Oracle® Cloud

Provisioning and Administering Oracle Integration 3

G13369-30
March 2025

Oracle Cloud Provisioning and Administering Oracle Integration 3,

G13369-30

Primary Author: Oracle Corporation

Contents

3 Manage Access and Assign Roles

4 Create and Edit Oracle Integration 3 Instances

5 Manage Oracle Integration 3 Instances

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.

Features

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 several editions: Standard, Enterprise, or Healthcare. 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 Patching Updates to Your Oracle Integration 3 Instance.

Topics:

Availability

Oracle Integration 3 is currently available in the regions listed below. Some regions allow you to create instances for both Production and Development shapes, while others allow only Production. Some regions support Oracle-managed disaster recovery and robotic process automation (RPA).

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*.
- For information on Oracle-managed disaster recovery, see *Configuring an Oracle-Managed Disaster Recovery Solution for Oracle Integration 3*

Geography	Region location	Region key	Development shape available?	Oracle-managed disaster recovery supported?	Robotic process automation (RPA) supported?
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	✓	✓ Paired with SIN.	✗
APAC	Singapore	SIN	✓	✓ Paired with NRT.	✓
APAC	Singapore West	XSP	✗	✗	✗
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	✓	✓ Paired with AMS.	✓
EMEA	Israel (Jerusalem)	MTZ	✓	✗	✗

Geography	Region location	Region key	Development shape available?	Oracle-managed disaster recovery supported?	Robotic process automation (RPA) supported?
EMEA	Italy (Milan)	LIN	✓	✗	✗
EMEA	Netherlands Northwest (Amsterdam)	AMS	✓	✓ Paired with FRA.	✓
EMEA	Saudi Arabia Central (Riyadh)	RUH	✗	✗	✗
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)	DXB	✓	✗	✓
EMEA	UK Gov South (London)	LTN	✓	✗	✗
EMEA	UK Gov West (Newport)	BRS	✓	✗	✗
EMEA	UK West (Cardiff)	CWL	✓	✓ Paired with LHR.	✗
EMEA	UK South (London)	LHR	✓	✓ Paired with CWL.	✓
LAD	Brazil East (Sao Paulo)	GRU	✓	✗	✓
LAD	Brazil Southeast (Vinhedo)	VCP	✓	✗	✗
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	✗	✗	✗

Geography	Region location	Region key	Development shape available?	Oracle-managed disaster recovery supported?	Robotic process automation (RPA) supported?
North America	US DoD North (Chicago)	PIA	✗	✗	✗
North America	US DoD West (Phoenix)	TUS	✗	✗	✗
North America	US East (Ashburn)	IAD	✓	✓ Paired with PHX.	✓
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	✓	✓ Paired with IAD.	✓
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.

> **Note:**
>
> The service limits described below are enforced.

Oracle Cloud Infrastructure Console Service Limits

For more Oracle Cloud Infrastructure Console service limits, see Service Limits in the OCI documentation.

Resource	Service Limit
Integration service instance count	200 service 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.
Service instance creation	The ability to create service instances outside your home region depends on several factors. See Restrictions.
Private endpoint limits	• 1 private endpoint per service instance • 1 subnet per private endpoint
Custom endpoints - maximum number	1 custom endpoint
Oracle Integration internal diagnostic logs retention in Oracle Cloud Infrastructure Logging	Retained for 30 days for debugging use. See Logging Analytics.

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.

Resource	Service Limit
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.
Private endpoint support	You can configure access to private endpoints with a growing list of adapters. See Adapters that Support Connecting to Private Endpoints in *Using Integrations in Oracle Integration 3*.
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). Write File operation: There is no limit.

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. **Note**: If the string length for fields in a JSON payload exceeds 20 MB, you receive a translation failure error. See ORABPEL-15235 Translation Failure Occurrence in *Using the REST Adapter with Oracle Integration 3*. • 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. • Response returned as part of invoke runtime binary data (application/octet-stream): 1 GB • Response returned from agent-based endpoints for structured content (for example, JSON/CSV/XML, and so on): 50 MB • Response returned from private endpoints for structured content (for example, JSON/CSV/XML, and so on): 100 MB • Response returned from public internet-based endpoints for structured content (for example, JSON/CSV/XML, and so on):100 MB

Resource	Service Limit
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 • Private endpoints: 100 MB • Public internet-based endpoints: 100 MB
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 • Private endpoints: 100 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, SAP ASE (Sybase) Adapter, and Snowflake Adapter)	**For trigger configurations** • Polling operation: – 50 MB with schema transformation for agent-based endpoints. – 100 MB with schema transformation through private endpoints **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: – 100 MB for public internet-based endpoints – 100 MB for private endpoints – 50 MB for agent-based endpoints

Resource	Service Limit
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	100 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.
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	800. 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.
Triggers (maximum number of concurrent requests)	• Synchronous: A maximum of 600 concurrent requests. Users receive 100 concurrent requests per message pack. This concurrent request increase is useful if you have high concurrency requirements in respect to synchronous integration executions. For details about how concurrent request scalability is calculated, see Message Pack Usage and Synchronous Requests. • Asynchronous: No limit (50 at a time can execute, the rest are queued).
Maximum number of integrations that can subscribe to events	50 integrations can subscribe to events per service instance.
Maximum number of tracking events per integration 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 the activity stream, but they continue to be processed and the integration instance overall state is calculated. This ensures that the integration instance state is updated in all scenarios.
Maximum activity stream payload sizes	The total payload size stored per integration instance in the activity stream is limited to 25 MB. There is no limit for payloads stored in the Object Store. Only payloads under 32k are stored in the activity stream.

Resource	Service Limit
Maximum duration for integration flows	• Asynchronous: Six hours (The integration instance is marked as aborted due to deadline timeout.) • Scheduled: Six hours (The integration 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.
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 integration 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 if using the user interface. If using the Observability (instances/errors) API, 50 requests per second are allowed.

Resource	Service Limit
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 integration 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.
Service instance data retention	Retention is based on the trace level set during integration activation: • Production: 32 days (default) for Standard and Enterprise editions, 184 days for Healthcare edition You can increase the data retention period for Standard and Enterprise editions if you want (this incurs extra costs). See Edit the Data Retention Period for an Instance. • Audit: 8 days • Debug (Not Recommended): 24 hours **Note**: After 24 hours, Debug (Not recommended) is automatically reset to Production. See Activate an Integration in *Using Integrations in Oracle Integration 3*.
Time window for recovering a failed integration instance that's recoverable	The integration 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 (default) for Standard and Enterprise editions, 184 days for Healthcare edition.
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 integration instances returned per monitoring request	50.
Maximum number of resubmissions allowed per integration instance ID	10.
Schedule parameter - value length	256 characters.
Maximum number of schedule parameters per integration	5 parameters.

Resource	Service Limit
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.
Maximum *limit* supported (REST API)	50.
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: Robotic Process Automation

Resource	Service limit
Maximum duration for a robot instance	4 hours.
Timeout for assigning a robot instance to an environment	Varies, depending upon the environments: • If the environment pool contains no environments: 0 seconds, and then the status of the robot instance changes to **Failed**. • If the robot agent on the environment doesn't accept the request: 30 seconds, and then Oracle Integration attempts to assign the robot instance to a different environment. • If all environments in the environment pool have a status of **Unavailable**: 240 seconds, and then the status of the robot instance changes to **Failed**. • If at least one environment in the environment pool has a status of **Available**: No limit.
Maximum wait time for downloading a file	180 seconds by default but the robot builder can specify a different value while creating a robot.
Maximum file size for downloading a file	50 MB.
Frequency at which the robot agent polls Oracle Integration for work	15 seconds.
Maximum time that Oracle Integration waits for the robot agent to poll for work before changing its environment's status to **Unavailable**	35 seconds.
Maximum number of environments in an environment pool	100 environments.

Resource	Service limit
Character limits for robots	• Name: 50 characters. • Description: 1024 characters. • Keywords: 1024 characters.
Character limits for environment pools	• Name: 50 characters. • Description: 1024 characters. • Keywords: 1024 characters.
Character limits for robot connection types	• Name: 50 characters. • Description: 1024 characters. • Keywords: 1024 characters.
Character limits for robot connections	• Name: 50 characters. • Description: 1024 characters. • Keywords: 1024 characters.

Component: File Server

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

Component: Process Automation

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

Message Pack Usage and Synchronous Requests

The following table describes the request limits based on the number of message packs.

Message Packs Assigned	Synchronous Request Limit
6	600
5	500
4	400
3	300
2	200
1	100

When to Increase Message Packs

Your message packs must equate with the number of messages you consume per hour. Ensure you know your hourly throughput. An increase in message packs is also beneficial if you want quicker processing of synchronous requests. The following examples describe when you need higher concurrency.

Examples	Message Packs
How quickly can a customer consume message packs with high synchronous concurrency?	Assume a customer has 2 message packs assigned (10K messages per hour). Each synchronous request takes 5 seconds to complete. Therefore: • A concurrency of 1 can execute 12 requests per minute. • A concurrency of 200 can execute 2400 requests per minute. • A 10-minute burst with 200 concurrent synchronous requests = 24000 messages, which provides an overage of 14K messages (`24K - 10K`) for that hour.
When is the 600 synchronous requests limit reached?	The 600 concurrent synchronous request limit is reached when the customer applies 6 message packs to the Oracle Integration instance. Consider the following example in which each synchronous request takes 10 seconds to execute: • A concurrency of 1 can execute 6 requests per minute. • A concurrency of 600 can execute 3600 requests per minute. • A 10-minute burst with 600 concurrent synchronous requests equals 36000 messages, which results in an overage of 6K messages (`36K - 30K`) for that hour.

Therefore, a customer with a high message throughput per hour already has a larger number of message packs assigned to the service instance. The need for a customer to increase the number of message packs to gain more synchronous request processing concurrency is as follows:

- Less than 5K messages per hour
- A burst of synchronous requests that exceed 100 messages

Oracle Integration Editions

Oracle Integration is available in several editions: *Standard*, *Enterprise*, and *Healthcare*.

Included in All Editions

- All editions give you the power to integrate your Software as a Service (SaaS) applications and your on-premises applications.
- Regardless of which edition you choose, Oracle handles cloud and database management and other administrative tasks for you.

Standard Edition

Standard edition lets you use integrations, *standard* adapters, recipes and accelerators, Visual Builder, and File Server.

> **Note:**
>
> All Enterprise-edition features are visible in Standard-edition instances. However, if you have a Standard-edition license, you're not entitled to use Enterprise-edition features, unless you update your instance to Oracle Integration Enterprise edition. See Edit the Edition, License Type, Message Packs, and Custom Endpoint of an Instance.

Enterprise Edition

Enterprise edition provides all the features of Standard edition, plus additional technologies and services, including *enterprise* adapters. Enterprise edition also enables you to design, automate, and manage your business processes in the cloud with Process Automation, perform UI-based automation with robots using robotic process automation, and support business-to-business communications using B2B for Oracle Integration.

Healthcare Edition

Healthcare edition provides all the features of Enterprise edition, plus additional technologies for Health Level 7 (HL7), including healthcare messages, healthcare adapters, and a healthcare action. See *Using Oracle Integration for Healthcare in Oracle Integration 3*.

> **Note:**
>
> The Healthcare edition is available only in tenancies that use Universal Credits.

Comparison of All Editions

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

Technology, service, or feature	Available in Standard edition	Available in Enterprise edition	Available in Healthcare edition
Integration	Yes	Yes	Yes
Visual Builder	Yes	Yes	Yes
Standard adapters	Yes	Yes	Yes
Enterprise adapters*	No	Yes	Yes
Process Automation	No	Yes	Yes
B2B**	No	Yes	Yes
File Server	Yes	Yes	Yes
Embedded recipes and business and technical accelerators	Yes	Yes	Yes
Robotic process automation	No	Yes	Yes
Healthcare message support	No	No	Yes
Healthcare adapters	No	No	Yes
Healthcare action	No	No	Yes

Technology, service, or feature	Available in Standard edition	Available in Enterprise edition	Available in Healthcare edition
Data retention	32 days	32 days***	184 days
Disaster recovery	No	Yes (incurs extra cost)	Yes (incurs extra cost)

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

**You can't 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.

***You can increase the data retention period for Enterprise editions if you want (may incur extra cost).

Patching Updates to Your Oracle Integration 3 Instance

Functional updates to Oracle Integration 3 occur every two months and involve zero downtime. Oracle completes all patching 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.

> **Note:**
>
> You can't change the shape after you create the instance. However, you can move data to another instance using the export and import features. See Clone the Design-Time Metadata of an Entire Service Instance in *Using Integrations in Oracle Integration 3*.

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.

New Feature Availability in Your Instance

You see the changes for a release only after your instance has been updated to the latest release and the feature is available in the realm where your instance is located. To identity the release version of your instance, select the **About** option in your Oracle Integration 3 instance. See Why Don't I See the Latest Changes? in *What's New for Oracle Integration 3*.

New features are described in the documentation when functional updates occur. See About This Guide in *What's New for Oracle Integration 3*.

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.

For details about how concurrent request scalability is calculated, see Message Pack Usage and Synchronous Requests.

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.

TLS Cipher Suites Support

Oracle Integration supports the following TLS cipher suites.

Supported Cipher Suites

- TLS_ECDHE_RSA_AES128_GCM_SHA256
- TLS_ECDHE_RSA_AES256_GCM_SHA384

See Inbound and Outbound Endpoints and Transport Layer Security Server Version Support in *Using Integrations in Oracle Integration 3*.

Deprecated Cipher Suites

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

- TLS_DHE-RSA-AES128-GCM-SHA256
- TLS_DHE-RSA-AES128-SHA256
- TLS_DHE-RSA-AES256-GCM-SHA384
- TLS_DHE-RSA-AES256-SHA256
- TLS_ECDHE-RSA-AES128-SHA256
- TLS_ECDHE-RSA-AES256-SHA384

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 usage. 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, UK, and Australia 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
• OC10 realm (Oracle Cloud for Australian Government and Defence) in the Australia (Canberra) region	Oracle Integration documentation on the Oracle Help Center

Oracle Integration in the Oracle EU Sovereign Cloud

Oracle Integration 3 is available in the Oracle EU Sovereign Cloud.

To learn about the Oracle EU Sovereign Cloud (OC19 realm), see Oracle EU Sovereign Cloud.

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	Oracle completes functional and security patching updates work on your behalf, with no work required by you. See Patching Updates to Your Oracle Integration 3 Instance. 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.
High availability	R, A	I	- -
Disaster recovery	C	R, A	- -

Task	Oracle's Role	Customer's Role	Comments
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 other Oracle Integration solutions?
>
> - For Oracle Integration for Oracle SaaS, see Can I Create an Oracle Integration for Oracle SaaS Instance?
> - For Oracle Integration in Government Regions, see Restrictions in *Using Oracle Integration 3 on Oracle Cloud Infrastructure US Government Cloud*.

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 3 Instances

Everyone can create Oracle Integration 3 instances. See Create an Oracle Integration Instance.

Additional resources:

- For the list of regions in which you can create an Oracle Integration 3 instance, see Availability.
- For information on restrictions when creating instances, see Restrictions.

Oracle Integration Generation 2 Instances

You can create a new Oracle Integration Generation 2 instance only if you have an existing Oracle Integration Generation 2 instance in the region. See Creating an Oracle Integration Instance in *Provisioning and Administering Oracle Integration Generation 2*.

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 example, you can't use an Oracle Integration Generation 2 instance for development and an Oracle Integration 3 instance for production.

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.

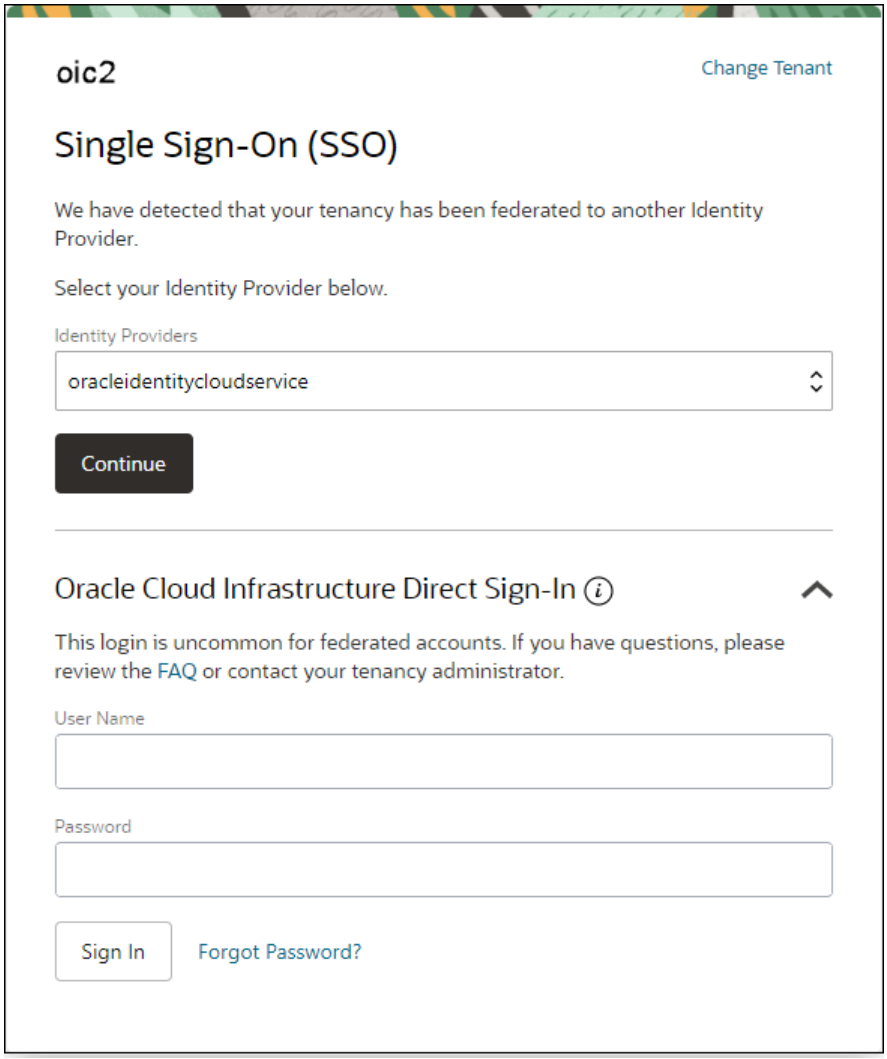
Sign In to the Console in Tenancies That Do Not Use Identity Domains

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.

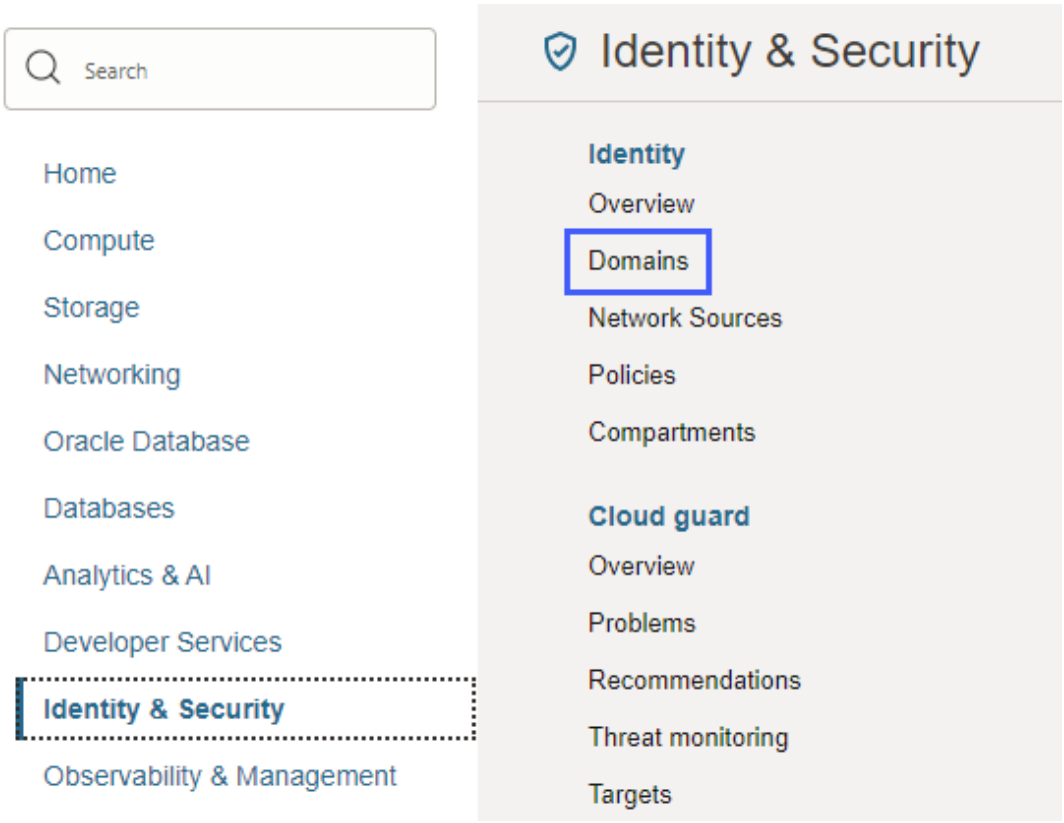
- Manage users, groups, and roles in both IDCS and Oracle Cloud Infrastructure IAM, linked using federation, if both of the following are true:
  - Oracle updated your region to use identity domains after you created your tenancy
  - And, Oracle has not yet migrated existing tenancies in your region 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 with Identity Domains or Managing Policies without Identity Domains in the Oracle Cloud Infrastructure documentation.

You can create a policy in any compartment. However, be aware that you can only view and manage policies one compartment at a time; you can't get a single list of all policies in a tenancy. You might want to set up a strategy to organize your policies so they're easy to find. Here are some things to take into account when creating policies:

- Policies are inherited from the parent compartment.
- The compartment in which you create the policy determines who can modify or delete the policy.
- Use compartments to separate resources between projects or business units.
- Use a consistent naming format and good descriptions to make it easier to know what policies are used for.

Resource Type

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`.
	`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

Verb	Permissions	APIs Fully Covered	APIs Partially Covered
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
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.

Oracle Integration	Description
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.
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 Technology or Service

In Oracle Integration, you assign a role to a group. All users in the group are granted that role for all the technologies and services in an instance. However, each role grants different privileges for each technology or service. For example:

- For the Integrations technology, users can design integrations.
- For the Process Automation service, 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

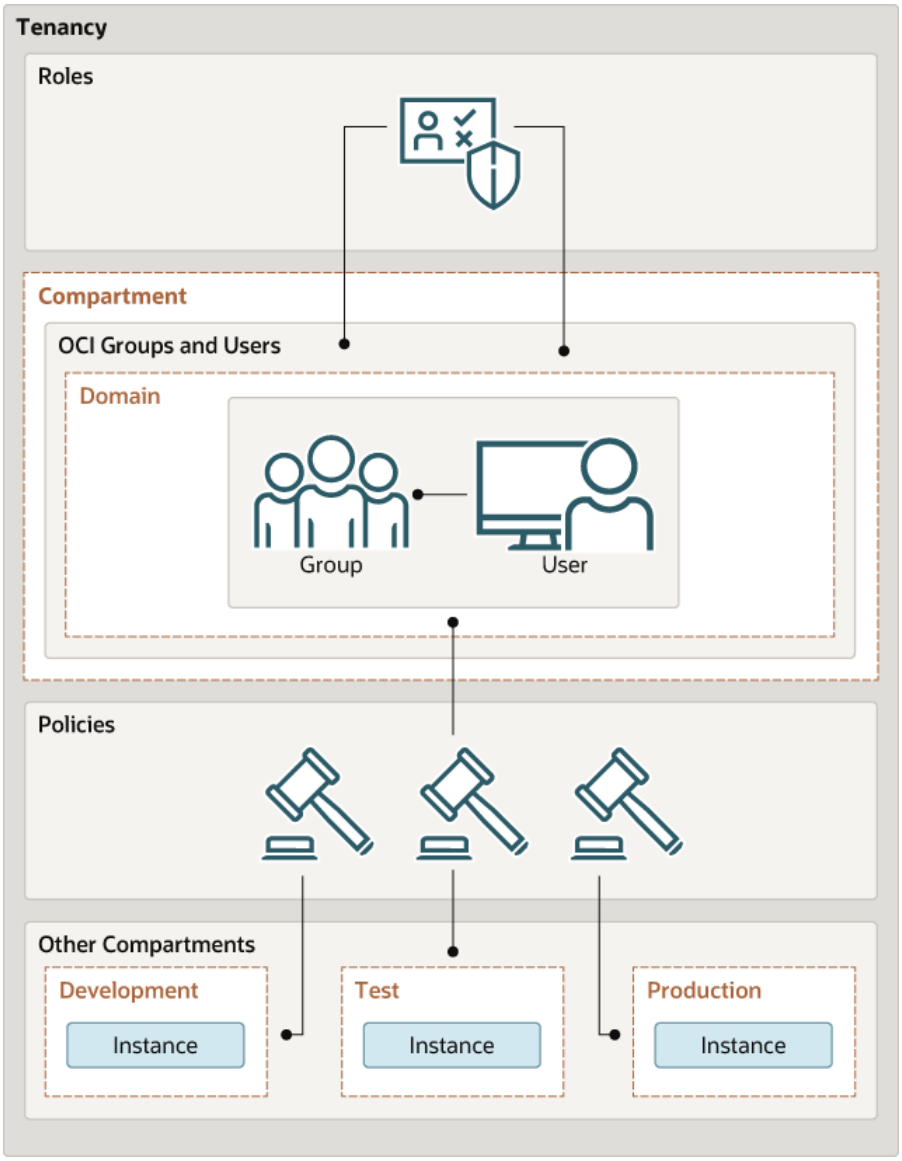
If you are not sure if your tenancy uses identity domains, see Differences Between Tenancies With and Without Identity Domains.

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
- Audit Users' Access to the Oracle Integration Instance 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. Your workflow varies, depending on where the user works.

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

Before You Begin

If you are using Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) as your identity system, you must create all users in Oracle Cloud Infrastructure Identity and Access Management. If you are federating with other identity providers, see Federating with Identity Providers in the Oracle Cloud Infrastructure documentation.

After creating a user, you grant them IAM policies or assign service roles, depending on where the user works. The following table provides more details.

Where the person works	Typical tasks	How to give the person access
In the Oracle Cloud Infrastructure Console OR With the Oracle Integration lifecycle APIs	Creating and configuring an Oracle Integration instance, and managing the lifecycle of an instance	Grant them IAM policies.
In the Oracle Integration instance OR With the Oracle Integration built-in REST APIs OR With customer-built APIs (for your integrations)	Designing and monitoring integrations	Assign them service roles for Oracle Integration.
Both places	All of the above tasks	Grant them IAM policies and service roles for Oracle Integration.

Workflow for Users Who Work in the Oracle Cloud Infrastructure Console or with Its APIs

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 example, 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.

Order	Task	More information
2	Create groups	Groups save you time when setting up access. You add multiple 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 the people who are in a specific group 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. Each IAM policy that you write governs 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.
5	Tell everyone they can start working	After completing all the tasks, inform everyone that they can start working in the Oracle Cloud Infrastructure Console.

Workflow for Users Who Work in the Oracle Integration Instance or with Its APIs

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 example, 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.

Order	Task	More information
2	Create groups	Groups save you time when setting up access. You add multiple 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, create another group for administrators, and so on. Everyone in the group gets the same access. See Create an IAM Group in an Identity Domain.
3	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.
4	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.
5	Tell everyone they can start working	After completing all the tasks, 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. Make sure you're in the compartment in which you want to create the policy. See the tips in About IAM Policies for Oracle Integration.
3. Click **Create Policy**.
4. In the Create Policy window, enter a name (for example, `IntegrationGroupPolicy`) and a description.
5. 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

6. 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
   ```

7. 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`

8. 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

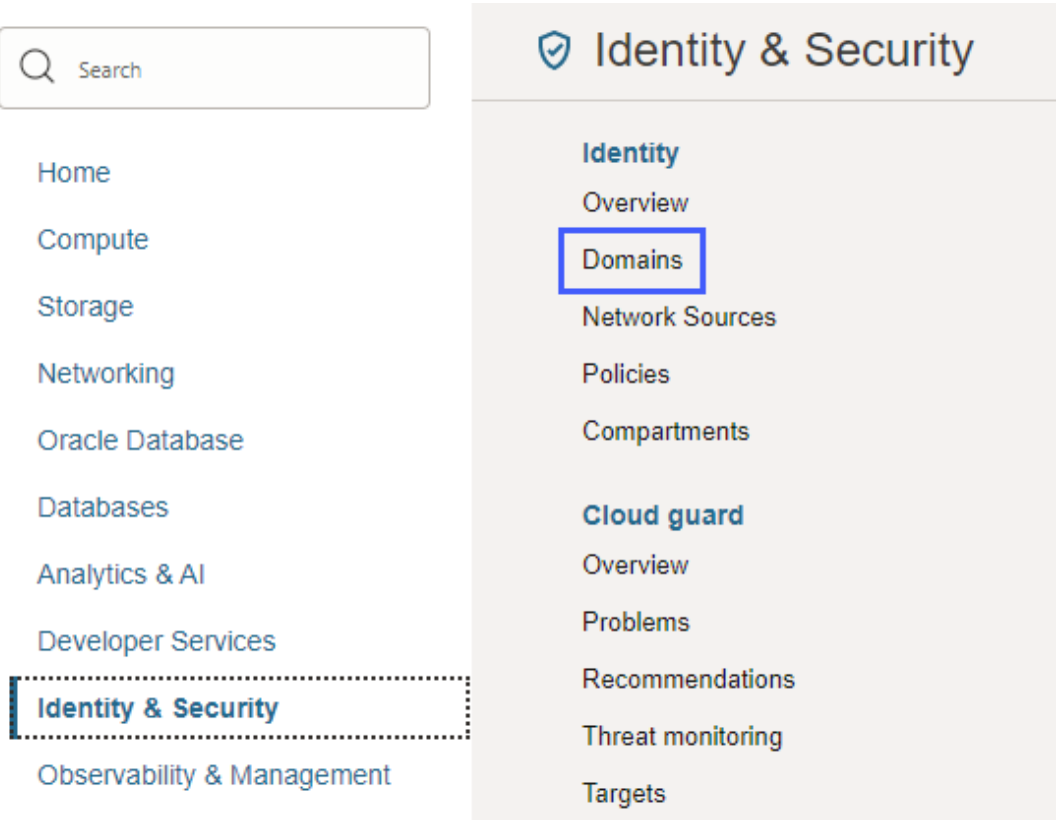
After an Oracle Integration instance has been created, assign Oracle Integration roles to groups of users to allow them to work with the features of the Oracle Integration instance.

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.

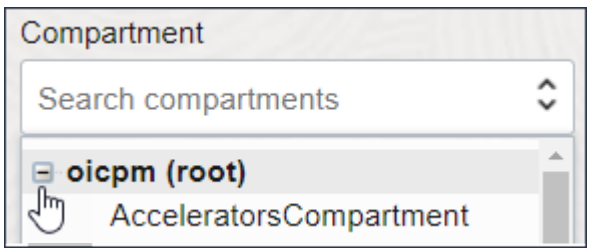
Oracle Integration provides a standard set of roles, which govern access to features. See Oracle Integration Service Roles. Depending on the Oracle Integration features your organization uses, you may choose to create groups named for the role they are granted. For example, `OICServiceAdministrators`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

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

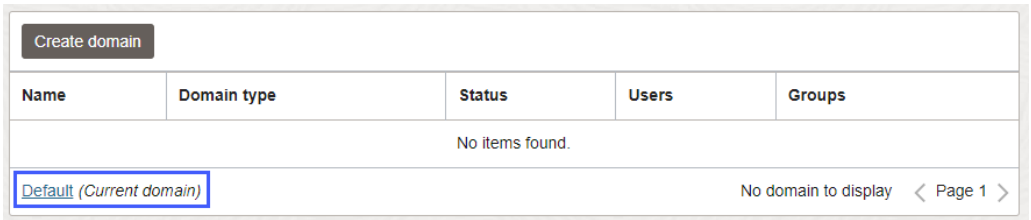


   The Domains page is displayed.

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 you want to assign to the group. Next to the role, click **Manage**.
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**.

Audit Users' Access to the Oracle Integration Instance in an Identity Domain

When required by your organization's operating procedures, audit users' access to the Oracle Integration instance and determine whether you need to change anyone's access.

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

To see the users assigned to roles in your service instance:

1. Open the Oracle Cloud Infrastructure Console.
2. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**.
3. Open your domain.
4. In the left navigation, click **Oracle Cloud Services**.
5. Open the service instance you want to view.
6. In the left navigation, click **Application roles**.
7. Expand the role you want to audit.
8. Next to **Assigned users**, click **Manage**.

   You see a list of the users assigned to the role. In the **Member type** column, **Indirect** means the user was assigned the role as part of a group.

You can edit the users in a role:

- To remove a user from the role, select the user and click **Revoke**.
- To ad a user to the role, click **+ Show available users**, select a user, 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

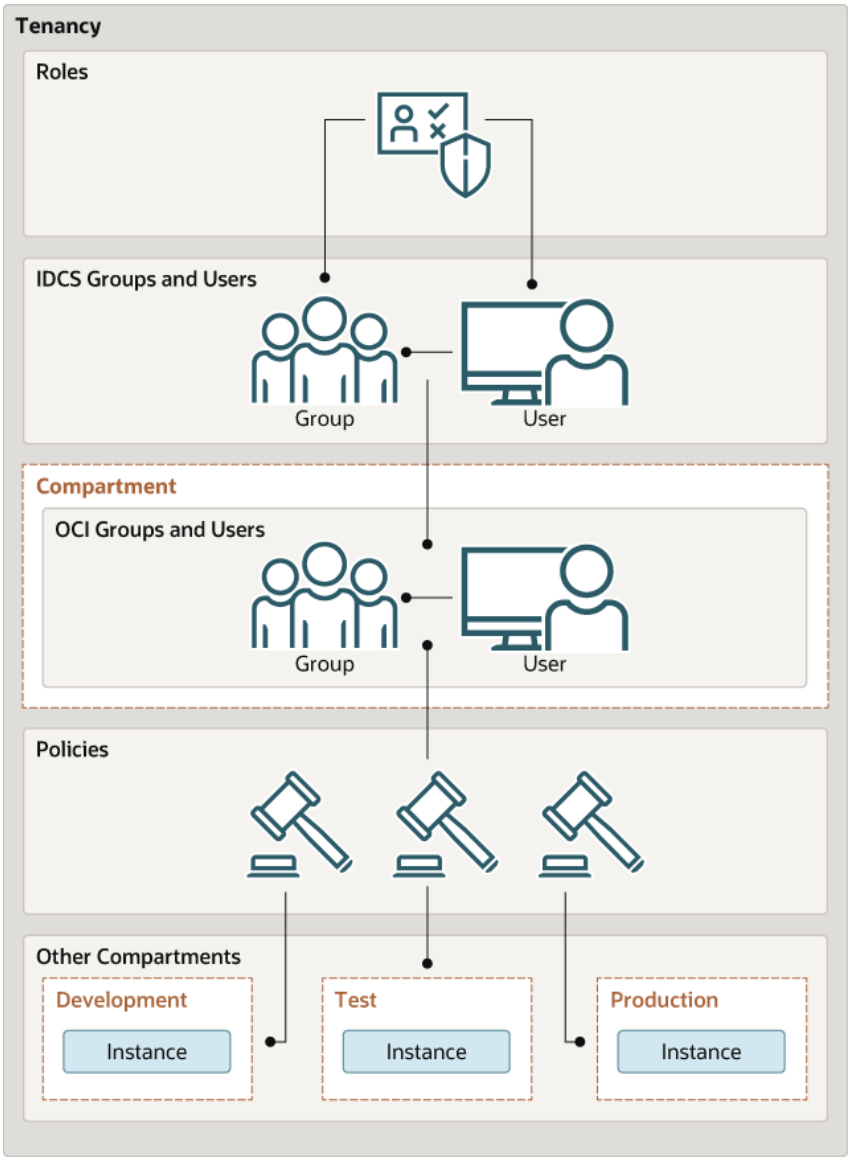
If you are not sure if your tenancy uses identity domains, see Differences Between Tenancies With and Without Identity Domains.

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:

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.

If you are federating with other identity providers, see Federating with Identity Providers in the Oracle Cloud Infrastructure documentation.

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.

Order	Task	More Information
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.
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.

Order	Task	More Information
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. Make sure you're in the compartment in which you want to create the policy. See the tips in About IAM Policies for Oracle Integration.
3. Click **Create Policy**.

4. In the Create Policy window, enter a name (for example, `IntegrationGroupPolicy`) and a description.
5. 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
6. 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
   ```
7. 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`

8. 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`

Entity	Naming convention
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**.

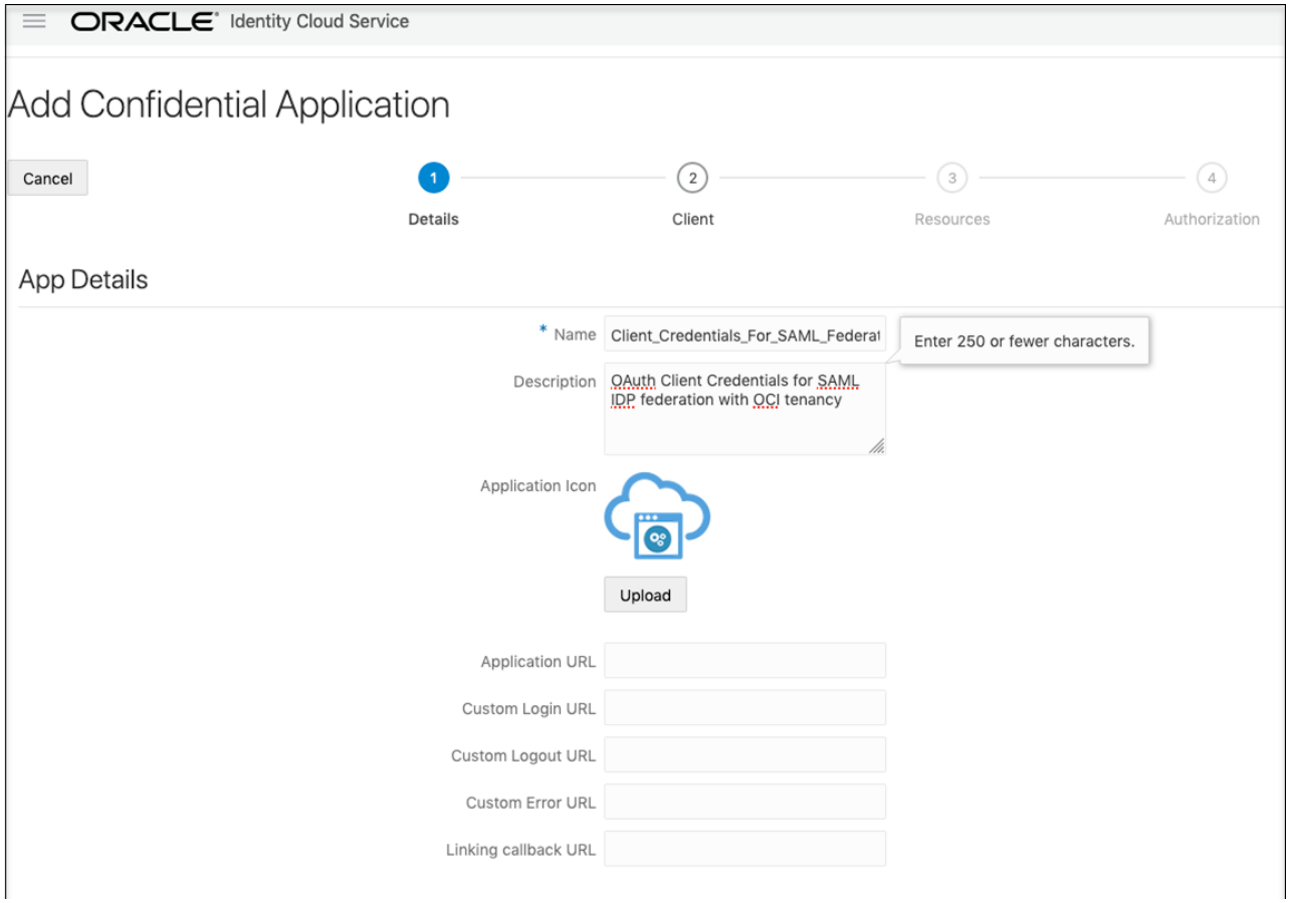
   For more information, see Create Groups in *Administering Oracle Identity Cloud Service*.

   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.

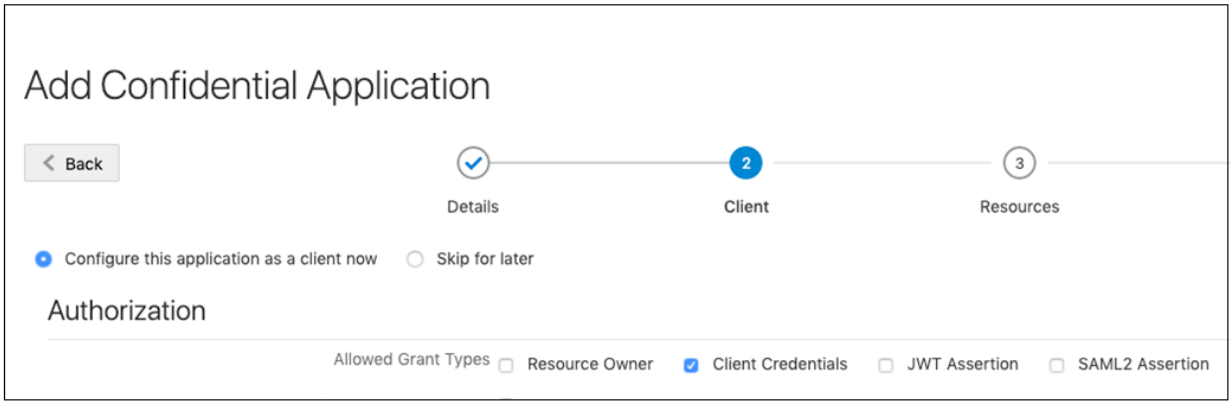
Create an OAuth Client in the Secondary Stripe

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.

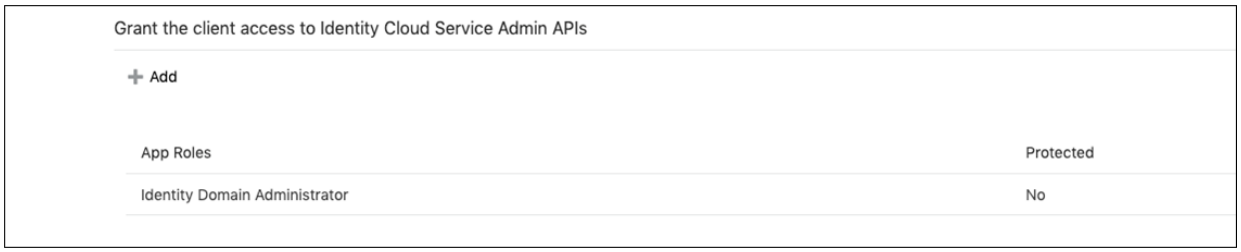
1. As an IDCS administrator, sign in to the secondary IDCS admin console.
2. Add a confidential application.
   a. Navigate to the **Applications** tab.
   b. Click **Add**.
   c. Choose **Confidential Application**.
   d. Name the application `Client_Credentials_For_SAML_Federation`.
   e. Click **Next**.



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

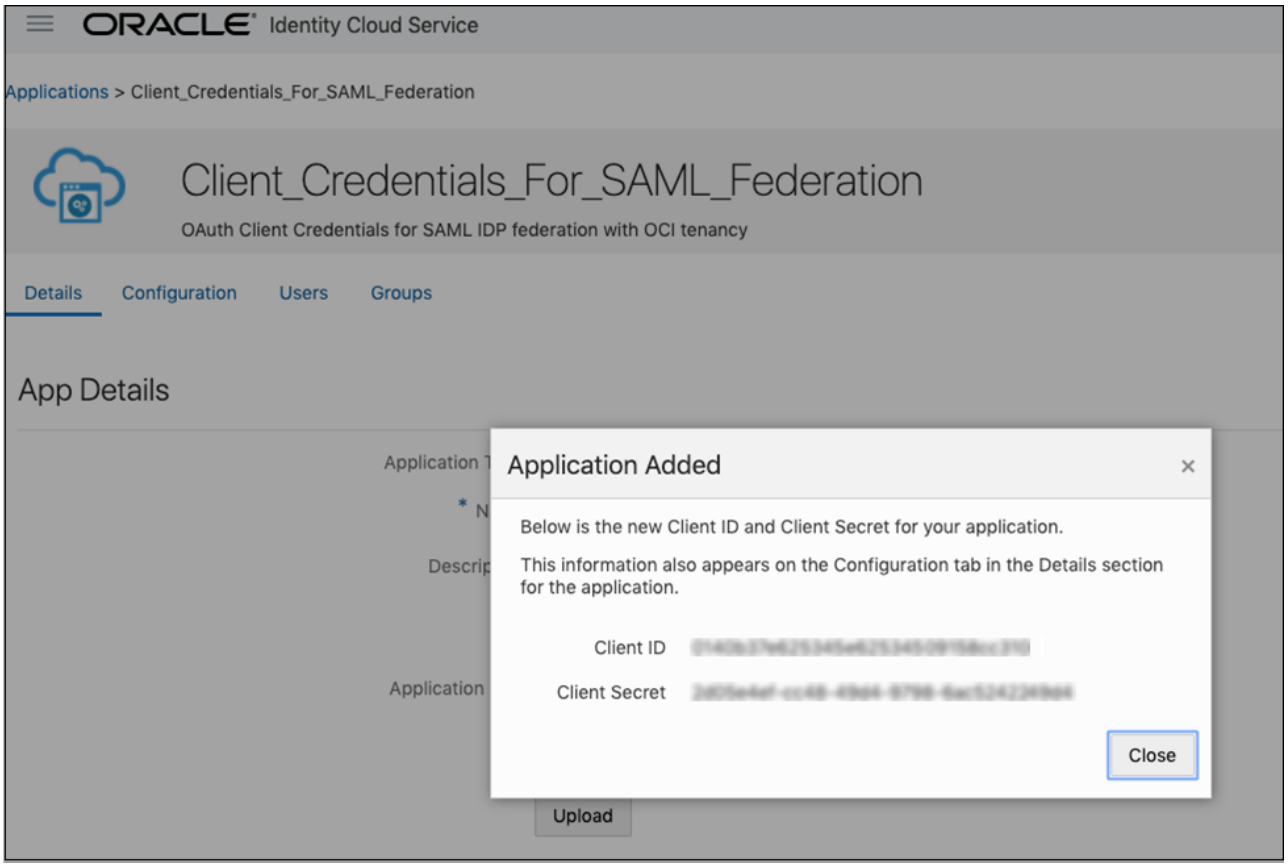


   c. Under **Grant the client access to Identity Cloud Service Admin APIs**, click **Add** and select the app role **Identity Domain Administrator**.



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.

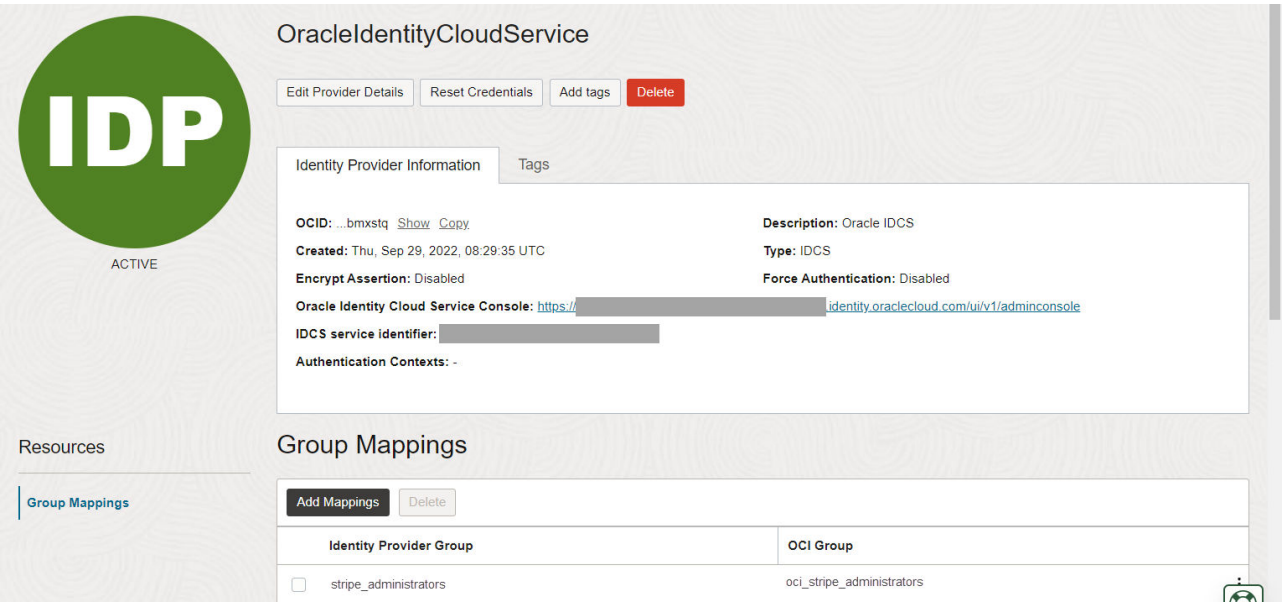
Field	Entry
Name	`<stripename>_service`
Description	`Federation with IDCS secondary stripe`
Type	Oracle Identity Cloud Service
Oracle Identity Cloud Service Base URL	Enter this URL using the format: `https://idcs-xxxx.identity.oraclecloud.com` Replace the `<idcs-xxxx>` domain part with your secondary 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* to*verb resource-type*in compartment*stripename_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).

Audit Users' Access to the Oracle Integration Instance

When required by your organization's operating procedures, audit users' access to the Oracle Integration instance and determine whether you need to change anyone's access.

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

To see the users assigned to roles in your service instance:

1. Open the Oracle Cloud Infrastructure Console.
2. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Federation**.
3. Select the identity federation in which users were created.

   For example, you might have created users in **OracleIdentityCloudService**, which is the default Oracle Identity Cloud Service (IDCS) identity federation.
4. Click the **Oracle Identity Cloud Service Console** link
5. Sign in to IDCS as an administrator.
6. Open the navigation menu and click **Oracle Cloud Services**.
7. Open the service instance you want to view.
8. Click the **Application Roles** tab.

9. Next to the role you want to audit, click ***Number*** **Users Assigned**.

   You see a list of the users assigned to the role. In the **Member Type** column, **Indirect** means the user was assigned the role as part of a group.

To edit the users in a role, click  to the far right of the role.

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.

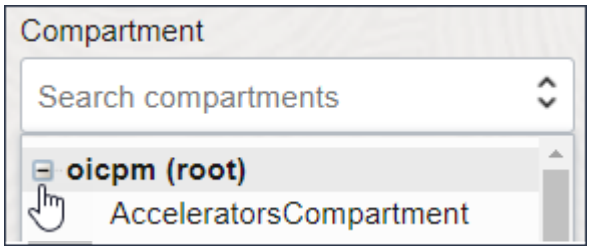
Some restrictions exist for creating instances. See Restrictions.

> **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:

Field	Description
Name	Enter a name for this instance. The name becomes part of the URL for accessing the instance.
Version	Select the version you want to use for this instance: • **Oracle Integration 3** is the latest generation of Oracle Integration, providing the latest features and infrastructure technology including Integrations, Process Automation, robotic process automation, healthcare, Visual Builder, B2B for Oracle Integration, File Server, and our portfolio of adapters. • **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. If you choose to create an Oracle Integration Generation 2 instance, see *Provisioning and Administering Oracle Integration Generation 2*. **Note**: This field appears only if you can provision both Oracle Integration Generation 2 and Oracle Integration 3 instances. Everyone can provision an Oracle Integration 3 instance. You can create a new Oracle Integration Generation 2 instance only if you have an existing Oracle Integration Generation 2 instance in the region.
Consumption model	Typically, only one consumption model is displayed, but if multiple consumption models are available in your tenancy, select the one you want to use for this instance: • **Metered (universal credit)** **Note:** The Healthcare edition is available only in tenancies that use Universal Credits. • **Subscription (OIC4SaaS)** • **Oracle Integration Government**
Edition	Select the edition you want to use for this instance: • **Standard**: Includes integrations, *standard* adapters, recipes and accelerators, Visual Builder, and File Server. • **Enterprise**: Includes all the features of Standard edition, plus additional technologies and services, including *enterprise* adapters, and enables you to design, automate, and manage your business processes in the cloud with Process Automation, perform UI-based automation with robots using robotic process automation, and support business-to-business communications using B2B for Oracle Integration. This edition also supports disaster recovery. • **Healthcare**: Includes all the features of Enterprise edition, plus additional technologies for Health Level 7 (HL7), including an MLLP adapter, a FHIR adapter, and healthcare action. This edition also supports disaster recovery. **Note:** The Healthcare edition is available only in tenancies that use Universal Credits. See Oracle Integration Editions to see what's licensed in each edition.

Field	Description
Shape	Select a shape for this instance. The shape determines when the instance receives updates, which happen every other month. • **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. If you're setting up disaster recovery, you must choose the Production shape. Only some regions allow you to choose a shape. If you don't see the option to choose a shape, your instance is created in the Production shape. For details about the shapes that each region supports, see Availability. **Note**: You can't change the shape after you create the instance. However, you can move data to another instance using the export and import features.
License type	**Subscribe to a new Oracle Integration license** **Note:** If you are provisioning Oracle Integration for SaaS, this field is read-only and displays **Subscribe to a new Oracle Integration license**. The message pack description in this entry—**License type**, doesn't apply to Oracle Integration for SaaS. For information on Oracle Integration for SaaS message packs, see the next entry—**Message packs**. Select a license type for this instance. • **Subscribe to a new Oracle Integration license**: Select this option if you want to purchase a new license. With this option, each message pack includes 5,000 messages per hour. • **Existing Oracle Fusion Middleware license (BYOL)**: Select this option if you want to use your existing license. With this option, each message pack includes 20,000 messages per hour. (This option isn't available for the Healthcare edition.)

Field	Description
Message packs	Message pack options are based on the type of Oracle Integration license you have. • For Oracle Integration: If you created a new Oracle Integration license in the cloud: – Each message pack includes 5,000 messages per hour. – You can select up to 12 message packs in the user interface. If you brought an existing Oracle Fusion Middleware license to the cloud (BYOL): – Each message pack includes 20,000 messages per hour. – You can select up to 3 message packs in the user interface. • For Oracle Integration for SaaS: – Each message pack includes one million messages per month. Note that usage is tracked on a monthly basis instead of hourly, which keeps costs predictable even when you have unpredictable hourly volumes. – You can select up to 43 message packs in the user interface. **Note:** • You are responsible for billing based on the number of message packs you select. Select enough message packs to adequately handle your instance's activity. See About Integrations Usage. • The number of message packs you subscribe to can also affect the processing time of synchronous requests. See Message Pack Usage and Synchronous Requests. • 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.
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. See Configure an Allowlist for Your Instance. **Disaster recovery**: If you want to configure disaster recovery, select **Enable disaster recovery**. This installs a primary instance in one region and a secondary instance in another region. See Introduction to Oracle-Managed Disaster Recovery in *Configuring an Oracle-Managed Disaster Recovery Solution for Oracle Integration 3*. **Tags**: Enter a key and optional value. Tags enable you to track resources within your tenancy. See Resource Tags. **Note:** If you want to configure a custom endpoint URL for this instance, you do so after the instance is created. See Configure a Custom Endpoint for an Instance.

6. Click **Create**.

   If you have any issues trying to create an instance, see Troubleshoot Oracle Integration Instance Creation.

7. 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.

- **Subscribe to a new Oracle Integration license**: Select this option if you want to purchase a new license. With this option, each message pack includes 5,000 messages per hour.
- **Existing Oracle Fusion Middleware license (BYOL)**: Select this option if you want to use your existing license. With this option, each message pack includes 20,000 messages per hour. (This option isn't available for the Healthcare edition.)

Note: If you are provisioning Oracle Integration for SaaS, this field is read-only and displays **Subscribe to a new Oracle Integration license**. The message pack description in this entry—**License type**, doesn't apply to Oracle Integration for SaaS. For information on Oracle Integration for SaaS message packs, see the next entry—**Message packs**.

Choose a Message Pack Number

Select a suitable number of message packs to handle the message usage you expect for your instance.

Message pack options are based on the type of Oracle Integration license you have.

- For Oracle Integration:
  If you created a new Oracle Integration license in the cloud:
  - Each message pack includes 5,000 messages per hour.
  - You can select up to 12 message packs in the user interface.

  If you brought an existing Oracle Fusion Middleware license to the cloud (BYOL):
  - Each message pack includes 20,000 messages per hour.
  - You can select up to 3 message packs in the user interface.
- For Oracle Integration for SaaS:
  - Each message pack includes one million messages per month.
    Note that usage is tracked on a monthly basis instead of hourly, which keeps costs predictable even when you have unpredictable hourly volumes.
  - You can select up to 43 message packs in the user interface.

Note:

- You are responsible for billing based on the number of message packs you select. Select enough message packs to adequately handle your instance's activity. See About Integrations Usage.
- The number of message packs you subscribe to can also affect the processing time of synchronous requests. See Message Pack Usage and Synchronous Requests.
- 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.

Troubleshoot Oracle Integration Instance Creation

This topic provides some tips for troubleshooting Oracle Integration instance creation.

Oracle Integration 3 is not available to all users or Missing parameter (isByol)

If you receive the error "Missing parameter (isByol)" when you click **Create**, perform the following steps:

1. Ensure you can see the Oracle Integration service in the Oracle Cloud Infrastructure Console.
    a. In the Oracle Cloud Infrastructure Console, open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**.
    b. Open your domain. The default domain is **OracleIdentityCloudService**.
    c. On the left, click **Oracle Cloud Services**.
    d. Search for `Integration` for the Oracle Integration service:
        - For Oracle Integration, you should see **INTEGRATIONCAUTO**.
        - For Oracle Integration for SaaS, you should see **INTEGRATIONSUB**.
    e. If you see the Oracle Integration service, submit a Service Request to Oracle Support. If you don't see it, move on to the next step.
2. If you don't see the Oracle Integration service, confirm that your Cloud Account Administrator activated the Oracle Integration service (by clicking the link in the email titled "XXX").
3. If the administrator didn't activate the service, have them do so, then try again to create an Oracle Integration instance.
4. If your Cloud Account Administrator already tried to activate the service or didn't receive the email, contact your account manager to confirm you have a subscription for Oracle Integration.

401: Authorization failed or 404: Not Found

If you click the Oracle Integration instance name just after creating the instance and receive a `401: Authorization failed` or a `404: Not Found` error, instance creation might still be in progress. Wait a minute and try again.

Enable Technologies

You must enable some technologies and services in the Oracle Cloud Infrastructure Console before you can start using them. Others are available without being enabled.

Must Be Enabled

To use the following technologies and services, 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*.

> **Note:**
>
> Additionally, some technologies and services are available only in Enterprise edition or Healthcare edition. For example, healthcare-related components are available only in Healthcare edition. See Oracle Integration Editions.

Don't Require Enabling

The following technologies are available without being enabled:

- Integrations
- B2B for Oracle Integration
- Robotic process automation

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 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	You can upgrade from the Standard or Enterprise editions to the Healthcare edition. However, once you have the Healthcare edition, you can't downgrade to the Standard or Enterprise editions. See Oracle Integration Editions to see what's licensed in each edition.
License Type	To change your license type, select an option: • **Subscribe to a new Oracle Integration license**: Select this option if you want to purchase a new license. With this option, each message pack includes 5,000 messages per hour. • **Existing Oracle Fusion Middleware license (BYOL)**: Select this option if you want to use your existing license. With this option, each message pack includes 20,000 messages per hour. (This option isn't available for the Healthcare edition.) **Note:** If you are provisioning Oracle Integration for SaaS, this field is read-only and displays **Subscribe to a new Oracle Integration license**. The message pack description in this entry—**License type**, doesn't apply to Oracle Integration for SaaS. For information on Oracle Integration for SaaS message packs, see the next entry—**Message packs**. There is no downtime when you change license types.

Field	Description
Message Packs	Message pack options are based on the type of Oracle Integration license you have. • For Oracle Integration: If you created a new Oracle Integration license in the cloud: – Each message pack includes 5,000 messages per hour. – You can select up to 12 message packs in the user interface. If you brought an existing Oracle Fusion Middleware license to the cloud (BYOL): – Each message pack includes 20,000 messages per hour. – You can select up to 3 message packs in the user interface. • For Oracle Integration for SaaS: – Each message pack includes one million messages per month. Note that usage is tracked on a monthly basis instead of hourly, which keeps costs predictable even when you have unpredictable hourly volumes. – You can select up to 43 message packs in the user interface. There is no instance downtime when you change the number of message packs. However, note that message pack updates can fail when maintenance and security patching are in progress. **Note:** • You are responsible for billing based on the number of message packs you select. Select enough message packs to adequately handle your instance's activity. See About Integrations Usage. • The number of message packs you subscribe to can also affect the processing time of synchronous requests. See Message Pack Usage and Synchronous Requests. • 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.
Show Advanced Options	**Custom Endpoint:** See Configure a Custom Endpoint for an Instance.

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.

You are responsible for billing based on the number of message packs you select. Select enough message packs to adequately handle your instance's activity. See About Integrations Usage.

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.

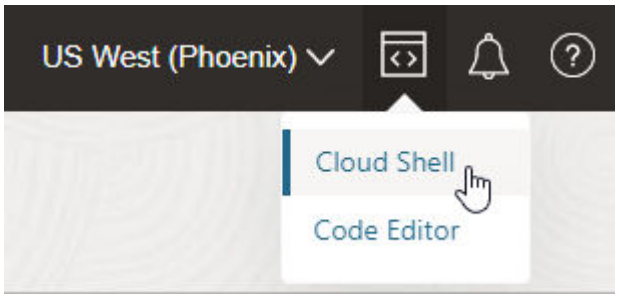
> **WARNING:**
>
> - Increasing the number of message packs increases your bill.
> - The number of message packs that you purchase does not impact your instance's concurrency limits. See Service Limits.

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.

Edit the Data Retention Period for an Instance

By default, Standard and Enterprise edition instances retain data for 32 days, and Healthcare edition instances retain data for 184 days. If you have an Enterprise edition instance, you can change the data retention period if you want.

> **Note:**
>
> - You can't change the retention period for Standard or Healthcare edition instances.
> - Increasing your data retention period will increase your message consumption, and may increase your message pack consumption cost.
> - If you later decrease your data retention period, your message consumption will decrease, but any data older than the newly selected period will be deleted when you save your selection.

For details on how extended data retention periods affect your message usage, see About Integrations Usage.

To edit the data retention period:

1. On the Integration instance details page, next to **Data retention**, click **Manage**.

   The Manage data retention dialog is displayed.
2. Select a new data retention period.

   Make sure to consider how this change will affect your message consumption, how it might affect your message pack cost, and, if decreasing your data retention period, the effect of losing any data older than the newly selected period.
3. Click **Save**.

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:

Button or Field	Description
Open console button	Click **Open console** to access Oracle Integration. See Get Familiar with the Home Page in *Getting Started with Oracle Integration 3*. **Note**: Alternatively, you can access Oracle Integration from the Integration instances page. Next to the instance you want to access, on the far right, click ⋮, and choose **Open console**.
Edit button	Click **Edit** to edit the settings for your instance. See Edit the Edition, License Type, Message Packs, and Custom Endpoint of an Instance.
Move button	Click **Move** 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 **Add tags** to add tags to the instance. You can use tags to search for and categorize your instances in your tenancy. See Resource Tags.
More Actions menu	Click **More Actions** to see other options: • **Stop**/**Start**: See Stop and Start an Oracle Integration Instance. • **Delete**: See Delete an Instance.

Button or Field	Description
Integration instance information tab	• **Created**: Shows the date the instance was created. • **Updated**: Shows the date the instance was last updated (for example, the last time it was started). • **Version**: Appears only when you have or can create Oracle Integration Generation 2 and Oracle Integration 3 instances. • **Consumption model**: Shows the consumption (billable) model used for the instance—Metered (Universal Credits), Subscription (OIC4SaaS), or Oracle Integration Government. • **Edition**: Shows the edition selected for the instance—Standard, Enterprise, or Healthcare. • **OCID**: Shows the value that uniquely identifies the instance. Click **Show** to see the full OCID. Click **Copy** to copy it. • **Service console URL**: Shows the URL to access the associated Oracle Integration instance application. Click **Show** to see the full URL. Click **Copy** to copy it. • **Shape**: Shows the shape selected for the instance—Development or Production. • **License type**: Shows the type of license used for the instance—either a new cloud license or an existing license brought over from Oracle Fusion Middleware (The second option isn't available for the Healthcare edition.) If you are viewing an Oracle Integration for SaaS instance, the License Type field is not displayed. • **Message packs**: Shows the number of message packs and the quantity of messages in each pack. See Choose a Message Pack Number. • **File Server**: Shows whether File Server is enabled for the instance. If it isn't, you can click the link to enable it. Cannot be undone. See Enable File Server in *Using File Server in Oracle Integration 3*. • **Visual Builder**: Shows whether Visual Builder is enabled for the instance. If it isn't, you can click the link to enable it. Cannot be undone. See Use Visual Builder in Oracle Integration. • **Process Automation**: Shows whether Process Automation is enabled for the instance. If it isn't, you can click the link to enable it. Can't be undone. See Enable Process Automation with Oracle Integration 3 in *Administering Oracle Cloud Infrastructure Process Automation*. • **Data retention**: Shows how long data is retained for the instance. By default, Standard or Enterprise edition instances retain data for 32 days, but you can increase the data retention period if you want (this incurs extra costs). Healthcare edition instances retain data for 184 days. To change the data retention period, click **Manage**. See Edit the Data Retention Period for an Instance. **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.

Button or Field	Description
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	Lists tags associated with this instance. You can use tags to search for and categorize your instances in your tenancy. See Resource Tags.
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.
Associated services page	Lists services associated with this instance, such as File Server and Visual Builder.
Private endpoints page	Lists private endpoints associated with this instance. See Connect to Private Resources.
Network access page	View and manage allowlist rules. See Configure an Allowlist for Your Instance.
Logs page	Enable and disable the capture of logging activity. See Capture the Activity Stream of Integrations in the Oracle Cloud Infrastructure Console.

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 features 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 

.

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.

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:

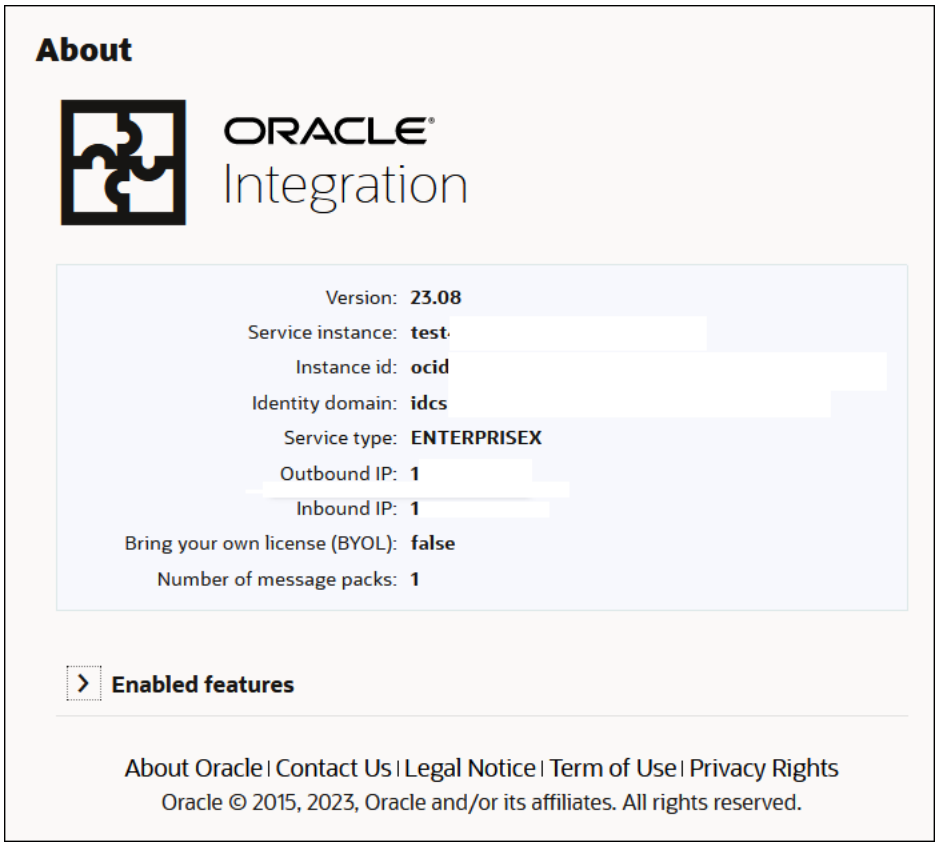
Obtain the Inbound and Outbound IP Addresses of the Oracle Integration Instance

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

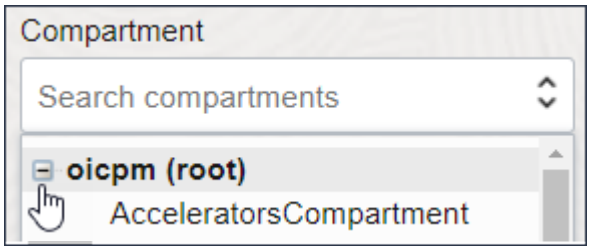
For information about console announcements, the types of information they contain, viewing options, and managing the email delivery of announcements, see Console Announcements.

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 to apply the latest updates to your instance.

Your Update Window is Determined by Instance Shape

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's applied to a production instance.

Instance Shape is Selected During Provisioning

The user 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 features.

> **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.

No Downtime During Update

Your service won't experience any downtime as part of the update.

Updates Are Mandatory

You can't skip or reschedule an update. Updates are mandatory, and Oracle can't accommodate individual schedules.

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*.

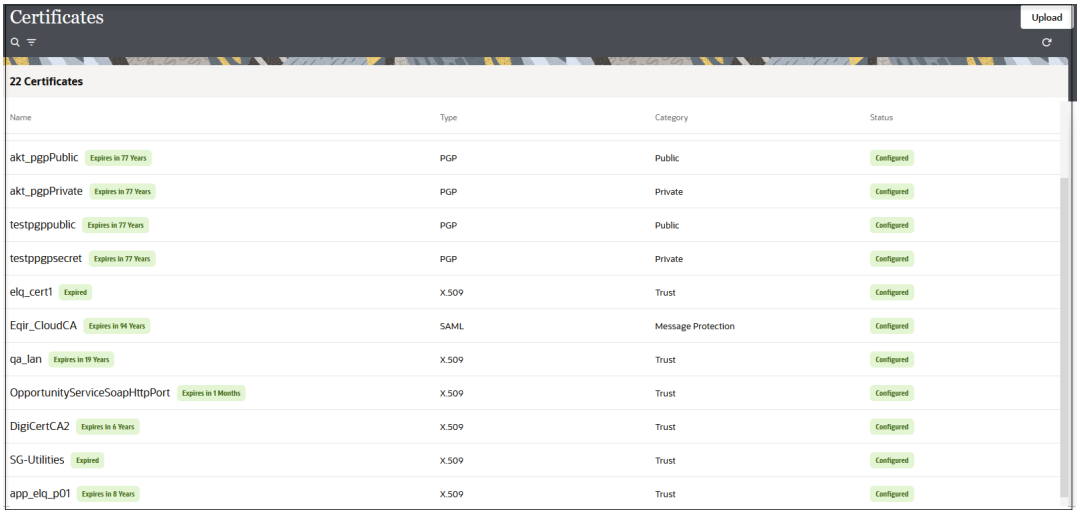
You can manage errors from the Errors pages in Oracle Integration at the integration level, connection level, or specific integration instance level. See Manage Errors in *Using Integrations in Oracle Integration 3*.

Upload a Certificate to Connect with External Services

Certificates allow Oracle Integration to connect with external services. If the external service/endpoint needs a specific certificate, request the certificate and then import it into Oracle Integration.

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.
   - Digital Signature
   - X.509 (SSL transport)
   - SAML (Authentication & Authorization)
   - PGP (Encryption & Decryption)
   - Signing key

Digital Signature

The digital signature security type is typically used with adapters created with the Rapid Adapter Builder. See Learn About the Rapid Adapter Builder in Oracle Integration in *Using the Rapid Adapter Builder with Oracle Integration 3*.

1. Click **Browse** to select the digital certificate. The certificate must be an X509Certificate. This certificate provides inbound RSA signature validation. See RSA Signature Validation in *Using the Rapid Adapter Builder with Oracle Integration 3*.
2. Click **Upload**.

X.509 (SSL transport)

1. Select a certificate category.
   a. **Trust**: Use this option to upload a trust certificate.
      i. Click **Browse**, 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 **Browse**, 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 **Browse**, 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 **Browse**, 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 **Browse**, 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 **Browse** 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.
4. Click **Upload**.

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.
> - You cannot use a private endpoint to connect to resources deployed on a non-Oracle Cloud Infrastructure cloud (for example, Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP)). Instead, use the connectivity agent for this type of connection (discussed below).

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. • 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*.

Area	Private endpoint	Connectivity agent
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

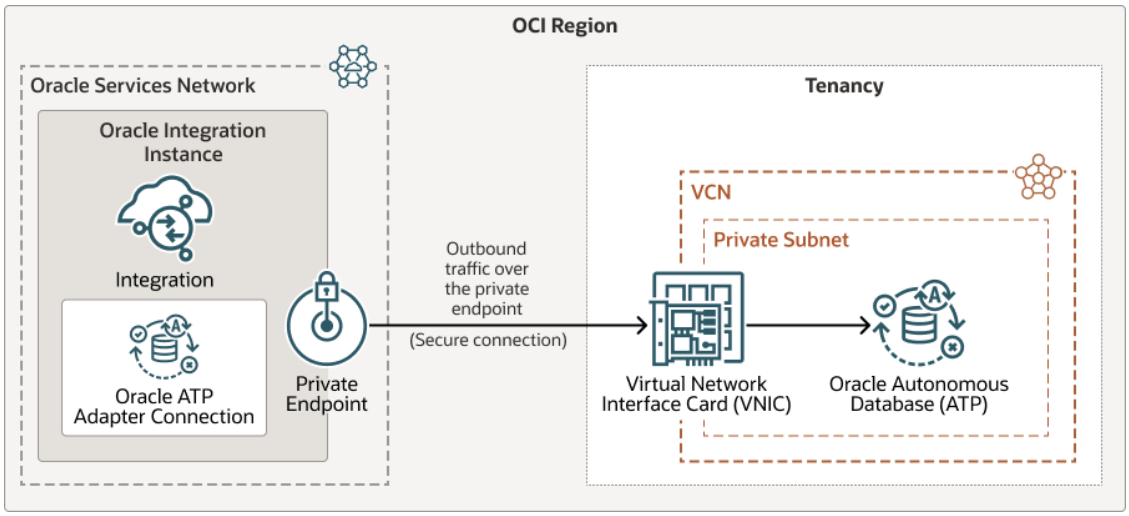
To use the private endpoint to connect to a private resource, create a connection based on an adapter that supports private endpoints, and select **Private endpoint** as the **Access type**.

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 private resources must be in the same customer tenancy in which Oracle Integration is provisioned.
- The VCN must be in the same region as your Oracle Integration instance.
- The VCN and subnet can be in any compartment within the customer tenancy.
- The subnet can be public or private.

> **Note:**
>
> When you create a private endpoint, three IPs will be selected from the available pool of free IPs in the classless inter-domain routing (CIDR) block; they won't be from the network reserved IPs.

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 private resources must be in the same customer tenancy in which Oracle Integration is provisioned.
   - The VCN must be in the same region as your Oracle Integration instance.
   - The VCN and subnet can be in any compartment within the customer tenancy.
   - 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 and Adapters that Support Connecting to Private Endpoints 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.

Error	Reason for the error and next steps

`{"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")`
or
`{"detail":"."status":"HTTP 500 Internal Server Error","Operation (testConnection) failed: This connection is configured with an address which is not in an allowable range","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.

Be aware of the following:

- 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.
- 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.
- An API gateway doesn't redirect access points such as design-time, Visual Builder, and Process Automation. If you use an API gateway for your instance, you'll need to access these resources using the original URLs. See Manage Oracle Integration Endpoints Using API Gateway.

You can create the following types of custom endpoints for an Oracle Integration instance:

- Oracle-managed custom endpoint
  If you use this option, Oracle procures and manages the public certificate for your host name.
- Customer-managed custom endpoint
  This option is appropriate if you want to use your own load balancer. However, be aware that, with this option, you are responsible for keeping your certificate up to date. If you let your certificate expire, any applications that use the custom endpoint will fail.

If you want to switch from a customer-managed custom endpoint to an Oracle-managed custom endpoint, or vice versa, you need to delete your existing custom endpoint, complete the prerequisites for the new type of custom endpoint, and then create the new custom endpoint.

Configure an Oracle-Managed Custom Endpoint

If you want Oracle to procure and manage the public certificate for your custom host name, you can create an Oracle-managed custom endpoint.

Perform the following steps to create an Oracle-managed custom endpoint for your instance.

1. Complete prerequisites.
2. Create the Oracle-managed customer endpoint.
3. Complete post-configuration tasks.

Prerequisites for Configuring an Oracle-Managed Custom Endpoint

To configure an Oracle-Managed custom endpoint, complete the following prerequisites.

Task	Where to perform the task	Associated documentation
Create your Oracle Integration instance	Oracle Cloud Infrastructure Console	Create an Oracle Integration Instance **Note:** • You add a custom endpoint when *editing* an instance, not during creation, so you must create the instance as a prerequisite. • You must have direct access to your Oracle Integration instance.
Choose a vanity URL or custom hostname for your Oracle Integration instance	N/A	N/A

Task	Where to perform the task	Associated documentation
Create a public DNS zone	Oracle Cloud Infrastructure Console	Creating a Public DNS Zone **Note:** DNS zones are region-specific. If you have Oracle Integration instances in multiple regions, you must create a DNS zone with a unique subdomain for each region.
Delegate the DNS zone and update the name servers with your registrar	Your domain name registrar	Delegating a Public DNS Zone **Note:** If you created DNS zones for multiple regions, you must perform this task for each DNS zone in their respective subdomain.
Register your Oracle Integration instance hostname with the DNS zone by adding a CNAME record	Oracle Cloud Infrastructure Console	Adding a Record to a DNS Zone
Create IAM policies to allow your Oracle Integration tenancy to manage the public DNS zone	Oracle Cloud Infrastructure Console	Create IAM Policies

Create IAM Policies

You must create the following IAM policies to allow your Oracle Integration instance to manage the DNS resources.

- A policy to grant your Oracle Integration instance to manage **dns-zones** and **dns-records** resources in your tenancy:

  ```
  ALLOW dynamic-group group-Name TO READ dns-zones IN compartment compartment-name
  ```

  ```
  ALLOW dynamic-group group-Name TO USE dns-records IN compartment compartment-name WHERE ALL {target.dns-zone.name='dns-zone-name'}
  ```

  where:

  - *group-Name* is the name of the dynamic group that defines the compartment that stores your Oracle Integration instance.
  - *compartment-name* is the name of the compartment that stores the DNS resources.
  - *dns-zone-name* is the public DNS zone you created.

  > **Note:**
  >
  > - The dynamic group is defined in the domain in which the Oracle Integration instance was created.
  > - The matching rule of the dynamic group definition should point to the IDCS application ID. For example:
  >
  >   ```
  >   Matching rule: any {resource.id='service-instance-IDCS-app-client-ID'}
  >   ```

- A generic endorse policy to allow your Oracle Integration instance to manage certificate resources in the Oracle Integration tenancy. This is the endorse part of the cross-tenant policy.

```
ENDORSE any-user TO MANAGE certificate-authority-family IN any-tenancy
```

For more information, see Managing DNS Resources Across Tenancies.

Create the Oracle-Managed Custom Endpoint

After completing the prerequisites, perform the following steps to configure an Oracle-managed 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. On the left, under **Resources**, click **Custom Endpoint**.
4. Click **Create custom endpoint**.
5. Select **Oracle managed**.
6. Make sure the correct compartment is selected.
7. Select the DNS zone you created as a prerequisite.
8. Enter your custom host name for the instance.
9. Click **Create**.

After configuring your Oracle-managed custom endpoint, you must complete some post-configuration tasks.

Post-Configuration Tasks for an Oracle-Managed Custom Endpoint

After creating your Oracle-managed custom endpoint, perform the following post-configuration tasks:

- Modify your custom hostname IP record to point to the Oracle Integration origin. If you use a CNAME record, you must enter the FQDN for your load balancer's public IP address.
- 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, they will continue to work without any issues. However, if you want to update your integrations to use the custom endpoint:
  – For triggers, deactivate and re-activate those integrations to regenerate the WSDLs.
  – For parent-child integrations, edit the existing connection to replace the hostname with the custom host; test and save the connection; then reactivate the integration.

> **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.

Configure a Customer-Managed Custom Endpoint

If you want to use your own load balancer, you can create a customer-managed custom endpoint. However, be aware that, with this option, you are responsible for keeping your certificate up to date. If you let your certificate expire, any applications that use the custom endpoint will fail.

Perform the following steps to create a customer-managed custom endpoint for your instance.

1. Complete prerequisites.
2. Create the customer-managed custom endpoint.
3. Complete post-configuration tasks.

Prerequisites for Configuring a Customer-Managed Custom Endpoint

To configure a customer-managed custom endpoint, complete the following prerequisites:

1. Create your Oracle Integration instance.

   > **Note:**
   >
   > - You add a custom endpoint when *editing* an instance, not during creation, so you must create the instance as a prerequisite.
   > - You must have direct access to your Oracle Integration instance.

2. Choose a vanity URL or custom hostname for your Oracle Integration instance.
3. Register the hostname with either the Oracle Cloud Infrastructure DNS or your DNS provider.
4. 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.
5. Front-end your instance with a load balancer, such as Oracle Cloud Infrastructure Load Balancer, to validate and terminate SSL for you custom hostname.

   > **Note:**
   >
   > If you use Oracle Cloud Infrastructure Load Balancer, you must set up a NAT gateway in the VCN/subnet where you plan to create your load balancer.

Task	Settings to use	Associated documentation
In the VCN/subnet where you will create your load balancer, add a routing rule for the Oracle Integration public IP address	• **Target Type**: Select NAT gateway. • **Destination CIDR Block**: `Oracle Integration_public_IP /32` You can get the Oracle Integration IP address via nslookup command. • **Compartment**: Select the compartment where your Oracle Integration instance is located. • **Target**: Your NAT gateway	VCN Route Tables
Set up a load balancer	• **Visibility type**: Select **Public**. • **Bandwidth**: Select **Flexible** and set the minimum and maximum bandwidth to `10 Mbps`.	Creating a Load Balancer
Configure a listener	• **Protocol**: Select **HTTPS**. • **Port**: Enter `443`. • **Use SSL**: Select this option. • **Certificate resource:** Select **Load balancer managed certificate** or **Certificate service managed certificate** and upload your custom hostname certificate.	Listeners for Load Balancers
Create a backend set	• **Use SSL**: Select this option. • **Certificate resource:** Select **Load balancer managed certificate** and upload the Oracle Integration certificate and certificate chain obtained through the browser.	Backend Sets for Load Balancers
Add Oracle Integration as a backend server	• **IP address**: Enter the Oracle Integration IP address you used in the routing rule. • **Certificate resource:** Select **Load balancer managed certificate** and upload the Oracle Integration certificate and certificate chain obtained through the browser.	Backend Servers for Load Balancers
Update the health check policies	• **Protocol**: Select **TCP**. • **Port**: Enter `443`.	Editing a Load Balancer's Health Check Policies

Task	Settings to use	Associated documentation
Add the certificate and certificate chain for your custom hostname	• Select **Choose SSL certificate file**, and upload the certificate provided by your certificate provider. • Select **Choose CA certificate file**, and upload the certificate chain provided by your certificate provider. • Select **Specify private key**, and upload the private key file.	SSL Certificates for Load Balancers
Set up logging	N/A	Logging for Load Balancers
Add the load balancer to the Oracle Integration allowlist	N/A	Configure an Allowlist for Your Instance
If you want to create other policies to protect the endpoint (for example, DDOS, smuggling, or restricting traffic for geo-political reasons), manage the policies in the load balancer	N/A	Details for Load Balancing (information on writing policies to control access to the Load Balancer service)

Create the Customer-Managed Custom Endpoint

After completing the prerequisites, 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. On the left, under **Resources**, click **Custom Endpoint**.
4. Click **Create custom endpoint**.
5. Select **Customer Managed**.
6. Enter your custom host name for the instance.
7. Click **Create**.

After configuring your custom endpoint, you must complete some post-configuration tasks, like pointing your custom host IP record to your load balancer.

Post-Configuration Tasks for a Customer-Managed Custom Endpoint

After configuring your custom endpoint, perform the following post-configuration tasks:

- Modify your custom hostname IP record to point to your load balancer. If you use a CNAME record, you must enter the FQDN for your load balancer's public IP address.
- 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, they will continue to work without any issues. However, if you want to update your integrations to use the custom endpoint:
  - For triggers, deactivate and re-activate those integrations to regenerate the WSDLs.
  - For parent-child integrations, edit the existing connection to replace the hostname with the custom host; test and save the connection; then reactivate the integration.

> **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.

Edit or Delete a Custom Endpoint

You can't edit a custom endpoint. You must delete and recreate it. To delete your custom endpoint, complete the following steps.

For example, if you want to switch from a customer-managed custom endpoint to an Oracle-managed custom endpoint, or vice versa, you need to delete your existing custom endpoint, complete the prerequisites for the new type of custom endpoint, and then create the new custom endpoint.

> **Note:**
>
> You won't be able to create a new custom endpoint immediately after deleting your custom endpoint. You'll have to wait a few minutes for the update to complete.

1. Open the Oracle Cloud Infrastructure Console.
2. Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Integration**.
3. Open your instance.
4. On the left, under **Resources**, click **Custom Endpoint**.
5. Click .
6. Click **Delete**.
7. Confirm deletion.

Restrict Access to an Instance Using the Self-Service Allowlist

Restrict the networks that have access to your Oracle Integration instance, including File Server, by configuring allowlists (formerly a whitelists).

- About the Allowlist
- Prerequisites for Configuring an Allowlist

- Configure an Allowlist for Your Instance
- REST API for Allowlisting

About the Allowlist

An allowlist lets you limit access to Oracle Integration and File Server. You configure the Oracle Integration allowlist when you create the instance or any time afterward. You configure the File Server allowlist when you enable File Server or any time afterward.

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)

Only the specified IP addresses, CIDR blocks, 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.

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

What Kind of Access Can Be Managed by an Allowlist

Your instance allowlist lets you manage access to Oracle Integration and/or File Server for the following entities:

- Your organization's VCN, through the service gateway, if you have one
- Specified partner networks and applications, specified by IP addresses or CIDR blocks
- SOAP requests
- REST requests that aren't handled by an API gateway, if you're using one
- If you *are* using an API gateway, you add the API gateway's VCN to the allowlist. The API gateway manages access for all REST traffic in that VCN. Only calls from APIs deployed to the API gateway are passed through to Oracle Integration. See Manage Oracle Integration Endpoints Using API Gateway.

> **Note:**
>
> Visual Builder and Process Automation bypass the API gateway.

Limitations

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

Prerequisites for Configuring an Allowlist

You must add all resources that require access to your instance to your allowlist. Before you create your allowlist, you should determine what those resources are and collect the information you'll need to add to the allowlist.

Collect the following information before creating your allowlist:

1. **Your organization's VCN OCID**
   The resources in your organization's virtual cloud network (VCN) should be able to access Oracle Integration. 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. **Outbound IP addresses for applications that are event sources**
   All event sources, such as Oracle Fusion Cloud Applications ERP events, need access to Oracle Integration.

   To get these outbound IP addresses, contact the application providers.

3. **Outbound 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.

   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

   To get the outbound IP address for your SaaS instance, go to the **About** dialog in Oracle Integration. See Obtain the Inbound and Outbound IP Addresses of the Oracle Integration Instance.

   For a list of external IP addresses (by data center) 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 .

4. **Outbound IP addresses for partner systems that require access to Oracle Integration and File Server**
   All partner networks and applications that require access to Oracle Integration and File Server must be added to the allowlist. Make sure you consider all partner systems when compiling the list. For example, if a CRM platform requires access, you must add the individual IP address 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.

5. **Your API gateway VCN** (if using one)
   If you're using an API gateway to manage Oracle Integration endpoints, add the API gateway VCN to the allowlist. See Manage Oracle Integration Endpoints Using API Gateway.

You must also enable loopback in the allowlist so that Oracle Integration and File Server can call themselves. For example, enabling loopback allows Oracle Integration to call its own REST APIs.

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 your 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.

Make sure you have all the necessary information for the resources you need to add to your allowlist. See Restrict Access to an Instance Using the Self-Service Allowlist.

To configure an allowlist for your instance, perform the following steps:

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 Edit network access dialog is displayed. You can skip to step 7.
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 Edit network access dialog is displayed.
7. In the Edit network access dialog, make sure **Restrict Network Access** is selected so that you can add and apply allowlist rules.

   When this option is selected, only users from networks that meet the configured settings are allowed to access your Oracle Integration instance. If you don't select this option, there are no allowlist rules, and therefore no network restrictions to access your instance.

   > **Caution:**
   >
   > If you deselect **Restrict Network Access** after configuring allowlist rules, all configured allowlist rules are deleted.
8. If you want to allow Oracle Integration to call itself, select **Enable Loopback**.

   > **Note:**
   >
   > If you enable loopback, any Oracle Integration instance 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.

This setting doesn't apply to File Server.

9. Configure your allowlist rules.
   a. If you don't have any rules yet, you see a blank rule. If you already have rules, you'll need to click **Add Rule**, located below the last rule in the list, to add a new rule. You might need to scroll down to see the button.
   b. In the **Protocol** field, select an option.
      - **HTTP and File Server**: Apply the rule to Oracle Integration and File Server.
      - **HTTP**: Apply the rule only to Oracle Integration.
      - **File Server**: Apply the rule only to File Server.
   c. In the **Type** field, select the type of rule to configure, and then specify the required information.
      - **IP Address/CIDR Block**: Provide access to an IP address or a CIDR block (an IP address range).
      - **Virtual Cloud Network**: Provide access to a specific virtual cloud network (VCN). To display a list of networks in other compartments, click **Change Compartment**. In addition to a specific VCN, you can specify an IP address or IP address range within the VCN.
      - **Virtual Cloud Network OCID** (not available for File Server): Provide access to an Oracle Cloud ID (OCID) of the VCN. For information about the OCID format, see Resource Identifiers.
   d. To add another rule, click **Add Rule**.
10. After adding all the desired rules to the allowlist, click **Save**.

    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**.

REST API for Allowlisting

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

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

Manage Oracle Integration Endpoints Using API Gateway

You can manage Oracle Integration endpoints using API Gateway.

The API Gateway service enables you to publish APIs (such as integrations) with private endpoints that are accessible from within your network, and which you can expose with public IP addresses if you want them to accept internet traffic. The endpoints support API validation, request and response transformation, CORS, authentication and authorization, and request limiting.

Using a single API gateway as a front end for your Oracle Integration instance enables you to present a single cohesive API to API consumers and API clients, even though it actually consists of multiple integrations. You can use a single API gateway to link multiple back-end services (such as load balancers, compute instances, and OCI Functions) into a single consolidated API endpoint.

- About API Gateways
- Implement an API Gateway for Oracle Integration

Additional API Gateway Documentation

- API Gateway documentation
- Deploy Integration Endpoints to Oracle Cloud Infrastructure API Gateway

About API Gateways

An API gateway is a private endpoint that routes REST API calls to a back-end resource, in this case Oracle Integration. You control which API requests can be processed by the API gateway by publishing (or deploying) specified APIs to the gateway.

> **Note:**
>
> An API gateway allows you to create nuanced rules for REST calls. However, the process can be complex, time consuming, and error prone. If you don't configure everything exactly as required, users might experience issues accessing Process Automation or Visual Builder. See Adding Request Policies and Response Policies to API Deployment Specifications.

What Kind of Traffic Is Handled by an API Gateway

REST API calls from the API gateway's virtual cloud network (VCN) to Oracle Integration are routed through the API gateway. Only those APIs you publish (or deploy) to the API gateway are passed through to Oracle Integration.

However, the API Gateway service doesn't support SaaS event-based APIs, so if you're using SaaS event-based integrations, you must use a custom endpoint instead. See Configure a Custom Endpoint for an Instance.

What Kind of Traffic Isn't Handled by an API Gateway

Non-REST API calls aren't handled by an API gateway.

The following traffic is non-REST API traffic:

- Users working in the Oracle Integration user interface (design-time), including using Process Automation and Visual Builder
- Users working in the Oracle Cloud Infrastructure Console user interface
- SOAP calls

Access for non-REST API traffic is managed with the Oracle Integration instance allowlist. See Configure an Allowlist for Your Instance.

Implement an API Gateway for Oracle Integration

To implement an API gateway for Oracle Integration, perform the following steps:

1. Configure an API gateway according to your organization's requirements. See Creating API Gateways and Resources.
2. Add your organization's VCN OCID to the Oracle Integration allowlist. This allows your VCN to bypass the API gateway. See Configure an Allowlist for Your Instance.
3. Add your API gateway's VCN to the Oracle Integration allowlist. This allows the API gateway to pass through calls from APIs deployed in the gateway's VCN to Oracle Integration.
4. Enable loopback in the Oracle Integration allowlist so that Oracle Integration can call itself. For example, enabling loopback allows Oracle Integration to call its own REST APIs.
5. Deploy APIs to your gateway. See Creating API Gateways and Resources and Deploy Integration Endpoints to Oracle Cloud Infrastructure API Gateway.

> **Note:**
>
> You must complete these steps manually and use the correct format, or users will experience access issues.

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.
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*.

Field	Description
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
- Suppression List
- Invalid Email Addresses in Distribution Lists (DL)

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*.

Invalid Email Addresses in Distribution Lists (DL)

If an email DL includes an invalid email address, *all* email addresses in the list are impacted. When a notification alert is sent, none of the recipients in the DL receive the alert.

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

Use the public logging service features 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.

Move Oracle Integration 3 Instances

There are several ways to move Oracle Integration instances.

- Move an Instance to a Different Compartment
- Move an Oracle Integration Instance to a Different Region

Move an Instance to a Different Compartment

You can move an Oracle Integration instance to a different compartment.

If you instead want to move an instance to a different *region*, see Move an Oracle Integration Instance to a Different Region.

> **Note:**
>
> Moving an instance to another compartment doesn't affect runtime or design-time access to the Oracle Integration instance. However, it can potentially change who has access to the instance in the Oracle Cloud Infrastructure Console. For example, if User A has permission to manage items only to Compartment 1, and you move the instance to Compartment 2, User A will lose access to the instance. Before moving an instance to a new compartment, make sure that all users that need access to the instance will still be able to access the instance after the move.

1. You can move an instance from the list of Oracle Integration instances or while viewing the instance's details:
   - From the list of Oracle Integration instances, to the far right of the instance you want to move, click ⋮, and choose **Move**.
   - From the instance's Details page, 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.

Move an Oracle Integration Instance to a Different Region

You can move your Oracle Integration instance to a different region.

If you instead want to move your instance to a different *compartment*, see Move an Instance to a Different Compartment.

> **Note:**
>
> You can't move an Oracle Integration instance from one *tenancy* to another, even if the tenancies are both within the same region, but you can export/import integrations across tenancies with appropriate permissions for object storage or explicit transfer of the export file.

If you are considering this type of move, here are some best practices to ensure the move is smooth.

- Use a custom endpoint for your Oracle Integration instances. See Configure a Custom Endpoint for an Instance. Ensure all clients are using the new custom endpoint.
- Export and import design-time metadata to move the existing configuration to the new instance in the new region. See Clone the Design-Time Metadata of an Entire Service Instance in *Using Integrations in Oracle Integration 3*.
- Do as much verification in the new region as possible. However, do not start polling or schedules to avoid duplicate processing.
- Configure the same custom endpoint for the new instance, but do *not* update the DNS Canonical Name (CNAME) at this time.
- When all verification in the new region is complete and all non-polling integrations are activated, switch the custom endpoint CNAME to point to the new Oracle Integration instance hostname.

- Deactivate the polling integrations and stop the schedules in the old instance.
- Activate the polling integrations and start the schedules in the new instance.
- If using File Server, a load balancer is probably required in each region and hostname. The load balancer performs port mapping because there is no guarantee that the File Server port number matches across instances. This is a great opportunity to use a standard SFTP port for external clients, along with a hostname. Once the load balancer is set up in each region and verified to be working, you can switch the hostname to the new region load balancer when you are ready to move traffic to the new File Server.
- These best practices can be used to move to a new stripe. However, both instances cannot be active at the same time and the original instance must be deleted.

Monitor Oracle Integration 3 Instances

Monitor your Oracle Integration instances and their features.

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

There are several tools available to help you monitor your instances:

- **Service instance metrics:** View message metrics for a particular Oracle Integration instance. See View Message Metrics and Billable Messages.
- **Custom metrics charts:** Create custom charts to view exactly the metrics you're interested in. See Viewing a Custom Metric Chart.
- **Service metrics:** View metrics for multiple Oracle Integration instances at the same time. See Viewing Default Metric Charts for a Metric Namespace (Multiple Resources).
- **Alarms:** Use alarms to notify you when metrics meet specified triggers. See Managing Alarms.
- **Logging Analytics dashboards:** Oracle Integration includes several preconfigured dashboards to help you monitor resources, diagnostics, and key metrics for your tenancy.
  - Oracle Integration: Health Overview—Shows an overview of monitored Oracle Integration instances, integrations, and their health based on metrics and logs.
  - Oracle Integration: Key Metrics—Shows requests, processing time, and invocation times for all integration environments in a compartment.
  - Oracle Integration: Time Taken Analysis—Shows flow execution time analysis across integration versions and drill down to Actions and Action Types level time taken for integration instances.

  See Using Dashboards.

You can also monitor integrations in the **Observability** section of Oracle Integration. See Monitor Integrations During Runtime.

Topics:

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)

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.

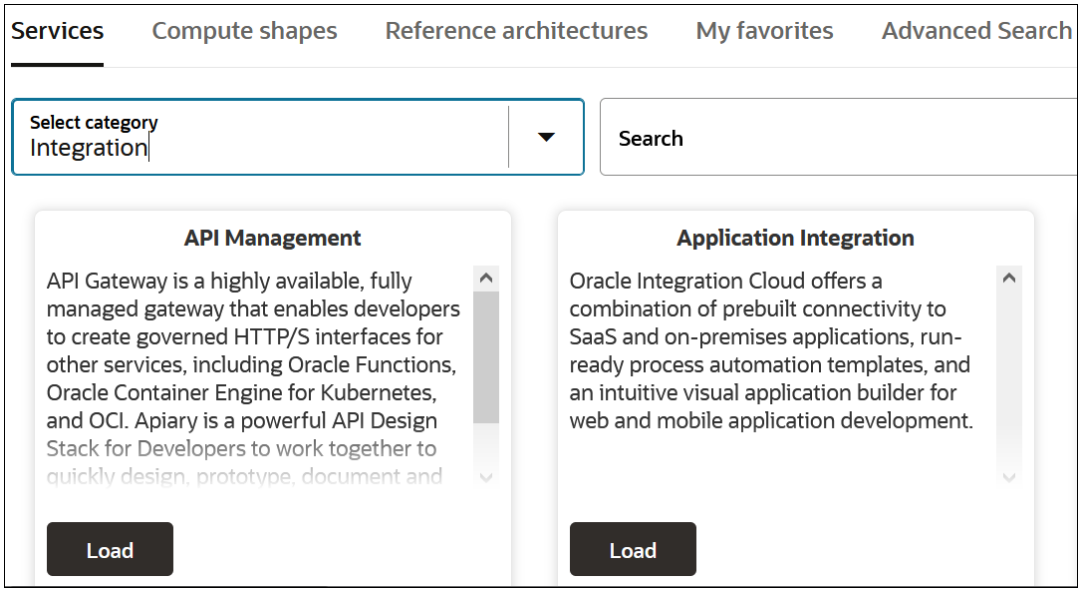
If an integration is likely to exceed the instance's maximum concurrency, the integration is probably going to experience timeouts when built as a synchronous integration. Instead, build the integration as an asynchronous integration.

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
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.

View Message Metrics and Billable Messages

View and analyze service instance metrics, including 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.

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

Access the Metrics Page for an Oracle Integration Instance

1. Sign in to the Oracle Cloud Infrastructure Console.
2. Ensure you have permission to view message metrics for the compartment.

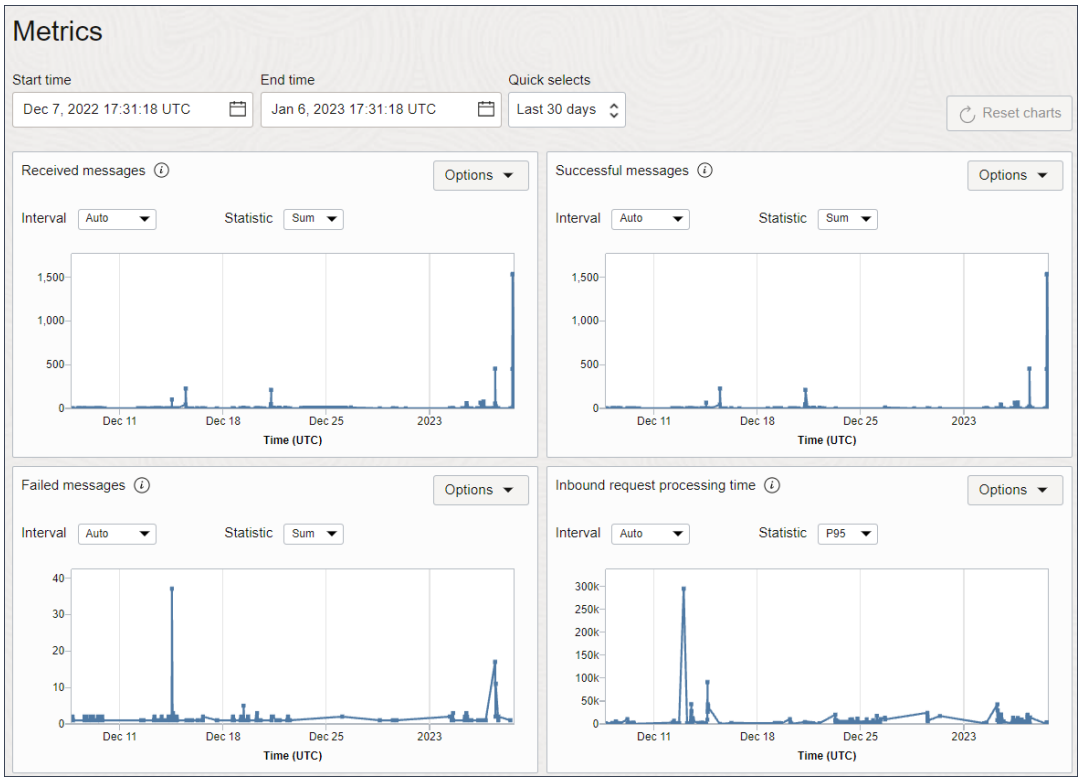
- If you are an administrator with manage access, you can automatically view message metrics for the compartment. For manage access, you must be part of an Oracle Cloud Infrastructure group assigned a `manage` policy.
- If you are an administrator with read only access, you must be part of an Oracle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

3. Open the navigation menu and click **Developer Services**. Under **Application Integration**, click **Integration**.
4. Click an Oracle Integration instance to view it.
A **Metrics** section shows graphs with default values.



Available Metrics 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.

Chart	Description
Inbound request processing time	Shows adapter inbound processing times for the instance.
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 and Configured messages	These two charts show the following information: • Consumed messages: Shows the number of messages that the instance used for incoming and outgoing messages for trigger and invoke requests. • Configured messages: Shows the number of messages that you purchased. This number is calculated by multiplying the number of message packs you purchased by the number of messages in each pack. Use this data to make informed decisions about the number of message packs to purchase for the instance. See Choose a Message Pack Number. For details on how message usage is calculated, see About Integrations Usage.
Consumed messages from data retention	Shows the number of messages used for extended data retention. If you have an Enterprise edition instance and you choose to retain data longer than the default 32 days, an extra percentage will be added to your message consumption: • 93 days (3 months) increases your message consumption by 10%. • 184 days (6 months) increases your message consumption by 20% For details on how to manage your data retention period, see Edit the Data Retention Period for an Instance.
Configured messages for Visual Builder	Shows the number of messages that Visual Builder used. • 3,500 messages for the first OCPU • 4,500 messages for each additional OCPU
Consumed messages for process automation	Shows the number of process messages that Process Automation used. • +1 message per process invocation A process invoking another process doesn't incur this charge • +1 message per hour of process duration after the first hour
Consumed messages for decisions	Shows the number of messages that decisions used. • +1 message per decision invocation
Consumed messages for robotic process automation	Shows the number of messages that Robotic Process Automation used. • +1 message per robot invocation • +1 message per 5 minutes of robot duration after the first 5 minutes
Total consumed messages	Shows the total number of messages used by all components and extended data retention.
Consumed message packs from overage	Shows the number of message packs used to cover any message usage overage.
Consumed message packs from breakglass	Shows the number of message packs that the instance used for breakglass.
Total consumed message packs	Shows the grand total of message packs used by your instance.

Using the Metrics Charts

You can change the metrics that appear in each chart. Additionally, you can create custom charts to further analyze your data. For example, imagine you created two compartments for

your organization, one for your engineering team and another for your finance team. Using custom charts, you could measure the resources that each compartment 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.

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
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

Metric Name in Metrics Explorer	Unit	Description	Dimension Name in Metrics Explorer	Commonly Used Statistics in Metrics Explorer
MessagesReceivedCount	count	Number of messages that were received. This count doesn't indicate whether the messages processed successfully.	• flowCode • flowVersion • resourceId	Min Max
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

Metric Name in Metrics Explorer	Unit	Description	Dimension Name in Metrics Explorer	Commonly Used Statistics in Metrics Explorer
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

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
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)
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

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
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
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

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
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
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

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
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
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

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
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
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

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
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
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 >

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
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_oraclecommerceclo ud	Oracle Commerce Cloud Adapter	N/A	N/A
responsys	Oracle Responsys Adapter	N/A	N/A
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

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
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
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

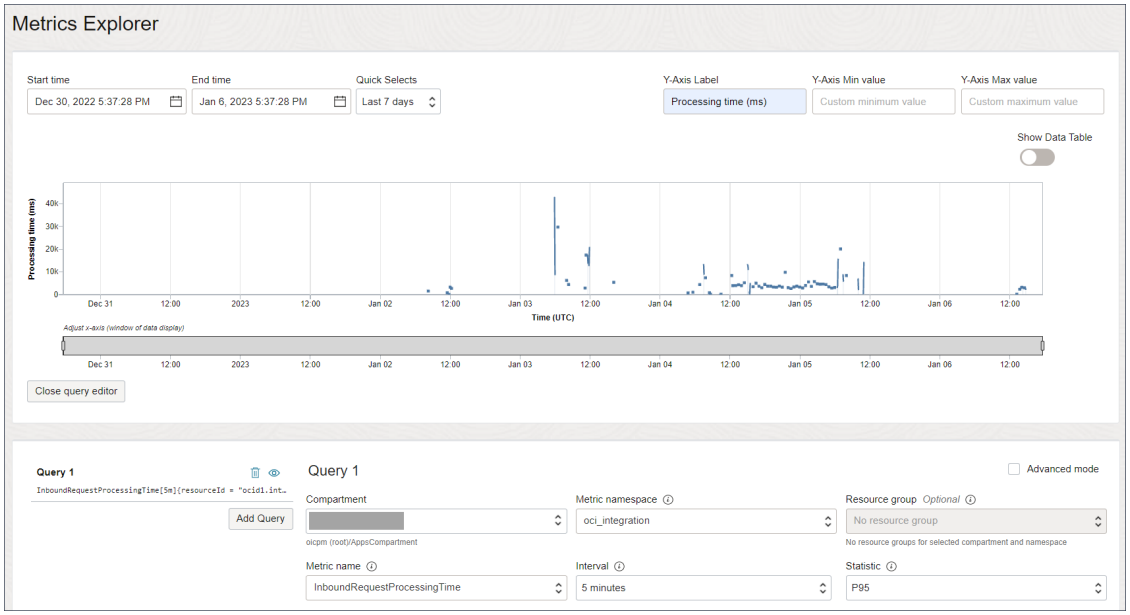
Dimension Value in Metrics Explorer	Adapter Display Name	Inbound Processing Event Information Naming Conventions in Dimension Value Field	Outbound Invocation Endpoint Information Naming Conventions in Dimension Value Field
servicenow	ServiceNow Adapter	• Receive <business object> notifications from ServiceNow	• 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
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

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
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
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

Rename a Tenancy

You can rename the tenancy that includes your service instance. The name change does *not* impact the following:

- Your service instance.
- Other Oracle Integration resources.

For example, if the tenancy name in your URL was `global-chips` prior to tenancy renaming, the original name continues to be used unchanged:

```
https://myoic-global-chips-px.integration.ocp.oraclecloud.com/ic/home
```

See Renaming a Tenancy and Cloud Account.

If your service instance needs to use the new tenancy name, you must perform the following steps:

1. Provision a new service instance in the renamed tenancy.
2. Clone (create) and export archives of the integration design-time metadata from the original service instance.
3. Import the archives into the new service instance.

   See Clone the Design-Time Metadata of an Entire Service Instance in *Using Integrations in Oracle Integration 3*.

6

Upgrade from Oracle Integration Generation 2 to Oracle Integration 3

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

Topics:

Watch a high-level overview of what to expect and what you need to do when upgrading from Oracle Integration Generation 2 to Oracle Integration 3.

Video

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:

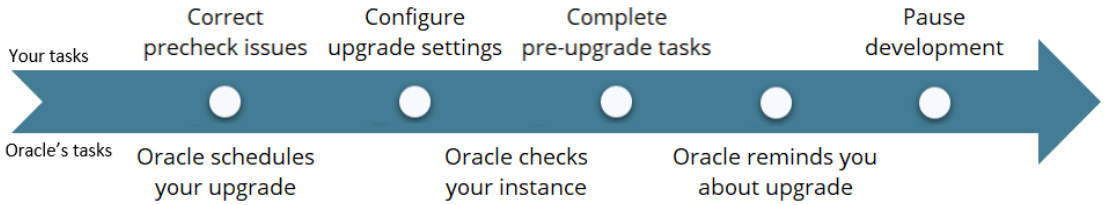
Upgrade Workflow Quick Reference

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

Read the FAQs

Read through the Upgrade FAQs to know what to expect from upgrade and to plan any tasks you need to complete.

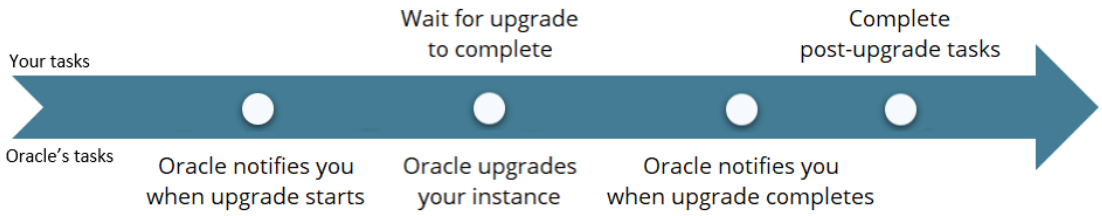
Before the Upgrade



Timing	Oracle	You	Task	Details
Any time before upgrade		**You**	Correct precheck issues	**Time to complete:** Varies To ensure that your instance is upgraded successfully, check your upgrade readiness and correct any precheck issues. You'll perform additional pre-upgrade tasks as your upgrade date approaches.
Ongoing basis	Oracle		Checks your instance	Oracle periodically checks whether your instance is ready for upgrade. **Note:** Oracle will continue these periodic checks even after your instance has been scheduled for upgrade to make sure that it's still ready. If Oracle finds any issues, we will email you so that you can address them. See Correct an Instance with Failed Readiness Checks.
At least one month before upgrade	Oracle		Schedules your upgrade	Oracle sends you an email with your upgrade date. You can also see this on the **Upgrade** page and in a message in the banner. Continue working in Oracle Integration Generation 2 until upgrade.
After receiving upgrade email		**You**	Configure upgrade settings	**Time to complete:** 10 minutes After you receive the upgrade email, configure your upgrade settings.
Up to one week before upgrade		**You**	Reschedule upgrade if needed	**Time to complete:** 5 minutes If you need to change your upgrade window, you can reschedule it if your upgrade date is three or more business days away. Oracle sends an email confirmation after you reschedule.

Timing	Oracle	You	Task	Details
Two weeks before upgrade		**You**	Complete pre-upgrade tasks and familiarize yourself with Oracle Integration 3	**Time to complete:** Varies As your upgrade date approaches, about two weeks before upgrade: • Complete pre-upgrade tasks. • Update your allowlists. • Inform users and stakeholders about upgrade. • **IMPORTANT:** Read through the Upgrade FAQs to understand how Oracle Integration 3 differs from prior versions, how upgrade affects your components of your instance, and known issues in Oracle Integration 3.
Two days before upgrade	Oracle		Reminds you about the upgrade	Several days before upgrade, Oracle sends an email reminding you about the upgrade.
Two days before upgrade		**You**	Pause development	**Time to complete:** Not applicable Pause or limit your development work to help ensure a successful 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	Oracle upgrades your instance.
Day of the upgrade		**You**	Wait for the upgrade to complete	**Time to complete:** Not applicable. The upgrade generally takes less than ten minutes. Your Oracle Integration Generation 2 instance is unavailable during the downtime. See What to Do During Upgrade.
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. Complete post-upgrade tasks. 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.

Upgrade Notifications

By default, upgrade notifications are automatically sent to the specified administrator email. Oracle recommends you have notifications sent to a distribution list or group email so that you don't miss important emails if someone leaves the company.

You set who receives notifications on the **Upgrade** page. See "Upgrade Notifications" in Configure Your Upgrade Settings.

Notification Subject	Description
Upgrade OIC Gen 2 instances to OIC 3	Oracle sent out an email notifying anyone who has or had a Oracle Integration Generation 2 instance that Generation 2 is being retired, as a reminder that, if you haven't already, you should upgrade all your instances to Oracle Integration 3.
Upgrade to Oracle Integration 3	Oracle sends you an email indicating that your upgrade has been scheduled. You can also see this on the **Upgrade** page and in a message in the banner.
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.
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. 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. 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.

General Upgrade FAQs

1. **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
   - *What's New for Oracle Integration 3*

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

Some previous features may have been permanently removed, replaced, enhanced, or not currently supported in Oracle Integration 3. Many of those changes are mentioned in these FAQs. You might also want to look through the following documentation:

- Differences from Prior Versions of Oracle Integration
- *Known Issues for Oracle Integration 3*
- Troubleshoot Upgrade Issues

3. **Am I required to upgrade my instances to Oracle Integration 3?**

   Yes, but only after all the features that you use, other than those that have been deprecated, are available for upgrade in Oracle Integration 3.

   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. Contact your account representative or customer success manager.

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. **What happens during upgrade?**

   See What to Do During Upgrade.

7. **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 you were using before the upgrade.

   In such situations, Oracle informs you by 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.

   You'll also see an **Upgrade Summary** on the Upgrade page, which will include when the upgrade was attempted and why it didn't complete.

   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 Configure Upgrade Settings or Reschedule Upgrade.

Upgrade Timing and Scheduling FAQs

1. **When will my instance be upgraded?**

   All instances have been scheduled for upgrade. Oracle sent you an email with your upgrade date. You can also see this on the **Upgrade** page and in a message in the banner.

2. **Can I choose or reschedule my upgrade date?**

   Yes. Oracle selects an upgrade window for you, but you can change your upgrade window if it's three 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. Contact your account representative or customer success manager.

3. **Will there be downtime?**

   Yes. Upgrades generally take less than ten minutes, but may take longer if you have a lot of files or a complex setup. 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.

4. **My upgrade was scheduled. What if I don't confirm the date or specify upgrade details?**

   Your upgrade will proceed as scheduled even if you don't confirm your date.

5. **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. See Correct an Instance with Failed Readiness Checks.

   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.

Pre-Upgrade FAQs

1. **What do I have to do before the upgrade?**

   - Check upgrade readiness and correct precheck issues.
   - Configure your upgrade settings.
   - As your upgrade date approaches, perform some pre-upgrade tasks, including updating your allowlists.

2. **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.

3. **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.

Post-Upgrade FAQs

1. **How do I know when the upgrade is finished?**

   Upgrades generally take less than ten minutes, but may take longer if you have a lot of files or a complex setup. 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.

2. **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.

3. **What do I have to do after the upgrade?**

   See Complete Post-Upgrade Tasks.

4. **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.

5. **What if issues occur after the upgrade?**

   After the upgrade completes, sign in and perform your typical verification tasks, and 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.

   > **Important:**
   >
   > If you determine that you need to roll back your instance, your instance will be rolled back to Oracle Integration Generation 2 in the same state it was when upgrade was performed. Any changes you made in the upgraded environment won't be reflected in the Oracle Integration Generation 2 environment if you roll back.

Service Instance FAQs

1. **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 Update Allowlists.

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

Note that the incoming IP addresses for development and production instances are different, even within the same region. However, the outgoing IP address is the same for all shapes (development or production) in a single region.

2. **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 in the following format.
     `https://design.integration.region.ocp.oraclecloud.com/?integrationInstance=query_parameter_repersenting_instance`

     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.
   - The Process URL will change.

3. **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. However, be aware that, as of October 2024, Oracle Integration Generation 2 and Oracle Integration 3 are different enough that work done in Oracle Integration Generation 2 isn't compatible with Oracle Integration 3 and vice versa. See the new features and differences from prior versions in *What's New for Oracle Integration 3*.

   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.

4. **Can I switch to a different region or compartment during upgrade?**

   No. Moving regions and compartments is not part of the upgrade process.

5. **Is basic authentication still supported?**
   See When is Basic Authentication Supported in Oracle Integration 3?.

6. **How else might upgrade affect my service instance?**

   - **Custom endpoint:** If you use a custom endpoints, be aware of the following changes:
     - If you're using Visual Builder, your custom endpoint and any alternate custom endpoints will be configured on Visual Builder during the upgrade process. After upgrade, your Visual Builder apps must invoke Oracle Integration using the original Oracle Integration 3 URL rather than the custom endpoint.
     - Visual Builder supports alternate custom endpoints, but Oracle Integration 3 currently doesn't.
     - If you're not using Visual Builder and your custom endpoint uses SSL, you'll need to set up a load balancer as a front end for your Oracle Integration Generation 2 instance, and remove the SSL certificate.
     - If you're not using Visual Builder, after upgrade, *runtime access to your integrations* will continue to work as it did for Oracle Integration Generation 2. For all other access points—such as design-time and Process Automation—you still access the custom endpoint, but the custom endpoint then redirects to the appropriate URL

     See Custom Endpoint URL precheck.
   - **Instance ID value:** The system-generated instance ID that is displayed on the Instances page and in the activity stream for an integration instance has changed from

a numeric value to an alphanumeric value in Oracle Integration 3. You can choose to keep the instance ID as numeric when configuring your upgrade settings. See FlowId Conversion Support and Instance ID Action precheck.

- **Daily email limit:** Oracle Integration 3 can send a limit of 10,000 emails in a rolling 24-hour window. See Daily Email Limit precheck.
- **Custom scopes in IDCS:** Oracle Integration 3 adds a default scope to Oracle Identity Cloud Service (IDCS) when the instance is created; no other custom scopes are supported in IDCS. See Custom scopes in IDCS precheck.
- **Activity stream data:** The activity stream isn't migrated, but you can capture this data in the Oracle Cloud Infrastructure Console. See Instance Pre-Upgrade Tasks.
- **Network rules configuration:** If you've enabled network rules in any Oracle Cloud Infrastructure services, you might need to configure them to include Oracle Integration. See Instance Pre-Upgrade Tasks.
- **Update window:** The update window is now determined by the shape of your instance, rather than tags as it was in Oracle Integration Generation 2. Production instances are updated two weeks after Development instances. Depending on when you upgrade during the release cycle, there can be a version mismatch between your Development instances and Production instances. See Patching Updates to Your Oracle Integration 3 Instance.
- You might also want to look through the following documentation:
  - Benefits of Upgrading
  - *What's New for Oracle Integration 3*
  - Common Issues in *Known Issues for Oracle Integration 3*
  - Troubleshoot Upgrade Issues

7. **Will I need to perform any post-upgrade tasks for my service instance?**
   - Make sure you have access to the Oracle Integration 3 instance, which might include updating an IAM policy with the new OCID. See Ensure Access to the Instance.
   - Complete your organization's post-upgrade verification tasks. See Follow Your Organization's Verification Procedures.

Connectivity FAQs

1. **If I use the connectivity agent, do I need to recreate any connections?**

   No. However, you should be aware of several points:

   - **Agent Java version and KeyStore:** For Oracle Integration 3, your connectivity agents must use JDK 17 and PKCS 12 KeyStore. See Agent Java Version precehck.
   - **Allowlists:** *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 IP addresses. See Update Allowlists.
   - **Agent group identifiers:** Oracle Integration 3 doesn't support spaces in agent group identifiers, they won't be migrated to Oracle Integration 3. See Unsupported AgentGroup Identifier precheck.
   - **Conversion to OAuth 2.0:** During the upgrade, your connectivity agents are automatically converted from using basic authentication to using OAuth 2.0 token-based authentication to communicate with Oracle Integration. As long as your agents are running when upgrade begins, all agents are automatically upgraded to OAuth 2.0,

so you don't need to manually recreate any agents yourself. See Connectivity Agent Pre-Upgrade Tasks.

- **Proxy server caching:** Set your proxy server's Cache property for the Oracle Integration URLs to refresh as frequently as possible. See Set the proxy server's Cache property.
- **Additional firewall traffic after upgrade:** 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.

2. **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).

3. **How else might upgrade affect my connectivity?**

   You might also want to look through the following documentation:

   - Benefits of Upgrading
   - *What's New for Oracle Integration 3*
   - *Known Issues for Oracle Integration 3*
   - Troubleshoot Upgrade Issues

4. **Will I need to perform any post-upgrade tasks for connectivity?**

   - 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.
   - Make sure your connectivity agents were upgraded and connections are working properly. See Ensure Connectivity.

Integrations FAQs

1. **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.

2. **Are Oracle Integration Generation 2 and Oracle Integration 3 integrations forward and backward compatible?**

   No. As of October 2024, Oracle Integration Generation 2 and Oracle Integration 3 are different enough that integrations aren't forward or backward compatible. See the new features and differences from prior versions in *What's New for Oracle Integration 3*.

3. **How does upgrade affect my activity stream and actively running integrations?**

   - **Data retention:** Oracle Integration 3 Standard and Enterprise editions support 32 days of data retention by default. During upgrade only the most recent 32 days of retained data will be migrated.
   - **Activity stream data:** The activity stream isn't migrated, but you can capture this data in the Oracle Cloud Infrastructure Console. The activity stream has been greatly enhanced and can be viewed and downloaded from the Instances page, Instance Details page, and Errors page.
   - **Runtime activities are paused during upgrade downtime:** Oracle Integration stops accepting incoming integration requests during the brief downtime during upgrade.

See How Upgrade Affects Runtime Data.

4. **How else might upgrade affect my integrations?**
   - **Delayed (asynchronous) response:** The delayed (asynchronous) response pattern was previously supported in the some adapters. See Delayed (Asynchronous) Response precheck.
   - **Identity certificates:** If you have identity certificates, you'll need to upload new identity certificates after upgrade. See Ensure Connectivity.
   - **Basic routing duplicate app name:** In Oracle Integration 3, you can't have multiple basic routing integrations that have the same source and target endpoint names. See Basic Routing Duplicate App Name precheck.
   - **Number of active integrations:** An instance can have a maximum of 800 active integrations, as specified in the Service Limits.
   - **Multiple read file:** The Read Multiple File operation was deprecated in Oracle Integration Generation 2. See Multiple Read File precheck.
   - **Publish/subscribe integrations:** Publish/subscribe (or pub/sub) integrations have been replaced by event-driven orchestrations in Oracle Integration 3. See Publish/Subscribe Integrations precheck.
   - **API calls must use OAuth:** Design-time (DT) built-in API calls using a REST connection must use OAuth. See DT API Basic Auth to OAuth action precheck.
   - You might also want to look through the following documentation:
     - Benefits of Upgrading
     - *What's New for Oracle Integration 3*
     - Integration Issues in *Known Issues for Oracle Integration 3*
     - Troubleshoot Upgrade Issues
5. **Will I need to perform any post-upgrade tasks for integrations?**
   - Check your integrations for any failed activations or schedules that failed to start.
   - If needed, take action on requests that any clients sent to Oracle Integration during the downtime.
   - If you selected to ignore precheck failures, you might need to perform additional post-upgrade tasks. See Complete Post-Upgrade Tasks for Ignored Precheck Failures.

   See Ensure Integrations Work.

Adapters FAQs

1. **How might upgrade affect my adapters?**
   - **Custom adapters:** Custom adapters aren't supported by Oracle Integration 3 yet. See Custom Adapters precheck.
   - **Oracle utilities adapter:** Swagger 2.0 is no longer supported in the Oracle Utilities Adapter. See Oracle Utilities Adapter precheck.
   - **Unsupported adapters:** Some adapters are no longer supported in Oracle Integration 3. See Unsupported Adapters precheck.
   - **Unsupported REST types:** Some connection types are deprecated and not supported in a REST Adapter connection. See Unsupported REST Types precheck.

- **Decommissioned 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. See Adapters Pre-Upgrade Tasks.
- You might also want to look through the following documentation:
  - Benefits of Upgrading
  - *What's New for Oracle Integration 3*
  - Integration Issues in *Known Issues for Oracle Integration 3*
  - Troubleshoot Upgrade Issues

2. **Will I need to perform any post-upgrade tasks for adapters?**

   If you selected to ignore precheck failures, you might need to perform post-upgrade tasks. See Complete Post-Upgrade Tasks for Ignored Precheck Failures.

B2B FAQs

1. **How might upgrade affect my B2B features?**
   - **Data retention:** Oracle Integration 3 Standard and Enterprise editions support only 32 days of data retention. During upgrade only the most recent 32 days of retained data will be migrated.
   - **B2B passwords:** Your identity certificate file (JKS) requires two sets of passwords: Key Passwords and Keystore Password. All the passwords must be identical. See B2B for Oracle Integration Pre-Upgrade Tasks.
   - You might also want to look through the following documentation:
     - Benefits of Upgrading
     - *What's New for Oracle Integration 3*
     - Common Issues in *Known Issues for Oracle Integration 3*
     - Troubleshoot Upgrade Issues
2. **Will I need to perform any post-upgrade tasks for B2B?**

   No.

File Server FAQs

1. **How does upgrade affect File Server?**

   A lot will stay the same after upgrade. During the upgrade, Oracle migrates your File Server files, folder structure, and allowlists (permissions) from Oracle Integration Generation 2 to Oracle Integration 3. After the upgrade, access the File Server REST APIs the same way you did in Oracle Integration Generation 2.

   However, there are some changes you should be aware of:

   - **IP and port values:** During upgrade, Oracle assigns new IP and port values for the File Server SFTP server. See How Upgrade Affects File Server. After upgrade, you'll need to complete some post-upgrade tasks described below.
   - **Access to File Server:** In Oracle Integration 3, you can access File Server using the File Server URL and credentials.
   - **Allowlists:** In Oracle Integration Generation 2 you had to submit a service request (SR) to request changes to your File Server allowlists. In Oracle Integration 3, you can update the allowlist yourself. For information on managing your allowlists for File

Server after migration, see Restrict Access to an Instance Using the Self-Service Allowlist.

- **Legacy algorithms:** There are several legacy exchange algorithms that FTP no longer supports. During upgrade, FTP connections will be updated with the current algorithms. See How Upgrade Affects File Server.
- **API calls must use OAuth:** If you use File Server REST API calls, they must use OAuth. See Integrations Pre-Upgrade Tasks.
- You might also want to look through the following documentation:
  - Benefits of Upgrading
  - *What's New for Oracle Integration 3*
  - File Server Issues in *Known Issues for Oracle Integration 3*
  - Troubleshoot Upgrade Issues

2. **Will I need to perform any post-upgrade tasks for File Server?**
   - Update your integrations and SFTP clients to use the new IP and port values.
   - Add the new IP address to your internal firewall allowlist.

   See Ensure Connectivity

Process FAQs

1. **What are the benefits of upgrading Process?**

   See:

   - Benefits of Upgrading Process
   - *What's New for Oracle Cloud Infrastructure Process Automation*

2. **How does upgrade affect Process features?**
   - Process functionality has undergone some important changes that you should be aware of. See How Upgrade Affects Process Features.
   - After the upgrade, Process will be accessible via a new URL. See Complete Post-Upgrade Tasks for Process Automation.
   - The upgrade affects any clients calling Process via a REST API (for example, integrations or Visual Builder apps). See Complete Post-Upgrade Tasks for Process Automation.
   - Process instance data is not migrated to Oracle Integration 3. This means you won't see historical transactions created or completed in Oracle Integration Generation 2 after upgrade.
   - You might also want to look through Process Automation Issues in *Known Issues for Oracle Integration 3*.

3. **What upgrade paths are available for me if I use process?**

   Depending on how you're using Process in Oracle Integration Generation 2, you'll use a different option to upgrade or migrate. See Process Upgrade Options.

   Here's a brief description of the options:

   - If you don't have active process instances or you can complete all process instances before upgrade, you use the automated in-place upgrade performed by Oracle.

- If you have active process instances in production and need to continue to serve requests without disruption, you migrate your process applications to a new OCI Process Automation instance. That OCI Process Automation instance serves new process requests, while your Oracle Integration Generation 2 instance continues to serve existing requests until those transactions complete. Then, you upgrade your Oracle Integration Generation 2 instance to Oracle Integration 3 and attach the OCI Process Automation instance to Oracle Integration 3.

4. **Will I need to perform any post-upgrade tasks for Process?**

   Your post-upgrade steps are dependent on which upgrade option applies to your implementation. See Process Upgrade Options.

5. **Why does the manual migration process recommend that the OCI Process Automation instance I create should be a standalone instance?**

   A standalone OCI Process Automation instance is recommended because:

   - It ensures that there's no impact to existing process integrations or Visual Builder applications.
     If you instead provisioned a new Oracle Integration 3 instance, you would also need to migrate your existing process integrations and Visual Builder applications to the new environment and update your clients to the new Oracle Integration 3 URL. Additionally, you wouldn't be able to take advantage of the Oracle Integration 3 upgrade to automatically upgrade the rest of your environment.
   - It limits costs during migration.
     OCI Process Automation standalone can leverage the Oracle Cloud Free Tier pricing model. See Process Automation Pricing.

6. **I'm following the manual migration process and need help. Who can I turn to?**

   You can contact your Oracle Account Representative and discuss available options if you need guidance throughout the migration process. If you've encountered a specific error or issue, create a service request (SR) on My Oracle Support.

7. **Will Oracle Integration Generation 2 process data be retained as part of the upgrade or migration process?**

   No. To save or export this data prior to upgrade, complete the steps outlined in Archiving and Purging Process Automation Data in Oracle Integration.

8. **If I wait, will there eventually be an automatic upgrade for instances with actively used process applications?**

   No. You should perform the manual migration to Oracle Integration 3.

Visual Builder FAQs

1. **How does upgrade affect Visual Builder?**

   See the following sections:

   - Visual Builder Prechecks
   - Visual Builder Pre-Upgrade Tasks
   - Complete Post-Upgrade Tasks for Visual Builder

2. **Will I need to perform any post-upgrade tasks for Visual Builder?**

   See Tasks to Complete After the Upgrade in *Administering Oracle Visual Builder in Oracle Integration 3*.

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
Integrate business and health data	Use the Healthcare edition to modernize applications, business processes, APIs, and data using industry standards such as HL7 and the latest advances in healthcare interoperability, such as Fast Healthcare Interoperability Resources (FHIR). See Introduction to Oracle Integration for Healthcare in *Using Oracle Integration for Healthcare in Oracle Integration 3*.
Create UI-based automation	Complement your integrations, which provide API-based automation, with robots, with provide UI-based automation. This robotic process automation (RPA) technology is available directly within Oracle Integration. See Learn About Robots and Build a Robot in *Using Robots in Oracle Integration 3*.
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.
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.

Feature	Description
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
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 feature 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.

Feature	Description
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.

Benefits of Upgrading Process

Feature	Description
Intelligent Document Processing	OCI Process Automation offers Intelligent Document Processing (IDP) capabilities via a new Document Understanding control that can be found in OCI Process Automation forms. This control exposes pretrained Key-Value extraction models provided by OCI Document Understanding (ODU) to perform text extraction on documents such as passports, driver's licenses, receipts, and invoices. By leveraging these pretrained models, you can instantly use document extraction capabilities without needing prior knowledge of Oracle's AI service or training your own custom models. See Implement Intelligent Document Processing in Forms in *Using Oracle Cloud Infrastructure Process Automation*.
Process Analytics	OCI Process Automation introduces analytical capabilities for process owners. Process Analytics brings rich visualizations that enables you to easily monitor, understand, and optimize a particular process by allowing you to: • Monitor the current state of process executions. • Understand the flow or paths that process instances take. • Understand the average time taken for activities to complete. • Understand where errors occur and why. The insight gathered from the above data can be used to optimize your processes by removing bottlenecks or implementing modeling changes that drive efficiencies. See View Analytics for ActivitiesView Analytics for Activities in *Using Oracle Cloud Infrastructure Process Automation*.
Business search	OCI Process Automation introduces a new search experience that enables you to search and find transactions based on business data using queries that are meaningful to you—the business user. For example, you can now search for records by a supplier, find patients by name or Medicare ID, locate requisitions where the amount was greater than a certain value, or even find a car part using its manufacturer. See the following topics in *Using Oracle Cloud Infrastructure Process Automation*: • Search for a Task • Configure Searchable Fields Based on Business Data • Apply Advanced Search Filters
Native support for Oracle Integration 3 integrations	Process designers can natively discover and use integrations from Oracle Integration 3. This capability supports standalone integrations as well as those that reside within a project. Using the capability, developers can easily find and invoke integrations without the need for configuring specific endpoints or specifying authentication settings. See OIC Project Integrations in *Using Oracle Cloud Infrastructure Process Automation*.

Feature	Description
Ad-hoc tasks	You can now create and assign human tasks to users on-the-fly (programatically). Oracle has taken our rich human task capabilities and exposed them via an easy to consume RESTful API that can be called outside the constructs of a process flow. This means you can now bring task management capabilities to integrations and front-end applications with ease. This feature allows you to introduce Human-in-the-Loop processing whenever intervention is needed to manage exceptions or serve approval needs. See REST API endpoints for Adhoc Tasks in *REST API for Oracle Cloud Infrastructure Process Automation*.
Out-of-office for administrators	The out-of-office feature now lets you define periods of leave during which any tasks assigned to you are automatically reassigned to another user or role. In addition to this previously available functionality, OCI Process Automation allows administrators to set out-of-office periods on behalf of others. This is important because administrators can prevent lengthy delays caused by users forgetting to set out-of-office rules before going on leave. See Manage Out of Office Records in *Using Oracle Cloud Infrastructure Process Automation*.
Editable CSS	External stylesheets enable you to customize the appearance of your process forms. OCI Process Automation enables you to make changes to the CSS file directly in OCI Process Automation until you get it just right. This editable CSS feature is important because you can remain within OCI Process Automation as you follow the iterative process of making your forms look great. See Work with CSS in *Using Oracle Cloud Infrastructure Process Automation*.
Availability of OpenAPIs	OCI Process Automation makes an OpenAPI Specification (OAS 3.0) available upon activation of processes applications or decision services. These specifications significantly reduce the effort required to understand the endpoint, payload structure, and authentication required to call an OCI Process Automation service. The specifications can be used to test processes or decisions via REST clients or to integrate them with other tools.
Schedule processes	You can now start processes with a timer based start. Scheduling of repetitive process flows enables you to handle use cases that need repetitive execution. You can use this functionality to send email reminders, assign reoccurring tasks to users, or send weekly reports to management. See Start Timer in *Using Oracle Cloud Infrastructure Process Automation*.
OAuth 2.0 Client Credential support	OCI Process Automation supports bearer tokens generated via the OAuth Client Credential flow. This flow is best suited for Machine-to-Machine (M2M) flows where you need to authenticate and authorize an application instead of a user. In practical terms, this means that you now have a dedicated method for handling requests from applications that don't usually carry user context (for example, Oracle Integration). See Users, Groups and Permissions in *Using Oracle Cloud Infrastructure Process Automation*.
File Manager control in forms	OCI Process Automation has introduced a new control in forms which enables you to upload files to an external document store as well as list, delete, and download previously uploaded files. This control provides a powerful way to manage documents from a process form. See Configure File Manager Controls in *Using Oracle Cloud Infrastructure Process Automation*.

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 Standard and Enterprise editions support 32 days of data retention by default. During upgrade only the most recent 32 days of retained data will be migrated. You can increase the data retention period for Standard and Enterprise editions if you want (may incur extra cost). See Edit the Data Retention Period for an Instance.

Oracle Integration 3 is also available in a Healthcare edition, which supports 184 days of data retention.

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.

Before upgrade, you must decide what to do with asynchronous messages from the client side for the duration of the downtime. See Decide what to do with asynchronous messages.

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 Determine what to do with failed instances.

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

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.

Although your integrations and SFTP clients can continue accessing File Server using the Oracle Integration Generation 2 IP and port values for the four-month window, Oracle recommends that you update IP and port value references within one week after upgrade. Otherwise you risk forgetting to update the values and then experiencing issues when Oracle retires the IP and port values.

You'll need to make the following updates as described in Complete Post-Upgrade Tasks.

- Update your integrations and SFTP clients to use the new IP and port values.
- Add the new IP address to your internal firewall 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.

> **Note:**
>
> In Oracle Integration Generation 2 you had to submit a service request (SR) to request changes to your File Server allowlists. In Oracle Integration 3, you can update the allowlist yourself. For information on managing your allowlists for File Server after migration, see Restrict Access to an Instance Using the Self-Service Allowlist.

Legacy FTP Exchange Algorithms Updated During Upgrade

There are several legacy exchange algorithms that FTP no longer supports. During upgrade, FTP connections will be updated with the current algorithms. For example:

- `diffie-hellman-group1-sha1` will be replaced with `diffie-hellman-group14-sha1`
- `diffie-hellman-group-exchange-sha1` will be replaced with `diffie-hellman-group-exchange-sha256"`

How Upgrade Affects Process Features

The following Oracle Integration Generation 2 Process features aren't supported in Process Automation in Oracle Integration 3. This topic describes possible workarounds and alternate solutions.

The following table lists Oracle Integration Generation 2 features that are affected by the upgrade, including any workaround or alternate solutions and the remark you see in the migration report that you get after upgrade.

Functional area	Oracle Integration Generation 2 feature	Description	Workaround or alternate solution	Remark in migration report	Deprecation status
Analytics	Business indicators	Capture and display business metrics specific to your process	Leverage reporting or visualization tools such as Oracle Analytics or Visual Builder. Process Automation processes can push data to these systems via REST or Oracle Integration connectors.		
Analytics	Dashboards	Dashboards are used to monitor the overall state of your processes and view specific process metrics	Leverage Oracle Integration 3's full-fledged Process Analytics, which provides similar reporting and process monitoring functionality.		Deprecated
Composer	Composer testing framework	Test process via composer	Test processes in a development/test environment after deployment.		Deprecated
Permissions (for applications in Composer)	Spaces	Control access to applications via spaces, which allow certain users to access to a subset of applications	Use Oracle Integration projects in Oracle Integration Generation 2 to enforce access control rules.		Deprecated
Mobile app	Mobile app	Oracle Process Mobile Application	Use your browser to interact with Process Automation via your mobile device or build a progressive web application for mobile devices with Visual Builder. A depreciation notice was published in *What's New for Oracle Integration 2*.		Deprecated
Workspace	Oracle Content Management (OCM) integration: OCM instance setup configuration	Test and persist OCM connection configuration	Evaluate whether process-based attachments will serve your needs. If you need a content management solution, evaluate the ability to integrate it via Oracle Integration. A depreciation notice was published in *What's New for Oracle Integration 2*.		Deprecated
Workspace	Task views	Create views and grant them to other users			Deprecated

Functional area	Oracle Integration Generation 2 feature	Description	Workaround or alternate solution	Remark in migration report	Deprecation status
Structured processes	Bot activity	Call an RPA integration created using one of the available RPA adapters in Oracle Integration	During upgrade, bot activities will be replaced with abstract activities. Re-establish connectivity to RPA bots as needed with REST or Oracle Integration connectors. A depreciation notice was published in *What's New for Oracle Integration 2*.	Couldn't migrate Activity Bot activity : Type Bot isn't supported. Replaced with an abstract activity.	Deprecated
Structured processes	OCM integration: document start event	Trigger a process instance when document details are received	During upgrade, document start events will be replaced with message start events. Evaluate whether process-based attachments will serve your needs. If you need a content management solution, evaluate the ability to integrate it via Oracle Integration. A depreciation notice was published in *What's New for Oracle Integration 2*.		Deprecated
Structured processes	OCM integration: folder start event	Trigger a process instance when folder details are received	During upgrade, folder start events will be replaced with start message events. Evaluate whether process-based attachments will serve your needs. If you need a content management solution, evaluate the ability to integrate it via Oracle Integration. A depreciation notice was published in *What's New for Oracle Integration 2*.		Deprecated

Functional area	Oracle Integration Generation 2 feature	Description	Workaround or alternate solution	Remark in migration report	Deprecation status
Structured processes	Dynamic process (DP) call activity	Incorporate a dynamic process within your structured process by using a Dynamic Process element	During upgrade, dynamic process activities will be replaced with abstract activities. If you need to call a dynamic process from a structured process you can use a REST connector that points to an instances REST endpoint.	Couldn't migrate Activity Calling DP : Type Dynamic Process isn't supported. Replaced with an abstract activity.	Deprecated
Structured processes	Multiple start events	Multiple starts support for structured process	Trigger a form start event via the instances REST endpoint, providing flexibility in starting a process from a form or via an API.		
Structured processes	Insight activity	Browse Insight models and send data to them	During upgrade, Insight activities will be replaced with abstract activities. Leverage reporting or visualization tools such as Oracle Analytics or Visual Builder. Process Automation processes can push data to these systems via REST or Oracle Integration connectors.	Couldn't migrate Activity Insight : Type Insight isn't supported. Replaced with an abstract activity.	Deprecated

Functional area	Oracle Integration Generation 2 feature	Description	Workaround or alternate solution	Remark in migration report	Deprecation status
Structured processes	Micro processes	Divide a large, complex business process into multiple reusable blocks called micro processes, created within separate applications; use an activity to link your micro process in structured processes	During upgrade, micro processes will be replaced with abstract activities. Replace the abstract activities with a REST connector to call a Process with certain limitations (for example, no auto-update of any changes in definition and message end).	Couldn't migrate Activity Micro process : Type Micro Process isn't supported. Replaced with an abstract activity.	Deprecated
Structured processes	Business parameters	Cross-process variables (only for structured processes) with values that can be modified without redeploying the application	You can replace business parameters with data objects, but the data objects will behave like regular variables without any way to update values after activation. Alternatively, you can implement a Decision or an Integration serving business parameter values that can be shared across process applications and updated independently.		Deprecated
Structured processes	Save process start form data	Save the entered data in start form	If you need to persist data prior to initiating a process, use Visual Builder-based forms.		Deprecated

Functional area	Oracle Integration Generation 2 feature	Description	Workaround or alternate solution	Remark in migration report	Deprecation status
Structured processes	Message end event	Message end events are used to send messages when the process reaches an end event.	During upgrade, message end events will be replaced with none end events. If you weren't using the message emitted by the error end event, you don't need to do anything; the replacement during upgrade will suit your purpose. If you need to notify another process or an external service, use a send task or a service task right before the end event.	Couldn't migrate End Event XXXXX: Type message isn't supported. Replaced with end none event.	Deprecated
Structured processes	Message throw	A message throw event is used to send data to another process or an external service.	Use the Send activity instead to initiate another process asynchronously. Use the Integration or Service Activity to communicate with an external service.	Throw event XXX converted to a send task. Implementation is not supported and is now empty (if the original implementation wasn't a Process call)	Deprecated

Functional area	Oracle Integration Generation 2 feature	Description	Workaround or alternate solution	Remark in migration report	Deprecation status
Structured processes	Message catch	A message catch event is used to receive data from another process or external service.	Use the Receive activity instead to receive data from another process or external service.	Catch event XXX converted to a receive task. Implementation is not supported and is now empty (if the original implementation wasn't a Define Interface call)	Deprecated

Functional area	Oracle Integration Generation 2 feature	Description	Workaround or alternate solution	Remark in migration report	Deprecation status
Structured processes	Event-based gateway	Event gateways allow you to make a decision based on events. The process will wait at the gateway until one event is triggered.	During upgrade, an event-based gateway will be replaced with an exclusive gateway. Use a timer boundary over a Receive activity to simulate situations where you need to wait for a message to arrive or a timer to expire. If the message is not received within a certain amount of time the timer boundary will fire.	Couldn't migrate Gateway Event based gateway : Type Event based gateway isn't supported. Replaced with an exclusive gateway.	Deprecated
Structured processes	Process-level variables	Predefined variables exposed by Process but not already supported, such as `componentName`, `dueDate`, `reviewer`	Remove references to invalid process variables. Some information may be available from our APIs. You could call the APIs from within the process using a connector in a service task to retrieve the values and assign them to process data objects.		
Structured processes	Error event sub-process error codes	Default errors produced by runtime that can be selectable as errors in a standard error catch	Errors won't be mapped/migrated during upgrade; they'll be left blank. You'll need to choose new errors. Oracle Integration 3 includes a new subset of exceptions provided by runtime.		
Dynamic processes	Dynamic process roles scoped to various resources within DP	Specific roles to stages, activities in DP	After upgrade, users won't have permissions for those dynamic process roles. Use a combination of global roles and task assignment rules to achieve a similar outcome.	Migrated as global roles	Deprecated

Functional area	Oracle Integration Generation 2 feature	Description	Workaround or alternate solution	Remark in migration report	Deprecation status
Dynamic processes	REST sentries	Drive conditional triggers with REST calls	Use a combination of data sentries, event sentries, and REST calls to achieve a similar outcome.	Couldn't migrate Data condition in Stage Global isn't supported	Deprecated
Dynamic processes	DMN sentries	Drive conditional triggers with DMN calls	Use a combination of data sentries, event sentries, and DMN calls to achieve a similar outcome.	Couldn't migrate Data condition in Stage Global isn't supported	Deprecated
APIs	SOAP/WSDL interface for Process	SOAP and WSDL APIs exposed by Processes	Update your clients to invoke Process via REST APIs.		Deprecated
APIs	Basic authentication	Provide a username and password when making a request to an API endpoint	Process Automation APIs are protected with OAuth token-based authentication. See Security, Authentication and Authorization in *REST API for Oracle Cloud Infrastructure Process Automation*.		Deprecated
APIs	REST endpoints	Perform a large number of operations such as creating new process instances, tasks fetching transaction information, or managing your user preferences	Equivalent APIs are available in Process Automation. Update your clients to reference the updated API endpoints and payload definitions. See *REST API for Oracle Cloud Infrastructure Process Automation*.		

Functional area	Oracle Integration Generation 2 feature	Description	Workaround or alternate solution	Remark in migration report	Deprecation status
Vacation rules	Delegation: delegation action in vacation rules	Automatically delegate tasks while the given user is on vacation	Configure out of office actions using re-assignment mechanics.	Note: the equivalent functionality in OPA is call Out-Of-Office(OOO).	
Human tasks	Escalation policy: escalation to manager	Escalate task to assignee's manager or role's escalation path			
Human tasks	Customize human task screen	Hide attachments/ comments			
Human tasks	Notifications: form as PDF/Image/ Inline	Configure human task notifications to contain the form as a PDF document, image, inline	Use notifications without attachments. Provide as much information as available and needed in the notification text.		Deprecated
Human tasks	Renew	When an expiration on a task is set, the renewal policy allows the expiration date to be extended until it reaches the specified amount of renewals allowed.	Consider setting up a timer boundary on the human task that will recreate a new task for the assignee once expiry is reached.	Couldn't migrate "Expiration type in activity XXX: Renew type isn't supported."	Deprecated

Functional area	Oracle Integration Generation 2 feature	Description	Workaround or alternate solution	Remark in migration report	Deprecation status
Human tasks	Assignment to groups	Assign user tasks to a specific group	During upgrade, groups are removed from the assignee list. Change group assignments to a role, and link the IDCS group to the newly created role.	Not supported "Group assignee for activity XXX"	

Human tasks	execData mappings	`execData.title`
		`execData.shortSummary`
		`execData.priority`
			You can't map these attributes as input data associations in Process Automation. Instead, define these attributes in the Human Task properties.		

Human tasks	execData mappings	`execData` Object containing all the task attributes	You can't map the entire `execData` object in an output data association. Instead, map the individual attributes under this object.		
Human tasks	execData mappings	`execData.systemAttributes.taskNumber` Object used to store a numeric identifier for a task	Use `taskId` instead. This is an alphanumeric identifier for a task. Note that this data type change may have downstream impact if persisted or referenced in external systems.		

Human tasks	execData mappings	`execData.customAttributes`
		`execData.systemMessageAttributes`
		Custom attributes used to pass data to the task; this data is not part of the form data attributes
			Use form data attributes instead. Add these attributes to your form and choose whether you want to display them. Remap custom attributes to the new form-level attributes.		

Human tasks	execData mappings	`execData.ownerUser`
		`execData.ownerGroup`
		`execData.ownerRole`
		Attributes used to store the owner of the task
			Create a role in your application with `Manage` permission. Assign users or groups to this role as needed. Remove any existing input mappings to these attributes.		

Functional area	Oracle Integration Generation 2 feature	Description	Workaround or alternate solution	Remark in migration report	Deprecation status
Human tasks	execData mappings	`execData.identificationKey` Key used to store a user-specified value that can later be used to identify and find the task	Add the custom identifier to the title of the task. This allows you to search for your task based on this value from the workspace or via the API using keyword search. Alternatively, add a form field to store this value, and use business search to locate data based on the field value via the workspace.		
Human tasks	Handlebars as the notification template	Define the notification template using Handlebars.	Use Mustache Template.		

Functional area	Oracle Integration Generation 2 feature	Description	Workaround or alternate solution	Remark in migration report	Deprecation status
Human tasks	Email template variables	The following email template variables are no longer supported: • acquiredBy • acquiredById • assignedDate • creatorId • endDate • fromUser • fromUserId • longSummary • outcome • ownerGroup • ownerRole • ownerUser • ownerGroupId • ownerRoleId • ownerUserId • priorityNum • startDate • state • taskNumber • taskDefinitionId • updatedBy • updatedById • updatedDate • externalUIURL • instanceId • processId • processName • processVersion • currentYear • comments • commentStr	Many of these variables (processID, commnets, outcome, updatedBy, and such) can be referenced via process-level data objects. This means that you need to assign these variables to a custom process-level Data Object first, and then reference them in your email template. For more information, see Configure Email Templates. Other variables such as OwnerGroup/ Role/User, taskNumber, taskDefinitionID are no longer available and can't be used in email templates.		

Functional area	Oracle Integration Generation 2 feature	Description	Workaround or alternate solution	Remark in migration report	Deprecation status

Human tasks	Email template variables	Action variables in email templates	Email templates that used action variables to display a list of options a user can take, such as Approve/Reject, need to be modified from the following format:
			
			`{{#actions}}`
			`  Actions: {{{actions}}}`
			`{{/actions}}`
			
			To the following format:
			
			`{{# hasActions }}`
			`  <div class="button-container">`
			`  <div class="label">Actions</div>`
			`  <div class="buttons">`
			`  {{# actions }}`
			`  <a class="action-button" href="{{workspaceURL}}">`
			`  <span title="{{actionDisplayName}}">{{actionDisplayName}}</span>`
			`  </a>`
			`  {{/ actions }}`
			`  </div>`
			`  </div>`
			`{{/ hasActions }}`		

SOAP connector	SOAP connector	Make a SOAP call from Process	During upgrade, SOAP connectors won't be imported. After upgrade, service tasks won't include an assigned connector, and data associations will be invalid. Temporarily mark the service tasks as a draft. Reimplement the connectors using REST, or use an integration to perform SOAP to REST conversion. A depreciation notice was published in *What's New for Oracle Integration 2*.	Couldn't migrate SOAP connector XXXX	Deprecated
Business objects	Module/namespace	Sort types into modules/ namespaces	During upgrade, business objects are migrated at the root level. After upgrade, you can select and use types as usual but they are all listed at the same level instead of grouped by modules/ namespaces.		Deprecated

Functional area	Oracle Integration Generation 2 feature	Description	Workaround or alternate solution	Remark in migration report	Deprecation status
Business objects	Default value for business object	Set a default value for a business object field so there's no need to map data unless needed for that specific instance (business object will contain default value otherwise)	During upgrade, default values for business objects won't be migrated. Map the default value of the business object field on each instance where its referenced. We recommend including a data association activity at the beginning of the process to centrally initialize any required attribute.		
Business objects	Business objects XSDs	Upload XSDs to the application so you can refer to them later for BO creation	During upgrade, business objects based on XSDs are migrated, but you won't be able to upload new XSDs. For any new definitions you need, create your business objects manually, or, for a connector, provide a JSON payload.		Deprecated
Forms	Connector in form preview	Test connector calls from form preview	After upgrade, connectors aren't executed when running the form in preview mode. Activate the application on your development instance and test using Workspace.		
Application life-cycle	Retire an application (and then activate it later)	Retire an active/ deployed Process application			

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

Prepare for the Upgrade to Oracle Integration 3

To ensure that your instance is upgraded successfully you must check your instance's upgrade readiness and correct any precheck issues prior to your upgrade date. Oracle runs periodic checks on your instance to make sure there are no precheck issues. If the precheck finds any issues, you'll be notified by email that you must address the issues before upgrade.

> **NOT_SUPPORTED:**
>
> On the Upgrade page, you can specify that you want to ignore precheck failures and proceed with upgrade. If you select this option, you must complete post-upgrade tasks for any precheck failures that were ignored. See Complete Post-Upgrade Tasks for Ignored Precheck Failures.

- Recommendations for Upgrading Multiple Instances
- Upgrade in an Oracle Cloud Infrastructure US Government Cloud Region
- Check Upgrade Readiness and Correct Precheck Issues
- Configure Upgrade Settings or Reschedule Upgrade
- Complete Pre-Upgrade Tasks
- Update Allowlists
- Inform Users and Stakeholders About Upgrade
- Limit Development Work Before the Upgrade

Recommendations for Upgrading 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.

Upgrade in an Oracle Cloud Infrastructure US Government Cloud Region

This topic describes how to upgrade Oracle Integration Generation 2 to Oracle Integration 3 in an Oracle Cloud Infrastructure US Government Cloud region.

The process to upgrade in an Oracle Cloud Infrastructure US Government Cloud region is similar to upgrading in other regions. However, you must complete some additional pre-upgrade steps:

1. Grant Oracle Integration access to your tenancy. Add the following policy statements to your tenancy:

```
allow service integration to read users in tenancy
allow service integration to read groups in tenancy
allow service integration to read group-memberships in tenancy
allow service integration to manage credentials in tenancy
allow service integration to read policies in tenancy
allow service integration to read compartments in tenancy
allow service integration to manage domains in tenancy
allow service integration to manage integration-instances in tenancy
```

2. On the **Upgrade** page of your Oracle Integration Generation 2 instance, in the **Policy OCIDs of Service Role** box, enter the OCIDs for the policies you created to grant access to your service role groups. See Assign Policies to Service Role Groups That Grant

Access and Permissions. These service role group mappings will be migrated to the Oracle Integration 3 instance during upgrade.

Continue with the remaining upgrade process, starting with Check Upgrade Readiness and Correct Precheck Issues.

Check Upgrade Readiness and Correct Precheck Issues

Oracle periodically performs some prechecks to determine your upgrade readiness so that your upgrade runs smoothly. If the prechecks don't pass, you may need to perform tasks to correct the issues.

After you correct any precheck issues, configure your upgrade settings.

View Your Precheck Status

To see your precheck status or to run the check again, perform the following steps:

1. In the navigation pane, click **Settings**, then **Upgrade**.
   You can see when the last precheck completed above the readiness check table.

   The readiness check table shows the following information about the status of the precheck items.

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 **More details...** to see additional information about the condition failure. To copy the details to the clipboard, click  .

2. If there are prechecks that didn't pass, perform the associated tasks to correct the issues.
3. To rerun the precheck, click **Check again**.
   It takes about an hour for the precheck to complete.

> **Note:**
>
> If Oracle attempted to upgrade your instance, you see the details of that attempt in the **Upgrade Summary** directly below the readiness check table.

Summary of Prechecks

This table summarizes the prechecks and associated tasks for each area. The details for each task are linked in the table and shown in the next section.

Area	Tasks
Connectivity Agent	• Agent Java Version • Agent Connectivity for Oracle Integration 3 - Connectivity agent must be running • Agent Connectivity for Oracle Integration 3 - Update your allowlist settings • Unsupported AgentGroup Identifier
Instances	• Custom Endpoint URL • Instance ID Action • Daily Email Limit • Custom scopes in IDCS • Other Failures
B2B for Oracle Integration	• B2B Retention Period
Integrations	• Delayed (Asynchronous) Response • Identity Certificates • Basic Routing Duplicate App Name • Multiple Read File • Publish/Subscribe Integrations • DT API Basic Auth to OAuth action
Adapters	• Custom Adapters • Oracle Utilities Adapter • Unsupported Adapters • Unsupported REST Types
Visual Builder	• Custom Endpoint URL • VBCS
Process Automation	• Process Automation • Process Automation Prechecks

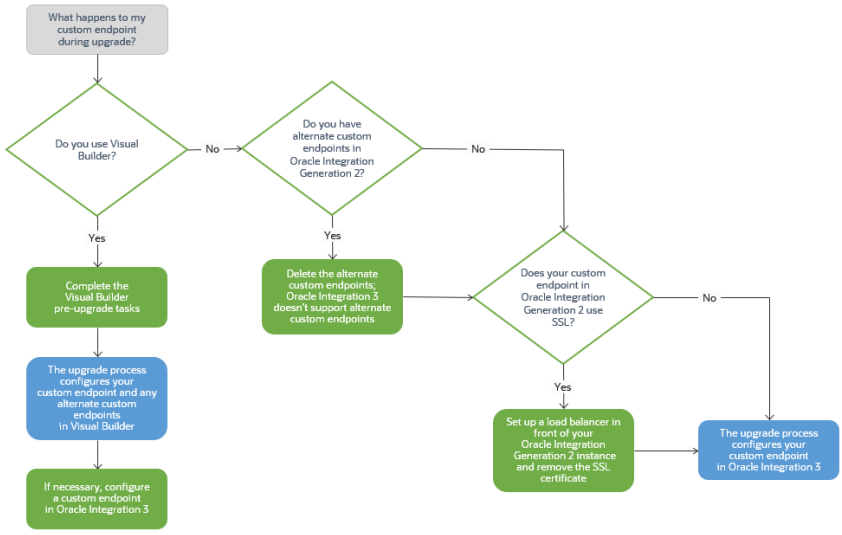
Connectivity Agent Prechecks

Eligibility condition	Typical owner	Blocks upgrade	Tasks to Complete
Agent Java Version	Development Operations team	No	Make sure that your connectivity agents use JDK 17 and PKCS12 KeyStore. Expand **More details** to see the connectivity agents that need review. To copy the details to the clipboard, click  . You can also view the **Connectivity Agent Status** section to see the status of all the connectivity agents in your instance. 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: 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. If you want to manually convert your JKS KeyStore to the PKCS12 KeyStore, complete the following steps before upgrade. 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.

Eligibility condition	Typical owner	Blocks upgrade	Tasks to Complete
Agent Connectivity for Oracle Integration 3 - Connectivity agent must be running	Development Operations team	No	Your connectivity agent should be up and running before the upgrade begins. Expand **More details** to see the connectivity agents that need review. To copy the details to the clipboard, click  . You can also view the **Agent Status** column in the **Connectivity Agent Status** section to see the status of all the connectivity agents in your instance, indicating whether each agent is offline (unavailable). Agents that aren't reachable during upgrade or don't meet upgrade requirements won't be upgraded, in which case you'll need to perform post-upgrade steps to regain connectivity.
Agent Connectivity for Oracle Integration 3 - Update your allowlist settings	Development Operations team	No	You should update your allowlist settings for your connectivity agents before upgrade. Expand **More details** to see the connectivity agents that need review. To copy the details to the clipboard, click  . You can also view the **Allowlist status** column in the **Connectivity Agent Status** section to see the status of all the connectivity agents in your instance, indicating whether the allowlist has been updated appropriately. As your upgrade window approaches, perform the following pre-upgrade tasks: • Add the IP address for Oracle Identity Cloud Service (IDCS) to the allowlist. • Add the design-time and runtime 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. Agents that aren't reachable during upgrade or don't meet upgrade requirements won't be upgraded, in which case you'll need to perform post-upgrade steps to regain connectivity.
Unsupported AgentGroup Identifier	Development Operations team	No	If any of your agent groups have a space in their identifiers, they won't be migrated to Oracle Integration 3. If you still need the agent groups, you'll need to recreate them after upgrade.

Instance Prechecks

Eligibility condition	Typical owner	Blocks upgrade	Tasks to Complete
Custom Endpoint URL	Administrator	Yes	Depending on how your custom endpoint is configured pre-migration you'll perform different steps and the upgrade process will handle the custom endpoint differently. Expand **More details** to determine how to proceed with upgrade.



- If you're using Visual Builder:
  1. To proceed with upgrade, complete the Visual Builder Pre-Upgrade Tasks.
  2. During upgrade, the upgrade process configures your custom endpoint and any alternate custom endpoints in Visual Builder.
- If you're *not* using Visual Builder and you have alternate custom endpoints, delete them from your Oracle Integration Generation 2 instance. Oracle Integration 3 currently doesn't support alternate custom endpoints.
- If you're *not* using Visual Builder and your custom endpoint uses SSL:
  1. To proceed with upgrade, set up a load balancer in front of your Oracle Integration Generation 2 instance and remove the SSL certificate.
  2. During upgrade, the upgrade process configures your custom endpoint in Oracle Integration 3.
  3. After upgrade, *runtime access to your integrations* will continue to work as it did for Oracle Integration Generation 2. For all other access points—such as design-time and Process Automation—you still access the custom endpoint, but the custom endpoint then redirects to the appropriate URL.
- If none of these situations apply and this precheck passed, the upgrade process configures your custom endpoint in Oracle Integration 3, and the custom endpoint will work as described in the previous bullet for the SSL scenario.

Eligibility condition	Typical owner	Blocks upgrade	Tasks to Complete
Instance ID Action	Administrator	No	The system-generated instance ID that is displayed on the Instances page and in the activity stream for an integration instance has changed from a numeric value to an alphanumeric value in Oracle Integration 3. The value's *data type* is unchanged; it remains a string data type. The change to an alphanumeric value may affect any systems that you use that rely on the instance ID being a numeric value. For example, if you parse the instance ID from a REST API and store the instance ID in a database as a number field, you'll need to update the database field. You can choose to keep the instance ID as numeric when configuring your upgrade settings. See FlowId Conversion Support. If you have integrations that use instance IDs, the precheck shows a warning. Expand **More details** to see the integrations that need review. To copy the details to the clipboard, click  . Update your systems and processes as required. See Adapting to Instance ID Change when upgrading to Oracle Integration 3. **Note:** This precheck just checks for the existence of integrations that use instance IDs, not the accuracy of the instance IDs. The warning will remain after you update your integrations, but doesn't impact your upgrade.
Daily Email Limit	Administrator	No	Oracle Integration 3 can send a limit of 10,000 emails in a rolling 24-hour window, as described in Service Limits. If your deployment needs to send more than that, you can instead use your customer tenancy. See Configure Notification Emails.
Custom scopes in IDCS	Administrator	Yes	Oracle Integration 3 adds a default scope (`/ic/api/` , `urn:opc:resource:consumer::all`) to Oracle Identity Cloud Service (IDCS) when the instance is created. It doesn't support any other custom scopes added to IDCS. If you have created custom scopes in IDCS, you must remove them.
Other Failures	Varies	Yes	If there are any other issues that will block upgrade that don't have specific prechecks, they'll be included under other failures. Expand **More details** to see the issues that need action. To copy the details to the clipboard, click  .

B2B for Oracle Integration Prechecks

Eligibility condition	Typical owner	Blocks upgrade	Tasks to Complete
B2B Retention Period	Administrator	No	Although you don't need to do anything to correct this precheck status, be aware that Oracle Integration 3 Standard and Enterprise editions support 32 days of data retention by default. During upgrade only the most recent 32 days of retained data will be migrated. Expand **More details** to see how many days of retained data you currently have. To copy the details to the clipboard, click  . After upgrade to Oracle Integration 3, you'll have the ability to increase the data retention period if you want (may incur extra cost); or upgrade to the Healthcare edition, which supports 184 days of data retention.

Integrations Prechecks

Eligibility condition	Typical owner	Blocks upgrade	Tasks to Complete
Delayed (Asynchronous) Response	Development team	Yes	The delayed (asynchronous) response pattern was previously supported in the following adapters: • Oracle CX Sales and B2B Service Adapter • Oracle ERP Cloud Adapter • Oracle HCM Cloud Adapter • Oracle Field Service Cloud Adapter • Salesforce Adapter • ServiceNow Adapter If you have integrations using delayed (asynchronous) response with one of these adapters, rework them by creating two invoke connections to achieve similar functionality: 1. Create a simple invoke for success callbacks. 2. Create an additional invoke for failure callbacks under the fault handler to catch the correct fault. Expand **More details** to see which integrations need review. To copy the details to the clipboard, click  .
Identity Certificates	Development team	No	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. Expand **More details** to see the names of the identity certificates and the connections that use them. To copy the details to the clipboard, click  . If you have identity certificates, after the upgrade, you'll need to upload new identity certificates as described in Ensure Connectivity:
Basic Routing Duplicate App Name	Development team	Yes	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, deleting the target endpoint, and adding it again with a different name. 2. Save your integration. Expand **More details** to see the integrations that need review. To copy the details to the clipboard, click  .
Multiple Read File	Development team	Yes	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. Expand **More details** to see the integrations that need review. To copy the details to the clipboard, click  .

Eligibility condition	Typical owner	Blocks upgrade	Tasks to Complete
Publish/ Subscribe Integrations	Development team	Yes	If your instance includes integrations that publish messages or subscribe to messages from Oracle Integration, be aware that publish/subscribe (or pub/sub) integrations need to be converted to event-driven orchestrations. The integrations will be handled differently depending on their configuration: • Pub/sub integrations that use attachments can't be automatically converted at this time. If you want to proceed with upgrade, you can either remove these integrations or ignore precheck failures. After upgrade, you can recreate them, pushing the attachment into the FTP server or Object Storage in your tenancy and passing the reference to the subscriber flow. See Define Header-Based Subscription Filtering in *Using Integrations in Oracle Integration 3*. • All other active pub/sub integrations are automatically converted during upgrade. Pub/sub integrations in a draft state can't be migrated, and will be blank post-upgrade. • If you've mapped data in the subscriber flow, the mappings are converted as accurately as possible. However, after upgrade, you should review the mappings and correct them if necessary. • If you see the error **Only Subscribers are present, no Publishers**, you have orphan subscribers that must be deleted before upgrade. Expand **More details** to see the integrations that *can't be* automatically converted. To copy the details to the clipboard, click  . **Note:** You might want to take this opportunity to delete any draft Publish flows.
DT API Basic Auth to OAuth action	Development team	No	If your instance includes integrations that access DT (design-time) built-in APIs using a REST connection with basic authentication, you must change them to use OAuth. In Oracle Integration Generation 2, you could use Basic Authentication to use the Oracle Integration REST API and File Server REST API. In Oracle Integration 3, you must use OAuth. You 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 details on using OAuth with the Oracle Integration REST API, see Security, Authentication, and Authorization, or with the File Server REST API, see Security, Authentication, and Authorization.

Adapters Prechecks

Eligibility condition	Typical owner	Blocks upgrade	Tasks to Complete
Custom Adapters	Development team	Yes	If your instance includes integrations that use a custom adapter, the instance can't be upgraded yet. Wait until Oracle starts upgrades for this feature. Expand **More details** to see the custom adapters you're using. To copy the details to the clipboard, click  .

Eligibility condition	Typical owner	Blocks upgrade	Tasks to Complete
Oracle Utilities Adapter	Development team	No	Swagger 2.0 is no longer supported in the Oracle Utilities Adapter. If there is any existing integration using the Swagger 2.0 REST catalog, runtime won't be impacted. However, if you try to edit the design-time connection, retest the connection, refresh the metadata, refresh the artifacts, or reactivate, the integration fails. You must update the catalog to use the OpenAPI 3.x definition. Expand **More details** to see the integrations that need review. To copy the details to the clipboard, click  . See Using Swagger 2.0 REST catalog with Oracle Utilities Adapter version 24.04.0 or higher.
Unsupported Adapters	Development team	Yes	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 **Note:** Robotic process automation (RPA) capabilities are available in Oracle Integration 3. See Learn About Robots and Build a Robot in *Using Robots in Oracle Integration 3*. Expand **More details** to see which unsupported adapters you're using. To copy the details to the clipboard, click  .
Unsupported REST Types	Development team	Yes	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 Expand **More details** to see which unsupported REST types you're using. To copy the details to the clipboard, click  . 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.

Visual Builder Prechecks

Eligibility condition	Typical owner	Blocks upgrade	Tasks to Complete
Custom Endpoint URL	Administrator	Yes	This was also covered in the Instance Prechecks, but is repeated here since it applies to Visual Builder. If you have a custom endpoint and you're using Visual Builder: 1. To proceed with upgrade, complete the Visual Builder Pre-Upgrade Tasks. 2. During upgrade, the upgrade process configures your custom endpoint and any alternate custom endpoints in Visual Builder.
VBCS	Administrator	Yes	If you use Visual Builder with your own Oracle database instance (BYODB), Autonomous Transaction Processing (ATP) must be up and running during upgrade. Make sure to complete the additional tasks described in Prepare Visual Builder for the Upgrade in *Administering Oracle Visual Builder in Oracle Integration 3*.

Process Automation Prechecks

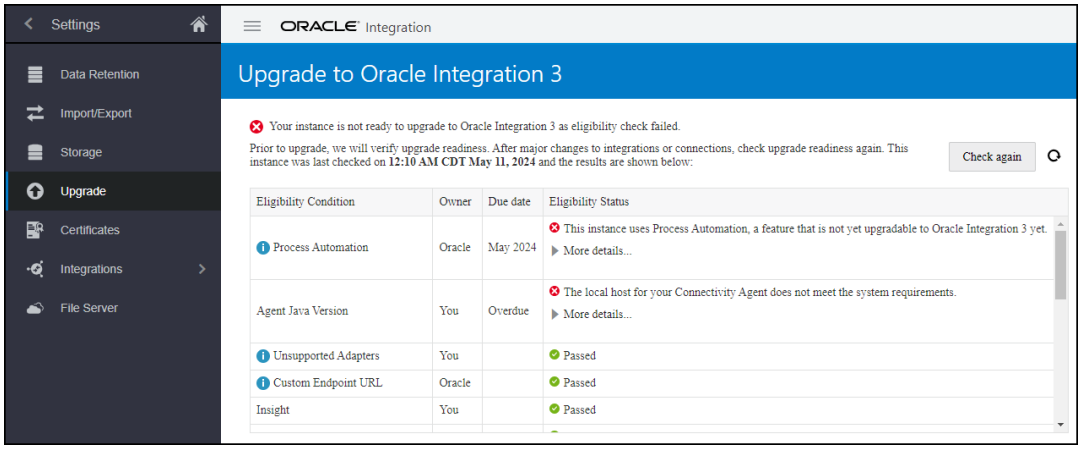
Eligibility condition	Typical owner	Blocks upgrade	Tasks to Complete
Process Automation	Administrator	Yes	There are several differences between Process in Oracle Integration Generation 2 and Process Automation in Oracle Integration 3. See Process FAQs. Depending on how you're using Process in Oracle Integration Generation 2, you'll use a different option to upgrade or migrate. See Process Upgrade Options.
Process Action	Administrator	Yes	If you're using the Process action in any integrations, you'll need to replace or remove the Process action prior to upgrade. Use the method described in the Process upgrade option that applies to your situation.

Correct an Instance with Failed Readiness Checks

If your upgrade was scheduled and your instance is no longer ready for upgrade, address the findings so that your upgrade completes successfully.

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 conditions that didn't pass, and take the appropriate action. See Check Upgrade Readiness and Correct Precheck Issues for steps to take.
3. After addressing all issues, check the instance again.
   a. Click **Check again**.

      It takes about an hour for the check to complete. You can see when the last check completed above the readiness check table.

   b. Continue making corrections until the check passes.

      If you aren't sure how to correct an issue, enter a service request (SR) on My Oracle Support.

Configure Upgrade Settings or Reschedule Upgrade

You should have received notification of your scheduled upgrade window, checked your upgrade readiness, and corrected any precheck issues. Before your upgrade, configure the upgrade settings. If you need to reschedule your upgrade, you can do so if the upgrade is more than three business days away.

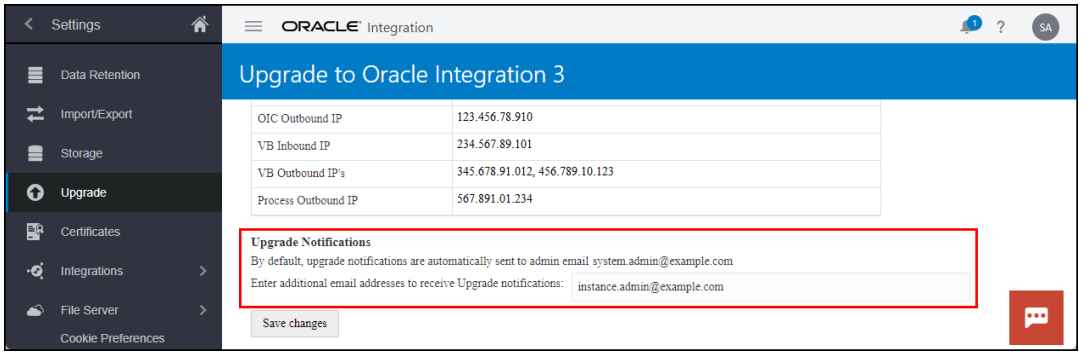
Prerequisites:

- If any upgrade readiness checks fail, address the issues that apply to your instance. For instructions on how to fix failed upgrade checks, see Check Upgrade Readiness and Correct Precheck Issues.
- 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.

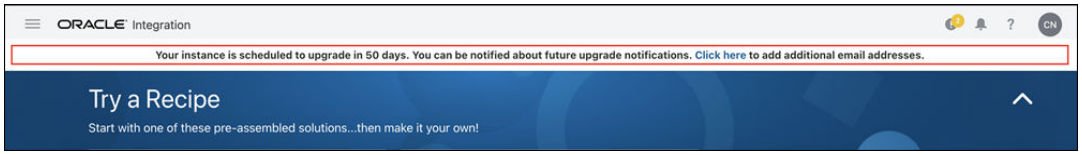
View Your Upgrade Window

You can see your scheduled upgrade window in the following places:

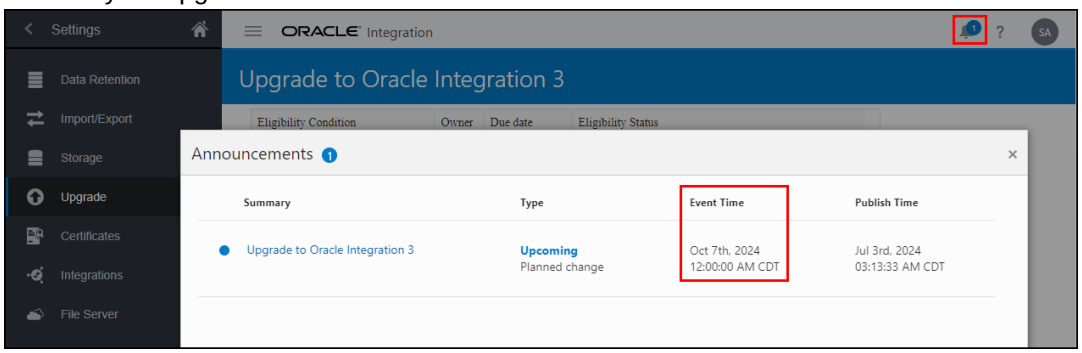
- Oracle sends an email, informing you of your upgrade window.
  By default, upgrade notifications are automatically sent to the listed administrator email. Oracle recommends you have notifications sent to a distribution list or group email so that you don't miss important emails if someone leaves the company Add the distribution list, group email, or any other stakeholders who should receive upgrade notifications, by entering their email addresses, separated with commas (,) in the box **Upgrade Notifications**. Oracle will include these email addresses in all future upgrade notifications.



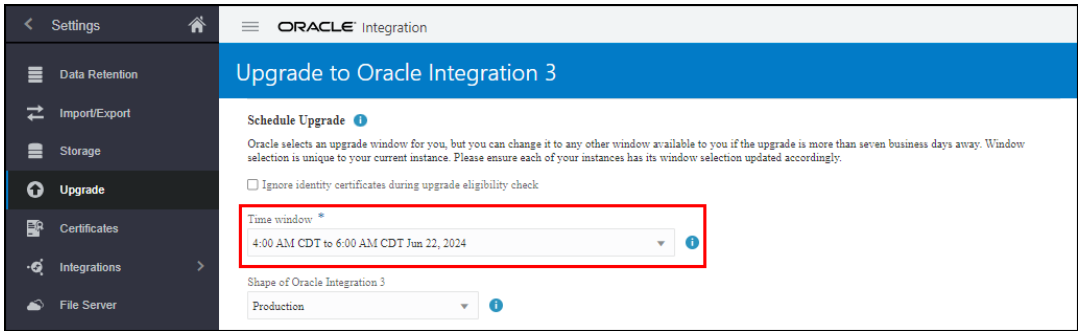
- An announcement appears in the user interface. You can see the announcement if you're part of an administrator group.



- Click **Announcements**  . Next to the upgrade announcement, under **Event Time**, you'll see the start time of your upgrade window. Click the notification to view the start and end times of your upgrade window.



- Click **Settings**, then click **Upgrade** to see your upgrade window.



Reschedule Your Upgrade

If you need to reschedule your upgrade, you can do so if the upgrade is more than three business days away.

1. In Oracle Integration, click **Settings**, then **Upgrade**.
2. Under **Time window** you see your upgrade window for your current instance.

You can change your upgrade window if it's three or more business days away. All upgrade dates that are available to you appear in the list.

> **Note:**
>
> If you change your upgrade window *after* new IP addresses have been allocated for you environment (shown in the **Allowlist IP Addresses** section), Oracle can't guarantee the IP address allocations will remain the same. The IP addresses originally allocated will continue showing in the user interface until new ones are assigned.

If you have multiple instances, choose your upgrade windows carefully. See Recommendations for Upgrading 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.

3. Click **Save changes**.
4. Oracle emails you confirming the availability of your requested window.

   By default, upgrade notifications are automatically sent to the listed administrator email. Oracle recommends you have notifications sent to a distribution list or group email so that you don't miss important emails if someone leaves the company Add the distribution list, group email, or any other stakeholders who should receive upgrade notifications, by entering their email addresses, separated with commas (,) in the box **Upgrade Notifications**. Oracle will include these email addresses in all future upgrade notifications.

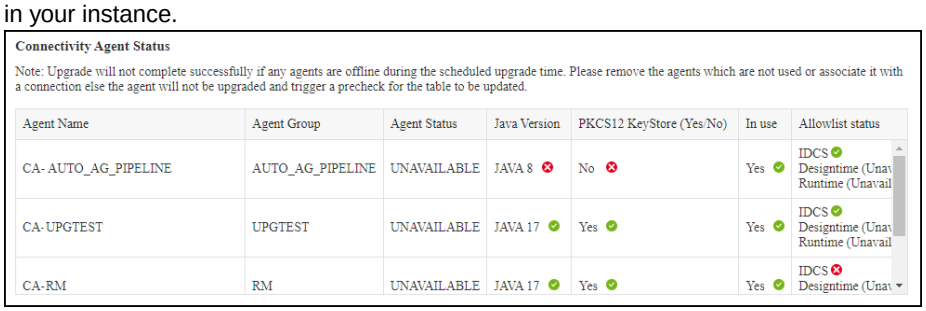
   You can continue with configuring your upgrade settings while waiting for the confirmation email.

Configure Your Upgrade Settings

1. Select the options appropriate for your instance.

Option	Description
Ignore precheck failures during upgrade	When selected, the readiness check ignores all precheck failures so that you can proceed with upgrade. **NOT_SUPPORTED:** You must complete post-upgrade tasks for any precheck failures that were ignored. See Complete Post-Upgrade Tasks for Ignored Precheck Failures.
Time window	If your upgrade has been scheduled, you see your upgrade window. You can change your upgrade window if it's three or more business days away, as described above. **Note:** If you change your upgrade window *after* new IP addresses have been allocated for you environment (shown in the **Allowlist IP Addresses** section), Oracle can't guarantee the IP address allocations will remain the same. The IP addresses originally allocated will continue showing in the user interface until new ones are assigned.
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. If you select Production, when you save your changes, you'll be prompted to confirm that you are satisfied with the testing you've 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 features.
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.

Option	Description
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 check box 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.
FlowId Conversion Support	Select the **Enable flowid as numeric post upgrade** check box to keep the instance ID as numeric.

Option	Description
Connectivity Agent Status	The Connectivity Agent Status section shows the status of all the connectivity agents in your instance.  The connectivity agent status table shows the following information: • **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. • **Allowlist status**: Shows whether the connectivity agent's allowlist has been updated to configure connectivity from the connectivity agent to Oracle Identity Cloud Service (IDCS) and Oracle Integration. See Complete Pre-Upgrade Tasks. **Caution:** You must update your allowlists *before* upgrade or you'll lose connectivity until it's done. 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.
Process upgrade	Make sure you fully understand these options before setting them. See Process Upgrade Options.

Option	Description
Allowlist IP Addresses	Two weeks before the upgrade, your new ingress and egress IP addresses are available: • **OIC Design-time IPs**: IP addresses for traffic entering into Oracle Integration 3 design time (the Oracle Integration 3 application). **Note:** The design-time URL supports the built-in Oracle Integration APIs. • **OIC Runtime IP**: IP address for traffic entering into your Oracle Integration 3 runtime applications. • **OIC Outbound IP**: IP address for traffic exiting Oracle Integration 3. • **VB Inbound IP**: IP address for traffic entering into Visual Builder. • **VB Outbound IPs**: IP addresses for traffic exiting Visual Builder. • **VB VCN OCID**: Oracle Cloud ID (OCID) of the Visual Builder service Virtual Cloud Network (VCN) for traffic exiting Visual Builder. • **Process Outbound IP**: IP address for traffic exiting Process Automation. You'll need these values to update your allowlists for your firewall and the server that hosts your connectivity agent.
Upgrade Notifications	By default, upgrade notifications are automatically sent to the listed administrator email. Oracle recommends you have notifications sent to a distribution list or group email so that you don't miss important emails if someone leaves the company Add the distribution list, group email, or any other stakeholders who should receive upgrade notifications, by entering their email addresses, separated with commas (,) in the box **Upgrade Notifications**. Oracle will include these email addresses in all future upgrade notifications.

2. Click **Save changes**.

As your upgrade date approaches, complete the pre-upgrade tasks.

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.

Summary of Pre-Upgrade Tasks

This table summarizes the pre-upgrade tasks for each area. The details for each task are linked in the table and shown in the next sections.

Area	Tasks
Connectivity Agent	• Prepare for conversion to OAuth 2.0 • Update your allowlist settings • Set the proxy server's Cache property
Instances	• Start capturing the activity stream in Oracle Cloud Infrastructure Console • Complete network rules configuration
B2B for Oracle Integration	• Ensure all B2B passwords for keystore match
Integrations	• Determine what to do with failed instances • Decide what to do with asynchronous messages • Change Oracle Integration built-in API calls from Basic Authentication to OAuth
Adapters	• Stop using decommissioned Microsoft adapters
Visual Builder	• Prepare Visual Builder for upgrade

Area	Tasks
Allowlists	• Update Allowlists
Communication	• Inform Users and Stakeholders About Upgrade
Development work	• Limit Development Work Before the Upgrade

Connectivity Agent Pre-Upgrade Tasks

Task	Typical owner	Tasks description
Prepare for conversion to OAuth 2.0	Development Operations team	In Oracle Integration Generation 2, the connectivity agent uses basic authorization to invoke Oracle Integration endpoints. Oracle Integration 3 instead uses OAuth 2.0 token-based authentication, which is more secure. During the upgrade, your connectivity agents connections are automatically converted from using basic authentication to using OAuth 2.0, so you don't need to manually recreate any connections yourself. 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 as described in Update Allowlists. And, after upgrade, as a result of the new authentication method, you'll see additional traffic to your firewall. This additional traffic occurs because the connectivity agent must communicate with the server to get new tokens. For more information on OAuth 2.0 support in Oracle Integration 3, see When is Basic Authentication Supported in Oracle Integration 3?.
Update your allowlist settings	Development Operations team	If your organization uses allowlists, you must update your allowlist settings for your connectivity agents. The **Allowlist status** column in the **Connectivity Agent Status** section shows the status of all the connectivity agents in your instance, indicating whether the allowlist has been updated appropriately. As your upgrade window nears, perform the tasks described in Update Allowlists. Agents that are offline during upgrade or don't meet upgrade requirements won't be upgraded, in which case you'll need to perform post-upgrade steps to regain connectivity.
Set the proxy server's Cache property	Development Operations team	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`.

Instance Pre-Upgrade Tasks

Task	Typical owner	Tasks description
Start capturing the activity stream in Oracle Cloud Infrastructure Console	Administrator	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.
Complete network rules configuration	Network administrator	This task can be completed pre-upgrade or immediately after upgrade. If any of your integration connections target an Oracle Cloud Infrastructure service that supports network rules, such as Oracle Cloud Infrastructure Object Storage or Oracle Autonomous Database, and you've enabled those rules, you must complete any network rules configuration, including adding the Oracle Integration Service VCN to the rule. See Ensure Connectivity.

B2B for Oracle Integration Pre-Upgrade Tasks

Task	Typical owner	Tasks description
Ensure all B2B passwords for keystore match	Administrator	Ensure that all passwords for the keystore file are identical. Your identity certificate file (JKS) requires two sets of passwords: Key Passwords and Keystore Password. All the passwords must be identical. If they're not identical, edit the passwords to match, and re-upload the keystore file. If you don't have the keystore file that was last uploaded, recreate the file. When uploading the certificate: • For **Type**, select **X.509 (SSL Transport)**. • For **Category**, select **Identity**. See Upload an SSL Certificate in *Using Integrations in Oracle Integration Generation 2*. **Caution:** If you don't complete this step, the upgrade will fail.

Integrations Pre-Upgrade Tasks

Task	Typical owner	Tasks description
Determine what to do with failed instances	Development Operations team	Failed integration instances fall into one of the following categories, which determines how you can handle them: • **Failed asynchronous instances - recoverable** Resubmit the failed instances and clear the queue. See Resubmit Failed Messages. If you have a failed asynchronous instance when your instance is upgraded, 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. • **Failed synchronous instances - non-recoverable** You can't resubmit synchronous integration instances, so they are not recoverable. **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.

Task	Typical owner	Tasks description
Decide what to do with asynchronous messages	Development Operations team	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.
Change Oracle Integration built-in API calls from Basic Authentication to OAuth	Developer	If you didn't already update your API calls to use OAuth while completing prerequisites, do so now or immediately after upgrade. In Oracle Integration Generation 2, you could use Basic Authentication to use the Oracle Integration REST API and File Server REST API. In Oracle Integration 3, you must use OAuth. You 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 details on using OAuth with the Oracle Integration REST API, see Security, Authentication, and Authorization, or with the File Server REST API, see Security, Authentication, and Authorization.

Adapters Pre-Upgrade Tasks

Task	Typical owner	Tasks description
Stop using decommissioned Microsoft adapters	Development team	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 See Invoke Operations Page in *Using the Microsoft Office 365 Calendar Adapter with Oracle Integration 3*. • Microsoft Office 365 People Adapter See Invoke Operations Page in *Using the Microsoft Office 365 People Adapter with Oracle Integration 3*. • Microsoft Office 365 Outlook Adapter See Invoke Operations Page in *Using the Microsoft Office 365 Outlook Adapter with Oracle Integration 3*.

Visual Builder Pre-Upgrade Tasks

Task	Typical owner	Tasks description

Prepare Visual Builder with custom endpoint using SSL for upgrade	Administrator	If Visual Builder is enabled, you use a custom endpoint or alternate custom endpoints, and you're using SSL, perform the following steps:
		1. To allow access to the SSL certificate secret for upgrade, add the following policies, replacing *MySecretCompartment* with the compartment that includes the SSL certificate secrets:
		`allow service vb-vbprod to manage secrets in compartment MySecretCompartment`
		`allow service vb-vbprod to manage keys in compartment MySecretCompartment`
		`allow service vb-vbprod to manage vaults in compartment MySecretCompartment`
		`allow service vb-vbprod to read secret-bundle in compartment MySecretCompartment`
		2. Update your Visual Builder tenant and app settings, and any integration applications, so that they point to the original Oracle Integration Generation 2 URL rather than the custom endpoint. During upgrade, the custom endpoint will be configured in Visual Builder, so, after upgrade, only Visual Builder apps will be accessible through the custom endpoint.

Prepare Visual Builder for upgrade	Development Operations team	Complete the tasks described in Prepare Visual Builder for the Upgrade in *Administering Oracle Visual Builder in Oracle Integration 3*.
Review known issues	Development Operations team	Review Known Issues for Live/Staged Apps Post-Upgrade to Oracle Integration 3 in *Known Issues for Oracle Integration 3* for issues that might result in Live or staged apps not working correctly after upgrading to Oracle Integration 3.

Update Allowlists

> **Important:**
>
> If your organization uses allowlists (also known as access control lists, or ACLs), you *must* add the IP addresses and URLs to your allowlists before upgrade to prevent errors and to make sure Oracle Integration can access your applications.

1. **Get the new IP addresses.**
   The new IP addresses appear on the **Upgrade** page approximately two weeks before your upgrade.
   a. In the navigation pane, click **Settings**, then **Upgrade**.
   b. Under **Allowlist IP Addresses**, note the following IP values:
      - **OIC Design-time IPs**: IP addresses for traffic entering into Oracle Integration 3 design time (the Oracle Integration 3 application).
        Note: The design-time URL supports the built-in Oracle Integration APIs.
      - **OIC Runtime IP**: IP address for traffic entering into your Oracle Integration 3 runtime applications.

- **OIC Outbound IP**: IP address for traffic exiting Oracle Integration 3.
- **VB Inbound IP**: IP address for traffic entering into Visual Builder.
- **VB Outbound IPs**: IP addresses for traffic exiting Visual Builder.
- **VB VCN OCID**: Oracle Cloud ID (OCID) of the Visual Builder service Virtual Cloud Network (VCN) for traffic exiting Visual Builder.
- **Process Outbound IP**: IP address for traffic exiting Process Automation.

c. You also need the IDCS IP address. To find the IDCS IP address, use the following command, replacing *IDCS_GUID* with the Identity Service ID:
`nslookup IDCS_GUID.identity.oraclecloud.com`

2. **Update your allowlists according to your organization's procedures to control traffic going into and coming out of Oracle Integration.**
For example, you may use allowlists to manage the following types of Oracle Integration traffic.

Type of traffic	Associated allowlist	How to update the allowlist
Inbound traffic going to Oracle Integration and File Server	Oracle Integration instance	If you use Visual Builder, you need to add the **VB VCN OCID** to the Oracle Integration Generation 2 allowlist before upgrade. See Allow Your Instance to Access Services in *Administering Oracle Visual Builder Generation 2*. Other than that, no action is needed. Oracle migrates your existing allowlist as part of the upgrade.
Inbound traffic going to Oracle Integration through your *internal firewall*	Internal firewall	If your organization restricts the sites that internal resources can access, add the following IP addresses to your internal firewall allowlist: • **OIC Design-time IPs** • **OIC Runtime IP** • **VB Inbound IP**
Inbound traffic going to File Server through your *internal firewall*	Internal firewall	If your organization restricts the sites that internal resources can access, you'll need to add the File Server IP address to your internal firewall allowlist. However, you won't know the IP address until after upgrade. See Complete Post-Upgrade Tasks.
Inbound traffic going to Oracle Integration and IDCS through your *connectivity agents*	Connectivity agent server	Configure connectivity from your connectivity agents to Oracle Integration and Oracle Identity Cloud Service (IDCS). Add the following IP addresses to the allowlists for the servers that host your connectivity agents: • **OIC Design-time IPs** • **OIC Runtime IP** • **VB Inbound IP** • **IDCS IP** Although the IDCS IP address doesn't change after upgrade, the connectivity agent now needs access to IDCS for OAuth. If you haven't already allowed IDCS access across your network, add the IDCS IP address.

Type of traffic	Associated allowlist	How to update the allowlist
Outbound traffic going out of Oracle Integration, Visual Builder, or Process Automation to your cloud systems	Target service	For each target service accessed by Oracle Integration technologies, add the appropriate outbound IP address to the service's allowlist. • For Oracle Integration, allowlist the **OIC Outbound IP**. • For Visual Builder, allowlist the **VB Outbound IP**. • For Process Automation, allowlist the **Process Outbound IP**.

> **Caution:**
>
> If you update allowlists before the upgrade, don't remove the IP addresses 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 and you can remove them.

Next, inform users and stakeholders about the upcoming upgrade.

Inform Users and Stakeholders About Upgrade

As your upgrade approaches, you need to 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.

Next, plan to limit or pause your development work during the days leading up to the upgrade. See Limit Development Work Before the Upgrade.

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.

By default, upgrade notifications are automatically sent to the specified administrator email. Oracle recommends you have notifications sent to a distribution list or group email so that you don't miss important emails if someone leaves the company. You set who receives notifications on the **Upgrade** page. See "Upgrade Notifications" in Configure Your Upgrade Settings.

Make sure you also complete all required tasks before the upgrade. See 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.
     By default, failed integration instances will be ignored during upgrade.
   - If you use Processes in Oracle Integration Generation 2, don't create any new Process applications or Process transactions.

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. Everyone should stop working in Oracle Integration Generation 2 and sign out.

> **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.

Next, on upgrade day, you need to wait for the upgrade to finish and then perform the post-upgrade tasks. See What to Do During Upgrade.

Process Upgrade Options

Depending on how you're using Process in Oracle Integration Generation 2, you'll use a different option to upgrade or migrate. The following workflow will help you determine how to proceed.

Upgrade option	When is this option appropriate?	Synopsis of the option
Automated In-Place Upgrade for Process	• You have no process usage (running or completed instances), or • Your process usage is in a pre-production state, or • You have short-lived process instances that can be completed in Oracle Integration Generation 2 before upgrade, or • You are only using decision applications.	**Before upgrade** You must perform the following steps: • Replace the Process action in any affected integrations. • Ensure that all required transactions complete in Oracle Integration Generation 2 prior to upgrade. **During upgrade** Oracle performs the following steps: • Exports your process applications from Oracle Integration Generation 2. • Enables Process Automation in your upgraded Oracle Integration 3 instance. • Converts your existing process applications and imports them into your Oracle Integration 3 instance. If any of your process applications use unsupported actions (for example, an Insight activity), Oracle replaces those actions with placeholder actions that you must replace or remove after upgrade. See Complete Post-Upgrade Tasks for Process Automation. **Note:** Process instance data is not migrated to Oracle Integration 3. This means you won't see historical transactions created in Oracle Integration Generation 2 after upgrade. **After upgrade** You must perform post-upgrade activities to restore your process applications to working order. See Complete Post-Upgrade Tasks for Process Automation.

Upgrade option	When is this option appropriate?	Synopsis of the option
Migrate Process Applications to a New OCI Process Automation Instance	• You are using process in production, and • You have long-running process instances which can't be completed prior to upgrade, and • You need to continue to serve new process application requests without any disruption, and • You have integrations or Visual Builder applications that you do not want to disrupt with the process migration.	**Migrate process applications to OCI Process Automation** • Provision a new OCI Process Automation instance. • Migrate process applications to the new instance. • Perform post-migration activities to restore process applications to working order. • Update clients that call OCI Process Automation. **Switch to OCI Process Automation for new transactions** • Promote process applications to production. • Perform switchover to OCI Process Automation. • Serve new process transactions from OCI Process Automation. • Run Oracle Integration Generation 2 in parallel with OCI Process Automation until existing transactions complete (coexistence period). **Upgrade to Oracle Integration 3** • Upgrade the Oracle Integration Generation 2 instance once all process instances complete. • Attach the OCI Process Automation instance to Oracle Integration 3.

Automated In-Place Upgrade for Process

You can use automated in-place upgrade for Process under the following situations:

- You have no process usage (running or completed instances), or
- Your process usage is in a pre-production state, or
- You have short-lived process instances that can be completed in Oracle Integration Generation 2 before upgrade, or
- You are only using decision applications.

If this upgrade option fits your situation, complete the steps detailed in this topic.

Prepare Your Initial Upgrade Environment

> **Important:**
>
> Oracle recommends that you first perform these steps on a non-production instance that isn't critical to your business. These steps may a while to complete, and this initial upgrade may identify issues that you need to resolve or account for prior to production upgrade.

If you have one of the following environments, you should follow the steps in this section to create a temporary environment for upgrade validation:

- If you're running production workloads in a single production instance and you don't have a non-production instance, any issues you encounter could cause downtime for process users.
- If your environment consists of a production instance and a single non-production instance that you rely on for backup and urgent fixes, you would be left without the backup until your production environment is upgraded.

If you have multiple non-production instances, you can skip to Upgrade Your Non-Production Environment.

To create a temporary environment for upgrade validation, perform the following steps:

1. Create a new Oracle Integration Generation 2 instance.
2. Copy your design-time metadata to the new instance.
   The metadata can come from either a production or non-production instance. However, using production instance metadata means that you'll be more prepared for what you need to do when it's time to upgrade your actual production instance.
3. Continue with the steps in Upgrade Your Non-Production Environment, and then test the upgrade.
   When you're ready to upgrade your other instances, you can export your refactored integrations and process applications to speed up the post-upgrade tasks for the instance that acted as the source of your copied design-time metadata.

Upgrade Your Non-Production Environment

> **Important:**
>
> If you don't have a non-production instance, Oracle recommends you create a temporary environment for upgrade validation as described above.

Perform the following steps on your non-production environment.

Task	When to perform the task	Who performs the task	Task details
Analyze any design-time gaps	Before upgrade	You	In the **Process Automation** precheck, expand **More details** and note any issues. See How Upgrade Affects Process Features for workarounds or alternate solutions. You'll need to implement these options after upgrade to restore and activate your process applications. If you're using an unsupported feature and you're unable to follow the suggestions, contact your Oracle representative or file a service request.

Task	When to perform the task	Who performs the task	Task details
Remove or replace Process action	Before upgrade	You	In the **Process Action** precheck, expand **More details** and note any integrations use this action. At least three to four days prior to upgrade perform the following steps for each integration that uses Process action: 1. Deactivate the integration. **Note:** Deactivating these integrations makes the associated applications unavailable for a while. Make sure you communicate this ahead of time to anyone who uses these applications. 2. Note the input and output mapping associations. 3. Remove the Process action, replace it with a placeholder (for example, a Note activity).
Bypass the active instances precheck	Before upgrade	You	Select **Ignore active instances and proceed with upgrade**, and then click **Save changes**. You will be asked to confirm your choice twice. **WARNING:** Selecting this option will result in the loss of running (in-progress) and completed process instances. Be careful when selecting this option, especially in a production instance. After you select this option, the Process Automation precheck changes to a warning, indicating that the precheck has been bypassed.
Reschedule your upgrade	Before upgrade	You	If necessary, reschedule your non-production instance upgrade.
Limit development work	Two to three days before upgrade	You	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 re-scheduled. For example: • Don't create or edit process or decision applications. • Don't create new process instances.

Task	When to perform the task	Who performs the task	Task details
Upgrade Process	During upgrade	Oracle	During upgrade, Oracle performs the following steps: • Exports your process applications from Oracle Integration Generation 2. • Enables Process Automation in your upgraded Oracle Integration 3 instance. • Converts your existing process applications and imports them into your Oracle Integration 3 instance. If any of your process applications use unsupported actions (for example, an Insight activity), Oracle replaces those actions with placeholder actions that you must replace or remove after upgrade. See Complete Post-Upgrade Tasks for Process Automation. **Note:** Process instance data is not migrated to Oracle Integration 3. This means you won't see historical transactions created in Oracle Integration Generation 2 after upgrade.
Complete post-upgrade tasks	After upgrade	You	Perform post-upgrade activities to restore your process applications to working order. See Service-Level Post-Upgrade Tasks for Process Automation. If your process applications are part of a solution that involves Visual Builder or integrations, you may need to perform additional steps to update your other clients. See Update Clients that Call Process Applications.

Upgrade Additional Non-Production Environments

If you have additional non-production environments, you can perform the pre-upgrade steps from the table above. However, instead of completing the post-upgrade tasks, you might want to export your restored process applications and related artifacts (for example, Visual Builder applications) from the first environment and import them into the additional environments after upgrade. This could save you time not having to perform the post-upgrade steps on multiple environments.

Upgrade Your Production Environment

> **Important:**
>
> If you want to follow this upgrade process for a production environment, be aware of the following:

- You may need to limit business users from creating new transactions prior to upgrade.
- You'll need to identify and complete running transactions prior to upgrade.
- There will be some downtime after upgrade to perform post-upgrade tasks. During this time, your business will not be able to run new processes.
- Process instance data is not migrated to Oracle Integration 3. This means you won't see historical transactions created or completed in Oracle Integration Generation 2 after upgrade.

Before deciding to proceed with this upgrade process:

- Evaluate how many running transactions are in your environment, and complete these transactions prior to upgrade. To view the running transactions:
  1. Sign in to your Oracle Integration Generation 2 instance as a user with the Service Administrator role.
  2. Click **My Tasks**, then choose **Processes**.
- Save runtime data from Oracle Integration Generation 2 Process. This step is important to ensure that you don't lose the history of completed transactions. You must do this *before* upgrade. See Archiving and Purging Process Automation Data in Oracle Integration. As part of these steps, you'll configure the Oracle Storage Service and schedule instances for archive and purge. Be aware of the following points:
  - The archived information will be available in the configured Object Storage bucket.
  - Attachments aren't included in the archive files. You must export these manually. See Retrieve a Process Attachment as a Stream in *REST API for Oracle Integration 2*.

If you decide to proceed with this upgrade process for your production environment, perform the steps from the table above.

Migrate Process Applications to a New OCI Process Automation Instance

If you're actively using Process in a production environment, Oracle can't automatically migrate you to Process Automation during the upgrade to Oracle Integration 3. You'll have to perform the migration manually.

Migrating process applications to a new standalone OCI Process Automation instance is appropriate under the following situations:

- You are using process in production, and
- You have long-running process instances which can't be completed prior to upgrade, and
- You need to continue to serve new process application requests without any disruption, and
- You have integrations or Visual Builder applications that you do not want to disrupt with the process migration.

The upgrade path proposed below has been designed to limit disruption and maintain business continuity. It offers a well-tested approach for environments that have active (and usually long-running) process instances. It may not be applicable in all situations, so you should assess your own needs and implementation details to determine whether its appropriate for you.

The upgrade path can be broken down into three phases.

Phase	Description	Where process users work	Tasks
Phase 1: Migrate Process Applications to OCI Process Automation	The goal of this phase is to migrate your Oracle Integration Generation 2 Process applications to OCI Process Automation and restore them to a working order. This enables you to identify and correct any issues. This phase won't affect your existing production environment.	During this phase your process users continue to work in Oracle Integration Generation 2.	1. Provision and Prepare an OCI Process Automation Instance 2. Migrate Process Applications to the New Instance 3. Map Users and Groups to New Application Roles 4. Validate and Activate Imported Process Applications 5. Update Clients that Call Process Applications
Phase 2: Switch to OCI Process Automation	The goal of this phase is to ensure that all new process requests are served by OCI Process Automation. In this phase, you promote your process applications and their dependencies to production and point all end users and clients to use OCI Process Automation going forward.	During this time your process users switch to using OCI Process Automation for all *new* requests. They may also need to complete *existing* requests in Oracle Integration Generation 2 until all instances started on Oracle Integration Generation 2 are complete.	1. Promote Process Applications to Production 2. Perform Switchover to OCI Process Automation 3. Coexistence Period
Phase 3: Upgrade to Oracle Integration 3	The goal of this phase is to complete the upgrade of your existing Oracle Integration Generation 2 instance to Oracle Integration 3. At this stage there should be no running process instances in Oracle Integration Generation 2, making your instance eligible for upgrade to Oracle Integration 3. At the end of this phase you'll have an Oracle Integration 3 instance linked with a standalone OCI Process Automation instance.	During this time your process users work exclusively in OCI Process Automation.	1. Prepare for Upgrade 2. Complete Post-Upgrade Tasks for Process Automation

Phase 1: Migrate Process Applications to OCI Process Automation

Perform the following tasks to migrate your process applications to OCI Process Automation:

1. Provision and Prepare an OCI Process Automation Instance
2. Migrate Process Applications to the New Instance
3. Map Users and Groups to New Application Roles
4. Validate and Activate Imported Process Applications
5. Update Clients that Call Process Applications

Provision and Prepare an OCI Process Automation Instance

Create a new OCI Process Automation instance. Oracle recommends you provision a standalone OCI Process Automation environment.

For more details on this recommendation, see Upgrade FAQs.

> **Important:**
>
> The rest of these instructions are based on using a OCI Process Automation standalone instance. Do not deviate from this recommendation unless you have an alternative migration plan in place.

1. **Create a new OCI Process Automation standalone instance.**
   See Provision a Process Automation Instance in *Administering Oracle Cloud Infrastructure Process Automation*.

   When you create the instance:

   - Select a metering model based on an Execution Pack to leverage free tier pricing during the upgrade.
   - The user that creates the OCI Process Automation standalone instance must be from the same identity domain as the user that created your Oracle Integration Generation 2 instance.
   - You must create the OCI Process Automation standalone instance in the same tenancy, the same region, and, preferably, the same compartment as your Oracle Integration Generation 2 instance.
     If you don't use the same compartment, make sure that the user that creates the OCI Process Automation instance has permissions to manage both the Oracle Integration instance and the OCI Process Automation instance.

     You manage these permissions with IAM policies.

     For Oracle Integration:

     - `allow group domain-name/group_name to manage integration-instance in compartment compartment-name`
     - `allow group domain-name/group_name to manage integration-instance in tenancy`

     For example:

     - `allow group admin/oci-integration-admins to manage integration-instance in tenancy`

     For OCI Process Automation:

     - `allow group domain-name/group_name to manage process-automation-instance in compartment compartment-name`

- `allow group domain-name/group_name to manage process-automation-instance in tenancy`

  For example:

- `allow group admin/oci-integration-admins to manage process-automation-instance in tenancy`

2. **Grant developers access to OCI Process Automation.**
   To ensure your developers can access the newly provisioned OCI Process Automation instance and can work on subsequent tasks, ensure that they're assigned the appropriate IDCS application role to access the instance. See Assign IDCS Application Roles to Groups in an Identity Domain in *Administering Oracle Cloud Infrastructure Process Automation*.
3. **Register a *non-production* Oracle Integration Generation 2 instance for testing.**
   If your process applications are calling existing integrations, register Oracle Integration Generation 2 in the new OCI Process Automation instance. This allows your OCI Process Automation instance to connect and discover your existing integrations.

   Ensure that you use a *non-production* Oracle Integration Generation 2 instance for service registration in this step. Make sure that registering the selected Oracle Integration Generation 2 instance won't adversely impact any processes in production.

   a. Choose a *non-production* Oracle Integration Generation 2 instance to register.
   b. In the Oracle Cloud Infrastructure Console, find and take note of the OCID of the selected Oracle Integration Generation 2 instance.
   c. In OCI Process Automation, register the Oracle Integration Generation 2 instance. See Register Services in *Using Oracle Cloud Infrastructure Process Automation*.

> **Note:**
>
> You may want to create a dedicated ServiceAccount user for this connection.

Migrate Process Applications to the New Instance

Migrate your existing process applications to the new OCI Process Automation standalone instance.

1. **Determine which applications you want to migrate.**
   You may want to take this opportunity to get rid of unnecessary applications. Think about whether you want to migrate only those applications that are in your production environment or if you want to also migrate applications that are in test and development.

   If you're going to migrate individual applications, take note of the applications you want to migrate and any dependencies they have.
2. Migrate your applications using one of the following methods:
   - **Migrate all applications in bulk**

     a. In the Oracle Cloud Infrastructure Console, create an Object Storage bucket. See Creating an Object Storage Bucket.
     The storage bucket URL you'll need in the next step is in the following format:

     `https://swiftobjectstorage.region.oraclecloud.com/v1/namespace/bucket`

     Where:

     - *region* is the identifier of your Oracle Cloud Infrastructure (OCI) data center.

- *namespace* is the tenancy where you created your bucket.
- *bucket* is your bucket name.

b. Make a POST request to your Oracle Integration Generation 2 instance to export your applications:
`curl -X POST https://Generation2_hostname/ic/api/process/v1/exportArtifactsInternal`

With the following payload:

```
{
    "jobId": "enter_a_descriptive_ID",
    "storageInfo": {
        "storageUrl": "Swift_storage_bucket_URL",
        "storageUser": "OCI_Console_user",
        "storagePassword": "OCI_Console_user_password"
    }
}
```

You'll know the export job is complete when you see the `process_status.json` file in your bucket. This file contains the status of the job, its completion percentage, and, if failed, the error message. You should also see the following content in your bucket:

- `Process/project folder`—contains all your process applications.
- `Process/dmn folder`—contains all your decision models.

c. After the applications have been exported into your bucket, make a POST request to your Oracle Integration 3 instance to migrate your applications:
`curl -X POST https://Integration3_hostname/process/api/v1/oic-migration/jobs/`

With your tenant ID:

`x-tenant-id: tenant_OCID`

And your bucket information:

```
{
    "bucketInfo": {
        "region": "region",
        "namespace": "namespace",
        "bucket": "bucket"
    }
}
```

See Security, Authentication and Authorization in *REST API for Oracle Cloud Infrastructure Process Automation*.

d. Wait for the migration job to complete. To check the status of the migration job:
`curl http://localhost:8080/process/internal-api/v1/oic-migration/jobs/job_ID`

- **Migrate individual applications**

a. Export the Oracle Integration Generation 2 process applications.
In the Oracle Integration Generation 2 instance that includes the applications you want to migrate, export each application you want to migrate. See Export an Application in *Using Processes in Oracle Integration Generation 2*.

b. Import the process applications into OCI Process Automation.
In OCI Process Automation, import the Oracle Integration Generation 2 process applications. See Import an Application in *Using Oracle Cloud Infrastructure Process Automation*.

OCI Process Automation converts the legacy process applications to the latest product version.

3. **Review the migration report.**
When the import and conversion is complete, you'll see a migration report showing what was successfully imported, what needs additional work, and any items that couldn't be migrated. This gives you an idea of migration issues that you'll need to handle.

You can refer back to the original migration report in the main menu. See Import an Application in *Using Oracle Cloud Infrastructure Process Automation*.

Map Users and Groups to New Application Roles

Application Roles have significantly changed in OCI Process Automation. ProcessOwner, AnalyticsViewer, and ProcessReviewer roles are now explicitly defined for each application, enabling you to control their members and permissions.

The following table shows how the Oracle Integration Generation 2 roles map to the OCI Process Automation roles.

Oracle Integration Generation 2	OCI Process Automation
<application-name>.**ProcessOwner**	Process Owner
<application-name>.**AnalyticsViewer**	N/A
<application-name>.<swim-lane>	<swim-lane>
<application-name>.**ProcessReviewer**	Process Reviewer

The new roles are available after the migration, but you need to add members (users and groups) to them. You'll probably need to reference your Oracle Integration Generation 2 environment to see which members should be assigned to each role.

If OCI Process Automation shares the same identity domain as your existing Oracle Integration Generation 2 instance, existing users and groups should be available for selection.

You can add members either before activation in the Designer or after activation in the Workspace.

- Work with Roles in Designer
- Manage Roles in Workspace

For additional information on OCI Process Automation, see Configure Roles for Process Applications in *Using Oracle Cloud Infrastructure Process Automation*.

Validate and Activate Imported Process Applications

To validate and activate your process applications, perform the following steps:

1. **Validate each application and fix any errors and warnings.**

Validate each application from the Designer by clicking  and choosing **Validate** from the menu.

To resolve validation issues, see How Upgrade Affects Process Features.

2. **Activate the application.**

After you've resolved all validation errors, you can activate your application. See Activate Applications in *Using Oracle Cloud Infrastructure Process Automation*.

Update Clients that Call Process Applications

Depending on your specific usage, you'll perform different steps to update your clients.

Perform the steps that apply to your implementation:

- Integrations Calling Process
- Integrations Called by Process
- Visual Builder Applications
- Non-Oracle-Integration Clients
- Verification

Integrations Calling Process

Process APIs and endpoints have changed after the upgrade. As a result, you must update any integrations that use the Process Action to use the REST adapter instead. Perform these steps in your Oracle Integration Generation 2 instance.

1. **Create a connection.**
   Create a new REST based connection for OCI Process Automation, using the following settings.

Setting	Value
Role	Invoke
Connector Type	REST API Base URL
Connection URL	Base URL taken from your OCI Process Automation environment. For example: `https://process-instance.process.oci.oc-test.com`

Setting	Value
Security Policy	OCI Process Automation supports several grant types that map to the following in Oracle Integration: • OAuth Client Credentials • OAuth Resource Owner Password Credentials • OAuth Authorization Code Credentials For more information on OCI Process Automation grant types, see Security, Authentication and Authorization in *REST API for Oracle Cloud Infrastructure Process Automation*. Regardless of which grant type you choose you'll need to provide the following information: • **Access Token URL**—Also referred to as the Oracle Identity Cloud Service URL. For example: `https://idcs-id.oraclecloud.com/oauth2/v1/token` • **Client ID**— The identifier you retrieved when you registered the confidential application in Oracle Identity Cloud Service (IDCS), or the identifier of your OCI Process Automation application. You can find the client ID when viewing the confidential application you configured in IDCS, on the **Configuration** tab, in the **General Information** section. • **Client Secret**— The client secret issued to the client during the application registration process. • **Scope**— The scope value associated with your OCI Process Automation instance registered in your confidential application. You can find the client ID when viewing the confidential application you configured in IDCS, on the **Configuration** tab, in the **Accessing APIs from Other Applications** section, under **Allowed Scopes**, in the scope that you added. For example: `https://process-instance.process.oci.oc-test.com/process` • **Client Authentication**—Send client credentials as basic auth in header.

2. **Test your connection to ensure it's configured correctly.**
3. **Update your integrations.**
   For each integration that uses the Process Action:
   a. Create a new version or clone your integration.
   b. Replace the Process Action with the REST Connector configured above, using the following settings.

Setting	Value
Relative URI	To initiate a new process instance use the following URI: `/process/api/v1/instances` To call any other OCI Process Automation API, see *REST API for Oracle Cloud Infrastructure Process Automation*.
Endpoint Action	POST
Request Payload	Retrieve this from the OpenAPI specification. You can find the specification under the API section of the OCI Process Automation activation panel. This specification provides the definition of the payload needed to call your process.

Setting	Value
Data Mapping	Map the following: • A parameter that uniquely identifies the process You can get the process Key from the title of the OpenAPI specification (see above) • Data objects These are process specific and contain the actual data payload used to initiate the process.

c. Activate your integrations.

d. Test your integrations and ensure that a new process instance is created in OCI Process Automation.

Integrations Called by Process

OCI Process Automation supports REST based communication only via Service Registration. This means that connectivity to SOAP based integrations will no longer be possible.

If you have integrations that use a SOAP trigger and these are called by processes in Oracle Integration Generation 2, you will need to take additional steps to present a REST based interface to OCI Process Automation. This may mean that you need to do *one* of the following:

- Create REST-based wrapper integrations.
  or
- Change the existing trigger from SOAP to REST.

Additionally, for service registration to work as expected, ensure that your REST trigger utilizes the OAuth 2.0 or Basic Authentication Security policy.

Visual Builder Applications

Process API endpoints change after the upgrade. As a result, you must update any Visual Builder applications that interact with them, replacing any deprecated integration patterns. See Work with Business Processes in *Building Responsive Applications with Visual Builder Studio*.

To do this you may need to evaluate current process usage. Look through each of your Visual Builder applications and determine if they're making calls to process APIs via Action Chains, Direct Calls, or using embeddable process components (also referred to as CCA).

If your applications are calling Process endpoints, perform the following steps:

1. **Connect to OCI Process Automation.**
   Create a backend connection to OCI Process Automation. This backend will be used to establish a connection to the new OCI Process Automation instance. See Connect to Oracle Process Automation APIs in *Building Responsive Applications with Visual Builder Studio*.
2. **Create a new version of your applications.**
   Oracle recommends, creating a new version of your Visual Builder applications to implement required changes. See How to Create Versions of an Application in *Developing Applications with Oracle Visual Builder*.
3. **Action Chains**
   If your application is using action chains to start a process or take action on a task, you'll need to replace each of these with a REST-based Service Connection. Repeat these steps for each process action chain task.

   Triggering a Process

   Replace the Start Process action chain with a Catalog based Service Connection.

a. Navigate to Oracle Integration Generation 2 and take note of the process you're calling. You can determine this either from the action chain process step or from the processes tab in the application menu on the left.

b. Create a Catalog-based Service Connection to your process in the new version of your Visual Builder application. See Create a Service Connection from an OCI Process Automation Catalog in *Building Responsive Applications with Visual Builder Studio*. Ensure that you select the same process you were referencing before.

> **Note:**
>
> Your process should already be activated.

c. Create a Type based on the endpoint of the above process. See Create a Type from an Endpoint in *Developing Applications with Oracle Visual Builder*.

d. Create a Variable based on the above type. See Create Variables in *Developing Applications with Oracle Visual Builder*.

e. Navigate to your action chains and perform the following actions:

   i. Drag an Assign Variable Action above your current Start Process Action.

   ii. Map the data fields and input parameters required to invoke your process. For an example, see Integrate Oracle Process Automation with Visual Builder.

   iii. Drag the Call REST Action above your current Start Process Action.

   iv. Configure the Call REST Action by selecting the POST/Instances endpoint.

   v. Map the above Variable to the request body of the REST Action.

   vi. Delete the legacy Start Process Acton.

f. Test the call, and ensure that your process is being called successfully in OCI Process Automation.

GET Process Instance

Replace the Get Process Instance action chain with a Catalog-based Service Connection.

If you created a Catalog-based Service Connection to your process by following the steps above, you'll notice that Get Process Instance endpoint is now available in your service connection.

Replace the legacy Get Process Instance Process Action with a Call REST Action that is configured with the above endpoint, and re-map the instanceID field.

> **Note:**
>
> The response payload values here have changed.

Other Process Actions

Perform the following steps for all other Process Actions such as Perform Task and Get Task:

a. Navigate to Oracle Integration Generation 2 and take note of the Process Actions you're using.

b. Replace these Actions with endpoint-based Service Connections.

The following table maps each of these actions to the corresponding OCI Process Automation API.

Visual Builder Action	OCI Process Automation REST API	Description
Perform Task	POST /process/api/v1/tasks/{id}/complete	Approval actions such as Approve, Reject, and so on.
Perform Task	PUT /process/api/v1/tasks/{id}	Update the Task Priority, Payload, Title, and such.
Perform Task	PUT /process/api/v1/tasks/{id}/payload	Update the Task Payload.
Perform Task	POST /process/api/v1/tasks/{id}/claim	Claim a task.
Perform Task	POST /process/api/v1/tasks/{id}/release	Release a task.
Perform Task	POST /process/api/v1/tasks/{id}/request-for-info	Request for information on a task.
Perform Task	POST /process/api/v1/tasks/{id}/submit-info	Submit the requested information for a task.
Perform Task	POST /process/api/v1/tasks/{id}/reassign	Reassign a task.
Get Task Collection	GET /process/api/v1/tasks	
Get Task	GET /process/api/v1/tasks/{id}	
Get Deployed Process Collection	GET /process/api/v1/instances	
Get Process Instance Collection	POST /process/api/v1/instances	

4. **Direct Calls**
   Process APIs and endpoints change after the upgrade. As a result, you must update any direct service connections. See *REST API for Oracle Cloud Infrastructure Process Automation*.

5. **CCA Components**
   If you're using Oracle Integration Generation 2 Process CCA components, you must replace them with their equivalent OCI Process Automation component.

Component Name	Oracle Integration Generation 2 CCA	OCI Process Automation Equivalent
Task List	oj-pcs-task-list	oj-opac-task-list
Task Detail	oj-pcs-task-detail	oj-opac-task-detail
App List	oj-pcs-app-list	oj-opac-applist
Start Form	oj-pcs-start-form	oj-opac-start-form
DP List	oj-pcs-dplist	oj-opac-instance-list (Displays both Structured Process and Dynamic process)
Visualization	oj-pcs-visualization	oj-opac-analytics (Cannot save visualizations)

Non-Oracle-Integration Clients

If you're calling process applications from outside Oracle Integration (for example, your own custom application), you need to update the REST endpoints and auth policies used to call the newly configured OCI Process Automation instance. For more information on the new API

endpoints and supported auth policies, see *REST API for Oracle Cloud Infrastructure Process Automation*.

Verification

Perform a System Integration Test to validate your work.

Test the connectivity to the new process environment. This test should focus on validating the following interaction patterns based on your usage:

- OCI Process Automation - Processes to Oracle Integration Generation 2 - Integrations
- Oracle Integration Generation 2 - Integrations to OCI Process Automation - Processes
- Visual Builder - Applications to OCI Process Automation - Processes

Phase 2: Switch to OCI Process Automation

Perform the following tasks to switch to OCI Process Automation:

1. Promote Process Applications to Production
2. Perform Switchover to OCI Process Automation
3. Coexistence Period

Promote Process Applications to Production

Move the OCI Process Automation applications to user acceptance and production instances.

Decide how many instances you want to use to promote your changes to production. Map each selected Oracle Integration Generation 2 instance to a new OCI Process Automation instance. For each instance, complete the following steps.

> **Note:**
>
> These steps are similar to the ones you performed during Phase 1: Migrate Process Applications to OCI Process Automation. The main difference is that you should follow the your standard workflow for promoting code to production.

1. Provision a new OCI Process Automation standalone instance.
   This instance will act as a higher-environment, that is user acceptance or production. See Provision a Process Automation Instance in *Administering Oracle Cloud Infrastructure Process Automation*.
2. Register with the corresponding user acceptance or production Oracle Integration Generation 2 instance. See Register Services in *Using Oracle Cloud Infrastructure Process Automation*.
3. Export the OCI Process Automation applications that were activated and tested as part of Phase 1: Migrate Process Applications to OCI Process Automation.
   You can perform the export from the user interface or a REST API. See Export an Application in *Using Oracle Cloud Infrastructure Process Automation* or *REST API for Oracle Cloud Infrastructure Process Automation*.
4. If you have integrations or Visual Builder applications calling process:
   - Export the Oracle Integration Generation 2 integrations that were updated to call OCI Process Automation. See Import and Export Integrations in *Using Integrations in Oracle Integration Generation 2*.

- Export the Visual Builder applications that were updated to call OCI Process Automation. See Export a Visual Application in *Developing Applications with Oracle Visual Builder*.

5. If you have integrations or Visual Builder applications calling process:
   - Promote the exported integrations into your higher user acceptance or production Oracle Integration Generation 2 environment. See Import and Export Integrations in *Using Integrations in Oracle Integration Generation 2*.
   - Promote exported Visual Builder applications into your higher user acceptance or production Oracle Integration Generation 2 environment. See Import a Visual Application in *Developing Applications with Oracle Visual Builder*.
6. Import process application in into the higher user acceptance or production OCI Process Automation instance. You can perform the import in the user interface or a REST API. See Register Services in *Using Oracle Cloud Infrastructure Process Automation* or *REST API for Oracle Cloud Infrastructure Process Automation*.
7. Configure your process applications:
   a. Update the credentials and base URL of any REST Connections. See Configure REST Connectors in Designer in *Using Oracle Cloud Infrastructure Process Automation*.
   b. Update role members, assigning the right users and groups to the appropriate application roles in the new environment.
   c. Activate your process applications. See Activate Applications in *Using Oracle Cloud Infrastructure Process Automation*.
8. Update any clients to connect to the higher user acceptance or production OCI Process Automation instance.
   - For Oracle Integration, update REST Connector to point to the new process instance.
   - For Visual Builder, create a new backend for the new process instance.
9. Perform system integration testing.

Perform Switchover to OCI Process Automation

Perform the following steps:

1. Activate and deploy client changes to ensure that all new system-driven requests are sent to OCI Process Automation as previously described.
2. Communicate the new OCI Process Automation Workspace URL with users and ensure that users:
   - Bookmark the OCI Process Automation workspace.
   - Create new processes *only* in OCI Process Automation.
   - Complete their new tasks in OCI Process Automation.
3. Retire the Oracle Integration Generation 2 applications so that no new processes can be created but the existing ones are allowed to complete. See Manage Active Applications in *Using Processes in Oracle Integration 2*.

> **Important:**
>
> From this point onwards, OCI Process Automation should handle all new requests.

Coexistence Period

When OCI Process Automation starts serving new transactions in production, you'll likely enter what is known as a *coexistence period*.

During this time:

- New process instances will be served by OCI Process Automation.
- Existing process instances will continue to run on Oracle Integration Generation 2 Process until they complete.

> **Note:**
>
> During the coexistence period users must perform tasks assigned to them in both OCI Process Automation and Oracle Integration Generation 2.

During this period process users should:

- Work primarily from the OCI Process Automation Workspace.
- Occasionally check the Oracle Integration Generation 2 My Tasks List.
- Rely on email-based approvals as much as possible, as the links in the emails will take them to the right place to perform the task.

The coexistence period lasts until all transactions created on Oracle Integration Generation 2 are complete. You should actively seek to shorten the duration of this period as much as possible. Here are some guidelines:

- Prevent the creation of new transactions on Oracle Integration Generation 2 by using the Retire functionality. This is applicable to all structured processes that don't contain receive activities. The retire functionality prevents the creation of new instances but also allows existing transactions to complete. See Manage Active Applications in *Using Processes in Oracle Integration 2*.
- Aim to actively expedite the completion of Oracle Integration Generation 2 instances as much as possible by following up with users to take action that sees them through to completion.
- For very long-running process, instances that can't be completed in several months, explore the following options:
  - Recreate the instance in OCI Process Automation and use the Alter Flow functionality to update the payload and move the process instance to the current action (where it is currently in Oracle Integration Generation 2 Process). After this is done, the existing Oracle Integration Generation 2 instance can be terminated. See Alter the Flow of a Process in *Using Oracle Cloud Infrastructure Process Automation*.
- Modify the migrated application so that it can be initiated using the latest state of the existing Oracle Integration Generation 2 process instance.

You can track the remaining Oracle Integration Generation 2 process transactions by clicking **My Tasks**, then choosing **Processes** in your Oracle Integration Generation 2 instance. You must sign in with a user who has the Service Administrator Role.

Phase 3: Upgrade to Oracle Integration 3

Perform the following tasks to upgrade to Oracle Integration 3:

1. Prepare for Upgrade
2. Complete Post-Upgrade Tasks for Process Automation

Prepare for Upgrade

Perform the following tasks to prepare for upgrade:

1. Correct all precheck issues before upgrade.
   The Process Automation precheck looks for any active process instances. This precheck may fail for a couple of reasons:
   - You have active process instances in Oracle Integration Generation 2. To see the active process instances, click **My Tasks**, then choose **Processes**. You must be signed in with a user that has the Service Administrator role to be able to see all process instances.
   - You've had active process instances in the past 30 days. Oracle allows an grace period of 30 days to ensure you have an opportunity to save and export your data from Oracle Integration Generation 2 Process. So, even if all runtime transactions are completed on your Oracle Integration Generation 2 instance and you've fully transitioned to OCI Process Automation, this precheck may fail.

   If the Process Automation precheck is failing, decide what to do:
   - If you have active process instances that you want to complete before upgrade, leave **Ignore active instances** unselected.
   - If all your active process instances are complete or you don't need them to complete, select **Ignore active instances**.
2. Select **Attach an OCI Process Automation instance** and supply the OCI Process Automation OCID. This option will attach your existing OCI Process Automation instance to your Oracle Integration 3 instance during upgrade. You must meet the following prerequisites:
   - The OCI Process Automation instance must be in the same region, tenancy, and compartment as the Oracle Integration instance.
   - The OCI Process Automation instance and the Oracle Integration Generation 2 instance must share the same identity domain.

   When your instance has passed all prechecks, Oracle sends you an email with your scheduled upgrade window. See View Your Upgrade Window.
3. Complete any other preparations you haven't already done. See Prepare for the Upgrade to Oracle Integration 3.
4. Save runtime data from Oracle Integration Generation 2 Process. This step is important to ensure that you don't lose the history of completed transactions. You must do this *before* upgrade. See Archiving and Purging Process Automation Data in Oracle Integration.
   As part of these steps, you'll configure the Oracle Storage Service and schedule instances for archive and purge. Be aware of the following points:
   - The archived information will be available in the configured Object Storage bucket.
   - Attachments aren't included in the archive files. You must export these manually. See Retrieve a Process Attachment as a Stream in *REST API for Oracle Integration 2*.

Complete Post-Upgrade Tasks for Process Automation

Complete the post-upgrade tasks 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.

As noted, you don't need to complete the post-upgrade tasks for Process Automation as those are for a different upgrade path.

> **Note:**
>
> Your existing service registration will continue to work for your upgraded Oracle Integration 3 instance, ensuring continued connectivity to integrations that you're already calling from your process applications.

Clean Up Legacy Client Code

If you still have integrations or Visual Builder applications that were used to communicate to Oracle Integration Generation 2, use this opportunity to clean them up.

Changes You'll See After Upgrade

After upgrade is complete, you'll see the following changes:

- In the Oracle Integration navigation menu, you'll see a **Process** option.
- In Oracle Cloud Infrastructure Console, when you view the Oracle Integration instance, you'll see that Process Automation is enabled.
- Process usage is metered under Oracle Integration.

What to Do During Upgrade

What can you expect during the upgrade? The upgrade generally take less than ten minutes, but may take longer if you have a lot of files or a complex setup. During this time, Oracle Integration Generation 2 is unavailable.

> **Note:**
>
> Prior to the upgrade, pause development work if you can. See Limit Development Work Before the Upgrade.

Here's what you need to do on the day of 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. By default, upgrade notifications are automatically sent to the specified administrator email. Oracle recommends you have notifications sent to a distribution list or group email so that you don't miss important emails if someone leaves the company. You set who receives notifications on the **Upgrade** page. See "Upgrade Notifications" in Configure Your Upgrade Settings.
3. **Wait for the upgrade to complete:** If you sign in during the downtime, a maintenance page indicates 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 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. You can schedule your upgrade for another time, and Oracle works with you to determine the next steps.

5. After you get the email saying the upgrade is complete, complete the post-upgrade tasks.

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.

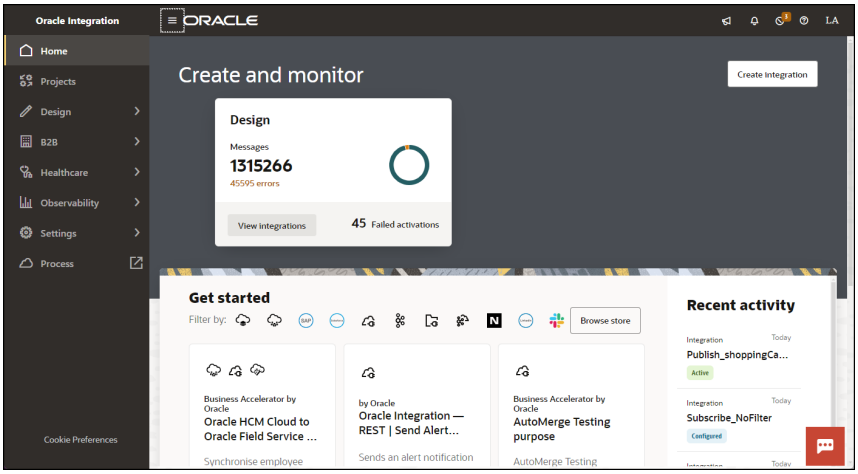
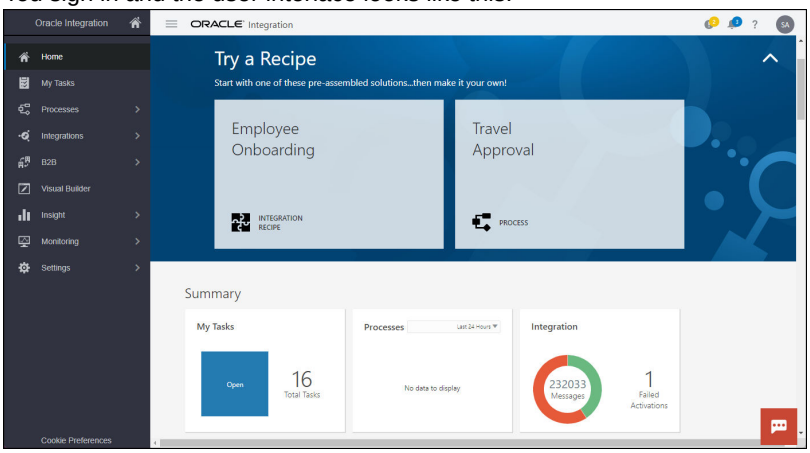
Make sure the upgrade has completed before starting these tasks. See What to Do During Upgrade.

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. Get the URL for the new instance and share it
Ensure connectivity	Immediately after upgrade	1. Complete network rules configuration 2. Upload new identity certificates for connections 3. Regain connectivity with agents that weren't upgraded 4. File Server: add the File Server IP address to your internal firewall allowlist Complete this task within one week after upgrade. 5. File Server: update integrations and SFTP clients to use the new IP and port values Complete this task within one week after upgrade.
Ensure integrations work	Immediately after upgrade	1. Change Oracle Integration built-in API calls from Basic Authentication to OAuth 2. Check integrations if you selected Ignore activation failures or Ignore start schedule failures 3. Take care of any requests that were rejected during the upgrade downtime
Complete post-upgrade tasks for ignored precheck failures	Immediately after upgrade	Complete Post-Upgrade Tasks for Ignored Precheck Failures
Complete Visual Builder post-upgrade tasks	Immediately after upgrade	Complete Post-Upgrade Tasks for Visual Builder

Impact	When	Tasks to complete
Complete Process Automation post-upgrade tasks	Immediately after upgrade	Complete Post-Upgrade Tasks for Process Automation
Complete post-upgrade verification	Within two weeks of upgrade	Follow Your Organization's Verification Procedures

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. 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 the interface looks like this:  The upgrade is still in progress if: • You sign in and a page indicates that the service is unavailable. • You sign in and the user interface looks like this: 

Task	Who	When	Tasks to complete
Update the IAM policy with the new OCID	IAM policy administrator	Immediately after upgrade	If your organization restricted access to the Oracle Integration Generation 2 instance based on the instance's Oracle Cloud ID (OCID), update the IAM policy to point to the new Oracle Integration 3 instance OCID. **Caution:** Users won't be able to sign in to Oracle Integration 3 until you update the OCID in the IAM policy. 1. Sign in to Oracle Cloud Infrastructure Console. 2. Get the new OCID value for the Oracle Integration 3 instance. See Viewing Instance Details. 3. Update the OCID in your IAM policy. For instructions on updating the statements in an existing policy, see Using the Console in the Oracle Cloud Infrastructure documentation.
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. This is in the following format: `https://design.integration.`*`region`*`.ocp.oraclecloud.com/?integrationInstance=`*`query_parameter_repersenting_instance`* To get the new URL: 1. Sign in to the Oracle Cloud Infrastructure Console. 2. Open the navigation menu and click **Developer Services**. 3. Under **Application Integration**, click **Integration**. 4. Click the name of the new Oracle Integration 3 instance. 5. To the right of the **Service console URL** field, click **Copy**. 6. Share the URL with anyone who needs it.

Ensure Connectivity

Task	Who	When	Tasks to complete
Complete network rules configuration	Network administrator	Prior to upgrade or immediately after upgrade	If any of your integration connections target an Oracle Cloud Infrastructure service that supports network rules, such as Oracle Cloud Infrastructure Object Storage or Oracle Autonomous Database, and you've enabled those rules, you must complete any network rules configuration, including adding the Oracle Integration Service VCN to the rule. 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. For example, for Oracle Autonomous Database Serverless, see 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're accessing is in a different region than your Oracle Integration instance, allowlist the **OIC Outbound IP** address you collected when you updated your other allowlists prior to upgrade.
Upload new identity certificates for connections	Developer with connections that use identity certificates Only one person from your organization needs to perform these steps	Immediately after upgrade	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 your instance includes connections that use identity certificates, perform the following steps: 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 weren't reachable during upgrade or didn't meet upgrade requirements weren't 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 Oracle Identity Cloud Service (IDCS) and Oracle Integration 3:
			• You should have added the IDCS and Oracle Integration 3 IP addresses and URLs to your allowlists prior to upgrade, as described in Update Allowlists.
			• Add the Oracle Integration 3 design-time IP address to your 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 manually upgrade your agents and regain connectivity with them:
			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: add the File Server IP address to your internal firewall allowlist	File Server administrator and developer	Within one week of upgrade	If your organization restricts the sites that internal resources can access, add the new File Server IP address to your internal firewall allowlist. The Oracle Integration Generation 2 IP address continues working for four months after the upgrade, and then Oracle retires them. However, Oracle recommends updating your firewall allowlist to use the new IP address now. That way, you don't risk forgetting to update the allowlist in the future. To get the File Server IP address: 1. Sign in to Oracle Integration 3. 2. In the navigation pane, click **Settings**, then **File Server**, then **Settings**. 3. Under General, obtain the IP address for the File Server SFTP server.
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. Sign in to Oracle Integration 3. 2. In the navigation pane, click **Settings**, then **File Server**, then **Settings**. 3. Under General, obtain the IP and port values for the File Server SFTP server. 4. Update all integrations that call File Server so that they use the new IP and port values. 5. Update all SFTP clients so that they use the new IP and port values.

Ensure Integrations Work

Task	Who	When	Details
Change Oracle Integration built-in API calls from Basic Authentication to OAuth	Developer	Prior to upgrade or immediately after upgrade	If you didn't already update your API calls to use OAuth while completing prerequisites or pre-upgrade tasks, do so immediately after upgrade. In Oracle Integration Generation 2, you could use Basic Authentication to use the Oracle Integration REST API and File Server REST API. In Oracle Integration 3, you must use OAuth. You 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 details on using OAuth with the Oracle Integration REST API, see Security, Authentication, and Authorization, or with the File Server REST API, see Security, Authentication, and Authorization.
Check integrations if you selected **Ignore activation failures** or **Ignore start schedule failures**	Administrator	Immediately after upgrade	If you configured your upgrade settings 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.
Take care of any requests that were rejected during the upgrade downtime	Designated team members	Immediately after upgrade	Oracle Integration rejected all requests that were sent during the upgrade downtime. If needed, take action on requests that any clients sent to Oracle Integration during the downtime.

Complete Post-Upgrade Tasks for Ignored Precheck Failures

If you selected to ignore precheck failures, perform the steps associated with any failed prechecks:

Precheck	Connection tasks	Integration tasks	Other tasks
Delayed (Asynchronous) Response		After upgrade, you must rework or recreate integrations that used delayed (asynchronous) response with one of the following adapters: • Oracle CX Sales and B2B Service Adapter • Oracle ERP Cloud Adapter • Oracle HCM Cloud Adapter • Oracle Field Service Cloud Adapter • Salesforce Adapter • ServiceNow Adapter **Application-driven integrations:** Application-driven integrations are changed to a draft state during upgrade. You must rework those integrations using the following steps: 1. Create a simple invoke for success callbacks. 2. Create an additional invoke for failure callbacks under the fault handler to catch the correct fault. 3. Recreate your data mappings. **Basic routing integrations:** Basic routing integrations aren't supported in Oracle Integration 3 and will show a blank canvas. You must delete those integrations and recreate them as application-driven integrations.	
Unsupported Adapters	During upgrade, connections that used the following unsupported adapters were deleted: • 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 You must create REST Adapter connections to replace the deleted unsupported adapter connections.	During upgrade, integrations that used unsupported adapters are changed to a draft state and any scheduled runs are canceled. You must rework those integrations using the following steps: 1. Delete the invoke corresponding to the unsupported adapter connection and replace it with the new REST Adapter connection. 2. After the integration is configured and activated,start the schedule.	

Precheck	Connection tasks	Integration tasks	Other tasks
Custom Adapters	During upgrade, connections that used the custom adapters were deleted. You must create new connections using equivalent Oracle Integration 3 adapters to replace the deleted custom adapter connections.	During upgrade, integrations that used unsupported adapters are changed to a draft state and any scheduled runs are canceled. You must rework those integrations using the following steps: 1. Delete the invoke corresponding to the custom adapter connection and replace it with the new connection you created. 2. After the integration is configured and activated, start the schedule.	
Multiple Read File		During upgrade, integrations that used the Read Multiple File operation are changed to a draft state. You must rework those 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.	

Precheck	Connection tasks	Integration tasks	Other tasks
Unsupported REST Types	During upgrade, connections that used the following unsupported REST types were changed to a draft state. • Metadata Catalog URL • Swagger Definition URL • RAML Definition URL You must update those connections using one of the following methods: • If you were using RAML or the Oracle metadata catalog, you can ask your REST service provider for a Swagger definition (if available). Oracle Fusion Applications should have a Swagger option available as this is a guideline for all Oracle Fusion Applications. 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 if you were using RAML, is to convert RAML into an OpenAPI specification. • If you were using the Swagger definition URL, you can use the REST Adapter's new unified option to specify all OpenAPI specifications in a single field. This option provides more robust and complete support for the Swagger/OpenAPI specifications. See Configure Connection Properties for Invoke Connections in *Using the REST Adapter with Oracle Integration 3*.	During upgrade, integrations that used unsupported REST types were changed to a draft state and any scheduled runs were canceled. You must rework those integrations using the following steps: 1. Activate the integration 2. After the integration is activated, start the schedule.	
Basic Routing Duplicate App Name		Basic routing integrations aren't supported in Oracle Integration 3 and will show a blank canvas. You must delete those integrations and recreate them as application-driven integrations.	

Precheck	Connection tasks	Integration tasks	Other tasks
Publish/Subscribe Integrations		Integrations that published messages or subscribed to messages from Oracle Integration, must be converted to event-driven orchestrations. You must delete the integrations and recreate them based on the precheck instructions for Publish/Subscribe Integrations.	
Custom Endpoint URL			Your custom endpoint wasn't migrated during upgrade. You must recreate your custom endpoint.

Complete Post-Upgrade Tasks for Visual Builder

To complete migration, perform the following steps:

Task	Who	When	Tasks description
Update DNS record for custom endpoint	Administrator	Immediately after upgrade	If you're using Visual Builder and you have a custom endpoint or alternate custom endpoints, update the custom endpoint DNS record's CNAME with the Visual Builder instance host name.

Task	Who	When	Tasks description
Complete additional post-upgrade tasks	Development Operations team	Immediately after the upgrade	Complete the tasks described in Tasks to Complete After the Upgrade in *Administering Oracle Visual Builder in Oracle Integration 3*.

Complete Post-Upgrade Tasks for Process Automation

Perform the following steps to complete migration to Process Automation in Oracle Integration 3.

> **Note:**
>
> If you performed a manual migration of actively-used process applications, you don't need to perform these post-upgrade tasks.

Application-Level Post-Upgrade Tasks for Process Automation

Perform the following tasks for each Process application.

Task	Who	When	Details
Update role mappings	Developer/ Administrator	Immediately after upgrade	Role assignments have changed in Oracle Integration 3, so you must map your existing roles to the new roles. See Configure Roles for Process Applications in *Using Oracle Cloud Infrastructure Process Automation*. **Process owners** Add members who had the following roles to the **Process Owner** role in the new application: • `<application-name>.ProcessOwner` • `<application-name>.AnalyticsViewer` • `auto-handler for the swim-lane` **Process reviewers** Add members who had the `<application-name>.ProcessReviewer` role to the **Process Reviewer** role in the new application. **Members with swimlane roles** Add members who had a `swim-lane` role to the role assigned to the swimlane in the new application. **Groups** Change the old group to a role in the new application, and either add the group to the new role or add the members of the group to the new role. **Roles** Change the old role to a role in the new application, and add members to the new role. **Members who can start a process** In the process start properties, select the members who can start the process from one of the following options: • **Role members with at least Use permission**: Allows any user assigned a role with Use or Manage permission to see and start the application. Note that in a structured process, a user does not need to be assigned to the swimlane to start the process. • **All users and external applications**: Allows any user or external application with access to Process Automation to see and start the application. **Dynamic process roles** Add members who had dynamic process roles to the dynamic process roles in the new application.
Update connector credentials	Developer/ Administrator	Immediately after upgrade	Credentials aren't migration to Oracle Integration 3, so you must reconfigure authentication for your REST connectors. If there are multiple applications connecting to the same server you may want to create a global credential that can then be reused across applications. See Configure Basic Auth Security in *Using Oracle Cloud Infrastructure Process Automation*.
Fix any errors and warnings	Developer/ Administrator	Immediately after upgrade	Because there are differences in process features between Oracle Integration Generation 2 and Oracle Integration 3, you'll need to validate your application and fix any errors or warnings. See "How are applications validated?" in Applications at a Glance in *Using Oracle Cloud Infrastructure Process Automation*.
Activate application	Developer/ Administrator	Immediately after upgrade	After you've resolved all validation errors, activate your application so new instances can be triggered and worked on. See Activate Applications in *Using Oracle Cloud Infrastructure Process Automation*.

Access Mapping Post-Upgrade Tasks for Process Automation

Some access mapping tasks are completed automatically during upgrade and some are your responsibility.

During upgrade, a new Oracle Identity Cloud Service (IDCS) App is added to help with mapping.

The following IDCS roles are automatically mapped from Oracle Integration Generation 2 to Oracle Integration 3 during upgrade.

Oracle Integration Generation 2	Oracle Integration 3
ServiceDeveloper	ServiceDeveloper
ServiceAdministrator	ServiceAdministrator
ServiceUser	N/A
ServiceMonitor	N/A
ServiceDeployer	ServiceDeployer
ServiceViewer	N/A
ServiceInvoker	N/A
ServiceEndUser	N/A

Service-Level Post-Upgrade Tasks for Process Automation

Depending on how you use Process, you'll perform different service-level steps after upgrade to Oracle Integration 3. Perform any steps that apply to your implementation.

Task	Who	When	Details
Allowlist the new Process Automation URL	Developer	Immediately after upgrade	Add the new Process Automation URL to your allowlists. To find the new URL, click **Process** in the Oracle Integration 3 menu. You'll be redirected to the Process Automation URL.
Update integrations to call Process Automation	Developer	Immediately after upgrade	Process APIs and endpoints have changed after the upgrade. As a result, you must update any integrations that use the Process action to use the REST adapter instead. See *REST API for Oracle Cloud Infrastructure Process Automation*.
Update Visual Builder applications to call Process Automation	Developer	Immediately after upgrade	Process APIs and endpoints have changed after the upgrade. As a result, you must update any Visual Builder application that calls Process, replacing any deprecated interaction patterns. See Connect to Oracle Process Automation APIs in *Building Responsive Applications with Visual Builder Studio*.
Update external clients to call Process Automation	Developer	Immediately after upgrade	If you're using Process CCA components in external applications, they won't work after the upgrade to Oracle Integration 3. You must transition to using the new Process Automation CCA components to leverage the APIs. See *REST API for Oracle Cloud Infrastructure Process Automation*.
Share the new Process Automation URL	Administrator	Immediately after upgrade	The URL used to access and interact with Process Automation has changed after the upgrade. Share the new URL with anyone who needs to administer Process Automation, start a new process, or view and act on their tasks.

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. Perform integration load testing in a development/stage instance before moving integrations to a production instance.

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.

> **Important:**
>
> Your instance will be rolled back to Oracle Integration Generation 2 in the same state it was when upgrade was performed. Any changes you made in the upgraded environment won't be reflected in the Oracle Integration Generation 2 environment if you roll back.

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 could use Basic Authentication to use the Oracle Integration REST API and File Server REST API. In Oracle Integration 3, you must use OAuth. You 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 details on using OAuth with the Oracle Integration REST API, see Security, Authentication, and Authorization, or with the File Server 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.

Known issues

You might run into other errors that are due to known issues.

- Common Issues
- Integrations Issues
- Process Automation Issues
- File Server Issues
- Visual Builder Issues

A

Oracle Integration 3 Reference

Topics:

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?

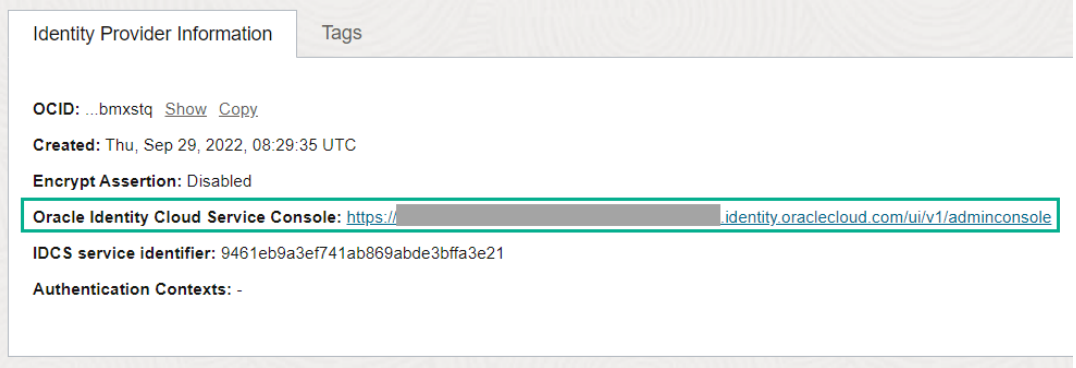
Oracle Integration requires that Oracle Cloud Infrastructure Identity and Access Management (IAM) be federated with Oracle Identity Cloud Service (IDCS) for your tenancy.

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

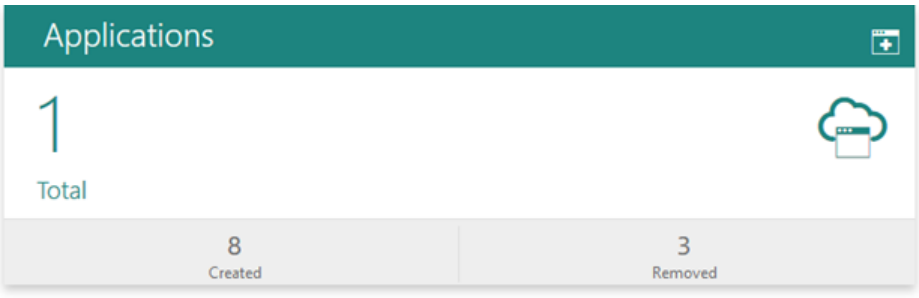
Follow these steps to create and configure an Oracle Identity Cloud Service application, activate the application, and create an IDCS administrator group.

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

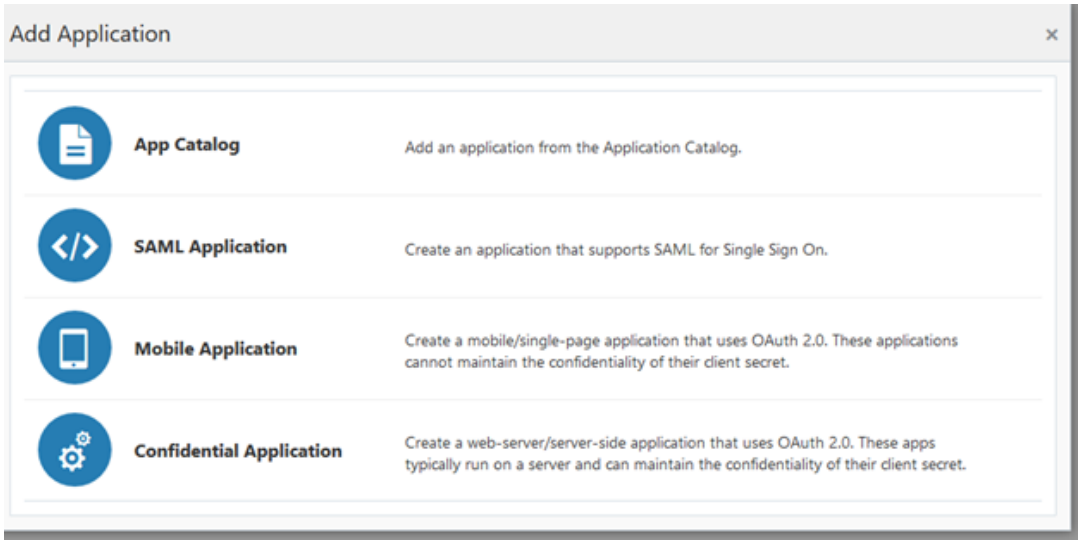
> **Note:**
>
> Follow the steps in this section only if manual federation is needed.

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**.

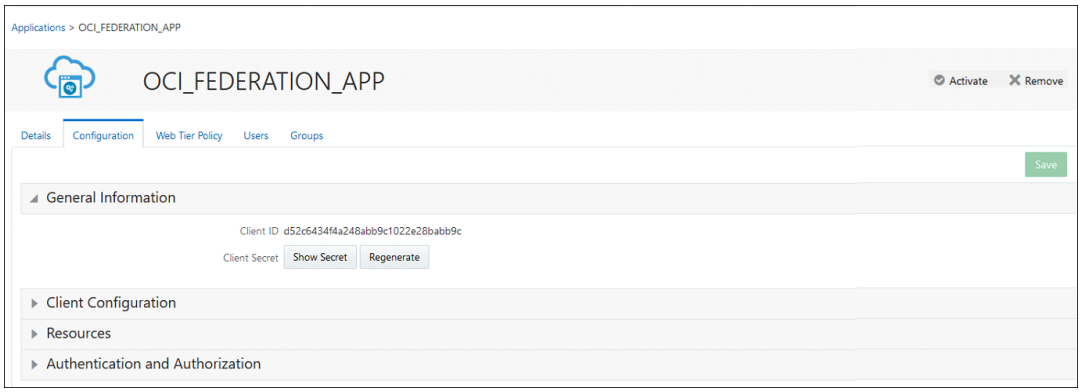


The Add Confidential Application page is displayed.

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	No	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

Robots

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
View	Yes	Yes	Yes	Yes	No	Yes
Create	Yes	Yes	No	No	No	No
Update	Yes	Yes	No	No	No	No
Delete	Yes	Yes	No	No	No	No
Activate	Yes	Yes	No	No	No	No
Deactivate	Yes	Yes	No	No	No	No
Run	Yes	Yes	No	Yes	Yes	No

Environments and environment pools

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
View environments	Yes	Yes	Yes	Yes	No	Yes
Create environments	No	No	No	No	No	No
Update environments	Yes	Yes	No	No	No	No
Delete environments	Yes	Yes	No	No	No	No
View environment pools	Yes	Yes	Yes	Yes	No	Yes
Create environment pools	Yes	Yes	No	No	No	No
Update environment pools	Yes	Yes	No	No	No	No
Delete environment pools	Yes	Yes	No	No	No	No
Add environments to environment pools	Yes	Yes	No	No	No	No
Remove environments from environment pools	Yes	Yes	No	No	No	No

Robot connection types

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
View	Yes	Yes	Yes	Yes	No	Yes
Create	Yes	Yes	No	No	No	No
Update	Yes	Yes	No	No	No	No
Delete	Yes	Yes	No	No	No	No

Robot connections

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
View a robot connection	Yes	Yes	Yes	Yes	No	Yes

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
Create	Yes	Yes	No	No	No	No
Update	Yes	Yes	No	No	No	No
Delete	Yes	Yes	No	No	No	No
View the contents of a robot connection	Yes	Yes	No	No	No	No

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
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

Action	Service Administrator	ServiceDeveloper	ServiceMonitor	ServiceUser	ServiceInvoker	ServiceViewer
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.

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 or File server action 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.
• ServiceMonitor • ServiceDeployer • ServiceInvoker • ServiceViewer	These roles do not have any privileges in File Server.

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
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)
Track B2B messages	Yes	Yes	Yes	Yes (Can view message details and download payloads only)	Yes (Can view message details and download payloads only)