Diving Deep into Bedrock AgentCore

Diving Deep into Bedrock AgentCore
Prerequisites
Amazon Bedrock AgentCore Fundamentals
AgentCore Runtime
AgentCore Gateway
AgentCore Identity
Inbound Auth
Outbound Auth
AgentCore Memory
AgentCore Tools
AgentCore Observability

AgentCore
AgentCore Documentation

AWS account access

Workshop catalog in AWS Builder Center

Content preferences

Language
English

Exit event

Event ends in 20 hours 27 minutes.

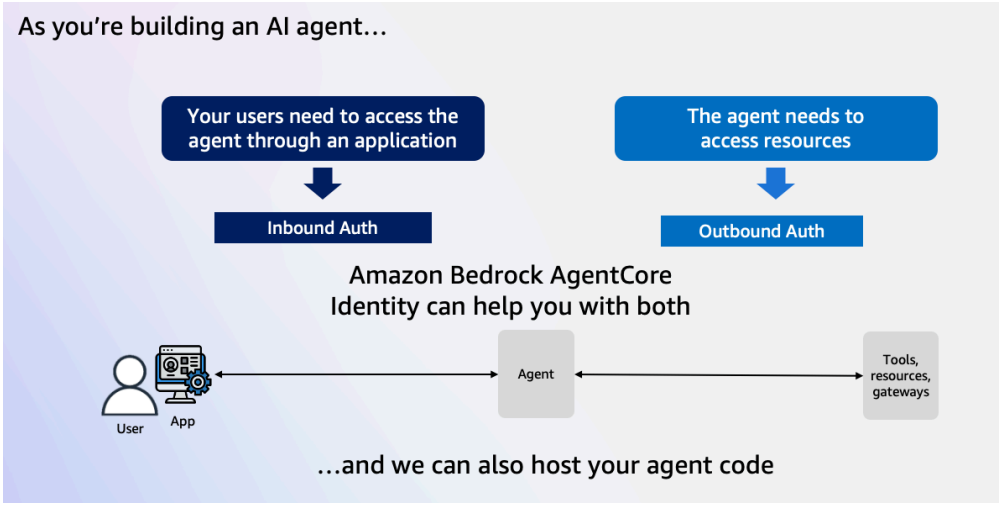
AgentCore Identity

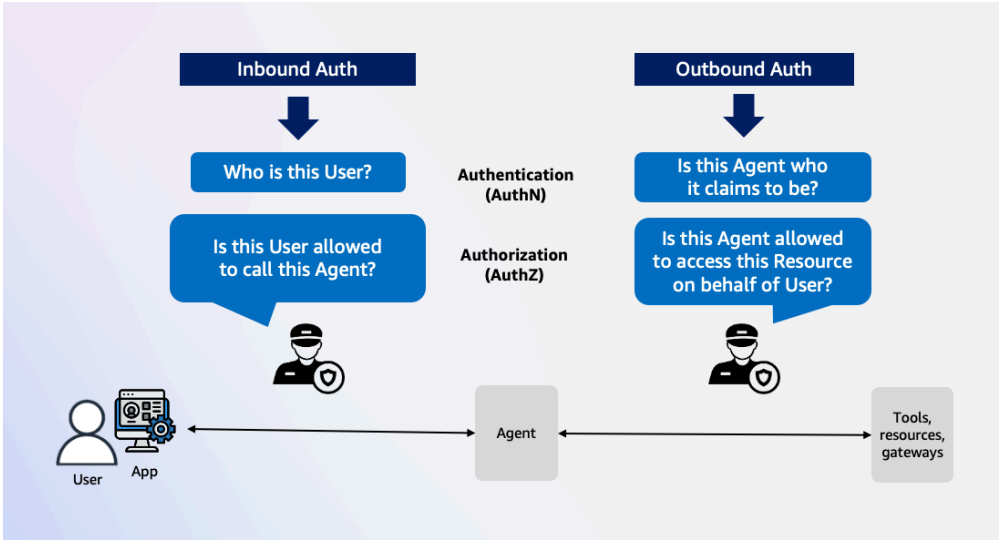
Introduction to Amazon Bedrock AgentCore Identity

Amazon Bedrock AgentCore Identity is a comprehensive identity and credential management service designed specifically for AI agents and automated workloads. It provides secure authentication, authorization, and credential management capabilities that enable users to invoke agents, and agents to access external resources and services on behalf of users while maintaining strict security controls and audit trails. Agent identities are implemented as workload identities with specialized attributes that enable agent-specific capabilities while maintaining compatibility with industry-standard workload identity patterns. The service integrates natively with Amazon Bedrock AgentCore to provide comprehensive identity and credential management for agent applications.

Types of Auth supported by AgentCore Identity

AgentCore Identity lets you validate inbound access (Inbound Auth) for users and applications calling agents or tools in an AgentCore Runtime or validate access to AgentCore Gateway targets. It also provide secure outbound access (Outbound Auth) from an agent or Gateway target to external services. It integrates with your existing identity providers (such as Amazon Cognito) while enforcing permission boundaries for agents acting independently or on behalf of users (via OAuth).



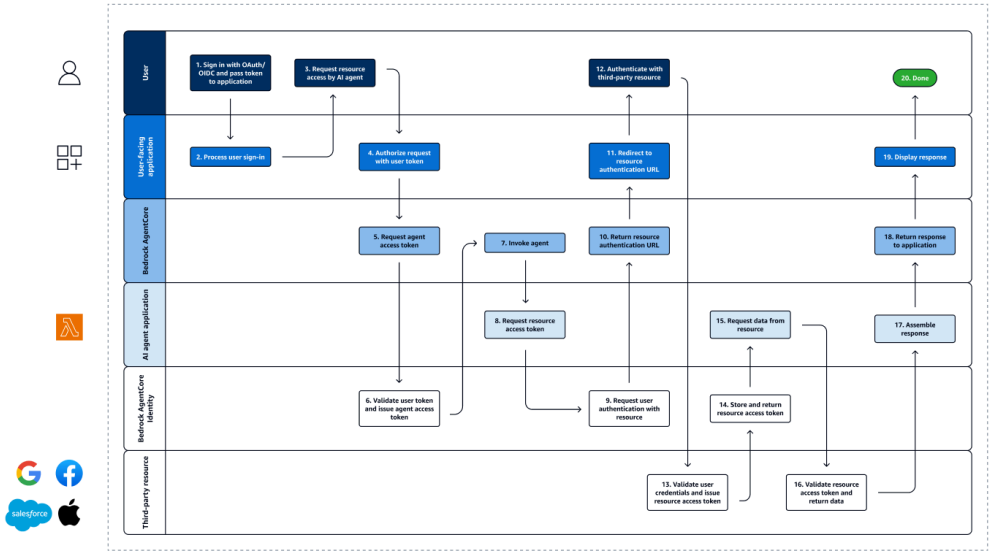


- Inbound: Inbound Auth is used to grant access to users to invoke agents or tools. Consider a scenario where a user wants to invoke an agent within an application. That user must have permissions to invoke the agent and the agent should retain who the user is when performing tasks. Inbound auth supports two mechanisms for auth, AWS IAM or Oauth. Oauth allows agents builders a way to invoke the agent without having to grant users IAM permissions.
- Outbound: Outbound auth is used to grant agents or AgentCore Gateways access to AWS services or external resources on behalf of users. AgentCore Identity will use the provided IAM execution role to access AWS resources. Oauth 2-leg or 3-leg access flows will be used for external resources.

How Bedrock AgentCore Identity works

At its core, AgentCore Identity provides secure authentication mechanisms for agents to access resources while maintaining proper security boundaries. This enables services to make appropriate authorization decisions, supporting sophisticated use cases like cross-service agents that can access internal calendar systems and external services like Google Calendar within a single workflow.

The following diagram illustrates the complete AgentCore Identity workflow, showing how users, applications, agents, and AWS resources and third-party services interact securely:



The AgentCore Identity workflow consists of the following steps:

1. User signs in with OAuth/OIDC and passes token to application
2. User-facing application processes user sign-in
3. User requests resource access by AI agent
4. User-facing application makes request to agent service with user token
5. Bedrock AgentCore requests workload access token from Agent Credential Provider
6. AgentCore Identity validates the user token and issues an workload access token
7. AI agent application invokes agent
8. Agent requests resource access token
9. Amazon Bedrock AgentCore Identity requests user authentication with resource
10. Bedrock AgentCore requests user authentication
11. User-facing application displays authentication and consent prompt
12. User consents to share data
13. Third-party resource validates user credentials and issues resource access token
14. AgentCore Identity stores and returns resource access token
15. Agent requests data from resource
16. Third-party resource validates resource access token and returns data
17. AI agent application assembles response
18. AgentCore returns response to application
19. User-facing application displays response
20. Process completes

Learn more about AgentCore Identity terminology

Use AgentCore Identity when you need to:

1. **Secure agent access** to prevent unauthorized usage
2. **Integrate with enterprise identity systems**
3. **Enable agents to access external services** securely
4. **Implement fine-grained access control** for agent capabilities
5. **Reduce consent fatigue** using a secure token vault

Labs

In the following labs, you'll learn how to implement both Inbound and Outbound authentication for your agents:

- **Lab: Inbound Auth** - Configure an agent with Amazon Cognito authentication
- **Lab: Outbound Auth** - Enable an agent to securely access external services

---

Previous Next