Oracle® Cloud

Using Oracle Agent Hub

G58186-01
November 2026

Oracle Cloud Using Oracle Agent Hub,

G58186-01

Copyright © 2026, Oracle and/or its affiliates.

Primary Author: Stefanie Rhone

Contributors: Oracle Analytics development and product management.

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.

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.

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Contents

1 Get Started with Oracle Agent Hub

What is Oracle Agent Hub? 1
Why Use Agent Hub? 1
How Does Agent Hub Fit with Oracle AI Data Platform? 2
Glossary 3

2 Understand How Agent Hub Works

How Enterprise AI Works in Agent Hub 1
How Agent Hub Processes Requests 2
AI Resources Supported by Agent Hub 3
How Enterprise AI Resources Become Available 4
How Agent Hub Supports Interoperability 5
A2UI Components Supported In Agent Hub 6
How Agent Hub Uses Large Language Models (LLMs) 9

3 Understand How Agent Hub Manages Access

About the Agent Hub Access Model 1
Understand Topic-Based Access 2
Understand Agent Hub Users and Administrators 3

4 Start Using Agent Hub

How to Open Agent Hub 1
- Open Agent Hub from a URL 1
- Open Agent Hub from AI Data Platform 1

Ways to Start a Chat 2
- Enter a Prompt 2
- Select an Agent 3
- Select a Topic 4

Write Effective Prompts 5
Continue a Chat 6

Copyright © 2026, Oracle and/or its affiliates.

5 Work with Agent Hub

About the Agent Hub Interface 1
Find and Select AI Resources 2
Understand How Topics Affect a Chat 3
How to Work with Files 4
Understand Working with Files 4
Upload a File to a Chat 5
Manage Chat History 6
Understand Responses and Agent Behavior 6
Understand Approvals in Agent Hub 8
Understand Request Activity 9
Manage Your Profile Settings 9

6 Create and Manage Topics

What Are Topics? 1
Guidelines for Creating Topics 2
Create and Configure a Topic 4
Modify a Topic 7
How to Work with Topic Access 8
Grant Users or Roles Access to a Topic 9
Change or Revoke Topic Access 9
Remove a Topic 10

7 Administer Agent Hub

About Agent Hub Administration 1
Configure the Agent Hub Model 1
Understand Agent Hub Model Configuration 1
Configure the Processing Region and Model 2
Configure Agent Hub Guardrails 3
Understand Agent Hub Guardrails 3
Configure Agent Hub Guardrails 4
Manage Access to Resources and Features in Agent Hub 5
Understand Agent Hub Administration and Access Responsibilities 5
Grant Access to the Topics Feature 7
Change or Revoke Access to the Topics Feature 8

8 Agent Hub Known Issues

Copyright © 2026, Oracle and/or its affiliates.

9 Agent Hub Frequenty Asked Questions

Access Agent Hub and AI Resources FAQs 1
Work with Agent Hub FAQs 2
Administer Agent Hub FAQs 3

Copyright © 2026, Oracle and/or its affiliates.

About This Content

This guide describes how to discover, access, use, and administer enterprise AI resources in Oracle Agent Hub.

Audience

This guide is intended for business users and Agent Hub administrators who use Oracle Agent Hub to:

- Discover and interact with their enterprise AI resources.
- Manage topics and topic-based access.
- Administer permissions and the Agent Hub experience for users.

Related Resources

See these Oracle resources:

- Introduction to Oracle AI Data Platform

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.

Copyright © 2026, Oracle and/or its affiliates.

1

Get Started with Oracle Agent Hub

This chapter introduces Oracle Agent Hub and explains how it provides a unified experience for users to discover and interact with their enterprise's AI resources.

Topics:

- What is Oracle Agent Hub?
- Why Use Agent Hub?
- How Does Agent Hub Fit with Oracle AI Data Platform?
- Glossary

What is Oracle Agent Hub?

Oracle Agent Hub provides a unified interface for discovering, accessing, and interacting with enterprise AI across your organization. It enables users to communicate with enterprise AI resources, such as agents, MCP servers, and tools, through a conversational experience, regardless of where those resources were developed or deployed.

> **Note**
>
> In this guide, *enterprise AI* refers to the AI resources that your organization develops, governs, and makes available to users through Agent Hub.

Agent Hub simplifies how users work with AI by bringing together AI resources from Oracle AI Data Platform, Oracle applications such as Fusion Applications, and supported external environments into a single application. Rather than requiring users to determine which AI resource is best suited to a task, users can ask questions or request assistance in Agent Hub, which helps connect them with the appropriate AI resource.

Organizations can use Agent Hub to provide a consistent AI experience across departments and business processes. For example, users can work with agents that help analyze financial information, answer procurement questions, assist with recruiting activities, or automate common business tasks.

Agent Hub works with AI Data Platform and the AI Registry to provide access to supported enterprise AI resources. AI Data Platform provides the underlying platform services, the AI Registry is a central location for all enterprise agents and provides registration and discovery, and Agent Hub provides the experience where users discover and interact with the resources available to them.

Why Use Agent Hub?

Agent Hub provides a centralized experience for discovering, accessing, and interacting with enterprise AI resources. Agent Hub brings AI resources together in a single application to help organizations boost AI adoption, simplify how users work with AI, and support enterprise governance.

Copyright © 2026, Oracle and/or its affiliates.

Agent Hub provides these benefits:

Unified AI Experience

Agent Hub provides a single interface for interacting with AI resources across the enterprise. Instead of accessing multiple AI applications or services, users can discover and interact with available AI resources from one location using a consistent conversational experience.

Cross-Platform AI Resource Access

Organizations can make AI resources available through Agent Hub regardless of where those resources were developed or deployed. Agent Hub supports AI resources developed or hosted in AI Data Platform and supported external environments, enabling users to access enterprise AI without switching between applications.

Increased Productivity

Agent Hub enables users to complete business tasks through natural language conversations with AI resources. Users can ask questions, retrieve information, receive recommendations, and complete business processes from a single application, reducing the time required to locate information or perform repetitive tasks.

Enterprise Governance

Agent Hub works with AI Data Platform and the AI Registry to support governed access to enterprise AI. Organizations can use role-based access control (RBAC), resource permissions, and topic access to help ensure that users can discover and interact only with the resources appropriate for them.

Enterprise AI Adoption

Agent Hub is designed to support the growing use of AI across your enterprise. Organizations can add new AI resources over time while continuing to provide users with a consistent interface for discovering and interacting with AI services. Support for open standards, such as Agent2Agent (A2A) and Model Context Protocol (MCP), helps organizations integrate supported AI resources from different environments.

How Does Agent Hub Fit with Oracle AI Data Platform?

Oracle Agent Hub, Oracle AI Data Platform, and the AI Registry work together to enable organizations to develop, manage, and use enterprise AI.

- **AI Data Platform**: Provides the underlying platform and services used to develop, deploy, manage, and govern enterprise AI resources.
- **AI Registry**: Provides the registration and discovery layer for supported AI resources. It enables resources developed in AI Data Platform or supported external environments to be registered and made discoverable for use through Agent Hub and other applications.
- **Agent Hub**: Provides the user experience where business users discover and interact with the enterprise AI resources available to them.

This separation enables developers and administrators to manage the underlying enterprise AI environment independently from the experience that business users use to accomplish their work. As new resources are developed or registered, they can become available through Agent Hub without requiring users to understand where those resources were developed or how they're managed.

Copyright © 2026, Oracle and/or its affiliates.

Why this matters

Agent Hub is designed to simplify how users interact with enterprise AI rather than how the organization builds and manages its AI resources. Users can focus on the work they want to accomplish while AI Data Platform, the AI Registry, and Agent Hub work together to provide access to the appropriate enterprise AI resources.

See How Enterprise AI Works in Agent Hub.

Glossary

Use this glossary to find definitions of Agent Hub terms and related AI Data Platform concepts that you encounter while using Agent Hub or reading this guide.

- **A2A** - Agent2Agent (A2A) is an open protocol that enables AI agents to discover and interact with one another. An agent's A2A metadata enables the agent to be registered and discovered.
- **A2A agent card** - An agent card contains metadata describing an agent, including its name, description, and skills. It supports agent discovery and interoperability.
- **A2UI** - Agent to UI (A2UI) is a structured user interface protocol that enables an agent to return interactive user interface components in addition to text.
- **Agent flow** - Agent flow is the code or visual definition that coordinates a model, instructions, and tools.
- **Agent Hub administrator** - An Agent Hub administrator is a user who administers Agent Hub configuration and functionality.
- **AI agent** - An AI agent is an AI resource designed to perform particular tasks or provide specialized knowledge and capabilities.
- **AI compute** - AI compute is the runtime capacity attached to an agent flow for deployment.
- **Oracle AI Data Platform** - AI Data Platform provides the environment where agents are built and deployed. Also provides platform services used by Agent Hub.
- **AI Registry** - A central enterprise registry for registering and discovering supported AI resources developed in Oracle AI Data Platform or supported external environments. Registered resources can be made available for use through Agent Hub and other applications.
- **AI Resources** - The AI capabilities that an organization makes available for use through Agent Hub, including agents, MCP servers, and tools.
- **Business user** - A business user is a user who uses Agent Hub to interact with the enterprise AI resources available to them.
- **Checkpointer** - A checkpointer provides conversation-scoped state storage used to retain multi-turn context.
- **Deployment** - A deployment is a runnable TEST or PROD endpoint created from an agent flow.
- **Direct response** - A direct response is a response that Agent Hub provides from its configured model without routing the request to a registered agent.
- **Enterprise AI** - Enterprise AI refers to the AI capabilities that an organization develops, manages, and makes available for business use.
- **Guardrails** - Guardrails are controls designed to protect AI interactions by detecting or preventing specified types of unwanted content or behavior.

Copyright © 2026, Oracle and/or its affiliates.

- **Knowledge base** - A knowledge base contains indexed documents that a retrieval-augmented generation tool can use to retrieve relevant evidence.
- **Large language model (LLM)** - An AI model that can understand and generate natural language. Agent Hub uses a configured LLM to support orchestration and provide direct responses when a request doesn't require a specialized agent.
- **MCP server** - A server that exposes tools through Model Context Protocol (MCP) so that agents and other supported functionality can discover and call them.
- **Model Context Protocol (MCP)** - Model Context Protocol (MCP) is a standard interface through which an agent can discover and call external tools.
- **Orchestrator** - An Agent Hub component that evaluates a user's request and determines how to handle it. The orchestrator can route requests to appropriate agents or tools, present agents for user selection, or provide a direct response using the configured large language model (LLM).
- **Prompt** - A prompt is a question, instruction, or request that a business user enters in Agent Hub.
- **Registry** - The Registry is the page in Agent Hub where business users browse and discover the agents, topics, and other supported AI resources available to them.
- **Retrieval-augmented generation (RAG)** - Retrieval-augmented generation (RAG) is a technique in which a model generates a response using information retrieved from a knowledge base.
- **Role-based access control (RBAC)** - Role-based access control (RBAC) controls access to functionality and resources based on roles and associated permissions.
- **Session variable** - A session variable is client-provided runtime metadata delivered separately from the user's prompt.
- **SQL tool** - A SQL tool provides a configured way for an agent to query registered data.
- **Thinking Activity** - A panel that the user can display during a chat. The panel provides a high-level view of request processing, including processing status, elapsed time, and information about agents or tools invoked during a request.
- **Tool** - A tool provides a capability that an agent or other supported Agent Hub functionality can use to perform a task or interact with another system.
- **Topic** - A topic groups related agents and tools around a particular business area or purpose. When a user starts a chat from a topic, the topic narrows the set of agents and tools the orchestrator can use to process the request.
- **User role** - A user role defines a set of permissions associated with a user's responsibilities or activities.

Copyright © 2026, Oracle and/or its affiliates.

2

Understand How Agent Hub Works

This chapter provides the key concepts, relationships, and high-level request flow you need to understand before using Agent Hub.

Topics:

- How Enterprise AI Works in Agent Hub
- How Agent Hub Processes Requests
- AI Resources Supported by Agent Hub
- How Enterprise AI Resources Become Available
- How Agent Hub Supports Interoperability
- A2UI Components Supported In Agent Hub
- How Agent Hub Uses Large Language Models (LLMs)

How Enterprise AI Works in Agent Hub

Agent Hub is the part of your enterprise AI environment where users discover and interact with the AI resources available to them. Agent Hub works with AI Data Platform and the AI Registry to provide a unified experience for accessing enterprise AI.

AI Data Platform, the AI Registry, and Agent Hub serve different purposes:

Component	Purpose
AI Data Platform	Provides the platform and services used to build, deploy, manage, and govern enterprise AI resources.
AI Registry	Provides the registration and discovery layer that makes supported AI resources available for use outside the environment where they were developed.
Agent Hub	Provides the conversational experience where users discover and interact with the enterprise AI resources available to them.

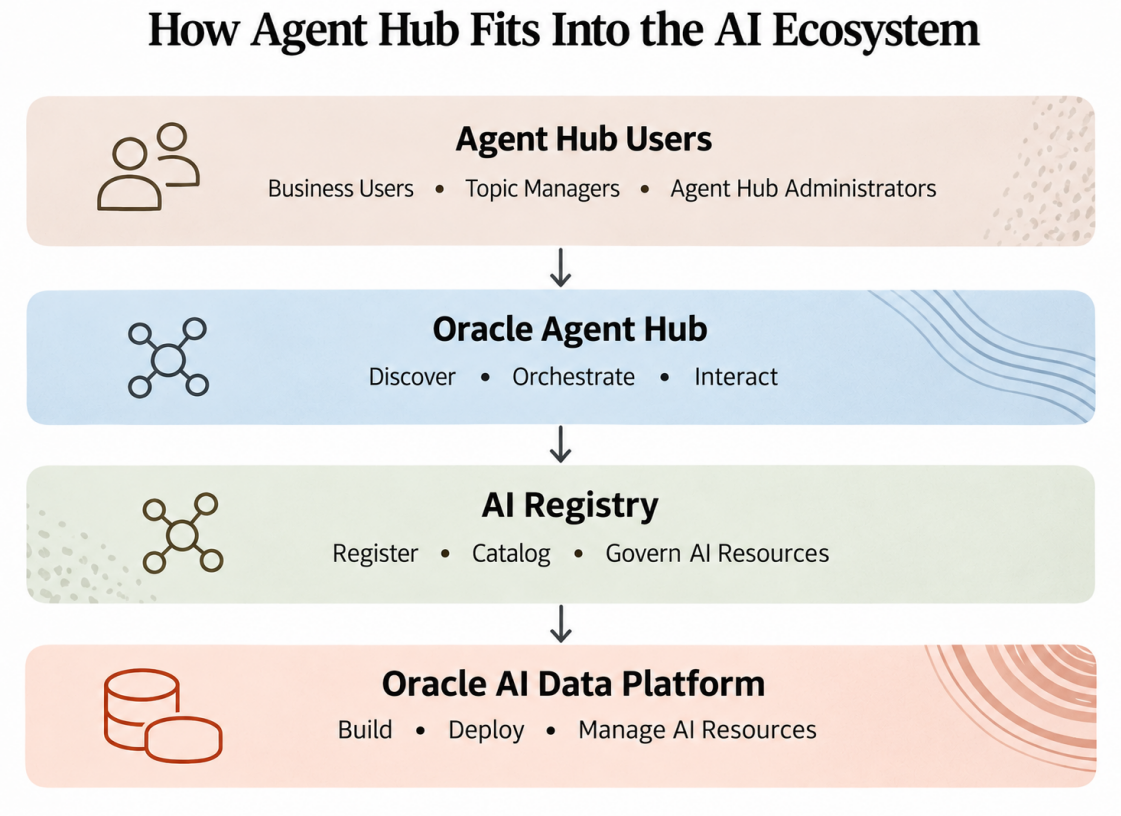
For example, an agent built in AI Data Platform is deployed and then registered in the AI Registry before it can become available for use in Agent Hub. Deployment makes the agent runnable, while registration makes it discoverable.

AI resources don't have to be developed in AI Data Platform. The AI Registry can also register supported external agents and MCP servers, enabling organizations to make AI resources from different environments available through Agent Hub.

Instead of requiring you to understand where an AI resource was developed or how it's managed, Agent Hub focuses on helping you accomplish your business tasks. You can select an available AI resource yourself or describe what you want to accomplish and let Agent Hub determine how to handle your request.

Copyright © 2026, Oracle and/or its affiliates.

The following diagram shows how AI Data Platform, the AI Registry, and Agent Hub work together to make enterprise AI resources available to Agent Hub users.



Why this matters

Agent Hub separates the business-user experience from the underlying AI platform and resource management. This allows your organization to continue developing, registering, governing, and expanding its enterprise AI resources while providing you with a consistent experience for discovering and using them.

For more information about the AI resources that you can use in Agent Hub, see AI Resources Supported by Agent Hub.

For information about how these resources are made available, see How Enterprise AI Resources Become Available.

How Agent Hub Processes Requests

Agent Hub uses an orchestrator to evaluate your request and determine how to handle it. The orchestrator helps connect your request with an appropriate AI capability without requiring you to know which agent or capability to use.

> **Note**
>
> Agent Hub orchestration uses AI models, and the tokens it consumes are billed in AIDP Units.

Copyright © 2026, Oracle and/or its affiliates.

When you enter a prompt without first selecting an agent, the orchestrator evaluates your request and the AI resources available to you. It continues to evaluate each new request as the conversation progresses. Depending on the request, Agent Hub can handle it in the following ways:

- **Route the request to an agent**: The orchestrator identifies one agent whose capabilities match your request and routes the request to that agent.
- **Present agents for selection**: If Agent Hub recommends multiple agents, you can use the suggested agent or choose another recommended agent.
- **Invoke a tool**: If the orchestrator identifies a tool that can handle your request, Agent Hub invokes the tool to perform the appropriate action.
- **Provide a direct response**: If your request doesn't require an additional AI capability, the orchestrator can provide a response directly using the configured large language model (LLM).

When you start a chat without selecting or tagging a particular agent, different agents can handle successive requests within the same conversation. For example, one agent might investigate a business issue, while another agent handles a follow-up request about how to address it.

When routing a request to a different agent, the orchestrator can provide relevant information from earlier in the conversation. The information available to the agent depends on what the orchestrator provides and how the agent processes it.

Depending on your approval setting, Agent Hub might ask you to select an agent before continuing or automatically use the agent it identifies as the best match.

To see which agent or tool Agent Hub invoked while processing your request, click the processing status indicator (for example, "Completed in 18s") in the chat to open the Thinking Activity panel.

To identify relevant agents, the orchestrator uses descriptive information from registered Agent Cards, including an agent's name, description, and skills. Clear and complete Agent Card information helps Agent Hub match requests with appropriate agents.

If you select or tag an agent when starting a chat, that agent remains associated with the conversation. You can't replace the selected agent within the same chat, although relevant MCP tools can still be invoked.

If you start the chat from a topic, the topic narrows the resources that Agent Hub considers when determining how to handle your request. See Understand How Topics Affect a Chat.

Why this matters

You don't need to know which agent is best suited to every task before you start a conversation. You can describe what you want to accomplish and let Agent Hub help connect your request with an appropriate AI capability.

AI Resources Supported by Agent Hub

Agent Hub works with different types of enterprise AI resources to help you complete tasks, access information, and interact with business systems. The way a resource is used depends on its type.

This table describes the types of AI resources that Agent Hub supports and how they're used.

Copyright © 2026, Oracle and/or its affiliates.

AI Resource	Description	How It's Used
Agent	An AI resource designed to provide specialized knowledge or perform particular business tasks.	You can discover and select an agent directly, or enter a prompt and let Agent Hub identify an appropriate agent for your request.
MCP server	A Model Context Protocol (MCP) server that exposes a set of tools through a standard interface.	An MCP server exposes tools that can be made available for use in Agent Hub. Users don't discover or select MCP servers directly from the Registry.
Tool	A capability that an agent or other supported Agent Hub functionality can use to access information, perform a task, or interact with another system.	Agent Hub can identify an appropriate tool when processing a request. Users don't discover or select tools from the Registry in the same way that they discover and select agents.

Agents from Different Environments

Agents available through Agent Hub can originate from AI Data Platform or supported external environments. Agent Hub supports the Agent2Agent (A2A) protocol, which enables interoperability between agents developed using different platforms and technologies.

An external agent is hosted outside AI Data Platform and registered with the AI Registry by using its Agent Card URL. After registration, an external agent can be used in Agent Hub subject to the applicable access permissions.

For more information about A2A and other supported standards, see How Agent Hub Supports Interoperability .

How AI Resources Work Together

AI resources can work together to process a request. For example, you might interact with an agent that uses a tool exposed by an MCP server to retrieve information or perform an action. You don't necessarily interact directly with every resource involved in processing your request. Some resources provide capabilities that agents use behind the scenes.

For information about how Agent Hub determines how to handle your request, see How Agent Hub Processes Requests.

For information about how your organization's AI resources become available in Agent Hub, see How Enterprise AI Resources Become Available.

How Enterprise AI Resources Become Available

Before users can discover and use an enterprise AI resource in Agent Hub, the resource must be prepared and registered for use and users must have the appropriate access.

Enterprise AI resources can originate from AI Data Platform or supported external environments. The AI Registry provides the registration and discovery layer that makes supported resources available for use through Agent Hub.

For example, an agent built in AI Data Platform must be deployed before it can be registered. Deployment makes the agent runnable by creating an endpoint. Registration publishes

Copyright © 2026, Oracle and/or its affiliates.

information about the agent to the AI Registry so that it can be discovered and used outside its development environment.

The AI Registry supports registration of agents built in AI Data Platform, supported external agents, and MCP servers.

Registration doesn't by itself give users access to a resource. Your organization must also configure the appropriate access before you can discover or use the resource in Agent Hub.

Enterprise AI Resource Flow

This process flow explains how your enterprise AI resources are made available in Agent Hub.

Resource Stage	Description
Create or provide	Developers create supported AI resources in AI Data Platform or make supported externally hosted resources available for registration.
Deploy	For agents built in AI Data Platform, developers deploy the agent to create a runnable endpoint.
Register	An administrator registers the supported resource in the AI Registry. Registration makes the resource discoverable outside its development environment.
Grant access	Administrators configure the permissions required for users to discover and use the resource.
Discover	Users discover the enterprise AI resources available to them through Agent Hub.
Use	Users interact with their available enterprise AI resources through Agent Hub.

Why this matters

Agent Hub separates the experience of using enterprise AI from the systems used to develop, register, and manage those resources. Your organization can continue adding and managing AI resources from different supported environments while providing users with a consistent experience for discovering and using the resources available to them.

For information about the types of resources Agent Hub supports, see AI Resources Supported by Agent Hub.

For information about how access determines which resources you can discover and use, see About the Agent Hub Access Model.

How Agent Hub Supports Interoperability

Enterprise AI environments can include agents and other AI resources developed using different platforms and technologies. Agent Hub and the AI Registry support open standards that enable these resources to work with the Oracle enterprise AI environment.

These standards provide different types of interoperability:

Standard	Purpose
Agent2Agent (A2A)	Provides a protocol and metadata model for describing and connecting agents.
Model Context Protocol (MCP)	Provides a standard interface through which agents can discover and call tools.

Copyright © 2026, Oracle and/or its affiliates.

Standard	Purpose
Agent-to-UI (A2UI)	Enables agents to describe interactive user interfaces that Agent Hub can render using supported components.

These standards help separate the Agent Hub user experience from the underlying implementation of the agents and other resources that support it.

Agent2Agent (A2A)

A2A provides a standard way to describe and connect agents. An Agent Card contains metadata that describes an agent, including its name, description, and skills. The AI Registry uses this information when an agent is registered, and Agent Hub can use descriptive agent information during orchestration to identify agents that are relevant to a user's request.

Model Context Protocol (MCP)

MCP provides a standard interface for exposing tools that agents can discover and call. An MCP server can expose multiple tools, and the tools selected when the server is registered become available for supported use in the platform.

Agent-to-UI (A2UI)

A2UI enables an agent to describe an interactive user interface as structured information. Agent Hub renders that information using supported user interface components rather than receiving executable user interface code from the agent. An A2UI response can include interactive elements such as forms, controls, charts, and other supported components in addition to conversational text.

Agent Hub supports A2UI responses from supported high-code agents.

For information about the user interface components that Agent Hub supports, see A2UI Components Supported In Agent Hub.

Why this matters

These interoperability standards enable your organization to integrate supported AI resources from different environments while providing users with a consistent Agent Hub experience.

For information about the AI resources supported by Agent Hub, see AI Resources Supported by Agent Hub.

For information about how resources are registered and made available, see How Enterprise AI Resources Become Available.

A2UI Components Supported In Agent Hub

Agent-to-UI (A2UI) enables supported agents to provide interactive user interface components in Agent Hub in addition to conversational text.

Agents can use supported A2UI components to collect user input, present information and choices, trigger actions, organize content, and visualize data directly within a conversation.

An agent provides structured information that describes the user interface, and Agent Hub renders that information using its supported A2UI components.

Copyright © 2026, Oracle and/or its affiliates.

> **Note**
>
> A2UI is supported in high-code agents only.

Standard Components

Agent Hub supports these standard A2UI components for presenting information, collecting user input, selecting options, triggering actions, and organizing content:

Component	Purpose	Description
`AudioPlayer`	Present audio	Provides a player for audio content.
`Button`	Trigger actions	Provides a button that users can select to perform an action.
`Card`	Organize content	Groups content within a card.
`CheckBox`	Present choices	Allows users to select or clear a single checked or unchecked value.
`ChoicePicker`	Present choices	Displays options from which users can make a single or multiple selection.
`Column`	Organize content	Arranges component vertically.
`DateTimeInput`	Collect input	Allows users to select a date, time, or both.
`Divider`	Organize Content	Displays a separator between content areas.
`Icon`	Present visual indicators	Displays an icon to represent an action or information.
`Image`	Present image	Displays an image from a specified URL.
`List`	Organize content	Arranges a collection of components in a list.
`Modal`	Present information	Displays content in a modal dialog.
`Row`	Organize content	Arranges components horizontally.
`Slider`	Collect input	Allows users to select or adjust a value within a defined range.
`Tabs`	Organize content	Organizes content into separate tabbed sections.
`Text`	Present information	Displays text with supported formatting and styles.
`TextField`	Collect input	Provides a field for entering short text, longer text, numbers, or obscured input.
`Video`	Present video	Displays video content from a specified URL.

Copyright © 2026, Oracle and/or its affiliates.

Custom Oracle JET Components

Agent Hub supports these custom Oracle JET components for presenting information, collecting user input, organizing content, triggering actions, and visualizing data:

Component	Purpose	Description
`OAActionCard`	Trigger actions	Displays content in a card that users can select to perform an action.
`OAChart`	Visualize data	Displays data using supported chart types, such as bar, line, pie, and scatter charts.
`OACombobox`	Present choices	Provides a field for selecting values from a set of options.
`OACollapsible`	Organize content	Displays sections that users can expand or collapse.
`OADataGrid`	Present tabular data	Displays data in a grid with configurable rows and columns.
`OAListView`	Present collections	Displays a collection of items in a list or card layout, with supported selection options.
`OAPopup`	Present information	Displays additional content in a popup associated with a UI element.
`OAProgressBar`	Show progress	Displays progress using a horizontal or vertical bar.
`OAProgressCircle`	Show progress	Displays progress using a circular indicator.
`OARadioSet`	Present choices	Allows users to select an option from a group of radio buttons.
`OASplitMenuButton`	Trigger actions	Combines a primary action button with a menu of additional actions.
`OASwitch`	Present choices	Provides a switch for turning an option on or off.
`OATruncatingText`	Present text	Displays text with configurable truncation and wrapping behavior.

Supported Chart Types

The OAChart component supports these chart types for visualizing data in Agent Hub:

Component	Purpose	Description
Area	Show trends	Displays values using filled areas to emphasize patterns and changes.
Bar	Compare values	Compares values across categories using bars.
Bubble	Compare multiple variables	Displays data points as bubbles, using bubble size to represent an additional value.

Copyright © 2026, Oracle and/or its affiliates.

Component	Purpose	Description
Funnel	Show stages	Displays values across stages of a process, such as a sales pipeline.
Line	Show trends	Connects data points to show patterns or changes across ordered values.
Pie	Show proportions	Displays the relative proportions of categories as slices of a circle.
Pyramid	Show hierarchical proportions	Displays values in pyramid-shaped segments to illustrate relative proportions.
Scatter	Show relationships	Plots data points to illustrate relationships between numeric values.

Why this matters

A2UI enables agents to present information and collect input using interactive components when a conversational text response alone isn't the most effective way to complete a task.

For information about how A2UI supports interoperability between agents and Agent Hub, see How Agent Hub Supports Interoperability .

How Agent Hub Uses Large Language Models (LLMs)

Agent Hub uses a configured large language model (LLM) to support orchestration and provide direct responses to user requests.

When you enter a prompt without selecting an agent, the orchestrator uses the configured LLM to help determine how to handle your request. If your request doesn't require a specialized agent or tool, Agent Hub can use the LLM to respond directly.

An LLM and an agent aren't the same thing. An LLM provides general language-understanding and generation capabilities, while an agent is designed to perform specific tasks using specialized instructions, tools, and other capabilities. Agents can also use their own configured LLMs.

The models available in Agent Hub depend on the selected processing region. An Agent Hub administrator selects the processing region and an available model for orchestration and direct responses.

For information about how Agent Hub processes requests, see How Agent Hub Processes Requests.

For information about configuring the processing region and model, see Understand Agent Hub Model Configuration.

Copyright © 2026, Oracle and/or its affiliates.

3

Understand How Agent Hub Manages Access

This chapter explains how access affects the Agent Hub features and AI resources available to users and describes the permissions required to work with topics.

Topics:

- About the Agent Hub Access Model
- Understand Topic-Based Access
- Understand Agent Hub Users and Administrators

About the Agent Hub Access Model

Agent Hub uses multiple levels of access control to determine which features and AI resources are available to you. Having access to Agent Hub doesn't automatically provide access to every agent or topic.

Your organization manages access to the underlying AI Data Platform environment and registered AI resources separately from Agent Hub. Within Agent Hub, administrators can also manage access to the Topics feature and individual topics.

Understanding these access requirements can help you determine why a particular feature or resource might not be available to you.

Direct and Topic-Based Access

Depending on the permissions granted by your organization, you can access an agent directly or through a topic.

When you have direct access to an agent, you can select that agent from the Registry and start a conversation with it.

Topic-based access provides another way to work with agents associated with a particular business area or purpose. Your organization manages access to the Topics feature and individual topics separately.

For more information about topic access, see Understand Topic-Based Access.

Why this matters

The features and AI resources available to you depend on the access granted by your organization. If you can't find or use a particular agent or topic, you might need additional access.

For information about using Agent Hub topic permissions, see Understand Topic-Based Access.

Copyright © 2026, Oracle and/or its affiliates.

Understand Topic-Based Access

Topics organize related agents and tools around a common business area or purpose. When a user starts a chat from a topic, the orchestrator can use the agents and tools associated with that topic to process the request.

Topic-based access can provide an alternative to granting a user access to each individual agent associated with the topic. When the required topic access is granted, the agents associated with that topic become available to the user through the topic. Other required Agent Hub and AI Registry access still applies.

How Topic Access Works

Topic access is controlled at two levels.

Access Level	What It Controls	Managed By
Topics feature access	Determines whether a user can access the Topics feature and what actions they can perform, such as using, creating, or managing topics. It doesn't grant access to individual topics.	Agent Hub administrator
Individual topic access	Determines whether a user can view, use, or manage a particular topic, provided they also have the required Topics feature access.	Topic administrator

An Agent Hub administrator grants access to the Topics feature from Agent Hub Administration. A topic administrator separately grants access to individual topics from the Topic access section of the Edit Topic page. Both levels of access are required to use a particular topic.

Topic Permission Levels

The Topics feature provides the following access levels:

Access Level	General Purpose
None	The user doesn't have access to the Topics feature.
Viewer	The user can view topics where the applicable topic access permits it.
User	The user can use topics where the applicable topic access permits it.
Manager	The user can manage topics where the applicable topic access permits it, including updating topic information and managing associated AI resources.
Administrator	The user has administrative capabilities for topics.

Access a Specific Topic

In addition to access to the Topics feature, a user must have access to the particular topic. Access to an individual topic determines whether the user can view, use, or manage that topic. A topic administrator manages this access.

Copyright © 2026, Oracle and/or its affiliates.

Permission to view a topic doesn't necessarily allow the user to start a conversation from it. The user must have the appropriate permission to use the topic.

Access Agents Through a Topic

Topic-based access provides an alternative to granting individual access to every agent associated with the topic.

For example, suppose a Recruiting topic contains agents that help with recruiting-related tasks. Instead of granting the user individual access to each agent in the topic, an administrator can provide the required topic access. The user can then reach the associated agents through the Recruiting topic, assuming the user's other required access is in place.

Topic-based access doesn't necessarily make the associated agents directly visible to the user outside the topic. The topic provides the access path to those agents.

Why this matters

Topic-based access can simplify access management when multiple users need to work with a related group of agents. Instead of granting direct access to each agent individually, administrators can use topics to provide an appropriate access path to the agents associated with a business area or purpose.

Topic access doesn't replace the other access requirements described in this chapter. The user must still have the permissions required to access Agent Hub and the applicable AI Registry areas.

For information about granting access to the Topics feature, see Grant and Manage Topic Access.

For information about granting access to an individual topic, see Grant Users or Roles Access to a Topic.

Understand Agent Hub Users and Administrators

Different users interact with Agent Hub in different ways. Some users primarily discover and use AI resources, while others create and manage topics or administer the Agent Hub environment.

The user types described in this guide identify the responsibilities associated with common Agent Hub activities. A user type isn't necessarily the same as a security role. The actions that a user can perform depend on the permissions and access granted to that user.

Business User

Business users use Agent Hub to interact with the enterprise AI resources available to them. Depending on their access, business users can discover available resources, start and continue conversations, upload files, and work with topics.

Typical business-user activities include:

- Discover and use available enterprise AI resources.
- Start and manage conversations.
- Upload files to provide additional context.
- Review responses and continue existing conversations.
- Use topics that are available to them.

Copyright © 2026, Oracle and/or its affiliates.

Topic Owners and Managers

Users with the appropriate permissions can create and manage topics that organize related agents and tools around a business area or purpose.

Depending on their permissions, these users can perform activities such as configuring a topic, managing its associated agents and tools, and managing access to the topic.

The permissions required to use, manage, or administer topics depend on both the user's Topics feature access and access to the specific topic.

See Understand Topic-Based Access.

Agent Hub Administrators

Agent Hub administrators configure and administer the Agent Hub environment. Administrative responsibilities can include configuring the orchestrator, managing Agent Hub settings, and managing access to Agent Hub functionality such as topics.

Agent Hub administrator access is provided through the predefined AGENT_HUB_ADMIN system role. Assign this role only to users who require Agent Hub administrative capabilities.

Agent Hub administrator access doesn't replace permissions required to work with capabilities managed elsewhere in AI Data Platform. Additional access can be required for resources or functionality outside Agent Hub.

Other Administrative Roles

Some access required to use Agent Hub is configured outside Agent Hub by other administrators or resource owners. For example, access to AI Data Platform environments and registered AI resources is managed separately.

Why this matters

Understanding the responsibilities associated with different Agent Hub users and administrators can help organizations assign appropriate access and identify who performs particular configuration and management tasks.

For information about Agent Hub access requirements, see About the Agent Hub Access Model.

For information about topic access, see Understand Topic-Based Access.

Copyright © 2026, Oracle and/or its affiliates.

4

Start Using Agent Hub

This chapter provides quick start information to help you open Agent Hub, interact with the enterprise AI resources available to you, start a chat, and write effective prompts.

Topics:

- How to Open Agent Hub
- Ways to Start a Chat
- Write Effective Prompts
- Continue a Chat

How to Open Agent Hub

Users can open Agent Hub directly from the Agent Hub URL provided by their organization. Users who have access to AI Data Platform can also open Agent Hub from the AI Data Platform home page.

Users must have the required access to Agent Hub before they can open and use it. For information about Agent Hub access requirements, see About the Agent Hub Access Model.

Topics:

- Open Agent Hub from a URL
- Open Agent Hub from AI Data Platform

Open Agent Hub from a URL

You can open Agent Hub directly from a URL provided by your organization. This is the most common way to access Agent Hub.

Your administrator must grant you permission to access Agent Hub before you can open and use it. For more information about Agent Hub access requirements, see About the Agent Hub Access Model.

From Agent Hub, you can start a chat or use the navigation panel to access recent chats, the Registry, and other Agent Hub functionality available to the user. See About the Agent Hub Interface.

1. Click the Agent Hub URL provided by your organization.
2. If prompted, enter your login credentials.

Open Agent Hub from AI Data Platform

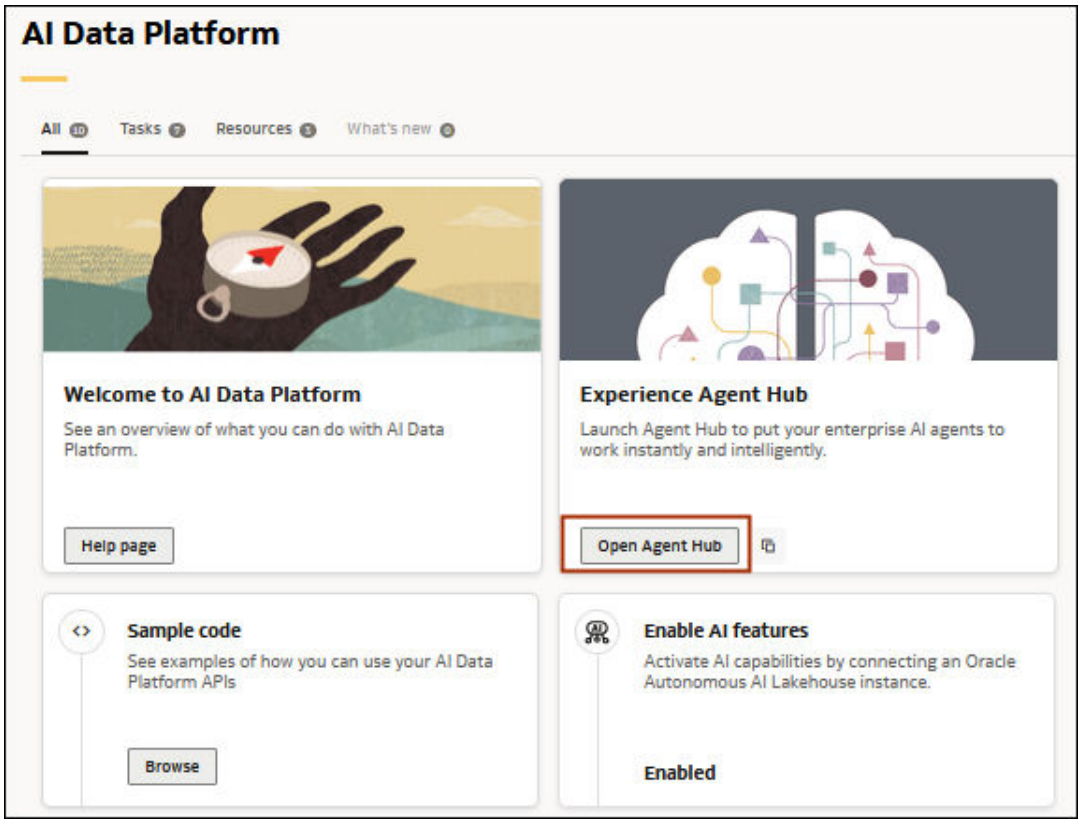
Users who have access to AI Data Platform can open Agent Hub from the AI Data Platform home page.

You must have the required access to both AI Data Platform and Agent Hub. See About the Agent Hub Access Model.

Copyright © 2026, Oracle and/or its affiliates.

From Agent Hub, you can start a chat or use the navigation panel to access your chats, available enterprise AI resources, and topics. See About the Agent Hub Interface.

1. Open the AI Data Platform instance that provides access to Agent Hub.
2. On the AI Data Platform home page, locate the **Experience Agent Hub** tile and click **Open Agent Hub**.



Ways to Start a Chat

Agent Hub provides several ways to start a chat. The method you choose depends on whether you want Agent Hub to determine how to handle your request or you already know which agent or topic you want to use.

Topics:

- Enter a Prompt
- Select an Agent
- Select a Topic

Enter a Prompt

Enter a prompt when you want Agent Hub to determine how to handle your request.

When you start a chat without selecting or tagging a particular agent, the orchestrator evaluates each request and determines which available agent or tool to use. Different agents can handle successive requests within the same conversation.

Copyright © 2026, Oracle and/or its affiliates.

Depending on your request and approval settings, Agent Hub can:

- **Route the request to an agent**: The orchestrator identifies an agent whose capabilities match your request and routes the request to that agent.
- **Present agents for selection**: When agent selection is required, Agent Hub presents recommended agents. You can select a recommended agent or choose another available agent.
- **Invoke a tool**: The orchestrator identifies and invokes an appropriate tool to process your request.
- **Provide a direct response**: If your request doesn't require a specialized agent or tool, Agent Hub can respond directly using its configured large language model (LLM).

Depending on your approval setting, Agent Hub might ask you to select an agent before continuing or automatically use the agent it identifies as the best match.

See How Agent Hub Processes Requests.

1. Open Agent Hub.
2. Click the prompt field and type your chat question or request. For example, What are the requirements for approving a new employee position?



3. Optional: Click **Attach** + if you want to provide your chat with additional context that it can use when processing your request.
4. Click **Send** .

   Agent Hub evaluates your prompt and determines whether to invoke an appropriate agent or tool, present agents for selection, or provide a direct response. Whether Agent Hub presents agent selection depends on your approval setting.

Select an Agent

Select an agent before entering a prompt when you know which agent you want to use for your task. You can select only agents that are available to you based on your access.

When you select an agent from the Registry, that agent remains associated with the conversation. You can't remove or replace the selected agent within the same chat. However, relevant MCP tools can still be invoked while processing your requests.

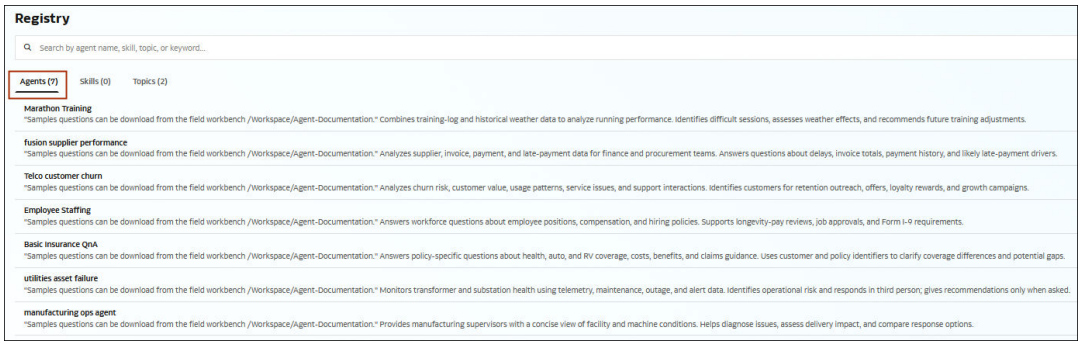
The same behavior applies when you explicitly tag an agent at the start of a chat.

To work with a different agent, start a new chat and select that agent.

Copyright © 2026, Oracle and/or its affiliates.

For information about finding available agents, see Find and Select AI Resources

1. Open Agent Hub.
2. In the navigation panel, click **Registry** Registry .
3. On the Registry page, click the Agents tab Agents.
4. Locate and select the agent you want to use.



5. Optional: In the Chat page, click **What can this agent help with?** to learn about the types of requests the agent can handle.
6. Click the prompt field and type your chat question or request. For example, Summarize my open purchase orders and identify any that require my attention.
7. Optional: Click **Attach** + if you want to provide your chat with additional context that the agent can use when processing your request.
8. Click **Send** .

   Agent Hub starts a chat with the selected agent and displays the response.

Select a Topic

Select a topic when you want to start a chat within a particular business area or purpose. A topic defines which agents and tools the orchestrator can use when processing requests within that topic.

You can select only topics that are available to you based on your access.

Agent Hub evaluates your request within the context of the selected topic and determines how to handle it using the agents and tools available through that topic.

For information about topic access requirements, see Understand Topic-Based Access.

1. Open Agent Hub.
2. In the navigation panel, click **Registry** Registry .
3. On the Registry page, click the **Topics** tab Topics.
4. Locate and select the topic that you want to use.

Copyright © 2026, Oracle and/or its affiliates.



5. Optional: In the Chat page, click **What can this topic help with?** to learn about the types of requests the topic can handle.
6. Click the prompt field and type your chat question or request. For example, Summarize my open purchase orders and identify any that require my attention.
7. Optional: Click **Attach** + if you want to provide your chat with additional context that the topic's AI resources can use when processing your request.
8. Click **Send** .

   Agent Hub starts a chat and uses the selected topic's AI resources to evaluate and respond to the prompt.

Write Effective Prompts

Effective prompts help Agent Hub understand what you want to accomplish and provide more useful responses.

Include enough information about your goal, relevant context, and the result you expect. You can refine your request with follow-up prompts as the conversation continues.

Use these guidelines when writing prompts in Agent Hub:

Describe What You Want to Accomplish

Clearly describe what you want to accomplish. Focus on the task or outcome rather than trying to determine which agent or other AI resource should handle the request.

For example:

Instead of: *Help me with sales.*

Try: *Summarize my open purchase orders and identify any that require my attention.*

Provide Relevant Context

Include information that can help Agent Hub understand your request, such as the business area, time period, audience, or other details that are relevant to the task.

For example:

Summarize my team's open purchase orders for this quarter and identify any that are overdue.

If the information needed to complete your request is contained in a file, attach the file to your prompt to provide additional context.

Describe the Result You Want

If you need the response presented in a particular way, describe the format, level of detail, or information that you want included.

For example:

Copyright © 2026, Oracle and/or its affiliates.

Summarize my open purchase orders in a table. Include the supplier, amount, due date, and status.

You don't need to specify an output format when it isn't important to your request.

Refine Your Request

You don't need to create a perfect prompt the first time. After reviewing the response, continue the chat with follow-up prompts to clarify your request, provide more context, change the requested output, or ask for additional detail.

For example:

Show only the purchase orders that are more than 30 days overdue.

As you continue the chat, use your follow-up prompts to guide the AI resource toward the information or result you need.

Continue a Chat

You can reopen an existing chat and enter follow-up prompts to continue the conversation.

When you start a chat without selecting or tagging a particular agent, the orchestrator evaluates each new request and can invoke different agents as the conversation progresses. When routing a request to a different agent, the orchestrator can provide relevant information from earlier prompts and responses. The receiving agent determines how to use and retain that information.

If you selected or tagged an agent when starting the chat, that agent remains associated with the conversation and is responsible for maintaining its own conversation context.

For example, after asking *Summarize the key changes in sales performance for the Western region this quarter*, you could follow up with *Which of those changes had the largest impact?*

Start a new chat when you want to begin a separate conversation or explicitly select a different agent. For information about the different ways to start a new chat, see Ways to Start a Chat.

1. Open Agent Hub.
2. In the navigation panel, go to the **Chats** and locate and click the chat you want to continue.

   Agent Hub opens the chat and displays the existing conversation.
3. Enter and submit your follow up prompt.

   Agent Hub submits your follow-up prompt to continue the conversation.

Copyright © 2026, Oracle and/or its affiliates.

5

Work with Agent Hub

This chapter describes how to use Agent Hub to discover and select AI resources, manage chats and profile settings, and understand responses and agent behavior.

Topics:

- About the Agent Hub Interface
- Find and Select AI Resources
- Understand How Topics Affect a Chat
- How to Work with Files
- Manage Chat History
- Understand Responses and Agent Behavior
- Understand Approvals in Agent Hub
- Understand Request Activity
- Manage Your Profile Settings

About the Agent Hub Interface

The Agent Hub interface provides a single place to start and manage conversations and discover the agents and topics available to you. Use the navigation panel to move between conversations and the Registry, and use the chat page to interact with Agent Hub.

Navigation Panel

Use the navigation panel to start a new chat, open the Registry, and return to recent conversations.

The navigation panel includes:

- **New chat**: Starts a new conversation.
- **Registry**: Opens the Registry where you can browse and search the agents and topics available to you.
- **Chats**: Lists your conversations. Select a chat to review or continue the conversation.
- **Search**: Searches chat names to help you find previous conversations.

You can close the navigation panel when you need more space for your conversation.

Registry Page

Use the Registry page to discover the agents and topics available to you. You can browse the Registry or use search to find a particular agent or topic.

When you already know which agent you want to use, you can select it from the Registry to start a conversation with it directly.

Copyright © 2026, Oracle and/or its affiliates.

For information about browsing and selecting agents and topics, see Find and Select AI Resources.

Chat Page

Use the chat page to enter prompts, view responses, and continue a conversation.

Depending on how you start a conversation, you can enter a prompt and let Agent Hub determine how to handle your request, select an agent directly, or start the chat from a topic.

The chat page includes the prompt field where you enter questions, instructions, or requests and continue the conversation. You can also attach supported files to provide additional information for your request. See Upload a File to a Chat.

When you start a chat by selecting or tagging a particular agent, that agent remains associated with the conversation. To work with a different agent, start a new chat.

When you start a chat without selecting or tagging an agent, the orchestrator can invoke different agents for successive requests within the same conversation. To see which agent handled a request, open **Thinking Activity**.

For information about the different ways to start a chat, see Ways to Start a Chat.

The chat page also includes a control for choosing when Agent Hub requests your involvement before selecting agents or tools or performing certain actions. See Understand Approvals in Agent Hub.

User Menu

Open the user menu from the bottom of the navigation panel to access options associated with your account. From the user menu, you can access your profile settings or sign out of Agent Hub. If you have Agent Hub administrative access, you can also open the Administration settings.

For information about user profile settings, see Manage Your Profile Settings.

Find and Select AI Resources

Use the Registry to find the agents and topics available to you. You can browse available items or use search to find a particular agent or topic.

The Registry shows only the agents and topics that you have access to. For information about how access determines which resources are available to you, see About the Agent Hub Access Model.

Agent Hub can also use tools when processing requests. However, you don't browse or select tools from the Registry in the same way that you browse and select agents. Agent Hub's orchestrator can identify an appropriate tool based on your request.

For information about the types of AI resources that Agent Hub supports, see AI Resources Supported by Agent Hub.

Browse Available Agents

Use the **Agents** tab on the Registry page to browse the agents available to you.

The Registry provides descriptive information about each agent to help you understand what the agent is designed to do and whether it's appropriate for your task. This information can include the agent's name, description, and capabilities.

Copyright © 2026, Oracle and/or its affiliates.

The same descriptive information also helps Agent Hub determine whether an agent is relevant to a request when the orchestrator selects an agent for you. The newer AI Registry source specifically identifies the agent's name, description, and capabilities as information used for orchestration.

When you find an agent that you want to use, select the agent to start a chat with it. For information about starting a chat with a selected agent, see Select an Agent.

Browse Available Topics

Use the **Topics** tab on the Registry page to browse the topics available to you.

A topic groups related agents and tools around a particular business area or purpose. For example, a Recruiting topic might provide access to agents that support recruiting-related tasks.

When you select a topic and start a chat, Agent Hub uses the topic to focus how it handles your request.

For information about topics, see What Are Topics?

For information about starting a chat from a topic, see Select a Topic.

For information about how a selected topic affects a chat, see Understand How Topics Affect a Chat.

Search the Registry

Use Registry search to find a particular agent or topic or to narrow the items displayed in the Registry. Search results include only items that are available to you based on your access.

Understand How Topics Affect a Chat

Starting a chat from a topic provides a business context for the conversation and defines which agents and tools Agent Hub can use when processing your requests.

For example, a Finance topic might contain agents and tools that support reconciliation, period close, and financial reporting. When you start a chat from the Finance topic, the orchestrator considers the agents and tools associated with that topic rather than all the resources available to you.

Using a topic can make it easier to work within a particular business area without having to select an individual agent before starting the conversation. For information about topics and how they're organized, see What Are Topics?

Understand How Agent Hub Uses the Selected Topic

The orchestrator evaluates each request and determines whether to invoke an appropriate agent or tool associated with the topic. Different agents associated with the topic can handle successive requests within the same conversation.

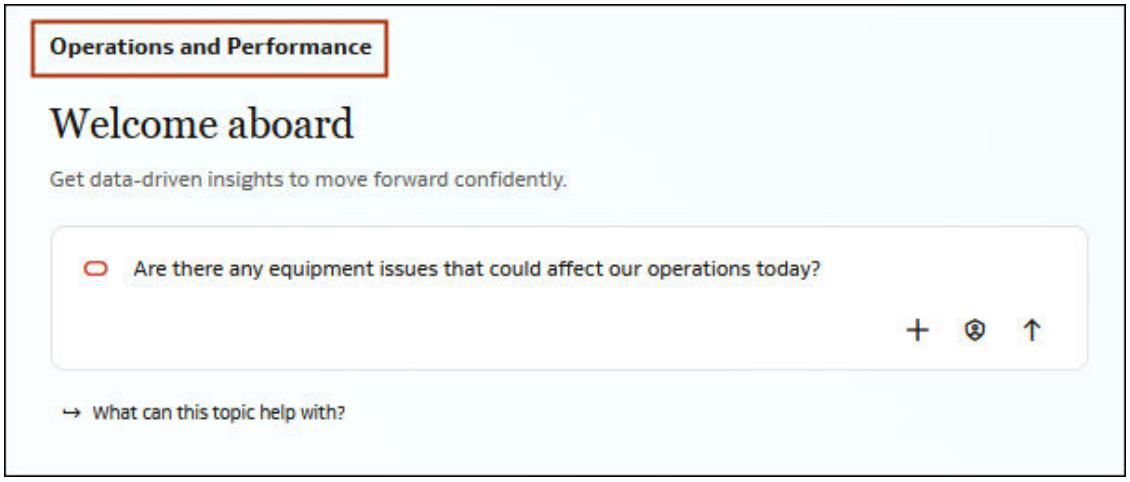
For example, one agent might investigate a business issue, while another agent handles a follow-up request about how to address it. Depending on your approval setting, Agent Hub can present agents for selection or invoke the selected agent automatically. If no associated agent or tool is needed to handle your request, the orchestrator can respond directly using the configured large language model (LLM).

See How Agent Hub Processes Requests.

Copyright © 2026, Oracle and/or its affiliates.

Identify the Topic Associated with a Chat

When you start a chat from a topic, Agent Hub identifies the selected topic with the conversation. This helps you identify the business context in which you're working.



Work with a Different Topic

A topic remains associated with the chat in which it was selected. To work within a different topic, start a new chat and select the topic that you want to use.

You can't change the topic associated with an existing chat.

For information about starting a chat from a topic, see Select a Topic.

Why this matters

Topics help focus a conversation on a particular business area without requiring you to know which individual agent is appropriate before you begin. Understanding that the selected topic remains associated with the chat can also help you decide when to continue an existing conversation and when to start a new one.

For information about how access to a topic affects the agents available through it, see Understand Topic-Based Access.

How to Work with Files

You can work with files in Agent Hub to provide additional information for your requests and save generated output for use outside Agent Hub.

Topics:

- Understand Working with Files
- Upload a File to a Chat

Understand Working with Files

You can upload files to Agent Hub to provide additional information for a request. For example, you might upload a document that you want Agent Hub to summarize, analyze, or use when answering questions.

Copyright © 2026, Oracle and/or its affiliates.

When you upload a file, include a prompt that explains what you want Agent Hub to do with the file. You can continue the conversation with follow-up prompts to ask additional questions or refine the result.

The ability to process a file can depend on the file type, file size, and the capabilities available for the conversation.

Supported Files and Limits

Agent Hub supports specific file types and limits for uploaded files. Before uploading a file, make sure that the file meets the supported requirements.

Work with an Uploaded File

An uploaded file provides information that Agent Hub can use when processing your request. Clearly describe the result you want rather than uploading the file without instructions.

For example, *Summarize the key findings in this document and identify any recommended actions* or *Compare the proposed policy with the current policy and summarize the significant differences*.

You can use follow-up prompts to continue working with information from an uploaded file within the conversation. For information about writing effective prompts, see Write Effective Prompts.

File Availability in Chat

Uploaded files are associated with the conversation in which you provided them.

Why this matters

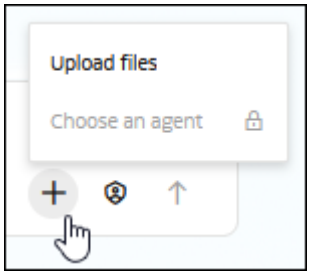
Working with files lets you provide information for a request without copying the file's contents into the prompt and lets you save generated output for use outside Agent Hub. Describing what you want Agent Hub to do with an uploaded file can help you get a more useful result.

Upload a File to a Chat

Upload a file to provide additional information that Agent Hub can use when processing your request.

Before you upload a file, make sure that it meets the supported file type and size requirements. See Understand Working with Files.

1. Open Agent Hub.
2. Go to the prompt field and Click **Attach** + and then select **Upload files**.



Copyright © 2026, Oracle and/or its affiliates.

3. Locate and select the file you want to upload.

   The file is added to the chat.

4. Enter a prompt to describe what you want Agent Hub to do with the attached file.

5. Click **Send**.

   Agent Hub uses the information in the uploaded file to process your request.

Manage Chat History

Agent Hub saves your chats so that you can return to previous conversations and manage your chat history.

Agent Hub automatically names each new chat using the first few words of your first prompt. Chats appear in the **Chats** area of the navigation panel and are grouped based on when the conversations occurred.

You can search for a previous chat or use the chat menu to open, rename, or remove a chat. The Chats search searches chat names only, and not the prompts or responses within a conversation.

1. Open Agent Hub.
2. In the navigation panel, go to **Chats**.
3. Optional: To find a particular chat, click **Search chat titles** and enter text to identify the chat you want to find.
4. Optional: To open a chat, click it.
5. Optional: Click a chat's **More actions** icon and do one of the following:
   - To rename a chat, click **Rename**. Type the new name and press Enter to save it.
   - To remove a chat, click **Remove**.

Understand Responses and Agent Behavior

As you work in a chat, Agent Hub provides information that helps you understand how your request is being handled. Depending on your request and how you start the chat, Agent Hub can use an agent or tool to process the request or provide a direct response using its configured large language model (LLM).

Understanding how Agent Hub handles requests can help you interpret responses and decide whether to continue the current conversation or start a new chat.

For information about how Agent Hub determines how to handle a request, see How Agent Hub Processes Requests.

Identify the Agent Associated with a Chat

When you start a chat by selecting or tagging an agent, that agent remains associated with the conversation. To work with a different agent, start a new chat.

When you start a chat without selecting or tagging an agent, the orchestrator can invoke different agents for successive requests within the same conversation. To see which agent handled a particular request, click the processing status indicator in the chat to open **Thinking Activity**.

Copyright © 2026, Oracle and/or its affiliates.

Understand Direct Responses from Agent Hub

Not every request requires a specialized agent or tool. When you enter a prompt without first selecting an agent, the orchestrator evaluates your request and determines how to handle it.

If a specialized agent or tool isn't required, Agent Hub can use its configured LLM to provide a direct response.

A direct response is different from a response provided by a registered agent. An agent can have specialized instructions, tools, and capabilities configured for a particular business purpose, while a direct response uses the LLM configured for Agent Hub.

For information about configuring LLM, see How Agent Hub Uses Large Language Models (LLMs).

See How Agent Hub Processes Requests.

Understand When Agent Hub Uses a Tool

Agent Hub can identify and use an appropriate tool when processing a request. Unlike agents, tools aren't resources that you browse and select directly from the Registry.

To see which tool Agent Hub invoked, click the processing status indicator (for example, **Completed in 18s**) in the chat to open the **Thinking Activity** panel. The panel displays the name of the tool used to process your request.

Continue Working with an Agent

Enter follow-up prompts to continue the conversation. In an orchestrated conversation, Agent Hub can invoke different agents as needed and provide relevant information from earlier prompts and responses to an agent handling a follow-up request. The receiving agent determines how to use and retain that information.

If you selected or tagged an agent when starting the chat, that agent remains associated with the conversation and is responsible for maintaining its own conversation context.

For example, after asking an agent to summarize your open purchase orders, you might follow up with a request such as Show only the purchase orders that are more than 30 days overdue.

See Write Effective Prompts.

Know When to Start a New Chat

Start a new chat when you want to begin a separate task or explicitly select a particular agent. If you started the current chat by selecting or tagging an agent, you must start a new chat to work with a different agent.

In an orchestrated conversation, you can continue submitting requests without starting a new chat when your work requires different agents.

Review Responses

Review Agent Hub responses before relying on the information provided or taking further action. Depending on the request and the capabilities used to process it, a response can include text, supporting information, generated files, or interactive content.

If a response doesn't provide the result you need, use a follow-up prompt to clarify or refine your request.

Copyright © 2026, Oracle and/or its affiliates.

When Agent Hub requests approval before performing an action, review the requested action before deciding whether to approve it. See Understand Approvals in Agent Hub.

For information about the processing information displayed while Agent Hub handles a request, see Understand Request Activity.

For help resolving problems with a response or agent behavior, see Troubleshooting.

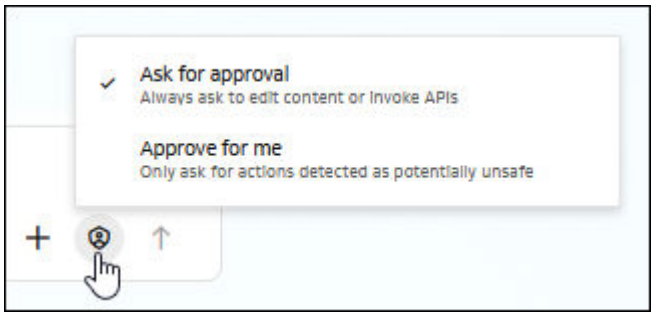
Why this matters

Understanding how Agent Hub handles a request can help you interpret the response you receive and decide what to do next. You can refine your request with a follow-up prompt, continue an orchestrated conversation that uses different agents as needed, or start a new chat when you want to begin a separate task or explicitly select a different agent.

Understand Approvals in Agent Hub

Agent Hub provides approval settings that control when you review agent or tool selections and when Agent Hub can proceed automatically. You can choose how much control you want over the agents and tools used to process your requests.

You can select an approval control setting in the chat prompt field.



Agent Hub provides two approval options:

- **Ask for approval**: When the orchestrator presents an agent for execution, Agent Hub displays the suggested agent and alternatives regardless of the LLM's confidence in its selection. You can approve the suggested agent or choose another available agent. This approval setting also applies to tools.
- **Approve for me**: Agent Hub automatically invokes the agent or tool selected by the LLM. You need to approve an action only when the LLM identifies it as especially sensitive.

In an orchestrated conversation, the approval setting also applies when the orchestrator selects an agent for a follow-up request. Depending on the setting, Agent Hub can present agents for selection or invoke the selected agent automatically.

For information about how Agent Hub selects agents and tools, see How Agent Hub Processes Requests.

Copyright © 2026, Oracle and/or its affiliates.

Understand Request Activity

Agent Hub provides status and activity information that helps you understand what happens as it processes your requests. Depending on the request and the agent handling it, Agent Hub can display processing status, elapsed time, and additional request activity information.

Understand Request Status

While an agent processes your request, Agent Hub displays status information in the chat to indicate that processing is in progress. For example, the current interface can display **Starting chat with the selected agent...** while Agent Hub initiates the request. After processing ends, Agent Hub displays the elapsed processing time, such as **Completed in 25s**.

Understand Thinking Activity

After Agent Hub processes a request, click the processing status indicator (for example, **Completed in 18s**) to open the **Thinking Activity** panel.

Thinking Activity provides a high-level view of how Agent Hub processes your request, including which agents or tools were invoked and the processing steps performed. In an orchestrated conversation, different agents can handle successive requests. You can use Thinking Activity to identify the agent invoked for a particular request. The amount of information displayed can vary depending on the agent.

The panel also displays processing statuses and elapsed time.

For information about how Agent Hub selects agents during a conversation, see How Agent Hub Processes Requests.

Understand Timestamps

Agent Hub displays timestamps with prompts and responses to help you identify when activity occurred in a conversation.

Work with Prompts and Responses

Agent Hub provides controls that you can use to perform actions on prompts and responses. The available controls can vary depending on the content or activity in the conversation.

Manage Your Profile Settings

Use your profile settings to manage preferences that apply to your Agent Hub experience.

1. Open Agent Hub.
2. At the bottom of the navigation panel, click your user name, and then click **Profile**.
3. In the Profile Settings page, modify your settings as needed.
4. Click **Save**.

Copyright © 2026, Oracle and/or its affiliates.

6

Create and Manage Topics

This chapter describes how topic creators, managers, and administrators plan, create, configure, and manage topics for use in Agent Hub.

Topics:

- What Are Topics?
- Guidelines for Creating Topics
- Create and Configure a Topic
- Modify a Topic
- How to Work with Topic Access
- Remove a Topic

What Are Topics?

Topics help users work with agents and tools that support a particular business area or purpose.

When a user starts a chat from a topic, Agent Hub considers the agents and tools associated with that topic rather than all of the agents available to the user. Selecting a topic doesn't select a particular agent or tool. The orchestrator evaluates the user's request and determines whether to invoke an appropriate agent or tool associated with the topic or provide a direct response.

How Topics Work

A topic defines the agents and tools that Agent Hub can use when processing requests made from that topic.

For example, suppose your organization creates a Finance topic that contains agents and tools for reconciliation, period close, and financial reporting. When a user submits a request from the Finance topic, the orchestrator evaluates the request using the agents and tools associated with that topic. Different agents within the topic can handle successive requests in the same conversation.

Depending on the request and approval setting, Agent Hub can invoke an appropriate agent or tool, present agents for selection, or provide a direct response using its configured large language model (LLM).

For more information about working in a topic, see Understand How Topics Affect a Chat.

Why Use Topics

Topics help organizations organize agents and tools around the business work they support rather than requiring users to understand every AI resource available across the enterprise.

For users, topics provide a focused way to work with resources related to a particular business area or purpose.

Copyright © 2026, Oracle and/or its affiliates.

For topic owners and managers, topics provide a way to group related agents and tools and define the resources the orchestrator can use when users work within the topic.

Topics can also provide users with an access path to the agents associated with the topic instead of requiring direct access to each agent individually. Other required Agent Hub and AI Registry access still applies.

Topic Access

Which topics a user can discover and use depends on the access granted to that user.

Topic access is controlled at two levels: access to the Topics feature and access to a specific topic. Having access to topics generally doesn't automatically provide access to every topic.

To start a conversation from a topic, the user must have sufficient access to use that particular topic.

For more information about topic-based access, see Understand Topic-Based Access.

Topic Information

A topic includes information that helps users identify its purpose and understand when to use it. When creating a topic, the topic creator provides a name and description and can associate agents and tools with the topic.

A topic can also include an image that helps users recognize the topic in Agent Hub.

For guidance about defining a topic and choosing its agents, tools, and image, see Guidelines for Creating Topics.

Guidelines for Creating Topics

Topic creators should plan the purpose, contents, and access requirements for a topic before creating it. A well-defined topic groups related agents and tools around a recognizable type of business work and provides Agent Hub with a focused set of resources to consider when users work within the topic.

Use the following guidelines when planning a topic.

Organize Topics Around Business Areas

Create topics around a recognizable business area or type of work rather than around the teams that develop or own the agents.

For example, a Finance topic might contain agents that support reconciliation, period close, and financial reporting. Organizing agents this way helps users select a topic based on the work they want to accomplish rather than requiring them to know which team owns a particular agent.

Keep Topics Focused

Include agents and tools that are relevant to the purpose of the topic and support the types of requests users are likely to make.

When a user works within a topic, the orchestrator considers the agents and tools associated with that topic rather than all available resources. Keeping the topic focused provides a relevant set of resources for Agent Hub to consider.

Copyright © 2026, Oracle and/or its affiliates.

Use Clear Topic Names and Descriptions

Give each topic a clear name and description that communicate its business purpose and help users understand when to use it.

Agent Hub uses the topic description when answering questions about the topic's capabilities, such as What can this topic help with? The orchestrator doesn't use the topic description to select agents or tools when processing requests.

For example:

Name: Finance

Description: Use this topic to work with agents and tools that support reconciliation, period close, and financial reporting.

Add a Recognizable Topic Image

Add an image that helps users recognize the topic when they open and work with it. Choose an image that represents the topic's business area or purpose and helps distinguish it from other topics.

Topic images are displayed with the topic when the user works within the topic.

Select Resources That Support the Topic's Purpose

Add agents and tools that support the business area or work represented by the topic. Before adding a resource, consider whether its capabilities are relevant to the requests users are likely to submit while working within the topic.

Avoid adding a resource solely because it's available. Each resource should have a clear relationship to the topic's purpose.

For information about adding or removing agents and tools from existing topics, see Modify a Topic.

Plan Topic Access

Consider who needs to use, manage, and administer the topic when planning its configuration.

An Agent Hub administrator controls access to the Topics feature. A topic administrator controls access to the individual topic.

Topic access can provide users with an access path to the agents associated with the topic instead of requiring direct access to each agent individually. Other required Agent Hub and AI Registry access still applies.

When planning access, grant users only the level of access required for their responsibilities. Users who only need to work within a topic don't need the same permissions as users who manage the topic or administer access.

For information about how topic access works, see Understand Topic-Based Access.

For information about configuring access to a topic, see Grant Users or Roles Access to a Topic.

Why this matters

Copyright © 2026, Oracle and/or its affiliates.

A well-planned topic helps users recognize when the topic is relevant, provides Agent Hub with a focused set of agents to consider, and makes it easier to provide appropriate access to related business capabilities.

For information about creating and configuring a topic, see Create and Configure a Topic.

Create and Configure a Topic

Create a topic to organize related agents and tools around a business area or purpose and provide users with a focused context for working with those resources.

When creating a topic, you can also grant users or roles access to the topic to control who can view, use, or manage it.

When a user starts a chat from a topic, the orchestrator can invoke the agents and tools associated with that topic. The orchestrator can invoke tools directly without routing requests through an agent.

You must have the appropriate Topics feature permission to create a topic. For information about topic permissions, see Understand Topic-Based Access.

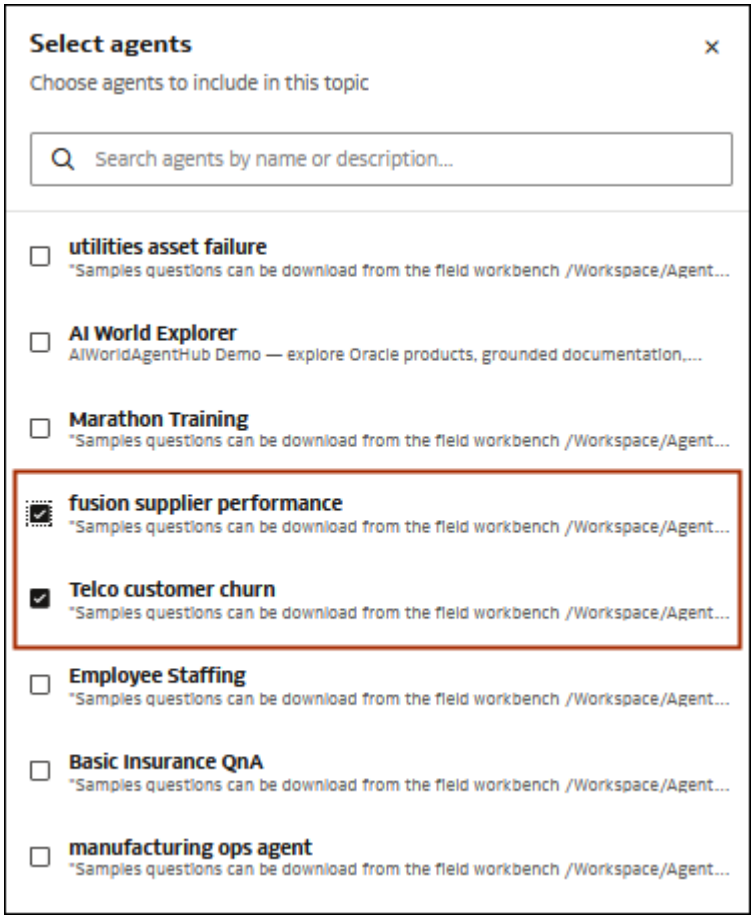
1. Open Agent Hub.
2. In the navigation panel, click **Registry** 

.
3. On the Registry page, click the **Topics** tab 

.
4. Click **Add Topic**.

   The Create Topic page is displayed.
5. In **Name**, enter a name that clearly identifies business area or purpose of the topic. For example, Finance.
6. In **Description**, enter the purpose of the topic to help the user understand when to use the topic. For example, Use this topic to investigate supplier performance, review invoices and payment history, and identify procurement issues.
7. Optional: In **Topic Image**, click the field to upload an image that displays with the topic when a user opens the topic. Choose an image that represents the topic's business area or purpose and helps users recognize the topic when working with it.
8. In **Select agents**, click **Set agents**. In the Select agents panel, browse or search for and select the agents whose capabilities support the purpose of the topic.

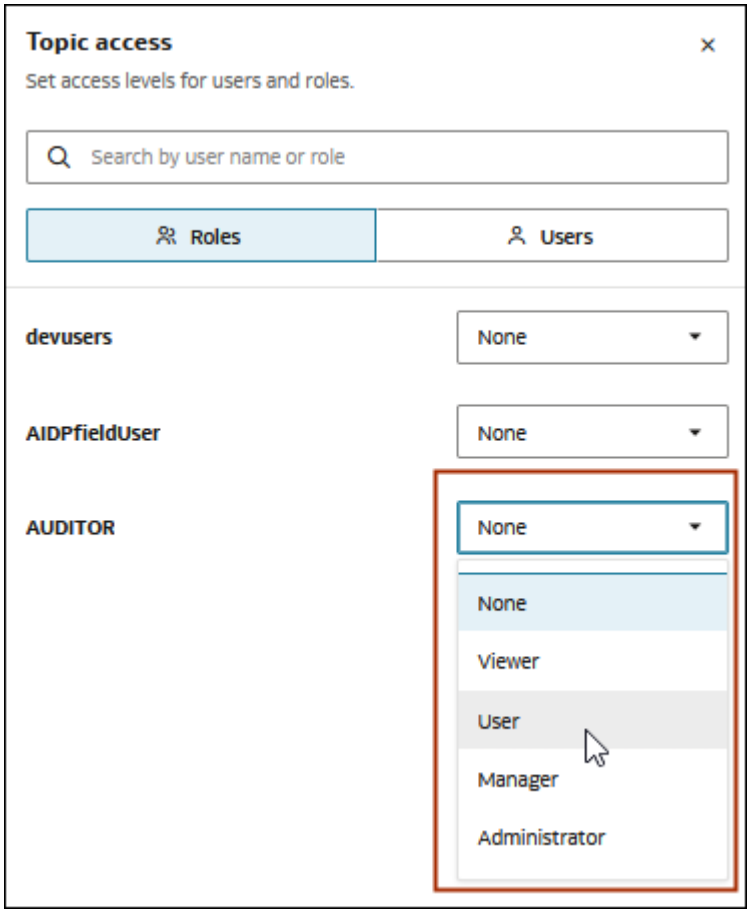
Copyright © 2026, Oracle and/or its affiliates.



Click **Done**.

9. In **Topic access**, click **Set access**. In the **Topic access panel**, select **Roles** or **Users**, locate the users or roles that you want to grant access to, and select the appropriate access level for each.

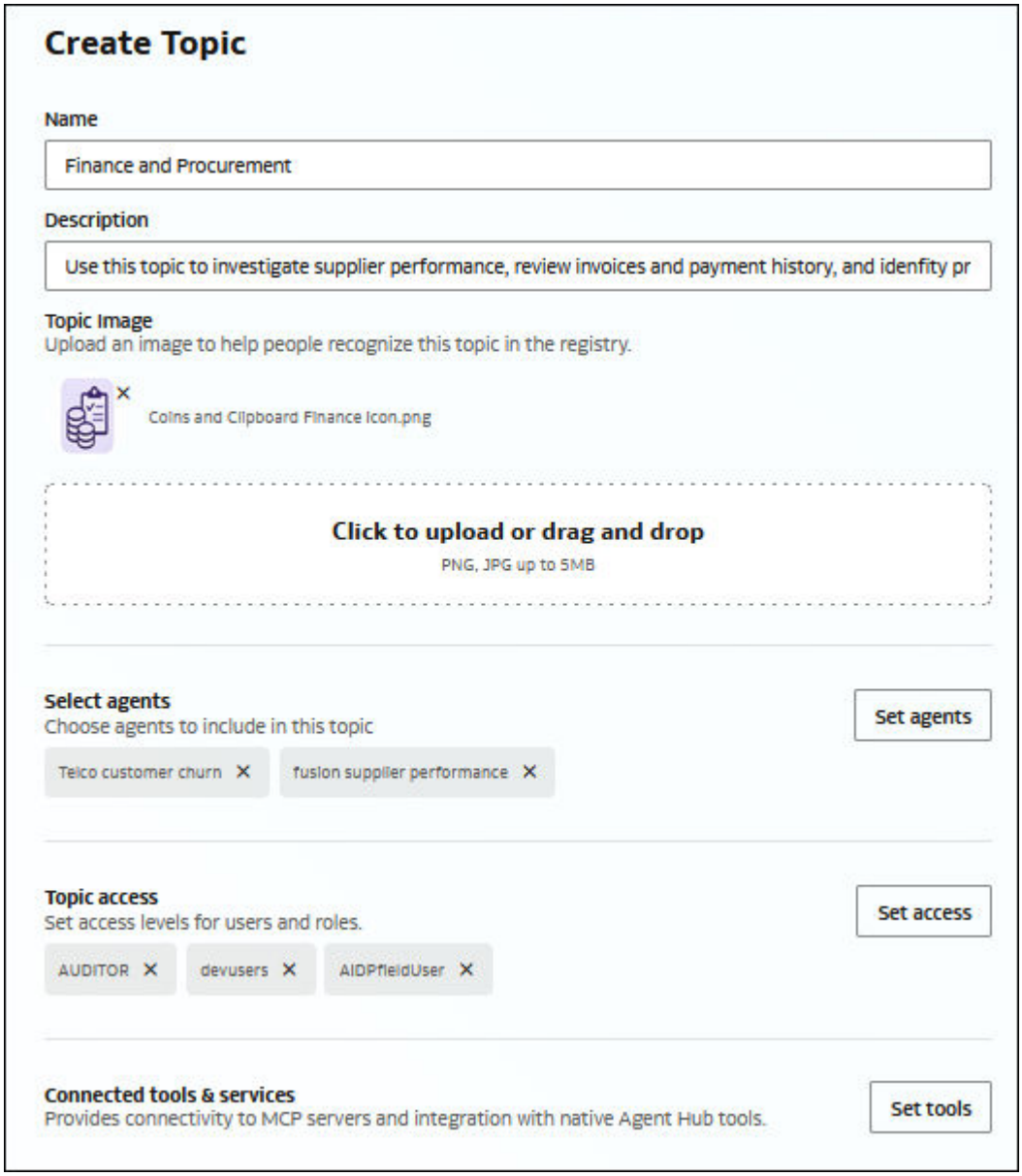
Copyright © 2026, Oracle and/or its affiliates.



Click **Done**.

10. In **Connected tools & services**, click **Set tools**. In the Connected tools & services panel, browse or search for and select the tools or MCP servers that you want to include in the topic. Click **Done**.
11. In the Create Topic page, confirm the topic's settings.

Copyright © 2026, Oracle and/or its affiliates.



12. Click **Save**.

Modify a Topic

Modify a topic when you need to update its name, description, image, associated agents, or connected tools and services.

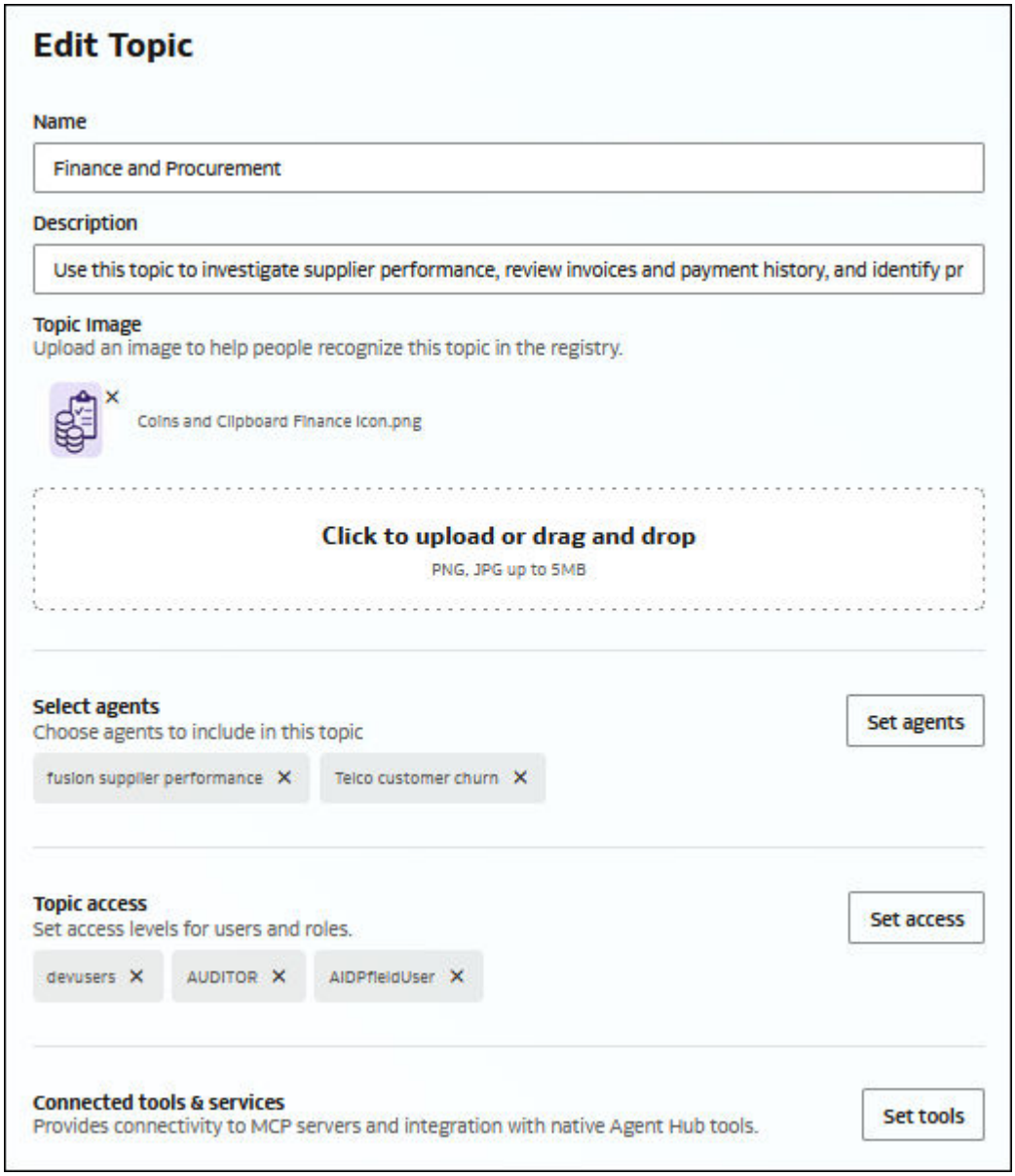
You must have the appropriate permission to modify a topic. For information about topic permissions, see Understand Topic-Based Access.

1. Open Agent Hub.
2. In the navigation panel, click **Registry** Registry .
3. On the Registry page, click the **Topics** tab Topics.
4. Locate the topic you want to modify, click **More Actions** *** and click **Edit**.

Copyright © 2026, Oracle and/or its affiliates.

The Edit Topic page is displayed.

5. Modify the topic's settings, selected agents, and connected tools and services as needed.



6. In the Edit Topic page, click **Save**.

How to Work with Topic Access

Use these topics to learn how topic administrators grant, change, and revoke access to individual topics in Agent Hub.

Before users or roles can be granted access to a specific topic, an Agent Hub administrator must grant them the appropriate access to the Topics feature.

Topics:

- Grant Users or Roles Access to a Topic

Copyright © 2026, Oracle and/or its affiliates.

- Change or Revoke Topic Access

Grant Users or Roles Access to a Topic

As a topic administrator, grant users or roles access to a topic to control who can view, use, manage, or administer the topic.

You must have ADMIN permission for the topic to perform this task. Before you grant access to a user or role, an Agent Hub administrator must grant the user or role the appropriate access to the Topics feature. See Grant Users or Roles Access to the Topics Feature.

A user needs USE permission or stronger on the topic to start a conversation from it. READ permission alone doesn't allow the user to start a conversation from the topic. For information about topic access and permission levels, see Understand Topic-Based Access.

1. Open Agent Hub.
2. In the navigation panel, click **Registry** Registry .
3. On the Registry page, click the **Topics** tab Topics.
4. Locate the topic you want to grant access to, click **More Actions** *** and click **Edit**.

   The Edit Topic page is displayed.
5. Click **Set access**.

   The Topic access panel is displayed.
6. Select Users or Roles depending on how you want to grant access.
7. Locate the user or role you want to grant access to.
8. Select the appropriate access level for the user or role.
9. Click **Done**.
10. On the Edit Topic page, click **Save**.

Change or Revoke Topic Access

As a topic administrator, you can change or revoke access when a user or role no longer needs its current level of access to a topic.

You must have ADMIN permission for the topic to perform this task.

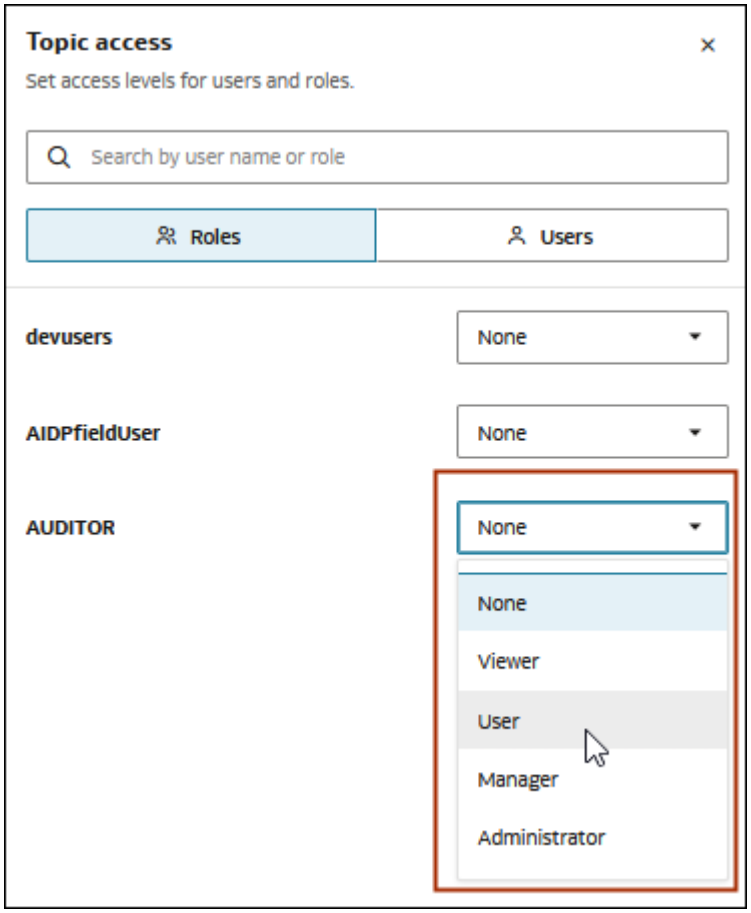
For information about topic access and permission levels, see Understand Topic-Based Access.

1. Open Agent Hub.
2. In the navigation panel, click **Registry** Registry .
3. On the Registry page, click the **Topics** tab Topics.
4. Locate the topic you want to modify access for, click **More Actions** *** and click **Edit**.

   The Edit Topic page is displayed.
5. Click **Set access**.

   The Topic access panel is displayed.

Copyright © 2026, Oracle and/or its affiliates.



6. Locate the user or role you want to modify access for.
7. Do one of the following:
   - To change access, select the new access level.
   - To revoke access, remove the user's or role's access.
8. Click **Done**.
9. On the Edit Topic page, click **Save**.

Remove a Topic

Remove a topic when it's no longer needed and you don't want users to access it in Agent Hub.

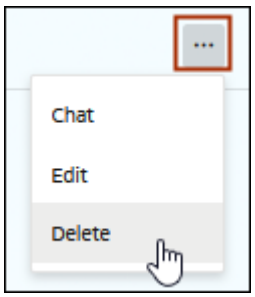
Before you remove a topic, consider how the topic is being used and the impact that removing it can have on users and existing conversations.

Before you remove a topic:

- Confirm that users no longer need the topic.
- Review the agents and connected tools and services associated with the topic.
- Consider whether users have existing conversations that they started from the topic.
- Confirm whether the topic is referenced or used by other Agent Hub configuration.

Copyright © 2026, Oracle and/or its affiliates.

1. Open Agent Hub.
2. In the navigation panel, click **Registry** Registry .
3. On the Registry page, click the **Topics** tab Topics.
4. Locate the topic you want to remove, click **More Actions** ***.
5. Click **Delete**.



Copyright © 2026, Oracle and/or its affiliates.

7

Administer Agent Hub

This chapter describes how to administer Agent Hub, including configuring the model and processing region, configuring guardrails, and managing access to the topics feature.

Topics:

- About Agent Hub Administration
- Configure the Agent Hub Model
- Configure Agent Hub Guardrails
- Manage Access to Resources and Features in Agent Hub

About Agent Hub Administration

Agent Hub administrators configure and manage settings that apply across the Agent Hub environment.

Agent Hub administration is separate from administration of the underlying AI Data Platform environment. An Agent Hub administrator and an AI Data Platform administrator can be different users. Some access and resources required by Agent Hub are configured in AI Data Platform or the AI Registry rather than in Agent Hub.

Agent Hub administrators perform the following types of configuration:

- **Model and processing region**: Configure the processing region and LLM that Agent Hub uses for orchestration and direct responses. See Understand Agent Hub Model Configuration.
- **Guardrails**: Configure controls that help protect Agent Hub interactions from specified types of unwanted content or behavior. See Understand Agent Hub Guardrails.
- **Topics feature access**: Grant users or roles the appropriate level of access to the Topics feature. See Grant Access to the Topics Feature.

Configure the Agent Hub Model

Configure the processing region and large language model (LLM) that Agent Hub uses for orchestration and direct responses.

Topics:

- Understand Agent Hub Model Configuration
- Configure the Processing Region and Model

Understand Agent Hub Model Configuration

Agent Hub uses a configured large language model (LLM) to support orchestration and provide direct responses. An Agent Hub administrator configures the processing region and model that Agent Hub uses for these capabilities.

Copyright © 2026, Oracle and/or its affiliates.

The models available for configuration depend on the selected processing region. When the administrator selects a region, Agent Hub provides a list of the models that are available for that region. Model availability can differ between regions and can change over time.

Understand the Processing Region

The processing region determines where Agent Hub performs model processing. The models available for selection depend on the selected region.

Understand Model Availability

The processing regions and models available in Agent Hub are based on Oracle Cloud Infrastructure (OCI) Generative AI availability. Model availability varies by region and can change over time.

For current information about model availability by region, see Generative AI Models by Region.

Understand the Configured Model

The model selected by the administrator becomes the configured LLM that Agent Hub uses to evaluate user requests and generate responses when no specialized agent or tool is needed.

When Agent Hub evaluates a prompt without a preselected agent, the orchestrator uses the configured LLM to help determine how to handle the request. If a specialized agent or tool isn't required, Agent Hub can use the configured LLM to provide the response directly.

The configured Agent Hub model doesn't determine which LLM an individual agent uses. Agents can use models as part of their own processing based on how those agents were developed and configured.

Why this matters

The processing region and model configuration determine which LLM Agent Hub uses for orchestration and direct responses. Understanding the relationship between region and model availability can help administrators select an available model that meets their organization's requirements.

For information about configuring these settings, see Configure the Processing Region and Model.

For information about how Agent Hub uses the configured LLM when processing user requests, see How Agent Hub Uses Large Language Models (LLMs).

Configure the Processing Region and Model

As an Agent Hub administrator, you can configure the processing region and large language model (LLM) that Agent Hub uses for orchestration and direct responses.

The models available for selection depend on the processing region. For information about how processing region and model configuration work together, see Understand Agent Hub Model Configuration.

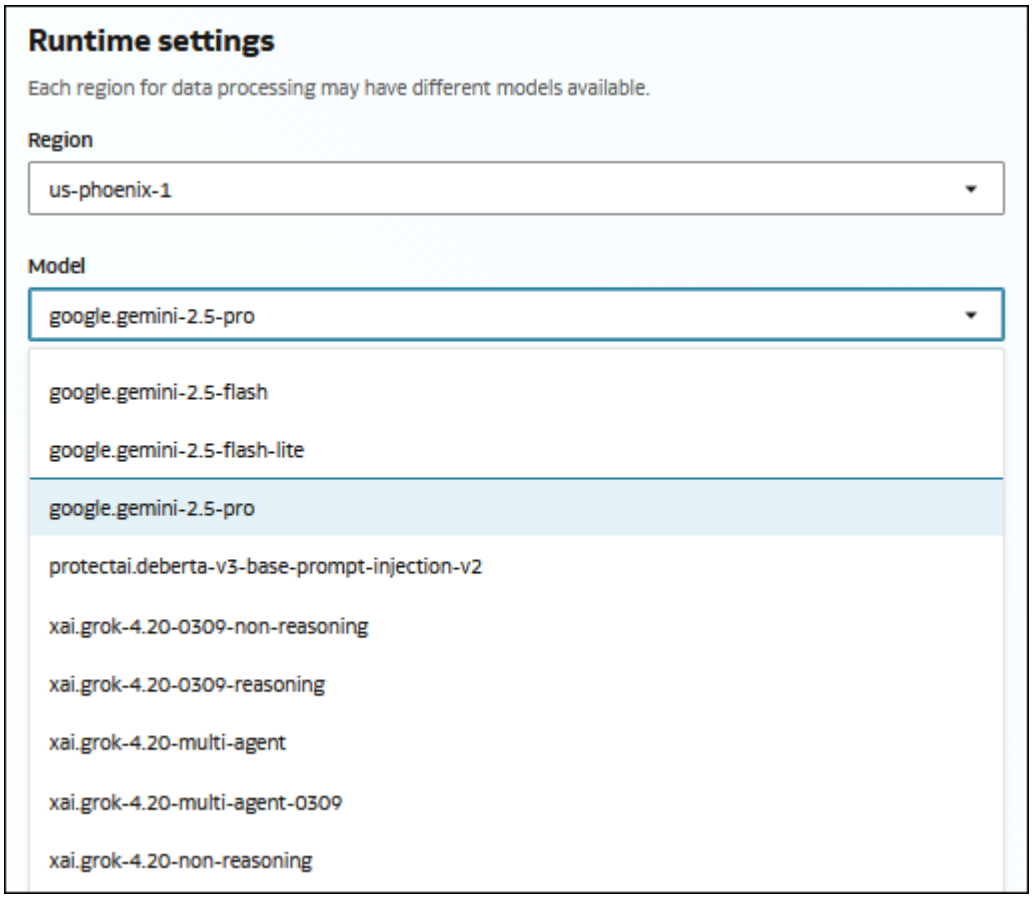
1. Open Agent Hub.
2. At the bottom of the navigation panel, click your user name, and then click **Administration**.
3. In the Administration page, go to **Runtime settings**.

Copyright © 2026, Oracle and/or its affiliates.

4. In **Region**, select the region to use for data processing.

   Agent Hub updates the list of models available for the selected region.

5. In **Model**, select the model that you want Agent Hub to use.



6. Click **Save**.

Configure Agent Hub Guardrails

Configure guardrails to help protect Agent Hub interactions from sensitive information, inappropriate content, and prompt injection attempts.

Topics:

- Understand Agent Hub Guardrails
- Configure Agent Hub Guardrails

Understand Agent Hub Guardrails

Guardrails help protect Agent Hub interactions by detecting or preventing specified types of unwanted content or behavior. Agent Hub administrators configure guardrails that apply to the Agent Hub orchestrator.

Agent Hub provides guardrails for personally identifiable information (PII), content moderation, and prompt injection detection.

Copyright © 2026, Oracle and/or its affiliates.

Changes to guardrail settings take effect immediately after you save them.

Personally Identifiable Information

The **Personally identifiable information (PII)** guardrail helps protect sensitive information by detecting PII in user input and generated responses. PII can include information such as names, email addresses, telephone numbers, and physical addresses.

When protection is enabled, the guardrail helps prevent sensitive information from being exposed during Agent Hub interactions.

Content Moderation

The **Content moderation** guardrail detects potentially harmful or inappropriate content in user input and generated responses. This can include hateful, sexual, violent, toxic, derogatory, or harassment-based content.

When protection is enabled, the guardrail helps prevent content that meets the detection criteria from being processed or generated.

Prompt Injection Detection

The **Prompt injection detection** guardrail detects potentially malicious instructions in user input that attempt to override an AI system's intended instructions or behavior.

When protection is enabled, the guardrail helps prevent detected prompt injection attempts from affecting request processing.

Guardrails and Other Platform Protections

Guardrails configured in Agent Hub Administration apply to the Agent Hub orchestrator. They don't replace or control the guardrails configured for individual agents.

When Agent Hub invokes an agent, that agent's own guardrail configuration applies to its processing. The protections provided by an agent depend on how that agent is configured.

Why this matters

Guardrails provide administrators with controls for protecting Agent Hub interactions from specific types of unwanted content or behavior. Understanding what each guardrail protects against can help administrators determine which protections are appropriate for their organization's Agent Hub environment.

For information about changing guardrail settings, see Configure Agent Hub Guardrails.

Configure Agent Hub Guardrails

As an Agent Hub administrator, configure guardrails for the Agent Hub orchestrator to help protect interactions from sensitive information, inappropriate content, and prompt injection attempts.

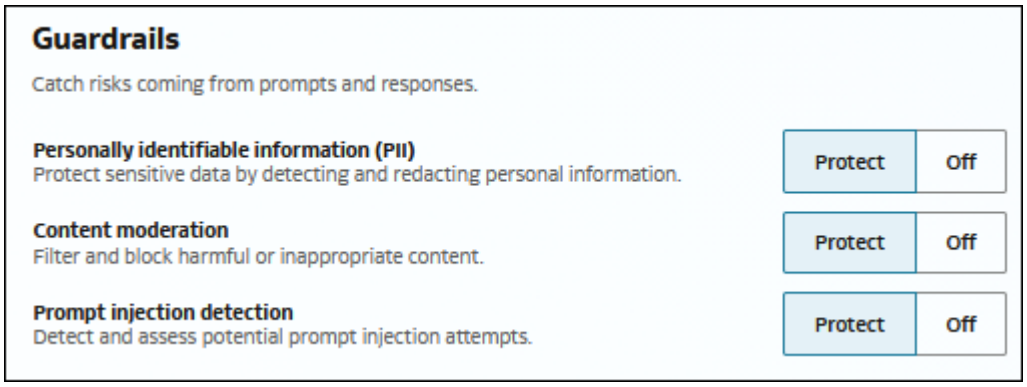
You can set each guardrail to **Protect** or **Off**. Changes to guardrail settings take effect immediately after you save them.

For information about the available guardrails, see Understand Agent Hub Guardrails.

1. Open Agent Hub.

Copyright © 2026, Oracle and/or its affiliates.

2. At the bottom of the navigation panel, click your user name, and then click **Administration**.
3. In the Administration page, go to **Guardrails**.
4. Configure the guardrail settings as needed for your organization.



5. Click **Save**.

Manage Access to Resources and Features in Agent Hub

Understand how to manage access to resources and features in Agent Hub and where to configure the required access.

Topics:

- Understand Agent Hub Administration and Access Responsibilities
- Grant Access to the Topics Feature
- Change or Revoke Access to the Topics Feature

Understand Agent Hub Administration and Access Responsibilities

Access to Agent Hub features and AI resources can depend on permissions configured in Agent Hub and AI Data Platform. Different administrators can be responsible for configuring access to these capabilities.

Agent Hub administrators manage access to Agent Hub-specific features, such as the Topics feature. Access to the underlying AI Data Platform environment and registered AI resources is managed separately.

Agent Hub administrators manage access to Agent Hub-specific features, such as the Topics feature. Access to the underlying AI Data Platform environment and registered AI resources is managed separately.

Understand Where Access Is Managed

This table summarizes where administrators configure the different types of access that can be required to work with resources and features in Agent Hub.

Copyright © 2026, Oracle and/or its affiliates.

Access	Where Managed
AI Data Platform environment and registered AI resources	AI Data Platform
Topics feature	Agent Hub Administration
Individual topic	Topic access section of the Edit Topic page in Agent Hub

Understand Access Managed Outside of Agent Hub

Some access required to use Agent Hub is configured in AI Data Platform. This includes access to the underlying platform environment and registered AI resources.

Having access to Agent Hub doesn't automatically provide access to every AI resource. Your organization must configure the appropriate access for the resources that users need.

Understand Direct and Topic-Based Agent Access

Users can work with an agent directly or through a topic, depending on the access granted by their organization.

With *direct access*, users can select an available agent from the Registry and start a conversation with it.

With *topic-based access*, users can work with agents associated with a topic without necessarily having direct access to each agent. Other required access still applies.

For more information about topic-based access, see Understand Topic-Based Access.

Understand Topic Access Responsibilities

Access to topics is configured at two levels.

An *Agent Hub administrator* grants access to the Topics feature from Agent Hub Administration. This feature-level access determines whether a user can access the Topics feature and what actions they can perform.

A *topic administrator* separately grants access to individual topics from the Topic access section of the Edit Topic page. Both levels of access are required to use a particular topic.

Both levels of access are required to use a particular topic.

For information about configuring Topics feature access, see Grant Access to the Topics Feature.

For information about configuring access to an individual topic, see Grant Users or Roles Access to a Topic.

Why this matters

Understanding where access is managed helps administrators identify which settings they can configure in Agent Hub and which require administration in Oracle AI Data Platform.

For information about Agent Hub access, see About the Agent Hub Access Model.

Copyright © 2026, Oracle and/or its affiliates.

Grant Access to the Topics Feature

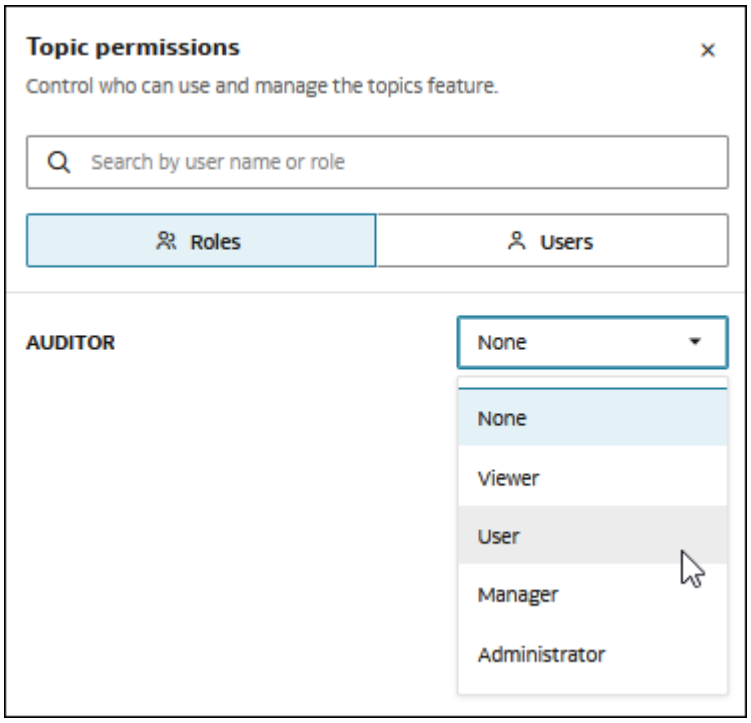
As an Agent Hub administrator, you can grant users or roles access to the Topics feature to control what business users can do with topics in Agent Hub.

Access to the Topics feature doesn't automatically provide access to an individual topic. A topic administrator separately grants access to specific topics.

For information about the two levels of topic access, see Understand Topic-Based Access.

For information about granting access to an individual topic, see Grant Users or Roles Access to a Topic.

1. Open Agent Hub.
2. At the bottom of the navigation panel, click your user name, and then click **Administration**.
3. In the Administration page, go to **Topic permissions** and click **Set permission**.
4. Select **Roles** or **Users**, depending on how you want to grant access.
5. Locate the role or user that you want to grant access to.



6. Select the appropriate access level:
   - **None**: The role or user doesn't have access to the Topics feature.
   - **Viewer**: The role or user can view topics where the applicable individual-topic access permits it.
   - **User**: The role or user can use topics where the applicable individual-topic access permits it.

Copyright © 2026, Oracle and/or its affiliates.

- **Manager**: The role or user can manage topics where the applicable individual-topic access permits it, including updating topic information and managing associated AI resources.
- **Administrator**: The role or user has administrative capabilities for topics.

7. Click **Save**.

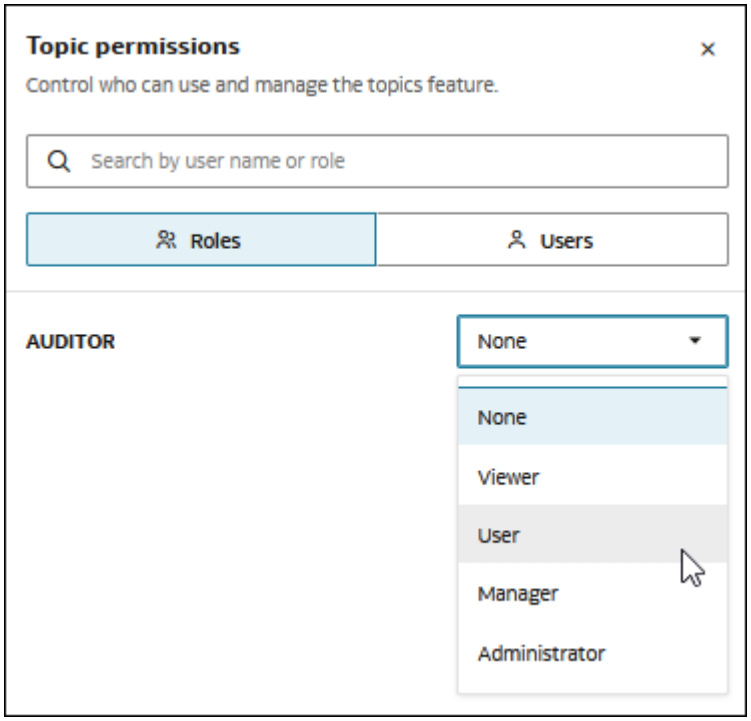
Change or Revoke Access to the Topics Feature

As an Agent Hub administrator, you can change or revoke access when a role or user no longer needs its current level of access to the Topics feature.

Changing or revoking Topics feature access can affect the user's ability to work with individual topics, even if the user still has access to those topics.

For information about Topics feature access levels, see Understand Topic-Based Access.

1. Open Agent Hub.
2. At the bottom of the navigation panel, click your user name, and then click **Administration**.
3. In the Administration page, go to **Topic permissions** and click **Set permission**.
4. Select **Roles** or **Users**, depending on the type of access you want to change.
5. Locate the user or role whose access you want to change.



6. Do one of the following:
   - To change access, select the new access level.
   - To revoke access, set the access level to **None**.
7. Click **Save**.

Copyright © 2026, Oracle and/or its affiliates.

8

Agent Hub Known Issues

This topic lists current limitations, bugs, and behavior inconsistencies identified in Oracle Agent Hub. These issues are actively being tracked and will be addressed in future updates.

Known Issues

Agent Registry Doesn't Apply the Selected Sort Order

When you sort agents in the Agent Registry, the selected sort order isn't applied. Agents are always listed with the newest agents first, regardless of whether you select ascending or descending order.

All Requests Are Routed to the Only Registered Agent

When only one agent is registered in Agent Hub, all chat requests are routed to that agent. This includes general conversational requests that would otherwise be handled by Agent Hub's default conversational capability.

Uploaded Files Might Not Display Correctly in Chat History

If an error occurs while processing an uploaded file, the file might not display correctly when you reopen the conversation from chat history.

Agent Hub Registry Displays Only the First 50 Agents

The Agent Hub Registry displays only the first 50 registered agents. Additional registered agents don't appear in the Registry and can't be found through Agent Hub.

MCP Server Registration Dialog Can Become Unresponsive

If MCP server registration fails, such as when invalid credentials are provided, the Register MCP Server dialog might remain in the *Processing...* state.

The **Cancel** and **Continue** buttons become unavailable, preventing you from closing the dialog or retrying the registration.

Pressing Enter Cancels a Delete Operation

In a delete confirmation dialog, pressing Enter selects **Cancel** instead of **Delete**.

Incorrect Prompt Dates and Times Appear in Chat History

When prompt timestamps are unavailable, Agent Hub might display December 31, 1969, instead of the correct date. This issue can also occur when you reopen an existing conversation.

Also, the timestamp displayed for a prompt might show December 31, 1969, at 4:00 PM instead of the time the prompt was submitted.

Previous Tool Approval Options Can Be Selected Again

Copyright © 2026, Oracle and/or its affiliates.

After Agent Hub finishes processing a request, options in an earlier tool execution approval prompt might remain selectable.

Selecting one of these options starts another request unintentionally.

Topic Chat Can't Resume After Stopping a Remote MCP Tool Call

If you select **Stop** while a remote MCP tool call is running in a topic-based conversation, the conversation might become unresponsive. Subsequent prompts aren't processed, including requests to cancel the operation.

Incorrect Stop Message Appears When Switching Between Chats

If you switch between chats while responses are still being processed, Agent Hub might display the message "You stopped this response" even though you didn't stop the response. The response might still be processing despite the message.

Copyright © 2026, Oracle and/or its affiliates.

9

Agent Hub Frequenty Asked Questions

Find answers to common questions about accessing, using, and administering Agent Hub.

Topics

- Access Agent Hub and AI Resources FAQs
- Work with Agent Hub FAQs
- Administer Agent Hub FAQs

Access Agent Hub and AI Resources FAQs

Find answers to common questions about accessing Agent Hub and the AI resources available through it.

Where can I find Agent Hub?

You can open Agent Hub directly from the Agent Hub URL provided by your organization. If you have access to AI Data Platform, you can also open Agent Hub from the AI Data Platform home page.

You must have the required access to Agent Hub before you can open and use it.

See How to Open Agent Hub.

Why can I access Agent Hub but not see an agent?

Access to Agent Hub doesn't automatically provide access to every agent. The agents available to you depend on the access granted by your organization.

If an agent isn't available to you, contact the appropriate administrator or resource owner.

For information about Agent Hub access requirements, see About the Agent Hub Access Model.

Why can I see an agent but not use it?

Permission to view an agent doesn't necessarily provide permission to use it. Your organization controls which agents you can interact with based on the access granted to you.

If you can see an agent but can't use it, contact the appropriate administrator or resource owner.

How do I get access to an agent or topic?

Access to agents and topics is managed by your organization's administrators.

For an agent, the required access can include permissions configured in AI Data Platform and the AI Registry.

For a topic, you need the appropriate access to the Topics feature and access to the individual topic. An Agent Hub administrator manages access to the Topics feature, and a topic administrator manages access to an individual topic.

Copyright © 2026, Oracle and/or its affiliates.

Contact the appropriate administrator or resource owner to request the access you need.

See About the Agent Hub Access Model and Understand Topic-Based Access.

Why can I use an agent through a topic when I don't have direct access to the agent?

Topic-based access can provide an alternative access path to the agents associated with a topic.

If you have the required access to a topic, you can use agents associated with that topic without receiving a separate individual-agent grant for each agent. Other required access still applies.

See Understand Topic-Based Access.

What access do I need to use a topic?

To use a topic, you need access at two levels:

- **Topics feature access**: Determines whether you can use the Topics feature and what actions you can perform.
- **Individual topic access**: Determines whether you can use a particular topic.

To start a conversation from a topic, you need the appropriate access at both levels. Other required Agent Hub and AI Registry access also applies.

See Understand Topic-Based Access.

Additional FAQs

If you didn't find the answer to your question, try these additional Agent Hub FAQs:

- Work with Agent Hub FAQs
- Administer Agent Hub FAQs

Work with Agent Hub FAQs

Find answers to common questions about working with AI resources and understanding Agent Hub behavior.

Can I register an agent or other AI resource from Agent Hub?

No. Agent Hub allows business users to discover and interact with AI resources that have been made available to them.

An administrator registers and manages supported resources through AI Data Platform's AI Registry and not from Agent Hub.

See How Enterprise AI Resources Become Available.

Why does the Orchestrator route me to a different agent than I expected?

When you enter a prompt without selecting an agent first, the orchestrator evaluates your request and the AI resources available to you. It uses descriptive information registered with agents, including their purpose and capabilities, to identify agents that are relevant to your request.

In an orchestrated conversation, Agent Hub evaluates each new request and might select a different agent when the request requires different capabilities.

Copyright © 2026, Oracle and/or its affiliates.

Depending on your approval setting, Agent Hub might automatically use the selected agent or present agents for you to choose from. When agent selection is presented, you can choose a different available agent.

If you already know which agent you want to use, select that agent before entering your prompt.

See How Agent Hub Processes Requests, Select an Agent, and Understand Approvals in Agent Hub.

How can I tell which agent or tool handled my request?

When Agent Hub uses an agent or tool to handle your request, click the processing status indicator (for example, **Completed in 18s**) in the chat to open the **Thinking Activity** panel. The panel displays information about request processing, including the names of agents or tools invoked.

In an orchestrated conversation, different agents can handle successive requests. You can use **Thinking Activity** to identify which agent handled a particular request.

See Understand Request Activity.

Why can't I find tools or MCP servers in the Agent Hub Registry?

Business users don't discover and select tools or MCP servers from the Agent Hub Registry in the same way that they discover and select agents.

Tools provide capabilities that agents or other supported Agent Hub functionality can use when processing requests. MCP servers expose tools that can be made available for supported use in Agent Hub. These resources can participate in processing even though you don't select them directly from the Registry.

See AI Resources Supported by Agent Hub.

Additional FAQs

If you didn't find the answer to your question, try these additional Agent Hub FAQs:

- Access Agent Hub and AI Resources FAQs
- Administer Agent Hub FAQs

Administer Agent Hub FAQs

Find answers to common questions about administering access, permissions, guardrails, and other Agent Hub settings.

What's the difference between Agent Hub access and AI Data Platform access?

Agent Hub and Oracle AI Data Platform manage different aspects of access to enterprise AI.

Agent Hub administrators manage access to Agent Hub-specific features, such as the Topics feature. Access to the underlying AI Data Platform environment and registered AI resources is managed separately.

Depending on the resources and functionality that users need, access configured in both environments might be required.

For information about Agent Hub access requirements, see About the Agent Hub Access Model.

Copyright © 2026, Oracle and/or its affiliates.

What's the difference between Topics feature access and access to an individual topic?

Topics feature access controls what a user or role can do with topics generally in Agent Hub. An Agent Hub administrator manages this access from Agent Hub Administration.

Individual topic access controls what a user or role can do with a particular topic. A topic administrator manages this access from the Topic access section of the Edit Topic page.

A user needs the appropriate access at both levels to work with an individual topic.

See Understand Topic-Based Access, Grant Access to the Topics Feature, and Grant Users or Roles Access to a Topic.

Do I need to grant users direct access to every agent in a topic?

No. Topic-based access can provide users with access to agents associated with a topic without requiring a separate individual-agent grant for each agent.

Other required access still applies. For example, users must have the applicable access to Agent Hub and the AI Registry in addition to the required topic access.

See Understand Topic-Based Access.

Which access settings are managed in Agent Hub and which are managed in AI Data Platform?

Agent Hub administrators manage access to Agent Hub-specific features, such as the Topics feature. Topic administrators manage access to individual topics.

Access to the underlying AI Data Platform environment and registered AI resources is managed separately in Oracle AI Data Platform.

For a summary of where different types of access are managed, see Understand Agent Hub Administration and Access Responsibilities.

For information about configuring access in AI Data Platform see the applicable AI Data Platform documentation.

Why are different models available for different processing regions?

The models available for Agent Hub depend on the selected processing region. Model availability can differ between regions based on service availability and regional or sovereign requirements.

For current model availability by region, see Generative AI Models by Region.

For more information about Agent Hub model configuration, see Understand Agent Hub Model Configuration.

Additional FAQs

If you didn't find the answer to your question, try these additional Agent Hub FAQs:

- Access Agent Hub and AI Resources FAQs
- Work with Agent Hub FAQs

Copyright © 2026, Oracle and/or its affiliates.