

Oracle® Cloud

Securing Oracle Integration 3



F83200-07
February 2026



Oracle Cloud Securing Oracle Integration 3,

F83200-07

Copyright © 2024, 2026, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

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

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

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

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

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

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

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

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

Contents

About This Content

1 Overview of Oracle Integration Security

About This Guide	1
Key Concepts for Oracle Integration Security	1
Oracle's Security Responsibilities	5
Additional Resources	7

2 Access Control

Learn About Users and Resources	1
Big Picture: Resources, Managers, and Users	1
Resources	2
Managers of the Resources	5
Users of the Resources	7
Explore the Oracle Integration APIs	8
Oracle Integration APIs	8
Process Automation APIs	10
File Server APIs	10
Control Network Access	11
Types of Traffic	11
Control Inbound Network Access	13
Control Outbound Network Access	15
Transport Layer Security for Inbound Traffic	18
Transport Layer Security for Outbound Traffic	18
Control User, Client System, and Connection Access	19
Oracle Integration Instance User Interface: Control User Access	19
Developer APIs: Control User and Client System Access	21
Projects: Control User Access	23
File Server: Control User and Client System Access	25
Target Systems: Control Connection Access	27

3 Data Protection

Credential Handling	1
Data Visibility	2

About This Content

This guide describes how to configure security for Oracle Integration.

Audience

This guide is intended for security professionals who are responsible for securing Oracle Integration.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Related Resources

See these Oracle resources:

- Oracle Integration documentation on the Oracle Help Center.

Conventions

The following text conventions are used in this document.

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

1

Overview of Oracle Integration Security

In today's world, the security of cloud resources is a top priority. To understand how to protect your cloud resources, including your Oracle Integration instance and its data, you must understand multiple themes related to security.

This guide helps you understand the themes and how they apply to protecting an Oracle Integration instance. This guide also provides information about protecting the resources and data associated with the instance.

Topics:

- [About This Guide](#)
- [Key Concepts for Oracle Integration Security](#)
- [Oracle's Security Responsibilities](#)
- [Additional Resources](#)

About This Guide

This guide explains your responsibilities for controlling access and protecting data. Understand these concepts at a high level before you explore all the details.

This guide introduces key security concepts and explains your responsibilities for securing Oracle Integration. Step-by-step instructions for your security responsibilities are available in other guides. This guide includes links to the relevant sections of these guides.

Key Concepts for Oracle Integration Security

Understand the key security concepts for Oracle Integration, including the services where you control access, the different types of network traffic, the ways that you control network traffic, and more.

Services for Controlling Access

You restrict the users and resources that access Oracle Integration in different ways using the following services.

Service	Usage
Oracle Integration	<p>All organizations that use Oracle Integration have one or more Oracle Integration instances. Within these instances, users with administrator-level service roles control access to:</p> <ul style="list-style-type: none"> • Projects • File Server • Target systems that integrations connect to <p>Users access an instance using its user interface or its developer APIs. See:</p> <ul style="list-style-type: none"> • Developer API for Oracle Integration 3 • Developer API for Oracle Cloud Infrastructure Process Automation • Developer API for File Server in Oracle Integration 3
Oracle Cloud Console	<p>All organizations that use Oracle Integration have access to the Oracle Cloud Console. Here, users with the appropriate IAM (identity and access management) policies perform the following tasks:</p> <ul style="list-style-type: none"> • Create and manage users, and control access to the Oracle Integration instance and its APIs. <p>Perform these tasks in Oracle Cloud Infrastructure Identity and Access Management, which is available within the Oracle Cloud Console.</p> <p>Alternatively, if your organization already has an identity and access management tool, you can federate Oracle Cloud Infrastructure IAM with this tool. See Federating with Identity Providers in the Oracle Cloud Infrastructure documentation.</p> <ul style="list-style-type: none"> • Manage the lifecycle of the Oracle Integration instance. <p>Users access the Oracle Cloud Console from the following:</p> <ul style="list-style-type: none"> • Its user interface • Its APIs: See Oracle Integration Administrative API. <p>These APIs are different from the Oracle Integration developer APIs, described in the previous row.</p> <ul style="list-style-type: none"> • Its CLI: See Oracle Integration CLI.

To learn more, see [Learn About Users and Resources](#).

Main Sections of This Guide

This guide presents the following information.

Area	Description
Access control	<p>Access control focuses on two areas:</p> <ul style="list-style-type: none"> • Network access Controlling network access involves routing and restricting the following traffic: <ul style="list-style-type: none"> – Inbound traffic to an Oracle Integration instance and other resources. You can restrict the IP addresses that can send inbound traffic. – Outbound traffic from an Oracle Integration instance. Outbound traffic is routed through different channels, depending on the location of the service that receives the traffic. <p>See Control Network Access.</p> <ul style="list-style-type: none"> • User, client system, and connection access Users, client systems, and connections require access to some or all of the following resources: <ul style="list-style-type: none"> – Oracle Integration instance: The service instance where you design, deploy, and monitor integrations. – Oracle Integration APIs and endpoints: The Developer API for Oracle Integration 3 and the integration endpoints for the Oracle Integration instance. – Projects: Containers for organizing resources in an Oracle Integration instance. – File Server: Embedded SFTP server for an Oracle Integration instance. – Target systems: Application or service that an integration connects to. – Oracle Cloud Infrastructure services: Any service that you access and manage from the Oracle Cloud Console, the Oracle Integration Administrative API, or the Oracle Integration Administrative CLI. <p>You control access to resources through <i>authentication</i>, and you control the activities that can be performed through <i>authorization</i>.</p> <p>See Learn About Users and Resources and Control User, Client System, and Connection Access.</p>
Data protection	<p>Learn how to ensure that only authorized people can view data, and understand how to handle credentials appropriately.</p> <ul style="list-style-type: none"> • Users access the Oracle Integration instance using their credentials. Follow the guidance for secure credential handling. See Credential Handling. • Sensitive data might include design-time and runtime auditing data and tracking data. You protect the visibility of this data in the Oracle Integration instance using role authorization. See Data Visibility.

Inbound and Outbound Network Traffic

To control network access, first familiarize yourself with the types of traffic to manage.

- Inbound traffic, also called ingress traffic, originates *outside* Oracle Integration and goes to:
 - An Oracle Integration instance
 - The Oracle Integration APIs, including the Developer API for Oracle Integration 3 and integration endpoints

- File Server
- Outbound traffic, also called egress traffic, originates *in an Oracle Integration instance* and goes to:
 - A target system

To learn more, see [Control Network Access](#).

Allowlists

Network access control for Oracle Integration is primarily oriented around restricting inbound traffic. To secure Oracle Integration, you must limit the IP addresses that can access an Oracle Integration instance and its related resources. Use an allowlist, also known as an access control list (ACL) or a whitelist, to restrict this traffic. An allowlist identifies trustworthy IP addresses, Classless Inter-Domain Routing (CIDR) block ranges, and Oracle-assigned unique IDs called VCN OCIDs (virtual cloud network Oracle Cloud Identifiers).

This guide refers to the following allowlists:

- Allowlist for Oracle Integration
- Allowlist for File Server
- Allowlists for the target applications for which allowlists are enabled

To learn more, see [Control Network Access](#).

Authentication and Authorization

Users and applications require access to resources. Authentication and authorization ensure that only the allowed users and applications gain access and can perform only their required tasks after they gain access.

- Authentication is the process of verifying the user or application that attempts to gain access.
- Authorization is the process that a resource uses to determine whether a user or application has access to specific activities or objects within the resource.

Oracle Integration and its related resources use various methods for authenticating and authorizing users. To learn more, see [Learn About Users and Resources](#) and [Control User, Client System, and Connection Access](#).

Encryption

Encryption is the process of protecting information or data by scrambling it. Oracle Integration provides the following options for encryption:

- **Wire encryption**

All inbound traffic is protected by either TLS or SFTP, which are used for secure encrypted transport. See [Oracle's Security Responsibilities](#).
- **Data encryption**

All Oracle Cloud Infrastructure services, including Oracle Integration, encrypt all data at rest.

See [Oracle's Security Responsibilities](#).
- **Encryption during processing**

You can encrypt and decrypt files using the stage file action. See Process Files in Schedule Integrations with a Stage File Action in *Using Integrations in Oracle Integration 3*.

The stage file action works with the following adapters:

- File Adapter

See Upload a Certificate to Connect with External Services in *Using the File Adapter with Oracle Integration 3*.

- FTP Adapter

See Configure a PGP Encryption Decryption Connection in *Using the FTP Adapter with Oracle Integration 3*.

The keys that you use for encryption and decryption are under your control: You load them into Oracle Integration, and you can choose to use them across multiple integrations.

Audit and Logging

Oracle Integration provides a design-time audit, which is a log of design time actions, the people who completed them, and the time they completed them. See [Data Visibility](#).

Oracle's Security Responsibilities

Security in the cloud is a shared responsibility between you and Oracle. In general, Oracle provides security of cloud infrastructure and operations, such as cloud operator access controls and infrastructure security patching.

Oracle is responsible for the following security requirements. Except where noted, these points are not covered in further detail in this guide.

Area	Details
Physical security	Oracle is responsible for protecting the global infrastructure that runs all services offered in Oracle Cloud Infrastructure. This infrastructure consists of the hardware, software, networking, and facilities that run Oracle Cloud Infrastructure services.
Security patching	Oracle conducts security patching monthly to ensure that Oracle Cloud Infrastructure services have up-to-date security patches.

Area	Details
Network security	<ul style="list-style-type: none"> <li data-bbox="643 247 1114 268">• DDoS attack detection and mitigation Oracle Cloud Infrastructure provides automated Distributed Denial of Service (DDoS) attack detection and mitigation of high-volume Layer 3/4 DDoS attacks. Oracle's tools and processes protect against network-based attacks, also known as volume-based attacks. You can enable additional network protection by subscribing to Oracle Web Application Firewall (WAF) service. <li data-bbox="643 457 870 478">• Network access All public traffic is terminated with one of the methods: <ul style="list-style-type: none"> <li data-bbox="691 527 1162 548">– Integration endpoints: TLS 1.2 or higher. <li data-bbox="691 562 1438 642">– Developer API for Oracle Integration 3: As set by the Oracle Cloud Infrastructure regional OpenID Connect (OIDC) proxy, TLS 1.2 or higher. <p data-bbox="691 653 1455 758">You can restrict which networks have access to Oracle Integration instances by configuring an allowlist (formerly known as whitelist). See <i>Restrict Access to an Instance</i> in <i>Provisioning and Administering Oracle Integration 3</i>.</p> <p data-bbox="691 772 1422 793">Allowlists are also covered in this guide. See Control Network Access.</p> <li data-bbox="643 810 878 831">• Private endpoint You can secure outbound traffic to specific resources by using a private endpoint. See <i>Connect to Private Resources</i> in <i>Provisioning and Administering Oracle Integration 3</i>. Private endpoints are also covered in this guide. See Control Network Access.
Data that you provide	Oracle Integration protects and encrypts all data received by using Oracle-managed keys.
Security and vulnerability scanning	Oracle performs security and vulnerability scanning using the Oracle Vulnerability Scanning service. Additionally, a process is available if your organization wants to run a vulnerability scan. See Oracle Cloud Security Testing Policies in the Oracle Cloud Infrastructure Documentation.
Compliance	Oracle Integration has reached compliance for SOC 1, SOC 2, ISO 27001, PCI DSS, and HIPAA. Certification details are available upon request, with some requiring an NDA Master Agreement with Oracle. For publicly available information, see Oracle Cloud Compliance .
Data encryption	<ul style="list-style-type: none"> <li data-bbox="643 1346 1455 1430">• Oracle follows all the guidelines from Oracle Cloud Infrastructure Vault and Oracle Cloud Infrastructure Secrets for rotating the service instance encryption keys. <li data-bbox="643 1440 1195 1461">• Oracle encrypts data at rest and data over wire. <li data-bbox="643 1472 1455 1545">• All inbound traffic is protected by either TLS or SFTP, which are used for secure encrypted transport. The following encryption options are available for inbound traffic: <ul style="list-style-type: none"> <li data-bbox="691 1566 1455 1650">– HTTP over TLS: This encryption option is available for inbound traffic to Oracle Integration and File Server. If you use REST APIs to access either resource, this encryption option is always used. <li data-bbox="691 1661 1455 1703">– SFTP: This encryption option connects to an FTP port directly, without using HTTP, and is available for inbound traffic to File Server.
Data durability	Oracle takes regular backups of your data. Oracle recommends that each organization perform their own backup, as well. See Data Visibility .

Area	Details
Service tenancy durability	Oracle is responsible for the retention of the data in the activity stream. Oracle retains the data for the time period specified by your Oracle Integration edition. See Oracle Integration Editions in <i>Provisioning and Administering Oracle Integration 3</i> . Your organization determines the level of data that is included in the activity stream as well as the retention period. For details, see Data Visibility .
Process isolation and data isolation	Oracle isolates data by service instance. Each service instance stores its data individually.

Additional Resources

Additional resources are available to learn about Oracle Cloud Infrastructure and its security.

New to Oracle Cloud Infrastructure?

If you're a new Oracle Cloud Infrastructure customer, spend some time familiarizing yourself with its components before reading this guide.

See the following resources:

- [Account and Access Concepts](#) in the Oracle Cloud Infrastructure documentation
- [Oracle Cloud Infrastructure Resources and Services](#) in *Establish a foundational Oracle Cloud Infrastructure Governance Model*

Additional Oracle Cloud Infrastructure Security Information

Administrators must manage their organization's applications and assets in Oracle Cloud. Information about this level of access is covered in the following resources:

- [Oracle Cloud Infrastructure Security Guide](#)
- [Oracle Cloud Infrastructure Security Architecture](#)
- [Learn About Security in Oracle Cloud Infrastructure](#) in *Security checklist for Oracle Cloud Infrastructure*

2

Access Control

To control access to Oracle Integration and its related resources, you must control network access and user access, as well as client system access and connection access, where applicable.

Learn

- [Learn About Users and Resources](#)
- [Explore the Oracle Integration APIs](#)

Manage Access

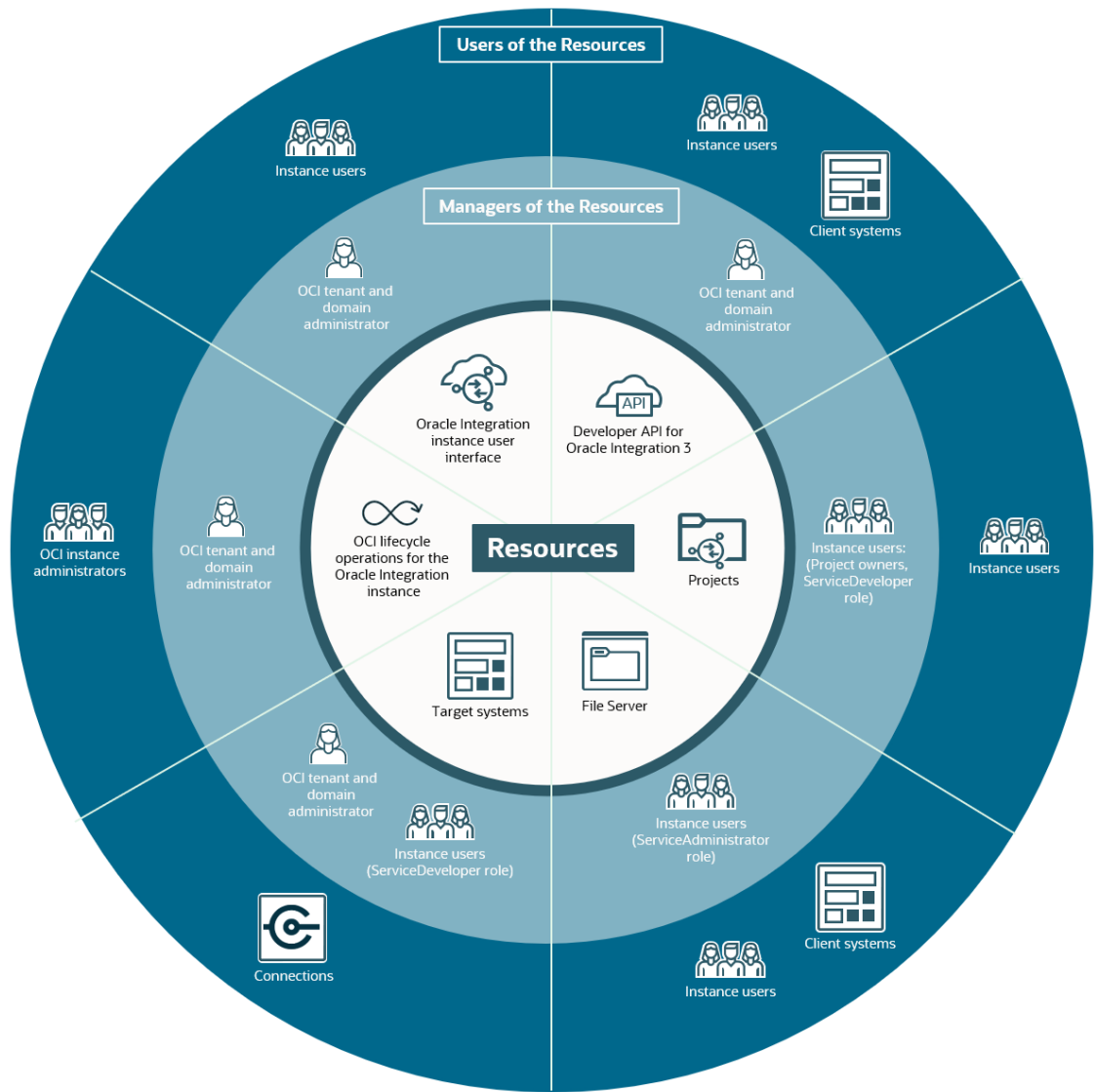
- [Control Network Access](#)
- [Control User, Client System, and Connection Access](#)

Learn About Users and Resources

To understand access control, familiarize yourself with the resources that can require permissions, and the people and resources who require those permissions.

Big Picture: Resources, Managers, and Users

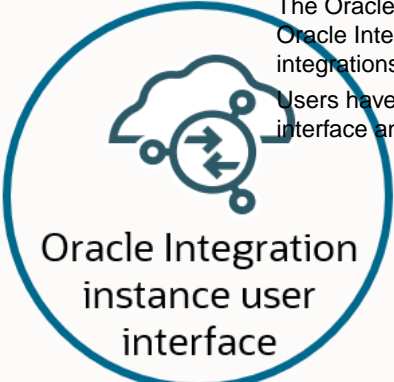
Before you dive into the details, review all the resources that require protection, the people who are responsible for protecting them, and the people and resources that access them.



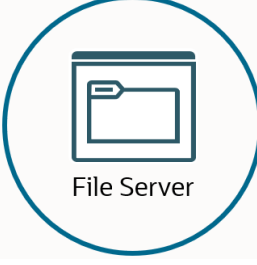




Resources

Familiarize yourself with all of the resources that your organization is responsible for protecting.



Resource	Description
 <p data-bbox="407 1608 724 1738">Oracle Integration instance user interface</p>	<p data-bbox="643 1371 1442 1457">The Oracle Integration instance user interface is the service instance where Oracle Integration users sign in and then design, deploy, and monitor integrations.</p> <p data-bbox="643 1467 1390 1522">Users have two ways to access an Oracle Integration instance: its user interface and its APIs.</p>

Resource	Description
 <p data-bbox="410 390 578 478">Developer API for Oracle Integration 3</p>	<p data-bbox="643 247 1406 275">The Oracle Integration instance APIs include the following types of APIs:</p> <ul data-bbox="643 285 1445 573" style="list-style-type: none"> <li data-bbox="643 285 1445 449"> Developer APIs The following APIs are the developer APIs: <ul data-bbox="691 359 1445 449" style="list-style-type: none"> <li data-bbox="691 359 1146 386">– Developer API for Oracle Integration 3 <li data-bbox="691 390 1445 417">– Developer API for Oracle Cloud Infrastructure Process Automation <li data-bbox="691 422 1292 449">– Developer API for File Server in Oracle Integration 3 <li data-bbox="643 453 1445 573"> Integration endpoints An integration endpoint is the API that Oracle Integration exposes when you activate an integration. Every activated integration has its own integration endpoint. <p data-bbox="643 579 1445 695">Note: The Oracle Integration Administrative API for provisioning and administering an Oracle Integration instance is separate from the Developer API for Oracle Integration 3. The Oracle Integration Administrative API is part of the Oracle Cloud Infrastructure APIs.</p> <p data-bbox="643 701 1390 762">Users have two ways to access an Oracle Integration instance: its user interface and its APIs.</p>
 <p data-bbox="451 947 545 974">Projects</p>	<p data-bbox="643 772 1308 800">Projects are components within an Oracle Integration instance.</p> <p data-bbox="643 806 1455 896">Instance users work in projects, which provide a single workspace for designing, managing, and monitoring integrations. See Design, Manage, and Monitor Integrations in Projects in <i>Using Integrations in Oracle Integration 3</i>.</p>
 <p data-bbox="435 1251 558 1278">File Server</p>	<p data-bbox="643 1066 1430 1127">File Server is an SFTP-compliant repository that is connected to an Oracle Integration instance.</p> <p data-bbox="643 1134 1455 1215">Use File Server for storing and retrieving files, and access it using its APIs or an SFTP client. People and integrations can access File Server. See About File Server in <i>Using File Server in Oracle Integration 3</i>.</p>
 <p data-bbox="407 1528 586 1556">Target systems</p>	<p data-bbox="643 1360 1430 1442">A target system is an application or service that an integration connects to and then completes a task in. An integration must be able to access target systems so that it can run as expected.</p> <p data-bbox="643 1449 1438 1509">Target systems can be Oracle services, third-party services, or applications that your organization has developed.</p>



Resource	Description
 <p>OCI lifecycle operations for the Oracle Integration instance</p>	<p>You perform Oracle Cloud Infrastructure (OCI) lifecycle operations for the Oracle Integration instance using the Oracle Cloud Console. You have the following options for accessing the Oracle Cloud Console:</p> <ul style="list-style-type: none"> • User interface <p>The lifecycle operations that you can perform in the user interface are documented in a separate guide. See Create and Edit Oracle Integration 3 Instances in <i>Provisioning and Administering Oracle Integration 3</i>.</p> • Oracle Integration Administrative API <p>The Oracle Cloud Infrastructure APIs include endpoints for every Oracle Cloud Infrastructure service that is accessible from the Oracle Cloud Console.</p> <ul style="list-style-type: none"> – To see a list of all the included APIs, see API Reference and Endpoints in the Oracle Cloud Infrastructure Documentation. – To see only the Oracle Integration Administrative API, which allows you to manage the lifecycle of an Oracle Integration instance, see Oracle Integration Administrative API. • Oracle Cloud Infrastructure Administrative CLI <p>See Oracle Integration Administrative CLI.</p>




Managers of the Resources

At most organizations, several or many people are responsible for managing users' access to resources. These individuals typically use this guide to learn how to protect their organization's resources and data.

Note


People often have several job functions. For instance, some instance users are also OCI (Oracle Cloud Infrastructure) instance administrators.




Job function	Description	Works in the Oracle Cloud Console through the user interface, APIs, or CLI	Works in the Oracle Integration instance through the user interface or the Developer API for Oracle Integration 3
 <p>OCI tenant and domain administrator</p>	<p>The highest-level administrator for Oracle services is responsible for managing all services in your organization's Oracle Cloud Infrastructure tenancy. Responsibilities include the following:</p> <ul style="list-style-type: none"> • Creating a compartment to hold one or more Oracle Integration instances for your organization. • Administering the users, groups, and policies that dictate the security posture of the tenancy. • Granting permissions to OCI instance administrators so that they can manage the Oracle Integration instances in the compartment. • Creating Oracle Integration users in the identity and access management tool. • Assigning service roles to other Oracle Integration users so that they have the appropriate access to do their jobs. 		
 <p>OCI instance administrators</p>	<p>This administrator manages the lifecycle of one or more Oracle Integration instances, including performing the following tasks:</p> <ul style="list-style-type: none"> • Creating and configuring one or more Oracle Integration instances. • Managing the lifecycle of each Oracle Integration instance. • Adding access control lists, configuring custom endpoints, and setting up the transfer of data to Oracle Cloud Infrastructure Logging. 		

Job function	Description	Works in the Oracle Cloud Console through the user interface, APIs, or CLI	Works in the Oracle Integration instance through the user interface or the Developer API for Oracle Integration 3
 <p data-bbox="427 611 630 638">Instance users</p>	<p data-bbox="699 422 1016 646">Users' service roles determine their access. Granular service roles are available. See Oracle Integration Service Roles in <i>Provisioning and Administering Oracle Integration 3</i>.</p> <p data-bbox="699 659 1016 800">Instance users have different responsibilities, depending on their roles. For example, they might be responsible for some or all of the following tasks:</p> <ul data-bbox="699 812 1016 1339" style="list-style-type: none"> <li data-bbox="699 812 1016 953">• Managing and administering the features provisioned in an Oracle Integration instance. <li data-bbox="699 959 1016 987">• Designing integrations. <li data-bbox="699 993 1016 1100">• Controlling the people who can edit, view, and monitor the resources in a project. <li data-bbox="699 1106 1016 1213">• Configuring the security of a connection that an integration uses to connect to an application. <li data-bbox="699 1220 1016 1247">• Monitoring integrations. <li data-bbox="699 1253 1016 1339">• Viewing information about integrations and other components. 		
<p data-bbox="362 751 678 835">Instance users with one or more of the following service roles:</p> <ul data-bbox="362 848 678 1066" style="list-style-type: none"> <li data-bbox="362 848 678 875">• ServiceAdministrator <li data-bbox="362 882 678 909">• ServiceDeveloper <li data-bbox="362 915 678 942">• ServiceMonitor <li data-bbox="362 949 678 976">• ServiceDeployer <li data-bbox="362 982 678 1010">• ServiceUser <li data-bbox="362 1016 678 1043">• ServiceInvoker <li data-bbox="362 1050 678 1077">• ServiceViewer 			

Users of the Resources

People and resources require permissions to access Oracle Integration and its related resources. In many cases, the people who manage access to Oracle Integration often also require access to Oracle Integration.

User or resource	Description
 <p data-bbox="410 1780 581 1839">OCI instance administrators</p>	<p data-bbox="643 1654 1390 1703">For details about Oracle Cloud Infrastructure (OCI) administrators, see Managers of the Resources.</p>

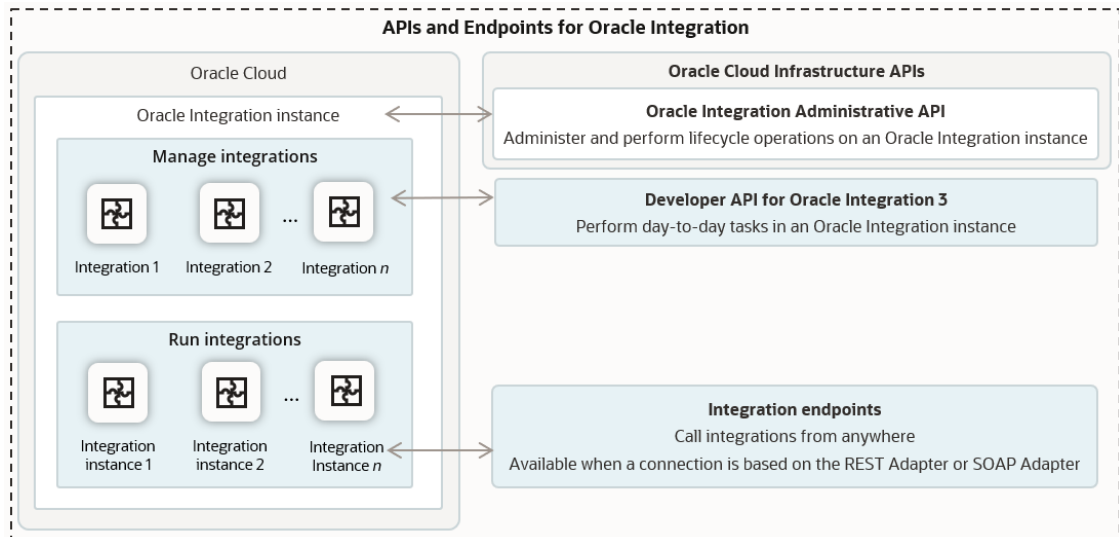
User or resource	Description
 <p>Instance users</p>	See Managers of the Resources .
 <p>Client systems</p>	An application that calls an integration in an Oracle Integration instance using a connection.
 <p>Connections</p>	The method that an Oracle Integration instance uses to connect to an application. Every connection is based on an adapter. For more information, see About Connections in <i>Using Integrations in Oracle Integration 3</i> .

Explore the Oracle Integration APIs

Oracle Integration provides administrative APIs, developer APIs, and endpoints for components.

Oracle Integration APIs

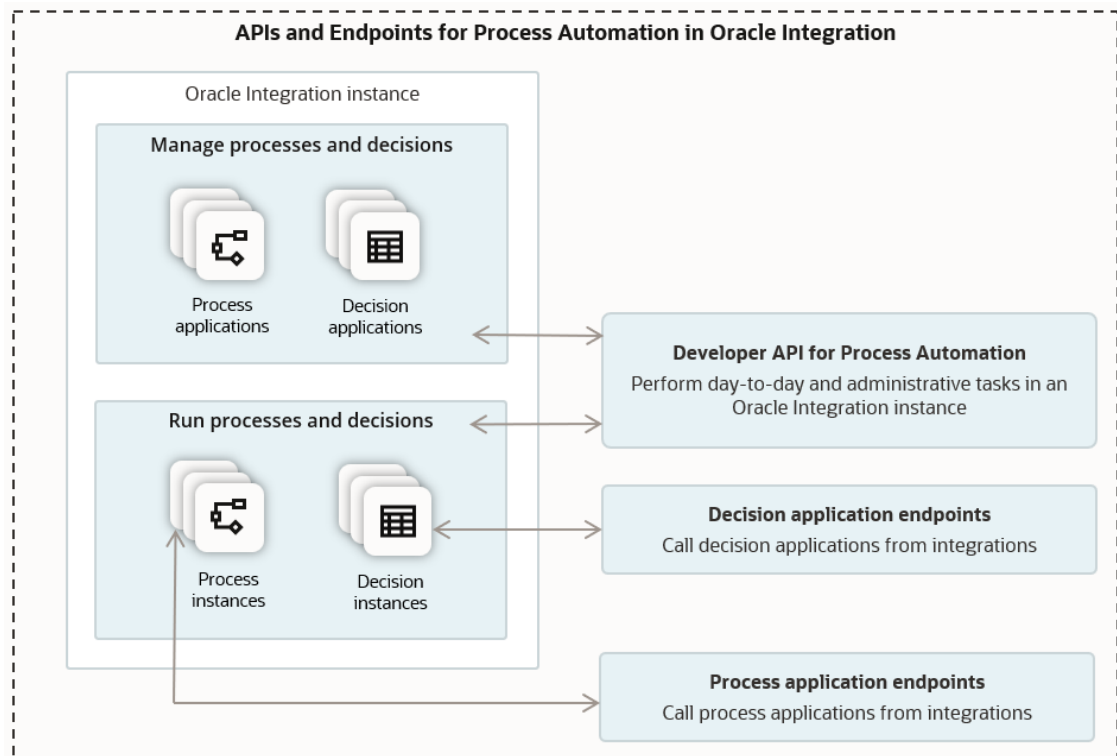
Every Oracle Integration instance includes access to the following APIs.



API	Typical users	Description	Alternate names
Oracle Cloud Infrastructure APIs	OCI tenant and domain administrators	The Oracle Cloud Infrastructure APIs contain service-specific APIs for Oracle Cloud Infrastructure services. Use the Oracle Cloud Infrastructure APIs to perform operations for each service. See API Reference and Endpoints in the Oracle Cloud Infrastructure Documentation.	Control plane APIs
Oracle Integration Administrative API	OCI tenant and domain administrators	Use the Oracle Integration Administrative API to perform lifecycle operations for an Oracle Integration instance, including provisioning an instance, managing custom endpoints, and extending data retention. This API provides access to the activities that you can perform in the user interface of the Oracle Cloud Console. A CLI is also available. See Oracle Integration API .	Control plane API Provisioning and administering APIs OCI lifecycle operations API
Developer API for Oracle Integration 3	Oracle Integration instance users	Use the Developer API for Oracle Integration 3 to perform day-to-day tasks in an Oracle Integration instance, including interacting with integrations and their related components. This API provides access to the activities that you can perform in the Oracle Integration user interface. See Oracle Integration 3 REST API .	Oracle Integration instance API Built-in API Factory API Application API
Integration endpoints	Oracle Integration instance users: integration developers	Use an integration endpoint to call an integration from anywhere. An integration endpoint is available only when a connection in an integration uses the REST Adapter, SOAP Adapter, or another adapter that exposes inbound REST or SOAP endpoints.	Customer-built APIs Dynamic APIs

Process Automation APIs

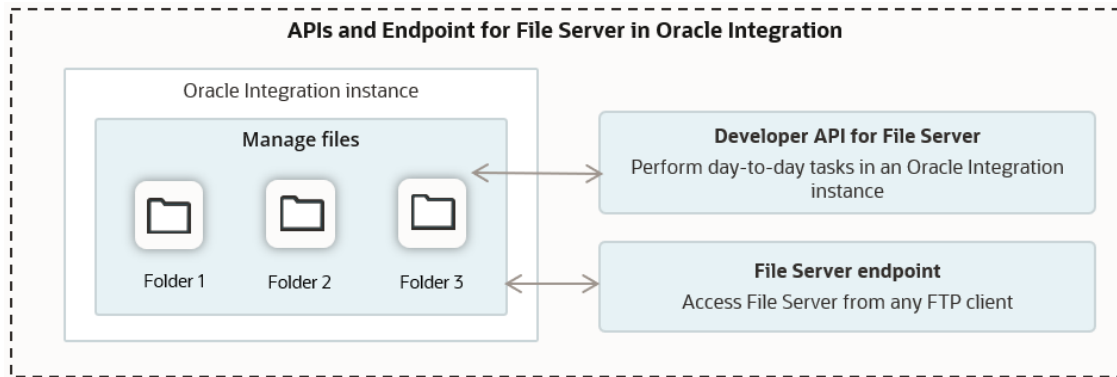
When you enable Process Automation in your Oracle Integration instance, you have access to the following APIs.



API	Typical users	Description	Alternate names
Developer API for Process Automation	Oracle Integration instance users	Use the Developer API for Process Automation to automate and manage business processes. This API provides access to the activities that you can perform in the Process Automation user interface. See OCI Process Automation REST API .	Process Automation instance API Built-in API Factory API Application API
Decision application endpoints	Oracle Integration instance users: decision application developers	Use a decision application endpoint to call a decision application from anywhere.	n/a
Process application endpoints	Oracle Integration instance users: process application developers	Use a process application endpoint to call a process application from anywhere.	n/a

File Server APIs

When you enable File Server in your Oracle Integration instance, you have access to the following APIs.



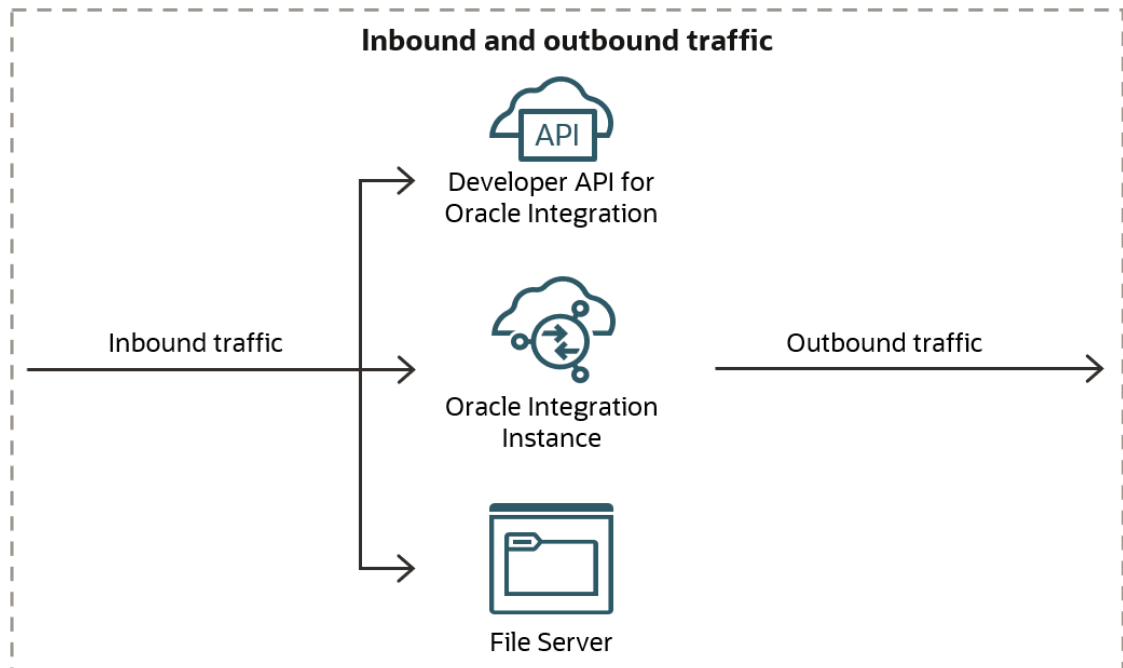
API	Typical users	Description	Alternate names
Developer API for File Server	Oracle Integration instance users	Use the Developer API for File Server to configure and administer File Server. File Server is an SFTP-compliant repository that is connected to an Oracle Integration instance. This API provides access to the activities that you can perform in the Oracle Integration user interface for File Server. See File Server in Oracle Integration 3 REST API .	Oracle Integration instance API for File Server Built-in API Factory API Application API
File Server endpoint	Oracle Integration instance users	Use the File Server endpoint to access File Server from any integration.	n/a

Control Network Access

To control network access, you protect the usability and integrity of your network and data by routing and restricting traffic appropriately. Network access control for Oracle Integration is primarily oriented around restricting the IP addresses that can access Oracle Integration and its related resources.

Types of Traffic

Inbound traffic originates *outside* an Oracle Integration instance, and outbound traffic originates *in* an Oracle Integration instance.



Oracle routes and restricts traffic according to its type. The following table provides a quick overview of the routing and restrictions for inbound and outbound traffic.

Type of traffic	Definition
Inbound traffic	<p>Also called ingress traffic, this traffic originates <i>outside</i> Oracle Integration and goes to:</p> <ul style="list-style-type: none"> • An Oracle Integration instance • The Oracle Integration APIs, including the Developer API for Oracle Integration 3 and the integration endpoints • File Server <p>To restrict the traffic, create an allowlist for the Oracle Integration instance. The allowlist applies to traffic from the service gateway and the public internet. Keep reading for more details and links to step-by-step instructions.</p>
Outbound traffic	<p>Also called egress traffic, this traffic originates <i>in an Oracle Integration instance</i> and goes to a target system.</p>

Inbound and outbound traffic is routed in the following ways.


Type of traffic	How the traffic is routed
Traffic across Oracle Cloud Infrastructure services that are <i>in the same region</i>	<p>Traffic within a region is routed through a service gateway:</p> <ul style="list-style-type: none"> Inbound traffic <p>If your organization creates a service gateway for the route rule All <region> Services in Oracle Services Network, and the service gateway is in the same region as the Oracle Integration instance, all inbound traffic that originates in an application that is within Oracle Cloud Infrastructure goes through the service gateway. Traffic that goes through a service gateway never leaves the regional Oracle Cloud Infrastructure.</p> Outbound traffic <p>If your organization creates a service gateway, outbound traffic goes through the service gateway if the target endpoint is an Oracle Cloud Infrastructure service that supports a service gateway. Traffic that goes through a service gateway never leaves Oracle Cloud Infrastructure.</p> <p>To see the list of services that support service gateways, see Service Gateway: Supported Cloud Services.</p>
Traffic across Oracle Cloud Infrastructure services that are <i>in different regions</i>	Cross-region traffic is routed through a NAT gateway or the internet gateway.
Traffic that comes through the public internet	Inbound and outbound traffic that comes through the public internet doesn't require any configuration.
Traffic that comes through either (1) the connectivity agent over the public internet or (2) FastConnect and VPN	<p>Inbound and outbound traffic that comes through an on-premises connectivity agent goes over the public internet.</p> <p>Inbound and outbound traffic that comes through FastConnect and VPN goes through the FastConnect link.</p>
Outbound traffic that comes through a private channel	If your organization configures a private endpoint to connect to private resources that are in your virtual cloud network (VCN), outbound traffic to these resources goes through a private channel that is set up within Oracle Cloud Infrastructure.



Control Inbound Network Access

After you create an Oracle Integration instance, access to the Developer API for Oracle Integration 3, the integration endpoints, and File Server is open by default. However, you can use allowlists to control the inbound access to the APIs and File Server.

An allowlist restricts access based on the source system or source networks and creates a stronger security posture.

If you choose to control inbound network access, you are responsible for completing the required tasks.


Security goal	Owner	More information
Restrict traffic that comes from the same Oracle Cloud Infrastructure region as your Oracle Integration instance	 <p>OCI instance administrators</p>	<p>About this traffic</p> <p>By default, all inbound traffic coming from an Oracle Cloud Infrastructure Virtual Cloud Network (VCN) that is in the same region as an Oracle Integration instance is open. However, you can restrict the traffic using a service gateway.</p> <p>How to achieve this goal</p> <ol style="list-style-type: none"> 1. Configure a Virtual Cloud Network (VCN) in the same region as your Oracle Integration instance. See Create and configure a virtual cloud network. 2. Create a service gateway as a configured route in the VCN. See Creating a Service Gateway in the Oracle Cloud Infrastructure Documentation. 3. Configure an allowlist for Oracle Integration so that the Oracle Integration instance allows only traffic from the IP address or the VCN ID of the service gateway. You can update the allowlist when you create the Oracle Integration instance or afterward. See <i>Restrict Access to an Instance in Provisioning and Administering Oracle Integration 3</i>. 4. If the connectivity agent is hosted in the same region, update the allowlist for the service gateway so that the connectivity agent can access the Oracle Integration instance. 5. Ensure that all source traffic comes from a VCN that is configured as an allowlisted IP address or VCN ID. <p>Notes</p> <ul style="list-style-type: none"> • If your organization doesn't use a VCN, your traffic comes over a network that is configured outside of Oracle Cloud Infrastructure. • If you don't create a service gateway and your organization has configured a NAT gateway, then traffic goes through the NAT gateway instead.

Security goal	Owner	More information
Restrict traffic that comes from outside the Oracle Cloud Infrastructure region of your Oracle Integration instance	 <p>OCI instance administrators</p>	<p>About this traffic</p> <p>Inbound traffic to Oracle Integration comes from the following sources:</p> <ul style="list-style-type: none"> • A request from an Oracle Cloud Infrastructure VCN that's in a different region than your Oracle Integration instance. • A request from outside an Oracle Cloud Infrastructure Virtual Cloud Network (VCN). <p>By default, this traffic comes over the internet. Restricting the traffic that comes in over the internet provides your organization with an additional level of security. Restrict this traffic by using a Classless Inter-Domain Routing (CIDR) block range.</p> <p>How to achieve this goal</p> <ol style="list-style-type: none"> 1. Configure an allowlist for Oracle Integration. The allowlist must allow access to only the specified individual IP addresses or Classless Inter-Domain Routing (CIDR) block (a range of IP addresses). You can update the allowlist when you create the Oracle Integration instance or afterward. See <i>Restrict Access to an Instance in Provisioning and Administering Oracle Integration 3</i>. 2. If the connectivity agent is hosted outside the Oracle Cloud Infrastructure region that holds your Oracle Integration instance, update the allowlist for internet traffic so that the connectivity agent can access the Oracle Integration instance. For example, this step applies when the agent is installed on a non-Oracle cloud, another region in the Oracle cloud, or your organization's data center. 3. Ensure that all source traffic that comes from the internet comes from the configured IP addresses or CIDR blocks.
Allow your network to access File Server	 <p>OCI instance administrators</p>	<p>Update the allowlist for File Server so that your organization's network can access File Server. This one-time task is required for every organization that uses File Server. See <i>Create an Allowlist for Public IP Addresses in Using File Server in Oracle Integration 3</i>.</p>



Control Outbound Network Access

Oracle Integration doesn't restrict outbound traffic from itself. However, Oracle Integration sends outbound traffic only as part of an integration that your organization configures.

The ways that you secure, enable, and allow this traffic depend upon the location of the external service that receives the outbound traffic. Keep reading for more details.

Security goal	Owner	More information
<p>Secure outbound traffic to endpoints that are in either of the following locations:</p> <ul style="list-style-type: none"> A virtual cloud network (VCN) in the same region as the Oracle Integration instance. Endpoints that are <i>within</i> the Oracle Services Network and in the same region as the Oracle Integration instance. 	 <p>OCI instance administrators</p>	<p>Secure this traffic using a private endpoint</p> <p>A private endpoint ensures that an Oracle Integration instance can communicate with target applications using an allowlist, also known as an access control list (ACL).</p> <p>If the endpoint is public facing, you must also configure a private NAT gateway.</p> <p>If your tenancy uses Zero Trust Packet Routing (ZPR) and you need to connect to ZPR-secured OCI resources, you must also assign security attributes to your instance.</p> <p>Learn more about private endpoints</p> <p>To learn more about private endpoints, including the traffic that you can secure using a private endpoint and the differences between private endpoints and the connectivity agent, see <i>Connect to Private Resources in Provisioning and Administering Oracle Integration 3</i>.</p> <p>Your responsibilities</p> <ol style="list-style-type: none"> If required, configure a private NAT gateway. Additionally, add the IP address for the NAT gateway to the allowlists for the endpoints that you need to connect to in the Oracle Services Network. Configure a private endpoint. See <i>Configure a Private Endpoint for an Instance in Provisioning and Administering Oracle Integration 3</i>. If your tenancy uses Zero Trust Packet Routing (ZPR), assign security attributes to your service instance. See <i>Assign Zero Trust Packet Routing (ZPR) Security Attributes to Your Instance in Provisioning and Administering Oracle Integration 3</i>.

Security goal	Owner	More information
Enable outbound traffic to endpoints that are in your organization's on-premises network, also known as a private cloud	<p data-bbox="643 247 857 327">Download the connectivity agent installer:</p> <div data-bbox="643 338 906 600" style="border: 1px solid #0070C0; border-radius: 50%; padding: 10px; text-align: center;">  <p data-bbox="695 491 857 518">Instance users</p> </div> <p data-bbox="643 617 889 697">Instance users with the ServiceAdministrator role</p> <p data-bbox="643 709 857 764">Complete all other tasks:</p> <div data-bbox="643 774 906 1037" style="border: 1px solid #0070C0; border-radius: 50%; padding: 10px; text-align: center;">  <p data-bbox="695 907 857 968">Other administrators</p> </div> <p data-bbox="643 1054 899 1163">Other administrators complete these tasks in third-party applications and on virtual machines.</p>	<p data-bbox="919 247 1409 302">Enable this traffic by using an agent-based configuration</p> <p data-bbox="919 308 1468 569">If an integration must connect to endpoints that are in your corporate network, use an agent-based configuration. You can use an on-premises connectivity agent, or an Oracle Cloud Infrastructure connectivity agent. You can use a FastConnect peering pattern with both options. Some adapters allow you to use a FastConnect peering pattern without installing the connectivity agent.</p> <p data-bbox="919 575 1468 655">With the connectivity agent, you don't need to relax any network conditions; for example, you don't need to open a port for Oracle Integration.</p> <p data-bbox="919 661 1468 808">The connectivity agent runs in your corporate network and polls Oracle Integration for work. The agent requires internet or Virtual Cloud Network (VCN) inbound access to the Oracle Integration instance.</p> <p data-bbox="919 821 1425 875">Organizations that must use an agent-based configuration</p> <p data-bbox="919 882 1468 936">Use an agent-based configuration if your organization has any of the following requirements:</p> <ul data-bbox="919 942 1468 1146" style="list-style-type: none"> <li data-bbox="919 942 1468 1031">• An integration must connect to an on-premises application in your corporate network or an application in a private cloud. <li data-bbox="919 1037 1468 1146">• You must route some or all traffic through an on-premises proxy. Typically, organizations route traffic this way as a means of controlling the traffic. <p data-bbox="919 1159 1386 1186">Learn more about the connectivity agent</p> <p data-bbox="919 1192 1468 1339">To learn about the connectivity agent, including its components, functionality, compatible adapters, diagrams, and more, see About Connecting to On-Premises Applications with the Connectivity Agent in <i>Using Integrations in Oracle Integration 3</i>.</p> <p data-bbox="919 1346 1159 1373">Your responsibilities</p> <ol data-bbox="919 1379 1468 1860" style="list-style-type: none"> <li data-bbox="919 1379 1468 1562">1. If your organization requires one or more connectivity agents, make sure that the connectivity agent is compatible with your organization's operating procedures. See Requirements for the Connectivity Agent in <i>Using Integrations in Oracle Integration 3</i>. <li data-bbox="919 1568 1468 1715">2. If required, install and configure the connectivity agent. See Download and Run the Connectivity Agent Installer and Key Points for the Installation of the Connectivity Agent in <i>Using Integrations in Oracle Integration 3</i>. <li data-bbox="919 1722 1468 1860">3. If desired, configure a FastConnect peering pattern. See Connection Patterns for Hybrid Integrations in <i>Using Integrations in Oracle Integration 3</i>.

Security goal	Owner	More information
Allow Oracle Integration to access endpoints that are <i>outside</i> the Oracle Services Network	<p>Obtain the IP address:</p>  <p>Instance users with the ServiceAdministrator, ServiceDeveloper, ServiceUser, or ServiceViewer role</p> <p>Update the allowlist:</p>  <p>Other administrators work in third-party applications and on virtual machines.</p>	<p>If a target application has an allowlist enabled, update the allowlist so that Oracle Integration has access by completing the following steps:</p> <ol style="list-style-type: none"> 1. Identify the IP address that the Oracle Integration instance uses to send traffic. See Obtain the Inbound and Outbound IP Addresses of the Oracle Integration Instance in <i>Provisioning and Administering Oracle Integration 3</i>. 2. Add the IP address to the allowlist for the endpoint's application.

Transport Layer Security for Inbound Traffic

An application that connects to Oracle Integration negotiates the Transport Layer Security (TLS) for inbound traffic. Oracle Integration currently supports TLS 1.2 for inbound traffic.

For details about the ciphers that are supported, see TLS Cipher Suites Support in *Provisioning and Administering Oracle Integration 3*.

Transport Layer Security for Outbound Traffic

Oracle Integration negotiates the Transport Layer Security (TLS) automatically with the target applications in an integration. Oracle Integration supports TLS 1.3 and 1.2 for outbound traffic.

If a target application supports TLS 1.3, Oracle Integration negotiates and communicates using 1.3. If not, Oracle Integration attempts to negotiate with 1.2. If your organization's preferred network protocol is TLS 1.3, configure TLS 1.3 as the preferred protocol in each of the applications that you integrate with.

Control User, Client System, and Connection Access

You control the people, client systems, and connections that can access various resources by *authenticating* their access. You control the activities that they can perform after they have access by *authorizing* this access.

Some resources support multiple authentication methods. In such cases, the authentication methods restrict access in identical ways. For instance, you have the same access in the Oracle Cloud Console whether you access it using the API, CLI, or user interface.

An API, rather than the client that accesses it, is the sole determiner of its authentication methods.

Topics:

- [Oracle Integration Instance User Interface: Control User Access](#)
- [Developer APIs: Control User and Client System Access](#)
- [Projects: Control User Access](#)
- [File Server: Control User and Client System Access](#)
- [Target Systems: Control Connection Access](#)
- [Oracle Cloud Infrastructure Lifecycle Operations for the Oracle Integration Instance: Control User Access](#)


Oracle Integration Instance User Interface: Control User Access

Understand your responsibilities for controlling access to the Oracle Integration instance user interface.

On This Page




- [Access at a Glance](#)
- [How to Control Access](#)


Access at a Glance

Area	More information
People who need access	
Authentication method: Login sessions	<p>To access the user interface of an Oracle Integration instance or the Oracle Cloud Console, people must sign in. To sign in, a user must be a member of an identity domain. The identity domain authenticates the user.</p> <p>To learn more, see Managing Identity Domains in the Oracle Cloud Infrastructure documentation.</p>

Area	More information
Authorization method: Service roles within the Oracle Integration application	Service roles govern access to actions <i>within an Oracle Integration instance</i> , including actions that you perform using the Developer API for Oracle Integration 3 and integration endpoints. See Oracle Integration Roles and Privileges in <i>Provisioning and Administering Oracle Integration 3</i> .

How to Control Access

Security goal	Owner	More information
Choose an identity and access management tool	 <p>OCI tenant and domain administrator</p>	<p>Oracle Cloud Infrastructure Identity and Access Management, or Oracle Cloud Infrastructure IAM, is an identity and access management tool in which you create Oracle Integration users, groups, and policies.</p> <p>Alternatively, you can use SAML 2.0 federation to federate Oracle Cloud Infrastructure IAM with an identity system that your organization already uses. When you federate an identity system with Oracle Cloud Infrastructure IAM, you delegate the responsibility of managing access for Oracle Integration to the other identity system.</p> <p>If your organization already uses an identity system, federating offers many benefits. You don't need to create new accounts for Oracle Integration users, and users don't need to remember yet another user name and password.</p>
If your organization doesn't use Oracle Cloud Infrastructure IAM as its identity system, federate Oracle Cloud Infrastructure IAM with your organization's identity system	 <p>OCI tenant and domain administrator</p>	<p>Use SAML 2.0 federation to federate Oracle Cloud Infrastructure IAM with your organization's existing identity and access management system</p> <p>See Federating with Identity Providers in the Oracle Cloud Infrastructure documentation.</p>
Configure access	 <p>OCI tenant and domain administrator</p>	<ul style="list-style-type: none"> If your tenancy uses identity domains, see <i>Workflow for Access in an Identity Domain</i> in <i>Provisioning and Administering Oracle Integration 3</i>. If your tenancy doesn't use identity domains, see <i>Workflow for Access Without an Identity Domain</i> in <i>Provisioning and Administering Oracle Integration 3</i>.

Security goal	Owner	More information
Add an additional layer of security by enabling multifactor authentication (MFA)	 <p>OCI tenant and domain administrator</p>	<p>When to enable MFA</p> <p>Oracle recommends enabling MFA only for users that access the Oracle Integration user interface.</p> <p>When not to enable MFA</p> <p>Do not enable MFA for user accounts that access REST APIs, including the Developer API for Oracle Integration 3 and integration endpoints.</p> <p>An MFA configuration restricts the authentication methods for invoking the APIs. For example, an MFA-enabled user typically cannot authenticate using basic auth. Additionally, when authenticating using an OAuth 2.0 token, the user account must use specific grants, such as the User Assertion grant or the Authorization Code grant, and not the Resource Owner Password Credentials grant.</p> <p>How to enable MFA</p> <ul style="list-style-type: none"> Write a policy that enables multifactor authentication (MFA) and assign it to the appropriate user groups. Do not modify the default sign-on policy. Instead, create a new sign-on policy. If you modify the default sign-on policy, you won't be able to invoke integration endpoints using your REST clients. <p>If you use Oracle Cloud Infrastructure IAM as your identity system, see Managing Multifactor Authentication in the Oracle Cloud Infrastructure documentation.</p>



Developer APIs: Control User and Client System Access

Understand your responsibilities for controlling access to the Developer APIs.

On This Page



- [Access at a Glance](#)
- [How to Control Access](#)

Access at a Glance

Area	More information
People and systems that need access	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  <p>Instance users</p> </div> <div style="text-align: center;">  <p>Client systems</p> </div> </div>

Area	More information
Authentication method: Several, depending on the API	<p>The APIs have different authentication methods:</p> <ul style="list-style-type: none"> • Developer API for Oracle Integration 3: OAuth 2.0 token, obtained on behalf of a user or cloud application. • Integration endpoints: Determined by the adapter that builds the API. The adapter that you use as the trigger for an integration builds the integration endpoint.
Authorization methods: Service roles	<p>The APIs have different authorization methods:</p> <ul style="list-style-type: none"> • Developer API for Oracle Integration 3 and integration endpoints: Oracle Integration service roles. See Oracle Integration 3 Service Roles in <i>Provisioning and Administering Oracle Integration 3</i>. • Developer API for Process Automation: Process Automation roles and process application roles: <ul style="list-style-type: none"> – Process Automation roles provide <i>functional security</i>. See Process Automation Roles in <i>Administering Oracle Cloud Infrastructure Process Automation</i>. Process Automation roles control access to the administration and designer APIs. – Process application roles provide <i>data security</i>. See About Process Application Roles in <i>Using Oracle Cloud Infrastructure Process Automation</i>. Process application roles control access to the runtime APIs. <p>The following list identifies the administration, designer, and runtime APIs in the Developer API for Process Automation:</p> <ul style="list-style-type: none"> – Credentials: Administration APIs – Decision Applications: Designer APIs – Decisions: Runtime APIs – Dynamic Processes: Runtime APIs – Process Applications: Designer APIs – Processes: Runtime APIs – Roles: Administration APIs – User Configurations: Runtime APIs – User Tasks: Runtime APIs <p>In some situations, users have implicit access to resources, regardless of their roles. For instance:</p> <ul style="list-style-type: none"> – A task's assignee, candidate, and creator have implicit view access to a task. – The creator of an instance has implicit view access for the instance. – The Process Application Administrator role has irrevocable manage permission of all process applications. <p>A user's access is a combination of their assigned roles and their implicit permissions.</p> • Developer API for File Server: For details about this API's authorization methods, see File Server: Control User and Client System Access.

How to Control Access

Security goal	Owner	More information
Create an OAuth client application with the appropriate scopes so that the client can access the API	 <p>OCI tenant and domain administrator</p>	<p>Follow the guidance for the API that you need to access:</p> <ul style="list-style-type: none"> Developer API for Oracle Integration 3 See <i>Use OAuth 2.0 in Oracle Integration in Using Integrations in Oracle Integration 3</i>. Developer API for Process Automation See <i>Security, Authentication and Authorization in Developer API for Oracle Cloud Infrastructure Process Automation</i>. Developer API for File Server See <i>OAuth Authentication in Oracle Integration for File Server in Developer API for File Server in Oracle Integration 3</i>. Integration endpoints Oracle provides a guide for using each adapter. See <i>Configure Connection Properties in Using Integrations in Oracle Integration 3</i> for links to all adapter guides.
Provision the users who need to access the REST APIs	 <p>OCI tenant and domain administrator</p>	<ul style="list-style-type: none"> If your tenancy uses identity domains, see <i>Workflow for Access in an Identity Domain in Provisioning and Administering Oracle Integration 3</i>. If your tenancy doesn't use identity domains, see <i>Workflow for Access Without an Identity Domain in Provisioning and Administering Oracle Integration 3</i>. <p>If any users must access the customer-built-APIs, assign them the <code>ServiceInvoker</code> role.</p>

Note

Instance users, typically integration developers, are responsible for configuring connections to integration endpoints. Afterward, the developer uses the connection in an integration, finalizes the integration, and activates the integration. When the integration runs, Oracle Integration exposes the integration endpoints. These integration endpoints follow the authentication for the adapter upon which the connection is based. Each adapter supports different authentication patterns. Oracle provides a guide for using each adapter. See *Available Adapters for Connections in Using Integrations in Oracle Integration 3* for links to all adapter guides.


Projects: Control User Access

Understand your responsibilities for controlling access to projects.


On This Page

- [Access at a Glance](#)
- [How to Control Access](#)

Access at a Glance

Area	More information
People who need access	
Authentication method: Authentication method that is used by the user interface or APIs	<p>The way that you access a project determines your authentication method. You have the following options for accessing projects:</p> <ul style="list-style-type: none"> • Through the Oracle Integration instance user interface. For details, see Oracle Integration Instance User Interface: Control User Access. • Through the Developer API for Oracle Integration 3. For details, see Developer APIs: Control User and Client System Access.
Authorization method: Role-based access control	<p>Role-based access control governs access to a project and its integration components <i>within an Oracle Integration instance</i>, including actions that you perform using the Developer API for Oracle Integration 3. Role-based access control, sometimes called RBAC, determines the users and groups who can edit, view, and monitor a project.</p> <p>Role-based access control can be <i>more restrictive</i> than a service role but can <i>never</i> give a user more permissions than a service role allows. For example:</p> <ul style="list-style-type: none"> • When a user with a developer service role has monitoring rights in a project, the user can view but not update the components. The user's service role would ordinarily grant the user edit rights, but the role-based access control in the project limits the user to read-only access. • When a user with a monitoring service role is granted developer access in a project, the user cannot delete components in the project. The user's service role doesn't allow the user to delete components, and the role-based access control in the project does not provide more access than the user's service role. <p>Notes:</p> <ul style="list-style-type: none"> • A project administrator can add and remove other project administrators within a given project. • People with the ServiceAdministrator role always have unrestricted access to every project in an instance.

How to Control Access

Security goal	Owner	More information
Control the people who can access each project	 <p data-bbox="683 436 813 457">Instance users</p> <p data-bbox="643 537 850 758">Instance users with the ServiceAdministrator role, or project administrators with the ServiceDeveloper role</p>	<p data-bbox="865 310 1430 338">Assign role-based access control within each project.</p> <p data-bbox="865 348 1474 432">To learn about role-based access control, and to set up access, see <i>Control Who Can Edit, View, and Monitor in a Project</i> in <i>Using Integrations in Oracle Integration 3</i>.</p>



File Server: Control User and Client System Access

File Server is the embedded SFTP server within Oracle Integration. Like all SFTP servers, it authenticates access using user IDs. Understand your responsibilities for controlling access to File Server.

On This Page



- [Access at a Glance](#)
- [How to Control Access](#)

Access at a Glance

Area	More information
People and systems that need access	 <p data-bbox="699 1482 886 1503">Instance users</p>  <p data-bbox="1000 1503 1195 1530">Client systems</p>

Area	More information
Authentication method: IP address, and either user login or public key	<p>Ways that people connect to File Server:</p> <ul style="list-style-type: none"> User interface in the Oracle Integration instance Developer API for File Server Supported SFTP client or an SFTP command line interface <p>Ways that integrations connect to File Server:</p> <ul style="list-style-type: none"> File server action from within an integration FTP Adapter <p>Authentication method for people and integrations</p> <p>To access File Server, your IP address must be added to the File Server allowlist.</p> <p>Additionally, File Server authenticates access using either user logins or a public key.</p>
Authorization method: File Server permissions	Configure users' access to File Server by assigning permissions to users and groups, assigning users to groups, and then setting permissions for individual folders in File Server.

How to Control Access

Security goal	Owner	More information
Specify the authentication method for File Server	 <p>Instance users</p> <p>Instance users with the ServiceAdministrat or role</p>	See Configure File Server Settings in <i>Using File Server in Oracle Integration 3</i> .
Configure access to File Server	 <p>Instance users</p> <p>Instance users with the ServiceAdministrat or role</p>	See Configure Users in <i>Using File Server in Oracle Integration 3</i> .

Note

An integration can always connect directly to File Server using the File server action. Your organization does not need to take any action to grant this access. See Interact with Files in File Server in *Using Integrations in Oracle Integration 3*.

Target Systems: Control Connection Access


Outbound traffic, also called egress traffic, originates in an Oracle Integration instance. Outbound traffic goes to a target system, which is a service that an integration invokes, or calls. All outbound traffic from an integration is routed through an adapter. Understand your responsibilities for controlling access to target systems.

Integration developers must configure connections based on the target system's requirements. The target system is responsible for authenticating and authorizing requests to it. To learn how to connect to a target system, refer to the documentation for the target system.



On This Page

- [Access at a Glance](#)
- [How to Control Access](#)

Access at a Glance

Area	More information
Connections that need access	 <p data-bbox="708 1041 873 1073">Connections</p>
Authentication and authorization methods: Its own methods	<p data-bbox="643 1150 1468 1289">Each target system specifies one or more own authentication and authorization method(s). The adapter for the target system supports at least one authentication and authorization method. Additionally, technology-specific adapters (REST, SOAP, and FTP) support one or more authentication and authorization methods.</p> <p data-bbox="643 1304 1403 1356">For details about the methods that each target system supports, see the documentation for the target system.</p> <p data-bbox="643 1371 1430 1482">For details about the methods that each adapter supports, see the adapter documentation. Oracle provides a guide for using each adapter. See <i>Configure Connection Properties and Security Properties in Using Integrations in Oracle Integration 3</i> for links to all adapter guides.</p>

How to Control Access

Security goal	Owner	More information
When creating an integration, ensure that the credentials that access each target application are configured appropriately	 <p>Instance users with the ServiceDeveloper role</p>	<p>Ensure that the credentials that you configure in a connection can authenticate and authorize successfully in the target application. For example, the credentials must have valid roles to perform the required tasks in the target system.</p> <p>For applications with adapters</p> <p>Oracle Integration connects to other applications and resources using adapters. When an integration developer designs an integration, the developer configures this access by defining a trigger connection that is based on an adapter. Most adapters require either OAuth tokens or signature-based authentication to authenticate a resource's access to the Oracle Integration instance.</p> <p>For applications without adapters</p> <p>When an adapter isn't available for an application that needs to access your Oracle Integration instance, Oracle recommends creating connections using the REST Adapter or the SOAP Adapter and providing an OAuth token. You can also build your own adapter using the Rapid Adapter Builder. See <i>What Is the Rapid Adapter Builder?</i> in <i>Using the Rapid Adapter Builder with Oracle Integration 3</i>.</p> <p>See the adapter documentation</p> <p>Oracle provides a guide for using each adapter. See <i>Configure Connection Properties and Security Properties</i> in <i>Using Integrations in Oracle Integration 3</i> for links to all adapter guides.</p>
Write IAM (identity and access management) policies that give Oracle Integration access to the resources	 <p>OCI tenant and domain administrator</p>	<p>Several actions allow you to access Oracle Cloud Infrastructure resources directly from an integration. To use these actions, you must complete several prerequisite tasks, including writing IAM policies that grant the Oracle Integration instance access to the resources and creating dynamic groups. See the following in <i>Using Integrations in Oracle Integration 3</i>:</p> <ul style="list-style-type: none"> Invoke Oracle Cloud Infrastructure Functions Directly from an Integration with an OCI Function Action Invoke Oracle Cloud Infrastructure Object Storage from an Integration with an OCI Object Storage Action

Oracle Cloud Infrastructure Lifecycle Operations for the Oracle Integration Instance: Control User Access


Use IAM (identity and access management) policies to secure access to the Oracle Cloud Infrastructure lifecycle operations for the Oracle Integration instance.

On This Page






- [Access at a Glance](#)

- [How to Control Access](#)

Access at a Glance

Area	More information
People who need access	 <p>OCI tenant and domain administrator</p>
Authentication method: Several methods	<p>One of the following methods:</p> <ul style="list-style-type: none"> • User interface authentication: User logins To access the user interface of Oracle Integration or the Oracle Cloud Console, people must sign in. To sign in, a user must be a member of an identity domain. The identity domain authenticates the user. • API authentication: Several methods An API, rather than the client that accesses it, is the sole determiner of its authentication methods. To learn about the authentication methods, see OCI SDK Authentication Methods in the Oracle Cloud Infrastructure documentation. To review your options for accessing the Oracle Integration Administrative API, see Accessing Oracle Cloud Infrastructure in the Oracle Cloud Infrastructure documentation.
Authorization method: IAM (identity and access management) policies	<p>Users access the Oracle Cloud Console using its user interface, the Oracle Integration Administrative API, and the Oracle Integration Administrative CLI. IAM policies govern access to these resources. IAM policies apply to a single tenancy and govern outbound access, which is access from an Oracle Integration instance to another application or resource.</p> <p>IAM policies determine the types of operations that someone can perform on a resource. For example, a user with a READ policy for a resource cannot update the resource.</p> <p>IAM policies provide immense flexibility in declaring the individuals or groups who have access to Oracle Cloud Infrastructure resources and the level of access that they have. Every IAM policy contains a verb that describes the actions the group is allowed to do. The following verbs are available and are ordered from the <i>least</i> amount of access to the <i>most</i> amount of access:</p> <ul style="list-style-type: none"> • INSPECT • READ • USE • MANAGE <p>To learn more about IAM policies in general, see the following pages in the Oracle Cloud Infrastructure documentation:</p> <ul style="list-style-type: none"> • Getting Started with Policies • How Policies Work • Example Scenario <p>To learn about IAM policies for Oracle Integration, including the verbs to use when writing an IAM policy, see <i>About IAM Policies for Oracle Integration in Provisioning and Administering Oracle Integration 3</i>.</p>

How to Control Access

Security goal	Owner	More information
Understand your responsibilities and Oracle's responsibilities for various administrative tasks	 <p>OCI tenant and domain administrator</p>	<p>The tenancy administrator receives the welcome email from Oracle and is responsible for managing the lifecycle operations on the instance.</p> <p>See Oracle and Customer Responsibilities in Oracle Integration 3 in <i>Provisioning and Administering Oracle Integration 3</i>.</p>
Determine whether your tenancy uses identity domains	 <p>OCI tenant and domain administrator</p>	<p>Some tenancies use identity domains, while others don't. You have different requirements, depending on whether your tenancy uses identity domains.</p> <p>To understand the differences between tenancies with and without identity domains, and to determine whether your tenancy uses identity domains, see <i>Differences Between Tenancies With and Without Identity Domains</i> in <i>Provisioning and Administering Oracle Integration 3</i>.</p>
Configure access to the Oracle Integration instance	 <p>OCI tenant and domain administrator</p>	<ul style="list-style-type: none"> If your tenancy uses identity domains, see <i>Workflow for Access in an Identity Domain</i> in <i>Provisioning and Administering Oracle Integration 3</i>. If your tenancy doesn't use identity domains, see <i>Workflow for Access Without an Identity Domain</i> in <i>Provisioning and Administering Oracle Integration 3</i>.
If you configure Oracle Integration to send data to Oracle Cloud Infrastructure Logging or Oracle Cloud Infrastructure Monitoring, restrict the people who can look at the data	 <p>OCI tenant and domain administrator</p>	<p>You can send activity stream data to Oracle Cloud Infrastructure Logging. See Logging in the Oracle Cloud Infrastructure documentation.</p> <p>You can send message pack data to Oracle Cloud Infrastructure Monitoring. See Monitoring in the Oracle Cloud Infrastructure documentation.</p> <p>Ensure that you authorize only the correct people to view the logs and other data.</p> <p>Associate a policy with the log or log group. The policy should allow only select viewers.</p>
Periodically audit users' access to the Oracle Integration instance	 <p>OCI tenant and domain administrator</p>	

3

Data Protection


Oracle ensures the security of information within Oracle Integration. You are responsible for securing the accessing and exporting of information.



Topics:

- [Credential Handling](#)
- [Data Visibility](#)

Credential Handling

Everyone who works in Oracle Integration requires user credentials. Additionally, an integration that connects to an application requires credentials for the application.


Security goal	Owner	More information
Ensure that users handle their credentials securely	 <p>Oracle Integration administrators</p>	<p>About user credentials</p> <p>User credentials consist of a user name and password that people use to sign in to Oracle Integration, including File Server.</p> <p>You manage user credentials in Oracle Cloud Infrastructure Identity and Access Management, including creating users and resetting passwords. Oracle Integration authenticates users against Oracle Cloud Infrastructure Identity and Access Management.</p> <p>See IAM Credentials.</p> <p>Guidelines for handling credentials</p> <p>See IAM Credentials.</p>


Security goal	Owner	More information
Limit the people who can access connection credentials	<p>Create the credentials:</p>  <p>Other administrators</p> <p>Provide the credentials while configuring a connection:</p>  <p>Instance users</p> <p>Instance users with the ServiceDeveloper role</p>	<p>Oracle Integration uses credentials for a target application to connect to the application. An integration developer or an administrator for the target application provides these credentials when configuring a connection in an integration.</p> <p>After a user enters these credentials into Oracle Integration, sensitive security properties are obfuscated in the user interface. For example, the password appears as a series of asterisks (*****) rather than the password itself. Oracle Integration encrypts and stores these credentials securely in an internal Oracle Cloud Infrastructure Vault.</p> <p>Your responsibilities</p> <p>You are responsible for securely handling credentials outside Oracle Integration. Oracle recommends limiting the people who can access the credentials.</p>



Data Visibility


Protect data using role authorization.

For the list of service roles, see Oracle Integration Service Roles.

Security goal	Owner	More information
Secure access to design-time auditing data	 <p>Instance users</p> <p>Instance users with the ServiceAdministrator role, or project administrators with the ServiceDeveloper role</p>	<p>About design-time log data</p> <p>A design-time log is available for all integration artifacts. The log includes actions, the people who completed them, and the time they completed them.</p> <p>To learn more, see View the Design-Time Audit in Using Integrations in Oracle Integration 3.</p> <p>How to secure access</p> <p>For integrations that are outside a project, all log data is visible to anyone who can sign in to the Oracle Integration instance.</p> <p>The only way to restrict access to log data is to create an integration in a project, and restrict access to the project using role-based access control. If someone doesn't have view permissions in a project, the person can't view the log data for integrations in the project. See Projects: Control User Access.</p>

Security goal	Owner	More information
Secure access to runtime auditing information	 <p data-bbox="683 373 813 394">Instance users</p> <p data-bbox="643 474 846 699">Instance users with the ServiceAdministrator role, or project administrators with the ServiceDeveloper role</p>	<p data-bbox="865 247 1149 275">About the activity stream</p> <p data-bbox="865 285 1471 394">Runtime auditing in Oracle Integration appears in the activity stream, which shows details about the movement of messages through an integration. The activity stream also includes message payloads.</p> <p data-bbox="865 405 1271 432">Different tracing levels are available</p> <p data-bbox="865 443 1409 520">Several levels of tracing are available for the activity stream. The tracing level determines the following information:</p> <ul data-bbox="865 531 1471 653" style="list-style-type: none"> <li data-bbox="865 531 1409 588">• The amount of information that appears in the activity stream. <li data-bbox="865 598 1471 653">• The amount of time that the activity stream persists for an integration instance within Oracle Integration. <p data-bbox="865 663 1300 690">If you need to keep the data for longer</p> <p data-bbox="865 701 1442 835">You cannot change the amount of time for which the activity stream persists in Oracle Integration. However, you can save the activity stream details for a longer period of time and perform additional audit activities in the Oracle Cloud Console.</p> <p data-bbox="865 846 1446 903">See Use OCI Logging to Analyze Integration Activity in Provisioning and Administering Oracle Integration 3.</p> <p data-bbox="865 913 1101 940">Your responsibilities</p> <ul data-bbox="865 951 1471 1640" style="list-style-type: none"> <li data-bbox="865 951 1471 1297">• Be aware of the fields that appear in the activity stream for each level of tracing, and set the tracing level appropriately for each integration. The person who activates the integration sets the tracing level. <ul data-bbox="914 1066 1471 1297" style="list-style-type: none"> <li data-bbox="914 1066 1471 1144">Use the DEBUG option only for debugging purposes. The DEBUG option generates a lot of data, and the data is retained for only 24 hours. Change to a different tracing level after completing your debugging work. Be aware that after 24 hours, any integrations that are set to DEBUG tracing are automatically updated to use production-level tracing. <li data-bbox="865 1371 1471 1640">• Be aware that integrations that involve sensitive data could result in payload tracking that violates one or more of the following rules and standards: <ul data-bbox="914 1465 1471 1640" style="list-style-type: none"> <li data-bbox="914 1465 1471 1522">– Payment Card Industry (PCI) data security standards. <li data-bbox="914 1528 1471 1585">– Health Insurance Portability and Accountability Act (HIPAA) privacy rules. <li data-bbox="914 1591 1471 1640">– Personally identifiable information (PII) standards. <p data-bbox="914 1650 1446 1726">To review Oracle's recommendations, see Activate an Integration in Using Integrations in Oracle Integration 3.</p>

Security goal	Owner	More information
Keep sensitive data out of tracking variables	 <p data-bbox="683 373 816 394">Instance users</p> <p data-bbox="643 474 849 583">Instance users with the ServiceDeveloper role</p>	<p data-bbox="865 247 1143 275">About tracking variables</p> <p data-bbox="865 285 1476 394">An integration developer can track message fields during runtime by defining business identifiers on payload fields. During runtime, users can view details about the status of the business identifiers and their values.</p> <p data-bbox="865 405 1078 432">Recommendations</p> <p data-bbox="865 443 1442 499">Do not use a tracking variable to store information that might violate privacy rules or standards, such as:</p> <ul data-bbox="865 510 1451 688" style="list-style-type: none"> • Payment Card Industry (PCI) data security standards. • Health Insurance Portability and Accountability Act (HIPAA) privacy rules. • Personally identifiable information (PII) standards. • Any other sensitive data, such as passwords.
Ensure that your organization's data loss prevention policy includes guidance on creating backups of assets from Oracle Integration	 <p data-bbox="683 831 816 852">Instance users</p> <p data-bbox="643 932 849 1066">An instance user with the ServiceAdministrator can export any project</p> <p data-bbox="643 1077 849 1276">An instance user with the ServiceDeveloper can export a project if they have Edit permissions for the project</p> <p data-bbox="643 1287 849 1486">An instance user with the ServiceDeveloper can export individual integration artifacts outside a project</p>	<p data-bbox="865 705 1451 762">To protect against human error and insider threats, you have the following options:</p> <ul data-bbox="865 772 1476 1413" style="list-style-type: none"> • Take regular backups by exporting a project and all of its components regularly. See <i>Export a Project</i> in <i>Using Integrations in Oracle Integration 3</i>. • Take regular backups by exporting integration artifacts individually: <ul data-bbox="914 961 1476 1203" style="list-style-type: none"> – Integrations: See <i>Export an Integration</i> in <i>Using Integrations in Oracle Integration 3</i>. – Packages: See <i>Export a Package</i> in <i>Using Integrations in Oracle Integration 3</i>. – Lookups: See <i>Export a Lookup</i> in <i>Using Integrations in Oracle Integration 3</i>. – Library file: See <i>Export a Library File</i> in <i>Using Integrations in Oracle Integration 3</i>. • Clone an entire service instance. Most organizations choose this option when creating a new service instance, but you can also follow these steps to create an archive of your environment. See <i>Clone the Design-Time Metadata of an Entire Service Instance</i> in <i>Using Integrations in Oracle Integration 3</i>. <p data-bbox="865 1423 1403 1480">If you choose to export data, you're responsible for managing the exported data appropriately.</p> <p data-bbox="865 1491 1403 1543">If needed, you can import the exported integration artifacts into another instance.</p>

Security goal	Owner	More information
Send data intentionally to an external application	 <p data-bbox="683 373 813 394">Instance users</p> <p data-bbox="643 474 850 583">Instance users with the ServiceDeveloper role</p>	<p data-bbox="865 247 1365 275">About sending data to external applications</p> <p data-bbox="865 283 1446 340">You have several options for configuring connectivity to external applications. For example:</p> <ul data-bbox="865 348 1476 464" style="list-style-type: none"> <li data-bbox="865 348 1476 405">• Configuring a connection to an application using an adapter. <li data-bbox="865 413 1476 464">• Add an action for an Oracle Cloud Infrastructure (OCI) service. <p data-bbox="865 472 1101 499">Your responsibilities</p> <ul data-bbox="865 508 1476 684" style="list-style-type: none"> <li data-bbox="865 508 1382 564">• Determine when to send data to an external application. <li data-bbox="865 573 1395 627">• Send only the appropriate data to an external application. <li data-bbox="865 636 1476 684">• Configure the connection so that it conforms to your organization's security requirements. <p data-bbox="865 693 1166 720">See the following resources:</p> <ul data-bbox="865 728 1476 900" style="list-style-type: none"> <li data-bbox="865 728 1476 814">• For links to all adapter guides, see <i>Configure Connection Properties and Security Properties in Using Integrations in Oracle Integration 3</i>. <li data-bbox="865 823 1476 900">• For help using the OCI actions, see <i>OCI AI Services Category in Using Integrations in Oracle Integration 3</i>.