

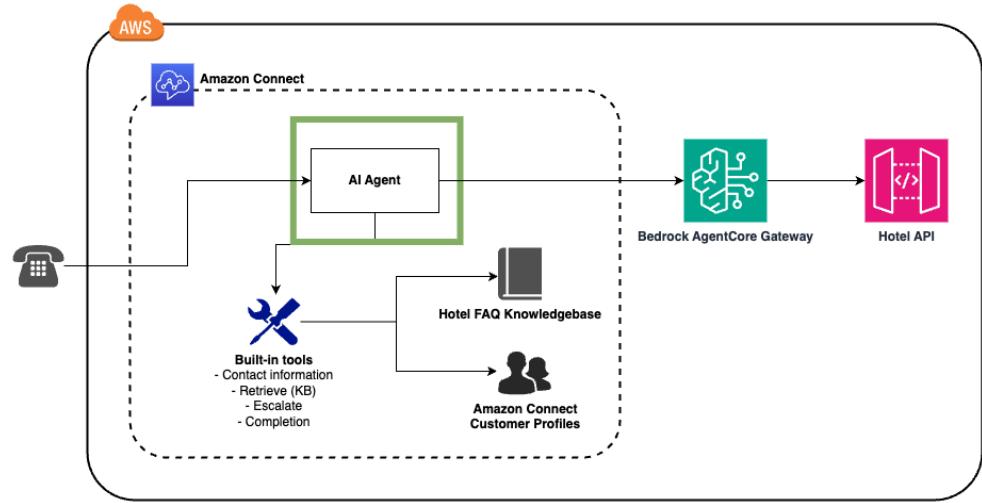


Building Intelligent Customer Service with Agentic AI on Amazon Connect

- ▼ Welcome to AnyCompany Hotels
 - Choose Your Deployment Path
 - Prerequisites Setup (Path B Only)
 - ▼ Building the Reservation System
 - Task 1: Get Your Stack Outputs
 - Task 2: Creating Your MCP Server
 - Task 3: Associating Your MCP Server with Amazon Connect
 - Task 4: Enable Customer Profiles
 - Task 5: Access Amazon Connect Admin Interface
 - Task 6: AI Agent Setup**
 - Task 7: Configure AI Prompt
 - Task 8: Create Lex Bot for Connect
 - Task 9: Build Your Flow
 - Task 10: Create Your Customer Profile
 - Task 11: Associate a Phone Number
 - Task 12: Test Your AI Agent
 - Task 13: Experience Agentic Voice
 - ▼ Handling Customer Questions
 - Task 1: Upload FAQ Documents
 - Task 2: Add the Retrieve Tool
 - Task 3: Test Knowledge Base Queries
 - ▼ Human Escalation
 - Task 1: Configure the Escalate Tool
 - Task 2: Build the Escalation Flow
 - Understanding Step-by-step Guides (Optional)
 - Task 3: Test Escalation
 - ▼ Experiment and Explore
 - Experiment 1: Change Your Agent Personality
 - Experiment 2: Custom Voices
- Workshop catalog in AWS Builder Center [🔗](#)
- ▼ Content preferences
- Language [▼](#)
- English

Task 6: AI Agent Setup

In this section we'll create our AI Agent in Amazon Connect along with the security permissions the agent will operate under.



Step 1: Create a Security Profile for Your AI Agent

Now that you're logged into the Connect admin interface, let's create the security profile that defines what your AI agent can do.

Amazon Connect uses the same security controls for AI agents as it does for human agents and contact center support staff. Security profiles define what actions an agent can perform within Amazon Connect and which APIs from your MCP server the agent can access. This ensures consistent access management, unified audit trails, and granular permissions following least-privilege principles across your entire contact center—whether the agent is human or AI.

Create the AI Agent Security Profile:

1. Click "Users" in the left navigation, then select **Security profiles**
2. Click "Add new security profile"
3. Configure the profile:
 - **Security profile name:** Hotel-Booking-AI-Agent [🔗](#)
 - **Description:** Security profile for AI agents handling hotel reservations [🔗](#)
4. Set permissions for the AI agent:
 - **Contact Control Panel (CCP):** Select "Access Contact Control Panel"
 - **Agent Applications:** Select "Connect assistant - View"
 - **Tools:** Select "Access" for all 5 of your hotels APIs (cancelReservation, createBooking, etc)
5. Click Save

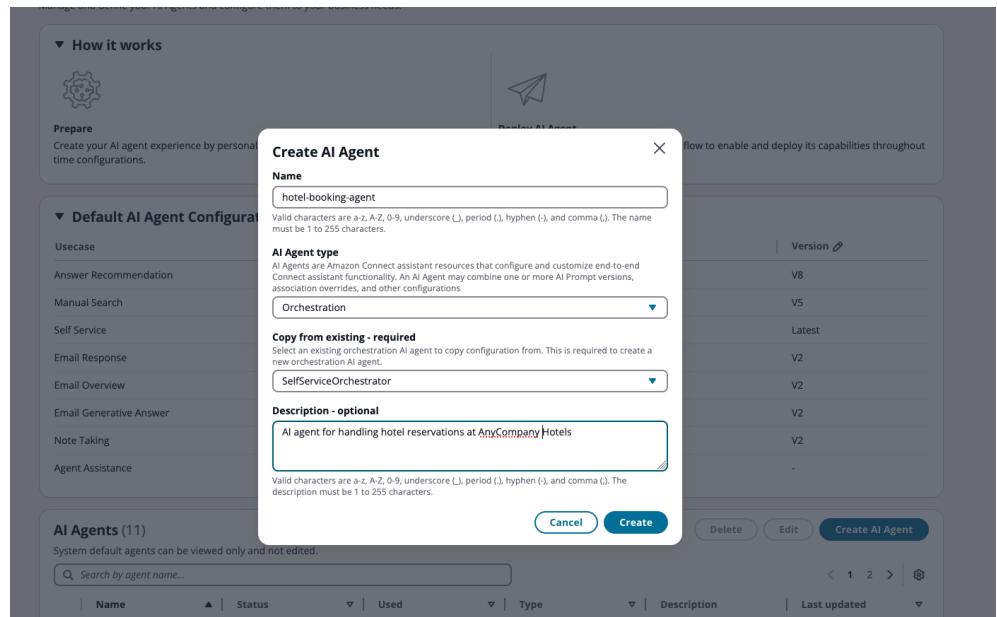
Your AI agent now has a security profile that defines its operational boundaries within Amazon Connect, just like your human agents.

Step 2: Create Your AI Agent

Now let's create the AI agent that will handle customer calls.

Create the Agent:

1. Click "AI agent designer" in the left navigation
2. Click "AI agents" to view AI agents
3. Click "Create AI agent"
4. Configure the agent:
 - o **Name:** hotel-booking-agent
 - o **AI Agent type:** Select Orchestration
 - o **Copy from existing:** Select SelfServiceOrchestrator
 - o **Description:** AI agent for handling hotel reservations at AnyCompany Hotels
5. Click "Create"



Your AI agent is now created and the configuration page will open.

Step 3: Configure Your AI Agent

Now let's configure the basic settings for your AI agent.

Configure Basic Settings:

1. Set the locale: English (US)
2. Select the security profile: Hotel-Booking-AI-Agent (the one you created in Step 1)
3. Save your AI Agent to apply the security profile

Your AI agent is now configured with the proper security profile. The tool configuration is just below which we will go through in the next steps.

Step 4: Add Hotel API Tools

Let's add the hotel reservation tools from your MCP server.

Add the Tools:

1. Click "Add tool" in the Tools tab
2. Select a Namespace from the dropdown: gateway_anycompany-hotels-mcp-server-{shortcode}
3. Select the AI tool from the dropdown: anycompany-hotels-api__cancelReservation
4. Check the "User Confirmation" toggle to require the agent to confirm cancellation details with the customer before executing
5. Scroll to the bottom and click the "Add" button
6. Repeat steps 1-5 for the remaining four tools (in alphabetical order):
 - o anycompany-hotels-api__createBooking - **Enable "User Confirmation"** to confirm booking details before creating
 - o anycompany-hotels-api__getCustomerReservations (no user confirmation needed)
 - o anycompany-hotels-api__modifyReservation (no user confirmation needed)
 - o anycompany-hotels-api__searchHotels (no user confirmation needed)

Step 5: Remove the Knowledge Base Tool

Since we haven't set up the knowledge base yet, let's remove the existing **Retrieve** tool to keep things clean.

Delete the Retrieve Tool:

1. In the Tools section, find and select the **Retrieve** tool
2. Click the "Remove" button
3. Click "Save" to save your AI agent configuration

The tool will be removed from your agent. Don't worry — we'll add it back in Module 3 when we configure the knowledge base.

Step 6: Verify Your Tool Configuration

Let's verify everything is set up correctly.

Tools Overview:

Your final tool list should include these tools:

Tool Name	Type	Description	Status
Complete	Return to Control	Completes the interaction	Added by default
Escalate	Return to Control	Transfers to human agent for complex issues	Added by default
anycompany-hotels-api__searchHotels	MCP Server	Search hotels by city and check availability	<input checked="" type="checkbox"/> Added
anycompany-hotels-api__getCustomerReservations	MCP Server	Retrieve customer's existing bookings	<input checked="" type="checkbox"/> Added
anycompany-hotels-api__createBooking	MCP Server	Book new reservations	<input checked="" type="checkbox"/> Added
anycompany-hotels-api__modifyReservation	MCP Server	Change existing bookings	<input checked="" type="checkbox"/> Added
anycompany-hotels-api__cancelReservation	MCP Server	Cancel bookings (with confirmation)	<input checked="" type="checkbox"/> Added

Tool Name	Type	Description	Status
Retrieve	Connect assistant	Search knowledge base (added in Module 3)	X Removed

Tools (7)
Tools provide agentic capabilities that your AI agents can use to perform actions and access external systems.

Name	Instructions	Namespace	Permissions
anycompany_hotels_api_cancelRese...	-	gateway_anycompany-hotels-mcp-ser...	Sufficient
anycompany_hotels_api_createBook...	-	gateway_anycompany-hotels-mcp-ser...	Sufficient
anycompany_hotels_api_getCustom...	-	gateway_anycompany-hotels-mcp-ser...	Sufficient
anycompany_hotels_api_modifyRes...	-	gateway_anycompany-hotels-mcp-ser...	Sufficient
anycompany_hotels_api_searchHotels	-	gateway_anycompany-hotels-mcp-ser...	Sufficient
Complete	Mark the conversation as complete O...	-	Sufficient
Escalate	Escalate the conversation to a human ...	-	Sufficient

What's Next?

Your AI agent is now configured with the hotel reservation tools. In the next task, you'll configure the AI prompt that defines your agent's personality and behavior.

[Previous](#)
[Next](#)