `HTTP 502` occurs.)
Stage file action (in integrations) - file size	Read Entire File operation: 100 MB. For files greater than 100 MB, use the Read File in Segments operation. Encrypt File operation: 1 GB. Decrypt File operation: 1 GB.
Synchronous integration message timeout	300 seconds. Synchronous integrations (integrations that return a response payload) return a timeout error if they run more than 300 seconds.
Oracle Integration Messaging - message size	10 MB.
Encode and decode file attachment content (mapper)	The functions `encodeReferenceToBase64(String reference)` and `decodeBase64ToReference(String base64Content)` have a file size limit of 10 MB.
Lookup column length	1024 characters.
Notification action - attachments size	• If using the default method: 2 MB. • If using your customer tenancy: A default value of 2 MB that can be increased until the maximum value supported by the Oracle Cloud Infrastructure Email Delivery Service is reached. Both the email body and attachment are considered in calculating the total size. See Configure Notification Emails and Email Delivery Service Capabilities and Limits.
Maximum number of outbound emails you can send from Oracle Integration in a rolling 24-hour window	• If using the default method: 10,000 emails. • If using your customer tenancy: Sets your limit to the number allowed by the Oracle Cloud Infrastructure Email Delivery Service. See Configure Notification Emails and Email Delivery Service Capabilities and Limits.

Resource	Service Limit
JavaScript execution timeout threshold	15 seconds.
JavaScript function maximum parameter support	20 parameters.
Maximum duration of an XSLT execution	120 seconds.
Concurrency	• Synchronous concurrent request: 100. • Asynchronous concurrent executions: 50. Asynchronous concurrent execution includes scheduled + triggered + connectivity agent.
Number of concurrent instances of given schedule integration	1 for scheduled and out-of-band and 1 for ad-hoc. Where: • Out-of-band: A *run now* run associated with a schedule. • Ad-hoc: A *run now* run not associated with a schedule.
Tenant and user requests	100 requests per second per tenant and 20 requests per second per user.
Execution time threshold for long running schedule integrations	Terminated by Oracle Integration if integration exceeds 6 hours. See When a Schedule Integration Instance Gets Terminated in *Using Integrations in Oracle Integration 3*.
Maximum number of iterations to execute for a while loop	5000. **Note**: There is *no* limit for a for-each loop.
Maximum number of iterations captured across all loops for a single instance ID for which tracking data is captured	1000.
Project limits	• 100 integrations, 20 connections, 50 lookups, and 20 JavaScript libraries per project. • 50 deployments per project.
Deployments to Oracle Cloud Infrastructure API Gateway	An Oracle Cloud Infrastructure API Gateway instance supports a maximum of 20 deployments. Each deployment can contain up to 50 routes. This provides you with a capacity of 1000 integration endpoints to which to deploy.
Maximum number of branches in a parallel action	5.
Tracking variable - value	8191 characters.
Instance data retention	Retention is based on the trace level set during integration activation: • Production: 32 days • Audit: 8 days • Debug: 24 hours
Time window for recovering a failed integration instance that's recoverable	The instance is recoverable until one of the following occurs: • It is aborted. This can happen due to integration deactivation. • It is successfully recovered or the recovery leads to a nonrecoverable error. • It is beyond its associated retention time, which is 32 days by default.
Activity stream displayable rows	5000 rows maximum are displayable when expanding the tree.
Total size of activity stream (REST response)	No limit.
Maximum number of instances shown on Instances and Errors pages	500.

Resource	Service Limit
Maximum number of tracking events per instance	40,000.
Maximum number of resubmissions allowed per instance ID	10.
Schedule parameter - value length	256 characters.
Maximum number of schedule parameters per integration	5 parameters.
Integration properties - value	256 characters.
Integration/Connection - name	50 characters.
Integration/Connection - package name	50 characters.
Integration/Connection - version	10 characters.
Integration/Connection - description	1024 characters.
B2B for Oracle Integration - Trading partner management and B2B message tracking	See Manage Trading Partners and Track B2B Messages in *Using B2B for Oracle Integration 3*.
Maximum *offset* supported (REST API)	500 (Cannot be overridden).
Maximum *limit* supported (REST API)	500 (Cannot be overridden).
Maximum timeout for a factory API	2 minutes.
Payload size for publishing and subscribing to events in integrations	The same limit supported by the inbound (trigger) adapter. See Component: Adapters.

Component: File Server

Resource	Service Limit
Storage	500 GB.
Concurrent connections	Maximum of 50 connections per service instance.

Other Service Limits

- For Process Automation service limits, see Service Limits in *Administering Oracle Cloud Infrastructure Process Automation*.
- For Oracle Cloud Infrastructure service limits, see Service Limits.

Oracle Integration Editions

Oracle Integration is available in two editions: *Standard* and *Enterprise*.

Either edition gives you the power to integrate your Software as a Service (SaaS) applications and your on-premises applications. Enterprise edition provides additional capabilities, including enterprise adapters. Enterprise edition enables you to also design, automate, and manage your business processes in the cloud.

Regardless of which edition you choose, Oracle handles cloud and database management and other administrative tasks for you.

> **Note:**
>
> All Oracle Integration Enterprise Edition features are visible in Standard Edition instances. However, if you have a Standard Edition license, you are not entitled to use features that are only available in Enterprise Edition (such as enterprise adapters, Process Automation, and B2B for Oracle Integration, unless you update your instance to Oracle Integration Enterprise Edition. See Edit the Edition, License Type, Message Packs, and Custom Endpoint of an Instance.

Here's a side-by-side comparison of what's licensed in each edition.

Capability	Available in Standard edition	Available in Enterprise edition
Integration	Yes	Yes
Visual Builder	Yes	Yes
Standard adapters	Yes	Yes
Enterprise adapters*	No	Yes
Process Automation	No	Yes
B2B**	No	Yes
File Server	Yes	Yes
Embedded recipes and business and technical accelerators	Yes	Yes

*Enterprise adapters consist of Oracle E-Business Suite Adapter, Oracle JD Edwards EnterpriseOne Adapter, Oracle Siebel Adapter, and SAP Adapter.

**You cannot create new integrations in standalone mode in Oracle Integration 3, but you can continue using the AS2 Adapter in standalone mode in integrations that you created in Oracle Integration Generation 2 and that were upgraded to Oracle Integration 3 (for example, for file transfer protocol use cases). To use the AS2 Adapter with B2B features such as the B2B action, B2B design time, and B2B runtime, you must use Enterprise edition.

Updates to Your Instance

Functional updates to Oracle Integration 3 occur every two months and involve zero downtime. Oracle completes all update work on your behalf, with no work required by you.

> **Note:**
>
> During an update existing flows continue to run. If you have flows that run longer than five minutes, you may see an increase in runtime of up to five additional minutes.

Shapes Determine When Updates Occur

Every instance has either a Development or Production shape, which you choose when you create the instance. Both instances have the same service level agreements (SLAs); the only difference is the timing of functional updates. Production instances are updated two weeks after Development instances.

Notifications

Oracle provides a notification about two weeks before installing a functional update on your instance. You receive the notification only if an administrator has enabled announcements. Everyone can see the notification in the user interface, and one or more people might also receive an email notification. See Enable Announcements for Oracle Integration.

Other Updates

Oracle delivers security updates in addition to functional updates. These updates don't impact end users. Oracle does not send notifications for these updates.

Dynamic Scaling

Oracle Integration scales to meet the demands of the user. Oracle Integration takes advantage of its modern architecture to scale dynamically based upon the current load. You define the number of messages to which to subscribe. Oracle Integration can handle at least twice the number of subscribed messages to account for peaks in usage.

Oracle Integration uses the message subscription value to bill the usage of the service instance and to pre-reserve a minimum level of resources to ensure prompt response times. If your usage increases, additional resources are dynamically added by Oracle Integration's horizontal scaling rules. You do not need to take any action other than ensuring that your message level subscription is in line with your expected usage.

Oracle Integration for Oracle SaaS

Oracle Integration for Oracle SaaS, a streamlined version of Oracle Integration, gives you the features and benefits of Oracle Integration with a focus on SaaS. You can create Oracle Integration for Oracle SaaS instances in any Oracle data region if you created a new Oracle Cloud account on or after February 11, 2020.

Here are the key differences between Oracle Integration for Oracle SaaS and Oracle Integration:

- **Purpose-built for connecting and extending Oracle SaaS.** Specifically, every integration you create must have an endpoint in an Oracle Cloud SaaS application, every Visual Builder application you create must use at least one business object or API call from an Oracle Cloud SaaS application, and every process application you create must include at least one business object or API call from an Oracle Cloud SaaS application.
- **Flexibility for hourly bursting**. Oracle Integration for Oracle SaaS is offered as a monthly subscription in packs of one million messages per month, which keeps costs predictable even when you have unpredictable hourly volumes. Usage is reported monthly instead of hourly.
- **Reuse of message packs across instances**. Oracle Integration for Oracle SaaS users can apply their message packs across instances. The following example describes this capability. Assume you perform the following tasks:
  - Buy five message packs, each consisting of one million messages.
  - Create three separate instances for development, test, and production.
  - Assign one message pack to all three instances.
  - Keep the two remaining message packs in a savings pool for future use.

If the load on the production instance increases, assign one message pack from the savings pool to the production instance. The production instance now consists of two message packs of one million messages each. You decide later to assign the remaining message pack to a new pre-production instance. If you delete the pre-production instance in three months, you can return the message pack from that instance to the savings pool for re-assignment to an existing instance. Or, you can provision a new instance to which you assign that message pack.

- **Provisioning**. Creating an instance for Oracle Integration for Oracle SaaS is slightly different from creating an instance for Oracle Integration, and Bring Your Own License (BYOL) is not available in Oracle Integration for Oracle SaaS. Differences in provisioning are noted in Create an Oracle Integration Instance.

Oracle Integration in Government Regions

Oracle Integration 3 is available in US and UK government regions.

To learn about the Oracle Integration features available in government regions, see the following documentation resources.

Government Regions	Documentation
• OC2 realm (Oracle Cloud Infrastructure US Government Cloud with FedRAMP Authorization) in the US Gov East (Ashburn) and West (Phoenix) regions • OC3 realm (Oracle Cloud Infrastructure US Federal Cloud with DISA Impact Level 5 Authorization) in the US DoD East (Ashburn), North (Chicago), and West (Phoenix) regions	*Using Oracle Integration 3 on Oracle Cloud Infrastructure US Government Cloud*
• OC4 realm (United Kingdom Government Cloud) in the UK Gov South (London) and UK Gov West (Newport) regions	Oracle Integration documentation on the Oracle Help Center

Oracle and Customer Responsibilities in Oracle Integration 3

This table summarizes the division of responsibilities between Oracle and customers in Oracle Integration 3.

R=Responsible, A=Accountable, C=Consulted, I=Informed

Task	Oracle's Role	Customer's Role	Comments
Patching and upgrade	R, A	I	Do not stop or start instances on a nightly basis. During routine maintenance patching, lifecycle operations are disabled. This may lead to a situation where the service instance cannot be started or stopped for several hours while the patching cycle completes. See Stop and Start an Oracle Integration Instance.

Task	Oracle's Role	Customer's Role	Comments
High availability	R, A	I	- -
Disaster recovery	C	R, A	- -
Security and compliance	R, A	I	- -
Data retention	R, A	I	There is a fixed time period for storage based on the tracing level you set when activating an integration. See Activate an Integration.
Maintenance notifications	R, A	I	- -
Service provisioning	C, A	R, I	- -
User setup, roles, and permissions	C	R, A	- -
Overage tracking and management	C	R, A	- -
Test-to-production promotion	C	R, A	- -
On-premises connectivity agent installation	C	R, A	- -
On-premises connectivity agent upgrade/patching	R, A	I	**Note**: When a new version of the on-premises connectivity agent becomes available, your host is automatically upgraded with the latest version. There is no downtime or interruption of service for in-progress integrations that use the connectivity agent. You are notified of upgrade success.
Source control and continuous integration	C	R, A	You can implement continuous integration/ continuous delivery in Oracle Integration. See this blog.
Integration monitoring and management	C	R, A	- -

See Preserve Your Instance Data.

2
Before You Begin with Oracle Integration 3

Get started with Oracle Integration 3 on Oracle Cloud Infrastructure.

Topics:

Can I Create an Oracle Integration 3 Instance?

Oracle Integration 3 refers to Oracle Integration running natively on Oracle Cloud Infrastructure.

> **Note:**
>
> Interested in Oracle Integration for Oracle SaaS instead, as described in Oracle Integration for Oracle SaaS? See Can I Create an Oracle Integration for Oracle SaaS Instance?

Differences Between Oracle Integration Generation 2 and Oracle Integration 3

Some features in Oracle Integration Generation 2 are different in Oracle Integration 3, or aren't yet available. For Oracle Integration Generation 2 features that aren't in Oracle Integration 3, see Differences from Prior Versions of Oracle Integration.

Additionally, Oracle has delivered some new features only to Oracle Integration 3. For a list of new features in Oracle Integration 3, see Whats New for Oracle Integration 3.

Oracle Integration Generation 2 Instances

Everyone can create new Oracle Integration Generation 2 instances. See Creating an Oracle Integration Instance in *Provisioning and Administering Oracle Integration Generation 2*.

Oracle Integration 3 Instances

Oracle Integration 3 is currently being rolled out. You can create an Oracle Integration 3 instance if:

- You've never created an Oracle Integration Generation 2 instance in your region.

  or

- Any Oracle Integration Generation 2 instances in your region were created after October 2022.

Additional resources:

- For details about the regions in which you can create an Oracle Integration 3 instance, see Availability.
- For guidance on creating instances, see Restrictions and Create an Oracle Integration Instance.

Combining Instances

If you have a continuous integration and deployment (CI/CD) process for Oracle Integration, you can have either Oracle Integration Generation 2 or Oracle Integration 3 instances, but not both. After Oracle upgrades your Oracle Integration Generation 2 instances to Oracle Integration 3, you can create additional Oracle Integration 3 instances. See Upgrade from Oracle Integration Generation 2 to Oracle Integration 3.

Additionally, you must use the same versions for all your environments. For instance, you can't use an Oracle Integration Generation 2 instance for development and an Oracle Integration 3 instance for production.

If Oracle hasn't upgraded your Oracle Integration Generation 2 instances yet and you want to explore the capabilities of Oracle Integration 3, file a service request on My Oracle Support.

Can I Create an Oracle Integration for Oracle SaaS Instance?

Oracle Integration for Oracle SaaS refers to Oracle Integration for Oracle SaaS running natively on the Oracle Cloud Infrastructure.

> **Note:**
>
> Interested in Oracle Integration 3 instead (not SaaS-specific)? See Can I Create an Oracle Integration 3 Instance? For information on differences, see Oracle Integration for Oracle SaaS.

Simply follow the instructions in this current guide to create an Oracle Integration for Oracle SaaS instance.

Sign In to the Oracle Cloud Infrastructure Console

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

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

Topics:

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

Sign In to the Console in Tenancies That Use Identity Domains

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

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

1. Go to http://cloud.oracle.com.
2. Enter your tenancy name and click **Next**.
3. Select the **default** domain.

> **Note:**
>
> If your sign-in page looks different, your tenancy may not use identity domains. See Sign In to the Console in Tenancies That Do Not Use Identity Domains

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

   The Oracle Cloud Infrastructure Console is shown.
5. Explore categories and options in the navigation menu.
   - Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Integration**. Use this landing page to access, create, and manage Oracle Integration instances.

     Click **pin** to save the selection under the **Pinned** category on the Home page.
   - Open the navigation menu and click **Identity & Security**. Under **Identity**, click identity links to to create compartments and domains if needed, and to perform tasks related to identity management. See Manage Access and Assign Roles.

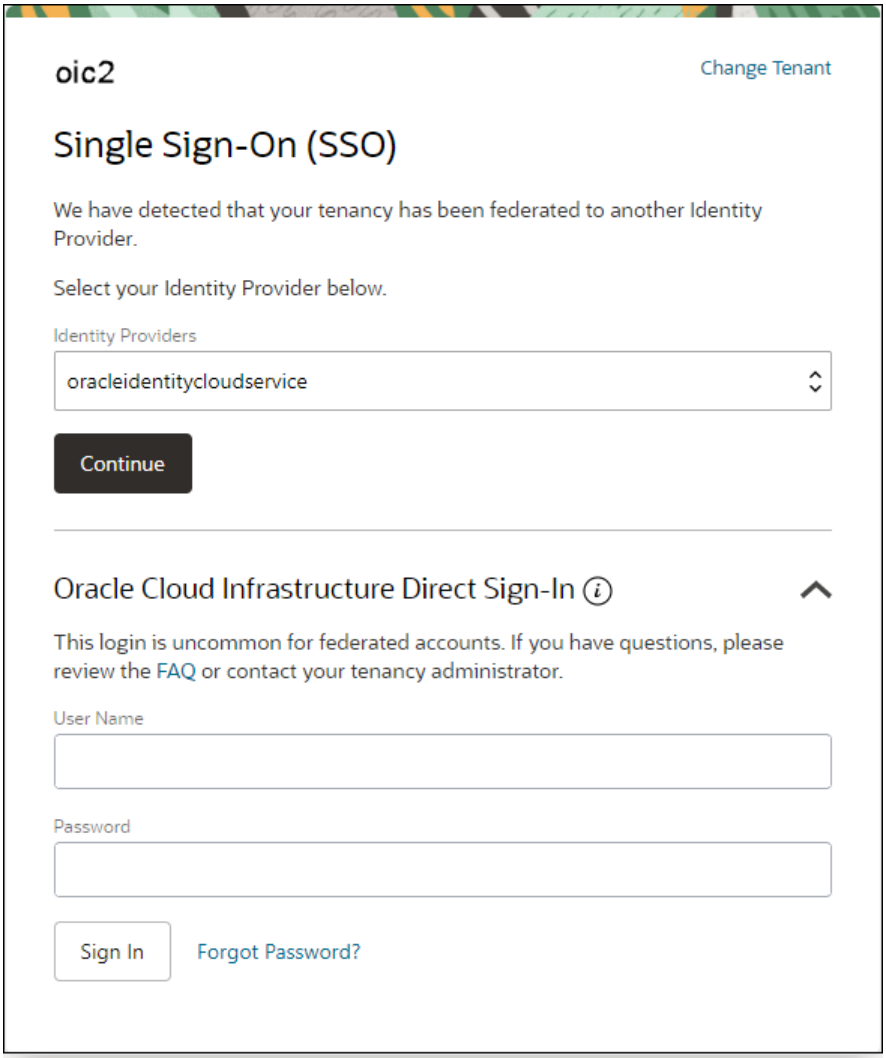
Sign In to the Console in Tenancies That Do Not Use Identity Domains

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

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

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

   Identity options are displayed.



> **Note:**
>
> If your sign-in page looks different, your tenancy may use identity domains. See Sign In to the Console in Tenancies That Use Identity Domains

- The *upper* portion displays federated sign in (Oracle Integration is federated with Oracle Identity Cloud Service).
- The *lower* portion displays native Identity and Access Management (IAM) options standard to Oracle Cloud Infrastructure.

> **Note:**
>
> If no federated sign in options are displayed in the upper portion, your tenancy requires manual federation. Sign in as an administrator using native IAM credentials and complete federation, including group mapping. See Understand Oracle Integration Federation and Manually Federate Your Tenancy.

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

The Oracle Identity Cloud Service sign in screen is shown.

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

   The Oracle Cloud Infrastructure Console is displayed.

4. Explore categories and options in the navigation menu.
   - Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Integration**. Use this landing page to access, create, and manage Oracle Integration instances.

     Click **pin** to save the selection under the **Pinned** category on the Home page.
   - Open the navigation menu and click **Identity & Security**. Under **Identity**, click identity links to to create compartments if needed, and to perform tasks related to identity management. See Manage Access and Assign Roles.

Create an Oracle Cloud Infrastructure Compartment

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

See Managing Compartments.

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

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Compartments**.
   A list of the compartments in your tenancy is displayed.
2. Select the compartment in which you want to create your instance or create a new compartment.
   To create a new compartment:
   a. Click **Create Compartment** to create the compartment to use for creating an instance.
   b. Enter the following:
      - **Name**: Enter a name that is unique across all compartments in your tenancy (maximum 100 characters, including letters, numbers, periods, hyphens, and underscores). For example, enter a name such as `OICCompartment`.

- **Description**: Enter a description for this compartment.
- **Tags**: Enter tags to organize and list resources based on your business needs. See Managing Tags and Tag Namespaces.

c. Click **Create Compartment**.

Return to the navigation pane.

3

Manage Access and Assign Roles

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

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

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

Topics:

Differences Between Tenancies With and Without Identity Domains

Managing users, groups, and policies for access to Oracle Integration differs depending on whether your tenancy uses identity domains.

Where You Manage Users and Groups

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

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

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

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

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

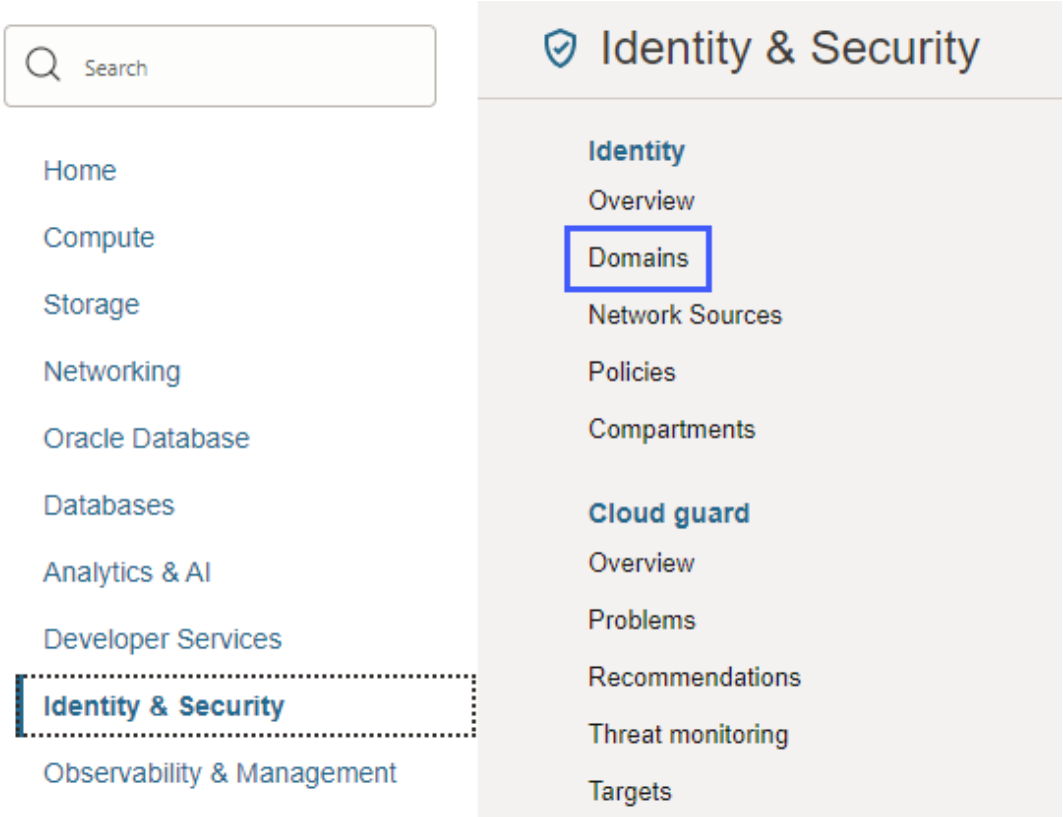
- Manage users, groups, and roles in both IDCS and Oracle Cloud Infrastructure IAM, linked using federation, if both of the following are true:
  - Oracle updated your region to use identity domains after you created your tenancy
  - And, Oracle has not yet migrated existing tenancies in your region to use identity domains

Determine Whether a Tenancy Uses Identity Domains

To determine whether your tenancy uses identity domains, open the Oracle Cloud Infrastructure navigation menu and click **Identity & Security**. Under **Identity**, check for **Domains**:

- If **Domains** is listed, then your tenancy uses identity domains.

  See Manage Access in an Identity Domain.



- If **Domains** is not listed, then your tenancy is still configured to link identities in IDCS and Oracle Cloud Infrastructure IAM using federation.

  See Manage Access Without an Identity Domain.

About Identity Domains

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

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

Differences

The following table outlines the differences between the two configurations.

Tenancies That Use Identity Domains	Tenancies That Do Not Use Identity Domains
Users and groups are configured in Oracle Cloud Infrastructure IAM.	Users and groups are configured in Oracle Cloud Infrastructure IAM and IDCS, linked through federation. See Understand Oracle Integration Federation. **Note**: Read only users can be assigned to an Oracle Cloud Infrastructure group only and not to an IDCS group.
The Oracle Cloud Infrastructure IAM service provides a single unified console for managing users, groups, dynamic groups, and applications in *domains*.	Oracle Cloud Infrastructure IAM must be federated with IDCS for your tenancy.
Provides Single Sign-On to more applications using a single set of credentials and a unified authentication process.	Requires separate federated credentials for IDCS.
The Federation page does not list any IDCS entries.	The Federation page lists the primordial IDCS type that is automatically federated as part of the tenancy creation.

About IAM Policies for Oracle Integration

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

You create IAM policies using the Oracle Cloud Infrastructure Console. See Managing Policies in the Oracle Cloud Infrastructure documentation.

Resource Types

The resource type available for Oracle Integration is:

- `integration-instance`

Supported Variables

The integration-instance resource type can use the following variables.

Supported Variables	Variable	Variable Type	Description
Required Variables Supplied by the Service for Every Request	`target.compartment.id`	`ENTITY`	The OCID of the primary resource for the request.
	`request.operation`	`STRING`	The operation id (for example `GetUser`) for the request.
	`target.resource.kind`	`STRING`	The resource kind name of the primary resource for the request.
Automatic Variables Supplied by the SDK for Every Request	`request.user.id`	`ENTITY`	For user-initiated requests. The OCID of the calling user.
	`request.groups.id`	`LIST(ENTITY)`	For user-initiated requests. The OCIDs of the groups of `request.user.id`.

Supported Variables	Variable	Variable Type	Description
	`target.compartment.name`	`STRING`	The name of the compartment specified in `target.compartment.id`.
	`target.tenant.id`	`ENTITY`	The OCID of the `target.tenant.id`.
Additional Variables for Oracle Integration	`target.integration-instance.id`	`ENTITY`	The OCID of the Oracle Integration instance that was created.

Details for Verb + Resource-Type Combinations

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

Verb	Permissions	APIs Fully Covered	APIs Partially Covered
`INSPECT`	• `INTEGRATION_INSTANCE_INSPECT`	• `ListIntegrationInstances` • `ListWorkRequests`	None
`READ`	• Inherits from `INSPECT`: – `INTEGRATION_INSTANCE_INSPECT` • `INTEGRATION_INSTANCE_READ`	• `GetIntegrationInstance` • `GetWorkRequest`	None
`USE`	• Inherits from `READ`: – `INTEGRATION_INSTANCE_INSPECT` – `INTEGRATION_INSTANCE_READ` • `INTEGRATION_INSTANCE_UPDATE`	• `UpdateIntegrationInstances` • `StartIntegrationInstance` • `StopIntegrationInstance`	None
`MANAGE`	• Inherits from `USE`: – `INTEGRATION_INSTANCE_INSPECT` – `INTEGRATION_INSTANCE_READ` – `INTEGRATION_INSTANCE_UPDATE` • `INTEGRATION_INSTANCE_CREATE` • `INTEGRATION_INSTANCE_DELETE` • `INTEGRATION_INSTANCE_MOVE`	• `CreateIntegrationInstance` • `DeleteIntegrationInstance` • `ChangeIntegrationCompartment`	None

Permissions Required for Each API Operation

API Operation	Permissions Required to Use the Operation
`ListIntegrationInstances`	`INTEGRATION_INSTANCE_INSPECT`
`GetIntegrationInstance`	`INTEGRATION_INSTANCE_READ`
`CreateIntegrationInstance`	`INTEGRATION_INSTANCE_CREATE`
`DeleteIntegrationInstance`	`INTEGRATION_INSTANCE_DELETE`
`UpdateIntegrationInstances`	`INTEGRATION_INSTANCE_UPDATE`

API Operation	Permissions Required to Use the Operation
`StartIntegrationInstance`	`INTEGRATION_INSTANCE_UPDATE`
`StopIntegrationInstance`	`INTEGRATION_INSTANCE_UPDATE`
`ListWorkRequests`	`INTEGRATION_INSTANCE_INSPECT`
`GetWorkRequest`	`INTEGRATION_INSTANCE_READ`
`ChangeIntegrationCompartment`	`INTEGRATION_INSTANCE_MOVE`

Oracle Integration Service Roles

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

For details on what you can do in each Oracle Integration feature by service role, see Oracle Integration Roles and Privileges.

About the Roles

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

Oracle Integration	Description
ServiceAdministrator	A user with the ServiceAdministrator role is a super user who can manage and administer the features provisioned in an Oracle Integration instance.
ServiceDeveloper	A user with the ServiceDeveloper role can develop the artifacts specific to the features provisioned in an Oracle Integration instance. For example, a user assigned the ServiceDeveloper role can develop process applications in Process Automation, whereas the same user can design integrations in Integrations.
ServiceMonitor	A user with the ServiceMonitor role can monitor the features provisioned in an Oracle Integration instance. For example, the user can view instances and metrics, find out response times, and track whether instance creation completed successfully or failed. This role provides privileges for users with limited knowledge of Oracle Integration, but with high-level knowledge of monitoring it. This user role does not grant permissions to change anything. The ServiceMonitor role does not have any privileges in File Server, and Visual Builder.
ServiceDeployer	A user with the ServiceDeployer role can publish the artifacts developed in a feature. This role is not applicable for the Integrations feature. The ServiceDeployer role does not have any privileges in File Server, B2B for Oracle Integration, and Visual Builder.
ServiceUser	A user with the ServiceUser role has privileges to utilize only the basic functionality of a feature such as access to the staged and published applications. For example, in Integrations the user can navigate to resource pages (such as integrations and connections) and view details, but can't edit or modify anything. The user can also run integrations.

Oracle Integration	Description
ServiceInvoker	A user with the ServiceInvoker role can invoke any integration flow in an Oracle Integration instance that is exposed through SOAP/REST APIs or a scheduled integration. See Run an Integration Flow. A user with ServiceInvoker role cannot: • Navigate to the Oracle Integration user interface or perform any administrative actions in the user interface. • Invoke any of the documented Oracle Integration REST APIs. See About the REST APIs. The ServiceInvoker role does not have any privileges in Process Automation, File Server, B2B for Oracle Integration, and Visual Builder.
ServiceViewer	A user with the ServiceViewer role can navigate to all Integration resource pages (for example, integrations, connections, lookups, libraries, and so on) and view details. This user cannot edit any resources or navigate to the administrative setting pages. The ServiceViewer role does not have any privileges in Process Automation, File Server, B2B for Oracle Integration, and Visual Builder.

Privileges Vary by Capability

In Oracle Integration, you assign a role to a group, and all users in the group are granted the role for all the capabilities in an instance. Additionally, each role grants different privileges for each capability. For example:

- For the Integrations capability, users can design integrations.
- For the Process Automation capability, users can develop process applications.

Some predefined roles give access for only some features. For details on the privileges that each role grants, see Oracle Integration Roles and Privileges.

Manage Access in an Identity Domain

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

Determine Whether You Use Identity Domains

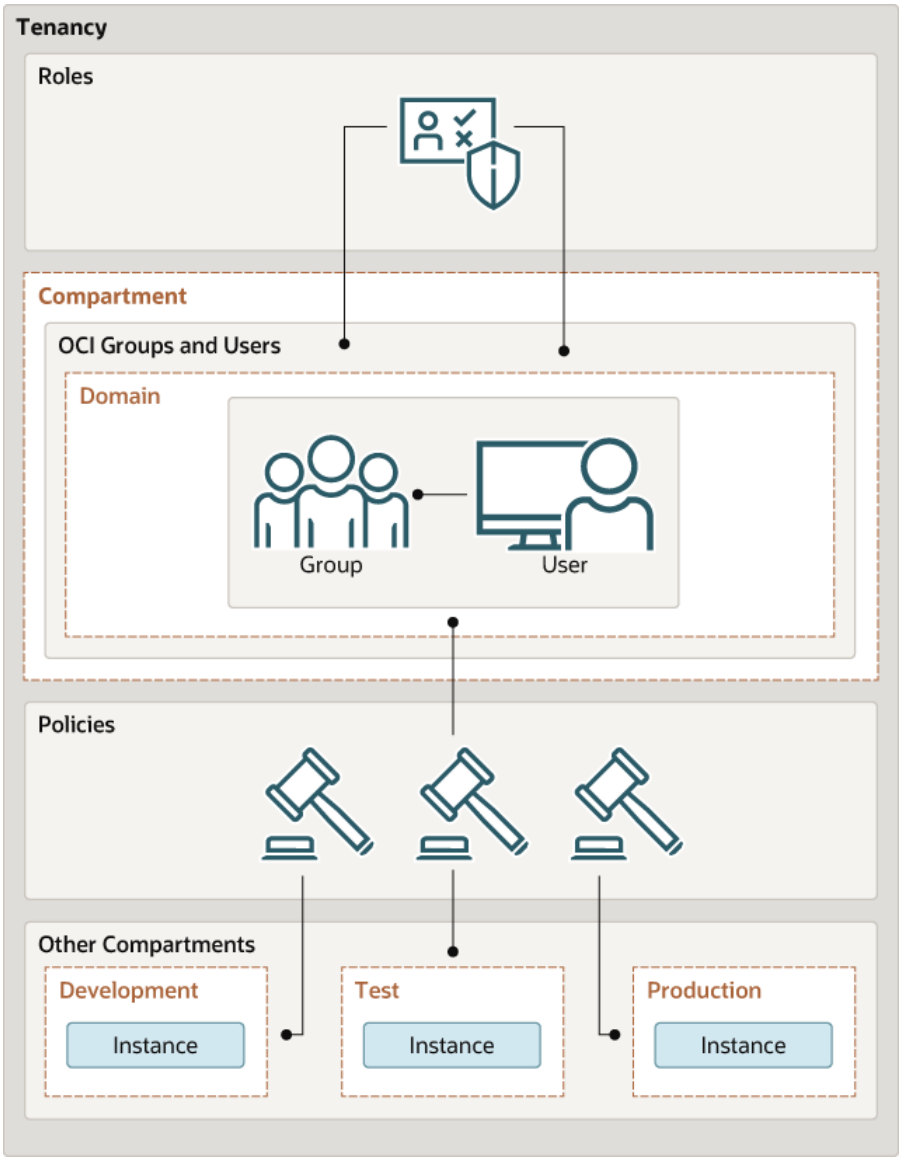
If you are not sure if your tenancy uses identity domains, see Differences Between Tenancies With and Without Identity Domains.

Documentation for Identity Services

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

How Roles Are Assigned in Identity Domains

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



Topics:

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

Workflow for Access in an Identity Domain

To give people access to Oracle Integration when your tenancy uses identity domains, complete a few tasks. Tasks include creating users, assigning them to groups, and assigning roles to groups.

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

Order	Task	More Information
1	Determine whether to create additional identity domains	Every tenancy comes with a default identity domain. An identity domain is a container for users, groups, and other access-related information. You can work exclusively in the default identity domain or create additional identity domains. You typically create additional identity domains for compliance reasons, when you want to maintain isolation among users, policies, and roles. For instance, you might create multiple identity domains to maintain the following types of isolation: • Between geographies, such as one domain for users in India and another domain for users in the United States. • Between services, such as one domain for Oracle Integration and another domain for another service. • Between instances of a service, such as one domain for each Oracle Integration instance. See Create an Identity Domain.
2	Create groups	Groups save you time when setting up access. You add several or many users to a group and then give the same access to everyone in the group. That way, you don't need to assign roles and policies to individual users. For example, create a group for developers, another for administrators, and so on. Everyone in the group gets the same access. See Create an IAM Group in an Identity Domain.
3	Create policies	Policies allow people to work with instances in specific tenancies and compartments. For example, if your company has multiple tenancies, policies let you specify the tenancies that each group can work in. You include the group name in each policy, so you don't need to assign the policies to groups separately after creating them. To learn about IAM policies in general, see How Policies Work and Example Scenario. To learn about IAM policies for Oracle Integration, see About IAM Policies for Oracle Integration. To create IAM policies, see Create an IAM Policy in an Identity Domain. **Note:** Your organization might have multiple instances of Oracle Integration. For example, you might have a development instance, as well as testing and production instances. The IAM policies that you write govern only a single instance.
4	Create users	Create one user for each person who needs access. You assign users to one or more groups when you create them. See Create a User in an Identity Domain.

Order	Task	More Information
5	Assign roles to groups	You can't create your own roles. Instead, choose from a predefined list of roles. To learn about the service roles that an administrator can assign to groups of users, see Oracle Integration Service Roles. To understand the actions that users can perform in each area of the user interface based upon their roles, see Oracle Integration Roles and Privileges. To assign service roles to users, see Assign Oracle Integration Roles to Groups in an Identity Domain.
6	Tell everyone they can start working	After you've set up your users, roles, and policies, inform everyone that they can start working in Oracle Integration.

Create an Identity Domain

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

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

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

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

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

You can also create multiple domains in a single compartment.

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**.

   The Domains page is displayed.
2. If not already selected, select the **Compartment** where you want to create the domain.
3. Click **Create domain**.
4. Enter required information in the Create domain page. See Creating Identity Domains in the Oracle Cloud Infrastructure documentation.

Create an IAM Group in an Identity Domain

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

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

For more information about IAM groups in identity domains, see Managing Groups in the Oracle Cloud Infrastructure documentation.

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**.

   The Domains page is displayed.
2. If not already selected, select the **Compartment** in which the domain where you want to create the group resides.
3. In the **Name** column, click the domain in which you want to create the group for creating and managing instances.

   The domain Overview page is displayed.
4. Click **Groups**.

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

Create an IAM Policy in an Identity Domain

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

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

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

   Syntax:

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

   Example: `allow group admin/oci-integration-admins to manage integration-instance in compartment OICCompartment`

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

Notes:

- If you omit the domain name, the default domain is assumed.
- When defining policy statements, you can specify either verbs (as used in these steps) or permissions (typically used by power users).
- You can create separate groups for different permissions, such as a group with `read` permission only.
- The `read` and `manage` verbs are most applicable to Oracle Integration. The `manage` verb has the most permissions (`create`, `delete`, `edit`, `move`, and `view`).

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

To learn more about policies, see:

- How Policies Work and Policy Reference in the Oracle Cloud Infrastructure documentation
- About IAM Policies for Oracle Integration

5. If desired, you can add a policy to allow members of the group to view message metrics, as described in View Message Metrics and Billable Messages.

   For example:

   ```
   allow group oci-integration-admins to read metrics in compartment
   OICPMCompartment
   ```

6. If you intend to use custom endpoints, add one or more additional policy statements. Otherwise, skip this step.

   Add policies that specify the compartment in which vaults and secrets reside and allow the admin group to manage secrets in it. See Configure a Custom Endpoint for an Instance.

   Note that you should specify the resource to return in *`resource-type`*, as described in Details for the Vault Service. Also note that Oracle Integration requires the `read` verb only but `manage` is recommended if the same group will also be administering the secrets (uploading/lifecycle operations).

   Examples::

   - `allow group admin/oci-integration-admins to manage secrets in compartment SecretsCompartment`
   - `allow group admin/oci-integration-admins to manage vaults in compartment SecretsCompartment`

7. Click **Create**.

   The policy statements are validated and syntax errors are displayed.

Create a User in an Identity Domain

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

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

For more information about users, see Managing Users in the Oracle Cloud Infrastructure documentation.

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**.

   The Domains page is displayed.
2. If not already selected, select the **Compartment** in which the domain that contains the group to which you want to add a new user resides.
3. In the **Name** column, click the domain for the group in which you want to create the user.

   The domain Overview page is displayed.
4. Click **Users**.

   The Users page for the domain is displayed.
5. Click **Create user**.
6. In the Create user screen, enter the user's first and last name, and their username, then select the one or more groups to which the user should be assigned.
7. Click **Create**.

   The new user is added to the selected group(s) and has permissions assigned to the group by its policy statement.
8. On the user details page that is displayed, you can edit user information as needed, and reset the user's password.
9. Provide new users with the credentials they need to sign in to their tenancy. Upon signing in, they will be prompted to enter a new password.

Assign Oracle Integration Roles to Groups in an Identity Domain

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

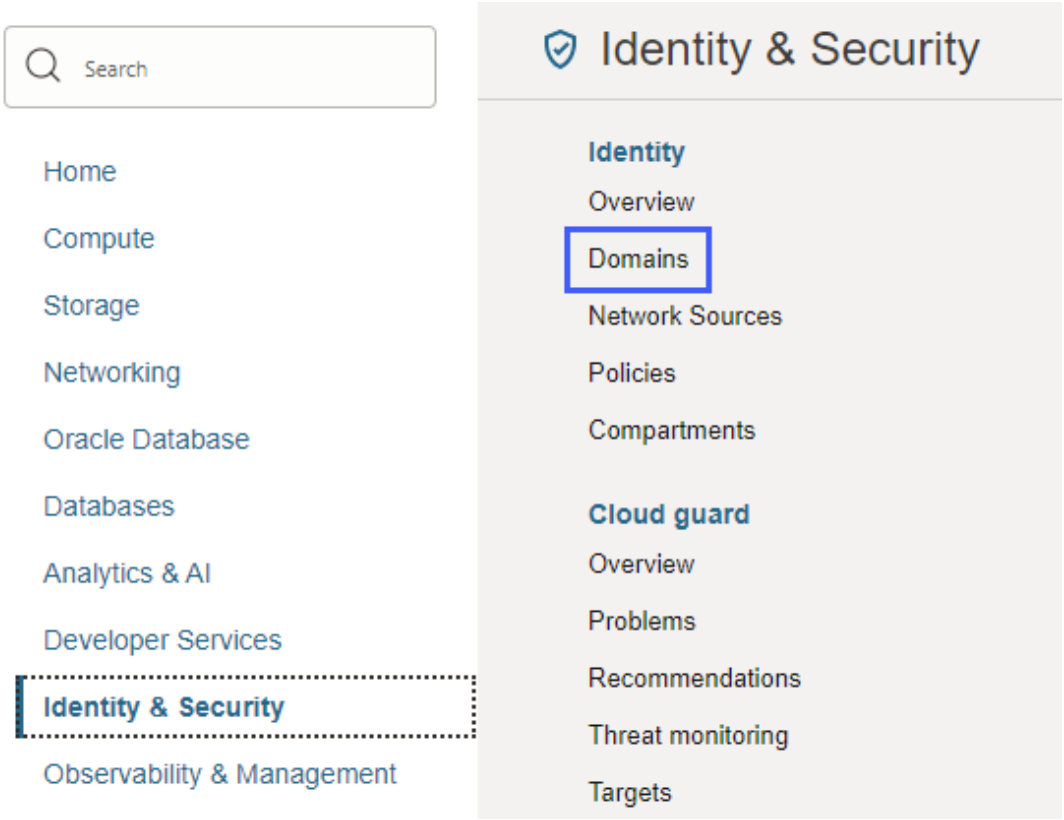
This topic applies only to tenancies that use identity domains. See Differences Between Tenancies With and Without Identity Domains.

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

Oracle Integration provides a standard set of roles, which govern access to features. See Oracle Integration Service Roles. Depending on the Oracle Integration features your

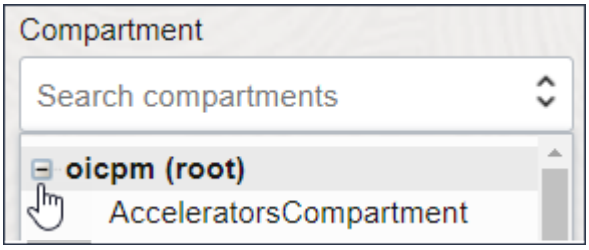
organization uses, you may choose to create groups named for the role they are granted. For example, `OICServiceAdministrators` for the Oracle Integration ServiceAdministrator role.

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**.

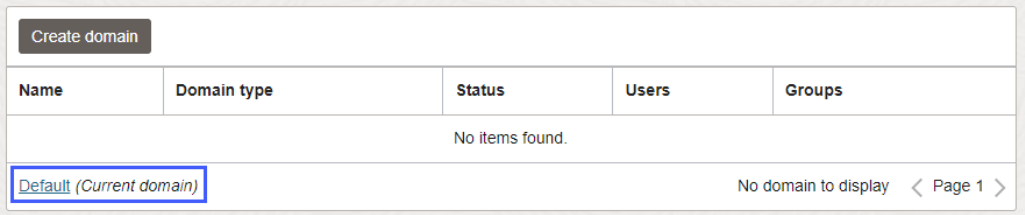


   The Domains page is displayed.

2. If not already selected, select the **Compartment** in which the domain that contains the group to which you want to assign Oracle Integration roles resides.



3. Open the domain for the group to which you want to assign roles:
   - To work in the default domain, click **Default**, located below the table.



   - To work in a different domain, click its name in the **Name** column.

   The domain Overview page is displayed.

4. In the navigation pane, click **Oracle Cloud Services**.

   The Oracle Cloud Services page is displayed.

5. In the **Name** column, click the Oracle Integration instance for which you want to assign group roles.

   The instance details page is displayed.

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

Manage Access Without an Identity Domain

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

Determine Whether You Use Identity Domains

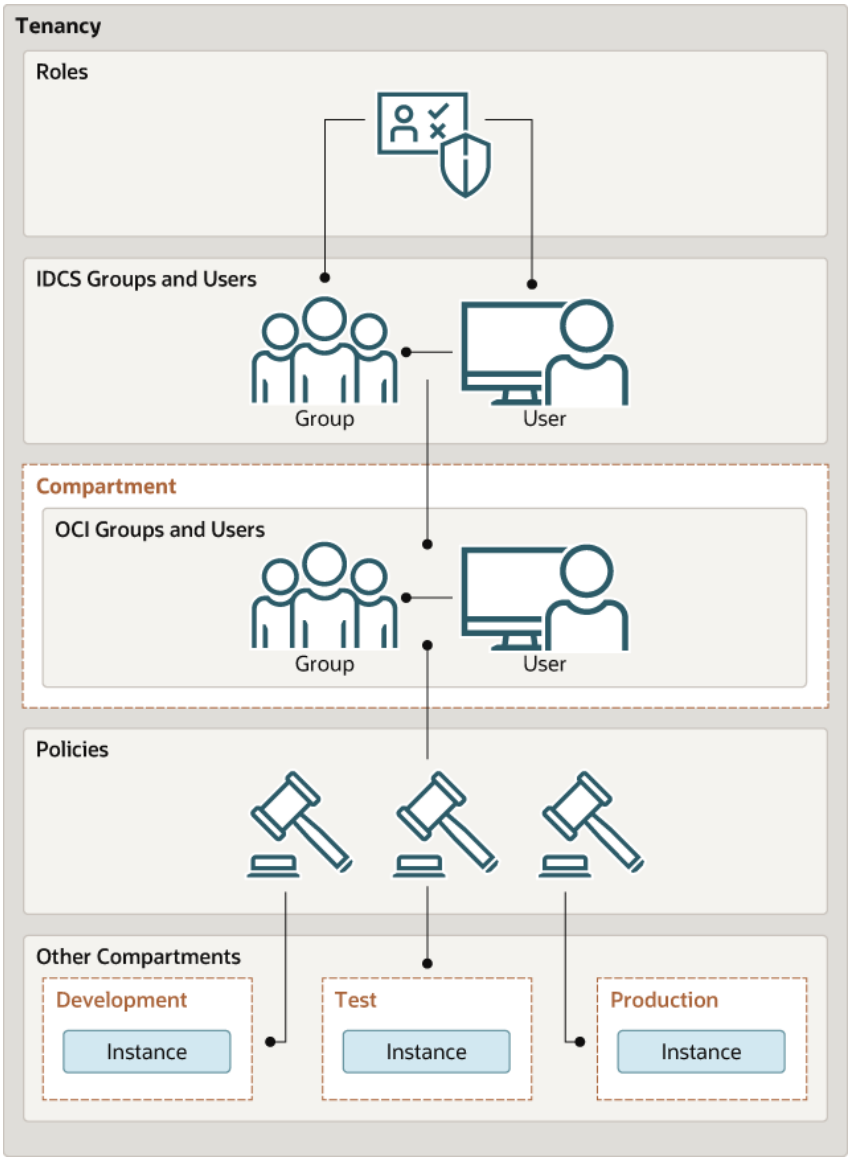
If you are not sure if your tenancy uses identity domains, see Differences Between Tenancies With and Without Identity Domains.

Documentation for Identity Services

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

How Roles Are Assigned in Identity Domains

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



Topics:

- Understand Oracle Integration Federation
- Create an IDCS Group
- Create an IAM Group
- Create an IAM Policy
- Map the IDCS and IAM Groups
- Create IDCS Users
- Create IAM Users
- Assign Oracle Integration Roles to Groups
- Configure Multiple Identity Stripes for Oracle Integration 3

Workflow for Access Without an Identity Domain

To give people access to Oracle Integration when your tenancy does not use identity domains, complete a few tasks. Tasks include creating users, assigning them to groups, and assigning roles to groups.

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

Order	Task	More Information
1	Create groups	Groups save you time when setting up access. You add several or many users to a group and then give the same access to everyone in the group. That way, you don't need to assign roles and policies to everyone individually. For example, create a group for developers, another for administrators, and so on. Everyone in the group gets the same access. You create each group in two places: Oracle Identity Cloud Service and Oracle Cloud Infrastructure Identity and Access Management. The groups must have different names. Later, you'll associate the groups by mapping them together. See Create an IDCS Group and Create an IAM Group.
2	Create policies	Policies allow people to work with instances in specific tenancies and compartments. For example, if your company has multiple tenancies, policies let you specify the tenancies that each group can work in. You include the group name in each policy, so you don't need to assign the policies to groups separately after creating them. To learn about IAM policies in general, see How Policies Work and Example Scenario. To learn about IAM policies for Oracle Integration, see About IAM Policies for Oracle Integration. To create IAM policies, see Create an IAM Policy. **Note:** Your organization might have multiple instances of Oracle Integration. For example, you might have a development instance, as well as testing and production instances. The IAM policies that you write govern only a single instance.
3	Map the groups	You created groups in Oracle Identity Cloud Service and Oracle Cloud Infrastructure Identity and Access Management. Now, you must associate them by mapping them together. See Map the IDCS and IAM Groups.

Order	Task	More Information
4	Create users	**Create Oracle Integration users in Oracle Identity Cloud Service** Create one user for each person who needs access to Oracle Integration. You assign users to one or more groups when you create the users. See Create IDCS Users. **Create superuser administrators in Oracle Cloud Infrastructure Identity and Access Management** Create administrators who require superuser access in Oracle Cloud Infrastructure Identity and Access Management. Users created in Oracle Cloud Infrastructure Identity and Access Management don't have access Oracle Integration. To give users access to Oracle Integration, you must create them in Oracle Identity Cloud Service and associate them with an application role. See Create IAM Users.
5	Assign roles to groups	You can't create your own roles. Instead, choose from a predefined list of roles. To learn about the service roles that an administrator can assign to groups of users, see Oracle Integration Service Roles. To understand the actions that users can perform in each area of the user interface based upon their roles, see Oracle Integration Roles and Privileges. To assign service roles to users, see Assign Oracle Integration Roles to Groups.
6	Decide whether to create additional stripes	Every tenancy comes with a stripe. A stripe is a container for access-related information. You can work exclusively in the primary stripe or create one or more secondary stripes. You create additional stripes for various business reasons, such as when you want to maintain isolation among users, policies, and roles for compliance reasons. To create one or more secondary stripes, complete the tasks in Configure Multiple Identity Stripes for Oracle Integration 3.
7	Tell everyone they can start working	After you've set up your users, roles, and policies, inform everyone that they can start working in Oracle Integration.

Understand Oracle Integration Federation

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

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

User federation refers to linking a user's identity and attributes across multiple identity management systems. Oracle Integration federation means that identities are linked in IDCS and Oracle Cloud Infrastructure Identity and Access Management (IAM).

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

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

For background information on federation with Oracle Identity Cloud Service, see Federating with Identity Providers and Federating with Oracle Identity Cloud Service.

Whether your tenancy needs federation depends on several factors, such as when your tenancy was created and the Oracle Integration version you're provisioning. Your tenancy may be:

- **Already fully federated:** Nearly all accounts in regions that have not yet been updated to use identity domains fall into this category. You'll follow standard steps to manage users and groups, as described in the topics in this section.
- **Mostly federated:** If you have an older account that was created before 21 December 2018, you may need to complete a final federation step. You'll follow steps to manage users and groups, as described in the topics in this section. At the mapping step (Map the IDCS and IAM Groups), you'll be asked to enter information.

Not sure about your federation? See Is My Tenancy Federated Between Oracle Cloud Infrastructure IAM and Oracle Identity Cloud Service?

Create an IDCS Group

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

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

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Federation**.

   The Federation screen is shown, and includes the identity provider, called **OracleIdentityCloudService**. This is the default federation between the Oracle Identity Cloud Service stripe and the OCI tenancy in a tenancy.
2. Select the **OracleIdentityCloudService** link to view the default Oracle Identity Cloud Service identity federation.
3. Select **Groups** from the **Resources** options.
4. Click **Create IDCS Group**.
5. Enter a name (for example, `idcs-integration-admins`).
6. Click **Create**.

Create an IAM Group

Create an instance administrator group in Oracle Cloud Infrastructure IAM and map it to your previously created IDCS group.

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

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Groups**.

The Groups screen is shown.

2. Click **Create Group**.
3. In the Create Group screen, assign a name to the group that differentiates it from the IDCS group (for example, `oci-integration-admins`), and enter a description.
4. Click **Create**.

Create an IAM Policy

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

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

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

   Syntax:

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

     `allow group` *`group_name`* `to` *`verb resource-type`* `in tenancy`

   Example: `allow group oci-integration-admins to manage integration-instance in compartment OICCompartment`

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

   Notes:

   - If you omit the domain name, the default domain is assumed.
   - When defining policy statements, you can specify either verbs (as used in these steps) or permissions (typically used by power users).
   - You can create separate groups for different permissions, such as a group with `read` permission only.
   - The `read` and `manage` verbs are most applicable to Oracle Integration. The `manage` verb has the most permissions (`create`, `delete`, `edit`, `move`, and `view`).

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

To learn more about policies, see:

- How Policies Work and Policy Reference in the Oracle Cloud Infrastructure documentation
- About IAM Policies for Oracle Integration

5. If desired, you can add a policy to allow members of the group to view message metrics, as described in View Message Metrics and Billable Messages.

   For example:

   ```
   allow group oci-integration-admins to read metrics in compartment
   OICPMCompartment
   ```

6. If you intend to use custom endpoints, add one or more additional policy statements. Otherwise, skip this step.

   Add policies that specify the compartment in which vaults and secrets reside and allow the admin group to manage secrets in it. See Configure a Custom Endpoint for an Instance.

   Note that you should specify the resource to return in *`resource-type`*, as described in Details for the Vault Service. Also note that Oracle Integration requires the `read` verb only but `manage` is recommended if the same group will also be administering the secrets (uploading/lifecycle operations).

   Syntax: `allow group` *`group-name`* `to manage` *`resource-type`* `in compartment` *`secrets-compartment`*

   Examples:

   - `allow oci-integration-admins to manage secrets in compartment SecretsCompartment`

     `allow oci-integration-admins to manage vaults in compartment SecretsCompartment`

7. Click **Create**.

   The policy statements are validated and syntax errors are displayed.

Map the IDCS and IAM Groups

Map your instance administrator group in Oracle Cloud Infrastructure IAM to your previously created IDCS group.

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

1. Open the Oracle Cloud Infrastructure navigation menu and click **Identity & Security**. Under **Identity**, click **Federation**.
2. On the Federation page, select the **OracleIdentityCloudService** link.
3. From the **Resources** options, choose **Group Mapping**.
4. Click **Edit Mapping**.
5. In the Edit Identity Provider dialog, click **Add Mapping** at the bottom.
   a. If the following dialog appears prompting you to provide credentials, enter this information from the COMPUTEBAREMETAL IDCS application in your IDCS account. This dialog indicates that your tenancy is mostly federated and requires only this final step. See Understand Oracle Integration Federation. (If you aren't able to locate this information, file a service request to get help from Oracle Support.)

   b. Click **Continue**.

6. Select your IDCS group in the **Identity Provider Group** field and your Oracle Cloud Infrastructure group in the **OCI Group** field.
7. Click **Submit**.

Create IDCS Users

You can create Oracle Identity Cloud Service users to add to Oracle Cloud Infrastructure IAM groups for specific access. To simplify access and permission management, grant permissions to groups instead of directly to users.

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

1. Open the Oracle Cloud Infrastructure navigation menu and click **Identity & Security**. Under **Identity**, click **Federation**.
2. On the Federation page, select the **OracleIdentityCloudService** link to view the default Oracle Identity Cloud Service federation.
3. Click **Create User**.
4. Complete the fields to identify the user. In the **Groups** field, select the IDCS group you want this user to belong to.
5. Click **Create**.

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

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

Create IAM Users

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

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

For more information about IAM users, see Managing Users in the Oracle Cloud Infrastructure documentation.

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Users**.
2. Click **Create User**.
3. In the resulting page, select **IAM User**.
4. Fill the required fields, and click **Create**.
5. Add the user to an IAM group with specific access.
   a. Under **Identity**, select **Groups**.
   b. From the groups list, click the group to which you want to add the user.
   c. Click **Add User to Group**.

   d. In the Add User to Group dialog, select the user you created from the drop-down list in the **Users** field, and click **Add**.

6. Create the user's password.
   a. From the Group Members table on the Group Details screen, select the user you added.
   b. Click **Create/Reset Password**. The Create/Reset Password dialog is displayed with a one-time password listed.
   c. Click **Copy**, then **Close**.
7. Provide read only users the information they need to sign in.
   a. Copy the password in an email to the user.
   b. Instruct the user to sign in using the **User Name** and **Password** fields.
   c. Upon signing in, the user will be prompted to change the password.

Assign Oracle Integration Roles to Groups

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

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

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

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

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Federation**.
2. On the Federation page, select the **OracleIdentityCloudService** link to view the default Oracle Identity Cloud Service identity federation.
3. On the Identity Provider Details page, select **Groups** from the **Resources** options.
4. From the table, select an IDCS group to grant the users in the group access.
5. On the Group Details page, click **Manage Roles**.
6. On the Manage Roles page, locate your integration service (`Integrationcauto` for Oracle Integration, `Integrationsub` for Oracle Integration for SaaS). At the far right, click ⋮, and select **Manage instance access**.

   The Manage Access screen lists instances. Note that you must assign roles for each instance individually.

   - Instance names follow this format: *`displayname-tenancyid-regionid`*

- Instance URLs follow this format: `https://displayname-tenancyid-regionid.integration.ocp.oraclecloud.com/ic/home/`

7. From the Manage Access options, select instance roles for the group under one or more specified instances.
8. Click **Update Instance Settings**, then **Apply Role Settings**.

Configure Multiple Identity Stripes for Oracle Integration 3

For Oracle Integration 3, the primary (primordial) stripe is automatically federated using preconfigured groups. However, you can create separate environments for a single cloud service or application (for example, create one environment for development and one for production), where each environment has a different identity and security requirements. Implementing one or more secondary stripes enables you to create and manage multiple instances of Oracle Identity Cloud Service to protect your applications and Oracle Cloud services.

> **Note:**
>
> Once provisioned, you cannot change the Oracle Identity Cloud Service stripe or change the association of the Oracle Integration instance to another IAM domain.

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

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

For benefits to using multiple Oracle Identity Cloud Service instances, see About Multiple Instances.

Follow the steps below to manually federate a secondary stripe for your tenancy. You must be the owner of the tenancy.

1. Define a Stripe Naming Convention
2. Create an IDCS Group for Secondary Stripe Users
3. Create an OAuth Client in the Secondary Stripe
4. Create an Oracle Cloud Infrastructure Group for Secondary Stripe Users
5. Create the Federation and Its Group Mapping
6. Create an Oracle Cloud Infrastructure Policy for Federated Users to Create Instances
7. Provide Access to a Federated Stripe in the Oracle Cloud Infrastructure Console Group for Secondary Stripe Users
8. Create Oracle Integration Instances in the Secondary Stripe Compartment

Define a Stripe Naming Convention

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

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

Entity	Naming convention
IDCS group	*`stripename`*`_administrators`
OCI group	`oci_`*`stripename`*`_administrators`
Compartment	*`stripename`*`_compartment`
Identity Provider	*`stripename`*`_service`
Policy	*`stripename`*`_adminpolicy`
Policy Statement	`allow group oci_`*`stripename`*`_administrators to manage integration-instances in compartment` *`stripename`*`_compartment`

Create an IDCS Group for Secondary Stripe Users

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

1. Add a group in the secondary stripe, and name it *`stripename`*`_administrators`. See Define a Stripe Naming Convention. For example, name it `stripe2_administrators`. Click **Finish**.

   For more information, see Create Groups in *Administering Oracle Identity Cloud Service*.

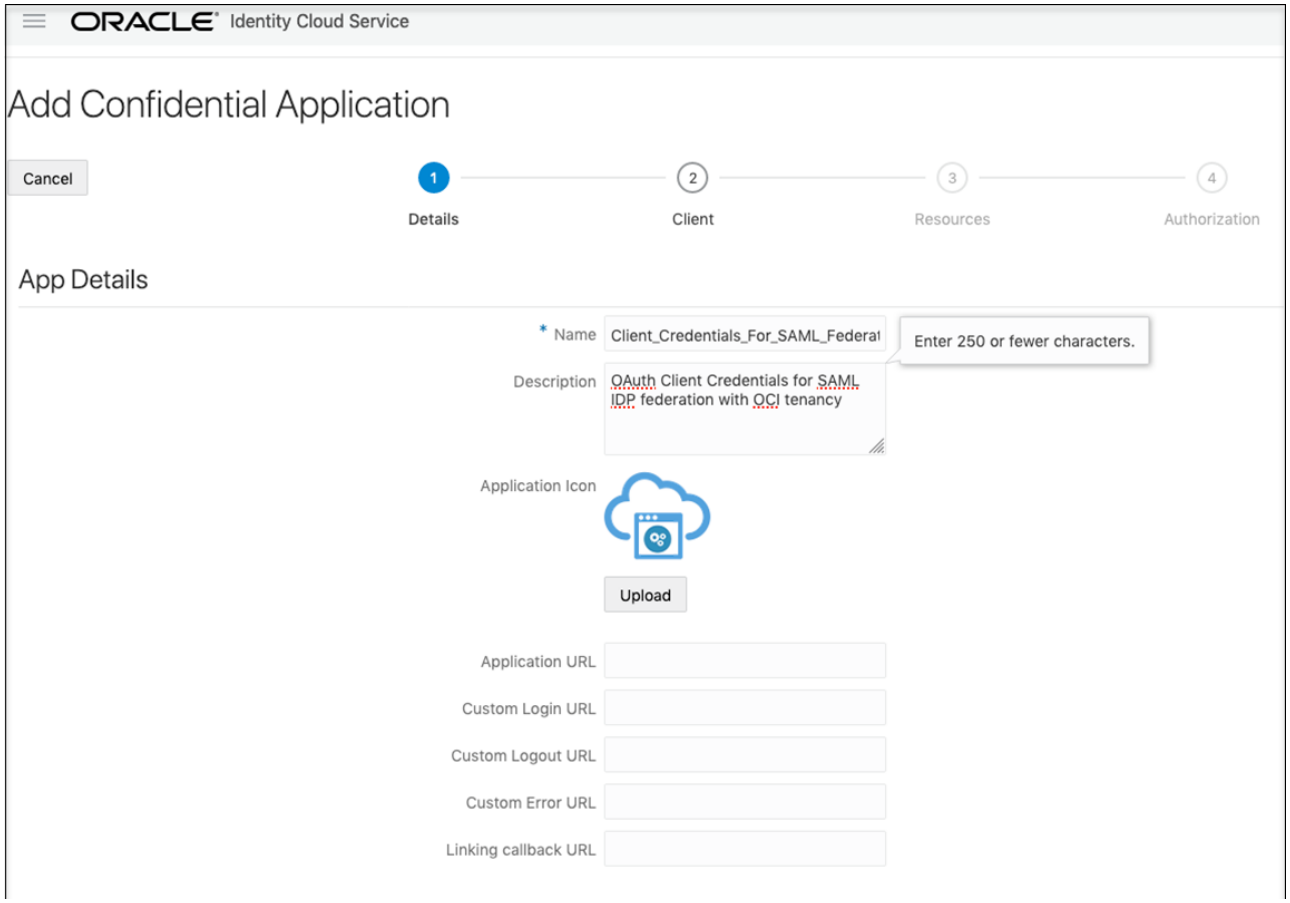
   These administrators will be granted permission to create Oracle Integration instances. This IDCS group will be mapped with an Oracle Cloud Infrastructure group.

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

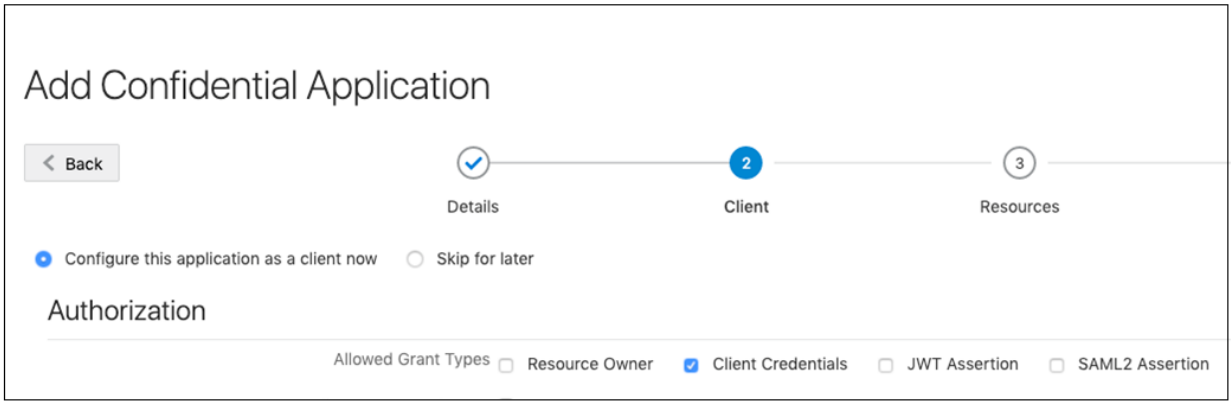
Create an OAuth Client in the Secondary Stripe

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

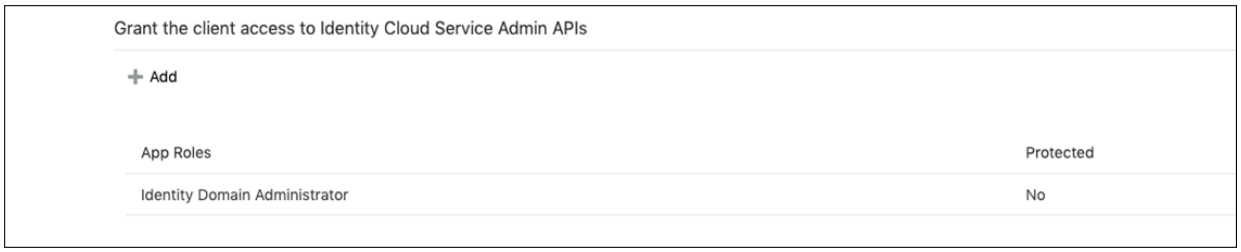
1. As an IDCS administrator, sign in to the secondary IDCS admin console.
2. Add a confidential application.
   a. Navigate to the **Applications** tab.
   b. Click **Add**.
   c. Choose **Confidential Application**.
   d. Name the application `Client_Credentials_For_SAML_Federation`.
   e. Click **Next**.



3. Configure client settings.
   a. Click **Configure this application as a client now**.
   b. Under **Authorization**, select **Client Credentials**.

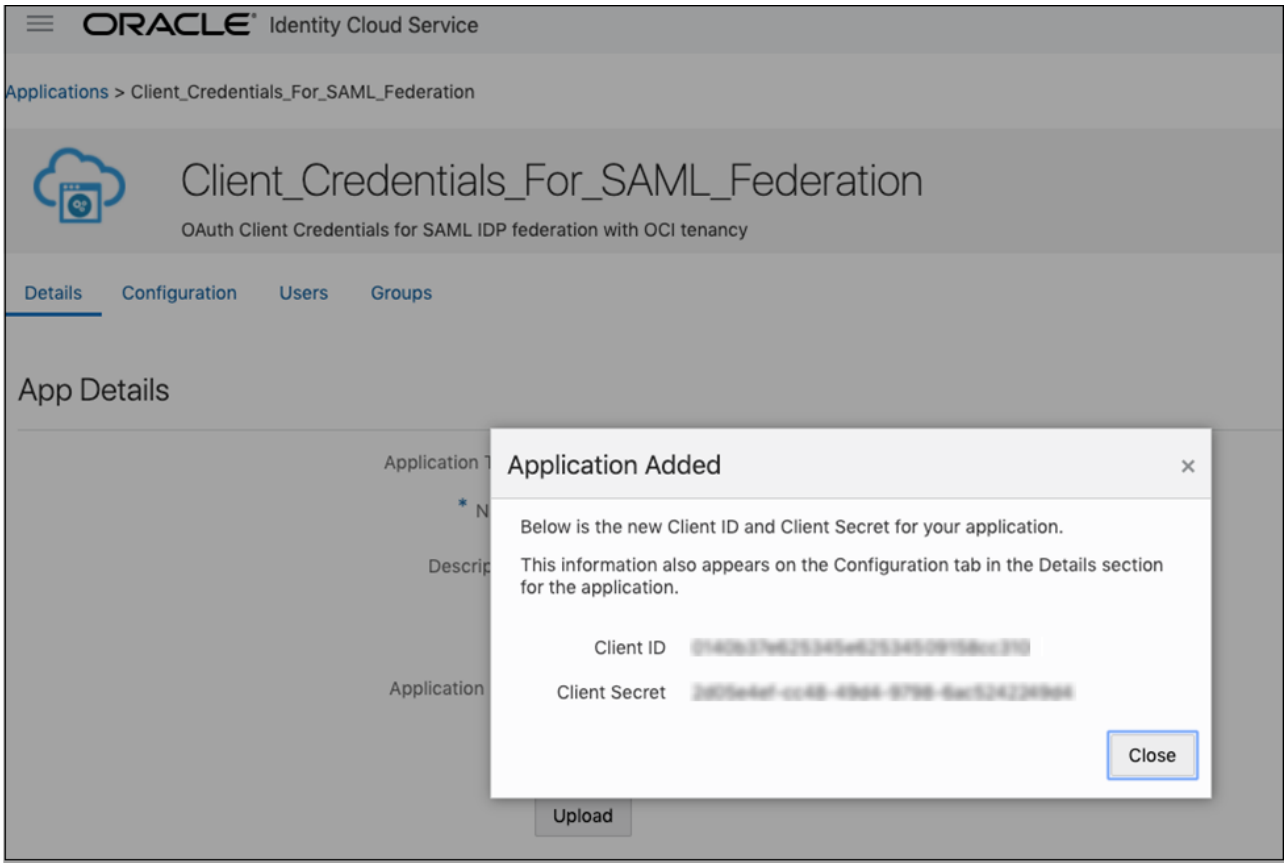


   c. Under **Grant the client access to Identity Cloud Service Admin APIs**, click **Add** and select the app role **Identity Domain Administrator**.



d. Click **Next** twice.

4. Click **Finish**. Once the application is created, note its client ID and client secret. You'll need this information in upcoming steps for federation.



5. Click **Activate** and confirm activating the application.

Create an Oracle Cloud Infrastructure Group for Secondary Stripe Users

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

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

   This Oracle Cloud Infrastructure group will be mapped with the IDCS group you created.

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

Create the Federation and Its Group Mapping

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

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

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

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

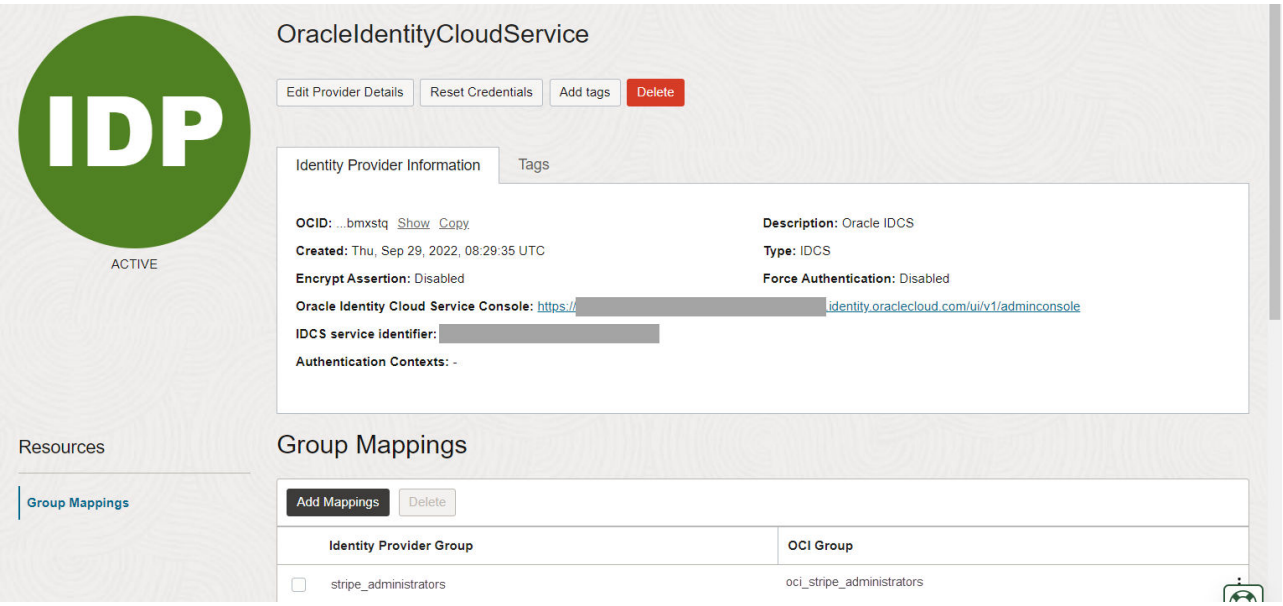
Field	Entry
Name	`<stripename>_service`
Description	`Federation with IDCS secondary stripe`
Type	Oracle Identity Cloud Service
Oracle Identity Cloud Service Base URL	Enter this URL using the format: `https://idcs-xxxx.identity.oraclecloud.com` Replace the `<idcs-xxxx>` domain part with your secondary IDCS stripe.
Client ID/Client Secret	Enter this information that you created in the secondary stripe and noted during Create an OAuth Client in the Secondary Stripe steps.
Force Authentication	Select this option

5. Click **Continue**.
6. Map the IDCS secondary stripe and OCI groups you previously created.

   Map the IDCS secondary stripe group (created in Create an IDCS Group for Secondary Stripe Users) and the OCI group (created in Create an Oracle Cloud Infrastructure Group for Secondary Stripe Users).

7. Click **Add Provider**.

   The secondary stripe federation is complete. Notice that the group mapping is displayed.



8. Verify the secondary stripe, and configure visibility for secondary stripe administrators and users.
   - The tenant administrator can see all federated IDCS stripes in the OCI console:
   - The secondary stripe administrator and all other secondary stripe users will not see any stripes under federation. To resolve that, see Provide Access to a Federated Stripe in the Oracle Cloud Infrastructure Console Group for Secondary Stripe Users.

Create an Oracle Cloud Infrastructure Policy for Federated Users to Create Instances

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

1. Create a compartment where Oracle Integration instances for the secondary IDCS stripe can be created. Name the compartment `stripename_compartment`.

   For example, create a compartment named `stripe2_compartment`.

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

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

   - **Syntax**: `allow group stripename_administrators toverb resource-typein compartmentstripename_compartment`
   - **Policy**: `allow group oci_stripe2_administrators to manage integration-instances in compartment stripe2_compartment`

   This policy allows a user who is a member of the group in the policy to create an Oracle Integration instance (**integration-instance**) in the compartment named **stripe2_compartment**.

Provide Access to a Federated Stripe in the Oracle Cloud Infrastructure Console Group for Secondary Stripe Users

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

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

   Several of the examples show how to grant access to a specific federated stripe, by using a `where` clause that identifies the secondary stripe. You can get the federation's OCID from the federation view in the Oracle Cloud Infrastructure console.

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

Manage ALL or ONLY a specific secondary stripe identity provider (manage)	• ALL:
	`allow group oci_stripe2_federation_administrators to manage identity-providers in tenancy`
	• ONLY specific secondary stripe identity provider:
	`allow group oci_stripe2_federation_administrators to manage identity-providers in tenancy where target.identity-provider.id = "ocid1.saml2idp.oc1..aaaaaaaaa…"`

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

Additional information about where clauses

Suppose you define a policy for a group (as in the example shown below) that uses the manage verb with a where clause restricting it to a specific identity provider (ocid).

Example policy:

```
allow group OCISecStripeAdmin to manage identity-providers in tenancy where
target.identity-provider.id='ocid1.saml2idp.oc1..aaaaaaaa...'
```

When a user from the group logs into the Oracle Cloud Infrastructure Console and navigates to the Federation page, the following message appears within the table: `Authorization failed or requested resource not found.`

Adding the following additional policy enables users in the group to navigate to the same page and see the identity providers. They can inspect both, but are only able to see the group mappings (read) of the allowed identity provider:

Additional example policy: `allow group OCISecStripeAdmin to inspect identity-providers in tenancy`

Create Oracle Integration Instances in the Secondary Stripe Compartment

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

1. Sign in to the Oracle Cloud Infrastructure Console as a federated user from the secondary stripe.

   Users will need to select the secondary stripe in the Identity Provider field (`idcs-secondary-stripe-service`, in this case).

2. Authorized administrators can create Oracle Integration instances in the specified compartment (`idcs-secondary-stripe-compartment`, in this case).

4

Create and Edit Oracle Integration 3 Instances

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

> **Note:**
>
> As a tenancy administrator, you have the permissions required to create and edit Oracle Integration instances. To allow other users to perform these tasks, you must complete the steps to manage users and groups for access to Oracle Integration. These steps differ depending on whether or not your tenancy uses identity domains. See Differences Between Tenancies With and Without Identity Domains.

Topics:

Create an Oracle Integration Instance

Create an Oracle Integration instance in a selected compartment.

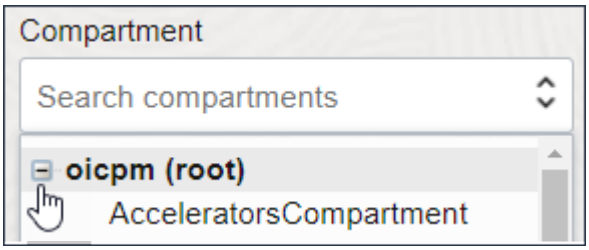
Some restrictions exist for creating instances. See Restrictions.

> **Note:**
>
> - Your Oracle Integration 3 instance is associated with an IDCS instance during instance creation. You cannot change this association after instance creation.
> - The steps here apply to Oracle Integration 3 and Oracle Integration for SaaS. Differences in instance creation are noted. For more information about the SaaS version, see Oracle Integration for Oracle SaaS.
> - You cannot split a single instance into two shapes (for example, into test and development shapes). Instead, you must create separate instances for each shape.

1. After signing in to the Oracle Cloud Infrastructure Console, note your selected region.

   For information about regions, see Regions and Availability Domains.

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



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

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

4. Click **Create**.
5. Enter the following details, and click **Create**:

Field	Description
Display Name	Enter the display name for the instance. Note that the display name becomes part of the URL for accessing the instance.
Version	**Note**: This field appears only if you can provision both Oracle Integration Generation 2 and Oracle Integration 3 instances. You can provision both instances if at least one of your instances has been upgraded to Oracle Integration 3. Select the version for the instance: • **Oracle Integration Generation 2** is the full-featured premier service, providing features and infrastructure technology including Integrations, Processes, Integration Insight, Visual Builder, B2B for Oracle Integration, File Server, and our portfolio of adapters. • **Oracle Integration 3** is the latest generation of Oracle Integration, providing the latest features and infrastructure technology including Integrations, Process Automation, Visual Builder, B2B for Oracle Integration, File Server, and our portfolio of adapters.
Consumption Model	Lists consumption models available in this tenancy. Typically, one model is displayed, but multiple consumption models are listed if your tenancy is enabled for more than one. Available models include: • Metered (Universal Credits) • Subscription (OIC4SaaS) • Oracle Integration Government
Edition	Two editions are provided. See Oracle Integration Editions to see what's licensed in each edition.
Shape	Choose a shape for the instance. The shape determines when the instance receives updates, which happen every other month. **Note**: You can't change the shape after you create the instance. However, you can move data to another instance using the export and import capabilities. • **Development**: Instances with this shape receive updates two weeks before instances with a Production shape. • **Production**: Instances with this shape receive updates two weeks after instances with a Development shape.
License Type	See Choose a License Type.
Message Packs	See Choose a Message Pack Number.
Access Token	If this field is displayed, you are creating an instance as a non-federated user. Sign in as a federated user and restart creating an instance.

Field	Description
Show Advanced Options	**Identity domain:** (Available only if you are provisioning an Oracle Integration 3 instance that uses identity domains. See Differences Between Tenancies With and Without Identity Domains.) Configure this tab to associate this instance with a secondary identity domain—an identity domain other than the one you're signed into. This allows you to manage all your instances in your tenancy from one domain, rather than having to sign into each domain to manage the associated instances. • **Change compartment**: The compartment you select here is the one that includes the secondary identity domain, not the one in which the instance will be created. The instance will be created in the compartment you selected in step 3. • **Domain**: Select the secondary identity domain you want to associate with this instance. **Note**: You must have ***read*** permission for the secondary identity domain. If you don't, the secondary identity domain administrator needs to add an IAM policy such as the following: `Allow group primary_identity_domain/group_name to read domains in compartment secondary_identity_domain_compartment` See Managing Policies and Details for IAM with Identity Domains. If you configure a secondary identity domain, Oracle Integration creates an Oracle Identity Cloud Service (IDCS) application in the secondary identity domain when it provisions your Oracle Integration 3 instance. If you don't configure a secondary identity domain, the IDCS application is created in the primary identity domain—the one you're signed into. After the Oracle Integration 3 instance has been created in the secondary identity domain, you need to assign administrators the ServiceAdministrator role in the IDCS application that was created. See Assign Oracle Integration Roles to Groups in an Identity Domain. **Network access:** Configure an allowlist for your instance. • For Oracle Integration Generation 2, see Configure an Allowlist for Your Instance in *Provisioning and Administering Oracle Integration Generation 2*. • For Oracle Integration 3, see Configure an Allowlist for Your Instance in *Provisioning and Administering Oracle Integration 3*. **Custom Endpoint:** Configure a custom endpoint URL for the instance. • For Oracle Integration 3, you configure a custom endpoint in the instance editor, not during instance creation. See Configure a Custom Endpoint for an Instance. • For Oracle Integration Generation 2, the custom hostname you want to map to the instance must already be registered on a DNS provider and its SSL certificate stored as a secret in an OCI Vault. See Configure a Custom Endpoint for an Instance. – **Hostname:** Enter the custom hostname chosen for the instance. – **Certificate:** Provide the location of the hostname's certificate in your OCI tenancy. * **Compartment:** Select the OCI compartment that contains your certificate vault.

Field	Description
	* **Vault:** Select the vault that contains the hostname's certificate. * **Secret:** Select the secret corresponding to the hostname's certificate. **Tags:** Enter a key and optional value. Tags enable you to track resources within your tenancy. See Resource Tags.

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

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

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

   Once created, an instance is visible only in the region in which it was created.

Choose a License Type

Select a license type for your Oracle Integration instance.

> **Note:**
>
> Choosing a license type applies when provisioning Oracle Integration only. It doesn't apply to Oracle Integration for SaaS.

- Select to create a new Oracle Integration license in the cloud. This provides you with packages of 5K messages per hour.
- Select to bring an existing Oracle Fusion Middleware license to the cloud for use with Oracle Integration. This provides you with packages of 20K messages per hour. This option is also known as bring your own license (BYOL).

Choose a Message Pack Number

When creating or editing an instance, specify the number of messages to use.

The message pack options available for selection are based on the version of Oracle Integration instance you are creating or editing. You are responsible for billing based on the message packs value you select.

- For Oracle Integration: Select the number of message packs. The total number of messages available per pack is based on the **License Type** option you selected. You can select up to 3 message packs if you bring an existing Oracle Fusion Middleware license (BYOL) to the cloud. You can select up to 12 message packs if you create a new Oracle Integration license in the cloud.
- For Oracle Integration for SaaS: Select the number of message packs to use per month. Each message pack consists of one million messages. You can select up to 43 message packs.

> **Note:**
>
> - Message pack updates can fail when maintenance and security patching are in progress.
> - You can also specify the number of message packs using the command line option. This enables you to specify larger values than permitted by the user interface. See Override the Message Pack Limit Using the Command Line.

Enable Capabilities

You must enable some capabilities in the Oracle Cloud Infrastructure Console before you can start using the capabilities. Other capabilities are available to everyone, without being enabled.

Must Be Enabled

To use the following capabilities, you must enable them:

- Process Automation

  See Use Process Automation in Oracle Integration.
- Visual Builder

  See Use Visual Builder in Oracle Integration.
- File Server

  See Enable File Server in *Using File Server in Oracle Integration 3*.

Available to Everyone

The following capabilities are available to everyone, without being enabled:

- B2B for Oracle Integration
- Integrations

Use Process Automation in Oracle Integration

You must complete a few tasks before you can start using Process Automation in Oracle Integration, including enabling Process Automation.

For instructions, see Enable Process Automation with Oracle Integration 3 in *Administering Oracle Cloud Infrastructure Process Automation*.

Use File Server in Oracle Integration

You must enable File Server before you can start using it.

For instructions, see Enable File Server in *Using File Server in Oracle Integration 3*.

Use Visual Builder in Oracle Integration

You must complete a few tasks before you can start using Visual Builder, including enabling Visual Builder.

Prerequisites

1. Create a policy that allows an administrator to enable Visual Builder.

   See Set the OCI Policy for Managing the Instance in *Administering Oracle Visual Builder in Oracle Integration 3*.

2. Enable Visual Builder.

   See Enable Visual Builder in *Administering Oracle Visual Builder in Oracle Integration 3*.

3. Add a connection to your Oracle Integration instance.

   See Add a Connection to Integration Applications in *Administering Oracle Visual Builder in Oracle Integration 3*.

Manage Your Visual Builder Instance

After you enable Visual Builder for Oracle Integration, Oracle Integration creates a Visual Builder instance. The *Administering Oracle Visual Builder in Oracle Integration 3* guide is available to help you manage this instance. See the following sections to get started managing the instance:

- View and Manage the Visual Builder Instance
- Configure Tenant Settings

Access an Oracle Integration Instance

Navigate to an Oracle Integration instance in the Oracle Cloud Infrastructure Console to open it.

> **Note:**
>
> The steps described in this section assume that you have view permission to the compartment containing one or more Oracle Integration instances. For users without view (or greater) permission to the console, a URL to the Oracle Integration instance should be provided by the administrator.

> **Note:**
>
> A user who creates an instance automatically has the ServiceAdministrator role assigned. All other users must have the appropriate role assigned for access. See:
>
> - For new tenancies in regions updated to use identity domains: Assign Oracle Integration Roles to Groups in an Identity Domain
> - For existing tenancies and new tenancies in regions not yet updated to use identity domains: Assign Oracle Integration Roles to Groups

1. Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Integration**.
2. If needed, select a compartment in the **Compartment** field.

   The page is refreshed to show any existing instances in that compartment. If needed, select another region. Note that instances are visible only in the region in which they were created.
3. At the far right, click ⋮, and select **Service Console** to access the Oracle Integration login page.

   If a message appears that access was denied, or the home page flashes, you don't have access to the Oracle Integration instance. See Assign Oracle Integration Roles to Groups.

   At this point, you are ready to:

   - Learn about the features and capabilities of Oracle Integration. See Oracle Integration.
   - Assign service roles to users (such as Developer or Administrator) to allow them to work with the features of Oracle Integration. See Assign Oracle Integration Roles to Groups.

Edit the Edition, License Type, Message Packs, and Custom Endpoint of an Instance

You can edit the edition, license type, and number of message packs of an Oracle Integration 3 instance. For Oracle Integration for SaaS instances, you can edit the edition and number of message packs. In addition, you can add (or update) a custom endpoint for Oracle Integration instances of both types. You cannot rename an instance.

1. In the **Name** column, click the instance to edit.
2. On the Integration Instance Details page, click **Edit**.

   The Edit Integration Instance dialog is displayed.
3. Update appropriate fields:

Field	Description
Edition	Update the edition. See Oracle Integration Editions to see what's licensed in each edition.
License Type	**Note**: If you are provisioning Oracle Integration for SaaS, this field is not shown. • Update to create a new Oracle Integration license in the cloud. This provides you with packages of 5K messages per hour. • Update to bring an existing Oracle Fusion Middleware (known as BYOL) license to the cloud for use with Oracle Integration. This provides you with packages of 20K messages per hour. This option is also known as Bring Your Own License (BYOL). There is no downtime when you change license types.

Field	Description
Message Packs	The message pack options available for selection are based on the version of Oracle Integration you are installing. • For Oracle Integration installations: Edit the number of message packs. The total number of messages available per pack is based on the **License Type** option you selected. You can select up to 3 message packs if you bring an existing Oracle Fusion Middleware license to the cloud. You can select up to 12 message packs if you create a new Oracle Integration license in the cloud. • For Oracle Integration for SaaS installations: Edit the number of message packs to use per month. Each message pack consists of one million messages. You can select up to 43 message packs. There is no instance downtime when you change the number of message packs. **Notes**: • You can also specify the number of message packs using the command line option. This enables you to specify larger values than permitted by this dialog. See Override the Message Pack Limit Using the Command Line. • You are responsible for billing based on the message packs value you select. • The number of message packs that you purchase does not impact your instance's concurrency limits. See Service Limits.

Field	Description
Show Advanced Options	**Custom Endpoint:** Configure this section to use a custom endpoint URL for the instance. The custom hostname you want to map to the instance must already be registered on a DNS provider and its SSL certificate stored as a secret in an OCI Vault. See Configure a Custom Endpoint for an Instance. • **Hostname:** Enter the custom hostname chosen for the instance. • **Certificate:** Provide the location of the hostname's certificate in your OCI tenancy. – **Compartment:** Select the OCI compartment that contains your certificate vault. – **Vault:** Select the vault that contains the hostname's certificate. – **Secret:** Select the secret corresponding to the hostname's certificate. **Note:** You can also update or replace a custom endpoint that was previously associated with the instance. You can modify the hostname as well as the certificate details. However, to update the certificate details, you must have access permissions to the vault containing the required certificate.

4. Click **Save Changes**.

Override the Message Pack Limit Using the Command Line

The user interface limits the message packs that you can choose, but you can override the limit using the Oracle Cloud Infrastructure command line (OCI CLI).

The limit in the user interface is 12 message packs if you create a new Oracle Integration license and 3 message packs if you bring an existing Oracle Fusion Middleware license (BYOL) to the cloud.

The OCI CLI is part of the Cloud Shell. The Cloud Shell provides access to a pre-installed Linux shell with a pre-authenticated Oracle Cloud Infrastructure command line. See Cloud Shell.

WARNING:

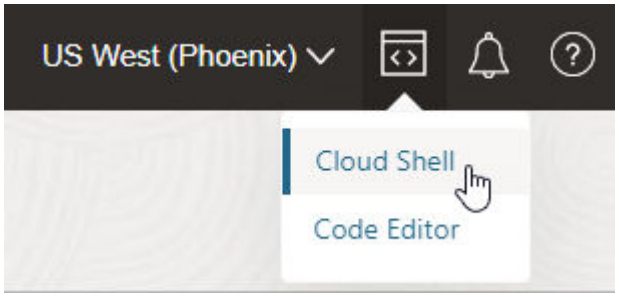
- Increasing the number of message packs increases your bill.
- The number of message packs that you purchase does not impact your instance's concurrency limits. See Service Limits.

The following steps provide an example of how to increase the number of message packs for your instance. The Cloud Shell supports a variety of features, tools, and utilities. You must also grant a specific IAM policy to the user requiring access to the Cloud Shell. See Cloud Shell.

1. Grant the following IAM policy to the group containing the user requiring access to the Cloud Shell. See Manage Access and Assign Roles.

   ```
   allow group group_name to use cloud-shell in tenancy
   ```

2. In the upper-right corner, click the **Developer Tools** icon, and select **Cloud Shell** to open the Cloud Shell.

   The Cloud Shell drawer opens at the bottom of the screen. The Cloud Shell executes commands against the selected region in which you opened the Cloud Shell (for this example, Phoenix is the selected region).

   ```
   Welcome to Oracle Cloud Shell.
   Try the new file upload/download capability in Cloud Shell. Access this
   new feature from the
   Cloud Shell menu.

   Your Cloud Shell machine comes with 5GB of storage for your home
   directory. Your Cloud Shell (machine
   and home directory) are located in: US East (Ashburn).
   You are using Cloud Shell in tenancy oicpm as an OCI Federated user
   oracleidentitycloudservice/my_login_name@example.com

   Type `help` for more info.
   my_login_name@cloudshell:~ (us-phoenix-1)$
   ```

3. Enter the following command to increase the number of message packs.

   For this example, the instance is using an existing Oracle Fusion Middleware license type brought to the cloud (BYOL) that is configured with 20K messages per pack (3 is the maximum value you can select for this license type in the Edit Integration Instance dialog). This example shows how to increase the value to 10.

   ```
   oci integration integration-instance update --id OCID_value --message-
   packs 10
   ```

   Where:

   - `--id` is the unique OCID identifier of your instance. This option is required. You get this value by clicking **Copy** in the **OCID** field on the details page for the instance.

- `--message-packs` is the number of allowed message packs to which to increase your instance. For this example, `10` is specified.

These are the minimum required options to specify. Additional command line options are also available. See Update Oracle Integration instances.

The following tasks occur during command execution:

- You receive an immediate response with a work request ID. For example:

```
{
  "opc-work-request-id": "ocid1.integrationworkrequest.oc1.geography-region-1.vmaerdicjfhkgfyaqrkihl6weoxhg6dxktxpdhh5ln6yi2en52xr3bplth4x"
}
```

  View the response in the **Work Requests** section at the bottom of the details page for the instance.

- Configuration changes occur quickly and the **Work Requests** section shows this operation as completed. The new message pack number is visible on the details page for the instance. Note that the value does not automatically refresh. You may need to return to the page with the list of all integrations, then click the specific instance again to see the changes on the details page.

View Instance Details

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

1. Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Integration**.
2. Click a specific instance name. The Details page is displayed. The word **Active** is displayed beneath the green circle to indicate that this instance is running. If you are viewing an Oracle Integration for SaaS instance, the License Type field is not displayed.

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

Field	Description
Service Console button	Click to access the login page. See Oracle Integration. **Note**: You can also access the login page from the main Oracle Cloud Infrastructure Console page for Oracle Integration. At the far right, click ⋮ for the specific instance, and select **Service Console**.
Edit button	Click to edit your settings. See Edit the Edition, License Type, Message Packs, and Custom Endpoint of an Instance.
Move button	Click to move the instance to a different compartment. This action can take some time to complete. See Move an Instance to a Different Compartment.
Add Tags button	Click to add tags to the instance. You can use tags to search for and categorize your instances in your tenancy. See Resource Tags.
Delete button	See Delete an Instance.

Field	Description
Integration Instance Information tab	• Creation date • Last updated date (for example, the last time started) • Version (appears only when you have or can create Oracle Integration Generation 2 and Oracle Integration 3 instances) • Selected consumption (billable) model • Edition, either standard or enterprise (appears only for Oracle Integration Generation 2 instances) • OCID value that uniquely identifies the instance, which can be shown in full and easily copied • Service console URL, which can be shown in full and easily copied • License type (either a new cloud license or an existing license brought over from Oracle Fusion Middleware). If you are viewing an Oracle Integration for SaaS instance, the License Type field is not displayed. • Number of message packs and the quantity of messages in each pack • Link for enabling File Server (cannot be undone) See Enable File Server in *Using File Server in Oracle Integration 3*. • Link for enabling Visual Builder (cannot be undone) See Use Visual Builder in Oracle Integration. • Link for enabling Process Automation (cannot be undone) See Enable Process Automation with Oracle Integration 3 in *Administering Oracle Cloud Infrastructure Process Automation*. **Note**: The IP address of your instance is not visible in the Oracle Cloud Infrastructure Console. If you need the outbound NAT address, file a service request with Oracle Support Services to obtain this value.
Custom Endpoint tab	This tab is displayed only for instances that have a configured custom endpoint. See Configure a Custom Endpoint for an Instance. Click the tab to view the custom endpoint URL, certificate details, and the original URL of the instance. **Note:** You can view the Certificate Secret Name only if you are granted the necessary permissions.
Tags tab	Click to add a tag.
Metrics page	Displays message metrics. See View Message Metrics and Billable Messages.
Work Requests page	Lists instance life cycle activity, such as instance creation time, instance stop and start times, and so on.
Network Access page	Displays allowlist rules.
Logs tab	Enable and disable the capture of logging activity.

Stop and Start an Oracle Integration Instance

You can stop and start Oracle Integration 3 instances. After a stop request is initiated, the instance goes into a pausing state. During the pausing state, no new integrations and processes are started. In-flight integrations and processes continue until they either complete or reach a checkpoint. When the integrations and processes are no longer running, the

instance goes into a completely paused state. While the instance is in this state, Oracle Integration design time, settings, and monitoring capabilities are unavailable.

> **Note:**
>
> - Oracle recommends that you do not stop instances running in a production environment.
> - Oracle recommends that you do not stop or start instances on a nightly basis. During routine maintenance patching, lifecycle operations are disabled. This may lead to a situation where the service instance cannot be started or stopped for several hours while the patching cycle completes.

1. Start or stop an instance in either of two ways:
   a. On the Integration Instances page, go to the end of the row for the specific instance, and click ⋮. Note that an active instance is identified as **Active** and an inactive/stopped instance is identified as **Inactive** in the **State** column.
   b. On the details page of a specific instance, select More Actions .
2. Select the action to perform:
   a. To stop your instance, select **Stop**, then select **Stop** again when prompted to confirm your selection.

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

      This action causes the following to occur:

      - For Oracle Integration users, billing is paused for the duration that the instance is paused.
      - For Oracle Integration for SaaS users, billing is not impacted by pausing an instance.
      - Integration endpoints are paused.
      - Process instances are paused.
      - Runtime is paused.
      - Scheduled integrations do not execute.
      - Database purging continues to run.
      - REST APIs are unavailable for use. If you attempt to use the APIs while your instance is in a paused state, you receive a `409` error.
      - Design time is not available for use. If you access the Oracle Cloud Infrastructure Console, it displays a page indicating the stopped state and asks you to start the instance for the console to become available.
      - You cannot stop an instance if patching is in progress.
   b. To resume your instance, select **Start**, then select **Start** again when prompted to confirm your selection.

> **Note:**
>
> You cannot start an instance when maintenance and security patching are in progress.

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

> **Note:**
>
> You can use the REST APIs to stop and start an instance. See Oracle Integration API. Oracle Integration APIs are available in the left navigation pane.

Move an Instance to a Different Compartment

You can move an instance to a different compartment.

> **Note:**
>
> Moving an instance can potentially change who has access to the instance. For example, if user A has the manage or read permission for one compartment and you move the instance to another compartment, they lose access. Ensure that the user has the necessary permissions for the compartment to which to move the instance.

> **Note:**
>
> Moving an instance affects access within the Oracle Cloud Infrastructure Console Console only (view or manage permissions). Access to an Oracle Integration instance does not change.

1. Determine where to start.
   - To work on the main Oracle Cloud Infrastructure Console page for Oracle Integration:
     a. Identify the instance to move.
     b. At the far right, click ⋮, and select **Move**.
   - To work on the details page for an existing Oracle Integration instance:
     a. Click a specific instance name in the Oracle Cloud Infrastructure Console. The Details page is displayed.
     b. Click **Move**.
2. Select the compartment to which to move the instance, then click **Move**.

   The move can take several minutes to complete. When done, the instance is displayed in the new compartment.

Delete an Instance

You have two options for deleting an Oracle Integration instance.

> **Note:**
>
> Deleting an Oracle Integration instance cannot be undone. This action permanently removes all design-time and runtime data.

- Choose where to delete the instance:
  - Delete the instance from the main Oracle Cloud Infrastructure Console page for Oracle Integration.
    1. Identify the instance to delete.
    2. At the far right, click ⋮, and select **Delete**.
  - Delete the instance from the details page for an existing Oracle Integration instance.
    1. Click the name of the instance to delete in the Oracle Cloud Infrastructure Console.
    2. Click **Delete**.
    3. When prompted to confirm your selection, click **Yes**.

Create an Access Token to Provision an Instance with the CLI, REST API, or SDKs

Before you can provision an Oracle Integration instance as a user with the command line interface (CLI), REST API, or any of the SDKs (Java and non-Java), you must create an application and generate an access token. You specify the access token when provisioning the instance.

For information on how to create an instance with the CLI, REST API, and Java SDKs, see:

- OCI CLI Command Reference
- Oracle Integration API
- Java SDK

Create the Application

Before you can provision an Oracle Integration instance as a user, you must first create an application.

> **Note:**
>
> You can skip this section if you have already created the application.

1. Sign in as the tenant administrator to the Oracle Cloud Infrastructure Console.

2. Open the Oracle Cloud Infrastructure navigation menu and click **Identity & Security**. Under **Identity**, click **Federation**.
3. Click the **OracleIdentityCloudService** link.
4. Click the link in the **Oracle Identity Cloud Service Console** field to access the console.
5. Open the Oracle Cloud Infrastructure navigation menu and click **Developer Services**. Under **Functions**, click **Applications**.
6. Click **Create application**.
7. Click **Confidential Application**.

   This starts the Add Confidential Application Wizard.
8. Enter a name (for this example, `PSO-AT-Gen-App` is provided) and optional description, and click **Next**.
9. Select **Configure this application as a client now** and provide the following details for client authorization:
   - **Allowed Grant Types**: **Resource Owner Client Credentials**, **JWT Assertion**
   - **Allowed Operations**: **Introspect**
10. Under **Grant the client access to Identity Cloud Service Admin APIs**, click **+ Add**.

    The Add App Role dialog is displayed.
11. Select **Identity Domain Administrator**, then click **Add**.
12. Click **Next** to access the next page in the wizard.
13. Select **Configure this application as a resource server now**.
14. Provide the following details, and click **Next**.
    - **Access Token Expiration**: **3,600** seconds.
    - **Is Refresh Token Allowed**: Select the check box.
    - **Refresh Token Expiration**: **604,800** seconds.
    - **Primary Audience**: For this example, `https://pso-at-gen-app.com/` is provided (the primary recipient where the token is processed).
15. Under **Scopes**, click **Add**.
16. In the **Scope** field, enter a value (for this example, `psoatgenapp`).
17. In the **Display Name** field, enter a value.
18. Leave the **Requires Consent** check box unselected, then click **Add**.
19. Click **Next** to go to the next page in the wizard.
20. Select **Skip for later**, then click **Next**.
21. Leave **Enforce Grants as Authorization** unselected, then click **Finish**.

    The application is created.
22. Click **Activate**, then click to confirm that you want to activate the application.

    The application (named **PSO-AT-Gen-App** for this example) is created and is ready to use to generate the access token for the users.

Generate the Access Token

Before you can provision an Oracle Integration instance as a user, you must create an access token.

> **Note:**
>
> The access token is only valid for one hour.

Generate the Access Token from the Oracle Cloud Infrastructure Console

1. Sign in as the tenant administrator to the Oracle Cloud Infrastructure Console.
2. Open the Oracle Cloud Infrastructure navigation menu and click **Identity & Security**. Under **Identity**, click **Federation**.
3. Click the **OracleIdentityCloudService** link.
4. Click the link in the **Oracle Identity Cloud Service Console** field to access the console.
5. Open the Oracle Cloud Infrastructure navigation menu and click **Developer Services**. Under **Functions**, click **Applications**.
6. Scroll down and click the application you created (for this example, named **PSO-AT-Gen-App**).
7. Select **Customized Scopes**.
8. Select **Invokes Identity Cloud Service APIs**, then specify **Identity Domain Administrator**.
9. Click **Download Token** and save the file.
   The `tokens.tok` file contains the access token with the attribute name **app_access_token**.

   ```
   cat tokens.tok

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

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

Generate the Access Token from the CLI or an API

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

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

Create an Oracle Integration Instance Using a Terraform Script

You can provision an Oracle Integration instance using a terraform script. Terraform is an infrastructure-as-code software tool that you can use in Oracle Cloud Infrastructure.

Details about using terraform in Oracle Cloud Infrastructure are provided. See Getting Started.

An example is provided for provisioning Oracle Integration with a terraform script. See Terraform Registry.

5

Manage Oracle Integration 3 Instances

Oracle manages instances, including performing database management, upgrading instances to the next version, installing patches, and more. You can perform these management tasks in Oracle Integration.

Topics:

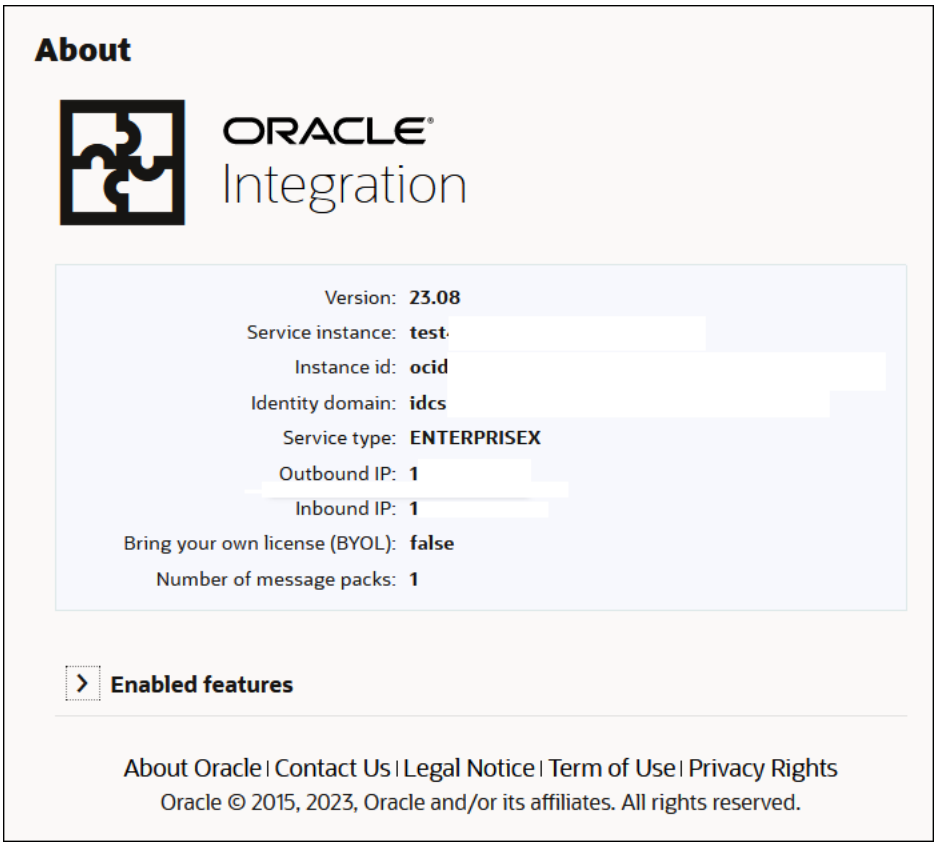
Obtain the Inbound and Outbound IP Addresses of the Oracle Integration Instance

You can obtain the NAT Gateway IP address (outbound IP address) and inbound IP address of your Oracle Integration instance from the **About** menu. The outbound IP address is required to allowlist the instance. This feature eliminates the need to file a service request to obtain the outbound IP address.

1. Go to the **About** menu in Oracle Integration. This menu is *not* available in the Oracle Cloud Infrastructure Console. You can access Oracle Integration from the URL listed in the **Service console URL** field on the details page of your Oracle Integration instance. See View Instance Details.

2. Select **About**.

   The outbound and inbound IP addresses are displayed.



3. Copy the values.
4. Use the outbound IP value to allowlist the instance.

Enable Announcements for Oracle Integration

System announcements provide timely and important information to Oracle Integration users. Your tenancy displays system announcements only after an administrator creates a policy that

allows the announcements. Creating the policy is a one-time action that applies to all Oracle Integration instances in the tenancy.

How to View Announcements

- **For administrators:** In the Oracle Cloud Infrastructure, click **Announcements** in the top panel.

  A green dot appears on the icon when there are new announcements for either Oracle Cloud Infrastructure or Oracle Integration.

- **For users:** In the top pane of Oracle Integration, click **Announcements**. An announcements window appears, listing past and ongoing announcements related to your Oracle Integration instance. See View Oracle Integration Announcements in *Getting Started with Oracle Integration 3*.

  Announcements appear only after an administrator sets the policy, described below. The list of announcements refresh every hour.

Learn More About Announcements

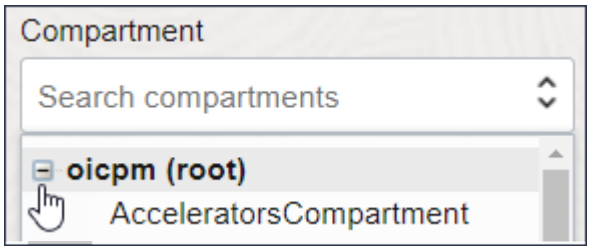
For information about console announcements, the types of information they contain, viewing options, and managing the email delivery of announcements, see Console Announcements.

Update the Recipients of Email Announcements

Oracle sends announcements to the default tenancy administrator email address on record. However, Oracle recommends changing the email address to a group address so that multiple people receive the email announcements. To change the email address, contact Oracle Support.

To Set the Oracle Integration Announcements Policy (One-Time Task):

1. In the Oracle Cloud Infrastructure console, open the Oracle Cloud Infrastructure navigation menu and click **Identity & Security**. Under **Identity**, click **Policies**.
2. From the **Compartment** list, select the root compartment.



   The announcements policy must be created at the root compartment.

3. Click **Create Policy**.
4. In the Create Policy window, enter a name (for example, `AnnouncementsPolicy`) and a description.
5. Complete the policy's **Statements** field, entering the following statements.

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

```
allow service integration to {ANNOUNCEMENT_LIST} in tenancy
allow service integration to {ANNOUNCEMENT_READ} in tenancy
```

6. Click **Create**.

   The policy statements are validated and syntax errors are displayed.

7. Go to Oracle Integration and verify that announcements are now displaying in the announcements window.

Choose Your Update Window

Functional updates occur every two months. Each functional update has two update windows. Your instance's update window is determined by the instance's shape. Instances with a Development shape receive updates two weeks before instances with a Production shape.

During the two-week interval between updates, your organization can sanity check the update before it is applied to a production instance.

The person who created the instance chose the shape during provisioning. You can't change the shape of an instance after the instance is created. However, you can move data to another instance using the export and import capabilities.

> **Note:**
>
> In Oracle Integration Generation 2, you chose your update window using tags. Oracle Integration 3 uses only an instance's shape to determine the update window.

Manage Integrations and Errors

You can manage integration errors in Oracle Integration.

Activate the service in Oracle Integration when the integration is ready to go live and you can deactivate an active Integration. You can modify or clone the integration. Delete an integration that is no longer needed. See Manage Integrations in *Using Integrations in Oracle Integration 3*.

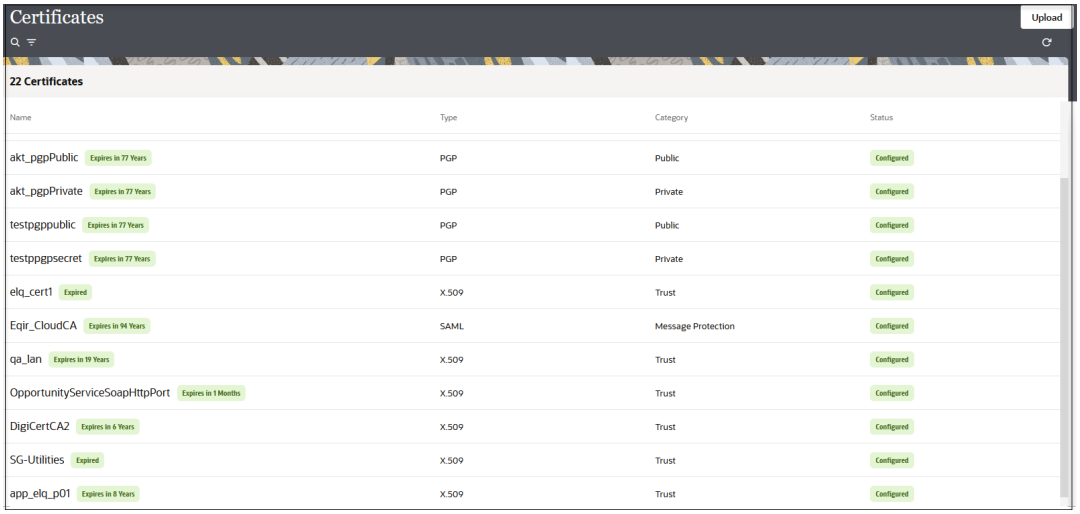
You can manage errors from the Errors pages in Oracle Integration at the integration level, connection level, or specific integration instance level. See Manage Errors in *Using Integrations in Oracle Integration 3*.

Upload an SSL Certificate

Certificates are used to validate outbound SSL connections.

If you make an SSL connection in which the root certificate does not exist in Oracle Integration, an exception error is thrown. In that case, you must upload the appropriate certificate. A certificate enables Oracle Integration to connect with external services. If the external endpoint requires a specific certificate, request the certificate and then upload it into Oracle Integration.

1. Sign in to Oracle Integration.
2. In the navigation pane, click **Settings**, then **Certificates**.
   All certificates currently uploaded to the trust store are displayed on the Certificates page.
3. Click **Filter** to filter by name, certificate expiration date, status, type, category, and installation method (user-installed or system-installed). Certificates installed by the system cannot be deleted.



4. Click **Upload** at the top of the page.
   The Upload certificate panel is displayed.
5. Enter an alias name and optional description.
6. In the **Type** field, select the certificate type. Each certificate type enables Oracle Integration to connect with external services.
   - X.509 (SSL transport)
   - SAML (Authentication & Authorization)
   - PGP (Encryption & Decryption)
   - Signing key

X.509 (SSL transport)

1. Select a certificate category.
   a. **Trust**: Use this option to upload a trust certificate.
      i. Click **Choose File**, then select the trust file (for example, `.cer` or `.crt`) to upload.
   b. **Identity**: Use this option to upload a certificate for two-way SSL communication.
      i. Click **Choose File**, then select the keystore file (`.jks`) to upload.
      ii. Enter the comma-separated list of passwords corresponding to key aliases.

      > **Note:**
      > When an identity certificate file (`.jks`) contains more than one private key, all the private keys must have the same password. If the private keys are protected with different passwords, the private keys cannot be extracted from the keystore.

      iii. Enter the password of the keystore being imported.
   c. Click **Upload**.

SAML (Authentication & Authorization)

1. Note that **Message Protection** is automatically selected as the only available certificate category and cannot be deselected. Use this option to upload a keystore certificate with SAML token support. Create, read, update, and delete (CRUD) operations are supported with this type of certificate.
2. Click **Choose File**, then select the certificate file (`.cer` or `.crt`) to upload.
3. Click **Upload**.

PGP (Encryption & Decryption)

1. Select a certificate category. Pretty Good Privacy (PGP) provides cryptographic privacy and authentication for communication. PGP is used for signing, encrypting, and decrypting files. You can select the private key to use for encryption or decryption when configuring the stage file action.
   a. **Private**: Uses a private key of the target location to decrypt the file.
      i. Click **Choose File**, then select the PGP file to upload.
      ii. Enter the PGP private key password.
   b. **Public**: Uses a public key of the target location to encrypt the file.
      i. Click **Choose File**, then select the PGP file to upload.
      ii. In the **ASCII-Armor Encryption Format** field, select **Yes** or **No**.
         - **Yes** shows the format of the encrypted message in ASCII armor. ASCII armor is a binary-to-textual encoding converter. ASCII armor formats encrypted messaging in ASCII. This enables messages to be sent in a standard messaging format. This selection impacts the visibility of message content.
         - **No** causes the message to be sent in binary format.
      iii. From the **Cipher Algorithm** list, select the algorithm to use. Symmetric-key algorithms for cryptography use the same cryptographic keys for both encryption of plain text and decryption of cipher text. The following supported cipher algorithms are FIPS-compliant:
         - AES128
         - AES192
         - AES256
         - TDES
   c. Click **Upload**.

Signing key

A signing key is a secret key used to establish trust between applications. Signing keys are used to sign ID tokens, access tokens, SAML assertions, and more. Using a private signing key, the token is digitally signed and the server verifies the authenticity of the token by using a public signing key. You must upload a signing key to use the OAuth Client Credentials using JWT Client Assertion and OAuth using JWT User Assertion security policies in REST Adapter invoke connections. Only PKCS1- and PKCS8-formatted files are supported.

1. Select **Public** or **Private**.
2. Click **Choose file** to upload a key file.

If you selected **Private**, and the private key is encrypted, a field for entering the private signing key password is displayed after key upload is complete.

3. Enter the private signing key password. If the private signing key is not encrypted, you are not required to enter a password.

Oracle Integration Instance Server Certificate Expiry

Generally, the Oracle Integration instance server certificate expiry will not affect you. If you have the DigiCert Global Root certificate in your trust store, you don't need to do anything. The Oracle Integration instance server certificate is automatically updated.

If you experience problems due to the expiry of the Oracle Integration instance server certificate, add the DigiCert Global Root certificate to your trust store.

Set Instance Quotas on Compartments

You can set quotas on the number of Oracle Integration 3 instances that can be created in a compartment.

Compartment quotas control resource consumption within compartments in Oracle Cloud Infrastructure. See Overview of Compartment Quotas.

1. In the banner, navigate to your home region.

If you attempt to create a compartment quota in a region that is not your home, you receive the following error:

```
Please go to your home region to execute Quota operations.
```

2. Open the navigation menu and click **Governance & Administration**.
3. Under **Governance**, click **Quota Policies**.
4. On the **Quota Policies** page, click **Create Quota**.
5. Enter a name and description.
6. Enter a quota policy string in the **Quota Policy** field. As an example, to set a quota limit of `10` instances for the compartment named `MyCompartment`, enter the following statement:

```
Set integration quota instance-count to 10 in compartment MyCompartment
```

Where:

- `integration`: Is the family name for Oracle Integration.
- `instance-count`: Is the quota name.

7. Click **Create Quota Policy**.

   The policy statement is validated and the details page for the new quota policy is displayed.

   If validation is unsuccessful, syntax errors are displayed for you to correct.

Connect to Private Resources

To connect to private resources that are in your virtual cloud network (VCN), use a private endpoint.

Overview

Outbound traffic, also called egress traffic, originates in your Oracle Integration instance and goes to your organization's network or a private cloud. All outbound traffic is routed through an adapter. When you use a private endpoint, the outbound traffic is routed on a private channel that is set up within Oracle Cloud Infrastructure. The traffic never goes through the public internet.

A private endpoint doesn't secure inbound traffic, also called ingress traffic, which originates outside Oracle Integration and goes to Oracle Integration. You restrict inbound traffic using access control lists (ACLs), also known as allowlists.

You can secure the following outbound traffic using a private endpoint:

- Outbound traffic that connects to a private resource in your VCN.
- Outbound traffic that connects to a public-facing endpoint with an access control list (ACL) that accepts requests from specific IP addresses.
  In such cases, you typically create a private NAT gateway, and the ACL accepts requests only from the IP address of the NAT gateway.

> **Note:**
>
> Because network topologies can vary greatly Oracle Integration supports and documents only the first scenario. However, other scenarios, such as using a NAT gateway, are possible. Refer to Oracle Integration Blogs for additional use cases.

Another option for connecting to resources on your on-premises network is the connectivity agent. Keep reading to learn when to use each option.

Differences between private endpoints and the connectivity agent

Area	Private endpoint	Connectivity agent
Usage	• Use a private endpoint to connect to resources in a single subnet within a VCN. • The private endpoint can route traffic through a private NAT gateway, if your organization requires it. This scenario is not documented in this guide or supported by Oracle Integration. Refer to Oracle Integration Blogs for use cases such as this one.	Use the connectivity agent to connect to resources on your on-premises network.
Security	Oracle Integration routes traffic and packages through the private endpoint. All traffic stays on your private network without going over the public internet.	Oracle Integration routes traffic over the public internet.
Setup and maintenance	Before you can create a private endpoint, complete the prerequisite tasks. These tasks can take some time and require your organization's networking team. However, most of this work might already be complete. For example, if you have resources in your private Oracle Cloud Infrastructure tenancy, you already have a VCN and subnet, which are required. After completing all prerequisite tasks, configure the private endpoint. Configure only one private endpoint per Oracle Integration instance.	Setup of the connectivity agent is fast. Create a virtual machine (VM) on your private network to host the connectivity agent, and then install the connectivity agent on the VM. The connectivity agent requires ongoing maintenance and management. For example, you must manage the VM and the upgrade cycles of the connectivity agent. See About the Connectivity Agent in *Using Integrations in Oracle Integration 3*.
Adapter support	All outbound traffic from Oracle Integration goes through a connection that is based on an adapter. Therefore, while you create a private endpoint for an instance, securing outbound traffic with the private endpoint is available on an adapter-by-adapter basis. See Adapters that Support Connecting to Private Endpoints in *Using Integrations in Oracle Integration 3*.	Similarly, outbound traffic for the connectivity agent goes through a connection that is based on an adapter. The connectivity agent works with a number of adapters. See About the Connectivity Agent

How to use the private endpoint in a connection

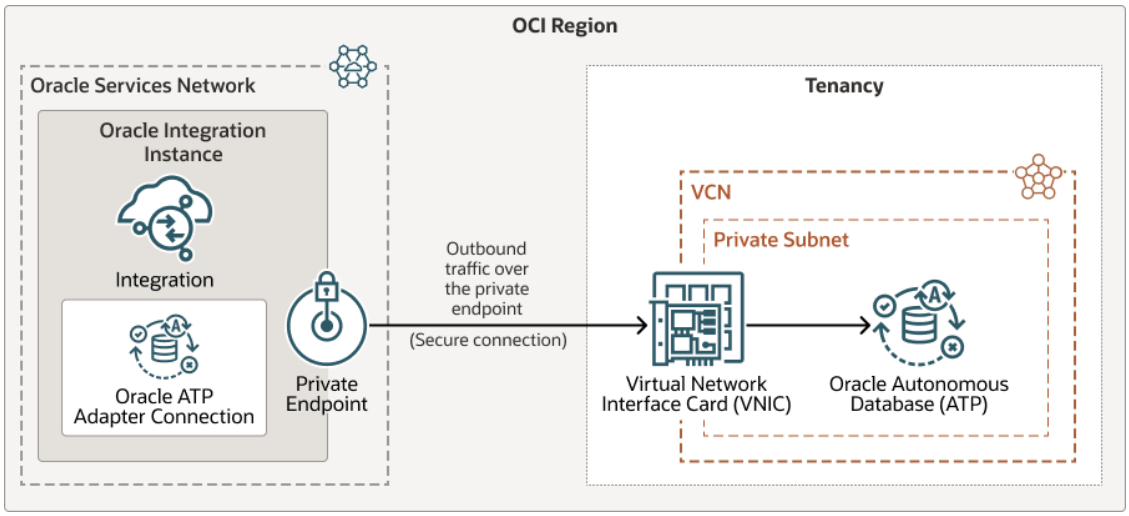
To use the private endpoint to connect to a private resource, all you need to do is select the **Private endpoint** option in the **Access type** section of the Connections page when you create the connection.

Within an integration, use different connection types as needed. For example, one connection can use the connectivity agent for a resource that's on your on-premises network, while another connection can use a private endpoint for a resource that's in your VCN.

See Create a Connection in *Using Integrations in Oracle Integration 3*.

Architecture diagram of private endpoints

The following diagram illustrates how you can connect to private resources using a private endpoint.



Prerequisites for Configuring a Private Endpoint

Complete all required tasks before configuring and using a private endpoint. If an error prevents you from creating a private endpoint, you might not have completed all prerequisites.

1. Create a VCN and subnet

Perform this task only one time per Oracle Integration instance.

A virtual cloud network (VCN) is a customizable, private network that you set up in Oracle Cloud Infrastructure. A subnet is a subdivision of a VCN. You place private resources, such as an Oracle database in your private network, in a subnet. Your integrations can access the private resources in the subnet using the private endpoint.

You might already have a VCN and subnet. For example, if you have Oracle Cloud Infrastructure resources that aren't on the public internet, you've already created a VCN and subnet to hold these resources. Examples of private resources include an instance of an Oracle Autonomous Database (ATP), a virtual machine that you set up as a private SFTP server, and a web server that you use to host private custom REST endpoints.

Requirements

- The VCN must be in the same region as your Oracle Integration instance.
- The VCN and subnet can be in any compartment and can be in either the same or different compartments.
- The subnet can be public or private.

Instructions

See Overview of VCNs and Subnets.

Information you'll need later

Make sure you note the following information. You'll need it when you create the private endpoint.

- Name of the compartment that holds the VCN, and the compartment that holds the subnet. They might be the same compartment.
- Name of the VCN.
- Name of the subnet within the VCN that the private endpoint will allow access to. The subnet contains your private resources, such as your Oracle Autonomous Database (ATP) instance.

2. Add resources to your subnet

Place any private resources that you want integrations to access in your subnet. Examples of private resources include an instance of an Oracle Autonomous Database (ATP), a virtual machine that you set up as a private SFTP server, and a web server that you use to host private custom REST endpoints.

3. Create a policy

Perform this task only one time per Oracle Integration instance. You need only one policy per Oracle Integration instance.

To create a private endpoint, you need permission to manage resources in the compartment that holds your subnet. To get these permissions, create a policy.

The policy allows the private endpoint to create a virtual network interface card (VNIC) in the compartment that contains the subnet. The private endpoint uses the VNIC to access the private resources in the subnet. To learn more about VNICs, see Virtual Network Interface Cards (VNICs).

Requirements

Use the following syntax:

```
allow group group_name to manage virtual-network-family in compartment
compartment-name
```

where:

- *group_name* is the user group that is allowed to create the private endpoint. Make sure that the person who will create the private endpoint belongs to the group.
- *compartment-name* is the name of the compartment that contains the subnet with the private resources. When you created the VCN and subnet, the compartment that contains your Oracle Integration instance was selected by default. However, you might have chosen different compartments.

Instructions

To create a policy, see the following:

- If your tenancy uses identity domains, see Create an IAM Policy in an Identity Domain.
- If your tenancy does not use identity domains, see Create an IAM Policy.

Configure a Private Endpoint for an Instance

A private endpoint lets your integrations connect to private resources in your virtual cloud network (VCN). All traffic goes through a private channel that is set up within Oracle Cloud Infrastructure. You can configure one private endpoint per instance.

Do you need a private endpoint?

To learn more about private endpoints, see Connect to Private Resources.

Prerequisites

Complete all prerequisites before configuring a private endpoint. Here is an overview of the prerequisites:

1. If you don't already have a VCN and subnet for your Oracle Integration instance, create them.
   - The VCN must be in the same region as your Oracle Integration instance.
   - The VCN and subnet can be in any compartment and can be in either the same or different compartments.
   - The subnet can be public or private.
2. Place any private resources that you want integrations to access in your subnet.
3. Create a policy that allows the private endpoint to create a virtual network interface card (VNIC) in the compartment that contains the subnet.

> **Note:**
>
> If you don't complete the prerequisite tasks, the endpoint can't be created.

To configure a private endpoint:

1. Open the Oracle Cloud Infrastructure Console.
2. Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Integration**.
3. Select an instance.
4. In the left menu, below Resources, click **Private endpoint**.
5. Below the Private endpoints heading, click **Create private endpoint**.
6. In the Create private endpoint panel, fill in the fields:
   - **Virtual cloud network in *compartment_name***: Select the virtual cloud network (VCN) that contains the subnet that contains the private resources. In the drop-down, each VCN includes its DNS domain name in parentheses.
   - **Subnet in *compartment_name***: Select the subnet that contains the private resources. The private endpoint connects to this subnet. In the drop-down, each subnet includes its DNS domain name and classless inter-domain routing (CIDR) block in parentheses.

   If the VCN or subnet is in a different compartment than the compartment that appears, click **Change Compartment**, and select the appropriate compartment.
7. Click **Create private endpoint**.

The private endpoint appears below the Private endpoint heading, but it isn't available for use yet. The entry is removed from the table if the private endpoint can't be created.

8. Monitor the work request until the private endpoint is completed.
   a. In the left menu, below Resources, click **Work requests**.
   b. Find the work request in the table.
   c. Periodically refresh the page, and wait until the **Status** for the work request changes to **Succeeded** and the **% Complete** value is **100**.
   d. To view details about a work request, click value in the **Operation** column.

      The Log messages page appears with details about the work request.

> **Note:**
>
> If the work request doesn't succeed, your policy might not be set correctly, or you might not have completed another prerequisite task. See Troubleshoot Private Endpoints.

About five minutes after you clicked **Create private endpoint**, the work request finishes processing, and the private endpoint is available to use.

After the private endpoint is created, you can begin creating connections that use the private endpoint to secure outbound traffic. See Create a Connection in *Using Integrations in Oracle Integration 3*.
You can't modify the private endpoint. If you need to make changes, simply delete the endpoint and create it again. See Delete a Private Endpoint.

Delete a Private Endpoint

When you delete a private endpoint, the outbound connection for an instance is deleted. You typically delete a private endpoint only if you made a mistake while creating it.

If a newly created private endpoint points to an incorrect VCN, subnet, or compartment, you must delete the private endpoint and create a new one. You cannot edit an existing private endpoint. When you delete a private endpoint, the Oracle Integration instance is not deleted.

If a connection uses a private endpoint, you can still delete the private endpoint. However, before deleting, deactivate any polling integrations that use private-endpoint–enabled connections. Otherwise, any invokes that use the connection in an integration will fail.

1. Open the Oracle Cloud Infrastructure Console.
2. Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Integration**.
3. Select an instance.
4. In the left menu, below Resources, click **Private endpoint**.
5. Below the Private endpoint heading, in the row for the private endpoint, click **Actions** ⋮, and select **Delete**.

   A work request is created for the task. View it on the Work Requests page. To check the status of the task, refresh the Work Requests page.

About a minute after you clicked **Delete**, the private endpoint is deleted.

If needed, you can now create a new private endpoint. See Configure a Private Endpoint for an Instance.

Troubleshoot Private Endpoints

Get help troubleshooting issues with private endpoints.

Error When Creating a Private Endpoint

The error message that appears on the Log messages page helps you troubleshoot. Which error message did you see?

> **Tip:**
>
> You can open the Log messages page from the Private endpoints page. In the left menu, below Resources, click **Work requests**. Then, in the table of work requests, find the work request for the private endpoint, and click the value in the **Operation** column.

Error	Reason for the error and next steps
`Unable to add or enable Private Endpoint Outbound Connection for the integration instance. This error can occur, if the customer tenancy is not configured with the required policy to enable the Private Endpoint. Update or add the policy, and retry.`	The error occurs when the policy is missing or incorrect, or you're not part of the group that is assigned to the policy. Check your policy, and make sure you're part of the group that is allowed to create private endpoints. See Prerequisites for Configuring a Private Endpoint.
`Unable to add Private Endpoint. The option to add a Private Endpoint for the integration instance is not supported.`	The error occurs when your region doesn't support private endpoints. If this message appears, you can't create or use private endpoints.
`Unable to add Private Endpoint outbound Connection for the Integration instance. This error can occur when all available IP addresses of the Subnet has already been allocated; ensure there are sufficient unassigned IP addresses available in the Subnetld` *`subnet_id`*`.`	The error occurs when all the subnet's available IP addresses have already been allocated. Increase the CIDR limit for the subnet.

Unable to Edit a Private Endpoint

You cannot edit an existing private endpoint. However, you can delete the endpoint and create another one.

See Delete a Private Endpoint.

Error When Testing a Connection

The error message that pops up after you test the connection helps you troubleshoot. Which error message did you see?

Error	Reason for the error and next steps
`Unable to fetch the value of dnsProxyIp , make sure the endpoint is connecting to a valid private endpoint`	The error occurs when the private endpoint hasn't been created yet, or when the private endpoint has been deleted. See Configure a Private Endpoint for an Instance.
`CASDK-003: Unable to parse the resource, connection_url. Verify that URL is reachable, can be parsed and credentials if required are accurate.`	The error occurs when you select **Public gateway** as the **Access type** when creating the connection. Select **Private endpoint** instead.
`{"detail":"","status":"HTTP 500 Internal Server Error","Operation (testConnection) failed: Error while performing AddressTranslation for private endpoint. Please check if the connection url is valid","type":"https://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html#sec10.5.1")`	This error can occur for the following reasons: • When you try to connect to a resource that's in a different VCN than the private endpoint connects to. A private endpoint can connect to a single subnet in a single VCN. Ensure that all private resources are in the subnet that the private endpoint connects to. • When you provide a host IP address on the Connections page. To connect through a private endpoint, you should always provide the host FQDN and not the IP address. • When the private endpoint is configured in a subnet of a VCN and the endpoint (database/REST service) exists in another subnet whose security list is not open to the private endpoint subnet for access, even though both are on the same VCN. See Security Lists. Open the ingress of the endpoint subnet CIDR to let the private endpoint subnet access the endpoint. Also, the egress of the private endpoint subnet should allow access to the endpoint CIDR. Ensure the network is open between the two subnets. • Your DNS zone is unable to resolve the Autonomous Transaction Processing custom host name. To resolve this issue, update your DNS zone and add an entry that maps the Autonomous Transaction Processing FQDN to the Autonomous Transaction Processing private IP.

Runtime Errors

Error	Reason for the error and next steps
`Error while performing AddressTranslation for private endpoint, Please check if the connection url is valid;`	The error occurs when the private endpoint hasn't been created yet, or when the private endpoint has been deleted. See Configure a Private Endpoint for an Instance.

Configure a Custom Endpoint for an Instance

Configure a custom endpoint to access your Oracle Integration instance with your own hostname (for example, `mycustom.example.org`), instead of the original instance URL generated in the Oracle Cloud Infrastructure Console.

Runtime access to your integrations will use the custom endpoint with no redirection. For all other access points—design-time, Visual Builder, Process Automation—you still access the custom endpoint, but the custom endpoint then redirects to the appropriate URL.

> **Note:**
>
> Associating a custom endpoint with your Oracle Integration instance doesn't affect the original instance URL. You can access your instance using the custom endpoint URL or the original instance URL.

To configure a custom endpoint, complete the following prerequisites:

- Choose a custom hostname for your instance.
- Register the hostname with either the Oracle Cloud Infrastructure DNS or your DNS provider.
- Obtain an SSL certificate from a certificate authority (CA) for your hostname. If you use a hostname certificate whose CA isn't in the Oracle Integration trust store, you must also upload the certificate to your Oracle Integration instance; otherwise, an exception is thrown in the scenarios the instance calls itself.
- Front-end your instance with a service such as OCI WAF Edge to validate and terminate SSL for your custom hostname. See Set Up a WAF Policy.

  > **Note:**
  >
  > API Gateway doesn't redirect access points such as design-time, Visual Builder, and Process Automation. If you use API Gateway for your instance, you'll need to access these resources using the original URLs.

- You must have previously created the instance. You add a custom endpoint when *editing* an instance, not during creation.
- You must have direct access to your Oracle Integration instance.

Perform the following steps to configure a custom endpoint:

1. If you're not already on the **Integration instances** page, open it.
   a. Open the Oracle Cloud Infrastructure Console.
   b. Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Integration**.
2. Open your instance.
3. Click **Edit**.
4. Click **Show advanced options**.
5. Enter your custom hostname for the instance.

6. Click **Save changes**.

Conditional Post-Configuration Tasks:

- If you're using three-legged OAuth with third-party identity providers (such as Google, Facebook, etc.), update the redirect URL in your identity provider (IdP) application with the custom hostname. If the custom hostname for your Oracle Integration instance is `mycustom.example.org`, your redirect URL must be, for example, `https://mycustom.example.org/icsapis/agent/oauth/callback`.
  After updating the redirect URL in the IdP application, you must reacquire the access token by providing consent on the connection page.
- If you created integration flows prior to mapping a custom endpoint to your instance, you must deactivate and re-activate those integrations to regenerate the WSDLs.

> **Note:**
>
> If you're using the Oracle NetSuite Adapter, the adapter's TBA Authorization Flow security policy won't work with custom endpoints for Oracle Integration.

Set Up a WAF Policy

To use a custom endpoint for Oracle Integration, you must front-end your instance with a service such as OCI WAF Edge to validate and terminate SSL for your custom hostname.

To understand WAF edge policy configuration, see Getting Started with Edge Policies.

> **Note:**
>
> Using a WAF Edge policy may cause conflicts with access control lists (ACLs). For example, if your WAF provides various source IPs, it may block legitimate requests coming from applications whose IPs are not included in the ACL for Oracle Integration.

Before you set up a WAF policy, you must:

- Choose a custom hostname for your instance.
- Register the hostname with either the Oracle Cloud Infrastructure DNS or your DNS provider.
- Obtain an SSL certificate from a certificate authority (CA) for your hostname. If you use a hostname certificate whose CA isn't in the Oracle Integration trust store, you must also upload the certificate to your Oracle Integration instance; otherwise, an exception is thrown in the scenarios the instance calls itself.

1. Create a WAF edge policy, configuring the following settings:
   - **Primary domain**: Enter the custom hostname for your instance.
   - **Origin name**: Enter a unique name for your Oracle Integration instance origin.
   - **URI**: Enter the original Oracle Integration URL.
   - (In the advanced origin options) **Header name**: Enter `Host`.
   - **Header value**: Enter your original Oracle Integration URL.

2. After the policy becomes active (within 15 minutes of creation), enable HTTPS support and upload your SSL certificate, starting with step 5 (showing the WAF settings). Configure the following settings:
   - **Enable HTTPS support**: Enable this option.
   - Select or upload your SSL certificate.

   Do not select the following options:
   - **Self signed certificate**
   - **HTTP to HTTPS redirect**
   - **Enable SNI**
   - Any advanced options

Restrict Access to an Instance

Restrict the networks that have access to your Oracle Integration instance, including File Server, by configuring an allowlist (formerly a whitelist). Only users from the specific IP addresses, Classless Inter-Domain Routing (CIDR) blocks, and virtual cloud networks that you specify can access the Oracle Integration instance and File Server.

For the Oracle Integration instance, configure the allowlist when you create the instance or after creating the instance. For File Server, configure the allowlist when you enable File Server or at any time afterward.

Topics:

Restrict Access Using the Self-Service Allowlist Capabilities

You can restrict access to Oracle Integration and File Server using an allowlist.

Overview

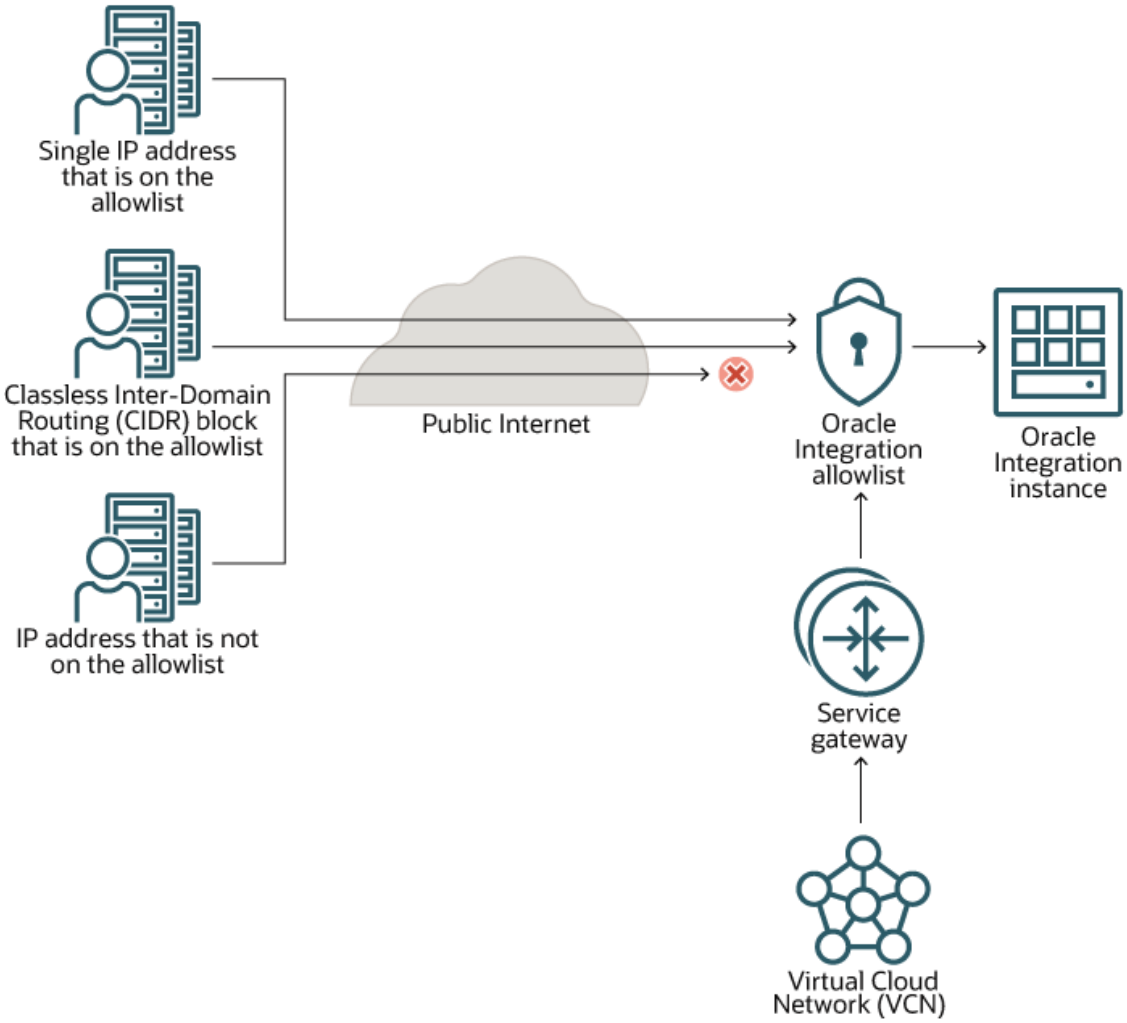
The allowlist restricts access based on the following parameters:

- Single IP address
- Classless Inter-Domain Routing (CIDR) block (that is, an IP address range)
- Virtual Cloud Network Oracle Cloud ID (VCN OCID)

Additionally, your organization might have a service gateway. The service gateway lets your virtual cloud network (VCN) privately access Oracle Integration without exposing the data to the public internet.

Only the specified IP addresses and VCN OCIDs can access Oracle Integration and File Server. Users and systems accessing Oracle Integration and File Server from listed VCNs have full access.

Diagram



Advantages

- Easy setup! You can configure your allowlist in just a few minutes, without having to create a custom endpoint.
- All traffic is supported, including REST, SOAP, and other internet traffic.

Disadvantages

- The rules allow for all-or-nothing access and don't allow for more nuanced control.
  For instance, all traffic for a particular IP address or range is allowed, even if someone using an allowed IP address passes SQL as a command line parameter.
- You're limited to 15 access rules.
  However, a CIDR block counts as only 1 entry, so you might not need more than 15 rules.

Tasks to Complete for this Scenario

1. Add your organization's VCN OCID to the allowlist. The VCN must be in the same region as Oracle Integration and should have a service gateway.
   When you add the VCN OCID to the allowlist, all resources on the VCN can access Oracle Integration.

2. For all partner networks and applications, add their IP addresses or address ranges to the allowlist.
   You need all the IP addresses for all applications and systems that require access to Oracle Integration and File Server. Make sure you consider all partner systems and SaaS applications when compiling the list. For example, if a CRM platform requires access, you must add the individual or range of IP addresses for the platform.

   When you add the IP addresses or address ranges to the allowlist, you grant full access to the user interface and integrations for your network.
3. Enable loopback so that Oracle Integration and File Server can call themselves.
   For example, enabling loopback allows Oracle Integration to call its own REST APIs.

REST API for Allowlisting

You can also use the REST API for creating and modifying allowlists.

See /integrationInstances/{integrationInstanceId}/actions/changeNetworkEndpoint.

Prerequisites for Configuring an Allowlist

When creating your allowlist, you must include all applications that require access to your instance.

> **Note:**
>
> These tasks are required for Oracle Integration and aren't relevant for File Server.

1. Get the Outbound IP Addresses for Applications That Are Event Sources

You must add all event sources, such as Oracle Fusion Applications ERP events, to the allowlist. To do so, you must get the outbound IP address of the applications. Contact the application providers to get the IP addresses.

2. Get the Public IP Addresses for Oracle SaaS Applications That Make HTTPS Calls to Oracle Integration

Oracle SaaS applications can make HTTPS calls to Oracle Integration depending on the design of the integration. Go to the **About** menu in Oracle Integration to get the public IP address of your SaaS instance to add to the allowlist in Oracle Integration. See Obtain the Inbound and Outbound IP Addresses of the Oracle Integration Instance.

Some examples:

- Integrations using SaaS adapter connections for trigger and callbacks
- When the connectivity agent is used with an adapter that does polling, such as for database polling and invoking
- When the connectivity agent is used to communicate with Oracle Integration

For a list of external IP addresses by data center that you can add to your allowlist for web service calls initiated by Oracle Cloud Applications, see the support note ID 1903739.1: IP Whitelist for Web Service Calls Initiated by Oracle Cloud Applications .

Configure an Allowlist for Your Instance

Your allowlist can contain up to 15 rules for File Server and up to 15 rules for HTTPS connections to the Oracle Integration instance. The allowlist restrictions that you create are in addition to the standard authorization mechanisms, such as user credentials, which are always in place.

1. Sign in to the Oracle Cloud Infrastructure Console.
2. Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Integration**.
3. In the **Name** column, click the instance to edit.
4. On the Integration Instance Details page, below Resources in the lower left, select **Network Access**.
5. Below the Network Access header, click **Edit**.

   One of the following dialogs is displayed:

   - If your organization has enabled File Server but hasn't created its allowlist yet, the Apply HTTP Settings to File Server dialog is displayed.
   - Otherwise, the Network Access dialog is displayed.
6. If the Apply HTTP Settings to File Server dialog is displayed, decide whether to apply your organization's HTTP allowlist rules to File Server. Applying your HTTP rules to File Server can save you some time when setting up your allowlist for File Server. Click **Apply** to carry the rules over to File Server, or click **Ignore** to skip this step.

   The Network Access dialog is displayed. If your list is empty, the first blank allowlist rule is added for you.
7. Complete the fields at the top of the dialog:

   - **Restrict Network Access**: Select this option to be able to add allow list rules and to apply the rules. When this option is selected, only users from networks that meet the configured settings are allowed to access the integration instance. When this option is not selected, there are no allowlist rules and there are no network restrictions to access your instance.

     > **Caution:**
     >
     > If you deselect **Restrict Network Access** after configuring allowlist rules, all configured allowlist rules are deleted.

   - **Enable Loopback**: Select this option to allow the integration to call itself.

     > **Note:**
     >
     > If you enable loopback, any Oracle Integrationinstance in your region can call your instance.

     Loopback is required for certain calls. You must enable loopback for the following scenarios:

  - To invoke an Oracle Integration API from within an integration. Use a REST connection to call the API.
  - To call your integration from *another* Oracle Integration instance.

  To call your integration from within your Oracle Integration instance, you can enable loopback, but we recommend using the local invoke instead. If you use the local invoke for this scenario, you don't need to enable loopback. You also don't need a connection when using the local invoke. This setting doesn't apply to File Server.

8. Configure your allowlist rules.
   a. To add a rule, click **Add Rule**, located below the last rule in the list. You might need to scroll down to see the button.
   b. In the **Protocol** field, select an option.
      - **HTTP**: The rule applies to Oracle Integration.
      - **File Server**: The rule applies to File Server.
      - **HTTP and File Server**: The rule applies to Oracle Integration and File Server.
   c. In the **Type** field, select the type of rule to configure.
      - **IP Address/CIDR Block**: Configure access from an IP address or an IP address range.
      - **Virtual Cloud Network**: Configure access from a specific virtual cloud network. To display a list of networks in other compartments, click **Change Compartment**. In addition to a specific virtual cloud network, you can specify an IP address or IP address range within the virtual cloud network.
      - **Virtual Cloud Network OCID** (Not available for File Server allowlists): Provide access to an Oracle Cloud ID (OCID) of the virtual cloud network. For information about the OCID format see Resource Identifiers.
9. After adding all the desired rules to the allowlist, click **Save Changes**.

   The work request is submitted and the changes go into effect when the instance status changes to **Active**. In the instance details, under **Integration Instance Information**, you'll also notice **Network Access: Restricted**.

Configure Email Authentication Settings for SPF and DKIM

Configure email authentication settings for SPF and DKIM for integrations. Apply these settings to your domain, then verify their configuration.

A simple yet effective way to validate emails, avoid spoofing, and reduce fraud attacks is configuring SPF and DKIM. Depending on email infra security, you may need to configure SPF and DKIM.

- Sender Policy Framework (SPF) lets domain owners identify servers they have approved to send emails on behalf of their domain. In Oracle Integration's case, domain owners need to approve OCI as an approve sender and to add a record for it in their domain.
- DomainKeys Identified Mail (DKIM) authenticates emails through a pair of cryptographic keys: a public key published in a Domain Name System TXT record, and a private key encrypted in a signature affixed to outgoing messages. The keys are generated by the email service provider.

Follow these steps to configure settings for SPF and DKIM. Also see An Advanced Guide to OIC Notification via Emails.

1. Configure **SPF (Sender Policy Framework)**.

   Add an SPF record to the domain of the `from` address to include the Oracle Cloud Infrastructure email delivery domain.

   Use the format below for the SPF record. The SPF record must identify the continent key of the Oracle Integration instance, as shown in the examples below.

   ```
   v=spf1 include:<continentkey>.oracleemaildelivery.com ~all
   ```

Sending Region	Example SPF Format
America	`v=spf1 include:rp.oracleemaildelivery.com ~all`
Asia/Pacific	`v=spf1 include:ap.rp.oracleemaildelivery.com ~all`
Europe	`v=spf1 include:eu.rp.oracleemaildelivery.com ~all`
All Commercial Regions	`v=spf1 include:rp.oracleemaildelivery.com include:ap.rp.oracleemaildelivery.com include:eu.rp.oracleemaildelivery.com ~all`

   In earlier Oracle Integration instances, sender verification was supported by adding the standard record `include:spf_c.oraclecloud.com` to the domain of the `from` address.

2. Configure **DKIM (DomainKeys Identified Mail)**.

   To configure DKIM keys for Oracle Integration 3 instances, please log a Service Request in My Oracle Support. Include the following details:

   - selector name
   - key size
   - `from` address that will be used to send emails

   Oracle provides you with the details to add the CNAME DNS record for your domain. The instructions to add the DNS record depend on your domain provider. The CNAME contains the location of the public key.

   For example, for a selector name of `me-yyz-20200502`, a sending domain of `mail.example.com`, and an email region code of `yyz`, the CNAME looks like this:

   ```
   me-yyz-20200502._domainkey.mail.example.com IN CNAME me-
   yyz-20200502.mail.example.com.dkim.yyz1.oracleemaildelivery.com
   ```

   Once the DNS is updated, update the service request, and Oracle will activate the DKIM settings for your domain.

3. In Oracle Integration, configure approved senders and confirm SPF and DKIM configuration.

   a. In the navigation pane, click **Settings**, then **Notifications**. The Notifications screen is displayed.

   b. In the **Senders** section, click **Add Email Address** to add approved senders, and complete the following fields.

Field	Description
Email Address	Enter your domain email address as the **from** address. You must set SPF and DKIM if using your own domain email address.

Field	Description
Approval Status	Either Approved or Not Approved, indicating email address approval. Email address approval is based on your version of Oracle Integration. In Oracle Integration, a verification email is sent. You must click the verification link you receive in the email. Upon successful verification, status is changed to Approved. In Oracle Integration 3, the email is automatically approved when you add the email ID.
SPF Status	This field verifies configuration for the Sender Policy Framework (SPF) for the sender email addresses. The status should be *Configured*.
Confirm DKIM	Check this field to confirm DKIM configuration for the sender.

c. Click **Save**.

For information about email notifications in integrations, see Sending Service Failure Alerts, System Status Reports, and Integration Error Reports by Notification Emails in *Using Integrations in Oracle Integration 3*. Also see Send Notification Emails During Stages of the Integration with a Notification Action in *Using Integrations in Oracle Integration 3*.

Troubleshoot Oracle Cloud Infrastructure Notification Email Configuration to Ensure Proper Delivery

Follow these recommendations to correctly configure and use the default `from` address and suppression list. These recommendations help you to avoid email delivery issues.

Default From Address

- Don't use `no-reply@oracle.com` as the `from` address.
- Don't use the `oracle` domain.
- Change the default `from` address from `no-reply@oracle.com` to `no-reply@mail.integration.`*`region`*`.ocp.oraclecloud.com`.
  The `region` attribute is provided by Oracle Integration.
- Change the `from` address in your integrations from `no-reply@oracle.com` to `no-reply@mail.integration.`*`region`*`.ocp.oraclecloud.com`.
  The `region` attribute is provided by Oracle Integration.

Suppression List

- Add `To` addresses to the suppression list for a number of reasons:
  - As of now, the `recipient` address when a hard bounce occurs (emails go undelivered for permanent reasons), when a soft bounce occurs (emails go undelivered for temporary reasons), and when a large number of emails are received are some of the reasons to add the `To` address to the suppression list.
- If DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) are not configured for the `from` address domain, the likelihood of having a bounce or messages being silently dropped by the receiving infrastructure is higher.
- You can remove email addresses from the suppression list. See Remove Email Addresses from the Suppression List in *Using Integrations in Oracle Integration 3*.

Capture the Activity Stream of Integrations in the Oracle Cloud Infrastructure Console

Use the public logging service capabilities of Oracle Cloud Infrastructure to collect and manage the activity stream of integrations.

The Oracle Cloud Infrastructure logging service provides a highly scalable and fully managed logging environment. See Logging Overview.

When you enable logging, Oracle Integration creates the `servicelogs-<>.log` file and pushes it to Oracle Cloud Infrastructure for analysis. See Service Logs and Service Logs for Oracle Integration 3.

By default, the Oracle Cloud Infrastructure Console saves thirty days of activity stream customer-facing logs, though you can store up to six months of data. Need to store data for longer periods of time? You have additional options. For example, use a service connector hub to send the log to your object storage or to a location outside of Oracle Cloud Infrastructure. You can also disable logging, as necessary.

Data in the logs is also available in the activity stream in Oracle Integration. See View the Dashboard in *Using Integrations in Oracle Integration 3*.

To create a log group and enable the log:

> **Note:**
>
> You have another option for creating a log group and enabling the log. In the Oracle Cloud Infrastructure Console, open the Oracle Integration instance details. In the left menu, below **Resources**, click **Log**. Next, in the table, enable the **Enable Log** toggle, and complete the fields in the dialog box.

1. Open the navigation menu and click **Observability & Management**. Under **Logging**, click **Logs**.

   The Logs page is displayed.
2. In the left menu, under **Logging**, click **Log Groups**.
3. In the left menu, below **List Scope**, select a compartment from the **Compartment** list.
4. Click **Create Log Group**.
5. Enter a log group name, optional description, and tag. Click **Create**.
6. In the left menu, under **Logging**, click **Logs**.
7. Click **Enable service log**.

   The Enable Resource Log dialog is displayed.
8. Enter the following details.

Field	Description
Resource Compartment	Select a resource compartment if you want to change the one you previously selected.

Field	Description
Service	Select **Integration** (the identifier for Oracle Integration).
Resource	Select the Oracle Integration instance.
Log Category	Select **Activity Stream**.
Log Name	Enter a log name.

9. Click **Enable Log**.

   The details page for the log is displayed. The **Status** field indicates that the log creation is in progress. Once log creation is complete and activated, you can perform tasks such as disabling the log (it is automatically enabled), editing the log name, changing the log group, adding tags, and deleting the log.
   You can also and take actions on your logs by creating rules to export your contents.

10. In the **Explore Log** section, sort and filter logs by the time.

11. Click **Explore with Log Search** to perform specific searches and analyze logs. See Searching Logs.

Preserve Your Instance Data

You can preserve your Oracle Integration instance data.

If you want to preserve individual integrations, there are several methods. Once exported, you can store the integrations in your own source control repository or preserve them using whatever method you want.

- Group your integrations into a package. When you import or export the package to or from Oracle Integration, all integrations in that package are imported or exported. See Manage Packages in *Using Integrations in Oracle Integration 3*.
- Available APIs:
  - Packages REST Endpoints
  - Integrations REST Endpoints (to import and export individual integrations)

See Oracle and Customer Responsibilities in Oracle Integration 3.

Monitor Oracle Integration 3 Instances

Monitor your Oracle Integration instance and its features.

For additional monitoring information, see:

- Monitor Integrations During Runtime in *Using Integrations in Oracle Integration 3*

Topics:

- About Integrations Usage
- View Message Metrics and Billable Messages
- Calculate Requests Per Second

About Integrations Usage

When creating Oracle Integration instances, administrators specify the number of message packs they plan to use for per instance.

Rules for tracking Integration billed messages

Follow these rules to determine how message consumption is calculated.

Number	Rule	Description
1	Trigger	Each trigger activity counts as at least one message, up to 50KB inbound. If the inbound message payload exceeds 50KB, 1 additional message is counted for each additional 50KB.
2	Invoke	Invoke requests don't count as messages, but invoke responses over 50KB count. If the message payload exceeds 50KB, 1 additional message is counted for each additional 50KB.
3	File	For file based scheduled flows where there are incoming files into integrations, each file is converted into a billed message (in multiples of 50KB) only when the size is greater than 50KB.
4	Internal	Internal calls within the same Oracle Integration instance aren't counted as messages. For example, the following aren't counted: • Process Automation to Integration • Visual Builder to Integration • Integration to Integration Calling another Oracle Integration instance does incur messages in the target Oracle Integration instance, and, depending on the response size, may also incur messages in the calling Oracle Integration instance.

Integration Usage Examples

This table shows by example how message billing is calculated and the rules that apply.

Integration Type	Scenario/Flow	Billing Message Calculation	Rules That Apply
Sync/Async (Trigger)	1. REST inbound with 120KB payload. 2. Data transformation. 3. External invoke to push data to Logfire.	Payload size is considered at trigger. ceil(120/50) = 3 messages	#1 (Trigger)
Sync/Async (Trigger)	1. SOAP inbound with 70KB payload. 2. Download files in a loop. 3. 3 files downloaded of sizes 20KB, 170KB, and 40KB, respectively. 4. Data transformation/ enrichment. 5. External invoke to push data to an external system via REST.	Payload size is considered at trigger. Any subsequent response greater than 50KB is also tracked. In this scenario, only files greater than 50KB are considered. ceil(70/50) + ceil(170/50) = 2 +4 = 6 messages	#1 (Trigger) #3 (File)

Integration Type	Scenario/Flow	Billing Message Calculation	Rules That Apply
Sync/Async (Trigger)	1. Database adapter pulling in 20KB data and 2 rows. 2. For each row, 1 outbound REST invoke is made, which results in 20KB data for each invoke. 3. Data enrichment/ transformation. 4. FTP to an external location.	Payload size is considered at trigger. Any subsequent response greater than 50KB is also tracked. ceil (20/50) = 1 message	#1 (Trigger)
Sync/Async (Trigger)	1. SOAP inbound with 10KB payload. 2. Download files in a loop. Two files downloaded of sizes 20KB and 70KB, respectively. 3. External invoke to get further data via REST adapter. Returns 100KB data. 4. FTP to an external location.	Payload size is considered at trigger. Any subsequent response greater than 50KB is also tracked. ceil(10/50)+ ceil (70/50) + ceil(100/50) = 1+2+2 = 5 messages	#1 (Trigger) #2 (Invoke) #3 (File)
Sync/Async (Trigger)	1. Simple REST GET request with template parameters without payload. 2. Call to Oracle Fusion Cloud B2C Service to get contact details. Returns a response of 40KB. 3. Return the contact data.	Payload size is considered at trigger. Any subsequent response greater than 50KB is also tracked. Since the trigger is just a GET request with no payload, it's considered 1 billed message. 1 message	#1 (Trigger)
Scheduled flow	1. Scheduled trigger. 2. Download files in a loop. Three files downloaded of sizes 20KB, 170KB, and 40KB, respectively. 3. Data transformation. 4. External invoke to transfer data which results in 10 bytes of response.	Each invoke/file is considered in multiples of 50KB when response data is more than 50KB. ceil(170/50) = 4 messages	#3 (File)
Scheduled flow	1. Scheduled trigger. 2. Database adapter pulling in 30KB data and 10 rows. 3. Data transformation. 4. External invoke to transfer data which results in 5 bytes of response.	Each invoke/file is considered in multiples of 50KB when response data is more than 50KB. Not counted.	None

Integration Type	Scenario/Flow	Billing Message Calculation	Rules That Apply
Scheduled flow	1. Scheduled trigger. 2. External SOAP invoke to get data via BIP reports. Returns 130KB data. 3. External invoke to get further data via REST adapter. Returns 10KB data. 4. Data transformation. 5. External invoke to transfer data which results in 5 bytes of response.	Each invoke/file is considered in multiples of 50KB when response data is more than 50KB. ceil(130/50) = 3 messages	#3 (File)
Scheduled flow	1. Scheduled trigger. 2. Download files in a loop. Two files downloaded of sizes 20KB and 40KB, respectively. 3. External invoke to get further data via REST adapter. Returns 100KB data. 4. FTP to an external location.	Each invoke/file is considered in multiples of 50KB when response data is more than 50KB. ceil(100/50) = 2 messages	#2 (Invoke)
Scheduled flow	1. Scheduled trigger. 2. External invoke to get data via REST adapter. Returns 10KB data. 3. Data transformation. 4. External REST invoke to transfer data which results in 500 bytes of response.	Each invoke/file is considered in multiples of 50KB when response data is more than 50KB. Not counted.	#4 (Internal) None counted
Child Integration flow	1. A parent Integration flow calls a child Integration flow via REST in a loop. 2. The child Integration flow sends a notification email with the information passed from a parent flow. 3. Child flow execution completes.	Integration child flow invoke is waived from metering. Not counted. Note that the parent may count.	#4 (Internal) None counted

Integration Type	Scenario/Flow	Billing Message Calculation	Rules That Apply
Child Integration flow	1. Parent Integration flow downloads a CSV file via the FTP adapter. The CSV contains 5 rows. 2. Each row in the CSV file calls a child Integration child flow. a. The child Integration flow reads a orderid passed as an input. b. Invokes a request to Oracle Fusion Cloud B2C Service to get data about the order. Each invoke returns 70KB data. c. Data transformation in child flow. d. Pushes the data via an FTP adapter to write it to a file. e. Child execution completes.	Integration child flow invokes are waived from metering. Any subsequent response is metered. Each child = ceil(70/50) = 2 messages Note that the parent may count.	#2 (Invoke)

About Process Usage

When creating Oracle Integration instances, administrators specify the number of message packs they plan to use for per instance.

Process message metering

Process metering tracks the number of concurrent, **unique** users **interacting** within a 1 hour interval. Sizing is based on concurrent users, which are converted to message packs. One Process user/hour is equivalent to 400 messages/hour.

- If you have 1,000 messages per hour and 10 distinct users, these would count as 1,000 integration messages + (400)*10 users = 5,000, so 1 message pack of 5,000 messages per hour.
- Another way to visualize Process sizing: 5,000 message packs per hour equate to 12.5 distinct concurrent users performing tasks.

What's counted?

A logged in user is counted for a minimum of one hour when performing any write operations that update a task or process instance, which includes:

- Updating or processing tasks (approve/reject a task, add an attachment/comment, re-assign, or request for information)
- Creating process instances

Within each hour of use, a distinct user can perform an unlimited number of write operations.

Oracle Integration has a 1 message pack minimum charge per hour to keep the system available, even with no usage. Note that you can turn off your Oracle Integration instance for billing purposes, but no instances are processed while the instance is stopped.

What's NOT counted?

This count doesn't include:

- Logged in users performing read-only only (query or read) operations.
- Integrations triggered from the process (integrations are waived).

Process Usage Examples

This table shows by example how message billing is calculated and the rules that apply.

Scenario Type	Scenario	Billing Message Calculation
Process Workspace	Between 9am and 10am, 20 employees access Workspace. Within the one hour timeframe: • 5 users (user1 through user5) create a total of 100 new process instances. • 10 other users (user6 through user15) process different tasks created by user1 through user5, and complete them. • The remaining 5 users (user16 through user20) only check the task and process instance status, but do not perform any update/write operations.	The 9am-10 am hour block reports 15 concurrent users (5 created new instances and 10 processed tasks).
Process Workspace and mobile app	Between 10 and 11am, 10 users access Workspace and 5 access the Oracle Process Mobile app. Within the one hour timeframe: • 10 users (user1 through user10) create new process instances and also approve at least 1 task total. • 5 users (user11 through user15) log into the mobile app: 3 of them create new instances, and the other 2 perform only read-only operations.	The 10am-11am hour block reports 13 concurrent users (10 workspace users plus 3 mobile users performed update/write operations, while 2 mobile users did not perform any update/write operations).
Process Workspace and Visual Builder	Between 11am and 12pm, 5 users access Oracle Integration from a Visual Builder application and 5 other users access Workspace. • 2 of the 5 Visual Builder users access Visual Builder, and interact with a Visual Builder app that in turn triggers execution of an API that creates new process instances and processes tasks. • The other 3 Visual Builder users access the Visual Builder app and read and access task and process instance status. • The 5 users access Workspace and approve a minimum of 1 task each within the hour timeframe.	The 11am-12pm hour block reports 7 concurrent users (2 Visual Builder users and 5 Workspace users performed update/write operations). This result does not include the Visual Builder concurrent user licenses. Visual Builder concurrent users are metered separately.

View Message Metrics and Billable Messages

View and analyze message data, processing and invocation times, adapter requests, and configured and consumed messages on the Metrics page. Use the data to monitor resources associated with Oracle Integration and the applications that you integrate with Oracle Integration.

Monitoring helps you detect anomalies and bottlenecks occurring within the Oracle Integration instances and connected applications. Actively and passively monitor cloud resources using the metrics and alarms features of the Oracle Cloud Infrastructure Monitoring, available with Oracle Integration. See Monitoring Overview in the Oracle Cloud Infrastructure documentation.

- View the Monitoring Charts
- Modify the Charts and Create Custom Charts
- About the Charts
- Options for Configuring the Charts
- Endpoint Metrics
- How Adapters Map to Dimension Values
- Examples of Endpoint Metric Charts
- Adapters with Limited Dimensions

> **Note:**
>
> Visual Builder message consumption is not included in Oracle Integration usage metrics.

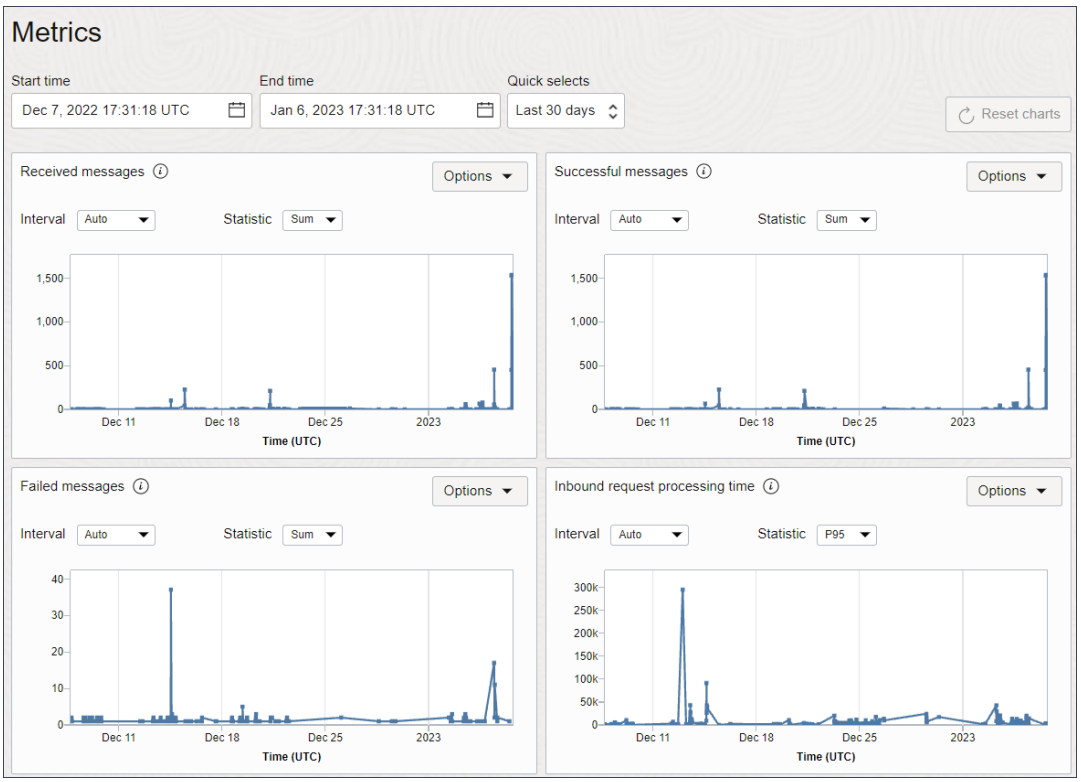
View the Monitoring Charts

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

   For example:

   - **Syntax:** `allow group` *`group_name`* `to` *`verb resource-type`* `in compartment` *`compartment-name`*
   - **Policy:** `allow group oci-integration-admins to read metrics in compartment OICPMCompartment`

   See Manage Access and Assign Roles.
2. Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Integration**.
3. Select an instance in the Oracle Cloud Infrastructure Console.
   A **Metrics** section shows graphs with default values.



Modify the Charts and Create Custom Charts

You can change the metrics that appear in each chart. Additionally, you can create custom charts to further analyze your data. For instance, imagine you created two compartments for your organization, one for your engineering team and another for your finance team. Using custom charts, you can measure the resources that each compartment has used and determine whether you purchased an appropriate number of message packs.

1. Change the message metrics displayed for each chart, if needed.
   Start Time and **End Time** are selected at the top of each chart. Change these values to select a different time period.

   Metric counts occur every five minutes.
2. To change the metrics displayed, change the **Interval** and **Statistic** fields for each chart.
3. To create custom dashboards and alerts, or to see data for all instances in a compartment: In the top right of a chart, from the **Options** drop-down list, select **View Query in Metrics Explorer**. For more information, see Viewing Default Metric Charts.

About the Charts

Chart	Description
Received messages	Shows the message requests that the instance received.
Successful messages	Shows the message requests that completed successfully.
Failed messages	Shows the message requests that did not complete successfully for the instance.
Inbound request processing time	Shows adapter inbound processing times for the instance.

Chart	Description
Outbound request invocation time	Shows adapter outbound message invocation times for the instance.
Inbound requests	Shows the number of adapter inbound requests for the instance.
Outbound requests	Shows the number of adapter outbound requests for the instance.
Consumed messages Configured messages	These two charts show the following information: • Consumed messages: Shows the messages that the instance used. • Configured messages: Show the messages that you purchased. Use this data to make informed decisions about the number of message packs to purchase for the instance. The type of license you choose determines how message packs are defined and metered. • **For Oracle Integration**: – **BYOL:** For Bring Your Own License users, one message pack is defined as 20,000 messages per hour. You can select up to 3 message packs if you bring an existing Oracle Fusion Middleware license to the cloud. – **Non-BYOL:** For these license types, one message pack is defined as 5,000 messages per hour. You can select up to 12 message packs if you create a new Oracle Integration license in the cloud. • **For Oracle Integration for SaaS**, usage is tracked on a monthly basis in packs of one million messages per month, which keeps costs predictable even when you have unpredictable hourly volumes. Usage is reported monthly instead of hourly. You can select up to 43 message packs. For details on how Integration billable messages are calculated, see About Integrations Usage.

Options for Configuring the Charts

You can configure and view metrics charts that show adapter inbound request processing times, outbound request invocation times, adapter inbound request numbers, and adapter outbound request numbers.

Endpoint metrics include the following dimensions that are available for selection in the Metrics Explorer.

> **Note:**
>
> Each endpoint metric has its own dimensions. Not all dimensions are available on all endpoint metrics.

- adapterIdentifier: Show data in the chart for a single adapter (internal name) that is used either as a trigger for receiving or as an invoke for sending the request to the external system.
- account_subscription: Show data in the chart for a specific account type, such as a universal credit model (UCM) account, an Oracle Integration for Saas account, or a government account.
- flowCode: Show data in the chart for a specific integration in Oracle Integration.

- flowVersion: Show data in the chart for a specific integration version, which you can specify at various times, including when you create or clone an integration.
- inboundProcessingEndpointInformation: Show data in the chart for a specific functional request received from the client.
- inboundProcessingResponseStatus: Show data in the chart for a specific status sent by the trigger to the external client.
- instanceName: Show data in the chart for a specific instance. This value matches the name that an administrator specified when creating the instance as well as the URL of the instance. This value is a more user-friendly value than the resourceid.
- meterType: Show data in the chart for a specific license type, such as BYOL, Cloud, or SaaS.
- outboundInvocationEndpointInformation: Show data in the chart for a specific functional request made to the external system.
- outboundInvocationResponseStatus: Show data in the chart for a specific status received from the external system.
- integrationFlowIdentifier: Show data in the chart for the integration receiving an incoming request or sending an outgoing request. The dimension includes both the identifier and the version.
- resourceid: Show data in the chart for a specific OCID of an integration instance. You can use this value to uniquely track the instance.

> **Tip:**
>
> To filter a chart by multiple metric dimensions, first select a dimension name and dimension value. Then, click **Additional dimension** and select another dimension name and value. Don't forget to click **Update Chart** after updating the query.

The metrics listed in the following tables are automatically available for selection for any instance you create.

The inboundProcessingEndpointInformation or outboundInvocationEndpointInformation dimension provides a concise summary of the adapter trigger or invoke configurations. For example, the inboundProcessingEndpointInformation dimension can look for ‘Receive Incident Created notification from ServiceNow’ for an integration that is triggered when an incident is created in the ServiceNow application. On the invoke side, the outboundInvocationEndpointInformation dimension can look for ‘Create Account in Salesforce.com’ if the invoke activity in the integration is configured to create an Account object in Salesforce.com.

The following table describes the available metrics and dimensions. The Commonly Used Statistics in Metrics Explorer column provides the following information.

- Mean: Average processing time (latency) taken for incoming requests received during the time interval and average invocation time taken by outbound requests sent during the time interval.
- Min: Minimum processing time (latency) taken for incoming requests received during the time interval and minimum invocation time taken by outbound requests sent during the time interval.

- Max: Maximum invocation time taken by outbound requests sent during the time interval and maximum processing time (latency) taken for incoming requests received during the time interval.
- P50: Maximum invocation time (latency) taken by 50% of outbound requests sent during the time interval and maximum processing time (latency) taken by 50% of incoming requests received during the time interval.
- P90: Maximum invocation time (latency) taken by 90% of outbound requests sent during the time interval and maximum processing time (latency) taken by 90% of incoming requests received during the time interval.
- P95: Maximum invocation time (latency) taken by 95% of outbound requests sent during the time interval and maximum processing time (latency) taken by 95% of incoming requests received during the time interval.
- P99: Maximum invocation time (latency) taken by 99% of outbound requests sent during the time interval and maximum processing time (latency) taken by 99% of incoming requests received during the time interval.
- Count: Total number of requests received during the time interval and total number of outbound requests made during the time interval.

Endpoint Metrics

Metric Name in Metrics Explorer	Unit	Description	Dimension Name in Metrics Explorer	Commonly Used Statistics in Metrics Explorer
ConfiguredMessages	count	Number of messages that were configured. This number determines billing.	• account_subscription • instanceName • meterType • resourceId	Max

Metric Name in Metrics Explorer	Unit	Description	Dimension Name in Metrics Explorer	Commonly Used Statistics in Metrics Explorer
InboundRequestProcessingTime	Duration in milliseconds	The time taken for processing inbound requests. In case of synchronous requests, it is the total time taken for processing a request and sending the response. In case of fire-and-forget inbound requests, it is the time taken to persist the request and send the acknowledgment. This metric captures the time elapsed (in milliseconds) by the trigger in processing the incoming request.	• adapterIdentifier • inboundProcessingEndpointInformation • inboundProcessingResponseStatus • integrationFlowIdentifier • resourceid	Mean Min Max P95 P99
MessagesFailedCount	count	Number of messages that could not be processed. For example, a message can't be processed when an external endpoint that is used in an integration goes down.	• flowCode • flowVersion • resourceId	Max
MessagesReceivedCount	count	Number of messages that were received. This count doesn't indicate whether the messages processed successfully.	• flowCode • flowVersion • resourceId	Min Max

Metric Name in Metrics Explorer	Unit	Description	Dimension Name in Metrics Explorer	Commonly Used Statistics in Metrics Explorer
MessagesSuccessfulCount	count	Number of messages that were processed successfully.	• flowCode • flowVersion • resourceId	Min Max
NumberofInboundRequests	count	Number of requests received by Oracle Integration using any adapter-specific trigger connection. This metric includes the HTTPs requests posted to Oracle Integration and the messages polled by adapters such as Oracle Advanced Queuing (AQ) Adapter, IBM MQ Series JMS Adapter, Apache Kafka Adapter, Oracle Database Adapter, and so on.	• adapterIdentifier • inboundProcessingEndpointInformation • inboundProcessingResponseStatus • integrationFlowIdentifier • resourceid	Count
NumberOfOutboundRequests	count	Number of outbound requests sent by the adapter as part of the invoke activity in Oracle Integration.	• adapterIdentifier • integrationFlowIdentifier • outboundProcessingEndpointInformation • outboundProcessingResponseStatus • resourceid	Count
OutboundRequestInvocationTime	Duration in milliseconds	Time (in milliseconds) spent by the adapter during the invocation of the target endpoint.	• adapterIdentifier • integrationFlowIdentifier • outboundProcessingEndpointInformation • outboundProcessingResponseStatus • resourceid	• Mean • Min • Max • P50 • P90 • P95 • P99

How Adapters Map to Dimension Values

The following table describes how each adapter maps to its dimension value in the Metrics Explorer.

Dimension Value in Metrics Explorer	Adapter Display Name	Inbound Processing Event Information Naming Conventions in Dimension Value Field	Outbound Invocation Endpoint Information Naming Conventions in Dimension Value Field
adobeesign	Adobe Sign Adapter	N/A	• Retrieve status of agreement from Adobe eSign • Upload a document in Adobe eSign • Retrieve IDs of agreement from Adobe eSign • Retrieve URL of the document from Adobe eSign
adwdatabase	Oracle Autonomous Data Warehouse Adapter	• New row is inserted into <table name> in Oracle ADW	• Insert rows into <table name> in Oracle ADW • Merge rows into < table name> in Oracle ADW • Update rows into <table name> in Oracle ADW
apachekafka	Apache Kafka Adapter	• Consume latest message from Topic: [TopicName=<Topic>,Partitions={<Partition>}] in Apache Kafka	• Produce message(JSON) in Topic: [TopicName=<Topic>,Partitions={<Partition>}] using Apache Kafka • Consume latest message from Topic: [TopicName=<Topic>,Partitions={<Partition>}] in Apache Kafka
aq	Oracle Advanced Queuing (AQ) Adapter	• Consume <message type> message from Queue: <queue name> in Oracle Advanced Queueing (AQ)	• Produce <message type> message in Queue: <queue name> using Oracle Advanced Queuing (AQ)

Dimension Value in Metrics Explorer	Adapter Display Name	Inbound Processing Event Information Naming Conventions in Dimension Value Field	Outbound Invocation Endpoint Information Naming Conventions in Dimension Value Field
ariba	SAP Ariba Adapter	• Receive notification from <operation name> from Ariba	• Create <business object> in SAP Ariba • Bulk upload for the task - <task name> <Data Mode: Master/ Transactional, Operation Mode: Incremental/Full> in SAP Ariba • Bulk extract for the task - <task name> <Data Mode: Master/ Transactional, Operation Mode: Incremental/Full> from SAP Ariba
as2adapter	AS2 Adapter	N/A	N/A
atpdatabase	Oracle Autonomous Transaction Processing Adapter	• New row is inserted into <table name> in Oracle ATP	• insert rows into <table name> in Oracle ATP • Merge rows into < table name> in Oracle ATP • Update rows into <table name> in Oracle ATP
bbtranslationadapter	EDI Translate Action	N/A	• B2B EDI Translation
box	Box Adapter	N/A	N/A
concur	SAP Concur Adapter	NA	• Create/Update/ Delete/Retrieve <business object> in SAP Concur. • Extracts reports of available data objects in SAP Concur. • Manage payment batches and retrieve their batch files in SAP Concur. • Get status for the Job in Concur • Download file from Concur application • Bulk data extract request for AP/GL Extract V.3.04 submitted in Concur
cpq	Oracle CPQ Adapter	N/A	N/A

Dimension Value in Metrics Explorer	Adapter Display Name	Inbound Processing Event Information Naming Conventions in Dimension Value Field	Outbound Invocation Endpoint Information Naming Conventions in Dimension Value Field
database	Oracle Database Adapter	• New row is inserted into <table name> in Oracle Database	• Insert rows into <table name> in Oracle Database • Merge rows into < table name> in Oracle Database • Update rows into <table name> in Oracle Database
dbaasdatabase	Oracle Database Cloud Service Adapter	• New row is inserted into <table name> in DBCS	• Insert rows into <table name> in DBCS • Merge rows into < table name> in DBCS • Update rows into <table name> in DBCS
db2database	IBM DB2 Adapter	• New row is inserted into <table name> in DB2	• Insert rows into <table name> in DB2 • Merge rows into < table name> in DB2 • Update rows into <table name> in DB2
docusign	DocuSign Adapter	N/A	• Create and send an envelope in DocuSign • Send an envelope created from an existing template in DocuSign • Get status changes of an envelope from DocuSign
ebay	eBay Marketplace Adapter	N/A	• Get Single Record: <Entity_NAME>s from eBay • Get List of Records: <Entity_NAME>s from eBay • Create a Record: <Entity_NAME> in eBay • Update a Record: <Entity_NAME> in eBay • Delete a Record: <Entity_NAME> from eBay

Dimension Value in Metrics Explorer	Adapter Display Name	Inbound Processing Event Information Naming Conventions in Dimension Value Field	Outbound Invocation Endpoint Information Naming Conventions in Dimension Value Field
ebusiness	Oracle E-Business Suite Adapter	N/A	N/A
eloqua	Oracle Eloqua Cloud Adapter	N/A	N/A
epm	Oracle Enterprise Performance Management Cloud Adapter	N/A	N/A
erp	Oracle ERP Cloud Adapter	• Receive notification for business event <event name> from ERP Cloud • Receive Status of ERP Import Job from ERP Cloud • Receive notification for business event OIC_MAT_349_FSCM_PARENT from ERP Cloud • Request Object Account from ERP Cloud • Request Object Item from ERP Cloud	• Get ESS Job Status in ERP Cloud • Submit Contract For Approval in ERP Cloud • Bulk Import of data into ERP Cloud using FBDI Job: <Job Name> • Upload File to UCM in ERP Cloud
eventbrite	Eventbrite Adapter	N/A	N/A
facebook	Facebook Adapter	N/A	N/A
file	File Adapter	• Read file from server • Read and delete file from server • Read file recursively in directory from server • Read file recursively in directory and delete from server	• Read file from Server • Write file <FileName>in directory <DirName> • Listing file with minimum age <N> seconds, maximum files in response <M> Recursive <True|False> • Move file with Overwrite option <True|False> • Delete file in Server • Download file in Oracle Integration from agent

Dimension Value in Metrics Explorer	Adapter Display Name	Inbound Processing Event Information Naming Conventions in Dimension Value Field	Outbound Invocation Endpoint Information Naming Conventions in Dimension Value Field
ftp	FTP Adapter	NA	• Read file from FTP Server in (binary|ASCII) format • Write(append) file to FTP Server in (binary|ASCII) format • (Encrypt|decrypt|Sign\Verify) and Write file to FTP Server • List (Recursive) files from FTP Server • Move (Overwrite) files from FTP Server • Delete file in FTP Server • Download file from FTP Server in (binary|ASCII) format • Download and (unzip|decrypt|Verify) file from FTP Server in (binary|ASCII) format
gmail	Google Gmail Adapter	N/A	• Get email attachment from Gmail • List emails from Gmail
googlecalendar	Google Calendar Adapter	N/A	N/A
googletask	Google Tasks Adapter	N/A	N/A
hcm	Oracle HCM Cloud Adapter	Receive <business object> from Client	• <verb> <business object / noun> in HCM Cloud • <verb> <rest resource> from HCM Cloud • Subscribe <atom feed> from HCM Cloud • Download bulk extract <extract name> from HCM Cloud • Upload File to UCM in HCM Cloud

Dimension Value in Metrics Explorer	Adapter Display Name	Inbound Processing Event Information Naming Conventions in Dimension Value Field	Outbound Invocation Endpoint Information Naming Conventions in Dimension Value Field
hybriscommerce	SAP Commerce Cloud (Hybris) Adapter	N/A	• Query/ Create/ Update / Delete <business object> in SAP Commerce Cloud
jdeeone	Oracle JD Edwards EnterpriseOne Adapter	N/A	• Call JD Edwards SOAP Service <SOAP Service> : <Operation>
jms	Oracle WebLogic JMS Adapter	• Consume message from Queue: <queue name> in Oracle Weblogic JMS • Consume message from Topic: <topic name> in Oracle Weblogic JMS	• Produce message in Queue: <queue name> using Oracle Weblogic JMS • Produce message in Topic: <topic name> using Oracle Weblogic JMS
linkedin	LinkedIn Adapter	N/A	N/A
mailchimp	Mailchimp Adapter	N/A	N/A
Marketo	Marketo Adapter	N/A	• Create Or Update Lead in Marketo • Import Lead in Marketo
microsoftcalendar	Microsoft Office 365 Calendar Adapter	N/A	N/A
microsoftcontact	Microsoft Contact Adapter	N/A	N/A
microsoftemail	Microsoft Office 365 Outlook Adapter	N/A	N/A
mqjms	IBM MQ Series JMS Adapter	• Consume message from Queue: <queue name> in MQSeries JMS	• Produce message (Persistent) in Queue: <Queue Name> using MQSeries JMS
mysqldatabase	MySQL Adapter	• New row is inserted into <table name> in MySQL DB	• Insert rows into <table name> in My SQL DB • Merge rows into < table name> in My SQL DB • Update rows into <table name> in My SQL DB

Dimension Value in Metrics Explorer	Adapter Display Name	Inbound Processing Event Information Naming Conventions in Dimension Value Field	Outbound Invocation Endpoint Information Naming Conventions in Dimension Value Field
netsuite	Oracle NetSuite Adapter	N/A	• Update Superseded Items in Netsuite • Update EBS Item Details in Netsuite • Add Invoice to Netsuite • Search <search> in Netsuite
ocistreaming	Oracle Cloud Infrastructure Streaming Service Adapter	N/A	• Message produced to: Sales-SP with Partition/s: <Partitions> of MessageType <Message Type>
ofsccloudadapter	Oracle Field Service Cloud Adapter	• Receive <event-name> notification from Oracle Field Service Cloud or • Receive <event1, event2...> notification from Oracle Field Service Cloud	• Get <resource-name> in Oracle Field Service Cloud • Get <resource-name> <sub-resource-name> in Oracle Field Service Cloud • <custom-action> <resource-name> in Oracle Field Service Cloud
oms	Oracle Messaging Cloud Service Adapter	N/A	N/A
rest	REST Adapter	• Trigger Oracle Integration REST Integration: <HTTP verb> <resource path>	• Call External REST API: <verb> <relative-path> • Call <App-name>: <verb> <relative-path> • Call Oracle Integration REST Integration: <integration flow >
rest_opa	Oracle Intelligent Advisor Adapter (formerly Oracle Policy Automation) Adapter	• Receive ${load/save} request for <interview> from Intelligent Advisor	• Send assessment request for <interview> to Intelligent Advisor.
rest_oraclecommercecloud	Oracle Commerce Cloud Adapter	N/A	N/A
responsys	Oracle Responsys Adapter	N/A	N/A

Dimension Value in Metrics Explorer	Adapter Display Name	Inbound Processing Event Information Naming Conventions in Dimension Value Field	Outbound Invocation Endpoint Information Naming Conventions in Dimension Value Field
rightnow	Oracle Service Cloud (RightNow) Adapter	• Receive <event name> Notification from Oracle Service Cloud • Receive <object name> (Oracle Service Cloud Object) from Client	• Query <object name> objects from Oracle Service Cloud • Query CSV records for <object name> from Oracle Service Cloud • Get file attachment from Oracle Service Cloud • Invoke Batch Operation in Oracle Service Cloud • Get <object name> from Oracle Service Cloud • Create <object name> in Oracle Service Cloud • Update <object name> in Oracle Service Cloud • Destroy <object name> in Oracle Service Cloud
oracleutilities	Oracle Utilities Adapter	• <Description of the business object from the service catalog> in Oracle Utilities	• <Description of the service from the service catalog> in Oracle Utilities
osc	Oracle CX Sales and B2B Service Adapter (formerly Oracle Sales Cloud) Adapter	• Request object <object name > from Engagement Cloud • Request Object Account from Engagement Cloud • Receive notification for business event FoundationParties_Person_Created from Engagement Cloud • Request Object Opportunity from Engagement Cloud	• Create Opportunity in Engagement Cloud • Create ICS Sales Custom Obj CO in Engagement Cloud
logistics	Oracle Logistics Adapter	N/A	N/A

Dimension Value in Metrics Explorer	Adapter Display Name	Inbound Processing Event Information Naming Conventions in Dimension Value Field	Outbound Invocation Endpoint Information Naming Conventions in Dimension Value Field
paypal	PayPal Adapter	• Receive <business object event> notification from PayPal	• For Query : <operation>from PayPal • For Create/Update/Delete:<operation> in PayPal
salesforce	Salesforce Adapter	• Receive <business object> notifications from Salesforce.com	• Create Account in Salesforce.com
sap	SAP Adapter	• Receive <business object> from SAP	• Invoke <business object> from SAP
saps4hana	SAP S/4HANA Cloud Adapter	N/A	• GET : Get specific item from the collection<Entity_NAME> from SAP S/4HANA • GET : GetAll entities in the collections of <Entity_NAME> from SAP S/4HANA • POST : Create new item in the collection <Entity_NAME> from SAP S/4HANA • PATCH : Update new item in the collection <Entity_NAME> from SAP S/4HANA • DELETE : Delete specific entity in the collection from SAP S/4HANA
servicenow	ServiceNow Adapter	• Receive <business object> notifications from ServiceNow	• For Query : <operation>from ServiceNow • For Create/Update/Delete:<operation> in ServiceNow • Upload Attachment to ServiceNow
shopify	Shopify Adapter	• Receive <business object event> from Shopify	• For Query : <<operationName>> from Shopify • For Create/Update/Delete:<<operation Name>> in Shopify

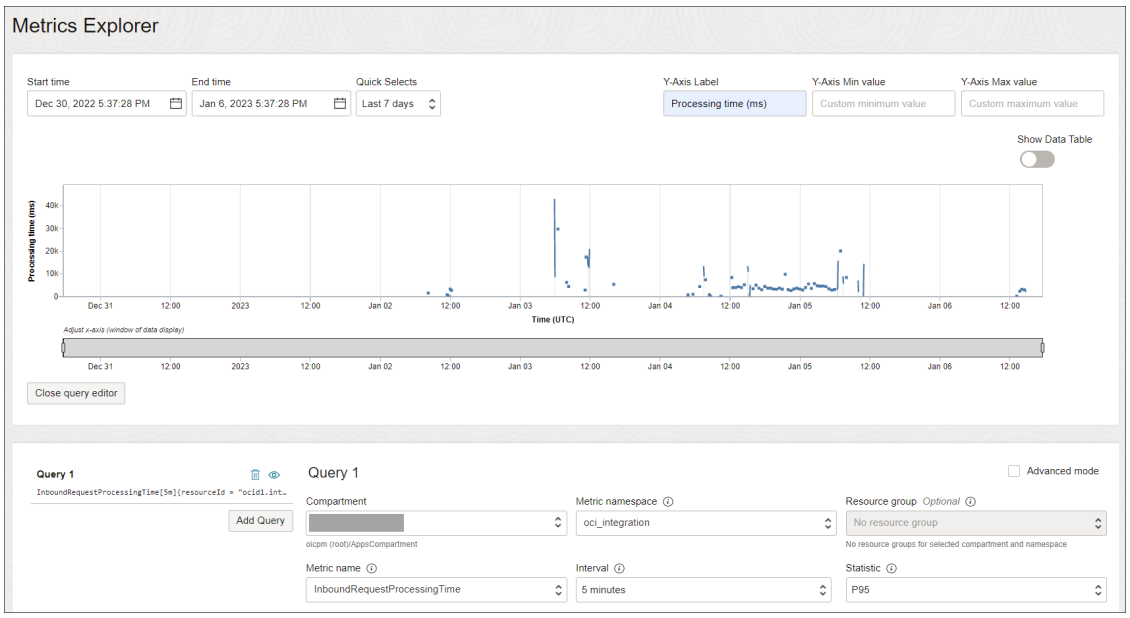
Dimension Value in Metrics Explorer	Adapter Display Name	Inbound Processing Event Information Naming Conventions in Dimension Value Field	Outbound Invocation Endpoint Information Naming Conventions in Dimension Value Field
siebel	Oracle Siebel Adapter	N/A	• Call Siebel SOAP Service OS FS Get Stock Oracle Integration <Service>:<Operation>
slack	Slack Adapter	N/A	N/A
SOAAdapter	Oracle SOA Suite Adapter (includes Oracle Service Bus and Oracle SOA Cloud Service)	N.A.	Call a << REST / SOAP >> service on a << SOA Composite / Service Bus project >>
soap	SOAP Adapter	• Trigger Oracle Integration SOAP Integration for the interface <Port Type> : <operation name>	• Call External SOAP API <Port Type> : <operation-name>
sqlserverdatabase	Microsoft SQL Server Adapter	• New row is inserted into <table name> in MS SQL Server DB	• Insert rows into <table name> in MS SQL Server DB • Merge rows into < table name> in MS SQL Server DB • Update rows into <table name> in MS SQL Server DB
Successfactors	SAP SuccessFactors Adapter	• Receive <<operationName> > <<BusinessObject> > from SuccessFactors	• Query data from SuccessFactors using SFQL query • Create <<BusinessObject> > in SuccessFactors • Update <<BusinessObject> >in SuccessFactors • Delete <<BusinessObject> >in SuccessFactors • Create or update <<BusinessObject> > in SuccessFactors
sugarcrm	SugarCRM Adapter	N/A	• For Query(Retrive single/list of Records) : <operation>from SugarCRM • For Create/Update/ Delete:<operation> in SugarCRM
surveymonkey	SurveyMonkey Adapter	N/A	N/A

Dimension Value in Metrics Explorer	Adapter Display Name	Inbound Processing Event Information Naming Conventions in Dimension Value Field	Outbound Invocation Endpoint Information Naming Conventions in Dimension Value Field
otac	Oracle Taleo Enterprise Edition Adapter	N/A	• Get request status from Oracle Talent Acquisition Cloud (Taleo EE) • Get request status from Oracle Talent Acquisition Cloud (Taleo EE)
trello	Trello Adapter	N/A	N/A
twilio	Twilio Adapter	N/A	N/A
twitter	Twitter Adapter	N/A	N/A
workday	Workday Adapter	N/A	• Create, Update, Delete, and Import records in Workday • Extract bulk data from workday

Dimension Value in Metrics Explorer	Adapter Display Name	Inbound Processing Event Information Naming Conventions in Dimension Value Field	Outbound Invocation Endpoint Information Naming Conventions in Dimension Value Field
zendesk	Zendesk Adapter	N/A	• Get Single Record: Get <Entity_NAME> from Zendesk • Get List of Records: Get <Entity_NAME>s from Zendesk • Create a Record: Create <Entity_NAME> in Zendesk • Update a Record: Update <Entity_NAME> in Zendesk • Update multiple Records: Update <Entity_NAME>s in Zendesk • Update multiple Records in batches: Update <Entity_NAME>s in batches in Zendesk • Search multiple Records: Search <Entity_NAME>s in Zendesk • Delete a Record: Delete <Entity_NAME> from Zendesk • Create or Update a Record: Create or Update <Entity_NAME> in Zendesk • Upload an Attachment: Upload Attachment in Zendesk • Redact Attachment: Redact Comment Attachment in Zendesk

Example of an Endpoint Metric Chart

The following example of an endpoint metrics chart is provided. The chart shows adapter inbound request processing times. A metrics namespace is provided that is a container for message metrics. The namespace identifies the service sending the metrics. The namespace for message metrics is oci_integration.



Adapters with Limited Dimensions

The following adapters do not publish inboundProcessingEndpointInformation and outboundInvocationEndpointInformation dimensions in the Metrics Explorer.

- AS2 Adapter
- Google Tasks Adapter
- Microsoft Office 365 People Adapter
- Oracle Commerce Cloud Adapter
- Oracle CPQ Adapter
- Oracle E-Business Suite Adapter
- Oracle Eloqua Cloud Adapter
- Oracle Logistics Adapter
- Oracle Messaging Cloud Service Adapter
- Oracle Responsys Adapter
- Slack Adapter

Calculate Requests Per Second

If a synchronous integration keeps timing out or is taking longer than usual to complete, the integration might be trying to process too many requests. Knowing the requests that your instance processes in a second helps you design synchronous integrations that deliver the fast responses that you need.

The requests-per-second calculation helps you determine the *approximate* number of concurrent requests that your system can receive from client applications. For example, when a mobile application calls Oracle Integration, how many concurrent requests from the mobile app can your instance process?

This calculation is specifically for synchronous integrations, for which Oracle Integration waits for a response from the target service. If you have an integration that completes a large task

and needs a long time to run, Oracle recommends creating an asynchronous integration instead.

> **Note:**
>
> - Generally, the words "message" and "request" are synonymous. However, when you're working with large payloads, you might consume more than one message per request. This change impacts your calculations. See View Message Metrics and Billable Messages.
>
> The calculations in this section assume that every request is 50 KB or smaller.
> - This calculation is typically called TPS, or transactions per second. TPS doesn't apply directly to Oracle Integration for two reasons:
> - Oracle Integration processes requests, rather than transactions.
> - Sizing in Oracle Integration is based on the hourly consumption of messages, rather than the per-second consumption.
>
> The Oracle Integration equivalent to TPS is requests per second, which is your concurrency.

1. Determine the approximate number of requests that an instance can process in one minute.
   a. Determine the number of message packs that you purchased per hour for the instance.

      For this example, we'll say that you have an Oracle Integration license and purchased **4 packs**.
   b. Multiply the number of message packs by the number of messages in the message pack (5,000 messages for non-BYOL customers, and 20,000 messages for BYOL customers).

      For this example, we'll say that you're a non-BYOL customer, so your message packs contain 5,000 messages.

      4 message packs x 5,000 messages per hour = 20,000 requests per hour
   c. Divide the number of hourly requests by 3,600 to determine your approximate per-second capacity.

      20,000 requests per hour / 3600 = 5.6 requests per second
   d. Multiply the per-second requests by 2; an instance can typically handle about twice your purchased capacity.

      5.6 requests per second x 2 = 11 requests per second
2. Calculate your concurrency (the number of concurrent requests your system can handle from client applications).
   a. Determine the typical response time in seconds.

      For example, run a few requests and check the response times in the activity stream timestamps. See Track the Status of Integration Instances in *Using Integrations in Oracle Integration 3*.

      The response time can vary depending on circumstances. When the volume of transactions increase in your instance, your response times might also increase.

For this example, we'll say that your response time is **5 seconds**.

b. Multiply the number of requests you can process per second by the response time.

11 requests per second x 5 seconds = 55 concurrent requests

This value is your approximate concurrency.

Example 5-1 Processing the maximum number of concurrent requests

Let's take a look at a sample request queue when an instance that can handle 55 concurrent requests is working at full capacity.

The following table illustrates how requests arrive and complete as each second passes. The total requests in the queue increase until they reach 55 and remain at 55 indefinitely. After 5 seconds (the response time), requests start completing.

Time that has elapsed	Requests that arrive	Requests that complete	Total requests in the queue
1 second	11	0	11
2 seconds	11	0	22
3 seconds	11	0	33
4 seconds	11	0	44
5 seconds	11	11	55
6 seconds	11	11	55
7 seconds	11	11	55
8 seconds	11	11	55

Example 5-2 Exceeding the maximum concurrent requests

Imagine the same instance is receiving a higher number of requests per second than the maximum concurrency value. The following table illustrates how quickly the number of requests in the queue can build, even when you exceed the concurrency by just a few requests. After 3 seconds, the instance has already exceeded its maximum number of concurrent requests, and within 8 seconds, the instance is dealing with twice the maximum number of concurrent requests.

If an integration is likely to exceed the instance's maximum concurrency, the integration is probably going to experience timeouts when built as a synchronous integration. Instead, build the integration as an asynchronous integration.

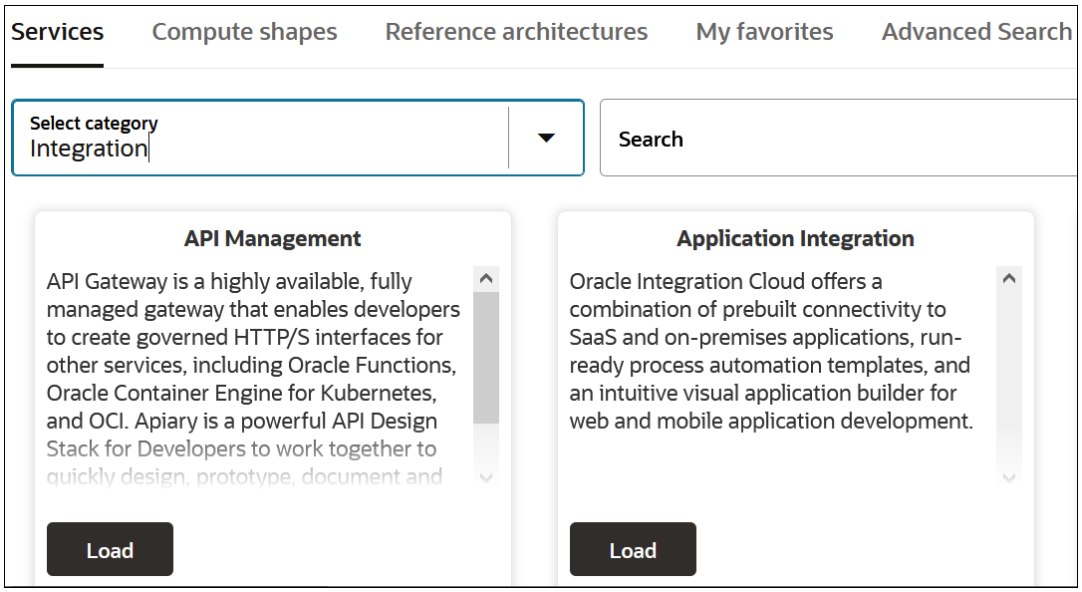
Time that has elapsed	Requests that arrive	Requests that complete	Total requests in the queue
1 second	20	0	20
2 seconds	20	0	40
3 seconds	20	0	60
4 seconds	20	0	80
5 seconds	20	11	89
6 seconds	20	11	98
7 seconds	20	11	107

Time that has elapsed	Requests that arrive	Requests that complete	Total requests in the queue
8 seconds	20	11	116

Use the Cost Estimator Tool to Determine Your Monthly Bill

Oracle provides a cost estimator tool to help you determine your monthly usage and bill for Oracle Integration.

1. Go to the cost estimator tool.
2. From the **Select category** list, choose **Integration**.
3. In the **Application Integration** box, click **Load**.



4. Follow the instructions on the page to calculate your costs.

   The estimated monthly cost is displayed.

   See Estimate Your Monthly Cost.

6

Upgrade from Oracle Integration Generation 2 to Oracle Integration 3

Upgrades from Oracle Integration Generation 2 to Oracle Integration 3 have begun and are available at no extra cost. Learn more about your prerequisites and the upgrade workflow.

Topics:

Learn About Upgrading to Oracle Integration 3

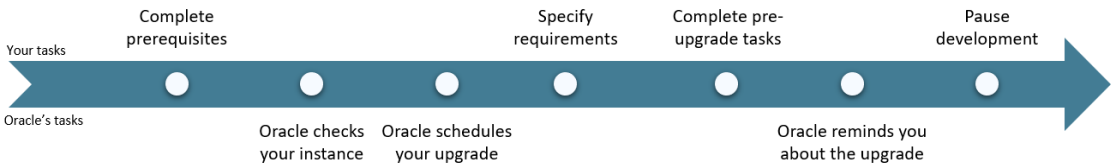
Get answers to your questions about upgrading an Oracle Integration Generation 2 instance to Oracle Integration 3, and understand the upgrade process.

Topics:

Upgrade Workflow Quick Reference

Oracle completes the majority of upgrade work on your behalf. All you need to do is complete some required steps and specify your requirements.

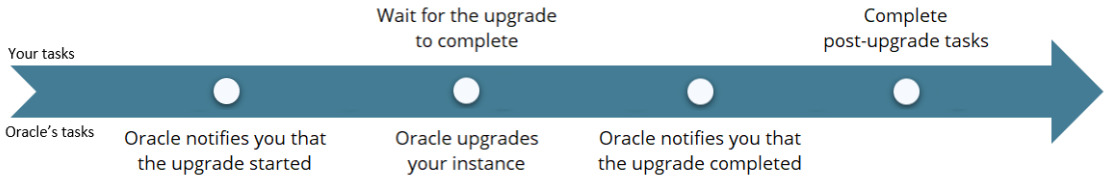
Before the Upgrade



> **Note:**
>
> Oracle schedules your upgrade after you complete all prerequisites, and all features that you use are ready to be upgraded. These requirements are covered in more detail in the following steps.

Timing	Oracle	You	Task	Details
Any time		**You**	Complete prerequisites	**Time to complete:** Varies. To get your instance ready for upgrade, complete all prerequisites. See Complete Upgrade Prerequisites.
Ongoing basis	Oracle		Checks your instance	Oracle periodically checks whether your instance is ready for upgrade. Until it's ready, continue working in Oracle Integration Generation 2.
One month before upgrade	Oracle		Schedules your upgrade	When your instance is ready for upgrade, Oracle sends you an email with your upgrade date. You can also see this on the **Upgrade** page.
After receiving the email		**You**	Specify upgrade requirements	**Time to complete:** 10 minutes. After you receive the email, complete the following tasks within Oracle Integration Generation 2: • Reschedule the upgrade, if needed. Oracle sends an email confirmation after you reschedule. • Specify your upgrade requirements. For details, see 2. Schedule the Upgrade and Configure Settings. **Note:** After scheduling the upgrade, Oracle checks the instance often to make sure that it is still ready for upgrade. If not, Oracle emails you about any issues so that you can address them. See Correct an Instance with Failed Eligibility Checks.
Two weeks before upgrade		**You**	Complete pre-upgrade tasks	**Time to complete:** Varies, about 15 minutes. For example, two weeks before upgrade, update your allowlists. See 3. Update Allowlists and Complete Pre-Upgrade Tasks.
Two days before upgrade	Oracle		Reminds you about the upgrade	Several days before upgrade, Oracle reminds you about the upgrade by sending an email.
Two days before upgrade		**You**	Pause development	**Time to complete:** Not applicable. Pause or limit your development work to help ensure a successful upgrade. See Limit Development Work Before the Upgrade.

During and After Upgrade



Timing	Oracle	You	Task	Details
Day of the upgrade, before it starts	Oracle		Informs you that the upgrade started	Oracle sends an email to inform you that the upgrade started.
Day of the upgrade	Oracle		Upgrades your instance	See Wait for the Upgrade to Complete.
Day of the upgrade		**You**	Wait for the upgrade to complete	**Time to complete:** Not applicable. The upgrade takes less than ten minutes. Your Oracle Integration Generation 2 instance is unavailable during the downtime. See Wait for the Upgrade to Complete.
Day of the upgrade, after it finishes	Oracle		Informs you that the upgrade completed	After the upgrade, Oracle sends an email to inform you that the upgrade completed successfully or if there was an issue.
Day of the upgrade, or up to ten days after		**You**	Complete post-upgrade requirements	**Time to complete:** Varies, about 20 minutes, or longer for comprehensive regression testing. Access the new Oracle Integration 3 instance using your existing URLs and credentials, and perform verification tasks as needed. For example, some organizations perform regression testing after upgrades. See 5. Complete Post-Upgrade Tasks.

Upgrade Notifications

Everyone who gets emails about Oracle Integration Generation 2 quarterly updates will receive several notifications prior to, during, and after upgrade.

Notification Subject	Description
Upgrade to Oracle Integration 3	After your instance passes the pre-eligability checks, Oracle sends you an email indicating that your instance is ready for upgrade and that your upgrade has been scheduled. You can also see this on the **Upgrade** page.
Upgrade to Oracle Integration 3 Reminder	The Friday before your scheduled upgrade date, Oracle sends you a reminder about the upgrade.
Upgrade to Oracle Integration 3 started	When the upgrade begins, Oracle sends an email telling you what to expect during upgrade. You won't be able to access Oracle Integration 3 during the upgrade.
Upgrade to Oracle Integration 3 complete	When the upgrade completes successfully, Oracle sends you an email reminding you to complete the post-upgrade tasks. You can resume work on Oracle Integration 3 after you receive this email.

Notification Subject	Description
Upgrade to Oracle Integration 3 failed	If there's an issue during upgrade, Oracle sends you an email indicating what you should do to correct the issues. **Note:** This notification doesn't include a new upgrade date.
Upgrade to Oracle Integration 3 Canceled	If your upgrade is canceled, Oracle sends you an email indicating that your integrations will continue to function normally with no changes and that Oracle will follow up with you on the next steps. **Note:** This notification doesn't include a new upgrade date.
Upgrade to Oracle Integration 3 rescheduled	If you reschedule your upgrade, Oracle sends you an email with the new upgrade date.

Upgrade FAQs

Get answers to questions about the upgrade from Oracle Integration Generation 2 to Oracle Integration 3.

1. **Am I required to upgrade my instances to Oracle Integration 3?**
   Yes, but only after all the capabilities that you use and that have not been deprecated are ready for upgrade in Oracle Integration 3.

   You are not required to upgrade unless your Oracle Integration Generation 2 instances meet the upgrade prerequisites for capabilities that have not been deprecated in Oracle Integration 3.

   After your instance passes the upgrade check, Oracle selects an upgrade window for you and sends an email notification. Everyone who receives emails about Oracle Integration Generation 2 quarterly updates receives the email.

   If needed, you can select a different upgrade window, but you can't opt out of the upgrade.

   If you have to go live during your assigned upgrade window, Oracle can change the upgrade window to a month earlier or a month later. Enter a service request (SR) on My Oracle Support.

2. **What are the benefits of upgrading?**
   Oracle Integration 3 is the next generation of the Oracle Integration platform. The upgrade to Oracle Integration 3 delivers a modern and intuitive user interface and improved performance. Additionally, the latest features will be delivered only to Oracle Integration 3.

   See Benefits of Upgrading.

3. **Are all the features from prior versions of Oracle Integration available in Oracle Integration 3?**

See Differences from Prior Versions of Oracle Integration.

4. **Is there a charge to upgrade?**
   No. The upgrade is available at no additional cost.

5. **What is the upgrade workflow?**
   See Upgrade Workflow Quick Reference.

6. **When will my instance be upgraded?**
   Oracle is currently scheduling upgrades on a limited basis. The timeline for your upgrade depends on a number of factors, including whether upgrade is available for the features that you use.

   To prepare for the upgrade, make sure that the instance meets all prerequisites. Then, all you need to do is wait for Oracle to schedule your upgrade. Or, if you're ready to start working in Oracle Integration 3 right away, enter a service request (SR) on My Oracle Support and request an earlier upgrade.

7. **How do I submit an upgrade request?**
   If you're ready to start working in Oracle Integration 3 right away, enter a service request (SR) on My Oracle Support.

   Before you submit the request, spend a few minutes determining whether your instance is ready for upgrade:

   - Check whether the capabilities that you use are ready to be upgraded.
     See Instances That Cannot Be Upgraded Yet.
   - Make sure you've completed all the prerequisites for scheduling the upgrade.
     See Complete Upgrade Prerequisites.

8. **Can I choose or reschedule my upgrade date?**
   Yes. After your instance is ready for upgrade, Oracle selects an upgrade window for you.

   You can change your upgrade window if it's seven or more business days away.

   All upgrade dates that are available to you appear on the **Upgrade** page, in the **Upgrade Window** list.

   If you have to go live during your assigned upgrade window, Oracle can change the upgrade window to a month earlier or a month later. Enter a service request (SR) on My Oracle Support.

9. **Will there be downtime?**
   Yes. Your upgrade takes less than ten minutes. During this time, Oracle Integration is unavailable, and all in-flight instances stop running. See How Upgrade Affects Runtime Data.

   Everyone must stop working in Oracle Integration. If you try to sign in during the downtime, a Service Unavailable page informs you that Oracle Integration is unavailable.

10. **My upgrade was scheduled. What if I don't confirm the date or specify upgrade details?**
    As long as your instances passes the upgrade check, the upgrade proceeds as scheduled.

11. **Can I have both Oracle Integration Generation 2 and Oracle Integration 3 instances?**
    Yes. For example, if you have multiple Oracle Integration Generation 2 instances, you can upgrade them at different times. Even if your instances have different versions, you can continue working in all of them.

    If you are an administrator who works in the Oracle Cloud Infrastructure Console, your Oracle Integration 3 instances appear in the same list as your Oracle Integration Generation 2 instances. Each instance is clearly labeled so you can identify its version.

12. **Can I migrate some integrations in my instance to Oracle Integration 3 and keep some integrations in my existing Oracle Integration Generation 2 instance?**
    No. When you upgrade, you must upgrade the entire instance.
13. **How does the upgrade affect my activity stream and actively running integrations?**
    See How Upgrade Affects Runtime Data.
14. **How does the upgrade affect File Server?**
    See How Upgrade Affects File Server.
15. **How does the upgrade affect Process?**
    Processes functionality has been replaced by Oracle Cloud Infrastructure Process Automation. See Process Automation.
16. **How does the upgrade affect Visual Builder?**
    Upgrade doesn't affect Visual Builder (VB); you remain on the same version of VB as you were prior to upgrade.

    However, if your instance uses Visual Builder with your own Oracle database instance, a configuration which isn't currently supported in Oracle Integration 3, revert back to using the embedded database. See the note about reverting your database in Switch to a Different Oracle DB instance in *Administering Oracle Visual Builder in Oracle Integration 3*.
17. **How do I know when the upgrade is finished?**
    Upgrade finishes in less than ten minutes. Oracle sends you an email when the upgrade completes.

    You can also see if your instance is available by trying to sign in:

    - If you sign in and the user interface remains unchanged, the upgrade hasn't begun yet.
    - If you sign in and a page informs you that the service is unavailable, the upgrade is still in progress.
    - If you sign in and the user interface has changed, the upgrade is finished.
      Confirm the upgrade finished by checking the version number in the About dialog.
18. **Is basic authentication still supported?**
    See When is Basic Authentication Supported in Oracle Integration 3?.
19. **What do I have to do before the upgrade?**
    See 3. Update Allowlists and Complete Pre-Upgrade Tasks.
20. **Will the IP address of my instance change?**
    Yes. After the upgrade, the Oracle Integration 3 instance has a different IP address than the Oracle Integration Generation 2 instance.

    If you have allowlists, you need to allowlist the new IP addresses. See 3. Update Allowlists and Complete Pre-Upgrade Tasks.

    After the upgrade finishes, the Oracle Integration Generation 2 IP addresses are no longer assigned to you.

    Note that the ingress IP addresses for development and production instances are different, even within the same region. However, the egress IP address is the same for all shapes (development or production) in a single region.
21. **Will my URLs change?**
    The *runtime* URL for Oracle Integration 3 won't change; it will be your Oracle Integration Generation 2 URL. The *design-time URL* will change, but your bookmarks will still work. The design-time URL for Oracle Integration 3 is a combination of your Oracle Integration 3 base URL, your instance name, and your region.

After the upgrade, the design-time URL for your Oracle Integration Generation 2 instance redirects to the new Oracle Integration 3 instance URL, so you can continue using your existing bookmark or update it. It's up to you.

22. **Can I switch to a different region or compartment during the upgrade?**
    No. Moving regions and compartments is not part of the upgrade process.

23. **What happens during an upgrade?**
    See Wait for the Upgrade to Complete.

24. **What if a scheduled integration is running when the upgrade begins?**
    Prior to the upgrade, Oracle stops the schedule if it's running. After the upgrade, the schedule starts in Oracle Integration 3 from the point where it stopped in Oracle Integration Generation 2.

25. **Should I stop my scheduled integrations before the upgrade?**
    Oracle doesn't recommend stopping your scheduled integrations. If you stop your integrations in your Oracle Integration Generation 2 instance, the integrations remain stopped in the Oracle Integration 3 instance after the upgrade is complete, and you'll have to manually restart everything.

26. **Will my Oracle Integration Generation 2 instance still be available after the upgrade?**
    No. Your Oracle Integration Generation 2 isn't available after the upgrade.

27. **Are Oracle Integration Generation 2 and Oracle Integration 3 integrations forward and backward compatible?**
    No. Oracle Integration 3 includes many new features that aren't available in Oracle Integration Generation 2, making integrations incompatible between the two versions.

28. **What do I have to do after the upgrade?**
    See 5. Complete Post-Upgrade Tasks.

29. **What if something changes after my upgrade is scheduled and my instance can't be upgraded anymore?**
    After scheduling the upgrade, Oracle checks your instance often to make sure it's still ready. If the check identifies any issues, Oracle emails you so you can address the issues and proceed with the scheduled upgrade.

    Oracle also checks your instance at the beginning of the upgrade window. If the check identifies any issues, Oracle cancels the upgrade and emails you about the change. Everyone who gets emails about Oracle Integration Generation 2 quarterly updates receives the email, which includes information about next steps.

30. **Will my user, group, and policy information be available after upgrade?**
    Yes. All security-related information from your Oracle Integration Generation 2 instance is present in your Oracle Integration 3 instance after the upgrade. Additionally, the upgrade doesn't change anything related to identity domains. For example, if your tenancy uses identity domains before the upgrade, it continues using identity domains after the upgrade.

31. **What if issues occur during the upgrade?**
    In rare situations, an issue prevents an upgrade from completing. When an upgrade doesn't complete, Oracle rolls back the changes, turns on the schedule in the Oracle Integration Generation 2 instance, and restores your access to the instance during the downtime period. You continue working in the Oracle Integration Generation 2 instance, with the same features and capabilities you were using before the upgrade.

    In such situations, Oracle informs you over email that you can continue working in Oracle Integration Generation 2. Expect the email to arrive either within your upgrade window or soon after. Everyone who gets emails about Oracle Integration Generation 2 quarterly updates receives the email. You can schedule your upgrade for another time, and Oracle works with you to determine the next steps.

When you specify upgrade requirements, you can also choose to ignore specific issues during upgrade. For instance, you determine whether to proceed with the upgrade if Oracle is unable to activate all integrations and start the schedule for all integrations. See 2. Schedule the Upgrade and Configure Settings.

32. **What if issues occur after the upgrade?**
After the upgrade completes, sign in and perform your typical verification tasks. Additionally, complete the required post-upgrade tasks.

    If you experience any issues after the upgrade, either while performing verification tasks or performing day-to-day activities, enter a service request (SR) on My Oracle Support.

33. **If I use the connectivity agent, do I need to recreate any connections?**
No. However, you should be aware of several points:

    - *Before* upgrade, you must update your allowlist settings to configure connectivity from your connectivity agents to Oracle Identity Cloud Service (IDCS) and the Oracle Integration runtime URL and IP addresses.
    - During the upgrade, the connectivity agent is automatically converted from using basic authentication to using OAuth 2.0 token-based authentication to communicate with Oracle Integration. All agents are automatically upgraded to OAuth 2.0, so you don't need to manually recreate any agents yourself.
    - After the upgrade, you'll see additional traffic to your firewall because the connectivity agent must get new authentication tokens from the Oracle Identity Cloud Service or the identity domain.
    - Agents that are offline during upgrade or don't meet upgrade requirements won't be upgraded. You'll need to perform post-upgrade steps to regain connectivity.

34. **If I convert the JKS KeyStore to the PKCS12 KeyStore for the connectivity agent, does this affect my Oracle Integration Generation 2 connectivity agent?**
No. Converting the JKS KeyStore to the PKCS12 KeyStore does not impact your Oracle Integration Generation 2 connectivity agent, and only takes effect after you have upgraded to Oracle Integration 3. You can convert your keystore manually or let it happen automatically during upgrade (requires agent to use JDK 17).

Benefits of Upgrading

Oracle Integration 3 is the next generation of the Oracle Integration platform. The upgrade to Oracle Integration 3 delivers a modern and intuitive user interface and improved performance. Additionally, the latest features will be delivered only to Oracle Integration 3.

Here's a look at *some* of the new features in Oracle Integration 3, but more new features are added in every release. For details on *all* the new features, see What's New for Oracle Integration:

Feature	Description
Connect to private resources	Secure traffic to private resources that are in your virtual cloud network (VCN) using a private endpoint. With a private endpoint, all traffic goes through a private channel that is set up within Oracle Cloud Infrastructure and never goes over the public internet. See Connect to Private Resources, and Adapters that Support Connecting to Private Endpoints.
Deployment of new connectivity agents is easier and more reliable	The connectivity agent now requires zero configuration, thanks to the replacement of user credentials with a system-generated OAuth 2.0 token-based authentication. See Create an Agent Group.

Feature	Description
Increased payload size for adapters	The supported sizes for some payloads have increased. • You can process 100 MB structured payloads and 50 MB payloads with the connectivity agent with these adapters: – REST and SOAP SaaS-based adapters – Oracle Autonomous Transaction Processing Adapter – Oracle Autonomous Data Warehouse Adapter – Oracle Database Cloud Service Adapter – FTP Adapter • The stage file action can process 100 MB structured payloads. For more details, see Service Limits.
Inbound polling support without the connectivity agent	You can poll the Oracle Autonomous Data Warehouse database, Oracle Autonomous Transaction Processing database, and Oracle Database Cloud Service database without using the connectivity agent. See: • Oracle Autonomous Data Warehouse Adapter: Perform Inbound Database Polling Without the Connectivity Agent • Oracle Autonomous Transaction Processing Adapter: Perform Inbound Database Polling Without the Connectivity Agent • Oracle Database Cloud Service Adapter: Perform Inbound Database Polling Without the Connectivity Agent
Use projects to manage and monitor integration assets	Use projects to develop, deploy, and monitor related integrations and their components from a single workspace. The number of projects you create and the integrations you include in each project is up to you. You can use role-based access control (RBAC) to define which users and groups can edit, view, and monitor a project. See About Integration Projects and Design, Manage, and Monitor Integrations in Projects.
Invoke Oracle Cloud Infrastructure functions directly from an integration	Directly invoke Oracle Cloud Infrastructure functions from an integration in the integration canvas. See Invoke Oracle Cloud Infrastructure Functions from integrations with the OCI Function Action.
Publish and subscribe to events in integrations	Create events in Oracle Integration and then publish the events in integrations. You can then create an integration that subscribes to the events. See Create Integrations to Publish and Subscribe to Events and Publish Events in an Integration with a Publish Event Action.
Use parallel actions in integrations to improve performance	You can use a parallel action in integrations to process tasks in parallel to improve integration performance and response times. With a parallel action, the path of an integration is split into multiple branches. Each branch is processed in parallel and messages are sent to each service endpoint in parallel. When all tasks are completed, all branches are synchronized at their termination points in the parallel action, and the main path of the integration is resumed. See Process Tasks in Parallel with a Parallel Action.
Self-diagnose event delivery for Oracle Fusion Applications	Self-diagnose the delivery of business events between Oracle Fusion Applications and Oracle Integration, such as determining if delivery issues are occurring in Oracle Fusion Applications or Oracle Integration. You can also perform some management tasks, such as retrying the delivery of business events that have failed. See Diagnose and Manage Event-Based Oracle Fusion Applications Integrations.
New adapters	• PostgreSQL • Snowflake • Netezza • OData • Oracle Primavera Cloud • Primavera Unifier

Feature	Description
B2B for Oracle Integration enhancements	• Support for Open Applications Group Integration Specification (OAGIS) documents. See Open Applications Group (OAGIS) Support. • Support for Custom XML schema and documents. See Custom XML Support. • Support for message resubmission. See Track B2B Messages. • New B2B metrics dashboard. See Monitor the Overall Health of B2B Transactions. • Support for RosettaNet. See About RosettaNet and RosettaNet Adapter Capabilities.
Build your own adapters with the Rapid Adapter Builder	The Rapid Adapter Builder transforms the adapter experience in Oracle Integration by allowing you to build an adapter for any application that exposes REST APIs. Oracle provides a Visual Studio Code extension for the Rapid Adapter Builder. Use the extension to develop, validate, and publish an adapter to an Oracle Integration instance. See Learn About the Rapid Adapter Builder in Oracle Integration.
Test an integration from the canvas	You can test REST Adapter trigger connection-based integrations and scheduled integrations with the ▷ button in the integration canvas. This button automatically activates your integration with the tracing level set to debug and lets you specify request details from inside the integration canvas. This capability simplifies integration testing and eliminates the need to separately exit the canvas, activate the integration and set the tracing level, and access the Configure and run page to specify your request details. See Test Integrations from Inside the Integration Canvas.
Private endpoint - OAuth 2.0 support	For private endpoints, an OAuth provider is now supported if it is privately hosted.
Associate an instance with a secondary domain	If your tenancy uses identity domains, you can now associate an Oracle Integration 3 instance with a secondary identity domain—an identity domain other than the one you're signed into. This allows you to manage all your instances in your tenancy from one domain, rather than having to sign into each domain to manage the associated instances. See Creating an Oracle Integration Instance.
Mapper enhancements	• Support for the for-each-group construct in the mapper. See Iterate Across Groups with a for-each-group Constructor. • Copy-of support in design mode in the mapper. See Perform a Deep Copy of Elements with a copy-of Constructor.

How Upgrade Affects Runtime Data

Understand how upgrade affects your activity stream and actively running integrations. For example, all runtime activities are paused during the downtime.

Integration Data Retention Time

Oracle Integration 3 supports only 32 days of data retention. During upgrade only the most recent 32 days of retained data will be migrated.

For integrations, 32 or fewer days of retained data are typically sufficient.

Historical Data in Activity Stream

The activity stream in Oracle Integration Generation 2 is not moved to Oracle Integration 3. Therefore, after the upgrade completes, historical data for your integrations isn't available in Oracle Integration 3.

The activity stream feature is available in Oracle Integration 3. Therefore, historical information is available from the upgrade date onward.

If you capture the activity stream in Oracle Cloud Infrastructure, this information remains available after the upgrade. If you don't capture this data yet, you can start at any time. See Capture the Activity Stream in Oracle Cloud Infrastructure Console.

Actively Running Synchronous Integrations

When the downtime begins as part of the upgrade, Oracle Integration stops accepting incoming requests for actively running synchronous integrations. Oracle Integration also finishes processing all previously received requests in a few minutes.

During the downtime, any client that sends a request to Oracle Integration gets a failure notice.

> **Note:**
>
> During the downtime, if an integration invokes a co-located integration using a local invoke call, or if an integration is a hybrid integration that uses the connectivity agent, the integration doesn't run successfully.

After the upgrade finishes, Oracle Integration accepts incoming requests again.

Actively Running Asynchronous Integrations

When the downtime begins as part of the upgrade, Oracle Integration stops accepting incoming requests for actively running asynchronous integrations. Oracle Integration also finishes processing the previously received requests. In most cases, Oracle Integration processes the requests in a few minutes.

After the upgrade finishes, Oracle Integration accepts incoming requests again.

Actively Running Scheduled Integrations

When the downtime begins as part of the upgrade, Oracle Integration stops accepting incoming requests for scheduled integrations and finishes processing all previously received requests. In most cases, Oracle Integration processes the requests in a few minutes.

Any requests that Oracle Integration doesn't process in a few minutes are discarded, but no data is lost. Here's why: Oracle migrates the global schedule parameters for the integration and starts the schedule in Oracle Integration 3. After the upgrade is complete and Oracle Integration 3 begins processing requests, Oracle Integration 3 uses the parameters to start processing where Oracle Integration Generation 2 stopped processing.

The post-upgrade cut over is seamless, but depending on when your upgrade occurs, you might experience some business impact. For instance, if an integration sends emails every 30 minutes starting at 9 AM, and your upgrade is from 8:30 AM to 10:30 AM, the email that usually arrives at 9 AM will probably be delayed.

Failed Integration Instances

Oracle does not migrate failed integration instances to Oracle Integration 3.

Additionally, by default, a failed integration instance prevents an upgrade from succeeding. However, an override is available. To upgrade even when you have one or more failed integration instances, you must select the override setting when you schedule the upgrade. If you don't select this setting and have one or more failed integration instances, the upgrade fails.

To learn about your options for failed integration instance, see Complete Upgrade Prerequisites.

To learn about the setting that lets you upgrade with a failed integration instance, see 2. Schedule the Upgrade and Configure Settings.

Integration Insight

Insight isn't supported in Oracle Integration 3. Your Insight models and consoles won't be migrated when you upgrade to Oracle Integration 3. As an alternative, use Oracle Cloud Infrastructure Logging Analytics and Process Automation Analytics.

How Upgrade Affects File Server

Upgrading from Oracle Integration Generation 2 to Oracle Integration 3 affects File Server in the following ways.

New IP and Port Values

After the upgrade, Oracle assigns new IP and port values for the File Server SFTP server. The Oracle Integration Generation 2 IP and port values remain valid for SFTP runtime traffic for four months after the upgrade.

If you had a File Server allowlist in Oracle Integration Generation 2 and upgraded to Oracle Integration 3, understand how the new IP and port values that Oracle assigns after the upgrade affect your File Server allowlist.

- For SFTP clients that were on your File Server allowlist in Oracle Integration Generation 2 These SFTP clients can continue accessing File Server using the Oracle Integration Generation 2 IP and port values. This access is granted for up to four months after the upgrade and persists even if you remove the SFTP clients from your self-service File Server allowlist.

  You have the following action items:

  - Within the four-month time window, you must update all integrations and SFTP clients so that they use the new IP and port values.
    While you don't have to update the values immediately after the upgrade, Oracle recommends completing this step then. Otherwise, you risk forgetting to update the values and then experiencing issues when Oracle retires the IP and port values. See 5. Complete Post-Upgrade Tasks.
  - If you want to block the integrations and SFTP clients from accessing File Server, enter a service request (SR).
- For SFTP clients that weren't on your File Server allowlist in Oracle Integration Generation 2, such as new SFTP clients that you configure after upgrading
  You have the following action items:

  - Ensure that all integrations and SFTP clients use the Oracle Integration 3 IP and port values to access File Server.
    See 5. Complete Post-Upgrade Tasks.
  - Add the SFTP clients to the File Server allowlist.

Access File Server with URL and Credentials

In Oracle Integration Generation 2 you accessed the File Server folder using the IP port and credentials. After the upgrade, in Oracle Integration 3, you can access it using the File Server URL and credentials.

No Change to File Server REST APIs

After the upgrade, access the File Server REST APIs the same way you did in Oracle Integration Generation 2.

File Server Migration

Oracle migrates your File Server files, folder structure, and allowlists (permissions) from Oracle Integration Generation 2 to Oracle Integration 3 for you.

For information on managing your allowlists for File Server after migration, see Restrict Access to an Instance.

When is Basic Authentication Supported in Oracle Integration 3?

Oracle Integration 3 supports OAuth 2.0, a token-based authentication method that is more secure. When you upgrade to Oracle Integration 3, we recommend you use OAuth whenever you can. However, this doesn't mean you need to immediately change *all* your interface connections.

The interface determines which authentication method to use, so some connections will instead use basic authentication or OCI Signature Version 1. For example, when using the Oracle Integration 3 REST API, you *must* use OAuth, but your existing integrations can still be invoked using basic authentication, and endpoints that are invoked by Oracle Integration can still be called over basic authentication. The following table lists various interfaces, which authentication method they use, and examples of each interface.

Interface	Authentication method	Interface examples
Oracle Integration built-in APIs • Oracle Integration 3 REST API • File Server in Oracle Integration 3 REST API • OCI Process Automation REST API	OAuth **Note:** OCI Signature Version 1 is not supported	• Visual Builder or Process Automation introspecting a list of available integrations • Find and resubmit failed integration via API • Create a folder in File Server using REST API • List processes via API
Oracle Cloud Infrastructure (OCI) lifecycle API and CLI • Oracle Integration API	OCI Signature Version 1	• Use Python to provision an Oracle Integration instance • Use the REST API to add an ACL to an Oracle Integration instance
APIs for integrations you create	Determined by the trigger; could be OAuth, basic authentication, or both **Note:** OCI Signature Version 1 is not supported	• Invoke an integration REST trigger from a mobile application

1. Prepare for the Upgrade to Oracle Integration 3

Your instance is ready for upgrade after you complete all prerequisites, and the instance passes the upgrade check.

Complete these steps at any time. Oracle schedules your upgrade only after all prerequisites have been met. You must address all issues that apply to your instance, or the instance won't be ready for upgrade.

- Timeline for Preparing for Upgrade

- Instances That Cannot Be Upgraded Yet
- Prerequisites When You Have Multiple Instances
- Complete Upgrade Prerequisites

Timeline for Preparing for Upgrade

Overview of steps required to prepare for the upgrade to Oracle Integration 3.

Timeline	Required Task
One month before upgrade	Complete Upgrade Prerequisites
One month before upgrade	Once all the prerequisites checks have passed, you can schedule your upgrade. You'll need to specify settings for the upgrade. 2. Schedule the Upgrade and Configure Settings
Two weeks before upgrade	After your upgrade is scheduled, update your allowlists and complete additional pre-upgrade tasks. 3. Update Allowlists and Complete Pre-Upgrade Tasks
Two days before upgrade	Limit Development Work Before the Upgrade

Instances That Cannot Be Upgraded Yet

Instances that use certain features and capabilities can't be upgraded yet.

1. If a custom endpoint was configured for the instance, the instance can't be upgraded yet.
2. An instance that doesn't meet all prerequisites can't be upgraded yet.
   See Complete Upgrade Prerequisites.

Prerequisites When You Have Multiple Instances

Consider several factors when planning upgrades for multiple instances.

All Instances Must Be Ready for Upgrade

If you have multiple instances within a tenancy, all instances must be ready for upgrade before any instances can be upgraded.

Oracle upgrades each instance separately, so you must choose an upgrade window for every instance. You can choose a different upgrade window for each instance.

Upgrade Non-Production Instances First

Oracle recommends upgrading your non-production instances first and your production instances second. Use the time between the upgrades to verify the environment in your non-production instances.

Additionally, if you use an instance for disaster recovery, Oracle recommends upgrading your disaster recovery instance first. Use your own discretion to determine the time between your disaster recovery instance and your production instance.

Keep in mind that during the time period between upgrades, any new features in Oracle Integration 3 aren't available in your Oracle Integration Generation 2 instance.

If You Experience Issues Between Upgrades

If you experience issues in your production instance after your non-production instance has been upgraded, you can't make corrections in the non-production environment, since it has already been upgraded. In such situations, enter a service request (SR) on My Oracle Support so that Oracle can help you plan your next steps.

Complete Upgrade Prerequisites

You must complete all the prerequisites that apply to your instance and your instance must pass the upgrade eligibility check before your instance is ready for upgrade. You can complete these steps at any time.

After you complete the upgrade prerequisites, you can check your instance's upgrade eligibility. In the navigation pane, click **Settings**, then **Upgrade**. You can recheck eligibility at any time.

Eligibility Check Table

The eligibility check table shows the following information about status of your instance's upgrade eligibility:

Column	Description
Eligibility Condition	The condition that must be met to be ready for upgrade. Some conditions include links to associated documentation.
Owner	Who is responsible for managing the condition.
Due Date	The date by which the condition should be met.
Eligibility Status	The status of the condition, including explanations for conditions that haven't been met. Expand the **More details...** to see additional information about the condition failure.

Oracle periodically checks your instance's upgrade eligibility. When your instance is ready, Oracle will inform you in the interface and by email, so that you can schedule your upgrade. See 2. Schedule the Upgrade and Configure Settings.

Summary of Prerequisites

This table summarizes the prerequisite tasks for each area. The details for each task are linked in the table and shown in the next section.

Area	Tasks
Connectivity Agent	• Prepare for conversion to OAuth 2.0 • Agent Java Version and JKS KeyStore • Connectivity agent must be running • Update your allowlist settings
Instances	• Custom Endpoint URL • Instance ID change from integer to string
B2B for Oracle Integration	• B2B Passwords for Keystore • B2B AS2 adapter connections with identity certificates • B2B Retention Period

Area	Tasks
Integrations	• Delayed (Asynchronous) Response • Failed Instances • Identity Certificates • VBCS with BYODB • Basic Routing Duplicate App Name • Number of Active Integrations • Multiple Read File • Legacy Stage File action in integrations
Adapters	• API calls in Visual Builder application • Custom Adapter • Microsoft adapters • Unsupported Adapters • Unsupported REST Types - REST Adapter
Process Automation	Process Automation
Insight	Insight

Prerequisite Details

> **Note:**
>
> Some of the prerequisites listed here don't have associated checks on the **Upgrade** page. Make sure you complete all the prerequisites that apply to your instance.

Area	Typical owner	Eligibility condition	Tasks to Complete
Connectivity Agent	Development Operations team	Prepare for conversion to OAuth 2.0	During the upgrade, connectivity agents are automatically converted from using basic authentication to using OAuth 2.0 token-based authentication to communicate with Oracle Integration. OAuth 2.0 token-based authentication is more secure, and it makes connectivity agent configuration simpler in Oracle Integration 3 than in Oracle Integration Generation 2. However, before upgrade you must prepare for this conversion by allowing egress from the agent network to Oracle Integration design-time and runtime, and to the Oracle Identity Cloud Service or the identity domain. For more information on OAuth 2.0 support in Oracle Integration 3, see When is Basic Authentication Supported in Oracle Integration 3?.

Area	Typical owner	Eligibility condition	Tasks to Complete

Connectivity Agent	Development Operations team	Agent Java Version and JKS KeyStore	Ensure that the connectivity agent uses JDK 17 and PKCS12 KeyStore. The **Connectivity Agent Status** section shows the status of all the connectivity agents in your instance, indicating whether each agent is using the proper version of JDK and KeyStore and whether it's in use.
			1. For any connectivity agent that isn't already using JDK 17, install JDK 17 on the server that hosts the agent.
			2. For any agent that is still using the JKS KeyStore, convert the KeyStore to PKCS12 KeyStore. You can do the conversion in one of two ways:
			• Automatically, during upgrade: Your JKS KeyStore will automatically be converted to the PKCS12 KeyStore during upgrade.
			• Manually, before upgrade: Alternatively, you can convert the JKS KeyStore to the PKCS12 KeyStore manually, before upgrade, by following the steps below.
			Note: Converting the JKS KeyStore to the PKCS12 KeyStore doesn't impact your Oracle Integration Generation 2 connectivity agent, and only takes effect after you have upgraded to Oracle Integration 3.
			Complete the following steps before upgrade if you want to manually convert your JKS KeyStore to the PKCS12 KeyStore. These tasks require you to briefly stop and then restart the connectivity agent, so choose a time when the connectivity agent isn't being used.
			a. On the server that hosts the connectivity agent, create a backup of the `keystore.jks` file, which is located in the following folder:
			`Agent_Install_Location/agenthome/agent/cert`
			b. Move the backup file to a different folder.
			c. Convert the JKS KeyStore to the PKCS12 KeyStore by running the following command from the command line:
			`keytool -importkeystore -srckeystore keystore.jks -destkeystore keystore.p12 -srcstoretype JKS -deststoretype PKCS12 -deststorepass changeit -srcstorepass changeit`
			d. Stop the connectivity agent.
			e. Delete the `keystore.jks` file in the following location:
			`Agent_Install_Location/agenthome/agent/cert`
			f. Start the connectivity agent.

Area	Typical owner	Eligibility condition	Tasks to Complete
Connectivity Agent	Development Operations team	Connectivity agent must be running	Make sure the connectivity agent is up and running before the upgrade begins. The **Connectivity Agent Status** section shows the status of all the connectivity agents in your instance, indicating whether each agent is offline (unavailable) and whether it's in use. Agents that are offline during upgrade or don't meet upgrade requirements won't be upgraded. You'll need to perform post-upgrade steps to regain connectivity. In Oracle Integration Generation 2, the connectivity agent uses basic authorization to invoke Oracle Integration endpoints. During the upgrade, the connectivity agent is automatically converted from using basic authentication to using OAuth 2.0 token-based authentication to invoke Oracle Integration endpoints. All connections are automatically upgraded to OAuth 2.0, so you don't need to manually recreate any connections yourself. As a result of the new authentication method, you'll see additional traffic to your firewall after the upgrade. This additional traffic occurs because the connectivity agent must communicate with the server to get new tokens.
Connectivity Agent	Development Operations team	Update your allowlist settings	Before upgrade, you must update your allowlist settings to configure connectivity from your connectivity agents to Oracle Identity Cloud Service (IDCS) and the Oracle Integration runtime URL and IP addresses. Perform the following updates: • Add the URL for Oracle Identity Cloud Service (IDCS) to the allowlist. • Add the runtime URL and IP addresses for Oracle Integration to the allowlist. • Set the proxy server's Cache property for the Oracle Integration URLs to refresh as frequently as possible.
Instances	Administrator	Custom Endpoint URL	If your instance includes a custom endpoint, the instance can't be upgraded yet. Wait until Oracle starts upgrades for this capability.
Instances	Administrator	Instance ID change from integer to string	The system-generated instance ID that is displayed on the Instances page and in the activity stream for an integration instance has changed from an integer to a string in Oracle Integration 3. This may affect any systems that you use that rely on the instance ID being an integer. For example, if you are parsing the instance ID from a REST API and storing it in a database.
B2B for Oracle Integration	Administrator	B2B Passwords for Keystore	Ensure that all passwords for the keystore file are identical, or the upgrade fails. See 3. Update Allowlists and Complete Pre-Upgrade Tasks.
B2B for Oracle Integration	Administrator	B2B AS2 adapter connections with identity certificates	If you have AS2 Adapter connections that use identity certificates, you must complete some pre-upgrade and post-upgrade tasks. See the IDENTITY Certificates.
B2B for Oracle Integration	Administrator	B2B Retention Period	Oracle Integration 3 supports only 32 days of data retention. During upgrade only the most recent 32 days of retained data will be migrated. For integrations, 32 or fewer days of retained data are typically sufficient. However, some organizations that use B2B for Oracle Integration prefer a higher setting so they have access to a longer history of purchase orders, invoices, and other B2B-related transactions and documents. You may be able to request a higher data retention period in the future.

Area	Typical owner	Eligibility condition	Tasks to Complete
Integrations	Development team	Delayed (Asynchronous) Response	The delayed (asynchronous) response pattern isn't available in Oracle Integration 3. If any of your integrations use a delayed (asynchronous) response pattern, rework them to achieve the delayed response functionality: • Create a simple invoke for success callbacks. • Create an additional invoke for failure callbacks under the fault handler to catch the correct fault.
Integrations	Development Operations team	Failed Instances	Failed integration instances fall into one of the following categories: • Recoverable asynchronous instances • Non-recoverable synchronous instances **Recoverable asynchronous instances** Resubmit the failed instances and clear the queue. If the resubmission is successful and if Oracle detects no other issues, your instance is ready for upgrade. See Resubmit Failed Messages. If you have a failed asynchronous instance and choose to upgrade anyway, you can't resubmit the failed instance in Oracle Integration 3--at least not right away. You can't resubmit because runtime data, including errors and all activity stream data, isn't migrated to Oracle Integration 3 as part of the upgrade. However, after the upgrade completes, you can run the integration in Oracle Integration 3, collect error data, and then resubmit. **Non-recoverable synchronous instances** You can't resubmit synchronous integration instances, so they are not recoverable. It's up to you whether to upgrade with non-recoverable synchronous instances. **Note:** If you capture activity stream data in the Oracle Cloud Infrastructure Console, you can still view historical activity for the integration. See Capture the Activity Stream of Integrations in the Oracle Cloud Infrastructure Console.
Integrations	Development team	Identity Certificates	Identity certificates establish client identity during two-way SSL communication. Connections that are based on the AS2 Adapter and the REST Adapter can use identity certificates. If you have identity certificates, perform the following steps: • When scheduling the upgrade, you'll need to select **Ignore identity certificates during upgrade eligibility check**. See 2. Schedule the Upgrade and Configure Settings. • After the upgrade: Upload a new identity certificate, test the connections that use the identity certificate so their status changes from Draft to Configured, and activate any integrations that use the connections. See 5. Complete Post-Upgrade Tasks.

Area	Typical owner	Eligibility condition	Tasks to Complete
Integrations	Development team	VBCS with BYODB	If your instance uses Visual Builder with your own Oracle database instance, a configuration which isn't currently supported in Oracle Integration 3, revert back to using the embedded database. See the note about reverting your database in Switch to a Different Oracle DB instance in *Administering Oracle Visual Builder in Oracle Integration 3*.
Integrations	Development team	Basic Routing Duplicate App Name	If your instance contains basic routing integrations that have the same source and target endpoint names, perform the following steps: 1. Edit your basic routing integration, delete the target endpoint, and add it again with a different name. 2. Save your integration.
Integrations	Development team	Number of Active Integrations	An instance can have a maximum of 700 active integrations, as specified in the service limits. If you have more than 700 active integrations, reduce the number, such as by deactivating or remodeling integrations.
Integrations	Development team	Multiple Read File	The Read Multiple File operation was deprecated in Oracle Integration Generation 2. If you have integrations that include an operation to read multiple files, rework the integrations so that they don't use this pattern. For example, use a listFile operation to list the files, and use a for-each action to read each file individually.
Integrations	Development team	Legacy Stage File action in integrations	If your instance includes integrations that have legacy stage file actions from versions prior to Oracle Integration Generation 2, the upgrade eligibility check identifies the integration code and version. For each integration, update all stage file actions: 1. Edit the integration. 2. For each stage file action: a. Edit the stage file action. b. Click **Next** at each screen. c. At the last screen, click **Done**. 3. Save the integration.
Integrations	Development team	API calls in Visual Builder application	If you created Visual Builder applications by creating a service connection from the catalog and they call REST APIs other than Integrations REST Endpoints, you must rewrite the applications by creating a service connection from the catalog, and the applications must use Oauth to authenticate.
Adapters	Development team	Custom Adapter	If your instance includes integrations that use a custom adapter, the instance can't be upgraded yet. Wait until Oracle starts upgrades for this capability.

Area	Typical owner	Eligibility condition	Tasks to Complete
Adapters	Development team	Microsoft adapters	Microsoft decommissioned the Microsoft Outlook REST APIs in November 2022. If you use any of the following adapters, you must use the Microsoft Graph REST APIs instead. • Microsoft Office 365 Calendar Adapter • Microsoft Office 365 People Adapter • Microsoft Office 365 Outlook Adapter See: • Invoke Operations Page in *Using the Microsoft Office 365 Calendar Adapter with Oracle Integration 3* • Invoke Operations Page in *Using the Microsoft Office 365 People Adapter with Oracle Integration 3* • Invoke Operations Page in *Using the Microsoft Office 365 Outlook Adapter with Oracle Integration 3*
Adapters	Development team	Unsupported Adapters	If your instance includes an integration that uses one of the following adapters, which aren't supported in Oracle Integration 3, replace the adapters with the REST adapter: • Automation Anywhere Adapter • Evernote Adapter • Oracle Messaging Cloud Service Adapter • Oracle Monetization Cloud Adapter • Oracle Taleo Business Edition (TBE) Adapter • UiPath Robotic Process Automation Adapter
Adapters	Development team	Unsupported REST Types - REST Adapter	The following connection types are deprecated and not supported in a REST Adapter connection. Replace these connection types with different connection types. See Configure Connection Properties for Invoke Connections in *Using the REST Adapter with Oracle Integration 3*. • Metadata Catalog URL • Swagger Definition URL • RAML Definition URL Developers with a REST API that is described using RAML or the Oracle metadata catalog must take the following action: 1. Consult your REST service provider and ask for a Swagger definition (if available). Oracle Fusion Applications should have a Swagger option available. This is a guideline for all Oracle Fusion Applications. 2. If an alternative spec is not available, use the basic template in the REST Adapter by selecting REST API Base URL as the connection URL and defining the target API request using the Adapter Endpoint Configuration Wizard. Another option is to convert RAML into an OpenAPI specification to use with the REST Adapter connection. To provide more robust and complete support for the Swagger/OpenAPI specifications, the REST Adapter includes a unified option to specify all OpenAPI specifications in a single field. This option also replaces the option to provide a Swagger definition URL, which is no longer available.

Area	Typical owner	Eligibility condition	Tasks to Complete
Process Automation	Administrator	Process Automation	If you use the Processes capability but aren't using it in production, you have the option to skip process applications during upgrade. This approach is appropriate if you've tried Processes in non-production Oracle Integration Generation 2 environments but don't need or want to retain it in Oracle Integration 3. **Note:** • If you have process in production, wait until Processes upgrade is supported. • Importing process applications created in Oracle Integration Generation 2 into Oracle Integration 3 isn't currently supported. To skip process applications and move forward with upgrade, you must perform the following steps, which differ depending on your deployment. More than one situation might apply to your deployment. • **If you don't have any process runtime transactions:** The option to skip process applications is shown and is available. 1. If you want to keep your process applications to later be used in Oracle Integration 3, export your process applications. 2. When scheduling and configuring upgrade, select **Upgrade and lose process applications and runtime data**. 3. After upgrade, if you want to leverage process or decision capabilities, you can enable Process Automation with Oracle Integration 3. • **If you have process runtime transactions:** The option to skip process applications is shown but is unavailable. 1. Deactivate all your process applications. 2. Schedule an archive and purge of process applications to get rid of completed and stale structured process instances. Set **Purge Retention (Days)** to `0`. Wait 24 hours, then recheck upgrade eligibility as described above. 3. While you're waiting to recheck upgrade eligibility, export your process applications to later be used in Oracle Integration 3.

Area	Typical owner	Eligibility condition	Tasks to Complete
			Note: Importing process applications created in Oracle Integration Generation 2 into Oracle Integration 3 isn't currently supported. 4. After deactivating deployed applications, purging runtime data, and rechecking upgrade eligibility, the option to skip process applications should be available. When scheduling and configuring upgrade, select **Upgrade and lose process applications and runtime data**. 5. After upgrade, if you want to leverage process or decision capabilities, you can enable Process Automation with Oracle Integration 3. • **If you are calling Process from any integrations:** You must remove the process action from the integration in order to pass the upgrade eligibility check for Process. After the upgrade, if you need an integration to call Process, you can use the REST adapter to do so. • **If you are calling Process from any Visual Builder applications:** You must remove any references to process applications from your Visual Builder applications.
Insight	Administrator	Insight	Insight isn't supported in Oracle Integration 3. You can't use Insight in Oracle Integration 3. Use Oracle Cloud Infrastructure Logging Analytics and Process Automation Analytics.

2. Schedule the Upgrade and Configure Settings

Your instance is ready for upgrade after you complete all prerequisites and the instance passes the upgrade check. Oracle sends you an email indicating that your instance is ready for upgrade. Oracle selects an upgrade window, but you can change it if the upgrade is more than seven business days away (detailed below).

After you receive the email, you configure upgrade settings and can reschedule the upgrade, if needed. Complete these steps after Oracle sends your scheduled upgrade date over email.

Prerequisites:

- If any upgrade checks fail, address the issues that apply to your instance, or the instance won't be scheduled for upgrade. For instructions on how to fix failed upgrade checks, see Complete Upgrade Prerequisites.
- If you haven't received an email and want to schedule your upgrade, you can enter a service request. For additional information, see How do I submit an upgrade request?.
- Only people who are part of the `ServiceAdministrator` group can perform these tasks. See Create an IAM Policy in an Identity Domain for tenancies that use identity domains or Create an IAM Policy for tenancies that do not use identity domains.

Steps:

1. Once your instance has passed the upgrade check, wait for Oracle to inform you that your upgrade has been scheduled.

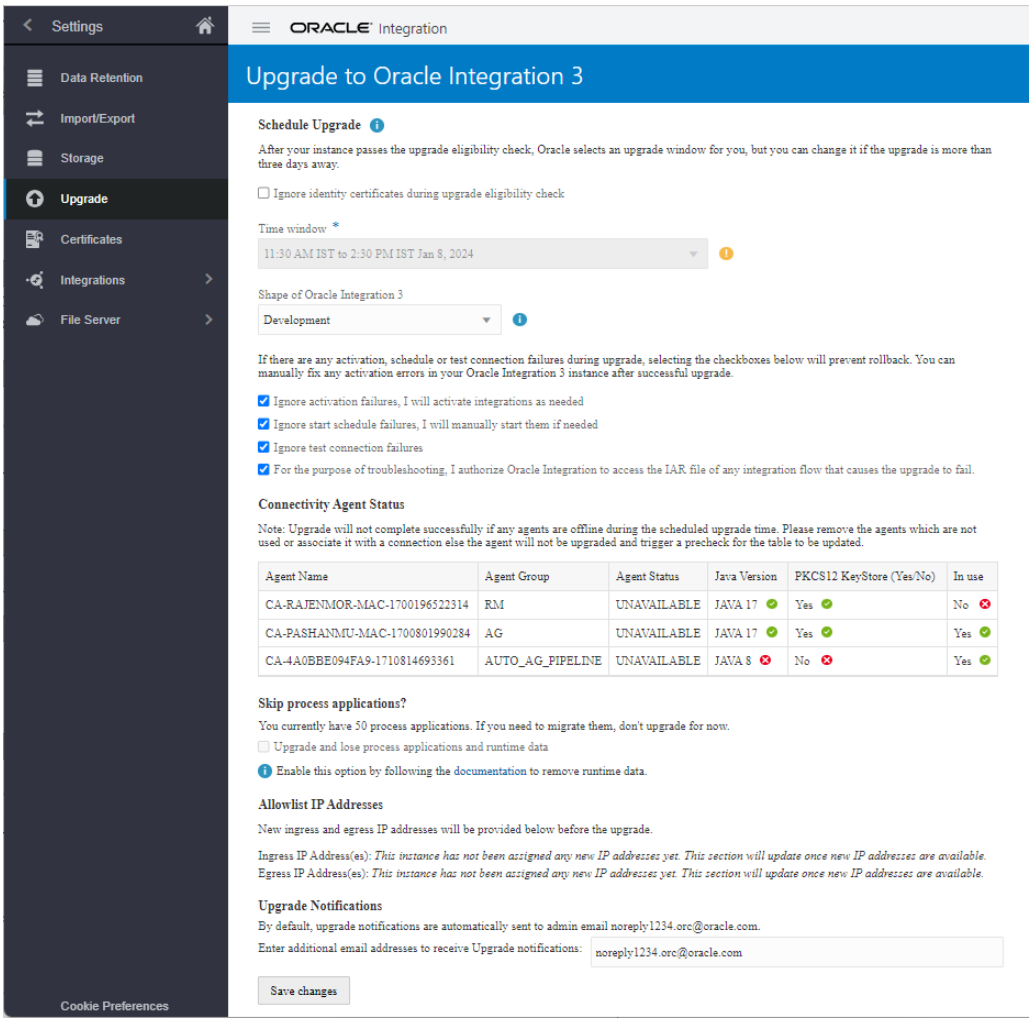
   Oracle informs you that your instance is ready for upgrade in the following ways:

- Click **Settings**, then click **Upgrade** to see your upgrade window.
- An announcement appears in the interface.
  You can see the announcement if you're part of an administrator group.
- Oracle sends an email, informing you that you're eligible for upgrade.
  Everyone who gets emails about Oracle Integration Generation 2 quarterly updates receives the email.

2. Review your upgrade window, change it if needed, and specify your requirements for the upgrade:

   a. In Oracle Integration, open the **Upgrade** page using one of the following methods:

      - In the navigation pane, click **Settings**, then **Upgrade**.
      - Click **Announcements** , and then click the link in the notification.



   b. On the Upgrade page, fill in the fields.

Field	Description
Ignore identity certificates during upgrade eligibility check	When selected, the upgrade proceeds, even if the instance contains connections that use identity certificates. After the upgrade, you'll need to upload new identity certificates into your Oracle Integration 3 instance, test the connections that use the identity certificate so their status changes from Draft to Configured, and activate any integrations that use the connections. If you do not select this field, the upgrade cannot proceed unless you manually delete the identity certificates.
Upgrade Window	If your upgrade has been scheduled, you see your upgrade window. You can change your upgrade window if it's seven or more business days away. All upgrade dates that are available to you appear in the list. If you have multiple instances, choose your upgrade windows carefully. See Prerequisites When You Have Multiple Instances. **Note:** Does your organization restrict access to the Oracle Integration Generation 2 instance based on the OCID value that uniquely identifies your instance? If so, consult the IAM policy administrator before scheduling the upgrade. The Oracle Integration 3 instance has a different OCID than the Oracle Integration Generation 2 instance. After the upgrade, the IAM policy administrator must update the IAM policy so that it refers to the Oracle Integration 3 OCID. People can sign in only after this work is complete. Make sure the upgrade window is during a time when the IAM policy administrator is available to update the policy. For information about updating the IAM policy, see About IAM Policies for Oracle Integration and Creating an IAM Policy.
Shape of Oracle Integration 3	The shape determines when the instance receives updates. The shape you select determines the upgrade time windows that are available. • **Development**: Instances with this shape are updated two weeks before instances with a Production shape. • **Production**: Instances with this shape receive updates two weeks after instances with a Development shape. When you select Production and click **Confirm** to schedule your upgrade, you'll be prompted to confirm again that you want to upgrade your production instance and that you are satisfied with the testing you have done on your Development instances. You can't change the shape after the instance has been assigned an ingress or egress IP address. If the shape is not correct and you're unable to change it, submit a service request (SR) on My Oracle Support. **Note:** You can't change the shape after the upgrade is complete. However, you can move data to another instance using the export and import capabilities.

Field	Description
Ignore activation failures, I will activate integrations as needed	Determine whether to roll back your upgrade if Oracle isn't able to activate all of your integrations in Oracle Integration 3. • When selected, if Oracle can't activate one or more integrations, the upgrade proceeds. If you select this option, plan to check the status of all your integrations after the upgrade finishes and activate integrations as needed. • When deselected, if Oracle can't activate one or more integrations, Oracle rolls back the upgrade. After the rollback, you continue working in the Oracle Integration Generation 2 instance. Oracle will schedule another upgrade in the future.
Ignore start schedule failures, I will manually start them if needed	Determine whether to roll back your upgrade if Oracle isn't able to start the schedule for an integration. • When selected, if Oracle can't start the schedule on one or more scheduled integrations, the upgrade proceeds. If you select this option, plan to check the schedules of your integrations after the upgrade, and manually start them if needed. • When deselected, if Oracle can't start the schedule on one or more scheduled integrations, Oracle rolls back the upgrade. After the rollback, you continue working in the Oracle Integration Generation 2 instance and can schedule another upgrade in the future.
Ignore test connection failures	Select this option to continue with the upgrade, even if connections don't pass testing in Oracle Integration 3 after the upgrade. If you deselect this option, the upgrade is rolled back after a connection doesn't pass testing in Oracle Integration 3. Oracle recommends selecting this checkbox and addressing any connection failures after the upgrade.
For the purpose of troubleshooting, I authorize Oracle Integration to access the IAR file of any integration flow that causes the upgrade to fail	If you select this option, should the upgrade fail, Oracle Integration Generation 2 saves the integration IAR file that caused the failure. This reduces the time required for troubleshooting when you contact Technical Support.

Field	Description
Connectivity Agent Status	The Connectivity Agent Status section shows the status of all the connectivity agents in your instance: • **Agent Name**: Shows the name of the agent. • **Agent Group**: Shows the agent group that the agent is associated with. • **Agent Status**: Your connectivity agents must be up and running before the upgrade of your connectivity agent begins or the upgrade will fail. For any agents that are failing this precheck, make sure that they're available before upgrade begins. • **Java Version**: The servers that host your connectivity agents must use JDK 17 or the upgrade of those connectivity agents will fail. For any agents that are failing this precheck, install JDK 17. • **PKCS12 KeyStore**: The servers that host your connectivity agents must use PKCS12 KeyStore. If your agents use JDK 17, your JKS KeyStores will automatically be converted to the PKCS12 KeyStore during upgrade. • **In use**: If an agent is marked as not in use it means it either isn't used in any connections or there hasn't been any recent traffic from the agent (agent-level messages). If an agent isn't in use it won't cause your upgrade to fail. However, you might want to consider removing unused agents. **Caution:** *Before* upgrade, you must update your allowlist settings to configure connectivity from your connectivity agents to Oracle Identity Cloud Service (IDCS) and the Oracle Integration runtime URL and IP addresses. Perform the following updates: • Add the URL for Oracle Identity Cloud Service (IDCS) to the allowlist. • Add the runtime URL and IP addresses for Oracle Integration to the allowlist. • Set the proxy server's Cache property for the Oracle Integration URLs to refresh as frequently as possible. If any of your agents are offline during upgrade or don't meet upgrade requirements, they won't be upgraded. You'll need to perform post-upgrade steps to regain connectivity.

Field	Description
Skip process applications?	If you use the Processes capability but aren't using it in production, you have the option to skip process applications during upgrade. This approach is appropriate if you've tried Processes in non-production Oracle Integration Generation 2 environments but don't need or want to retain it in Oracle Integration 3. If you want to proceed with the upgrade, select **Upgrade and lose process applications and runtime data**. **Note:** • If you see the option to skip process applications, but it's unavailable, you have process runtime transactions. If you want to proceed with upgrade at this time, export your process applications and remove your runtime transactions, as described in Complete Upgrade Prerequisites. • If you have process in production, wait until Processes upgrade is supported. • Importing process applications created in Oracle Integration Generation 2 into Oracle Integration 3 isn't currently supported. After upgrade, if you want to leverage process or decision capabilities, you can enable Process Automation with Oracle Integration 3.
Allowlist IP Addresses	Two weeks before the upgrade, the ingress and egress IP addresses are available: • **Ingress IP Address(es):** IP addresses for traffic entering into Oracle Integration 3. • **Egress IP Address(es):** IP addresses for traffic exiting Oracle Integration 3. You'll need these values to update your allowlists for your firewall and the server that hosts your connectivity agent. To copy an IP address, click next to the address.
Upgrade Notifications	By default, upgrade notifications are automatically sent to the listed admin email. Enter the email addresses of any additional stakeholders who should receive communications about the upgrade. Separate multiple email addresses using a comma (,). Oracle includes the stakeholders in all future communications for the upgrade.

c. Click **Save changes**.

3. If you selected a different upgrade window, wait for the email that confirms that your requested window is available.

   Oracle emails a confirmation of the upgrade window that you selected. Everyone who gets emails about Oracle Integration Generation 2 quarterly updates receives the email.

4. Inform users and stakeholders about the upcoming upgrade.

   For example, consider completing the following tasks:

   - Share the date of the upgrade.
   - Ask everyone to limit their development work starting two days before the upgrade, if possible.
     If teams can't pause their work, the upgrade continues as planned. But, limiting your work can help ensure a successful upgrade.
   - Tell everyone to expect downtime during the upgrade window.
   - Plan and assign the tasks to complete before and after the upgrade.
     See 3. Update Allowlists and Complete Pre-Upgrade Tasks and 5. Complete Post-Upgrade Tasks.

If you rescheduled your upgrade, Oracle sends an email confirmation for the new date and time.
Two weeks before your upgrade date, Oracle shares your new ingress IP address(es). Use the values to update your allowlists. See 3. Update Allowlists and Complete Pre-Upgrade Tasks.
Three days before your upgrade date, Oracle locks your upgrade window.

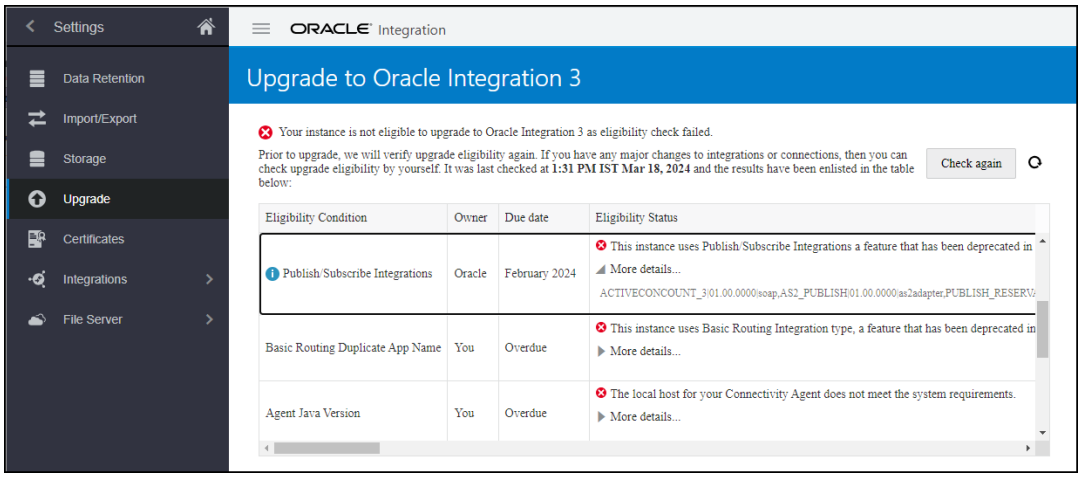
Correct an Instance with Failed Eligibility Checks

If your upgrade was scheduled and your instance is no longer ready for upgrade, address the findings so that your upgrade can continue as scheduled.

> **Note:**
>
> For details about features and capabilities that aren't ready for upgrade yet, see Instances That Cannot Be Upgraded Yet.

1. In Oracle Integration, open the Upgrade page using one of the following steps:
   - In the navigation pane, click **Settings**, then **Upgrade**.
   - Click **Announcements** , and then click the link in the notification.

   The Upgrade page appears.



2. Review the checks that didn't pass, and take the appropriate action. See Complete Upgrade Prerequisites for steps to take.
3. After addressing all items in the to-do list, check the instance again.
   a. In the navigation pane, click **Settings**, then **Upgrade**.
   b. Click **Check again**.
   c. Wait for the check to complete.

      The check usually finishes in just a few minutes.
   d. Continue making corrections until the check passes.

      If you aren't sure how to correct an issue, enter a service request.
4. Proceed with the upgrade as scheduled.

3. Update Allowlists and Complete Pre-Upgrade Tasks

There are several tasks you must complete as your upgrade date approaches to prevent errors during upgrade and to allow you to smoothly transition to the new Oracle Integration 3 instance after upgrade.

After your upgrade has been scheduled, complete the following steps.

1. **If you use B2B for Oracle Integration: Ensure that all passwords for the keystore file are identical.**
   Your identity certificate file (JKS) requires two sets of passwords: Key Password(s) and Keystore Password. All the passwords must be identical. If they're not, re-upload the keystore file and use identical passwords for all the key and keystore passwords.

   If you don't have the keystore file that was last uploaded and cannot locate it, recreate the file.

   See Upload an SSL Certificate in *Using Integrations in Oracle Integration Generation 2*. When uploading the certificate, for **Type**, select **X.509 (SSL Transport)**. For **Category**, select **Identity**.

   > **Caution:**
   >
   > If you don't complete this step, the upgrade will fail.

2. **Everyone: Add the IP addresses and URLs for the new instances to your allowlists.**
   If your organization uses allowlists, you must add the Oracle Integration 3 IP addresses to the allowlist before upgrade to prevent errors.

   a. **Get the new IP addresses:**
      The new IP addresses appear on the **Upgrade** page two weeks before your upgrade.

      i. In the navigation pane, click **Settings**, then **Upgrade**.

      ii. Find the values next to **New IP addresses**.

      iii. To copy an IP address, click next to the address.

   b. **Get the new URLs:**

      - Runtime URL for Oracle Integration—This is the same as your existing Oracle Integration Generation 2 runtime URL.
      - Oracle Identity Cloud Service (IDCS) URL—This is the URL you use to sign into Oracle Integration.

   c. **Update your allowlists according to your organization's procedures:**
      For example, you may use the following types of allowlists with Oracle Integration.

Type of allowlisting	Next steps
Control who accesses an Oracle Integration instance	None. Oracle migrates your existing access allowlists (also known as access control lists, or ACLs) as part of the upgrade.

Type of allowlisting	Next steps
Allow egress from your network to Oracle Integration	Add the new **ingress IP address** for Oracle Integration to the allowlist. Find the IP address on the Upgrade page two weeks prior to the upgrade.
Control access to your cloud systems	None. Controlling access to your cloud systems by adding the egress IP address for Oracle Integration to every service that Oracle Integration accesses is not currently supported in Oracle Integration 3.
Allowlist public IP addresses for File Server	None. Oracle updates these allowlists for you.
Allowlist IP addresses and URLs for your connectivity agents	Configure connectivity from your connectivity agents to IDCS and the Oracle Integration runtime URL and IP addresses. Add the following to the allowlists for the servers that host your connectivity agents: • The runtime URL for Oracle Integration • The **ingress IP address** for Oracle Integration • The URL for IDCS

> **Caution:**
>
> If you update allowlists before the upgrade, don't remove the IP address(es) for Oracle Integration Generation 2 yet. You might experience errors. After the upgrade finishes, the Oracle Integration Generation 2 IP addresses are no longer assigned to you.

3. **Everyone: Set your proxy server's Cache property for the Oracle Integration URLs to refresh as frequently as possible.**
   For example, if your proxy server uses the `Cache-ExpiresDefault` property, set it to `now`.

4. **Everyone: Determine whether you're relying on the instance ID for the Oracle Integration Generation 2 instance being an integer.**
   For example, if you store the instance ID in a database as a number field, you'll need to update the database field. The instance ID for Oracle Integration 3 is a string value.

   Update your systems and processes as required.

5. **Everyone: Decide what to do with asynchronous messages from the client side for the duration of the downtime.**
   Here's why: During the downtime, Oracle Integration rejects all incoming requests. To prepare, you have the following options:

   - Before the upgrade starts, suspend all asynchronous messages on the client side. With this approach, the client doesn't send the messages, and Oracle Integration doesn't reject them.

     If you choose this option, make sure you know the start and end times of the upgrade.

   - After the upgrade finishes, determine the appropriate next steps for the rejected messages.

6. **Everyone: If you don't already, start capturing the activity stream in Oracle Cloud Infrastructure Console.**
   Here's why: The activity stream isn't migrated. But if you capture this data in the Oracle Cloud Infrastructure Console, you'll still have access to historical data. See Capture the Activity Stream in Oracle Cloud Infrastructure Console.

Next, plan to limit or pause your development work during the days leading up to the upgrade. See Limit Development Work Before the Upgrade.

4. Upgrade to Oracle Integration 3

Leading up to the upgrade, you should limit your development work. Learn what to expect during the upgrade.

Topics:

- Limit Development Work Before the Upgrade
- Wait for the Upgrade to Complete

Limit Development Work Before the Upgrade

In the days and hours leading up to the upgrade, limiting your work in Oracle Integration Generation 2 can help ensure a successful upgrade. You'll receive an email reminder to pause your development work two days before the upgrade.

Everyone who gets emails about Oracle Integration Generation 2 quarterly updates receives email reminders about pausing work. Forward the emails as needed so that all stakeholders are informed.

Make sure you also complete all required tasks before the upgrade. See 3. Update Allowlists and Complete Pre-Upgrade Tasks.

During the two days leading up to the upgrade, Oracle completes the following tasks:

- Exports data from your Oracle Integration Generation 2 instance.
- Creates an Oracle Integration 3 instance in your existing tenancy.
- Imports Oracle Integration Generation 2 data into your new instance.

Runtime traffic continues to be routed to your Oracle Integration Generation 2 instance.

1. **During the two days leading up to the upgrade:** Pause or limit your development work as much as possible.

   Any changes that you make are saved, but they might cause the upgrade check to fail. In such cases, the upgrade would need to be rescheduled. For example:

   - Don't add metadata.
   - Don't create integrations.
   - Don't activate integrations.
   - Resubmit any failed integration instances.
     When you chose your upgrade window, you specified whether to upgrade even if you have one or more failed integration instances. If you chose not to upgrade and an integration instance fails, your upgrade will be postponed.

2. **One to two hours before the upgrade:**

   - If you can, avoid starting any long-running asynchronous integrations.
   - Check again for any failed integration instances, and resubmit them.

     If the instance contains any failed integration instances, recover them. If you don't need them anymore, you can also delete them.
   - Limit your work as much as possible.

For instance, try to limit your activation and deactivation work.

- Make sure that the connectivity agent is up and running.

  In Oracle Integration Generation 2, the connectivity agent uses basic authorization to invoke Oracle Integration endpoints. During the upgrade, the connectivity agent is automatically converted from using basic authentication to using OAuth 2.0 token-based authentication to invoke Oracle Integration endpoints. All connections are automatically upgraded to OAuth 2.0, so you don't need to manually recreate any connections yourself.

3. **Fifteen minutes before the upgrade:** Don't perform any business-critical tasks in Oracle Integration Generation 2.

> **Note:**
>
> Oracle recommends that you do not stop your scheduled integrations prior to upgrade. If you stop integrations in your instance, the integrations remain stopped in the instance after the upgrade is complete, and you'll have to manually restart everything.

4. **At least one minute before the upgrade:** Everyone should stop working in Oracle Integration Generation 2 and sign out.

Next, on upgrade day, you need to wait for the upgrade to finish and then perform the post-upgrade tasks. See Wait for the Upgrade to Complete.

Wait for the Upgrade to Complete

The upgrade takes less than ten minutes. During this time, Oracle Integration Generation 2 is unavailable.

Prior to the upgrade, pause development work if you can. See Limit Development Work Before the Upgrade.

1. **On the day of the upgrade:** Make sure everyone stops work in Oracle Integration Generation 2 before the beginning of the upgrade window.
2. **When the upgrade begins:** Oracle sends an email when the upgrade begins. Everyone who gets emails about Oracle Integration Generation 2 quarterly updates receives the email.
3. **Wait for the upgrade to complete:** If you sign in during the downtime, a message appears, indicating that the instance is temporarily unavailable.

   During the downtime, Oracle completes the following tasks:

   a. Checks to make sure that the instance is still ready for upgrade.
      For example, you might begin using a deprecated feature after your instance passes the upgrade check. In such a case, your instance is no longer ready for upgrade. Oracle emails you to inform you that everyone will continue working in the Oracle Integration Generation 2 and provides the next steps.
   b. Stops the scheduled integrations in the Oracle Integration Generation 2 instance.
   c. Stops all activity, including design time and runtime, in the instance.
      If a scheduled integration is running in Oracle Integration Generation 2, the integration starts where it left off in Oracle Integration 3.
   d. Moves data to the new instance.

The data that is moved includes integrations, connections, packages, certificates, settings, and other metadata, plus in-flight instance data. See How Upgrade Affects Runtime Data.

e. Updates the hostname of the Oracle Integration Generation 2 instance.
The hostname points to the new Oracle Integration 3 instance. This change ensures that requests are sent to your new Oracle Integration 3 instance after the upgrade.

f. Creates a mapping between the Oracle Identity Cloud Service and the new instance. This mapping ensures that security-related information from your Oracle Integration Generation 2 instance is present in your Oracle Integration 3 instance.

g. Starts the scheduled integrations in the Oracle Integration 3 instance.

> **Note:**
>
> For integrations that use three-legged OAuth 2.0, the redirect URIs that you specified for client applications do not change after upgrade, even though your instance gets a new URL. Additionally, when you need to register a new client application after the upgrade is complete, you must use the Oracle Integration Generation 2 redirect URI.

4. **After the upgrade finishes:** The Oracle Integration 3 instance starts processing all requests, and Oracle sends an email saying that the upgrade is complete.

> **Note:**
>
> In rare situations, an issue prevents an upgrade from completing. When an upgrade doesn't complete, Oracle rolls back the changes, turns on the schedule in the Oracle Integration Generation 2 instance, and restores your access to the instance during the downtime period. You continue working in the Oracle Integration Generation 2 instance, with the same features and capabilities you were using before the upgrade.
> In such situations, Oracle sends an email that you can continue working in Oracle Integration Generation 2. Expect the email to arrive either within your upgrade window or soon after. Everyone who gets emails about Oracle Integration Generation 2 quarterly updates receives the email. You can schedule your upgrade for another time, and Oracle works with you to determine the next steps.

Next, complete all required tasks. See 5. Complete Post-Upgrade Tasks.

5. Complete Post-Upgrade Tasks

Oracle upgrades your Oracle Integration Generation 2 development instances first. Complete all post-upgrade tasks within three days of the upgrade date, so that you can report any issues. Oracle upgrades your production instances about two weeks after your development instances.

Completing post-upgrade tasks is critical to make sure users can access the new instance, data going to and from integrations can be sent through the firewall, and integrations work as expected.

If you experience any issues after the upgrade, enter a service request (SR) on My Oracle Support or troubleshoot the issues. See Troubleshoot Upgrade Issues.

> **Note:**
>
> You'll see your stopped Oracle Integration Generation 2 instance in the Oracle Cloud Infrastructure Console for a period of time after the upgrade. Do not update, start, or delete this instance. Oracle removes it on your behalf when it is no longer needed.

Make sure the upgrade has completed before starting these tasks. See Wait for the Upgrade to Complete.

Summary of Post-Upgrade Tasks

Impact	When	Tasks to complete
Ensure access to the instance	Immediately after upgrade	1. Check the new Oracle Integration 3 instance 2. Update the IAM policy with the new OCID 3. Configure an IAM policy for Visual Builder 4. Configure the Oracle Integration 3 allowlist with the Visual Builder service VCN OCID 5. Get the URL for the new instance and share it
Ensure connectivity	Immediately after upgrade	1. Complete network rules configuration 2. Upload a new identity certificate for connections 3. File Server: update integrations and SFTP clients to use the new IP and port values Complete this task within one week of upgrade. 4. Regain connectivity with agents that weren't upgraded
Ensure integrations work	Immediately after upgrade	1. Change REST API calls from Basic Authentication to OAuth 2. Check integrations if you selected Ignore activation failures or Ignore start schedule failures
Follow your organization's procedures	Within two weeks of upgrade	Complete your organization's post-upgrade verification tasks

Ensure access to the instance

Task	Who	When	Tasks to complete
Check the new Oracle Integration 3 instance	Administrator	Immediately after upgrade	Sign in to your Oracle Integration 3 instance using your existing credentials. Your Oracle Integration 3 instance is in the same compartment and region as your Oracle Integration Generation 2 instance. Use your existing Oracle Integration Generation 2 bookmark(which redirects to the new URL) or use the new URL for the Oracle Integration 3 instance. See Access an Oracle Integration Instance. The upgrade completed if: • You sign in and the user interface is different from Oracle Integration Generation 2. Check the version number in the About dialog. The upgrade is still in progress if: • You sign in and the user interface is the same as in Oracle Integration Generation 2. • You sign in and a page indicates that the service is unavailable.
Update the IAM policy with the new OCID	IAM policy administrator	Immediately after upgrade	If your organization restricts access to the Oracle Integration Generation 2 instance based on the OCID value that uniquely identifies your instance, update the IAM policy so that it points to the new Oracle Cloud ID (OCID) for the Oracle Integration 3 instance. **Caution:** If your IAM policy restricts access based on OCID, users will not be able to sign in until after you perform these steps. Find the new OCID in the Oracle Cloud Infrastructure Console after the upgrade is finished. For information about updating the IAM policy, see About IAM Policies for Oracle Integration and Creating an IAM Policy.
Configure an IAM policy for Visual Builder	Administrator	Immediately after upgrade	If you used Visual Builder in Oracle Integration Generation 2, you'll need to configure IAM policies for Visual Builder in Oracle Integration 3. See Set the IAM Policy for Managing the Visual Builder Instance for details.
Configure the Oracle Integration 3 allowlist with the Visual Builder *service* VCN OCID	Administrator	Immediately after upgrade	If you used Visual Builder and configured allowlist or network access rules in Oracle Integration Generation 2, you'll need to add the Visual Builder *service* VCN OCID in Oracle Integration 3. See Allow Your Instance to Access Services in *Administering Oracle Visual Builder Generation 2*.
Get the URL for the new instance and share it	Administrator	Immediately after upgrade	Get the URL for the new Oracle Integration 3 instance and share it with everyone who needs it. Existing bookmarks also redirect to the new URL, but you want to make sure everyone has the new URL. 1. Sign in to the Oracle Cloud Infrastructure Console. 2. Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Integration**. 3. Click the name of the new Oracle Integration 3 instance. 4. To the right of the **Service console URL** field, click **Copy**. 5. Share the URL with anyone who needs it.

Ensure connectivity

Task	Who	When	Tasks to complete
Complete network rules configuration	Network administrator	Immediately after upgrade	If required, complete any network rules configuration, including adding the Oracle Integration Service VCN as part of the network rule. This step is required if you use an Oracle Cloud Infrastructure service that supports network rules as a target of an integration connection, such as Oracle Cloud Infrastructure Object Storage or Oracle Autonomous Database, and you have enabled the network rules. 1. Sign in to Oracle Cloud Infrastructure Console. 2. Get the OCID value for the Oracle Integration 3 instance. See Viewing Instance Details. 3. Follow the rules for your target service, such as Configure Access Control Lists When You Provision or Clone an Instance in *Using Oracle Autonomous Database Serverless*. 4. If the Oracle Cloud Infrastructure service you are accessing is in a different region than your Oracle Integration instance, allowlist the egress IP address.
Upload a new identity certificate for connections	Developer with connections that use identity certificates	Immediately after upgrade	Upload a new identity certificate, test the connections that use the identity certificate so their status changes from Draft to Configured, and activate any integrations that use the connections. Only one person from each organization needs to perform these steps, and only if you have connections that use identity certificates. 1. Upload a new identity certificate. See Upload an SSL Certificate in *Using Integrations in Oracle Integration 3*. 2. Test the connections that use the identity certificate so that their status changes from Draft to Configured. See Test the Connection in *Using Integrations in Oracle Integration 3*. 3. Activate any integrations that use the connections. See Activate an Integration in *Using Integrations in Oracle Integration 3*.

Task	Who	When	Tasks to complete

Regain connectivity with agents that weren't upgraded	Developer with agents that weren't upgraded	Immediately after upgrade	Agents that are offline during upgrade or don't meet upgrade requirements won't be upgraded. After upgrade, if you see a message stating that some agents didn't meet upgrade eligibility and weren't upgraded, perform the following steps.
			Prerequisites
			Ensure connectivity from your connectivity agents to IDCS and the Oracle Integration 3 runtime and design-time IP addresses:
			• You should have added the Oracle Identity Cloud Service (IDCS) URL and the Oracle Integration 3 runtime IP address to the allowlists prior to upgrade, as described in 3. Update Allowlists and Complete Pre-Upgrade Tasks.
			• Add the Oracle Integration 3 design-time IP address to the allowlists. Use the following command to get the design-time IP address, replacing `region` with the region from your Oracle Integration 3 URL:
			`nslookup design.integration.region.ocp.oraclecloud.com`
			To regain connectivity with your agents:
			1. Stop the connectivity agent.
			2. Make sure that the agent prerequisites are complete:
			a. Ensure that the connectivity agent is using JDK 17. If it isn't, set the `JAVA_HOME` and `PATH` environment variables to `JDK17`.
			b. Ensure that the agent is using the PKCS12 KeyStore. If it isn't, convert it using the following steps.
			i. On the server that hosts the connectivity agent, create a backup of the `keystore.jks` file, which is located in the following folder: `Agent_Install_Location/agenthome/agent/cert`
			ii. Move the backup file to a different folder.
			iii. Convert the JKS KeyStore to the PKCS12 KeyStore by running the following command from the command line:
			`keytool -importkeystore -srckeystore keystore.jks -destkeystore keystore.p12 -srcstoretype JKS -deststoretype PKCS12 -deststorepass changeit -srcstorepass changeit`
			iv. Delete the `keystore.jks` file in the following location: `Agent_Install_Location/agenthome/agent/cert`
			3. Download the agent installer ZIP file from Oracle Integration 3.
			a. In the navigation pane, click **Design**, then **Agents**.
			b. Click **Download**, then **Connectivity agent**.
			4. Extract `oic_conn_agent_installer.zip` to a new directory on your connectivity agent server.
			5. Delete your existing connectivity agent `lib` folder under `Agent_Install_Location/agenthome/` and replace it with the `lib` folder from the ZIP file.
			6. Delete your existing `version` file under `Agent_Install_Location/agenthome/` and replace it with the `version` file from ZIP file.
			7. Delete your existing `connectivityagent.jar` file under `Agent_Install_Location` and replace it with the `connectivityagent.jar` file from ZIP file.

Task	Who	When	Tasks to complete
			8. Delete your existing `cpi_upgradeutility.jar` file under *`Agent_Install_Location`* and replace it with the `cpi_upgradeutility.jar` file from ZIP file. 9. In Oracle Integration 3, on the **Agents** page, hover over the agent group, click **Actions** ⋯, then select **Download config**. This step downloads a preconfigured `InstallerProfile.cfg` file for the agent group. 10. Delete your existing `InstallerProfile.cfg` file under *`Agent_Install_Location`* and replace it with the `InstallerProfile.cfg` file you downloaded in the previous step. 11. Restart the connectivity agent by running the following command: `java -jar connectivityagent.jar` 12. Reactivate the integrations that are in the upgraded agent group.
File Server: update integrations and SFTP clients to use the new IP and port values	File Server administrator and developer	Within one week of upgrade	If you use File Server, update your integrations and SFTP clients so that they use the new IP and port values. The Oracle Integration Generation 2 IP and port values continue working for four months after the upgrade, and then Oracle retires them. However, Oracle recommends updating your integrations and SFTP clients to use the new values now. That way, you don't risk forgetting to update these values in the future. 1. In the navigation pane, click **Settings**, then **File Server**, then **Settings**. 2. Under General, obtain the IP and port values for the File Server SFTP server. 3. Update all integrations that call File Server so that they use the new IP and port values. 4. Update all SFTP clients so that they use the new IP and port values.

Ensure integrations work

Task	Who	When	Details
Change REST API calls from Basic Authentication to OAuth	Developer	Immediately after upgrade	In Oracle Integration Generation 2, you can use Basic Authentication to use the Oracle Integration REST API and File Server REST API. In Oracle Integration 3, you must use OAuth. You'll need to update any clients, scripts, integrations and commands that use the Oracle Integration REST API or the File Server REST API to connect using OAuth. For more information on authentication method support, see When is Basic Auth Supported in Oracle Integration 3. For more details on using OAuth with the REST API, see Security, Authentication, and Authorization.
Check integrations if you selected **Ignore activation failures** or **Ignore start schedule failures**	Administrator	Immediately after upgrade	When you specified the upgrade requirements, if you opted to proceed with the upgrade even if Oracle couldn't activate an integration or restart a schedule, take the appropriate steps: • If you selected **Ignore activation failures**, check the status of all your integrations, and activate integrations as needed. • If you selected **Ignore start schedule failures**, check the schedules of your integrations, and manually start them if needed. For information about these settings, see 2. Schedule the Upgrade and Configure Settings.

Follow your organization's verification procedures

Task	Who	When	Details
Complete your organization's post-upgrade verification tasks	Designated team members	Within two weeks after upgrade	Complete your organization's post-upgrade verification tasks, such as performing regression testing. If needed, take action for requests that any clients sent to Oracle Integration during the downtime. Oracle Integration rejected all requests that were sent during the downtime.

Troubleshoot Upgrade Issues

Get help troubleshooting issues that might occur after the upgrade.

Connection errors

If you don't add the new IP addresses to your allowlists, issues occur after the upgrade. For example, If you don't add the new ingress IP address, errors occur in your applications.

If you experience other issues, enter a service request (SR) on My Oracle Support.

Oracle Integration Generation 2 instance is visible

Your stopped Oracle Integration Generation 2 instance appears in the Oracle Cloud Infrastructure Console for a period of time after the upgrade. Do not update, start, or delete this instance. Oracle removes it on your behalf when it is no longer needed.

Go back to your Oracle Integration Generation 2 instance

After the upgrade finishes, if you want to go back to using your Oracle Integration Generation 2, you must submit a service request (SR) through My Oracle Support.

Do not delete your new Oracle Integration 3 instance, and do not start your Oracle Integration Generation 2 instance on your own.

> **Note:**
>
> - Only Production instances can be rolled back.
> - You must submit your SR requesting roll-back within three business days of upgrade completion.
> - Your SR must include a reason that impacts your business.
> - It can take up to one hour to roll back an instance.

FTP Adapter connection fails after upgrade

If you configured the FTP Adapter to communicate with an SFTP server through the connectivity agent and selected the `diffie-hellman-group1-sha1` algorithm for the **SFTP Key Exchange Algorithm**, the integration that uses the FTP Adapter connection fails after the upgrade.

Update the connection, and on the Connections page, choose a different algorithm for **SFTP Key Exchange Algorithm**.

401 error when using the REST API

In Oracle Integration Generation 2, you can use Basic Authentication to use the Oracle Integration REST API and File Server REST API. In Oracle Integration 3, you must use OAuth. You'll need to update any clients, scripts, integrations and commands that use the Oracle Integration REST API or the File Server REST API to connect using OAuth. For more information on authentication method support, see When is Basic Auth Supported in Oracle Integration 3. For more details on using OAuth with the REST API, see Security, Authentication, and Authorization.

Connectivity agent upgrade fails

If the connectivity agent fails to upgrade, you can roll back the upgrade.

To roll back the connectivity agent upgrade from Oracle Integration 3 to Oracle Integration Generation 2:

1. Log on to your connectivity agent on-premises host.
2. Stop the connectivity agent.
3. Make a note of the previous connectivity agent version listed in `agenthome/backups/`.
4. Run each of the following commands to overwrite the current version binaries with those of the previous version. Replace *previous_version* in the commands with the actual version you noted in the previous step.

   ```
   cp agenthome/backups/previous_version/CpiAgent.properties.old agenthome/
   agent/config/CpiAgent.properties
   cp agenthome/backups/previous_version/agentstore.caks.old agenthome/agent/
   cert/agentstore.caks
   cp agenthome/backups/previous_version/InstallerProfile.cfg.old
   InstallerProfile.cfg
   cp agenthome/backups/previous_version/connectivityagent.jar.old
   connectivityagent.jar
   cp agenthome/backups/previous_version/version.old agenthome/version
   rm agenthome/lib/*
   cp agenthome/backups/previous_version/lib.old/* agenthome/lib/
   ```

5. Start the connectivity agent.

A

Oracle Integration 3 Reference

Topics:

- Manually Federate Your Tenancy
- Automate with Events

Manually Federate Your Tenancy

In certain cases, your tenancy may need user federation between Oracle Cloud Infrastructure's IAM and Oracle Identity Cloud Service (IDCS).

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

> **Note:**
>
> Follow the steps in this section ONLY if your tenancy is not already federated. See Is My Tenancy Federated Between Oracle Cloud Infrastructure IAM and Oracle Identity Cloud Service?

For additional instructions for manually federating with IDCS, see Federating with Oracle Identity Cloud Service in the Oracle Cloud Infrastructure documentation. The *Instructions for Federating with Oracle Identity Cloud Service* section lists four main steps. However, step 1 differs for Oracle Integration: Instead of accessing client ID/secret information from a COMPUTEBAREMETAL IDCS application, you'll create an IDCS application to generate this information for federation, as described here.

- Is My Tenancy Federated Between Oracle Cloud Infrastructure IAM and Oracle Identity Cloud Service?
- Get Required Information from Oracle Identity Cloud Service
- Add Oracle Identity Cloud Service as an Identity Provider

Is My Tenancy Federated Between Oracle Cloud Infrastructure IAM and Oracle Identity Cloud Service?

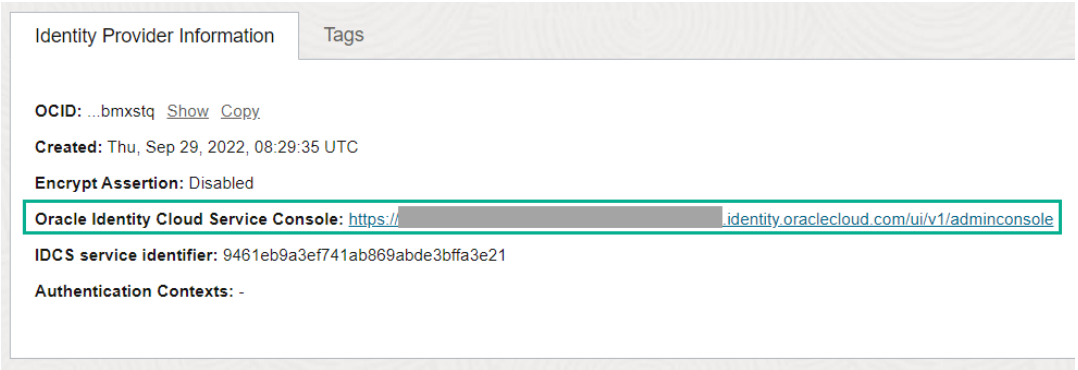
Oracle Integration requires that Oracle Cloud Infrastructure Identity and Access Management (IAM) be federated with Oracle Identity Cloud Service (IDCS) for your tenancy.

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

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Federation**.
2. On the Federation page, look for an **Oracle Identity Cloud Service** link.

The Federation page is shown. Its **Identity Provider Information** tab identifies the default federation configured between the Oracle Identity Cloud Service stripe and the Oracle Cloud Infrastructure tenancy in a tenancy. Note that this page may show more than the default identity provider.

If you see a console link, your instance is federated. If it's not, perform the steps in Manually Federate Your Tenancy.



Get Required Information from Oracle Identity Cloud Service

Follow these steps to create and configure an Oracle Identity Cloud Service application, activate the application, and create an IDCS administrator group.

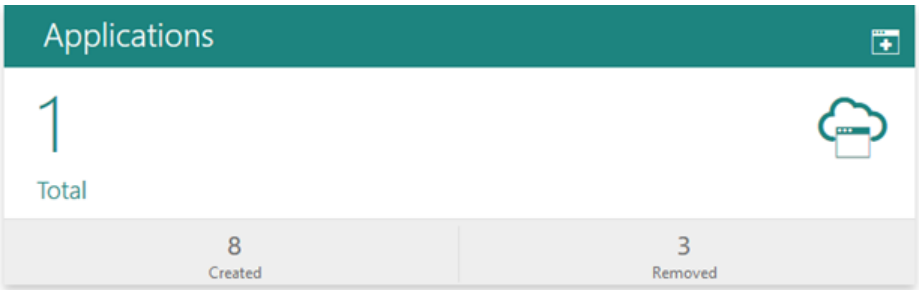
This topic applies only to tenancies that do not use identity domains. See Differences Between Tenancies With and Without Identity Domains.

> **Note:**
>
> Follow the steps in this section only if manual federation is needed.

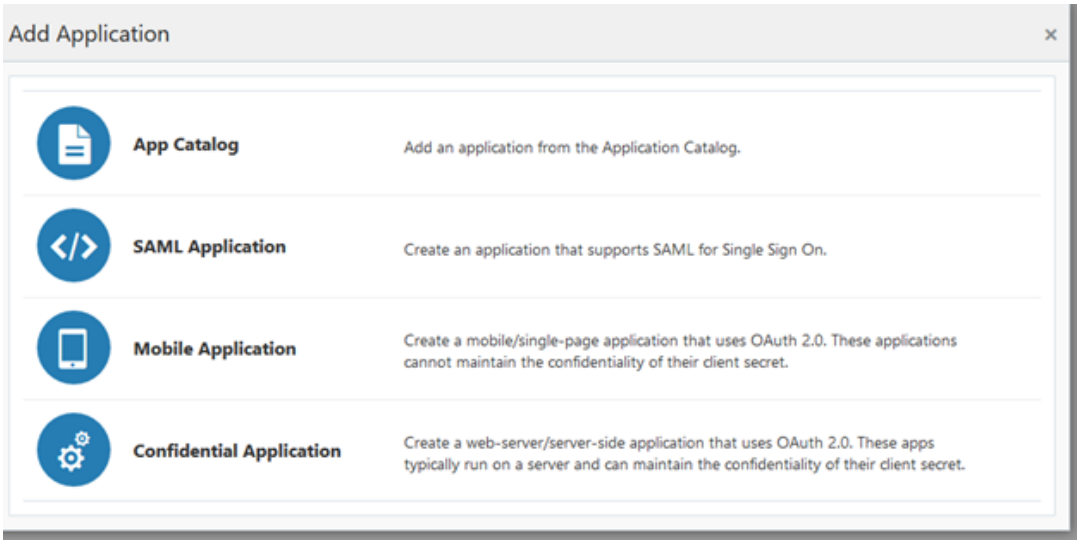
1. Sign in to Oracle Identity Cloud Service with admin privileges. You must be viewing the admin console.

   Use the link, username, and password provided in your account welcome email.

2. Select **Applications**.



3. Click **Add**.
4. Select **Confidential Application**.

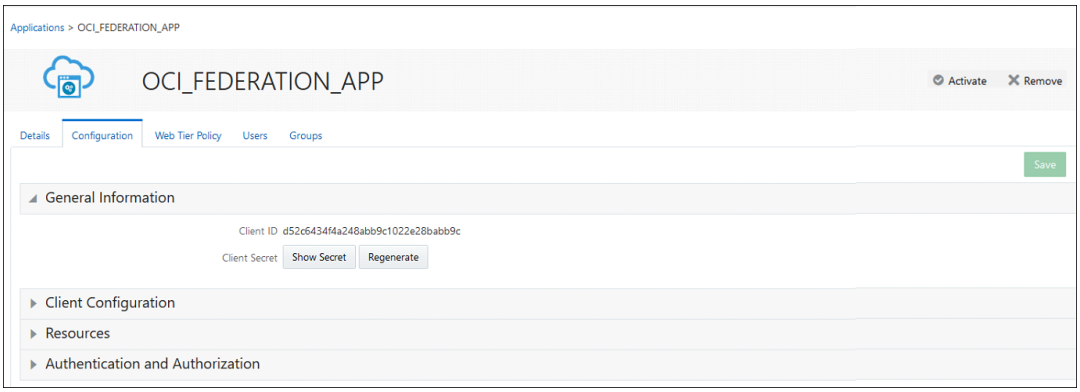


The Add Confidential Application page is displayed.

5. In the **Name** field under **App Details**, enter a name (such as `Oracle Cloud Infrastructure Federation`). Click **Next**.

   Client options are displayed.

6. Under **Authorization**, select **Client Credentials**.
7. Under **Token Issuance Policy**, click **+Add** by App Roles. Select **Identity Domain Administrator**. Click **Next**.
8. Click **Next** to skip the **Resources** options.
9. Click **Next** to skip the **Web Tier Policy** options.
10. Click **Finish**.



The application's **Client Id** and **Secret** are displayed.

11. Copy the **Client Id** and **Secret** for use later (in Add Oracle Identity Cloud Service as an Identity Provider). Close the window.
12. Activate the app by selecting **Activate** in the upper right corner.
13. Create an IDCS group for administrators. Make sure the federated user you plan to test federation with is part of that group.

a. Select **Groups** from the **Resources** options.

b. Click **Create IDCS Group**.

c. Enter a name (for example, `idcs-integration-admins`).

d. Click **Create**.

14. Copy the IDCS base URL (`https://<account>.identity.oraclecloud.com`) for use next in Add Oracle Identity Cloud Service as an Identity Provider.

Add Oracle Identity Cloud Service as an Identity Provider

If your tenancy needs user federation between Oracle Cloud Infrastructure's IAM and Oracle Identity Cloud Service (IDCS), complete steps in the console by adding Oracle Identity Cloud Service as an identity provider.

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

> **Note:**
>
> Follow the steps in this section only if manual federation is needed. You'll need the information you generated in the steps in Get Required Information from Oracle Identity Cloud Service.

1. Sign in to the Oracle Cloud Infrastructure Console as an IAM user (use the options on the right side).
2. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Federation**.
3. Click **Add Identity Provider** and enter data as below. Click **Continue**.

   a. **Name:** Enter a name, such as `oracleidentitycloudservice`.

   b. **Description:** Enter a description, such as `Federated IDCS stripe`.

   c. **Oracle Identity Cloud Service Base URL:** Enter the IDCS base URL you noted in step 14 in Get Required Information from Oracle Identity Cloud Service.

   d. **Client ID:** Enter the application's client ID you noted in step 11 in Get Required Information from Oracle Identity Cloud Service.

   e. **Client Secret:** Enter the client secret you noted in step 11 in Get Required Information from Oracle Identity Cloud Service.

   f. Click **Continue**.
4. When prompted, map your IDCS group to the OCI administrators group.

   Select your IDCS group in the **Identity Provider Group** field and your Oracle Cloud Infrastructure group in the **OCI Group** field.
5. Sign out and sign back in as one of your federated users. On the Federation page, verify that the Oracle Identity Cloud Service link is now shown. See Is My Tenancy Federated Between Oracle Cloud Infrastructure IAM and Oracle Identity Cloud Service?

Automate with Events

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

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

For more information, see Overview of Events.

The following Oracle Integration resource emits events:

- Integration Instance

Integration Instance Event Types

These are the event types that Integration Instances emit:

Friendly Name	Event Type
Create Integration Instance Begin	`com.oraclecloud.integration.createintegrationinstance.begin`
Create Integration Instance End	`com.oraclecloud.integration.createintegrationinstance.end`
Update Integration Instance Begin	`com.oraclecloud.integration.updateintegrationinstance.begin`
Update Integration Instance End	`com.oraclecloud.integration.updateintegrationinstance.end`
Start Integration Instance Begin	`com.oraclecloud.integration.startintegrationinstance.begin`
Start Integration Instance End	`com.oraclecloud.integration.startintegrationinstance.end`
Stop Integration Instance Begin	`com.oraclecloud.integration.stopintegrationinstance.begin`
Stop Integration Instance End	`com.oraclecloud.integration.stopintegrationinstance.end`
Delete Integration Instance Begin	`com.oraclecloud.integration.deleteintegrationinstance.begin`
Delete Integration Instance End	`com.oraclecloud.integration.deleteintegrationinstance.end`

Friendly Name	Event Type
Change Integration Instance Compartment Begin	com.oraclecloud.integration.changeintegrationcompartment.begin
Change Integration Instance Compartment End	com.oraclecloud.integration.changeintegrationcompartment.end

Integration Instance Event Example

This is a reference event for Integration Instances:

```
{
    "eventType":
"com.oraclecloud.integration.updateintegrationinstance.begin",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "eventID": "<unique_ID>",
    "source": "integration",
    "eventTime": "2019-01-10T21:19:24Z",
    "contentType": "application/json",
    "extensions": {
      "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    },
    "data": {
      "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
      "compartmentName": "example_compartment",
      "resourceName": "My test resource",
      "resourceId": "ocid1.integrationinstance.oc1.phx.<unique_ID>",
      "availabilityDomain": "<availability_domain>",
      "freeFormTags": {
        "Department": "Finance"
      },
      "definedTags": {
        "Operations": {
          "CostCenter": "42"
        }
      },
      "additionalDetails": {
        "integrationInstanceType": "STANDARD",
        "isByol": "false",
        "messagePacks": 1
          }
    }
  }
```

B

Oracle Integration Roles and Privileges

Roles define the privileges available to users and the tasks that they can perform. You can assign predefined roles to users to allow them to work with feature sets of Oracle Integration.

Topics:

What Users Can Do in the Integrations Design Section by Role

The following tables list Oracle Integration predefined roles available in the Integrations design section, and the tasks users granted those roles can perform.

Integrations

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
Create	Yes	Yes	No	No	No	No
Create new version	Yes	Yes	No	No	No	No
View	Yes	Yes	No	Yes	No	Yes
Edit	Yes	Yes	No	No	No	No
Delete	Yes	Yes	No	No	No	No

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
Activate • Enable tracing (include payload)	Yes	Yes	No	No	No	No
Reactivation after connection update	Yes	Yes	No	No	No	No
Deactivate	Yes	Yes	No	No	No	No
Clone	Yes	Yes	No	No	No	No
Run	Yes	Yes	No	Yes	Yes	No
Export	Yes	Yes	No	Yes	No	Yes
Import	Yes	Yes	No	No	No	No
Update Property Values	Yes	Yes	No	No	No	No
Configure	Yes	Yes	No	No	No	No
Assign Business Identifiers	Yes	Yes	No	No	No	No
Unlock	Yes	Yes	No	No	No	No
Add Schedule	Yes	Yes	No	Yes	No	No
Edit Schedule	Yes	Yes	No	Yes	No	No
Delete Schedule	Yes	Yes	No	Yes	No	No
Run Schedule	Yes	Yes	No	Yes	No	No
View Schedule Runs	Yes	Yes	No	Yes	No	Yes
Update Schedule Parameters	Yes	Yes	No	Yes	No	No
Convert scheduled integration to app-driven orchestration integration	Yes	Yes	No	No	No	No
Run or schedule integrations on behalf of another user	Yes	No	No	No	No	No

Connections

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
Create	Yes	Yes	No	No	No	No
Edit	Yes	Yes	No	No	No	No
Delete	Yes	Yes	No	No	No	No
View	Yes	Yes	No	Yes	No	Yes
Test	Yes	Yes	No	No	No	No
Clone	Yes	Yes	No	No	No	No
Unlock	Yes	Yes	No	No	No	No
Refresh Metadata	Yes	Yes	No	No	No	No

Lookups

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
Create	Yes	Yes	No	No	No	No
View	Yes	Yes	No	Yes	No	Yes
Edit	Yes	Yes	No	No	No	No
Clone	Yes	Yes	No	No	No	No
Delete	Yes	Yes	No	No	No	No
Export to CSV	Yes	Yes	No	Yes	No	Yes
Import	Yes	Yes	No	No	No	No

Packages

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
View	Yes	Yes	No	Yes	No	Yes
Create (during integration creation)	Yes	Yes	No	No	No	No
Import	Yes	Yes	No	No	No	No
Export	Yes	Yes	No	Yes	No	No
Update (through integration update)	Yes	Yes	No	No	No	No
Delete	Yes	Yes	No	No	No	No
Configure	Yes	Yes	No	No	No	No

Agents

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
View	Yes	Yes	No	Yes	No	Yes
Edit Agent Group	Yes	Yes	No	No	No	No
Delete Agent Group	Yes	Yes	No	No	No	No
Create Agent Group	Yes	Yes	No	No	No	No
Download connectivity agent	Yes	No	No	No	No	No

Adapters

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
View	Yes	Yes	No	Yes	No	No
Delete	Yes	Yes	No	No	No	No
Create Connection	Yes	Yes	No	No	No	No

Libraries

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
View	Yes	Yes	No	Yes	No	Yes
Edit	Yes	Yes	No	No	No	No
Create	Yes	Yes	No	No	No	No
Import	Yes	Yes	No	No	No	No
Delete	Yes	Yes	No	No	No	No
Update	Yes	Yes	No	No	No	No
Export	Yes	Yes	No	Yes	No	Yes

What Users Can Do from the Username Main Menu

The following table lists the Oracle Integration tasks available from the **Username** main menu in the upper right corner of the Integrations pages, and the roles users must be granted to perform those tasks.

Username Main Menu

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
Set Time Zone Preferences	Yes	Yes	No	Yes	No	Yes

What Users Can Do in the Observability Section by Role

The following tables list Oracle Integration predefined roles available in the Observability section, and the tasks users granted those roles can perform.

- Dashboards
- Integrations
- Agents
- Instances
- Errors

Dashboards

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
View Activity Stream	Yes	Yes	Yes	Yes	No	Yes
View Design-time Audit	Yes	Yes	Yes	Yes	No	Yes
View Runtime Health	Yes	Yes	Yes	Yes	No	Yes
View System Health	Yes	Yes	Yes	Yes	No	Yes
View Agent Health	Yes	Yes	Yes	Yes	No	Yes
View Integrations	Yes	Yes	Yes	Yes	No	Yes
View Scheduling	Yes	Yes	Yes	Yes	No	Yes
View Design-time Metrics	Yes	Yes	Yes	Yes	No	Yes
View the Hourly / Daily History	Yes	Yes	Yes	Yes	No	Yes

Integrations

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
View	Yes	Yes	Yes	Yes	No	Yes

Agents

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
View	Yes	Yes	Yes	Yes	No	Yes

Instances

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
View Details	Yes	Yes	Yes	Yes	No	Yes
Asserter Recordings	Yes	Yes	Yes	No	No	Yes
View Business Identifiers	Yes	Yes	Yes	Yes	No	Yes
View Activity Stream	Yes	Yes	Yes	Yes	No	Yes
Download Activity Stream	Yes	Yes	Yes	Yes	No	Yes

Errors

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
View	Yes	Yes	Yes	Yes	No	Yes
Abort	Yes	Yes	Yes	Yes	No	No
Resubmit	Yes	Yes	No	Yes	No	No

What Users Can Do in the Settings Section by Role

The following tables list Oracle Integration predefined roles available in the Settings section, and the tasks users granted those roles can perform.

- Certificates
- Notifications
- Tracing

- Schedule

Certificates

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
View	Yes	No	No	No	No	No
Upload	Yes	No	No	No	No	No
Update	Yes	No	No	No	No	No
Delete	Yes	No	No	No	No	No

Notifications

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
View	Yes	No	No	No	No	No
Revert	Yes	No	No	No	No	No
Save	Yes	No	No	No	No	No
Send Now	Yes	No	No	No	No	No
Reset All Notifications	Yes	No	No	No	No	No

Tracing

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
View	Yes	No	No	No	No	No
Save	Yes	No	No	No	No	No
Revert	Yes	No	No	No	No	No
Include payload	Yes	No	No	No	No	No

Schedule

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
Save	Yes	No	No	No	No	No

What Users Can Do in the Projects Section by Role

The following tables list Oracle Integration predefined roles available in the projects section, and the tasks users granted those roles can perform.

> **Note:**
>
> You can also control the users and groups that edit, view, and monitor a project with role-based access control (RBAC). See Control Editing, Viewing, and Monitoring Access in a Project in *Using Integrations in Oracle Integration 3*.

- Project Level
- Design
- Deploy
- **Observe**

Project Level

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
Projects - Navigation Pane	Yes	Yes	Yes	Yes	No	Yes
Create Project	Yes	Yes	No	No	No	No
Import Project	Yes	Yes	No	No	No	No
View Project	Yes	Yes	No	Yes	No	Yes
Activate Project	Yes	Yes	No	No	No	No
Deactivate Project	Yes	Yes	No	No	No	No
Export Project	Yes	Yes	No	No	No	Yes
Delete Project	Yes	Yes	No	No	No	No
Edit Project Description Details	Yes	Yes	No	No	No	No
Invoke Child Integrations	Yes	Yes	No	No	No	No

Design

Integrations

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
Create	Yes	Yes	No	No	No	No
Create new version	Yes	Yes	No	No	No	No
View	Yes	Yes	No	Yes	No	Yes
Edit	Yes	Yes	No	No	No	No

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
Delete	Yes	Yes	No	No	No	No
Activate	Yes	Yes	No	No	No	No
Reactivation after connection update	Yes	Yes	No	No	No	No
Deactivate	Yes	Yes	No	No	No	No
Clone	Yes	Yes	No	No	No	No
Run	Yes	Yes	No	Yes	Yes	No
Export	Yes	Yes	No	Yes	No	Yes
Import	Yes	Yes	No	No	No	No
Update Property Values	Yes	Yes	No	No	No	No
Configure	Yes	Yes	No	No	No	No
Assign Business Identifiers	Yes	Yes	No	No	No	No
Refresh Integration Endpoints	Yes	Yes	No	No	No	No
Unlock	Yes	Yes	No	No	No	No
Add Schedule	Yes	Yes	No	Yes	No	No
Edit Schedule	Yes	Yes	No	Yes	No	No
Delete Schedule	Yes	Yes	No	Yes	No	No
Run Schedule	Yes	Yes	No	Yes	No	No
View Schedule Runs	Yes	Yes	No	Yes	No	Yes
Update Schedule Parameters	Yes	Yes	No	Yes	No	No
Run or schedule integrations on behalf of another user	Yes	No	No	No	No	No
Update integration tracing level	Yes	Yes	No	No	No	No
Extend Accelerator Project	Yes	Yes	No	No	No	No
Upgrade Accelerator Project	Yes	Yes	No	No	No	No

Connections

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
Create	Yes	Yes	No	No	No	No
Edit	Yes	Yes	No	No	No	No
Delete	Yes	Yes	No	No	No	No
View	Yes	Yes	No	Yes	No	Yes
Test	Yes	Yes	No	No	No	No
Unlock	Yes	Yes	No	No	No	No
Refresh Metadata	Yes	Yes	No	No	No	No

Lookups

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
Create	Yes	Yes	No	No	No	No
View	Yes	Yes	No	Yes	No	Yes
Edit	Yes	Yes	No	No	No	No
Delete	Yes	Yes	No	No	No	No
Export to CSV	Yes	Yes	No	Yes	No	Yes

JavaScript Libraries

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
View	Yes	Yes	No	Yes	No	Yes
Edit	Yes	Yes	No	No	No	No
Create	Yes	Yes	No	No	No	No
Delete	Yes	Yes	No	No	No	No
Update	Yes	Yes	No	No	No	No
Import	Yes	Yes	No	Yes	No	Yes

Deploy

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
Create Deployment	Yes	Yes	No	No	No	No
Edit Deployment	Yes	Yes	No	No	No	No
View Deployment	Yes	Yes	No	No	No	Yes

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
Clone Deployment	Yes	Yes	No	No	No	No
Export Deployment	Yes	Yes	No	Yes	No	No
Delete Deployment	Yes	Yes	No	No	No	No

Observe

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
View Details	Yes	Yes	Yes	Yes	No	Yes
View Business Identifiers	Yes	Yes	Yes	Yes	No	Yes
View Activity Stream	Yes	Yes	Yes	Yes	No	Yes
Download Activity Stream	Yes	Yes	Yes	Yes	No	Yes
Abort	Yes	Yes	No	Yes	No	No
Resubmit	Yes	Yes	No	Yes	No	No
View Future Runs	Yes	Yes	Yes	Yes	No	Yes
View Audit Trail	Yes	Yes	Yes	Yes	No	Yes
Download the Audit Log	Yes	Yes	No	Yes	No	No

What Users Can Do in Processes by Role

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

See Process Automation Roles in *Administering Oracle Cloud Infrastructure Process Automation*.

What Users Can Do in File Server by Role

Permissions in File Server are defined by a subset of Oracle Integration roles.

> **Note:**
>
> The following roles do not have any privileges in File Server:
>
> - ServiceMonitor
> - ServiceDeployer
> - ServiceInvoker
> - ServiceViewer

The following table lists predefined roles available in Oracle Integration, and the File Server tasks that users with those roles can perform.

Oracle Integration Roles	Personas and Permissions in File Server
ServiceAdministrator	Users with this role can manage server settings and configure users, groups, and folders, including permissions. To administer File Server as described in this guide, you must be assigned the ServiceAdministrator role in Oracle Integration.
ServiceDeveloper	Users with this role can use File Server along with the FTP adapter in Integrations to read and write files.
ServiceUser	Users with this role can access File Server using an SFTP client. These users must be configured and enabled as users in File Server. Their access is controlled by their assigned folders and folder permissions.

What Users Can Do in Visual Builder by Role

The following table lists Oracle Integration predefined roles available in Visual Builder, and the tasks that users granted those roles can perform.

> **Note:**
>
> The following roles do not have any privileges in Visual Builder:
>
> - ServiceMonitor
> - ServiceDeployer
> - ServiceEndUser
> - ServiceInvoker
> - ServiceViewer

Oracle Integration Role	Tasks Users Can Perform in Visual Builder
ServiceAdministrator	A user with the ServiceAdministrator role can: • Use the visual design tool • Create, manage, and change the owners of applications • Create associations with other services • Configure security options for applications in an instance • Specify error messages for Access Denied pages

Oracle Integration Role	Tasks Users Can Perform in Visual Builder
ServiceDeveloper	A user with the ServiceDeveloper role can: • Use the visual design tool • Create, manage, secure, and publish web and mobile applications • Design pages, work with business objects, build and test applications
ServiceUser	A user with the role of ServiceUser can only access staged and published applications. The default permission is enforced only when the service administrator adjusts security settings for the entire service instance to restrict all access to runtime applications to the users granted the ServiceUser role.

What Users Can Do in B2B for Oracle Integration by Role

The following table lists Oracle Integration predefined roles available in B2B for Oracle Integration and the tasks that users granted those roles can perform.

> **Note:**
>
> The following roles do not have any privileges in B2B for Oracle Integration:
>
> - ServiceDeployer
> - ServiceEndUser
> - ServiceInvoker

The list of tasks that different user roles can perform on B2B integrations (integrations using the B2B action) are the same as the tasks they can perform on other integrations. See What Users Can Do in the Integrations Design Section by Role.

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceViewer
View B2B Documents	Yes	Yes	No	Yes	Yes
Create or Modify B2B Documents	Yes	Yes	No	No	No
View B2B Schemas	Yes	Yes	No	Yes	Yes
Create or Modify B2B Schemas	Yes	Yes	No	No	No
Generate Implementation Guide	Yes	Yes	No	Yes	Yes
Create or modify host profiles	Yes	Yes	No	Yes (Can view only)	Yes (Can view only)
Create or modify trading partners	Yes	Yes	No	Yes (Can view only)	Yes (Can view only)

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceViewer
Track B2B messages	Yes	Yes	Yes	Yes (Can view message details and download payloads only)	Yes (Can view message details and download payloads only)