Oracle® Cloud

Securing Oracle Integration 3

F83200-01
September 2024

Oracle Cloud Securing Oracle Integration 3,

F83200-01

Primary Author: Oracle Corporation

Contents

3 Data Protection

Preface

This guide describes how to configure security for Oracle Integration.

Topics:

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 `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

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.
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 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

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	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: • Projects • File Server • Target systems that integrations connect to Users access an instance using its user interface or its built-in APIs. See: • Oracle Integration 3 REST API • File Server in Oracle Integration 3 REST API • OCI Process Automation REST API
Oracle Cloud Infrastructure Console	All organizations that use Oracle Integration have access to the Oracle Cloud Infrastructure Console. Here, users with the appropriate IAM (identity and access management) policies perform the following tasks: • Create and manage users, and control access to the Oracle Integration instance and its APIs. Perform these tasks in Oracle Cloud Infrastructure Identity and Access Management, which is available within the Oracle Cloud Infrastructure Console. 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. • Manage the lifecycle of the Oracle Integration instance. Users access the Oracle Cloud Infrastructure Console from the following: • Its user interface • Its APIs: See Oracle Integration API. These APIs are different from the Oracle Integration built-in APIs, described in the previous row. • 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	Access control focuses on two areas: • **Network access** Controlling network access involves routing and restricting the following traffic: – 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. See Control Network Access. • **User, client system, and connection access** Users, client systems, and connections require access to some or all of the following resources: – Oracle Integration instance: The service instance where you design, deploy, and monitor integrations. – Oracle Integration APIs: The built-in APIs and the customer-built APIs 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 Infrastructure Console, the Oracle Cloud Infrastructure lifecycle API, or the Oracle Cloud Infrastructure lifecycle CLI. You control access to resources through *authentication*, and you control the activities that can be performed through *authorization*. See Learn About Users and Resources and Control User, Client System, and Connection Access.
Data protection	Learn how to ensure that only authorized people can view data, and understand how to handle credentials appropriately. • 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 built-in APIs and the customer-built APIs
  - 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 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	• **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. • **Network access** All public traffic is terminated with one of the methods: – Customer-built APIs: TLS 1.2 or higher. – Built-in APIs: As set by the Oracle Cloud Infrastructure regional OpenID Connect (OIDC) proxy, TLS 1.2 or higher. You can restrict which networks have access to Oracle Integration instances by configuring an allowlist (formerly known as whitelist). See Restrict Access to an Instance in *Provisioning and Administering Oracle Integration 3*. Allowlists are also covered in this guide. See Control Network Access. • **Private endpoint** You can secure outbound traffic to specific resources by using a private endpoint. See Connect to Private Resources in *Provisioning and Administering Oracle Integration 3*. 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	• Oracle follows all the guidelines from Oracle Cloud Infrastructure Vault and Oracle Cloud Infrastructure Secrets for rotating the service instance encryption keys. • Oracle encrypts data at rest and data over wire. • 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: – 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. – 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 *Provisioning and Administering Oracle Integration 3*. 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

Manage Access

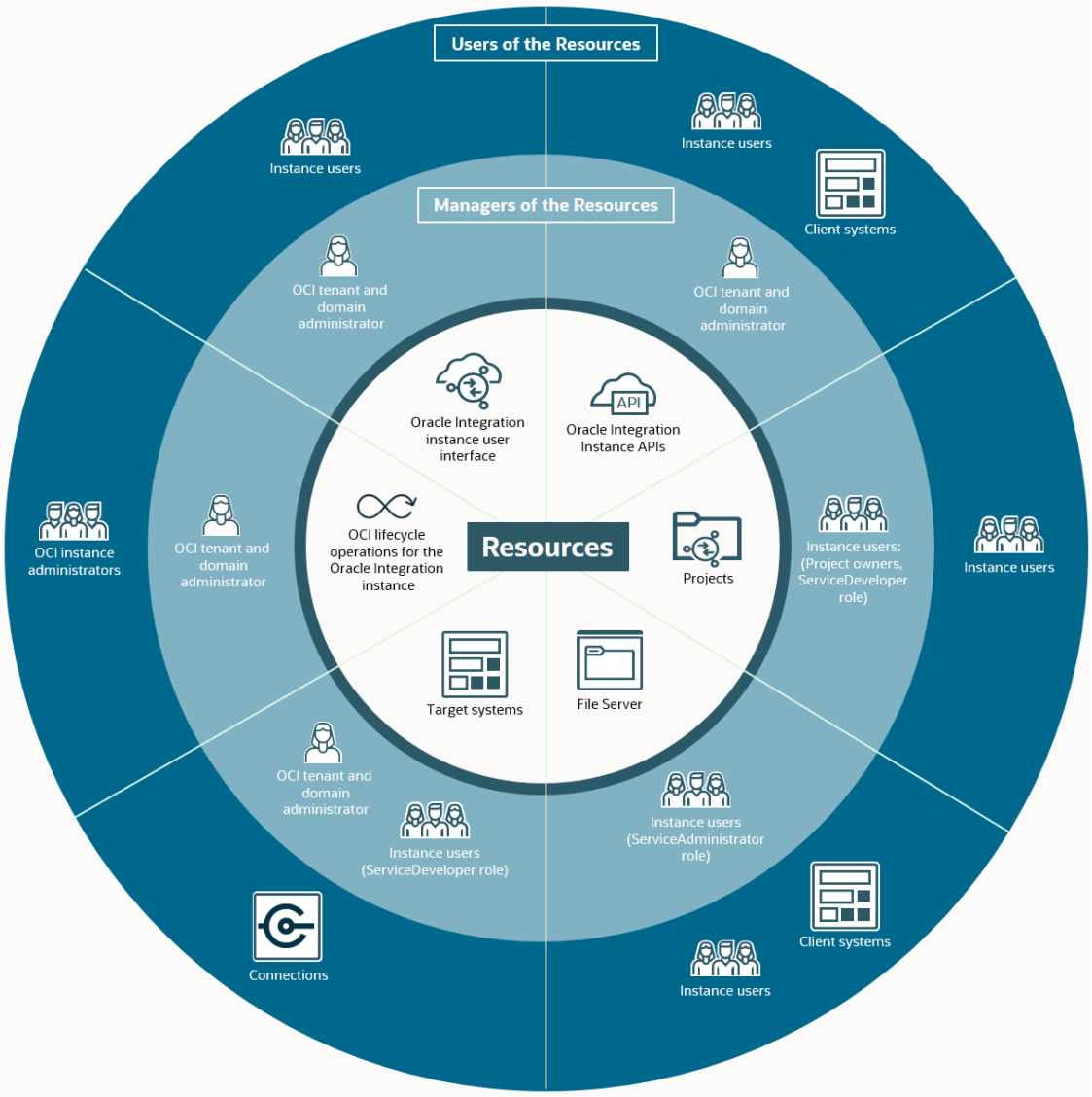
- Control Network Access
- Control User, Client System, and Connection Access

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
	The Oracle Integration instance user interface is the service instance where Oracle Integration users sign in and then design, deploy, and monitor integrations. Users have two ways to access an Oracle Integration instance: its user interface and its APIs.

Resource	Description
	The Oracle Integration instance APIs include the following types of APIs: • **Oracle Integration built-in APIs** The following APIs are the Oracle Integration built-in APIs: – Oracle Integration 3 REST API – File Server in Oracle Integration 3 REST API – OCI Process Automation REST API • **Customer-built APIs** A customer-built API is the API that Oracle Integration exposes when you activate an integration. Every activated integration has its own customer-built API. **Note:** The APIs for provisioning and administering an Oracle Integration instance are separate from the Oracle Integration APIs. The provisioning and administering APIs are part of the OCI (Oracle Cloud Infrastructure) lifecycle operations for the Oracle Integration instance entry in this table. Users have two ways to access an Oracle Integration instance: its user interface and its APIs.
	Projects are components within an Oracle Integration instance. 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 *Using Integrations in Oracle Integration 3*.
	File Server is an SFTP-compliant repository that is connected to an Oracle Integration instance. 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 *Using File Server in Oracle Integration 3*.
	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. Target systems can be Oracle services, third-party services, or applications that your organization has developed.

Resource	Description
	You perform Oracle Cloud Infrastructure (OCI) lifecycle operations for the Oracle Integration instance using the Oracle Cloud Infrastructure Console. You have the following options for accessing the Oracle Cloud Infrastructure Console: • User interface 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 *Provisioning and Administering Oracle Integration 3*. • Oracle Cloud Infrastructure lifecycle API The Oracle Cloud Infrastructure APIs include endpoints for every Oracle Cloud Infrastructure service that is accessible from the Oracle Cloud Infrastructure Console. – 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 lifecycle APIs, which allow you to manage the lifecycle of an Oracle Integration instance, see Oracle Integration API. • Oracle Cloud Infrastructure lifecycle CLI See Oracle Integration CLI.

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 Infrastructure Console through the user interface, APIs, or CLI	Works in the Oracle Integration instance through the user interface or built-in APIs
OCI tenant and domain administrator	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: • 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.	✓	✗
OCI instance administrators	This administrator manages the lifecycle of one or more Oracle Integration instances, including performing the following tasks: • 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 Infrastructure Console through the user interface, APIs, or CLI	Works in the Oracle Integration instance through the user interface or built-in APIs
 Instance users with one or more of the following service roles: • ServiceAdministrator • ServiceDeveloper • ServiceMonitor • ServiceDeployer • ServiceUser • ServiceInvoker • ServiceViewer	Users' service roles determine their access. Granular service roles are available. See Oracle Integration Service Roles in *Provisioning and Administering Oracle Integration 3*. Instance users have different responsibilities, depending on their roles. For example, they might be responsible for some or all of the following tasks: • Managing and administering the features provisioned in an Oracle Integration instance. • Designing integrations. • Controlling the people who can edit, view, and monitor the resources in a project. • Configuring the security of a connection that an integration uses to connect to an application. • Monitoring integrations. • Viewing information about integrations and other components.		

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
	For details about Oracle Cloud Infrastructure (OCI) administrators, see Managers of the Resources.

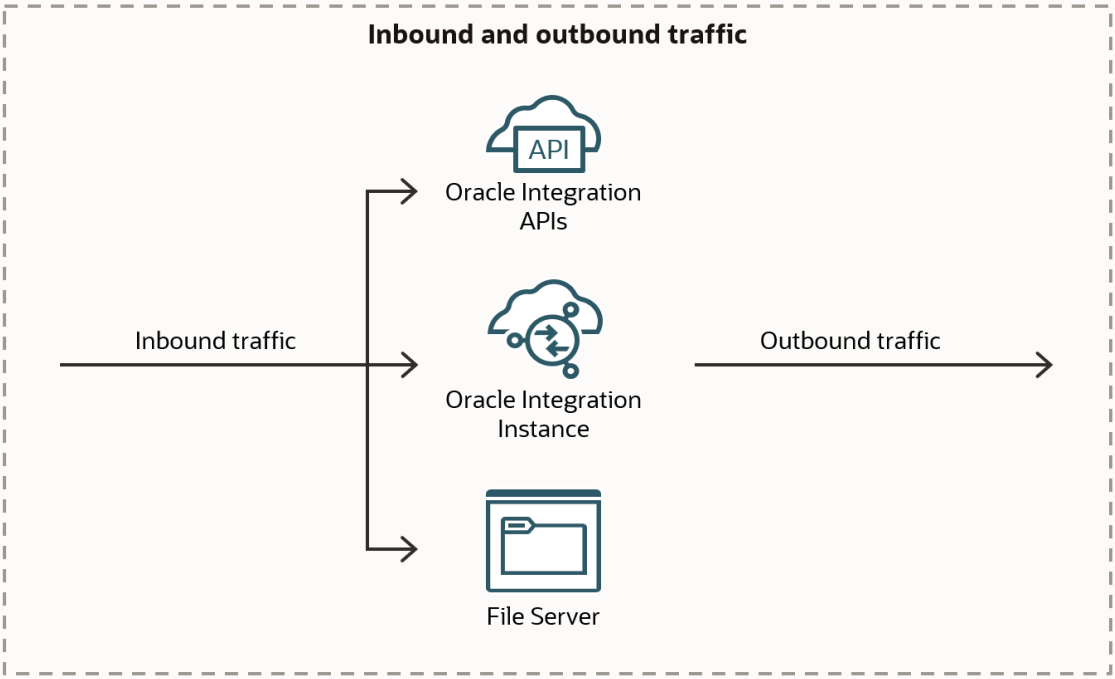
User or resource	Description
	See Managers of the Resources.
	An application that calls an integration in an Oracle Integration instance using a connection.
	The method that an Oracle Integration instance uses to connect to an application. Every connection is based on an adapter. For more information,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

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	Also called ingress traffic, this traffic originates *outside* Oracle Integration and goes to: • An Oracle Integration instance • The Oracle Integration APIs, including the built-in APIs and the customer-built APIs • File Server 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.
Outbound traffic	Also called egress traffic, this traffic originates *in an Oracle Integration instance* and goes to a target system.

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 *in the same region*	Traffic within a region is routed through a service gateway: • Inbound traffic 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. • Outbound traffic 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. To see the list of services that support service gateways, see Service Gateway: Supported Cloud Services.
Traffic across Oracle Cloud Infrastructure services that are *in different regions*	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	Inbound and outbound traffic that comes through an on-premises connectivity agent goes over the public internet. Inbound and outbound traffic that comes through FastConnect and VPN goes through the FastConnect link.
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 Oracle Integration's built-in APIs, the Oracle Integration customer-built APIs, 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		**About this traffic** 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. **How to achieve this goal** 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 Restrict Access to an Instance in *Provisioning and Administering Oracle Integration 3*. 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. **Notes** • 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		**About this traffic** Inbound traffic to Oracle Integration comes from the following sources: • 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). 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. **How to achieve this goal** 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 Restrict Access to an Instance in *Provisioning and Administering Oracle Integration 3*. 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		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 Create an Allowlist for Public IP Addresses in *Using File Server in Oracle Integration 3*.

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
Secure outbound traffic to endpoints that are in either of the following locations: • A virtual cloud network (VCN) in the same region as the Oracle Integration instance. • Endpoints that are *within* the Oracle Services Network and in the same region as the Oracle Integration instance.		**Secure this traffic using a private endpoint** 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). If the endpoint is public facing, you must also configure a private NAT gateway. **Learn more about private endpoints** 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 Connect to Private Resources in *Provisioning and Administering Oracle Integration 3*. **Your responsibilities** 1. 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. 2. Configure a private endpoint. See Configure a Private Endpoint for an Instance in *Provisioning and Administering Oracle Integration 3*.

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	**Download the connectivity agent installer:**  Instance users with the ServiceAdministrator role **Complete all other tasks:**  Other administrators complete these tasks in third-party applications and on virtual machines.	**Enable this traffic by using an agent-based configuration** 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. 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. 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. **Organizations that must use an agent-based configuration** Use an agent-based configuration if your organization has any of the following requirements: • An integration must connect to an on-premises application in your corporate network or an application in a private cloud. • 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. **Learn more about the connectivity agent** 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 *Using Integrations in Oracle Integration 3*. **Your responsibilities** 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 *Using Integrations in Oracle Integration 3*. 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 *Using Integrations in Oracle Integration 3*. 3. If desired, configure a FastConnect peering pattern. See Connection Patterns for Hybrid Integrations in *Using Integrations in Oracle Integration 3*.

Security goal	Owner	More information
Allow Oracle Integration to access endpoints that are *outside* the Oracle Services Network	**Obtain the IP address:**  Instance users with the ServiceAdministrator, ServiceDeveloper, ServiceUser, or ServiceViewer role **Update the allowlist:**  Other administrators work in third-party applications and on virtual machines.	If a target application has an allowlist enabled, update the allowlist so that Oracle Integration has access by completing the following steps: 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 *Provisioning and Administering Oracle Integration 3*. 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 Infrastructure 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

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

On This Page

Access at a Glance

Area	More information
People who need access	

Area	More information
Authentication method: **Login sessions**	To access the user interface of an Oracle Integration instance or the Oracle Cloud Infrastructure Console, people must sign in. To sign in, a user must be a member of an identity domain. The identity domain authenticates the user. To learn more, see Managing Identity Domains in the Oracle Cloud Infrastructure documentation.
Authorization method: **Service roles within the Oracle Integration application**	Service roles govern access to actions *within an Oracle Integration instance*, including actions that you perform using the Oracle Integration built-in APIs and customer-built APIs. See Oracle Integration Roles and Privileges in *Provisioning and Administering Oracle Integration 3*.

How to Control Access

Security goal	Owner	More information
Choose an identity and access management tool		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. 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. 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.
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		Use SAML 2.0 federation to federate Oracle Cloud Infrastructure IAM with your organization's existing identity and access management system See Federating with Identity Providers in the Oracle Cloud Infrastructure documentation.
Configure access		• If your tenancy uses identity domains, see Workflow for Access in an Identity Domain in *Provisioning and Administering Oracle Integration 3*. • If your tenancy doesn't use identity domains, see Workflow for Access Without an Identity Domain in *Provisioning and Administering Oracle Integration 3*.

Security goal	Owner	More information
Add an additional layer of security by enabling multifactor authentication (MFA)		**When to enable MFA** Oracle recommends enabling MFA only for users that access the Oracle Integration user interface. **When not to enable MFA** Do not enable MFA for user accounts that access REST APIs, including the Oracle Integration built-in APIs and the customer-built APIs. 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. **How to enable MFA** • 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 customer-built APIs using your REST clients. If you use Oracle Cloud Infrastructure IAM as your identity system, see Managing Multifactor Authentication in the Oracle Cloud Infrastructure documentation.

Oracle Integration Instance APIs: Control User and Client System Access

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

On This Page

Access at a Glance

Area	More information
People and systems that need access	 

Area	More information
Authentication method: **Several, depending on the API**	The APIs have different authentication methods: • Oracle Integration built-in REST APIs: **OAuth 2.0 token**, obtained on behalf of a user or cloud application. • Customer-built APIs: **Determined by the adapter** that builds the API. The adapter that you use as the trigger for an integration builds the integration's API.
Authorization methods: **Service roles**	The APIs have different authorization methods: • Oracle Integration 3 REST API and customer-built APIs: **Oracle Integration service roles**. See Oracle Integration 3 Service Roles in *Provisioning and Administering Oracle Integration 3*. • OCI Process Automation REST API: **Process Automation roles** and **process application roles**: – Process Automation roles provide *functional security*. See Process Automation Roles in *Administering Oracle Cloud Infrastructure Process Automation*. Process Automation roles control access to the administration and designer APIs. – Process application roles provide *data security*. See About Process Application Roles in *Using Oracle Cloud Infrastructure Process Automation*. Process application roles control access to the runtime APIs. The following list identifies the administration, designer, and runtime APIs in the OCI Process Automation REST API: – 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 In some situations, users have implicit access to resources, regardless of their roles. For instance: – 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. A user's access is a combination of their assigned roles and their implicit permissions. • File Server in Oracle Integration 3 REST API: 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	OCI tenant and domain administrator	Follow the guidance for the API that you need to access: • Oracle Integration REST APIs See OAuth Authentication in Oracle Integration in *REST API for Oracle Integration 3*. • OCI Process Automation REST APIs See Security, Authentication and Authorization in *REST API for Oracle Cloud Infrastructure Process Automation*. • File Server REST APIs See OAuth Authentication in Oracle Integration for File Server in *REST API for File Server in Oracle Integration 3*. • Customer-built REST APIs Oracle provides a guide for using each adapter. See Configure Connection Properties in *Using Integrations in Oracle Integration 3* for links to all adapter guides.
Provision the users who need to access the REST APIs	OCI tenant and domain administrator	• If your tenancy uses identity domains, see Workflow for Access in an Identity Domain in *Provisioning and Administering Oracle Integration 3*. • If your tenancy doesn't use identity domains, see Workflow for Access Without an Identity Domain in *Provisioning and Administering Oracle Integration 3*. If any users must access the customer-built-APIs, assign them the ServiceInvoker role.

Note:

Instance users, typically integration developers, are responsible for configuring connections to customer-built APIs. Afterwards, the developer uses the connection in an integration, finalizes the integration, and activates the integration. When the integration runs, Oracle Integration exposes the integration's customer-built APIs. These APIs 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

Area	More information
People who need access	
Authentication method: **Authentication method that is used by the user interface or APIs**	The way that you access a project determines your authentication method. You have the following options for accessing projects: • Through the Oracle Integration instance user interface. For details, see Oracle Integration Instance User Interface: Control User Access. • Through the Oracle Integration built-in REST APIs. For details, see Oracle Integration Instance APIs: Control User and Client System Access.
Authorization method: **Role-based access control**	Role-based access control governs access to a project and its integration components *within an Oracle Integration instance*, including actions that you perform using the Oracle Integration built-in APIs. Role-based access control, sometimes called RBAC, determines the users and groups who can edit, view, and monitor a project. Role-based access control can be *more restrictive* than a service role but can *never* give a user more permissions than a service role allows. For example: • 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. **Notes:** • 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	 Instance users with the ServiceAdministrator role, or project administrators with the ServiceDeveloper role	Assign role-based access control within each project. To learn about role-based access control, and to set up access, see Control Who Can Edit, View, and Monitor in a Project in *Using Integrations in Oracle Integration 3*.

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

Area	More information
People and systems that need access	 

Area	More information
Authentication method: **IP address, and either user login or public key**	**Ways that people connect to File Server:** • User interface in the Oracle Integration instance • File Server REST APIs • Supported SFTP client or an SFTP command line interface **Ways that integrations connect to File Server:** • File server action from within an integration • FTP Adapter **Authentication method for people and integrations** To access File Server, your IP address must be added to the File Server allowlist. Additionally, File Server authenticates access using either user logins or a public key.
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	 Instance users with the ServiceAdministrator role	See Configure File Server Settings in *Using File Server in Oracle Integration 3*.
Configure access to File Server	 Instance users with the ServiceAdministrator role	See Configure Users in *Using File Server in Oracle Integration 3*.

> **Note:**
>
> An integration can always connect directly to File Server using the File server action. You 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

Area	More information
Connections that need access	
Authentication and authorization methods: **Its own methods**	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. For details about the methods that each target system supports, see the documentation for the target system. For details about the methods that each adapter supports, see the adapter documentation. Oracle provides a guide for using each adapter. See Configure Connection Properties and Security Properties in *Using Integrations in Oracle Integration 3* for links to all adapter guides.

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	 Instance users with the ServiceDeveloper role	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. **For applications with adapters** 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. **For applications without adapters** 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 What Is the Rapid Adapter Builder? in *Using the Rapid Adapter Builder with Oracle Integration 3*. **See the adapter documentation** Oracle provides a guide for using each adapter. See Configure Connection Properties and Security Properties in *Using Integrations in Oracle Integration 3* for links to all adapter guides.
Write IAM (identity and access management) policies that give Oracle Integration access to the resources		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 *Using Integrations in Oracle Integration 3*: • 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

- How to Control Access

Access at a Glance

Area	More information
People who need access	
Authentication method: **Several methods**	One of the following methods: • **User interface authentication: User logins** To access the user interface of Oracle Integration or the Oracle Cloud Infrastructure 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 API, see Accessing Oracle Cloud Infrastructure in the Oracle Cloud Infrastructure documentation.
Authorization method: **IAM (identity and access management) policies**	Users access the Oracle Cloud Infrastructure Console using its user interface, its APIs, and its 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. 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. 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 *least* amount of access to the *most* amount of access: • `INSPECT` • `READ` • `USE` • `MANAGE` To learn more about IAM policies in general, see the following pages in the Oracle Cloud Infrastructure documentation: • Getting Started with Policies • How Policies Work • Example Scenario To learn about IAM policies for Oracle Integration, including the verbs to use when writing an IAM policy, see About IAM Policies for Oracle Integration in *Provisioning and Administering Oracle Integration 3*.

How to Control Access

Security goal	Owner	More information
Understand your responsibilities and Oracle's responsibilities for various administrative tasks	OCI tenant and domain administrator	The tenancy administrator receives the welcome email from Oracle and is responsible for managing the lifecycle operations on the instance. See Oracle and Customer Responsibilities in Oracle Integration 3 in *Provisioning and Administering Oracle Integration 3*.
Determine whether your tenancy uses identity domains	OCI tenant and domain administrator	Some tenancies use identity domains, while others don't. You have different requirements, depending on whether your tenancy uses identity domains. To understand the differences between tenancies with and without identity domains, and to determine whether your tenancy uses identity domains, see Differences Between Tenancies With and Without Identity Domains in *Provisioning and Administering Oracle Integration 3*.
Configure access to the Oracle Integration instance	OCI tenant and domain administrator	• If your tenancy uses identity domains, see Workflow for Access in an Identity Domain in *Provisioning and Administering Oracle Integration 3*. • If your tenancy doesn't use identity domains, see Workflow for Access Without an Identity Domain in *Provisioning and Administering Oracle Integration 3*.
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	OCI tenant and domain administrator	You can send activity stream data to Oracle Cloud Infrastructure Logging. See Logging in the Oracle Cloud Infrastructure documentation. You can send message pack data to Oracle Cloud Infrastructure Monitoring. See Monitoring in the Oracle Cloud Infrastructure documentation. Ensure that you authorize only the correct people to view the logs and other data. Associate a policy with the log or log group. The policy should allow only select viewers.
Periodically audit users' access to the Oracle Integration instance	OCI tenant and domain administrator	

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		**About user credentials** User credentials consist of a user name and password that people use to sign in to Oracle Integration, including File Server. 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. See IAM Credentials. **Guidelines for handling credentials** See IAM Credentials.

Security goal	Owner	More information
Limit the people who can access connection credentials	**Create the credentials:**  **Provide the credentials while configuring a connection:**  Instance users with the ServiceDeveloper role	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. 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 Oracle Cloud Infrastructure Vault. **Your responsibilities** You are responsible for securely handling credentials outside Oracle Integration. Oracle recommends limiting the people who can access the credentials.

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	 Instance users with the ServiceAdministrator role, or project administrators with the ServiceDeveloper role	**About design-time log data** 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. To learn more, see View the Design-Time Audit in *Using Integrations in Oracle Integration 3*. **How to secure access** For integrations that are outside a project, all log data is visible to anyone who can sign in to the Oracle Integration instance. 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.

Security goal	Owner	More information
Secure access to runtime auditing information	 Instance users with the ServiceAdministrator role, or project administrators with the ServiceDeveloper role	**About the activity stream** 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. **Different tracing levels are available** Several levels of tracing are available for the activity stream. The tracing level determines the following information: • The amount of information that appears in the activity stream. • The amount of time that the activity stream persists for an integration instance within Oracle Integration. **If you need to keep the data for longer** 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 Infrastructure Console. See Capture the Activity Stream of Integrations in the Oracle Cloud Infrastructure Console in *Provisioning and Administering Oracle Integration 3*. **Your responsibilities** • 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. 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. See Activate an Integration in *Using Integrations in Oracle Integration 3*. • Be aware that integrations that involve sensitive data could result in payload tracking that violates one or more of the following rules and standards: – Payment Card Industry (PCI) data security standards. – Health Insurance Portability and Accountability Act (HIPAA) privacy rules. – Personally identifiable information (PII) standards. To review Oracle's recommendations, see Activate an Integration in *Using Integrations in Oracle Integration 3*.

Security goal	Owner	More information
Keep sensitive data out of tracking variables	 Instance users with the ServiceDeveloper role	**About tracking variables** 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. **Recommendations** Do not use a tracking variable to store information that might violate privacy rules or standards, such as: • 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	 An instance user with the ServiceAdministrator can export any project An instance user with the ServiceDeveloper can export a project if they have Edit permissions for the project An instance user with the ServiceDeveloper can export individual integration artifacts outside a project	To protect against human error and insider threats, you have the following options: • Take regular backups by exporting a project and all of its components regularly. See Export a Project in *Using Integrations in Oracle Integration 3*. • Take regular backups by exporting integration artifacts individually: – Integrations: See Export an Integration in *Using Integrations in Oracle Integration 3*. – Packages: See Export a Package in *Using Integrations in Oracle Integration 3*. – Lookups: See Export a Lookup in *Using Integrations in Oracle Integration 3*. – Library file: See Export a Library File in *Using Integrations in Oracle Integration 3*. • 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 Clone the Design-Time Metadata of an Entire Service Instance in *Using Integrations in Oracle Integration 3*. If you choose to export data, you're responsible for managing the exported data appropriately. If needed, you can import the exported integration artifacts into another instance.