

Review AI Agents

Learning Objectives

After completing this unit, you'll be able to:

- Explain how Agentforce works, including the reasoning engine, security, and agent types.
- Configure agents by selecting topics, actions, and settings to meet business requirements.
- Connect and manage agents across channels while ensuring consistent and deterministic behavior.

Key Topics

This unit prepares you for the AI Agents section of the Salesforce Agentforce Specialist exam, which makes up 35% of the overall exam. This section of the exam tests these topics.

- Given a use case, manage deterministic behavior for the agent using filters and variables.
- Explain how an agent works and how the reasoning engine powers Agentforce.
- Given a scenario, select and configure standard topics, custom topics, standard Agent actions, and custom Agent actions based on Agent types.
- Explain how to manage Agentforce security, including the concept of the Agent User and how it applies to an Employee agent, Service agent, or Sales agent.
- Given a scenario, identify when to use an Employee agent, Service agent, or Sales agent.
- Explain the process for connecting agents to various channels such as digital experience, email, and Slack.

This unit provides a number of interactive, real-world, scenario-based questions that are a lot like the ones you'll encounter as a Salesforce Agentforce specialist. Looking at these scenarios helps prepare you to take the AI Agents section of the Salesforce Agentforce Specialist exam. As you tackle the practice questions, you get immediate feedback on your answers, along with detailed information on why your answers are correct (or incorrect).

The unit also contains interactive flashcards centered around study topics that help you prepare for the AI Agents section of the exam.

Exam Practice Questions

Ready to jump in? The sample tool is not scored—it's just an easy way to quiz yourself. To use it, read the scenario, then click the answer you think is correct. Some questions can have more than one correct answer. Click **Submit** to learn whether the answer you chose is correct or incorrect, and why. When you reach the end, you can review the answers or retake the questions.

Which statement accurately describes the fundamental difference between context variables and conversation variables?

A

Context variables (prefixed \$Context) are read-only after session initialization; conversation variables are created via action outputs in Agent Builder to store data from actions during the conversation.

B

Context variables are created during actions and can be modified; conversation variables are set at the start of a session and remain static

C

Context variables store conversation history updated by the LLM; conversation variables are system metadata that is not accessible during chats.

An Agentforce Specialist needs to verify a user and then use the verified customer ID in subsequent actions within Agentforce. How can the specialist efficiently pass the verified customer ID between actions?

A

Use a context variable

B

Use a custom conversation variable

C

Use a filter variable

An Agentforce Specialist wants to ensure that certain actions in Agentforce only execute if a customer is verified. What should the specialist use to enforce this condition?

A

Context variable

B

Custom conversation variable

C

Filter

An Agentforce Service Agent, which has been successfully assisting customers with service requests in Salesforce, is now unable to help customers with issues related to a new product replacement process. The company recently implemented a custom Product Replacement object in Salesforce to track and manage these replacements. Which Agentforce Agent User change must be implemented to address this issue?

A

The permission set assigned to the Agent User needs Read access to the custom Product Replacement object.

B

The profile assigned to the Agentforce Agent User needs AI training permission to the custom Product Replacement object.

C

The permission set group assigned to the Agent User needs to grant access to the Product Replacement flow.

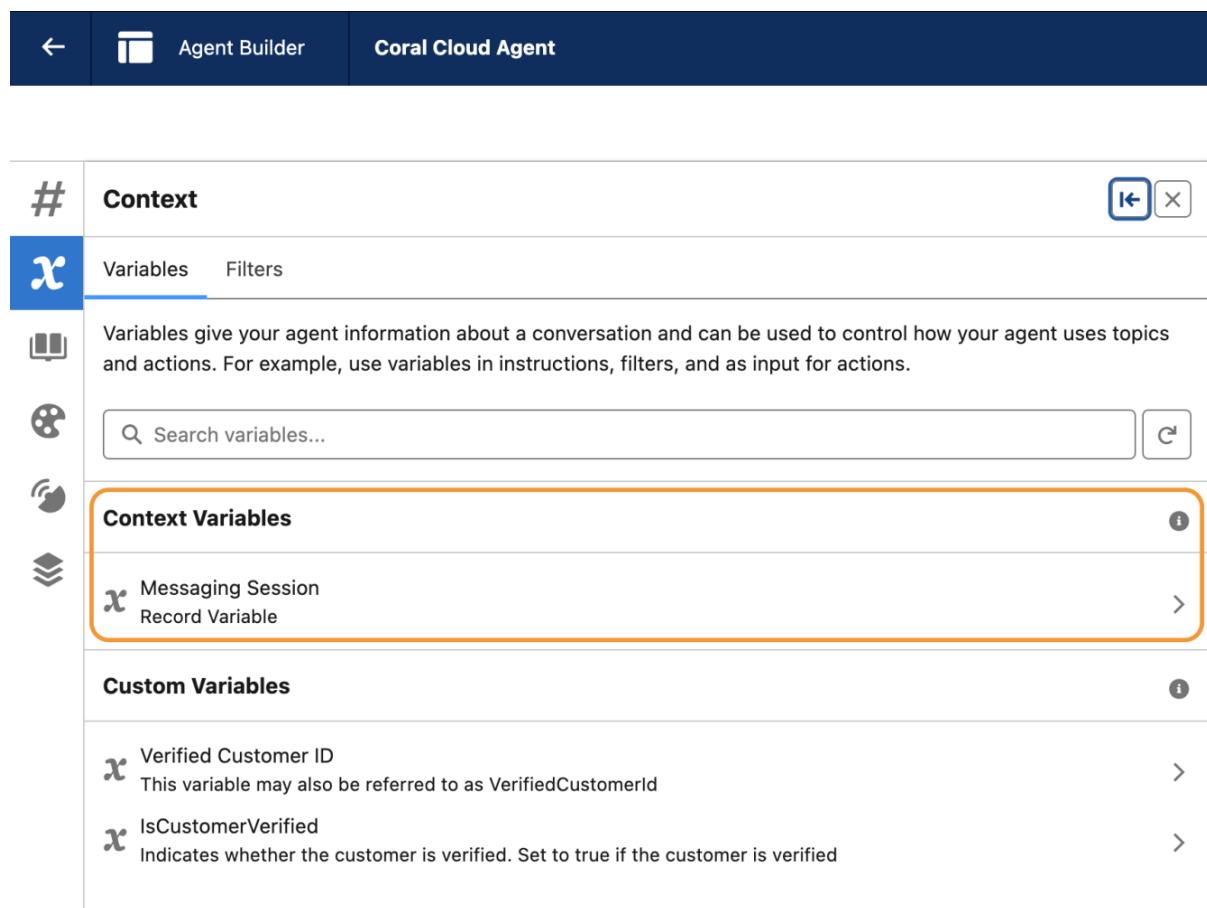
What are variables in Agentforce?

Variables in Agentforce act as secure data containers, enabling developers to control agent logic and ensure deterministic outcomes. There are primarily two types of variables: context variables and conversation variables.

Context variables

If your agent connects to customer messaging channels, it automatically includes context variables that come from [Messaging Session](#) object fields, including custom fields. Context variables are prefixed with \$Context and are read-only. They can be added to topic instructions using the syntax {!\$Context.VariableAPIName}.

The screenshot below shows context variables that come out of the box with the Messaging Session object.



The screenshot shows the Agent Builder interface with the title "Coral Cloud Agent". The main area is titled "Context" and contains a "Variables" tab selected. A search bar says "Search variables...". Below it, a section titled "Context Variables" lists "Messaging Session Record Variable". This item is highlighted with an orange border. Other items listed include "Verified Customer ID" and "IsCustomerVerified".

Example use case

Let's assume that you want your agent to always respond in the end user's language. You can write instructions as shown below using context variables.

"Always respond in {!\$Context.EndUserLanguage} language"

The above instructions assume that when a new Messaging Session record is created (upon a new agent session initiation), the EndUserLanguage field is populated with the language of the user. This EndUserLanguage is [mapped from a pre-chat or hidden channel variable](#) using an [Omni-Channel flow](#).

Conversation variables

Conversation variables are unique to the agent, and these variables hold a value only during a conversation session. There are conversation variables provided out of the box, but you can also create a custom conversation variable. Currently the variable can be of type text, boolean, or number. To learn how to create a new conversation variable, see the [documentation](#). To use conversation variables in instructions, use the format `{!VariableAPIName}`.

The screenshot below shows conversation variables.

The screenshot shows the Agent Builder interface with the title "Coral Cloud Agent". The main area is titled "# Context" and contains a "Variables" tab selected. A search bar says "Search variables...". Below it is a "Context Variables" section with a "Messaging Session Record Variable" entry. The "Custom Variables" section is highlighted with an orange border and contains two entries: "Verified Customer ID" and "IsCustomerVerified".

Note: The [creation of conversation variables](#) is only possible via the action output in Agent Builder.

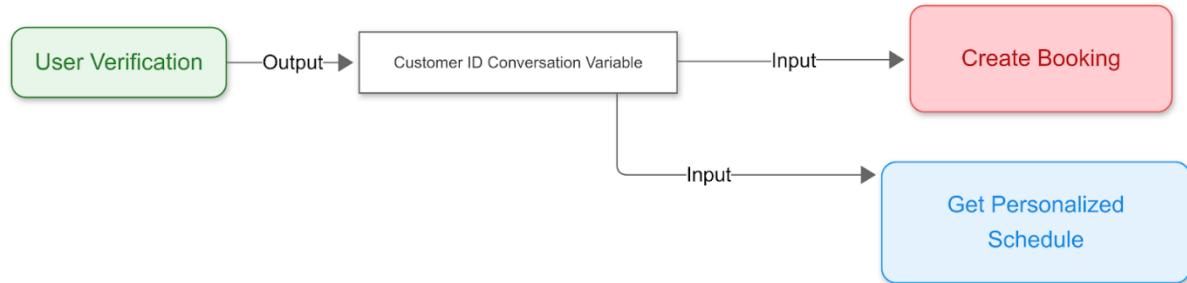
Example use case

Often, when building an agent, you need to save information from one action to use in another action. For example, imagine you have an action to verify a user. After verifying, this action gives you the user's customer ID. Later actions might need this same customer ID.

Instead of writing extra topic instructions for each action to pass along the customer ID, you can use a **custom variable**. When you save the customer ID in a custom variable, other actions can easily reuse it.

For instance, in the [Coral Cloud sample app](#), there's an action that verifies a user and returns the customer ID. Later, there's another action that lets the user book a session for a customer, and this action also requires the customer ID. By using a custom variable in Agentforce, you can automatically pass the customer ID from the verification action to the session booking action. This makes the agent instructions simpler and easier to manage.

Below is a simple diagram that helps visualize how the outputs from one action can be mapped back to custom variables, and then the same customer variables can be mapped back to the inputs of other actions.



The screenshot below from the Coral Cloud sample app shows the mapping of a variable to an action output in the Agent Builder.

View Action	
<p>#</p> <ul style="list-style-type: none"> The Member Number of the customer that is validating their identity. Advanced Settings <ul style="list-style-type: none"> Data Type: lightning__textType Require input <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> Collect data from user <input type="checkbox"/> Assign a Variable <div style="border: 1px solid #ccc; padding: 2px; width: 150px; margin-top: 10px;"> <input type="text" value="Search variables..."/> 🔍 </div> 	<p>←</p> <p>Agent Builder Coral Cloud Agent</p> <p>2 VerifiedCustomerId Instructions ⓘ</p> <p>Id of the verified customer</p> <p>✓ Advanced Settings</p> <p>Data Type: lightning__textType</p> <p>Filter from agent action <input type="checkbox"/></p> <p><input type="checkbox"/> Show in conversation</p> <p><input type="checkbox"/> Output Rendering: Text</p> <p>Map to Variable</p> <div style="border: 2px solid orange; padding: 5px; width: fit-content;"> Verified Customer ID ✖ </div> <p>3 contactDetails Instructions ⓘ</p> <p>Record holding customer details such as ID and interests.</p>

And below is a screenshot from Agent Builder showing how to map the conversation variables to the inputs of an action. In this case, we map the Verified Customer ID variable to the inputs of the Create Booking action.

← Agent Builder Coral Cloud Agent

View Action

Inputs Output

1 **contactId** Instructions ⓘ
The Id of the contact that will be used to create the related booking.

Advanced Settings

Data Type lightning__textType
Require input ⓘ
 Collect data from user ⓘ

Assign a Variable
Verified Customer ID

2 **numberOfGuests** Instructions ⓘ
The number of guests that will be included in the booking.

Advanced Settings

Output

1 **createdBooking** Instructions ⓘ
The booking that was created.

Advanced Settings

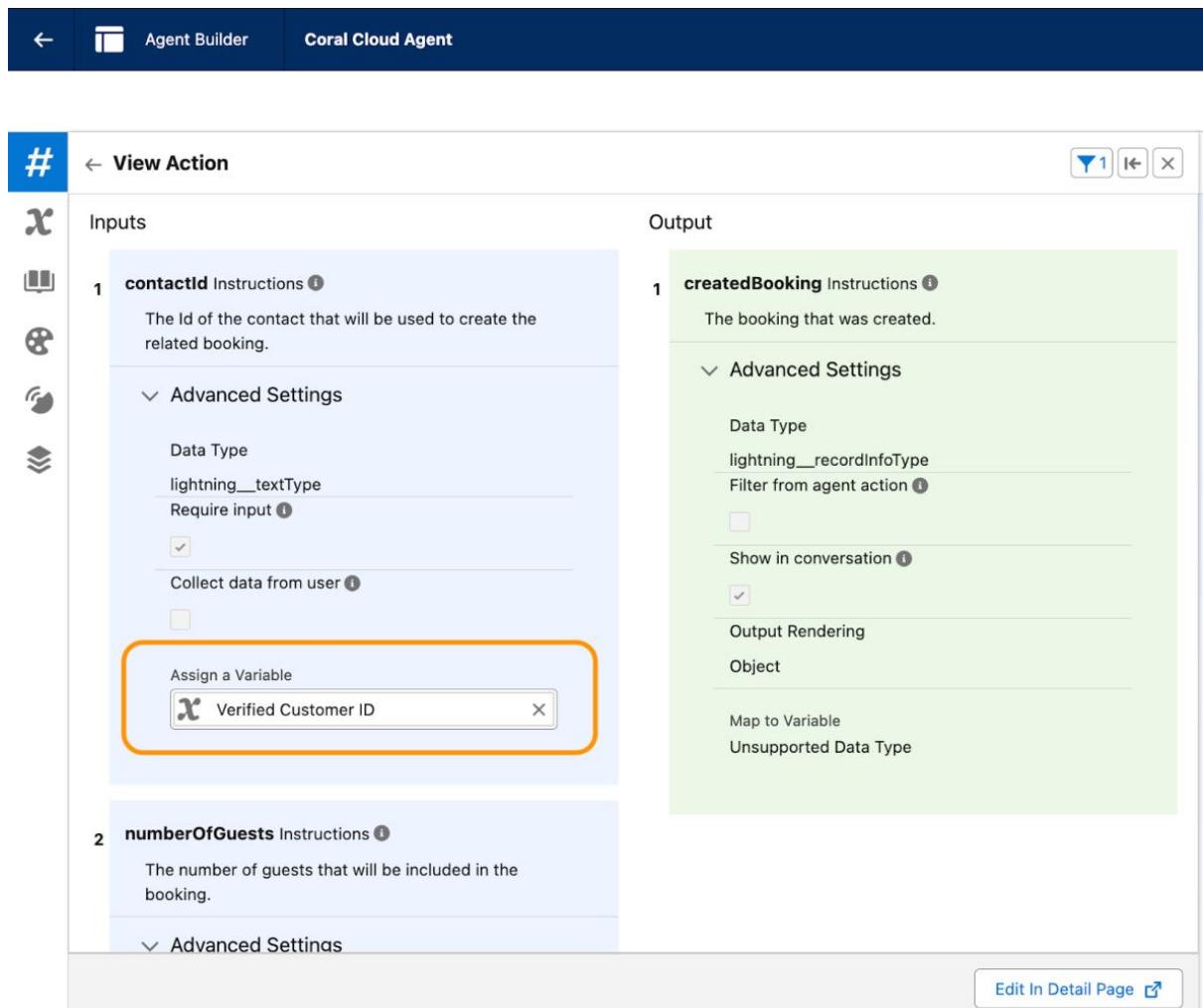
Data Type lightning__recordInfoType
Filter from agent action ⓘ

Show in conversation ⓘ

Output Rendering Object

Map to Variable Unsupported Data Type

Edit In Detail Page ↗



What are filters in Agentforce?

Filters in Agentforce use variables to create conditions that determine if topics or actions execute, enabling granular control over agent behavior. For example, a filter might check whether or not a custom conversation variable meets a certain condition (e.g., a Boolean flag is true) before proceeding with an action.

You can create filters that use variables in Agent Builder by writing simple expressions. An example is shown in the screenshot below. To learn more about creating a filter, check out the [documentation](#).

← Agent Builder Coral Cloud Agent

← Edit Filter

* Name: Is Customer Verified * API Name: Is_Customer_Verified

Filter Conditions

Use conditions to check the value of variables. When the filter conditions are met, your agent can use the topics and actions that have this filter.

All Conditions Are Met (AND)

* Resource: IsCustomerVerified * Operator: Equal * Value: True

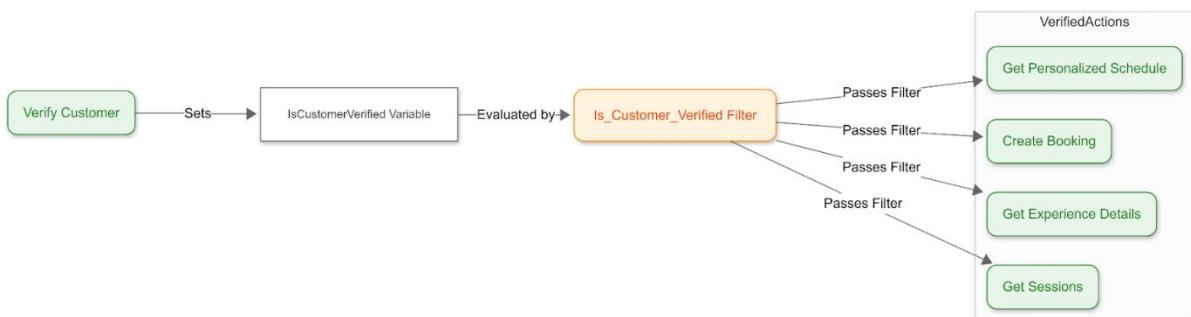
+ Add Condition

Cancel Save

Example use case

In the Coral Cloud app, we only allow actions like Create Booking, Get Experience Details, Get Personalized Schedule, or Get Sessions if the customer is verified. To track whether or not the customer is verified, we create a Boolean variable called IsCustomerVerified. This variable is set by an action called Verify Customer. Next, we make a filter named Is_Customer_Verified and use it for all the actions that require verification.

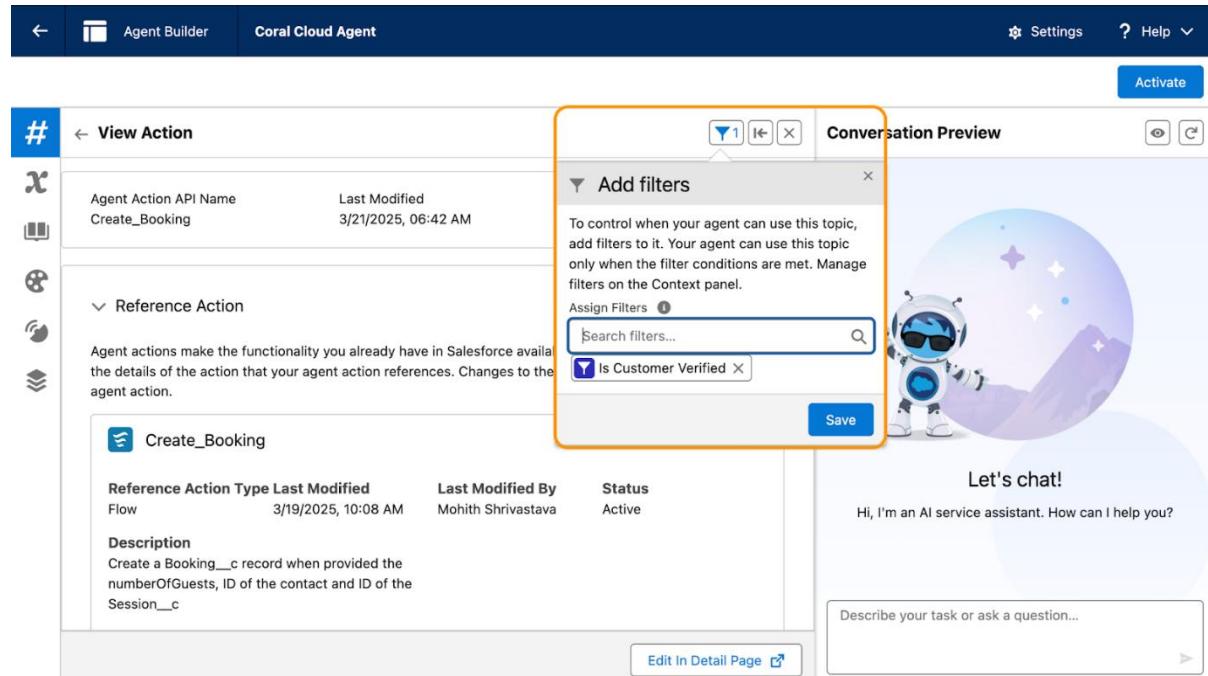
The diagram below visualizes this use case.



We also need a simple topic instruction (as shown below) that uses the variable to define the scope of user verification for Agentforce to reason correctly.

“Always check if the customer is verified before doing anything else. A customer is verified only if {!IsCustomerVerified} is true; if it’s false, the customer is not verified.”

The screenshot below shows how to add this filter to the Create Booking action.



Conclusion

We recently implemented Agent variables and filters for the Coral Cloud Sample app, and we have seen a significant reduction in Agent instructions along with improved security. Check out the [project](#) and [this pull request](#) on GitHub to learn more about variables and filters, including its metadata.

In conclusion, Agentforce offers powerful features for building secure, controlled, and efficient agent systems. By leveraging variables and filters, you can ensure deterministic business logic and control how your agent uses topics and actions — all while streamlining your agent’s decision-making process. This post provides a comprehensive overview of how context and conversation variables work together with filters to safeguard your private data and simplify agent orchestration.

II) Agent template :

Create an Agent from an Agentforce Service Agent Template

Agentforce Service agents intelligently support your customers by connecting to messaging and other channels and escalating to reps when necessary. Use the default Agentforce Service Agent template to create an agent designed to resolve common support cases and requests. Or select from more specialized templates to fit your use case.

Required Editions

Available in: Lightning Experience

Available in: **Enterprise, Performance, Unlimited, and Developer** Editions. [Required add-on licenses vary by agent type.](#)

User Permissions Needed

To build and manage Service Agents:	Manage Agentforce Service Agents AND Manage AI Agents OR Customize Application
-------------------------------------	--

Before you begin, [set up Einstein Generative AI](#) and [enable Agentforce](#).

1. From Setup, in the Quick Find box, enter Agents, and then select **Agentforce Agents**.
2. Click **New Agent**.
3. Select **Create from a Template**. Select the template you want to use to create an agent, and then click **Next**.
4. Review the topics that come with your template. You can customize these topics and actions later, but if any of them don't apply to your use cases, remove them. Then click **Next**.
5. Define your agent's settings, such as [system messages](#) and [language settings](#). These settings determine how agents behave and present themselves in conversations.
6. Under Agent User, select **New Agent User**. Then click **Next**.

To securely access data and perform actions, Service agents operate as an agent user—a Salesforce integration user with all the permissions that the agent needs to do its job. Creating a new agent user in the guided setup creates an agent user record with minimal access so that your agent is secure by default. Grant the agent the additional access that it needs. See [Best Practices for Agent User Permissions](#).

7. Select a data source to ground your agent responses with the Answer Questions with Knowledge action. Then click **Create**.

If you don't want to use any of the available data sources, you can create a library to limit Agentforce Service agents to specific articles or uploaded files. See [Assign a Data Library to Your Agent](#).

8. [Configure your agent with topics, actions, and other agent assets](#).
9. Test your agent in Agentforce Builder, to confirm that your agent performs as expected and [meets your security standards](#).

The service agent operates in the same Agent User context here as it does when deployed in messaging channels, so design-time testing reflects how your service agent behaves when deployed.

10. [Connect your service agent to channels](#) and [configure the escalation topic](#) to transfer agent conversations.
 11. When you're ready, [activate your agent](#).
- **[Best Practices for Agent User Permissions](#)**
- Many AI agents, such as agents that connect to Messaging channels, operate as Salesforce

users in your organization. The permissions that you give to these agent users determine the actions that AI agents can take.

- **Configure Service Agent Managers**

When Service agents are enabled for your Salesforce org, Salesforce admins can create and edit service agents. To define other users as Service agent managers so that they can also create and edit service agents, assign those users the Manage Agentforce Service Agents permission set.

UNIT 2

Study Up on Prompt Engineering

Learning Objectives

After completing this unit, you'll be able to:

- Determine when and how to use Prompt Builder based on business requirements and scenarios.
- Identify key considerations for creating effective prompt templates and selecting suitable grounding techniques.
- Describe the full process of creating, activating, and managing prompt templates within Salesforce.

Key Topics

This unit prepares you for the Prompt Engineering section of the Salesforce Agentforce Specialist exam, which makes up 20% of the overall exam. This section of the exam tests these topics.

- Given business requirements, identify when it's appropriate to use Prompt Builder.
- Identify the right user roles to manage and execute prompt templates.
- Identify the considerations for creating a prompt template using field generation and flex types.
- Given a scenario, identify the appropriate grounding technique.
- Explain the process for creating, activating, and executing prompt templates.
- Explain how to implement best practices for writing effective prompts.

This unit provides a number of interactive, real-world, scenario-based questions that are a lot like the ones you'll encounter as a Salesforce Agentforce specialist. Looking at these scenarios helps prepare you to take the Prompt Engineering section of the Salesforce Agentforce Specialist exam. As you tackle the practice questions, you get immediate feedback on your answers, along with detailed information on why your answers are correct (or incorrect).

The unit also contains interactive flashcards centered around study topics that help you prepare for the Prompt Engineering section of the exam.

Exam Practice Questions

Ready to jump in? The sample tool is not scored—it's just an easy way to quiz yourself. To use it, read the scenario, then click the answer you think is correct. Some questions can have more than one correct answer. Click **Submit** to learn whether the answer you chose is correct or incorrect, and why. When you reach the end, you can review the answers or retake the questions.

An Agentforce Specialist needs a prompt template that generates a personalized summary of only open cases for an account. To ensure reliability, the specialist has decided not to rely on the LLM to filter records. The grounding must return only the open cases directly, not all cases. The solution will be maintained by the company's administrator. Which approach best meets these requirements?

A

Ground with Apex Merge Fields

B

Ground with Flow Merge Fields

C

Ground with Record Merge Fields

Ground with Flow Merge Fields

3) What is a key benefit of grounding prompt templates with CRM data in Prompt Builder?

A

It scores content on toxicity to prevent unintended or harmful outputs by the LLM.

B

It automatically updates Salesforce records based on AI-generated responses.

C

It provides the large language model (LLM) with context to create personalized responses.

Ans:c

A company's marketing team wants to create a Flex prompt template that generates personalized event invitations based on the contact's interests and previous interactions with the company. How should the team ensure that the prompt template generates personalized invitations for each contact?

A

Include instructions in the prompt template to use the contact's name and interests when generating an invitation.

B

Manually input each contact's details into the prompt template before generating an invitation.

C

Integrate the template with dynamic CRM data fields for automatic customization.

Study Materials

Did you choose an incorrect answer? Check out the table for related study materials.

Prompt Template Types

Learn about the prompt template types available in Prompt Builder.

Required Editions

Available in: Lightning Experience

Available in: **Enterprise, Performance, and Unlimited** Editions with the Einstein for Platform, or Einstein or Agentforce for Sales or Service add-on, or Agentforce Foundations

Prompt Template Type	What it Creates
Campaign Brief	Content for a campaign brief including name, key message, audience description, and detailed campaign goals. See Agent Action: Draft a Campaign Brief
Case Summary	Summary of a Case object including a Summary, Issue, and Resolution. See Customize the Work Summaries for Case Prompt Template .
Contextual Service Replies	Customize your context based Service Replies prompt templates for Live Chat and Messaging Sessions. See Customize the Context Based Service Replies Prompt Templates .
Contract Analysis	Retrieves key information from contract documents to answer user questions or generate summaries of important clauses and sections. See Customize Prompt Templates for Contract Search .
Common Services AI	Content for any business purposes that requires context of current user object and its related fields. Used for enabling Einstein Summary component on the home page. For example, in Salesforce, users can create a prompt that summarises top leads and execute it through Einstein Summary directly at the homepage. This prompt template requires the EinsteinForSvcInovtAddOn add-on. See Add Einstein Summary to a page .
Extract Product Mentions	Identifies and retrieves product-related details from unstructured conversations such as emails, slack messages, or call transcripts. This prompt template requires Revenue Cloud and Einstein or Agentforce for Sales add-on or the Einstein 1 Sales add-on. See Configure Extract Product Mentions Template .

Prompt Template Type	What it Creates
Field Generation	<p>Content for record fields in Lightning Experience. In Salesforce, users click a button to run this prompt and populate the field with output.</p> <p>See Create a Field Generation Prompt Template and Field Generation Prompt Templates in Action.</p>
Flex	<p>Content for any business purposes that other templates don't cover. Flex prompt templates let you define your own resources.</p> <p>See Create a Flex Prompt Template and Flex Prompt Templates in Action.</p>
Grounded Service Replies	<p>Customize your grounded Service Replies prompt templates for Live Chat and Messaging Sessions.</p> <p>See Customize the Grounded Service Replies Prompt Templates.</p>
Generate case description	<p>Content for the case description, including key details discussed during the interaction to help support teams understand and resolve the issue.</p> <p>See Agent Action: Create Case with Enhanced Data.</p>
Generate case subject	Content for the case subject line that summarizes the reported issue.
Intent Retrieval	Content including the user's relevant conversation history and available filter options, to help the agent understand the user's intent.
Journey Decisioning Content	Content for the journey messages that are stored in a data extension for use in Journey Builder in Marketing Cloud Engagement.
Journey Decisioning Selection	Content is the subscribers that are sorted into their optimal journeys stored in a data extension for use in Journey Builder in Marketing Cloud Engagement.
Knowledge Answers	<p>Customize how Agentforce agents answer questions.</p> <p>See Create a Knowledge Answers Prompt Template and Agentforce Platform Answer Questions with Knowledge.</p>
Sales Emails	<p>Personalized customer email based on record data.</p> <p>See Create a Sales Email Prompt Template and Draft a Sales Email with Einstein Generative AI.</p>
Sales Pitch Coaching	Feedback for sales reps based on their transcript from a sales pitch or role play session.
Search Learning Courses	A list of recommendations based on record data in response to the user's query.
Security Risk Analysis	Next steps to remediate risks for instances where risks or threats are detected with Salesforce security posture data.
	See Agent Action: Classify Security Risk .

Prompt Template Type	What it Creates
Record Prioritization	<p>Prioritized records based on user input or available data. Using agents, the record prioritization prompt templates are used by the Prioritize Opportunities standard agent action.</p> <p>See Sales Prioritize Opportunities</p>
Record Research	<p>Summarized research results based on delivered prompt templates or user input. In Salesforce, users click a button on the Account Research component to run this prompt and generate the output. Record research prompt templates use the Einstein Search Web Retriever to perform research.</p>
Record Summary	<p>Summarized record data for a comprehensive view of a record. Record summary prompt templates are used by the Summarize Record standard invocable action. Agents use the Summarize Record standard agent action.</p> <p>See Agentforce Platform Summarize Record</p>
Work Summary	<p>Drafts a Summary, Issue, and Resolution in the Wrap Up component at the end of a Voice Call or Messaging Session.</p> <p>See Customize the Summarize Messaging Session Prompt Template and Customize the Summarize Voice Call Prompt Template.</p>

Prompt Builder Limits

Learn the numerical limits of prompt templates.

Required Editions

Available in: Lightning Experience

Available in: **Enterprise, Performance, and Unlimited** Editions with the Einstein for Platform, or Einstein or Agentforce for Sales or Service add-on, or Agentforce Foundations

Numerical Limits

Prompt templates have these numerical limits.

Numerical Limits

Limit Description	Limit
Maximum template size	128,000 characters
Maximum number of template versions	50
Maximum number of merge fields	50

Numerical Limits

Limit Description	Limit
Maximum number of flow merge fields	5
Maximum number of Apex merge fields	5
Maximum number of related list merge fields	5
Maximum number of inputs in a Flex template	5

File Upload Limits

Most models support at least one file type that can be used with prompt templates.

These file limits apply across all models:

- Maximum quantity: 10 images or 100 PDF pages per request
- Total file size: 15MB per request



Important Some models may have smaller limits than the ones listed here. Check with your model provider for exact details.

Unsupported files are excluded from the request. Due to post-processing, the size of a file may exceed the listed limits. A list of excluded files is displayed in the resolution panel after processing.

III) Review Data Cloud for Agentforce

Learning Objectives

After completing this unit, you'll be able to:

- Explain how to use the Agentforce Data Library effectively, including its types and applications.
- Enhance agent responses with unstructured data using techniques like chunking and indexing.
- Identify considerations for configuring retrievers and search types in Data Cloud.

Key Topics

This unit prepares you for the Data Cloud for Agentforce section of the Salesforce Agentforce Specialist exam, which makes up 20% of the overall exam. This section of the exam tests these topics.

- Explain the considerations of Agentforce Data Library and its types.
- Given a scenario, improve an agent's response with unstructured data using chunking and indexing.
- Identify the considerations for retrievers in Data Cloud such as individual and ensemble.
- Given a scenario, identify the considerations for search type such as keyword, semantic, and hybrid.

Like the previous units, this unit contains practice scenario-based questions and flashcards.

Exam Practice Questions

Ready to jump in? The sample tool is not scored—it's just an easy way to quiz yourself. To use it, read the scenario, then click the answer you think is correct. Some questions can have more than one correct answer. Click **Submit** to learn whether the answer you chose is correct or incorrect, and why. When you reach the end, you can review the answers or retake the questions.

What is the primary purpose of using retrievers in Data 360?

- A To store unstructured data such as documents and conversation histories
- B To create and manage search indexes in Data 360
- C To return relevant data from the vector database to augment a prompt

C

2) A company uses Data 360 to manage a large volume of customer interactions. The company needs to enhance the accuracy of its LLM-generated responses by incorporating relevant knowledge from various sources. Which action should the company take to achieve this using retrievers in Data 360?

A

Add active retrievers to prompt templates to retrieve knowledge from articles, email, and chat transcripts.

B

Use related lists and Apex to dynamically generate search text for the retrievers.

C

Deactivate all default retrievers and rely solely on custom retrievers created in Einstein Studio.

A)

Study Materials

Did you choose an incorrect answer? Check out the table for related study materials.

1. [Salesforce Help](#)
2. [Docs](#)
3. [Data 360](#)

Retrieve Data

Use a retriever to search and return relevant data from a search Index. Create and customize retrievers in Einstein Studio for Retrieval Augmented Generation (RAG) in Data 360. Retriever augment prompt templates by providing relevant, specialized grounding information for prompts.

Required Editions

Available in: **All Editions** supported by Data 360. See [Data 360 edition availability](#).

Data preparation for retrieval from a search index involves loading, chunking, vectorizing, and storing content in a search-optimized way. Data 360 uses a vector data store for unstructured data, such as documents and conversation histories. A search index stores chunked and vectorized data that can be searched and retrieved from other applications. You can create and manage search indexes in Data 360. They're defined in a data space and associated with a Data Model Object (DMO).

With advanced document processing and indexing capabilities in Data 360, retrievers can retrieve and ground agent responses by processing both text and images. Enable image processing for the unstructured data model object search indexes to process documents with images and other visuals such as tables or flow charts. For more information on advanced set up for search indexes, see [Use Search for AI, Automation, and Analytics](#).

Search indexes are often designed for general usage, such as indexing an entire knowledge base. You use retrievers to conduct specialized searches on search indexes and provide relevant results to agents, prompt templates, flows, and other features. Individual retrievers for search indexes apply the multi-purpose search index to a particular use case. For example, retrievers can return content that's filtered based on a category of articles or the most recent information (such as the last 90 days), a geographical region.

You build retrievers in Einstein Studio and then activate it to make it available to Prompt Builder users. In Prompt Builder, you ground a prompt template with knowledge by inserting and configuring a retriever. At run time, the retriever provides the LLM with accurate, current, and pertinent information to improve the relevance, accuracy, and value of LLM responses.

Retrievers adhere to the data governance policies set up for your data. Row-level access checks make sure that users have access to the data and knowledge returned by the retriever.

When you create a retriever in a Data 360 home org, you can use it in the companion org within Prompt Builder and Flow. For more information see, [Data Cloud One Companion Connections](#).

Individual Retriever

Use individual retrievers to retrieve data from a search index. To create an individual retriever in Einstein Studio, you select its search index, define filters, and specify what information it returns. Filters narrow the search focus to more relevant data. The search index defines the fields you can use for filtering. You can also configure the data returned to the prompt, including the fields of data to return and the number of results. Each time you edit and save an individual retriever, Einstein Studio creates another version. Only one version of a retriever can be active.



Note Data 360 no longer creates a default Retrievers automatically when you create a search index. Previously, when you created a search index in Data 360, a default retriever was created automatically. You can use existing default retrievers in applications, such as prompt builder or flow.

Ensemble Retrievers

An ensemble retriever is a collection of individual retrievers. When you run an ensemble retriever, it executes the individual retrievers, combines their results into a single list, reranks the list according to relevance to the search request, and returns just the most relevant information to applications such as prompt builder or flow.

Dynamic Retrievers

Dynamic retrievers use placeholders that accept run-time values from prompt templates. A dynamic retriever has a placeholder for a value specified at run time based on the needs of the prompt template.

- **Get Trusted AI Responses with Retriever Citations**

Citations link AI-generated responses to the source content relevant to each response. Citations allow users to compare the LLM response with the source data to verify the validity of the response and identify any potential inaccuracies or hallucinations. Enable citations in Einstein Studio at the individual retriever level to give access to citations to solution components that call the retriever, such as a prompt template.

- **Manage Retrievers**

Create and customize retrievers for Retrieval Augmented Generation (RAG) in Data 360. To see the list of retrievers, navigate to the Retrievers tab in Einstein Studio. To learn about a retriever, select View Details from the dropdown menu. Each time you edit a custom retriever and save the changes, a new version is created. You can create multiple versions, but you can have only one version active at a time.

Agentforce Data Library

Improve accuracy, add personalization, and build trust in gen AI responses when you assign data libraries to your Agentforce features. Agentforce Data Library uses grounding to index your knowledge articles and fields, your file uploads, or web sources, so that AI agents know which information to base responses on. With this index, AI agents can ensure the accuracy of LLM responses against your organization's information so that you get the best results.

Required Editions

Available in: Lightning Experience

Available in: **Enterprise, Performance, and Unlimited** Editions with the Einstein for Platform or Einstein or Agentforce for Sales or Service add-on, or Agentforce Foundations

To use Agentforce Data Libraries, you must have [Data 360 set up](#). Data libraries consume Data 360 credits.

Agentforce Data Library doesn't support companion orgs through Data Cloud One.

Dive deeper into Salesforce Help.



- [What Are Data Libraries?](#)
- [Using Retrieval Augmented Generation](#)

Use Trailhead to build and test your skills.



- [Agentforce Data Library Basics](#)
- [Retrieval Augmented Generation: Quick Look](#)

Get started with data library setup.



- [Setting Up Data Libraries](#)

Integrate data libraries with AI agents.



- [Assign a Data Library to Your Agent](#)
- [Answer Questions with Knowledge](#)
- [Customize the Knowledge Action prompt template in Prompt Builder](#)

Explore all data library enabled features.



- [Agentforce Agents](#)
- [Einstein Service Replies for Chat](#)

AGENT FORCE LIBRARY BASICS:

Upgrade AI with Real-World Data

Learning Objectives

After completing this unit, you'll be able to:

- Describe the benefits of using Agentforce Data Library.
- Define four key concepts involved in AI data transformation and organization.
- Explain how the Agentforce Data Library setup and runtime processes work.



New Agent Building Experience Coming Soon!

Agentforce is getting an update! At Dreamforce 2025, we announced the new agent building experience which may differ from the process and features you learn about in this badge. Expect the new experience to become available in open beta in the weeks following Dreamforce. General availability comes soon after. The current builder experience remains available to support previously built agents. Stay tuned for more information.

Before You Start

Before you start this module, consider completing this recommended content.

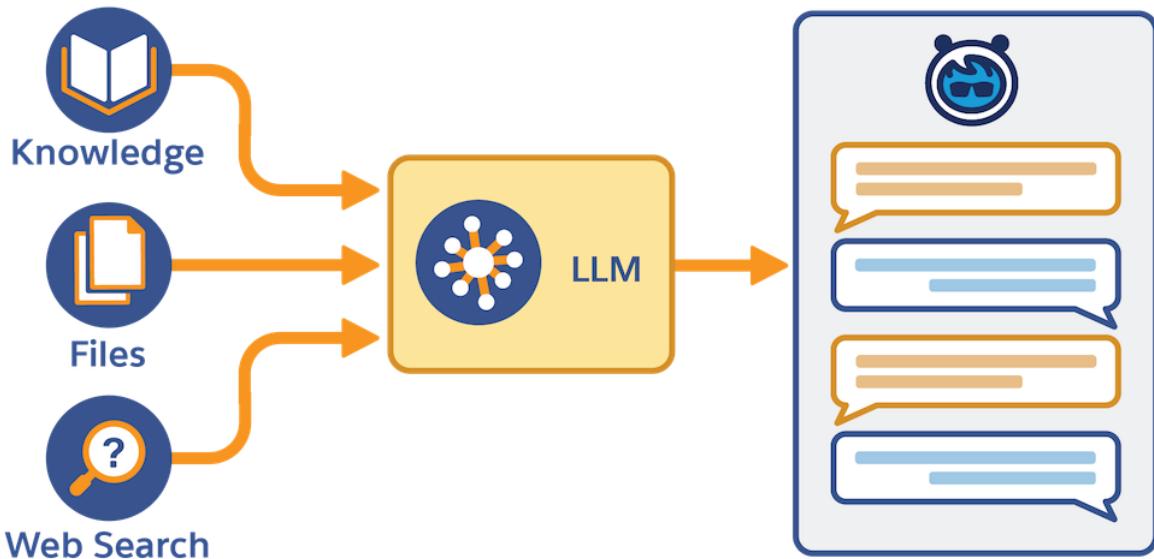
- [Knowledge Grounding for AI: Quick Look](#)

Why Ground AI with Data?

Your data plays a crucial role in ensuring that AI systems operate accurately and effectively. Give a customer the wrong answer, and it could discourage them from future purchases. Provide service reps with incorrect information, and they might frustrate customers rather than support them. Deliver outdated recommendations to your sales reps, and they could miss their earnings targets and lose valuable business opportunities.

While data is the backbone of any successful AI system, AI models are born generalists: They train on massive datasets that provide them with a broad base of knowledge. This broad knowledge base means they don't have the specialized information needed to perform specific tasks or answer technical questions for your unique use cases.

Real-world data grounding takes AI models beyond their static training sets. When you ground your AI model in verified sources of information like your Salesforce knowledge base, your uploaded files, or websites, the LLM can more accurately return responses to customer inquiries, suggest better replies to agents, provide sophisticated search summaries, and more.



The Challenge of Enterprise Data

Most companies store their knowledge bases in unstructured formats such as collections of videos, images, documents, emails, sensor data, social posts, and audio files, and more—formats that don’t fit neatly into spreadsheets or databases. Accounting for nearly 90% of enterprise data, this data is harder to search, but it’s packed with valuable insights such as customer feedback, perceptions, opinions, tone, and sentiment. So how can you unlock this data’s potential?

Enter Agentforce Data Library, a powerful tool that can help you ground AI in your real-world data. With the Agentforce Data Library, you can easily connect your knowledge base to Salesforce AI features, ensuring you get up-to-date, AI-generated content that’s tailored to your organization and use cases. When you set up an Agentforce Data Library, you get the tools you need to transform large sets of unstructured or semi-structured data into more useful, searchable content. Let’s see how.

Transform Data for Efficient Use with Large Language Models

Agentforce Data Libraries make it easy to link agents and large language models (LLMs) to your unstructured data by automating several configuration steps across Data 360 and Prompt Builder. This includes pushing data streams to Data 360, mapping data objects, and creating a search index and retriever. The end result is that your AI tools are always working with the most up-to-date and relevant information.

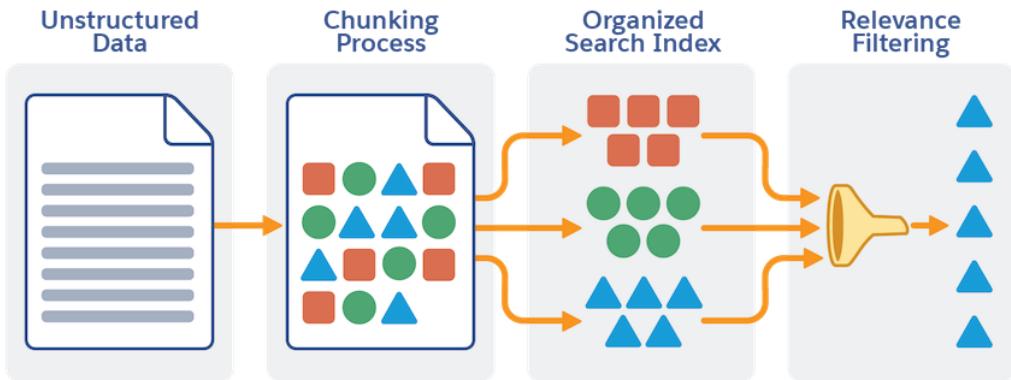
Before you learn the simple steps to set up a data library, let’s review a few key concepts: grounding, chunking, indexing, and retrievers.

Grounding

Grounding is when you add domain-specific knowledge or customer information to a prompt, giving the LLM the context it needs to respond more accurately to a question or task. As we’ve mentioned, your grounding sources can include knowledge articles, uploaded files, websites, conversation transcripts, and more. However, lengthy and complex documents can be time-consuming and resource-intensive to search through, and LLMs have a maximum token or word limit for the amount of text they can process at one time.

Chunking and Indexing

To address this, data sources are broken down into smaller parts, called chunks. We then search through the chunks and only return the most relevant pieces of information for the LLM to consider.



Once the data is chunked, it's organized and categorized into a search index. Storing information in an organized search index makes it easier and faster to retrieve specific data when needed. When data is chunked and organized like this, it makes searches more efficient, improves the relevance of results, and enables the handling of very large datasets.

Think of a large online store with millions of products. A well-organized store catalog or website taxonomy enables customers to quickly find the products they're looking for across categories like name, type, brand, or even specific features. Breaking up data into smaller pieces and organizing them in a search index is like creating a catalog for your content. LLMs can then use this catalog or index to find the right information to answer users' queries.

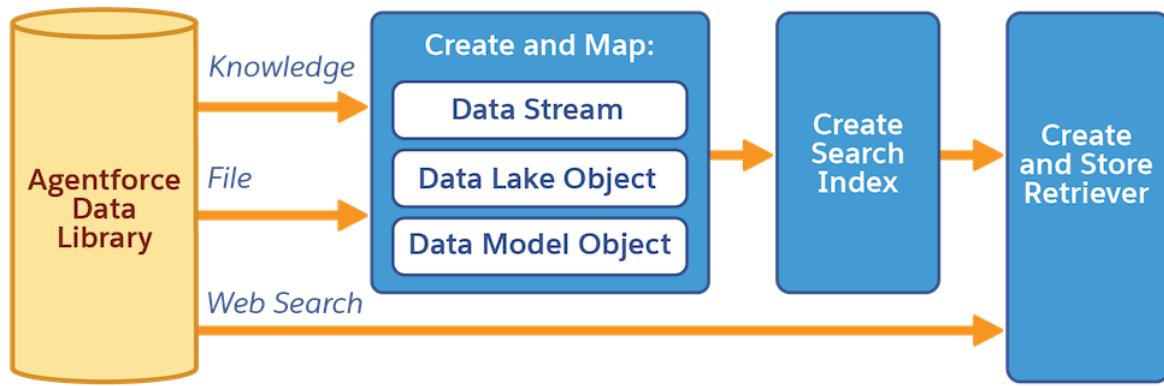
Retrievers

Retrievers act as pointers between data and features. They are designed to automatically extract and provide relevant data from different databases, systems, or platforms. When a user asks a question, the retriever assigned to each data library determines which datasets in Data 360 that Salesforce AI tools can access. This makes retrievers particularly important in applications like search engines, question-answering systems, and recommendation systems.

You just learned some basics about data organization in AI. Next, let's see how these processes play out during data library setup and runtime.

What Happens at Setup?

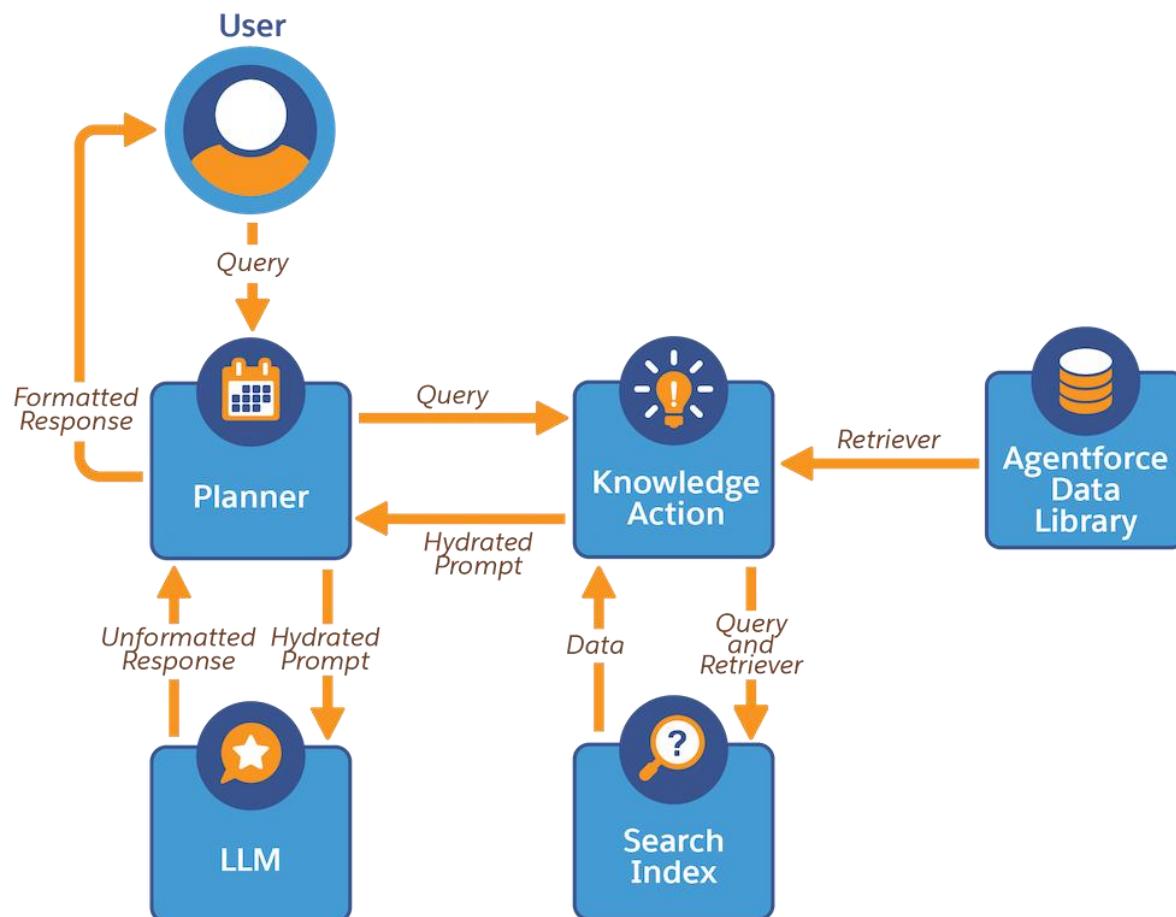
When you create a data library, the processes that connect your data with your AI agents and features begin immediately. First, a data stream is created, followed by the data lake and data model objects. These objects are then mapped together, and data chunking begins. The time required for chunking varies based on factors such as the number, size, and complexity of knowledge articles or uploaded files, and the number of knowledge fields selected for chunking. After chunking is completed and the search index is ready, a retriever is created. Each Agentforce Data Library has its own unique retriever, which can point to the same search index but operates independently.



What Happens at Runtime?

Once the retriever is set up and the search index is fully prepared, the system is ready to handle user queries at runtime.

At runtime, the user's query is added to the prompt template, which references the retriever connecting to relevant data. The system then searches through the search index to find the most pertinent information and incorporates it back into the prompt. The LLM receives this enriched prompt, which includes the user's query, the added information, and the prompt instructions, and then generates a response. The Service Planner reviews this response to ensure it aligns with the prompt instructions. Finally, the end user receives a response that accurately answers the query and is contextualized with relevant, domain-specific information tailored to the specific task.



Let's Recap

Great job! In this unit, you learned why it's important to ground AI with your data, and you explored some specialized terminology and technical processes. Now it's time to get to the setup, where you can see just how simple it can be!

Resources

- [Salesforce Blog: What Is Retrieval Augmented Generation \(RAG\)](#)
- [Salesforce Blog: CIOs Reveal Top 3 Strategies for Unlocking AI's Potential with Unstructured Data](#)
- [Salesforce Help: Learn About Data Libraries](#)

Quiz

To complete this unit, you need to answer all the quiz questions correctly.

+100 Points

1

What is the main challenge in integrating unstructured data into AI features?

A

Unstructured data is buried in spreadsheets and databases.

B

Unstructured data is harder to search but contains valuable insights.

C

Unstructured data is less valuable than structured data.

D

Unstructured data is not compatible with AI systems.

2

What occurs at runtime when a user asks a question in an Agentforce Data Library?

A

The data is rechunked and reindexed.

B

The user's query is added to the prompt template, and the retriever fetches the most relevant data.

C

The data stream is created.

D

The question is sent directly to the LLM.

Second attempt earns 50 points. Three or more earns 25 points.

Build a File-Based Data Library for an Agent

Learning Objectives

After completing this unit, you'll be able to:

- Create and configure a data library from Setup.
- Create or add a data library from Agentforce Builder.

Whether you're new to Agentforce or a seasoned user, it's easy to set up an Agentforce Data Library. All you need is Salesforce admin privileges and sufficient permissions to enable Agentforce Data Library. If you're not a Salesforce admin, that's OK. Read along to learn how your admin would take the steps in a production org or sandbox. A sandbox is a safe space to test out agents with data libraries. To try it out, see [Test Data Libraries in a Sandbox](#).

Meet Coral Cloud Resorts

Coral Cloud Resorts is a luxury hospitality company with hotels operating in some of the world's most glamorous destinations. The company has been experimenting with AI agents, and so far so good. But Coral Cloud Resorts admin Becca wants her agents to answer more specific questions and complete complex tasks based on the company's unique policies. The resort's current data? A massive collection of unstructured content—emails, PDFs, videos, and internal FAQs.

That's where Agentforce Data Libraries come in. After researching how to add unstructured data to her agents, Becca decides to set up an Agentforce Data Library to ground Coral Cloud's AI chatbots.

Let's follow along as she goes through the setup steps.

Create a Data Library

Becca is ready to create a data library. Here's what she does.

1. From Setup, search for and select **Agentforce Data Library**.
2. From the Agentforce Data Library setup page, click **New Library**.
3. Enter a unique library name and an optional description. This should reflect its purpose or content.

Add a Data Library

* Select a Data Space

default

* Name

Coral Cloud Spa Services

* API Name

Coral_Cloud_Spa_Services

Description

Recommend services based on the Coral Cloud spa menu and seasonal offerings.

[Cancel](#)

[Save](#)

4. Click Save.

Choose a Data Source

Next, Becca chooses the type of data source she wants to use. Agentforce offers two main options: Knowledge articles and file uploads. Once you choose a data source, you won't be able to change it later, so make sure to select the one that best fits your needs.

Becca wants this agent to recommend spa services to guests based on their needs and Coral Cloud's offerings. The spa manager writes up and circulates information about spa services and seasonal specials via PDF files. So, Becca decides to create a file-based data library. Here's what she does.

1. Click **Upload Files** and select your files. Ensure the files are within the size limits (4 MB for text/HTML, 100 MB for PDFs).

 **SETUP**
Agentforce Data Library

Library Setup	Library Name Coral Cloud Spa Services	API Name Coral_Cloud_Spa_Services	Data Space default	Description Recommend services based on the Coral Cloud spa menu and seasonal offerings.
Feature Assignments (0) Unassigned				
Edit				

Add Data Sources

Your library can have only one data type: Knowledge, files, or websites. After you create a data library, the data type can't be changed.

 [Learn More in Help](#)

* **Data Type** 

Add Files Data

Improve accuracy of AI responses using files such as PDF or HTML, up to 400 MB.

Add Files 

 [Upload Files](#)

Or drop files

File Name	Size	Uploaded By	Uploaded On
Coral Cloud Resort Spa Services.pdf	98.21 kB	Admin User	Apr 17, 2025
Summer and Holiday Seasonal Offerings ...	57.68 kB	Admin User	Apr 17, 2025

2. Click Save.

As soon as she clicks save, several configuration steps across Data 360 and Prompt Builder begin. Data streams are pushed to Data 360, data objects are created and mapped, and a search index and retriever are created. With these steps completed automatically, it's easy for Becca and Coral Cloud Resorts to link agents to their data. No heavy lifting. Just a clean, simple way to make agents smarter.

Assign Data Libraries to Features

The library is ready to use, and Becca wants to assign it to an agent for Coral Cloud's spa services web page. Here's how she assigns her new data library.

1. Click the name of your agent, and then click **Open in Builder**.
2. Click the **Knowledge** tab. Select a library for your agent (or, to create a library, click **New Library**).
3. Save your changes.
4. Click **Activate**.

The screenshot shows the Knowledge Builder interface. On the left, there's a sidebar with icons for Home, Data Library, Add Data Sources, and a search bar. The main area has tabs for Knowledge, Files, and Websites. The Knowledge tab is selected, showing a library named "Coral Cloud Spa Services". A message says "Manage the data your agent uses to complete tasks via Agentforce Data Library. To manage your libraries, go to Agentforce Data Library Setup." Below this, there's a section for "Add Data Sources" with a note about data type (Knowledge, files, or websites) and a "Data Type" dropdown set to "Files". There's also a "Add Files Data" section with a note about improving AI responses using PDF or HTML files up to 400 MB, and a "Upload Files" button. A table lists uploaded files: "Coral Cloud Resort Spa Se..." (98.21 kB, Admin User, Apr 17, 2025) and "Summer and Holiday Seas..." (57.68 kB, Admin User, Apr 17, 2025). At the bottom, there's a "Show sources" checkbox, "Cancel" and "Save" buttons, and a "Conversation Preview" window on the right featuring a cartoon character and the text "Let's chat!".

To see which features support data libraries, [go to Salesforce Help](#).

Try It Out

Now that she's added the data library to her agent, Becca is ready to see it in action. To test out her changes, she first checks that the search index and data library are ready, then restarts the preview conversation.

Becca asks the agent about available spa services for sensitive skin. After thinking for a moment, the agent recommends the Tropical Revitalizing facial and the Aloha Aromatherapy facial.

The response is quick and seamless; it works!

The screenshot shows a conversational AI interface with the following sections:

- Actions**: 1
- Select Action**: 2.53 sec
- Answer Questions with Knowledge (AnswerQuestion...)**: Answers questions about company policies and procedures, troubleshooting steps, or product information. For example: "What is your return policy?" "How do I fix an issue?" or "What features does a product have?"
- Input** (JSON):

```
{
  "citationsEnabled": "false",
  "ragFeatureConfigId": "AiRagFeaturePromptContent_d177bbca_5c5c_4399_ace8_f61905ad2a1"
}
```
- Output** (JSON):

```
{
  "knowledgeSummary": "The best facials for sensitive skin at Coral Cloud Resort include the Tropical Revitalizing Facial"
}
```
- Reasoning**: GROUNDED: The response accurately summarizes the information retrieved from the function call about the best facials for sensitive skin at Coral Cloud Resort.
- Agent Response**:
A facial uses natural tropical ingredients and a hydrating mask to gently exfoliate and rejuvenate the skin.\n2. **Aloha Aromatherapy Facial**: This 75-minute facial incorporates tropical fruits and essential oils, providing a gentle and soothing treatment for sensitive skin.\n\nBoth treatments are designed to be gentle and hydrating, making them ideal for sensitive skin types.
- Conversation Preview** (List of services):
 9. **Pampering Pedicure**: A 60-minute pedicure with a foot soak, exfoliation, and massage.
 10. **Heavenly Manicure**: A 45-minute manicure with a hand soak, exfoliation, and massage.
 11. **Aloha Aromatherapy Facial**: A 75-minute facial with tropical fruits and essential oils.
 12. **Sunrise Yoga and Meditation**: A 60-minute session combining yoga poses and guided meditation.
 13. **Coral Cloud Signature Treatment**: A 120-minute relaxation experience with a full-body massage, facial, and foot ritual.
 14. **Seaside Hot Stone Massage**: A 75-minute massage with heated basalt stones.
 15. **Tropical Fruit Scrub and Mask**: A 60-minute treatment with a fruit scrub and hydrating mask.

Feel free to ask if you need more details about any specific service!

Next, Becca wants to see if the agent can make a recommendation from the resort's specials menu. She asks about seasonal specials for sensitive skin, and the agent recommends the Holiday Bliss Package, even highlighting the complimentary cookie and hot chocolate that comes with the package. Becca looks over the agent's reasoning, which cites the files she uploaded to her data library. Finally, Becca asks the agent for the Holiday Bliss Package price to verify that it matches the menu. The agent swiftly responds with the correct price.

The screenshot shows the Agentforce Builder interface. On the left, a workflow step titled "Select Action" is displayed, with an input JSON object and an output JSON object. The output object includes a "knowledgeSummary" field. Below this is a "Reasoning" section with a message about the response being grounded. On the right, a "Conversation Preview" window shows a customer asking about seasonal spa specials for sensitive skin. The agent responds by mentioning the "Holiday Bliss Package" and its details. Another message asks about the price of the package, and the agent replies that it is \$250. At the bottom of the conversation preview, there is a text input field for describing a task or asking a question.

Satisfied with the agent's responses to her test questions, Becca clicks **Activate** one last time. The agent, grounded in the resort's data, is live and ready to help guests relax and unwind at Coral Cloud's premiere spa.

Wrap It Up

You've just seen how fast and easy it is to go from raw unstructured data to intelligent, grounded responses—all with Agentforce Data Libraries. Whether you're an experienced Salesforce admin or just starting out, you now have the tools to create, configure, and test data libraries that will make your AI agents smarter, more accurate, and ready to wow your customers. Ready to put your new skills to the test? Dive in to a sandbox and see the magic happen.

Resources

- [Salesforce Help: Setting Up Data Libraries](#)
- [Salesforce Help: Test Data Libraries in a Sandbox](#)
- [Salesforce Blog: 6 Ways Sandboxes Prepare Your Agents for the Real World](#)

Quiz

To complete this unit, you need to answer all the quiz questions correctly.

+100 Points

1

What should you do to test out changes made to a data library in the Agentforce Builder workflow?

A

Save your configuration.

B

Restart the preview conversation and chat with your agent.

C

Upload new files.

D

Log a case on your own website.

2

You're testing and want to see which sources of information your agent uses for its responses. Where can you find this?

A

In the response itself.

B

In the agent reasoning window.

C

From the data library.

D

You can't access the information.

Second attempt earns 50 points. Three or more earns 25 points.

1. IV [Salesforce Help](#)
2. [Docs](#)
3. [Data 360](#)

Retrieve Data

Use a retriever to search and return relevant data from a search Index. Create and customize retrievers in Einstein Studio for Retrieval Augmented Generation (RAG) in Data 360. Retriever augment prompt templates by providing relevant, specialized grounding information for prompts.

Required Editions

Available in: **All Editions** supported by Data 360. See [Data 360 edition availability](#).

Data preparation for retrieval from a search index involves loading, chunking, vectorizing, and storing content in a search-optimized way. Data 360 uses a vector data store for unstructured data, such as documents and conversation histories. A search index stores chunked and vectorized data that can be searched and retrieved from other applications. You can create and manage search indexes in Data 360. They're defined in a data space and associated with a Data Model Object (DMO). .

With advanced document processing and indexing capabilities in Data 360, retrievers can retrieve and ground agent responses by processing both text and images. Enable image processing for the unstructured data model object search indexes to process documents with images and other visuals such as tables or flow charts. For more information on advanced set up for search indexes, see [Use Search for AI, Automation, and Analytics](#).

Search indexes are often designed for general usage, such as indexing an entire knowledge base. You use retrievers to conduct specialized searches on search indexes and provide relevant results to agents, prompt templates, flows, and other features. Individual retrievers for search indexes apply the multi-purpose search index to a particular use case. For example, retrievers can return content that's filtered based on a category of articles or the most recent information (such as the last 90 days), a geographical region.

You build retrievers in Einstein Studio and then activate it to make it available to Prompt Builder users. In Prompt Builder, you ground a prompt template with knowledge by inserting and configuring a retriever. At run time, the retriever provides the LLM with accurate, current, and pertinent information to improve the relevance, accuracy, and value of LLM responses.

Retrievers adhere to the data governance policies set up for your data. Row-level access checks make sure that users have access to the data and knowledge returned by the retriever.

When you create a retriever in a Data 360 home org, you can use it in the companion org within Prompt Builder and Flow. For more information see, [Data Cloud One Companion Connections](#).

Individual Retrievers

Use individual retrievers to retrieve data from from a search index. To create an individual retriever in Einstein Studio, you select its search index, define filters, and specify what information it returns. Filters narrow the search focus to more relevant data. The search index defines the fields you can use for filtering. You can also configure the data returned to the prompt, including the fields of data to return and the number of results. Each time you edit and save an individual retriever, Einstein Studio creates another version. Only one version of a retriever can be active.



Note Data 360 no longer creates a default Retriever automatically when you create a search index. Previously, when you created a search index in Data 360, a default retriever was created automatically. You can use existing default retrievers in applications, such as prompt builder or flow.

Ensemble Retrievers

An ensemble retriever is a collection of individual retrievers. When you run an ensemble retriever, it executes the individual retrievers, combines their results into a single list, reranks the list according to relevance to the search request, and returns just the most relevant information to applications such as prompt builder or flow.

Dynamic Retrievers

Dynamic retrievers use placeholders that accept run-time values from prompt templates. A dynamic retriever has a placeholder for a value specified at run time based on the needs of the prompt template.

- **Get Trusted AI Responses with Retriever Citations**

Citations link AI-generated responses to the source content relevant to each response.

Citations allow users to compare the LLM response with the source data to verify the validity of the response and identify any potential inaccuracies or hallucinations. Enable citations in Einstein Studio at the individual retriever level to give access to citations to solution components that call the retriever, such as a prompt template.

- **Manage Retrievers**

Create and customize retrievers for Retrieval Augmented Generation (RAG) in Data 360. To see the list of retrievers, navigate to the Retrievers tab in Einstein Studio. To learn about a retriever, select View Details from the dropdown menu. Each time you edit a custom retriever and save the changes, a new version is created. You can create multiple versions, but you can have only one version active at a time.

You've studied up on Data Cloud for Agentforce. Next, let's take a look at the Deployment Lifecycle.

Quiz

To complete this unit, you need to answer all the quiz questions correctly.

+100 Points

1

The Data Cloud for Agentforce section makes up what percentage of the Salesforce Agentforce Specialist certification exam?

A

10%

B

15%

C

20%

D

30%

2

Which key topic does the Data Cloud for Agentforce section of the exam cover?

A

Explain the process for connecting agents to various channels such as digital experience, email, and Slack.

B

Given a scenario, improve an agent's response with unstructured data using chunking and indexing.

C

Identify the considerations for creating a prompt template.

D

Explain how an agent works and how the reasoning engine powers Agentforce.

Second attempt earns 50 points. Three or more earns 25 points.

Examine the Deployment Lifecycle

Learning Objectives

After completing this unit, you'll be able to:

- Implement and test agents to meet business requirements, from sandbox to production.
- Manage, monitor, and troubleshoot agents to drive adoption and performance.

Key Topics

This unit prepares you for the Deployment Lifecycle section of the Salesforce Agentforce Specialist exam, which makes up 20% of the overall exam. This section of the exam tests these topics.

- Given a scenario, test an agent using Testing Center.
- Identify the considerations for deploying an agent from sandbox to production.
- Explain the process for managing and monitoring Agent adoption.

Like the previous units, this unit contains practice scenario-based questions and flashcards.

Exam Practice Questions

Ready to jump in? The sample tool is not scored—it's just an easy way to quiz yourself. To use it, read the scenario, then click the answer you think is correct. Some questions can have more than one correct answer. Click **Submit** to learn whether the answer you chose is correct or incorrect, and why. When you reach the end, you can review the answers or retake the questions.

Study Materials

Did you choose an incorrect answer? Check out the table for related study materials.

Universal Containers needs to automate regression testing within CI pipelines. Which method should the team use?

A

Use Agentforce DX or Testing API to run scripted tests via CLI or REST API.

B

Manually rerun a comprehensive set of test cases using CSV uploads and verify results daily.

C

Defer regression testing until an error is reported in production and then manually investigate and resolve the issue.

A

2) Universal Containers wants to fast-track its testing process for an Agentforce agent. The team needs to create and upload their own test scenarios and also want to use AI-generated test cases. Which steps should they follow to create and upload their own test scenarios and generate AI-based test cases?

A

Deploy to production without testing and rely on feedback.

B

Use Testing Center, add context, generate AI test cases, and upload a CSV.

C

Manually rerun test cases daily using CSV uploads without AI.

B

Universal Containers is preparing to deploy an Agentforce agent from its sandbox environment to production. The team needs to ensure that all necessary steps are followed to avoid any issues during deployment. What is a critical predeployment step to ensure a successful Agentforce deployment from sandbox to production?

A

Ensure that the Target Org has the same user profiles as the sandbox environment.

B

Verify that the Target Org has the same data records as the sandbox environment.

C

Verify that the Target Org has valid licenses for Agentforce and ensure Einstein and Bots are enabled.

C

Universal Containers has recently deployed an Agentforce agent and wants to manage and monitor its adoption effectively. They plan to use Agentforce session tracing to capture detailed interaction data and derive insights. Which step is essential for managing and monitoring Agentforce agent adoption using session tracing?

A

Enable session tracing and review interaction logs directly in the console to monitor agent usage.

B

Enable session tracing and use Data 360 to build reports and dashboards.

C

Enable session tracing and use built-in real-time metrics to monitor agent performance.

B

Study materials:

Agentforce Testing Center

Build trust in your Agentforce agents with the Agentforce Testing Center.

[Trust Your Agents](#)

~5 mins

Incomplete

[Set Up Testing Criteria](#)

~25 mins

Incomplete

[Use AI to Generate Tests](#)

~25 mins

Incomplete

[View Test Results](#)

~5 mins

Incomplete

1. [Agentforce Testing Center](#)

2. [Trust Your Agents](#)

Trust Your Agents

Learning Objectives

After completing this unit, you'll be able to:

- Explain the benefits of different types of testing.
- Describe how automated tests build confidence in your agents.
- Explain the difference between manual and automated testing.



New Agent Building Experience Coming Soon!

Agentforce is getting an update! At Dreamforce 2025, we announced the new agent building experience which may differ from the process and features you learn about in this badge. Expect the new experience to become available in open beta in the weeks following Dreamforce. General availability comes soon after. The current builder experience remains available to support previously built agents. Stay tuned for more information.

Before You Start

If you're new to Agentforce agents, we recommend taking these other badges first so you'll be familiar with the terms in this badge.

- [Agentforce Key Components: Quick Look](#)
- [Agentforce Basics](#)
- [Trusted Agentic AI](#)

Trust Is Our Number One Value

At Salesforce, trust is deeply rooted in everything we do. That's why we rely heavily on testing. Apex tests are automatically run with every new deployment. Unit tests make sure each unit works as expected. Flows are tested to verify that everything functions as expected. To put it simply, testing is one of the best ways to ensure trust in our products and processes.

As a Salesforce admin, testing should also be a cornerstone to make sure everything runs smoothly in your org. You can test new processes in a dedicated sandbox. You can perform user acceptance tests (UAT) with large groups of users. And once you've verified everything through tests, you can deploy the new process to a production environment and monitor it to make sure everything is running smoothly.

Test Agents for Trust

But what about the agents you're creating with Agentforce? How do you make sure they're as trustworthy and reliable as the rest of your Salesforce org?

The answer, again, is testing.

You learn a bit more about testing agents later in the module, but first take a look at some of the challenges you might encounter when testing agentic AI.

Challenge	What this sounds like
Gen AI is nondeterministic producing different outputs for the same input on different runs	"Gen AI is so nondeterministic that I don't have time to test against."

Challenge	What this sounds like
Manual testing is not scalable	"Given the subjective nature of Gen AI, I need something that is not scalable."
Safety and ethical concerns	"Generative AI can produce harmful or unintended results."
Lack of standards	"Generative AI is still new, and there are no clear standards."

If you start encountering these types of challenges, fear not. The Agentforce Testing Center is here to help.

Say Hello to the Agentforce Testing Center

The Agentforce Testing Center is designed to help overcome the challenges you might encounter when building out your Agentforce, and helps you roll out trusted AI agents in a secure, repeatable way. Testing your agents in the Agentforce Testing Center is a critical step in creating trust in your AI agents.

The Agentforce Testing Center is designed with no-code testing tools to help you easily deploy trusted agents. The testing takes place in properly configured sandboxes to isolate testing from the production environment. You can also add more tests over time as your agents get updated or are given more actions. This means your agents continue to work as your business changes and grows.



Sandboxes now have access to Data Cloud and Agentforce to allow for agentic testing.

Testing Methods

There are two testing methods that are used to troubleshoot, verify, and maintain Agentforce agents: manual testing and automated testing.

Manual Testing

Agentforce Builder allows for manual testing and troubleshooting while you build and update the agent. Simply use the Conversation Preview while in the builder to ask the agent a question. You can then view the response and see how it was created. This is a great way to troubleshoot your agents and verify that the correct processes are being called based on the questions. But testing this way takes a long time, and it's challenging to test all the possible scenarios manually. It's also difficult and time-consuming to repeat these tests when needed. This is where the Agentforce Testing Center really shines.

Automated Testing

The Agentforce Testing Center lets you perform automated batch testing, which reduces the amount of testing time. Batch processing also lets you test large numbers of user inputs. These inputs, or questions, are called utterances. An utterance might be something like, "Show me all the open opportunities for the ACME account." There's one utterance for every test execution. Combining multiple utterances with expected responses lets you build a batch of tests. You can use the tests over and over, adding to them as needed to ensure the agent continues to be trustworthy.

The Agentforce Testing Center also helps you do performance testing by running through a large series of tests at one time in a test environment. The Agentforce Testing Center can also use AI to generate hundreds of dynamic interactions. The Agentforce Testing Center runs tests automatically

and in parallel to see what topics and actions the agents choose. After looking at the test results, you manually test and troubleshoot in Agentforce Builder to adjust instructions and guardrails as needed. Automated testing saves time that would have been lost on manually testing many different variations of a conversation.

Deploy with Confidence

Once testing is done, you can confidently deploy the agent to production without concerns of disrupting your business or corrupting your customers' data. And you can deploy the changes by migrating them to your production environment with whatever tool you're currently using, such as Change Sets, DevOps Center, and the Salesforce CLI that now supports Data Cloud and Agentforce.

Concerns and Limits

There are a few things to keep in mind when building and testing agents.

Cost

Running tests, manually or automatically, consumes requests and credits the same as your customers using the agent. This is true even when done in a sandbox environment. Although testing itself has a cost, the cost of not testing can be much higher. Testing consumes Einstein Requests and possibly Data Cloud credits. To learn more, see [Einstein Usage](#) and [Rate Limits](#).

Security

Testing agents can modify CRM data. To avoid modifying data unnecessarily, be sure to use the Agentforce Testing Center and Agentforce Builder tests only in your sandbox environment.

Limits

Currently you can run up to 10 test jobs at once in a 10-hour time frame and have up to 1000 test cases per test.

Ready to take a closer look at testing and using test cases? Get hands-on practice in the next unit.

Discover Agentforce

Learning Objectives

After completing this unit, you'll be able to:

- Define an autonomous agent.
- Explain how Agentforce helps get work done.

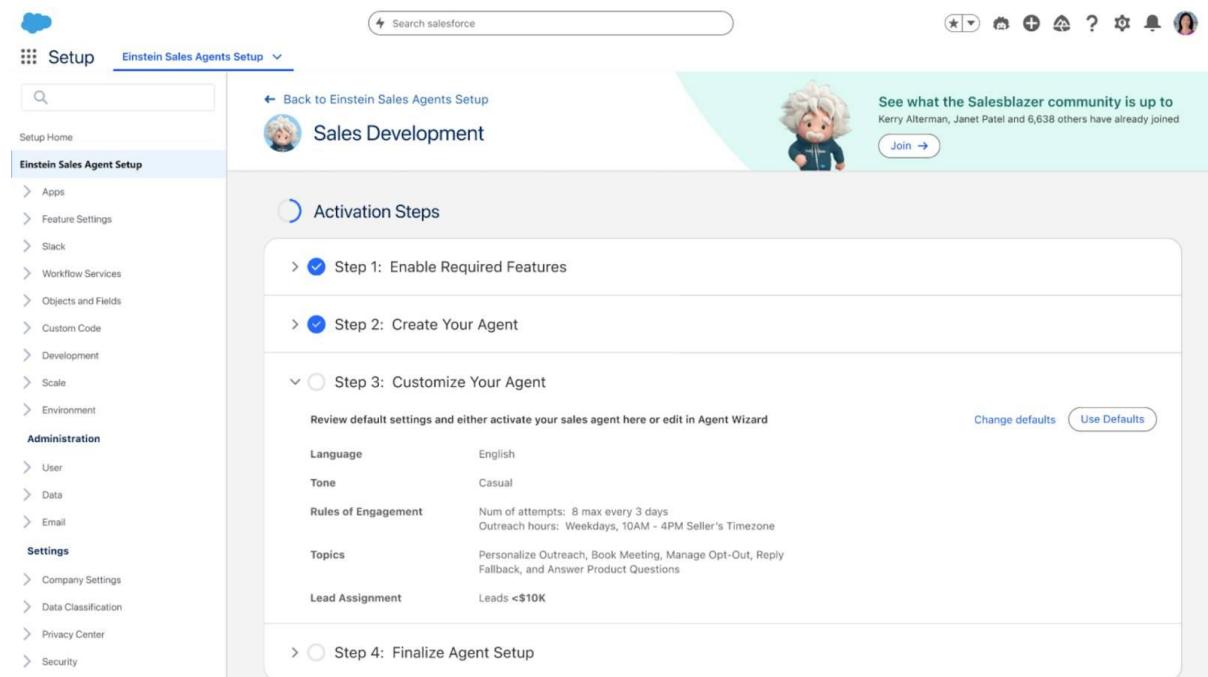
Meet Agentforce

Agents are autonomous, proactive applications designed to execute specialized tasks to help employees and customers. Agents use large language models (LLMs) to analyze and understand the full context of customer interactions or an automated trigger, then reason through decisions on the next steps autonomously.

These agents generate responses that are consistent with your company's brand voice and guidelines using trusted business data, including Salesforce CRM data, external data from Data 360, and more. These agents are capable of operating 24/7 across various platforms like self-service portals and

messaging channels, handling tasks proactively within set guardrails. When faced with complex issues beyond their scope, they can escalate the matter to human agents, ensuring that queries are resolved efficiently and accurately.

The Agentforce out-of-the-box agents are easy to customize and deploy with clicks, not code. They can be set up in minutes, are easily scalable, and work around the clock across any channel. Here are just some of the agents available.

The screenshot shows the Salesforce Einstein Sales Agents Setup interface. On the left, a sidebar lists various setup categories like Apps, Feature Settings, Slack, etc. The main content area is titled 'Sales Development' and shows 'Activation Steps'. Step 1: Enable Required Features (completed) and Step 2: Create Your Agent (completed) are listed under 'Activation Steps'. Step 3: Customize Your Agent is expanded, showing settings for Language (English), Tone (Casual), Rules of Engagement (Num of attempts: 8 max every 3 days, Outreach hours: Weekdays, 10AM - 4PM Seller's Timezone), Topics (Personalize Outreach, Book Meeting, Manage Opt-Out, Reply Fallback, and Answer Product Questions), and Lead Assignment (Leads <\$10K). Step 4: Finalize Agent Setup is also listed. A sidebar on the right encourages joining the Salesblazer community.

- **Service Agent** replaces traditional chatbots with AI that can handle a wide range of service issues without preprogrammed scenarios, improving customer service efficiency.
- **Sales Development Representative (SDR)** engages with prospects 24/7, answering questions, managing objections, and scheduling meetings based on CRM and external data, allowing your sellers to focus on building deeper customer relationships.
- **Sales Coach** provides personalized role-play sessions for your sales team, using Salesforce data and generative AI to help sellers practice pitches and objections tailored to specific deals.
- **Merchandiser** assists your ecommerce merchandisers with site setup, goal setting, personalized promotions, product descriptions, and data-driven insights, simplifying daily tasks.
- **Buyer Agent** enhances the B2B buying experience, helping your buyers find products, make purchases, and track orders via chat or within sales portals.
- **Personal Shopper** acts as a digital concierge on your ecommerce sites or messaging apps, offering personalized product recommendations and assisting with search queries.
- **Campaign Optimizer** automates the full campaign lifecycle, using AI to analyze, generate, personalize, and optimize marketing campaigns based on business goals.
- **Agentforce** supports employees in the flow of their work with specific tasks by searching for data, creating action plans, and executing them to increase workplace efficiency.

Key Components of an Agent

Each agent has parameters that define the job it can do and the action it can take.

- **Role:** An agent's purpose. This defines the job to be done and the broader goals the agent should achieve on your team.
- **Knowledge:** The data an agent needs to be successful. This could include company knowledge articles, CRM data, external data via Data 360, public websites, and so on.
- **Actions:** The goals an agent can fulfill. This is the predefined task an agent can execute to do its job based on a trigger or instruction. For example, it could run a flow, prompt template, or Apex.
- **Guardrails:** The guidelines an agent can operate under. These can be natural-language instructions telling the agent what it can and can't do, when to escalate to a human, or could come from built-in security features in the Einstein Trust Layer.
- **Channels:** The applications where an agent gets work done. This can be your website, CRM, mobile app, Slack, and more.

Agentforce Reasoning Engine, the Brain of an Agent

The Agentforce Reasoning Engine is designed to enhance user interaction through faster, more capable, and more multi-turn conversations. Here's a brief overview and key features.

- **Multi-turn chat:** The reasoning engine facilitates interactive communication with users by considering and adapting to added conversational context, enhancing the accuracy of the service provided.
- **Topic classification:** The reasoning engine classifies user utterances into topics based on predefined descriptions, ensuring relevant responses.
- **Instructions and actions:** Each topic includes specific instructions and actions, such as verifying order details or obtaining further information, to assist users accurately and efficiently.
- **Knowledge Retrieval:** The reasoning engine uses multiple techniques including advanced retrieval augmentation generation (RAG) which selectively uses multiple language models to iteratively refine the quality of queries, retrieving the most relevant knowledge chunks, while also evaluating the quality of the response.
- **Searchable public data:** Agents can now securely access public data through the Einstein Trust Layer, expanding its knowledge base.

How an Agent Takes Action

Agents take action and adhere to guardrails using natural language descriptions that outline the tasks and operational boundaries. Here's a summary of how they operate.

- The agent first receives a trigger, which can be a conversation with an employee or customer, a change in data, or an automation.
- The agent uses the LLM and natural language descriptions to identify the context and select a topic that best fits the job to be done, including the scope, data required, and necessary conditions.
- Depending on the task, an agent selects and chains actions. Those actions are executed via flows, apex classes, APIs, or direct prompts.

- Agents dynamically plan and execute tasks while strictly following predefined guardrails. They also have built-in mechanisms for harm and toxicity detection, using the Einstein Trust Layer, ensuring they avoid engaging in inappropriate or harmful activities.

Now you know a little about Agents, what they do, and how they do it. To learn more, see the Trailhead content listed in Resources—which includes an opportunity to get hands-on and build an agent.

Resources

- [*Trailhead: Quick Start: Build Your First Agent with Agentforce*](#)
- [*Trailhead: Agentforce Service Agent: Quick Look*](#)

Quiz

To complete this unit, you need to answer all the quiz questions correctly.

+100 Points

1

What is a topic classification?

A

A type of large language model

B

A group of user utterances based on predefined descriptions

C

A subset of a company's brand voice and guidelines pulled from trusted business data

D

A sublayer of the Einstein Trust Layer

2

Which of these can serve as guardrails for agents?

A

A list of triggers for conversations

B

Natural-language instructions telling the agent what it can and can't do

C

Built-in security features in the Einstein Trust Layer

D

A and B

E

B and C

Second attempt earns 50 points. Three or more earns 25 points.

Customize Your Agents

Learning Objectives

After completing this unit, you'll be able to:

- Explore the different ways you can customize agent actions.
- Compare the benefits of customizing agent actions.



New Agent Building Experience Coming Soon!

Agentforce is getting an update! At Dreamforce 2025, we announced the new agent building experience which may differ from the process and features you learn about in this badge. Expect the new experience to become available in open beta in the weeks following Dreamforce. General availability comes soon after. The current builder experience remains available to support previously built agents. Stay tuned for more information.

Trailcast

If you'd like to listen to an audio recording of this module, please use the player below. When you're finished listening to this recording, remember to come back to each unit, check out the resources, and complete the associated assessments.

Right out of the box, Agentforce can tackle many of the common challenges businesses face in data and customer relationship management. An agent can help when your team struggles to find the right answers to customer inquiries. Or when too many routine tasks demand your service reps' time. Or when you need content for an upcoming presentation, but lack the human resources to get it done. From automating customer points of contact to summarizing meetings and documents for key stakeholders, there's a lot you can do with the standard Agentforce configuration. But what about the advanced applications that are specific to your business, or that might emerge as you see how agents plug into your work? That's where customization comes in.

Custom Agent Actions

Custom agent actions are how you can influence the way your agents act. While agents can read any data you give them access to in Salesforce, they can't change records without a predefined agent action. These actions can be configured and chained together to create the functionality you need. This might involve greeting a hotel guest and offering options when they check in, or automatically sending summarized notes to all participants after a weekly meeting.

The good news about custom actions is that you don't have to create them out of thin air. In fact, custom actions are based on Salesforce technologies you already know and love. When you create a custom action, you build it on top of existing platform functionality that you want to make available in Agentforce—invocable and REST Apex classes, autolaunched flows, and prompt templates. In Agentforce, we refer to that underlying functionality as a *reference action*, and it's an awesome way to get more mileage out of your Salesforce Platform capabilities.

Deterministic or Non-Deterministic

When developing the underlying platform functionality for your agent actions, you might wonder when you should use a flow, Apex class, or prompt template to build the action. Essentially it comes down to whether the process you're automating is deterministic or not.

- **Deterministic:** Uses an invocable Apex class, REST Apex class, or autolaunched flow to generate output. Actions based on flows or Apex are deterministic and use business logic and rules to produce a consistent outcome.
- **Non-deterministic:** Uses one or more prompt templates to generate output, which involves a degree of randomness. A prompt-based action lets you control how a response is written or use the reasoning and generative capabilities of an LLM. For example, to generate a summary or perform sentiment analysis, you need to use a prompt template as a reference action. Prompt templates are also used to [ground an agent in data](#), such as knowledge or external system data.

Keep in mind that a single agent action can combine both deterministic and non-deterministic approaches. For example, say that when a guest cancels their hotel reservation, a flow-based action is triggered to complete the cancellation. At some point during that flow, the agent could also follow a prompt to ask the customer for information about why they're cancelling. The agent could even summarize the response from the customer and provide that summary for review if the customer indicates a particular reason for cancelling.

Let's take a closer look at each of the reference actions you can use when building a custom agent action: prompt templates, flows, and Apex.

Prompt Templates

Agents come with templated prompt types for a wide range of common tasks like answering emails or managing service cases. Prompt Builder's intuitive UI also has several features, like one-click copy for text fields and the ability to generate resolutions without full responses if you need to iterate quickly. To get the best performance out of your prompts, you'll want to refine the templates and create new ones to fit the specific use cases you experience in your business. With Prompt Builder, you can easily modify a default prompt to collect the right information, deliver personalized responses, and ensure things are running smoothly for your agents.

For example, if an agent is generating generic responses that don't make customers feel valued, you can use a prompt template to add instructions for the agent to use your existing customer data to provide more tailored responses. Prompts allow you to create context-aware and evolving commands that come in three main types.

- **Field generation templates** work well with a single object, such as an account, but have limitations in providing additional context.
- **Service email templates** are ideal for case-related responses but are restricted to that scope.
- **Flex templates** offer the most versatility, allowing you to use multiple objects, free text input, and data models for richer responses. These templates aren't as quick to use for simple tasks but work well when you need a specific solution that includes creative thinking.

Flows

The true power of Agentforce lies in its ability for agents to activate flows—low-code tools that enable users to perform complex business tasks, such as modifying customer records. And you can build agent-ready flows for your agents to make tasks easy. They can also improve an agent's accuracy by instructing agents to access specific and relevant data instead of using all the data they have access to in Salesforce.

Apex

While flows and prompts can do a lot to refine how Agents work with Salesforce, they only work with tasks you can automate through natural language instructions and traditional flows. However, because LLMs can also read and process code, agents can also help you take advantage of the power of Apex. With Apex customization, a single person can code advanced applications into simple-to-deploy agent actions that can be used and referenced by others. These actions can help you do things like check flight times at the airport closest to your business or pull and analyze data from a previously built Apex application already used by your teams. Once you've added your Apex code to an agent action, even teams with limited code knowledge can use the action.

Dive Deeper

Continue your AI agent learning journey by exploring other badges related to prompts, flows, and Apex customization to gain more hands-on experience and discover various ways to enhance how Agents work.

- [Service Agent Customization with Prompt Builder](#)
- [Agent Customization with Flows](#)
- [Agent Customization with Apex](#)

It won't take long for you to discover all the advantages of having agents that are tailored to your specific needs.

Resources

- [Salesforce Help: Customize Your Agents with Topics and Actions](#)
- [Salesforce: Agent Builder Overview](#)

Quiz

To complete this unit, you need to answer all the quiz questions correctly.

+100 Points

1

Which type of customization is best for complex automation, like retrieving data from a third-party service as part of a prompt?

A

Flows

B

Prompts

C

Apex

D

Apps

2

What do flows allow AI agents to do?

A

Make changes to your Salesforce data.

B

Repeat previously successful prompts.

C

Designate pathways for customers to interact with the right agent.

D

Use custom code to create advanced agent actions that you can easily deploy.

Second attempt earns 50 points. Three or more earns 25 points.

Get Started with Agentforce

Learning Objectives

After completing this unit, you'll be able to:

- Explain what Agentforce is.
- Identify the main characteristics of Agentforce.
- List a few use cases for Agentforce.



New Agent Building Experience Coming Soon!

Agentforce is getting an update! At Dreamforce 2025, we announced the new agent building experience which may differ from the process and features you learn about in this badge. Expect the new experience to become available in open beta in the weeks following Dreamforce. General availability comes soon after. The current builder experience remains available to support previously built agents. Stay tuned for more information.

Before You Start

Before you start this module, consider completing this recommended content.

- [Generative AI Basics](#)
- [Large Language Models](#)
- [Autonomous Agents](#)

The Hero of Our Journey

Meet Linda Rosenberg, the Salesforce admin at Cloud Kicks. Cloud Kicks sells stylish and comfortable custom sneakers, and the company is growing fast. Linda is always looking for ways to

better serve customers and make work easier for Cloud Kicks employees. She's excited about the value that Agentforce provides.

Linda aims to boost employee productivity by automating time-consuming and repetitive tasks, freeing people up for more strategic activities. She also wants to provide more personalized responses to customers, ensuring they get the help they need.



One day, a customer, Alex, reaches out to Cloud Kicks with a series of questions. Here's how the interaction currently unfolds without Agentforce.

Customer (Alex): "Hi, I just placed an order for a pair of custom sneakers. Can you tell me when it will be delivered?"

Customer service representative (CSR): "Hello, Alex! Your order will be shipped within the next 2 to 3 business days and should arrive at your address within 5 to 7 business days after shipping."

Alex: "Thanks! Do you have any stores in New York City?"

CSR: "I'm not sure. Let me check our store locations. One moment, please."

CSR, after a long pause: "I couldn't find any information on stores in New York City. You might want to check our website for more details."

Alex: "All right, thanks. One more thing—do you have any recommendations for a good running trail in New York City?"

CSR: "I'm sorry, but I don't have that information. I suggest checking a local running club or a tourism website for recommendations. Do you have any other questions?"

Alex: "No, that's all. Thanks for your help."

CSR: "You're welcome, Alex. Have a good day!"

Alex might be amiable, but this conversation highlights the challenges of automated customer service without comprehensive information and real-time data access. Delays and incomplete answers dampen the customer experience.

Linda is thrilled about Agentforce's potential to transform customer interactions. With Agentforce, customer service becomes more autonomous while delivering relevant information. Agentforce ensures every interaction is smooth, efficient, and helpful.

Meet Agentforce

Agentforce is a customizable suite of autonomous and assistive artificial intelligence (AI agents). AI agents are goal-oriented AI applications that perform tasks and business interactions. Designed to make intelligent decisions, Agentforce can initiate and complete a sequence of tasks, handle natural language conversations, and securely provide relevant answers drawn from business data. Whether your users are on a desktop or mobile device, Agentforce is there to help across a wide range of workflows and interactions.

The screenshot shows the Salesforce Seller Home dashboard with the following sections:

- Close Deals:** Opportunities owned by me and closing this quarter. Total Pipeline: \$0. Status: 0 Open, 0 Won, 0 Lost.
- Plan My Accounts:** Accounts owned by me. Total: 3. Status: 0 Upcoming Activity, 0 Past Activity, 3 No Activity.
- Grow Relationships:** Contacts owned by me and created in the last 90 days. Total: 7. Status: 0 Upcoming Activity, 0 Past Activity, 7 No Activity.
- Build Pipeline:** Leads owned by me and created in the last 30 days. Total: 4. Status: 0 Upcoming Activity, 0 Past Activity, 4 No Activity.
- My Goals:** Set personal weekly or monthly goals for emails, calls, and meetings. Includes a "Set goals" button.
- Today's Events:** Looks like you're free and clear the rest of the day.

Agentforce (Default) Sidebar:

- Hi!** I'm Agentforce, an AI assistant. I can do things like search your Salesforce data or the web, edit your Salesforce records, and draft or revise emails and fields. Ask me "What else can you do?" to see how I can help simplify your work day.
- Summarize the Acme deal.**
- Here is the summary of the Acme deal. How else can I assist you?**
- Account Overview:** Acme operates in the Manufacturing industry with 600 employees. The account is managed by OrgFarm EPIC. The sum of closed deal amounts is not provided, while the sum amount in the open pipe is 230,000 USD.
- Opportunities:** There are no won or lost opportunities over the last year. Top opportunities include Acme - 1,200 Widgets in the Value Proposition stage, Acme - 600 Widgets in the Needs Analysis stage, and Acme - 200 Widgets in the Prospecting stage.
- Open cases:** There are 2 open cases, with none escalated.
- Activity:** There are no recent activities or events.
- Describe your task or ask a question...**

Best of all, you don't need to know a stitch of code to set up an AI agent in Salesforce. All you have to do is enable Agentforce and then create an agent. Here are some actions an AI agent can take out of the box.

- Summarize Salesforce records, such as opportunities, accounts, and cases.
- Draft or revise emails.
- Find and update Salesforce records.
- Aggregate Salesforce data.
- Answer questions with information from your knowledge base.

On top of that, it's easy to extend your AI agent by using your existing Salesforce Platform. For example, if you already have a flow in Salesforce that makes product recommendations, you can add that capability to an agent with just a few clicks.

Agentforce Characteristics

Let's take a closer look at each characteristic of Agentforce so you can get more familiar with your new digital companions.

Trusted

At Salesforce, Trust is our #1 value. That's why we build generative AI tools like Agentforce with Trust at the core.

Your AI agents respect Salesforce's standard access controls, ensuring secure actions. Agentforce integrates with the [Einstein Trust Layer](#), a secure AI architecture built into the Salesforce Platform. You get the benefits of generative AI without compromising customer data, and you can use trusted data to enhance AI responses.

Here's how it works:

- **Data grounding:** The Trust Layer grounds and enriches generative prompts with trusted company data.
- **Zero-data retention:** Your data stays safe; it's never retained by third-party large language model (LLM) providers.
- **AI monitoring:** AI interactions are logged, giving you visibility into each user interaction.

For critical scenarios where accuracy is key, agents can seamlessly transfer the conversation to a human. For example, if a user needs help with a complex issue like resetting a password and prefers a human touch, an agent verifies their identity, then promptly transfers the conversation for personalized support.

Proactive

Some AI agents aren't just reactive, they're proactive, which is essential in dynamic business environments. AI agents use the reasoning engine in Agentforce to perform the reasoning and acting process. The reasoning engine helps agents automate routine tasks, handle tedious duties, and find the right solutions for customers. This simplifies the process for service reps at Cloud Kicks, making their jobs easier and more efficient.

Here's how AI agents use reasoning to enhance these actions.

Case Status Update:

- **Reason:** The agent reviews the case context, current status, and recent updates.
- **Act:** The agent notifies the customer of changes or escalates the issue to a higher-level support team.
- **Observe:** The agent monitors the case outcome and adjusts its approach to ensure efficient resolution.

Email Received:

- **Reason:** The agent reviews the email content and the nature of the request.
- **Act:** The agent processes the email, creates a new support ticket, or routes it to the relevant department.
- **Observe:** The agent monitors the response to ensure the issue is handled correctly, making adjustments if needed.

Sales Follow-Up:

- **Reason:** The agent reviews the customer's interest and the context of their inquiry.
- **Act:** The agent schedules a follow-up call with a sales representative to keep the lead engaged.
- **Observe:** The agent monitors the follow-up outcome and adjusts its approach to improve future interactions.

Natural Language

A conversational interface lets people ask questions or give instructions in natural language, just like talking to a human. Agentforce retains the conversation context, making follow-up questions and related requests seamless.

For example, instead of navigating the Salesforce UI to find records, a sales rep can simply type, “Show me my Acme deals.” The AI agent interprets the request, responds in natural language, and displays a list of matching opportunities. It feels just like chatting with a trusted colleague.

In the same conversation, the sales rep can then ask, “Show me their open cases.” The AI agent remembers the context and knows “their” refers to Acme. This capability ensures multiple, coherent, and efficient interactions.

But with Agentforce, you're not limited to conversational interfaces and chat windows. You can [trigger an agent](#) to complete background or event-driven tasks from anywhere you can call a flow or Apex class.



Agentforce Versus Einstein Bots

Not sure about the difference between Agentforce and Einstein Bots? Bots require a lot of expertise and time to set up, and they're based on complex, strictly defined conversational rules.

Agentforce is flexible and requires less configuration because it's powered by an LLM. For more information, see [What's the Difference Between an AI Agent and a Chatbot?](#)

Dynamic Information Retrieval

Dynamic information retrieval makes AI agents highly effective at handling complex tasks. Here's how it works.:

- **Retrieval augmented generation (RAG):** Agents use semantic search on structured and unstructured data in Data 360 to fetch relevant info from external sources and databases.
- **Generic information retrieval tools:** Tools like web search and knowledge Q&A help agents handle complex tasks. For instance, you can research a company or product online and combine it with internal knowledge to create an email summary.
- **Deployment in Flows, APIs, and Apex Classes:** Agents can be deployed in these environments, passing all contextual information to the agent. This eliminates the need for custom solutions in each scenario, making the agent more versatile and efficient.

Now that you see how Agentforce enhances seamless customer interactions and automates tedious tasks, let's revisit that initial conversation and see the transformation with Agentforce in action.

Customer (Alex): “Hi, I just placed an order for a pair of custom sneakers. Can you tell me when it will be delivered?”

Agentforce: “Hello, Alex! Your order will be shipped within the next 2 to 3 business days and should arrive at your address within 5 to 7 business days after shipping. Is there anything else you'd like to know about your order?”

Alex: “Thanks! Do you have any stores in New York City?”

Agentforce: “We don’t have any physical stores in New York City, but we have a popup shop opening next month at 123 Fashion Avenue from October 1 to October 15. You can also shop online for the latest styles.”

Alex: “Awesome, thanks! One more thing—do you have any recommendations for a good running trail in New York City?”

Agentforce: “Certainly! For a great running trail, I recommend Central Park’s Reservoir Loop, which is 1.58 miles and offers beautiful views. For a longer run, try the Hudson River Greenway, which stretches for about 13 miles. Enjoy your run!”

Alex: “That’s perfect, thanks so much for all the information!”

Agentforce: “You’re welcome, Alex! If you have any more questions, feel free to reach out. Have a great day!”

Wow, talk about more helpful! Each question was answered with specific details without any pauses or vague responses. Linda is convinced, and eager to start using Agentforce.

Follow along as Linda explores the different components of Agentforce and learns more about how the feature works.

Resources

- [*Trailhead: Generative AI Basics*](#)
- [*Trailhead: Large Language Models*](#)
- [*Trailhead: Prompt Fundamentals*](#)
- [*Trailhead: The Einstein Trust Layer*](#)
- [*Blog: AI Is Coming—Here’s How to Get Ready*](#)
- [*Salesforce Help: Einstein Generative AI*](#)
- [*Blog: What’s the Difference Between an AI Agent and a Chatbot?*](#)

Quiz

To complete this unit, you need to answer all the quiz questions correctly.

+100 Points

1

What is Agentforce?

A

A large language model

B

A customizable suite of autonomous and assistive AI agents

C

A suite of Einstein bots

D

A Lightning web component

2

What are some of the benefits of Agentforce being integrated with the Einstein Trust Layer?

A

Third-party LLM providers never retain your data.

B

Actions are available to all users regardless of permissions and settings.

C

AI interactions are captured in event logs.

D

A and B

E

A and C

Explore Agentforce Guardrails and Trust Patterns

Learning Objectives

After completing this unit, you'll be able to:

- Describe Platform guardrails.
- Describe Agentforce guardrails.
- Explain how to customize Agentforce guardrails.
- Explain the trust patterns used to build agents at Salesforce.

Trailcast

If you'd like to listen to an audio recording of this module, please use the player below. When you're finished listening to this recording, remember to come back to each unit, check out the resources, and complete the associated assessments.

Ensure Trust with Guardrails

AI is moving fast. And with such rapid change, it's natural to feel some anxiety. At Salesforce, our product team and [Office of Ethical and Humane Use \(OEHU\)](#) recognize that maintaining trust in our products is imperative and are tackling the agentic AI risks and concerns by:

- Identifying the necessary controls to build a trusted agent
- Building a testing strategy
- Adding in-product ethical guardrails
- Providing better ethical guidance to our customers

Building these guardrails into our products and giving clear ethical guidelines help companies handle AI technology responsibly, keeping things safe and reliable for everyone.

Let's get into some details, starting with the platform guardrails, which provide global controls across our products.

Platform Guardrails

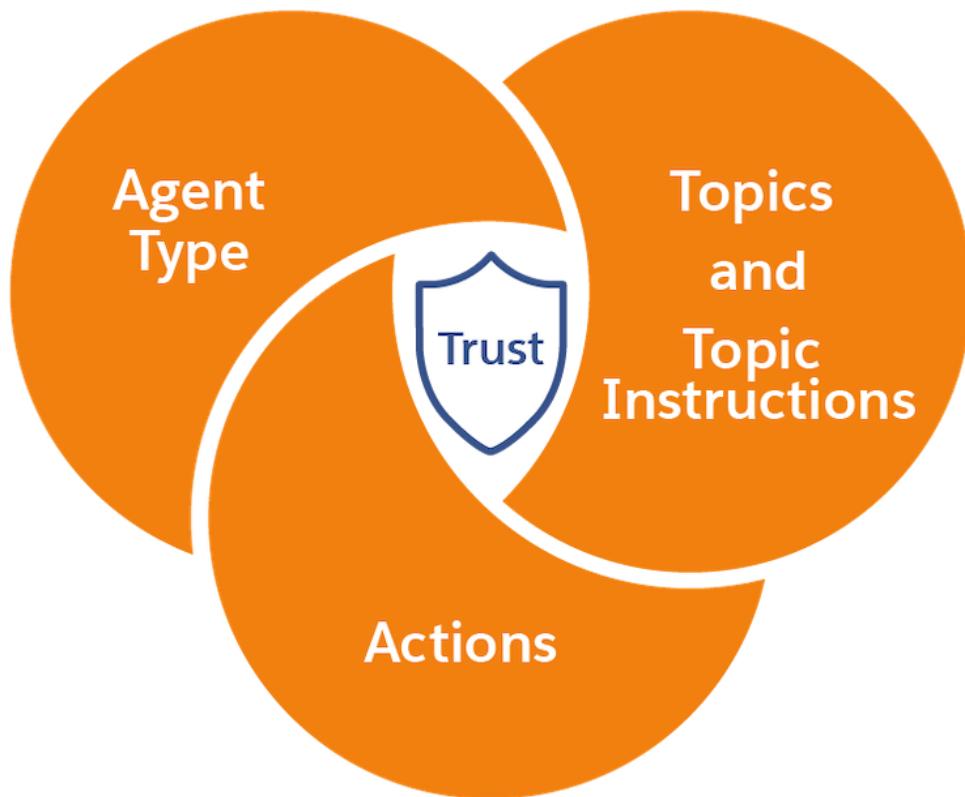
Salesforce includes a comprehensive set of policies, guidelines, and protocols designed to ensure the safe, ethical, and compliant operation of the platform. These guardrails include:

- **Acceptable Use Policy (AUP)**: General rules for customer use of Salesforce services, prohibiting activities that could harm the platform or its users.
- **AI Acceptable Use Policy (AI AUP)**: Specific rules for customer use of Salesforce AI technologies, ensuring our products are used in a responsible way.
- **Model Containment Policies**: Clear rules for how AI models are used. These rules make sure that AI models are used within certain limits to prevent them from being misused or having unintended effects.

These controls create a framework that maintains the platform's integrity, security, and ethical standards. For example, the AUP states that you can't use the platform to spam or phish. The AI AUP states that AI can't make legal or important decisions without a human making the final decision. Model containment policies can limit the types of data an AI model can access to help prevent data leakage or misuse.

Agentforce Guardrails

Agentforce guardrails are a set of rules, guidelines, and best practices that are made for a specific Salesforce Cloud or Product, business use, and to make sure agents follow local laws and standards. Agentforce includes ethical guardrails to minimize AI hallucinations and security guardrails to prevent threats and malicious attacks, such as prompt injections.



Agent Type

Salesforce provides out-of-the-box agents for specific clouds and common use cases. Different agent types can have their own settings and guardrails to define agent behavior. For example, the Agentforce Service Agent (ASA) type uses topic instructions to determine when to escalate a conversation from the AI agent to a human representative. The Sales Development Rep (SDR) agent type has admin-defined engagement rules for the conditions when the agent can start working on the lead and how and when agent emails can be sent.

Topic, Topic Instructions, and Actions

Each agent includes a set of prebuilt topics and actions.

Topics are a category of actions related to a particular job to be done by agents. Topics contain actions, which are the tools available for the job, and instructions, which tell the agent how to make decisions. Together, topics define the range of capabilities your agent can handle. Salesforce provides a library of standard topics for common use cases.

Topic instructions set guidelines for agent behavior, providing the context needed to perform their jobs effectively. Each topic is a category of actions related to a specific job, containing actions (tools) and instructions (decision-making guidelines). Instructions help agents make decisions about how to use the actions in a topic for different use cases. These instructions are typically phrased as “Always...”, “Never...”, “If x, then y...”, or “As a first step,...” to ensure clear and consistent behavior.

Actions are how agents get things done. Agents include a library of actions, which is a set of jobs an agent can do. For example, if a user asks an agent for help with writing an email, the agent launches an action that drafts and revises the email and grounds it in relevant Salesforce data. Salesforce

provides some actions out of the box, and these actions are called standard actions. The benefit of including standard topics and actions by default is that your agent is ready to help users with many common tasks right away.

Customize Guardrails

For more granular control, use agent topic instructions to create boundaries, set context, and define agent behavior. You can modify the instructions for a standard agent topic, or you can create a custom topic from scratch.

These guardrails are controlled by your admin and typically signed off by your internal leadership or key decision-makers. This ensures that the guidelines are authoritative and reflect your organization's values and compliance requirements.

Einstein Trust Layer

AI agents are integrated with the Einstein Trust Layer, which is a secure AI architecture natively built into Salesforce.

Designed for enterprise security standards, the Trust Layer lets you benefit from generative AI without compromising your customer data. It also lets you use trusted data to improve generative AI responses.

1. **Data grounding:** The Trust Layer ensures that generative prompts are grounded and enriched in trusted company data.
2. **Zero-data retention:** Your data is never retained by a third-party LLM provider.
3. **Toxicity detection:** Potentially harmful LLM responses are detected and flagged.
4. **AI monitoring:** AI interactions are captured in event logs, giving you visibility into the results of each user interaction.

Trust Patterns of Agents

Across our products, we implement several key trust patterns, standard product designs to improve safety. Here are a few examples.

Trust Pattern	Example
Reduce hallucinations.	We use topic classification to map user inputs to specific topics. This reduces the risk of generating incorrect or irrelevant information.
Limit the frequency of agent-generated emails.	We limit the frequency of agent-generated emails to prevent overwhelming users. Only meaningful communications are meaningful.
Respect user privacy.	We include an opt-out feature in the CRM software, allowing users to control how they receive communications from AI agents.
Create transparency by design.	We make sure that AI-generated content is directly and transparently disclosed.
Facilitate smooth AI-human handoffs.	We facilitate smooth transitions from agents to humans. Examples include copying generated emails, or providing a dashboard for human oversight.

Implementation Best Practices

When implementing Agentforce guardrails in your organization, follow these best practices.

Best Practice	Example
Understand the policies.	Create a list of the policies that are applicable to your industry, geography, and use case. Use what the agent can and can't do. These can help determine what topics can be assigned to your agents.
Implement robust security measures.	Limit the access of the agents to what they need to complete the assigned tasks. Make sure to protect sensitive data and comply with data protection and regulatory requirements. Use topic instructions to set the rules that the agent follows.
Facilitate human oversight.	Set clear guidelines for how and when to hand off to a human representative. Use topic instructions to provide context and ensure smooth transitions.
Monitor and audit.	In addition to initial testing, continuous monitoring helps to make sure the agents are performing as expected. Use the Audit Trail feature in the Einstein Trust Layer to gain detailed insights into AI actions and outcomes.
Respect user privacy.	Use the opt-out feature to allow users to control communication frequency and protect their privacy.
Conduct regular assessments.	Regularly conduct bias, explainability, and robustness assessments to monitor ongoing safety and performance.

Resources

- [*Salesforce Help: Best Practices for Writing Topic Instructions*](#)
- [*Salesforce: Trust Patterns: How Salesforce Builds Trust in Our AI Products*](#)
- [*Salesforce Help: Trust and Agents*](#)
- [*Salesforce Help: Einstein Trust Layer*](#)

Quiz

To complete this unit, you need to answer all the quiz questions correctly.

+100 Points

1

How can you adjust the agent's behavior in Agentforce?

A

Modify the agent's code directly.

B

Change the agent's name and profile picture.

C

Adjust topic instructions and actions.

D

Alter the agent's voice and tone.

2

True or false: Topic classification is used to map user inputs to specific topics.

A

True

B

False

Second attempt earns 50 points. T

Promote Responsible and Ethical Agents

Learning Objectives

After completing this unit, you'll be able to:

- Implement ethical red-teaming and testing strategies.
- Develop guiding principles and standards for your organization.

Trailcast

If you'd like to listen to an audio recording of this module, please use the player below. When you're finished listening to this recording, remember to come back to each unit, check out the resources, and complete the associated assessments.

Guiding Principles for Responsible Agents

Many organizations adopting AI find it helpful to establish responsible AI principles before developing their AI strategy. With a set of AI principles, businesses can clarify their position on AI and consider the technology's impact on employees, customers, and society. You can use our guidelines as inspiration for developing your own based on business needs and use cases. Think about what safety means for your use case. Do you have specific laws, rules, and regulations for your industry that can require specific safety requirements?

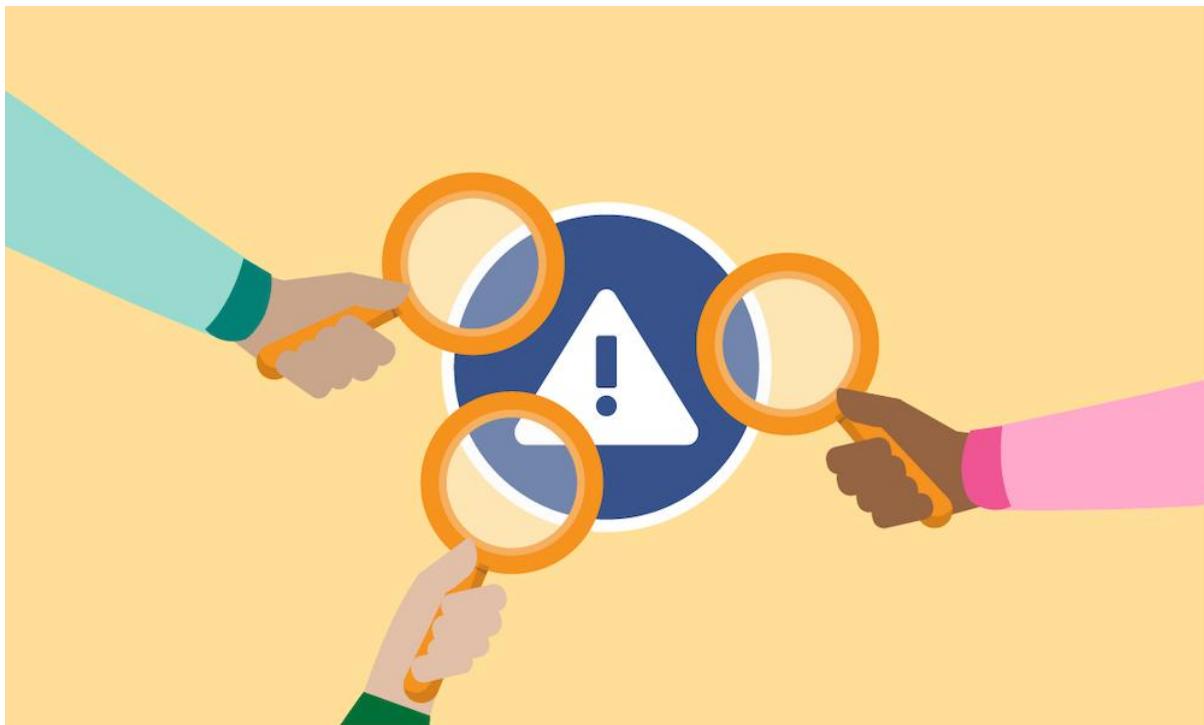
As a refresher, and to get you started establishing your own guiding principles, here's the Salesforce guiding principle for developing trusted AI.

- Accuracy
- Safety
- Honesty
- Empowerment
- Sustainability

Red-Teaming and Testing Strategies

A red team is a group of experts, usually security and AI ethics experts, who try to get into an organization's systems to find and fix security and other problems that involve undesirable outputs or outcomes.

Red-teaming can be defined as “a structured process for probing AI systems and products for the identification of harmful capabilities, outputs, or infrastructural threats.”



Testing is a key aspect of ensuring safety and preventing unintended consequences. Here are some key things to think about.

- Understand what harms you want to test for. Set the goals and objectives for testing and align them with your business goals and use case.
- Build the team to perform these tests. You can use both internal and external experts who are well-versed and have experience in adversarial thinking and creating attack strategies to test.
- Test periodically to make sure you're keeping up with the evolving technology and adversarial thinking around AI and agents.

Here's how we approach red-teaming at Salesforce. Salesforce uses both manual and automated red-teaming methods to make our AI products safer. We test for bad use, intentional integrity attacks like prompt injections, or accidental misuse. We conduct AI red-teaming for toxicity, bias, and security to make sure that if any malicious use or benign misuse occurs, our systems are safe.

Type of Testing	Description
Manual	Manual testing uses the creativity, experience, and specialized knowledge of human testers to craft complex attacks that automated systems can miss. Human testers can also adapt their approach to the specific environment, tailoring attacks more realistic and tailored.
Automated	Automated testing is used as an enhancement, not a replacement for human-driven testing and evaluation. It uses scripts, algorithms, and software tools to simulate many attacks or threats in a short time. It also explores the space of possible attacks by looking at the amount of risk.

We engage with external and internal experts to perform penetration tests and address the unique risks and use cases of agents.

To get a more comprehensive overview, check out our [responsible red-teaming blog](#).

Model Benchmarking

By comparing our AI models against industry standards, we can make sure that they perform at the highest level. We made this even better by publishing the [first LLM Benchmarks for CRM](#). These benchmarks share important measures that help us understand how well an AI system works and also inform our customers.

The Future of Ethical Testing

The testing, evaluation, and assessment team at Salesforce is dedicated to ensuring the trust and safety of our AI products. Through rigorous testing processes, proactive red-teaming, and comprehensive benchmarking, we strive to maintain the highest standards of AI integrity. By fostering a culture of continuous improvement and innovation, we're committed to delivering AI solutions that our customers can trust.

AI Acceptable Use Policy

Salesforce has published an [AI Acceptable Use Policy](#) (AI AUP) to align with industry standards and our partners, and to protect our customers. You can learn more by reviewing our [AI Acceptable Use Policy](#).

The Salesforce AI AUP is central to our business strategy, which is why we took the time to consult with our Ethical Use Advisory Council subcommittee, partners, industry leaders, and developers before its release. In doing so, we aim to entrust responsible innovation and protect the people who trust our products as they are developed. The Salesforce AI AUP is just a starting point, focusing on use of AI with Salesforce products. Think about making your own AI rules or principles to make sure your company uses AI in a way that respects your company's ethical values.

Agent Security Standards

Consider these security measures to develop security standards for access control, data protection, and responsible use of agents in your organization.

Category	Type	Recommendation
Access Control	Strict Access Controls	Implement appropriate access controls to ensure that only individuals with a need to know and appropriate authorization are allowed to interact with generative AI models and services. When designing agents, comprehensively identify the agent's entire scope and potential execution contexts. For critical actions, consider running agents within isolated environments to implement granular access controls and minimize potential security risks.
	Monitoring and Auditing	Create alerts and regularly monitor and audit access to generative AI models and services for unauthorized use.
Data Protection	Integrity Controls	Add integrity controls for both internal and customer data. Follow the right rules for access, use, and restore, and basic configurations.
Responsible Use	Customer Data Handling	Take steps to handle Customer Personal Data correctly. Make sure it is only collected for legitimate reasons and that data subjects are given the right notice and consent.
	Customer Transparency	Ensure services don't perform inferences invisible to your customer.
	Content Moderation	Provide a content moderation filter over generative AI services, and enable it by default.

Category	Type	Recommendation
	Ethical Use	Establish guidelines for the ethical use of generative AI to ensure it's used in a manner that prioritizes security.

From Theory to Practice

We covered a lot of ground about trusted agentic AI in this module and how Salesforce develops trusted agentic AI. Now you understand the key risks associated with agentic AI, such as unexpected behavior, bias, and data breaches. You also learned about the specific guardrails and trust patterns that make sure AI agents operate within safe and ethical parameters. You understand the importance of fostering responsible AI practices in your own organization with ethical red-teaming, testing, and the establishment of an AI Acceptable Use Policy.

With this knowledge, you're well on your way to creating AI agents that aren't only effective but also trustworthy and responsible!

Resources

- [Salesforce: AI Red Teaming: Testing for Trust](#)
- [Salesforce: LLM Benchmark for CRM](#)
- [Salesforce: Artificial Intelligence Acceptable Use Policy](#)

Quiz

To complete this unit, you need to answer all the quiz questions correctly.

+100 Points

1

How does Salesforce approach red-teaming for its AI products?

A

By focusing only on manual testing

B

By using both manual and automated red-teaming methods

C

By conducting tests once a year

D

By relying solely on external experts

2

True or false: Continuous improvement and innovation are crucial for maintaining the integrity of AI systems.

A

True

B

False

Second attempt earns 50 points. Three or more earns 25 points.

Set Up Testing Criteria

Learning Objectives

After completing this unit, you'll be able to:

- Explain how to get the testing template.
- Describe the different parts of test criteria.

What to Test

Testing is all about making sure you achieve an acceptable level of risk for your agent. After testing and troubleshooting your agent manually in Agentforce Builder, you've updated the instructions, topics, actions, filters, and guardrails based on those test results. Now, you can use the Agentforce Testing Center to store those tests and run them over and over again.

Your customers put your agents to the test because they want answers to their every question. Hackers, and sometimes even employees, might try to get around restrictions and attempt to perform tasks or manipulate the model's output in ways that the model wasn't designed for. These scenarios get added to the tests in the Agentforce Testing Center.

The trick is to try and predict the types of questions they're going to ask. You should try to cover every angle, every possibility. That's what you're designing your tests to cover.

You can expect to find errors or at least issues as you start testing. Test for positive, expected results. Then test for negative, unexpected, or even invalid results. You want to be sure the agent responds correctly to even the most wrong requests. This is called positive and negative testing. It makes for a more robust test suite.

Here's an example: While testing an agent email input, test for the correct email response. This is testing the positive, valid, and expected behavior. But don't stop there. Test for an incorrect email input to the agent, and be sure the correct response for that scenario is returned. This is testing the negative, invalid, and unexpected behavior.

While this can sound like a daunting task, doing your due diligence pays off in the end. Ready to get started?

Sign Up for a Developer Edition Org with Agentforce Testing Center

To complete this module, you need a special Developer Edition org that contains Agentforce Testing Center and our sample data. Get the free Developer Edition and connect it to Trailhead now so you can complete the challenges in this module. Note that this Developer Edition is designed to work with the challenges in this badge, and might not work for other badges. Always check that you're using the Trailhead Playground or special Developer Edition org that we recommend.

When you're finished completing the step-by-step instructions, click **Check Challenge to Earn 500 Points** at the bottom of the page.

1. Sign up for a free [Developer Edition org with Agentforce Testing Center](#).

2. Fill out the form:
 - For Email, enter an active email address.
 - For Username, enter a username that looks like an email address and is unique, but it doesn't need to be a valid email account (for example, yourname@example.com).
3. After you fill out the form, click **Sign me up**. A confirmation message appears.
4. When you receive the activation email (this might take a few minutes), open it and click **Verify Account**.
5. Complete your registration by setting your password and challenge question. Tip: Save your username, password, and login URL in a secure place—such as a password manager—for easy access later.
6. You are logged in to your Developer Edition.

Now connect your new Developer Edition org to Trailhead.

1. Make sure you're logged in to your Trailhead account.
2. In the Challenge section at the bottom of this page, click the org name and then click **Connect Org**.
3. On the login screen, enter the username and password for the Developer Edition you just set up.
4. On the Allow Access? screen, click **Allow**.
5. On the Want to connect this org for hands-on challenges? screen, click **Yes! Save it**. You are redirected back to the challenge page and ready to use your new Developer Edition to earn this badge.

Turn on Agentforce

1. Click the **Setup** icon  , then click **Setup**.
2. In the Quick Find box, search for and select **Einstein Setup**.
3. Verify Einstein is turned On. If it is already On, then turn it **Off** and then back **On** again.

Turn on Einstein

Enhance your Salesforce data with generative AI to create relevant, customized experiences for your users. [Learn more in help.](#)



4. Refresh your browser.
5. In the Quick Find box, search for and select **Agentforce Agents** under Agentforce Studio. If you can't find the Agentforce Agents page, refresh the browser and try again.
6. At the top of the Agentforce Agents page, click the **Agentforce** toggle, and ensure it is set to **On**.



7. Click the **Enable the Agentforce (Default) Agent** toggle, and ensure it is set to **On**.



8. Refresh the browser.
9. Verify that both **Agentforce Agents** and **Enable the Agentforce (Default) Agent** are on.

Agentforce is now enabled and the Agentforce Testing Center is available. But before we begin testing agents, let's talk about permissions.

Got Permissions?

The Developer Edition that you're using for this badge already has the correct permissions set up, but what if they weren't set up?

Part of creating trust is making sure only the right access is given. Working with Agentforce requires certain permissions. Not only for the Agentforce tools but also for the automations that agents might use. Like access to data, apps, and Apex. Let's start with getting access to Agentforce.

Control access to the Agentforce (Default) agent with type-specific permissions. To use Agentforce (Default), users must have the Access Agentforce Default Agent permission set group or be an admin with the Customize Application permission. Users who previously accessed Agentforce (Default) with only the Modify Metadata permission no longer have access.

To work with the Agentforce Testing Center, these permissions are needed:

- Manage AI Agents AND the required permissions for your agent type AND System Admin profile

Or

- Customize Application AND System Admin profile

Create Test Cases

To start crafting the test cases, you need a place to store them so you can upload them into the Agentforce Testing Center. The Agentforce Testing Center has a template you can use to help get you on your way, so let's start with that. Here's how you get the testing template.

1. From Setup, in the Quick Find box, search for and select **Testing Center**.
2. Click **New Test**.
3. For Test Name, enter **templateCopy**.
4. Select **Einstein Copilot - v1** or **Agentforce (Default) - v1** for the agent to test.
5. Click **Next**.
6. Click **Next**.

- Click the **Template** link.

Use the testing template to create a CSV file of your test cases and upload it. [Template](#)

This downloads a testing_template.csv file to your device.

- Close the New Test without saving. We were just looking for the testing template.
- Open the file in a text editor to see the comma-separated values.

testing_template.csv			
Utterance	Expected Topic	Expected Actions	Expected Response
Summarize account Acme	OOTBSingleRecordSummary	['IdentifyRecordByName', 'SummarizeRecord']	summary of Account details are shown
Summarize account Global Media	OOTBSingleRecordSummary	['IdentifyRecordByName', 'SummarizeRecord']	summary of Account details are shown
List contact names associated with Acme account	GeneralCRM	['IdentifyRecordByName', 'QueryRecords']	contacts available name available with Ac
Summarize account salesforce.com	OOTBSingleRecordSummary	['IdentifyRecordByName', 'SummarizeRecord']	summary of Account details are shown
What is priority of case number 00001001	GeneralCRM	['IdentifyRecordByName', 'GetRecordDetails']	Priority of provided case number is shown
show me details on all the activities of account Acme	GeneralCRM	['IdentifyRecordByName', 'GetActivitiesTimeline']	details of account associated activities sh
Summarize the open cases and Activities of acme from sep to nov 2024	GeneralCRM	['IdentifyRecordByName', 'QueryRecords', 'GetActivitiesTimeline']	summary of open cases and activities ass

CSV files are one of the most common ways to store tabular data. Each value is separated with a comma, and each line is a data record, or a test case. The top row is the header designating what each column is used for by the Agentforce Testing Center. Each question or utterance and its expected outcomes are on a separate line.

Here's a closer look at the first example from the testing_template.csv file.

Utterance	Expected Topic	Expected Actions	Expected Response
Summarize account Acme	OOTBSingleRecordSummary	['IdentifyRecordByName', 'SummarizeRecord']	summary

The *utterance* is "Summarize account Acme" and is looking for the *expected topic* to be OOTBSingleRecordSummary. Notice that the topic is the API name and not the Label for the topic. Utterances are the questions or inquiries that the agent can get. Since an agent can have multiple topics, the Expected Topic is the topic that the utterance should trigger to run.

Then it looks for the *expected actions* from that topic to be more than just a single action. There can be one or more actions used in generating a response. In this case the expected actions are set in a list denoted with brackets [] and each action is separated with single quotes 'Copy and a comma. The actions for this test case are 'IdentifyRecordByName' and 'SummarizeRecord'. Notice again that the actions in the list are the API names and not the Labels for the actions.

The last column is for the *expected response* to the actions and is set as a description of what the response should cover.

Now let's look at another example from the testing template file. The last line is similar to the first, but covers more data since it is looking for all open cases and activities of the Acme account in a certain data range.

Utterance	Expected Topic	Expected Actions	Expected Response
Summarize the open cases and Activities of Acme from sep to nov 2024	GeneralCRM	['IdentifyRecordByName', 'QueryRecords', 'GetActivitiesTimeline']	summary of open cases and activities ass



When creating your own test criteria, be sure to add utterances for positive and negative results and appropriate topics, actions, and responses. Also, the only required columns are Utterance and at least one other column. Empty values are treated as failures.

Run Your Tests

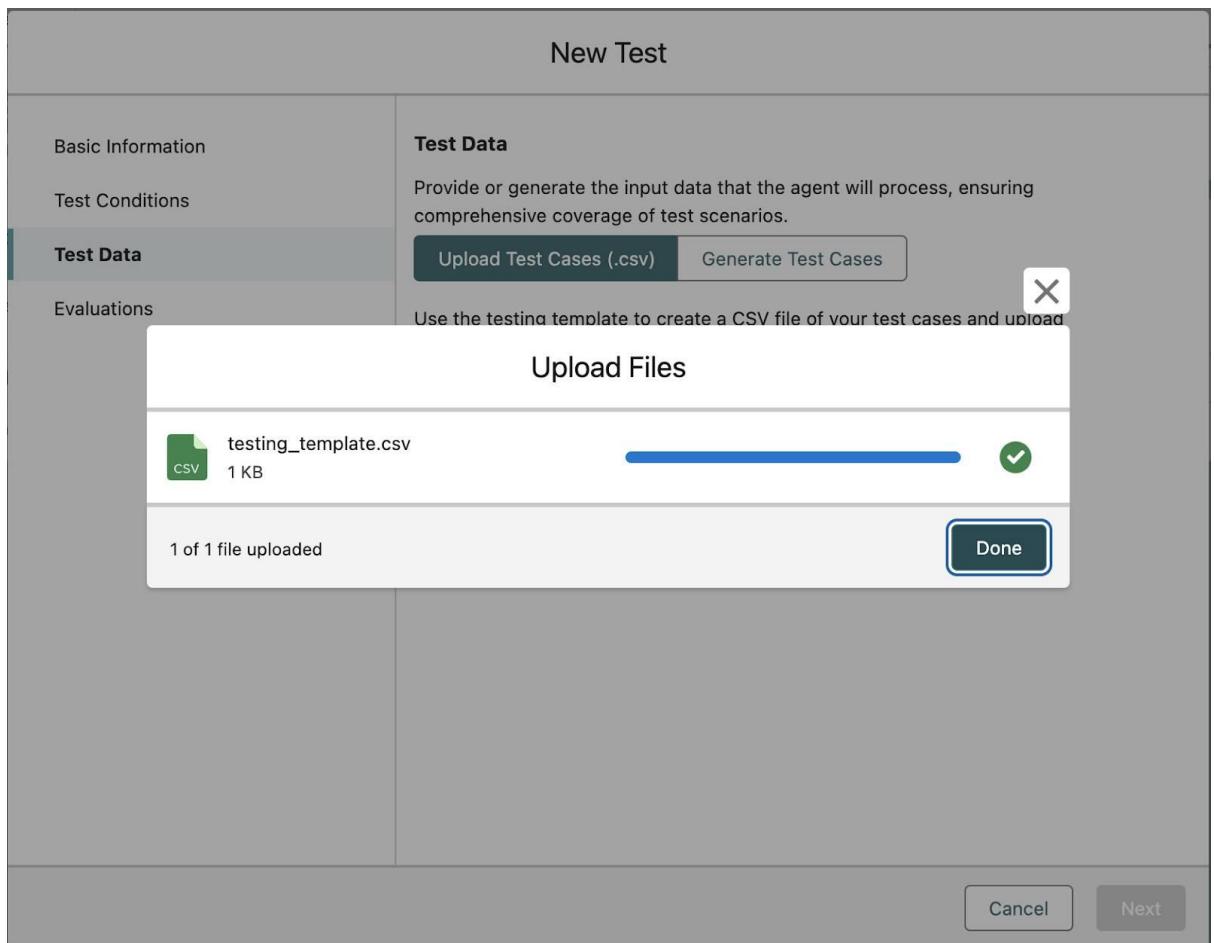
Once you have created your own test cases in a CSV file, you're ready to initiate the test. Let's see how to do that.



Important!

- Running tests consumes requests and credits. See [Considerations for Testing Center](#).
 - Testing agents can modify CRM data. To avoid issues, be sure to use the Agentforce Testing Center only in your sandbox environment.
1. From Setup, in the Quick Find box, search for and select **Testing Center**.
 2. Select **New Test**.
 3. For Test Name, enter Test Agentforce v1Copy. Note: When you create your own tests, use versions and be specific with the test name so they are easy to discern from other tests and versions.
 4. Select **Einstein Copilot - v1** or **Agentforce (Default) - v1**.
You can have more than one agent to select from. Each test only runs against one agent.
 5. For Description, enter Test cases for Agentforce to verify account summaries and detailsCopy.
Descriptions should be natural language describing the types of test cases being run.
 6. Click **Next**.
 7. Test Conditions allows you to specify Context Variables that are used in your tests by the agents when they need input values. For this test, we won't need to use them. Click **Next**.

8. Click **Upload Files** and select the **testing_template.csv** test file.



9. Click **Done**.

10. Click **Next**.

11. Click **Save & Run**.

The screenshot shows the 'Test Agentforce v1' results page. The summary section shows the following metrics:

- Status: Complete
- Duration: 1 min 11 sec
- Topic Pass %: 0.00%
- Action Pass %: 0.00%
- Response Pass %: 14.29%

Below the summary, detailed test information is listed:

Test Name	Test Agentforce v1
Created By	HOC Trailblazer
Created On	June 12, 2025 at 06:41 PM
Description	Test cases for Agentforce to verify account summaries and details
Last Run	June 12, 2025 at 06:41 PM
Agent	Einstein Copilot - v1

At the bottom, there is a 'Test Results' section with a dropdown menu labeled 'All Results'.

Way to go! You created your first test in the Agentforce Testing Center. You also gained an insight into the working of the test file and test parameters. In the next unit, you take a look at using AI to generate your tests.

Make sure to click **Check Challenge to Earn 500 Points** before moving on to the next unit.

Use AI to Generate Tests

Learning Objectives

After completing this unit, you'll be able to:

- Use AI to generate test cases.
- Execute batch testing in the Agentforce Testing Center.

Let AI Generate Your Tests

Manually creating a diverse and scalable set of test scenarios is time-consuming and complex. The Agentforce Testing Center has the solution. You can now use AI to effortlessly generate hundreds of synthetic interactions based on the agent's topics and actions to be used as test cases. This helps ensure that your agents handle various customer interactions accurately.

Then you run those tests automatically in parallel to see what topics and actions the agent chooses. From there, you can iterate by adjusting agent instructions and guardrails as needed—saving time that would have been lost on manually testing many different variations of a conversation. The result is a faster time to testing and a faster time to a more trusted agent that you feel confident deploying.

A good-quality test case dataset has three quality attributes.

- **Volume:** A sufficient number of test cases to ensure comprehensive coverage of different scenarios and edge cases.
- **Diversity:** A wide range of inputs, contexts, and variations to test the AI agent's adaptability across real-world use cases.
- **Quality:** Well-defined, accurate, and relevant test cases aligned with the AI agent's objectives.

To complete this unit, you'll need to use the special Developer Edition org you created in the last unit. When you're finished following the step-by-step instructions, click **Check Challenge to Earn 500 Points** at the bottom of the page.

Batch Testing

There are a couple of ways to get to the Agentforce Testing Center. You already used the direct way in the last unit. There's also a **Batch Test** button right in Agentforce Builder that takes you right to the Agentforce Testing Center. Let's give it a go.



Important!

- Running tests consumes requests and credits. See [Considerations for Testing Center](#).

- Testing agents can modify CRM data. To avoid issues, be sure to use the Agentforce Testing Center only in your sandbox environment.
1. From Setup, in the Quick Find box, search for and select **Agentforce Agents**.
 2. Click **Einstein Copilot or Agentforce (Default)**.
 3. Click **Open in Builder**.
 4. Click **Batch Test**. This opens up the Agentforce Testing Center in a new tab with the New Test window open and the Einstein Copilot - v1 or Agentforce (Default) v1 already selected.
 5. For Test Name, enter Generated Test Agentforce v1Copy.
 6. For Description, enter Test cases for Agentforce to verify account summaries and detailsCopy.
 7. Click **Next**.
 8. Click **Next**.
 9. Select **Generate test cases based on topics and actions**.
 10. For Number of test cases, leave it at 20.
 11. For Test Case Description, enter Generate realistic inquiries that customers might ask about their user account, orders, and other general questions about productsCopy. This is also where you can define the number of these test cases that are positive and negative to create diversity in your test cases.
 12. For Select the topics for your test cases, leave them all checked. Note that you can select different topics for the different tests you create.

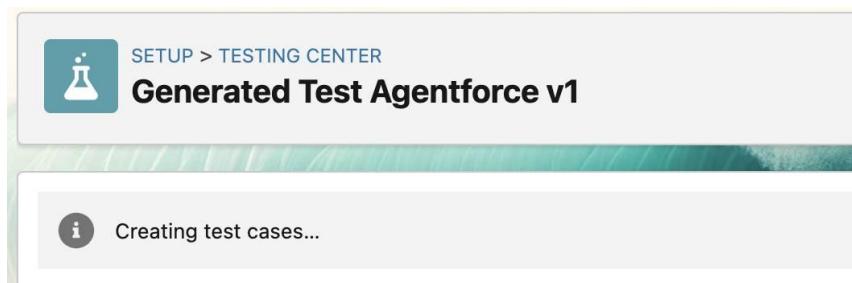
13. Click **Next**.

New Test

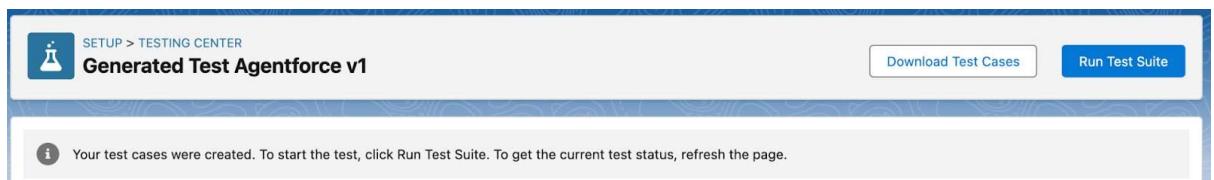
Basic Information	Test Data Upload or generate test cases. <input type="radio"/> Upload test cases <input checked="" type="radio"/> Generate test cases based on topics and actions <input type="radio"/> Generate test cases based on the knowledge available to the agent
Test Conditions	* Number of Test Cases 20
Test Data	Test Case Description Describe the test cases and provide some examples...
Evaluations	* Select the topics for your test cases <input checked="" type="checkbox"/> Topic Name <input checked="" type="checkbox"/> MigrationDefaultTopic

Cancel Next

14. Click **Generate Test Cases**.



15. Wait for the test to be generated. You may have to refresh your browser as it may take a bit to generate the tests. Click **Run Test Suite**. You might have to refresh the page.



16. Click  to refresh the results.

Utterance ↓	Run Status	Expected Topic	Actual Topic
Summarize account Acme	Completed	OOTBSingleRecordSummary	MigrationDefaultTopic

Once the tests are created, you can download them to make sure the agent is doing what you want it to do. You can also fine-tune the agent as needed. In the next unit, you take a closer look at the test results and use Agentforce Builder to troubleshoot a failed test.

Make sure to click **Check Challenge to Earn 500 Points** before moving on to the next unit.

View Test Results

Learning Objectives

After completing this unit, you'll be able to:

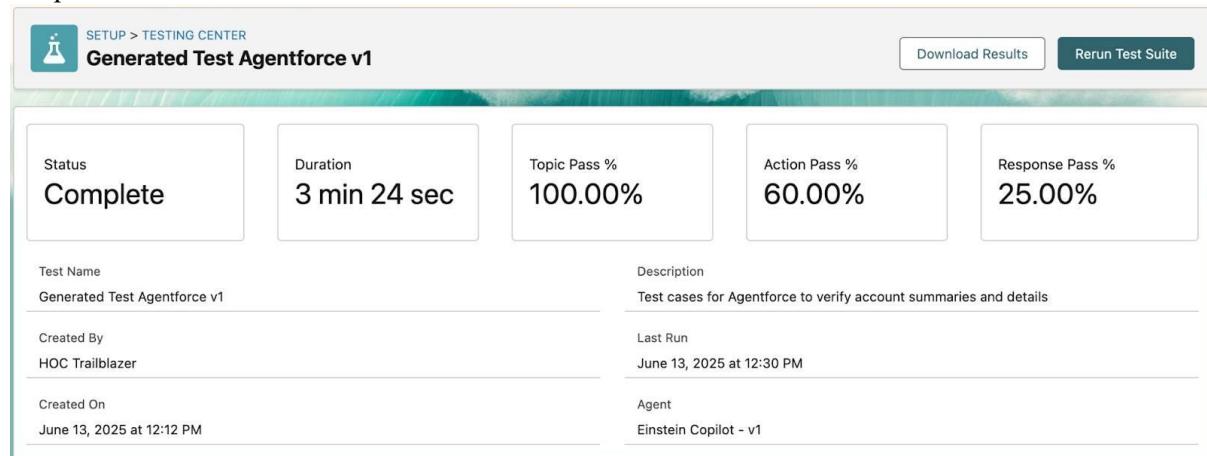
- Describe Agentforce Testing Center test results.
- Troubleshoot failed tests in Agentforce Builder.

Working with Test Results

Once the tests are completed, you can view the results and see what worked well and what didn't work as well as you hoped. Take a look at the results for the test you ran in the last unit.

1. From Setup, in the Quick Find box, search for and select **Testing Center**.
2. Select the Test Name **Generated Test Agentforce v1**.

At the top of the page you see the following: Status, Duration, Topic Pass %, Action Pass %, and Response Pass %.



The screenshot shows the results of a test named "Generated Test Agentforce v1". At the top, there are five summary statistics: Status (Complete), Duration (3 min 24 sec), Topic Pass % (100.00%), Action Pass % (60.00%), and Response Pass % (25.00%). Below these, detailed information is provided:

- Description:** Test cases for Agentforce to verify account summaries and details.
- Last Run:** June 13, 2025 at 12:30 PM
- Agent:** Einstein Copilot - v1

On the left side, there are sections for Test Name (Generated Test Agentforce v1), Created By (HOC Trailblazer), and Created On (June 13, 2025 at 12:12 PM). On the right side, there are sections for Description, Last Run, and Agent.

This section gives you a quick overview of how the different parts of the tests are completed. You can choose to download or rerun the tests. Rerunning the tests is helpful when you've made changes to the agent and need to see if modifications cause the current tests to fail. You can then add new tests to the

CSV test file to cover the updates made to the agent. Finally, you can create a new test with the updated test file and run the new tests.

The next section on the page is Test Results. Here, you can use a dropdown to select one of the three options: All Results (the default), Passed Results, and Failed Results.

Test Results All Results ▾						
20 Items • Sorted by Utterance • Filter by All Results • Updated 0 minutes ago						Search results...
Utterance ↓	Run Status	Expected Topic	Actual Topic	Topic Test Result	Expected Actions	
Please update the email address for Ilsa Galgey to new_email@example.com.	Completed	MigrationDefaultTopic	MigrationDefaultTopic	Pass	[!IdentifyRecordByName, 'ExtractFieldsAndValuesFromUserInput', 'UpdateRecordFields']	ⓘ
Can you give me a summary of the Dickensen Mobile Generators opportunity?	Completed	MigrationDefaultTopic	MigrationDefaultTopic	Pass	[!IdentifyRecordByName, 'SummarizeRecord']	ⓘ

The Test Results section displays several columns. Let's look at the first line in more detail.

Utterance	Please update the email address for Ilsa Galgey to new_email@example.com.
Run Status	Completed
Expected Topic	MigrationDefaultTopic
Actual Topic	MigrationDefaultTopic
Topic Test Results	Pass
Expected Actions	[!IdentifyRecordByName, 'ExtractFieldsAndValuesFromUserInput', 'UpdateRecordFields']
Actual Actions	[!IdentifyRecordByName, 'ExtractFieldsAndValuesFromUserInput']
Action Test Result	Fail
Expected Response	The email address for Ilsa Galgey has been updated to new_email@example.com.
Actual Outcome	Can I proceed with updating Ilsa Galgey's email address to new_email@example.com?
Outcome Test Result	Pass

You probably recognize Utterance, Expected Topic, Expected Actions, and Expected Response from the test file. The new information are the actual responses and results from running the tests.

- **Actual Topic** shows which topic was chosen for the utterance.
- **Topic Test Result** shows Pass or Fail if the actual topic matches the expected topic.
- **Actual Actions** shows which actions the agent ran from the topic.
- **Action Test Result** shows Pass or Fail if the actual action matches the expected actions.
- **Actual Outcome** shows the actual response from the agent.
- **Outcome Test Result** shows Pass or Fail if the actual outcome matches the expected response.

It looks like the first test had a fail for Actual Actions. The Expected Actions has IdentifyRecordByName and QueryRecords and the Actual Actions has only QueryRecords. You use the Agentforce Builder for the Agentforce (Default) agent to troubleshoot the utterance of this test to get a better idea of what the agent is doing.

Troubleshoot with Agentforce Builder

Switch to the Agentforce Builder and manually test the utterance in the Conversation Preview. Using Agentforce Builder in this way is a form of manual testing and lets you dig into the utterance to see the topics, actions, and responses the agent chooses. Then try changing the utterance to test getting different results.

1. From Setup, in the Quick Find box, search for and select **Agentforce Agents**.
2. Select the drop down for the Agent Name you want to open and select **Open in Builder**. We'll continue to look at the Einstein Copilot or Agentforce (Default) agent.

Agent Name	Type	Description	Created By	Active	Last Modified	
> Coral Cloud Agent	Digital Channel	This is the Coral Cloud Agent, our Einstein Servi...	HOC Trailblazer	Jun 12, 2023	Jun 12, 2023	Edit
> Coral Cloud Experience Agent	Service Agent	This is the Coral Cloud Agent that helps custom...	HOC Trailblazer	Jun 12, 2023	Jun 12, 2023	Delete
> Einstein Copilot	Employee	An AI assistant for in-org business tasks.	HOC Trailblazer	Jun 12, 2023	Jun 12, 2023	Open in Builder

3. In the Conversation Preview, enter the utterance Please update the email address for Ilsa Galgey to new_email@example.com. Copy and click **Enter**.

The Agentforce Builder center screen shows the results, including Session Start, User Prompt, Select Topic, and so on.



You also see Select Action, which shows the Identify Record by Name (IdentifyRecordByName) action was called.

The screenshot shows the 'Select Action' screen of the Agentforce Testing Center. At the top, there is a 'Select Action' button with a search icon and a timer indicating 2.09 sec. Below this, the action name 'Identify Record by Name (*IdentifyRecordByName*)' is displayed with a camera icon. A description follows: 'Searches for Salesforce CRM records by name and returns a list of matching Salesforce CRM record IDs.' The 'Input' section contains a JSON object: { "recordName": "Ilsa Galgey" }. The 'Output' section shows a partial JSON object: { "searchResults": [{ "sObjectInfo": { "apiName": "Contact" } }] }. The entire screenshot is framed by a light gray border.

The Expected Action test criteria was expecting three actions. The failure is due to the wrong expectation.

At this point there are a few options.

- The first one is to change the test Expected Action to just have the IdentifyRecordByName and ExtractFieldsAndValuesFromUserInput. But there is also the option to change the test Utterance if it was supposed to invoke both actions.
- Changing the utterance and checking the Actual Actions in the testing results allows you to reiterate over the tests, make changes, and verify that the agent is doing what is expected. The more tests and different test criteria you have, the higher the confidence and trust in the agent there is.
- Or this could be used as a negative test. Just add another test with the positive test criteria so that the criteria is covered.

Agentforce Testing Center Benefits

Testing is an essential part of building Agentforce agents. By creating and maintaining detailed positive and negative test criteria, you're building and maintaining the confidence and trust that your Agentforce agents are bringing to your users and customers.

The Agentforce Testing Center allows for repeated test runs that give you the ability to quickly determine if changes to your agents are having a negative impact on outcomes. You can even create the testing criteria first, run the tests, and then build the new functionality into the agents to get those tests to pass. This is known as test-driven development (TDD) in the coding community, and is a great way to build out new functionality with agents.

You now have a better idea of what the Agentforce Testing Center can do for you and the different ways you can work with test criteria to ensure your new agents are a sure way to interact with your users and customers. Now, go forth and create some tests!

Resources

- [Salesforce Help: Batch Test with Agentforce Testing Center](#)

Quiz

To complete this unit, you need to answer all the quiz questions correctly.

+100 Points

1

Which part of the test results does Actual Actions represent?

A

The expected action

B

Pass or fail if the actual action matched

C

The actions the agent ran

D

The topic the agent chose

2

Agentforce Builder allows for conducting which type of testing?

A

Manual testing

B

Single action testing

C

Batch testing

D

Single topic testing

Learn the Basics of Large Language Models

Learning Objectives

After completing this unit, you'll be able to:

- Describe a large language model (LLM).
- Explain how LLMs are trained.
- Achieve a better understanding of LLM fine-tuning.



As of October 14, 2025, Data Cloud has been rebranded to Data 360. During this transition, you may see references to Data Cloud in our application and documentation. While the name is new, the functionality and content remains unchanged.

Trailcast

If you'd like to listen to an audio recording of this module, please use the player below. When you're finished listening to this recording, remember to come back to each unit, check out the resources, and complete the associated assessments.

Before You Start

Large language models rely on natural language processing (NLP) and machine learning to understand and generate humanlike text. If you haven't already earned the [Natural Language Processing Basics](#) badge, we recommend that you earn that badge before you start this one.

What's a Large Language Model?

Imagine you have a supersmart digital assistant that has read vast amounts of text, including text from books, articles, websites, and other written content up to today. However, it doesn't "contain" entire books in the way that a library does. Instead, it can process patterns, draw connections, generate creative insights, or perform complex calculations from the textual data it is trained on.

You can ask this digital assistant any question, and it will try to give you an answer based on what it has "read." It doesn't really "understand" like people do, but it's really good at remembering and connecting information.

Large Language Models (LLMs) are like that assistant. LLMs are advanced computer models designed to understand and generate human-like text. They're trained on vast amounts of text data to learn patterns, language structures, and relationships between words and sentences.

How Do Large Language Models Work?

At their core, LLMs like ChatGPT, Gemini, or Claude predict one token (for example, a word or character) at a time, building a sequence from start to finish. Given a request, they try to predict the next token, and the next, and the next, and so on.

Predictions made by LLMs refer to their ability to generate or complete text based on patterns they've seen during training, performing impressive feats of pattern recognition over vast amounts of text. They can generate coherent and contextually relevant content across a wide range of topics.

The large part of large language models refers to the size and complexity of these models. They use significant computational resources, such as powerful servers with multiple processors and a lot of memory. These resources let the model handle and process huge amounts of data, which improves its ability to understand and generate high-quality text.

LLMs vary by size, but they typically contain billions of parameters. Parameters are the factors that the model learns during its training process, building the model's understanding of language. The more parameters, the more capacity the model has to learn and capture intricate patterns in the data, improving its ability to produce human-like text.

To give you an idea of how many parameters LLMs use, earlier versions of the GPT (generative pre-trained transformer) models, like OpenAI's GPT-3, have around 175 billion parameters. These models are considered quite large and have significantly advanced the capabilities of language processing. OpenAI's newer model, GPT-4 is estimated to have 1.76 trillion parameters.

These numbers are indeed impressive, but the sheer size of these models is also accompanied by challenges like the computational resources required to train them, their environmental impact, potential biases, and more.

Large language models are like incredibly knowledgeable virtual assistants that can help with a wide range of language-related tasks. They can assist in writing, provide information, offer creative suggestions, and even engage in conversation. The model creator's goal is to assist and make interactions with technology more natural and humanlike. However, users should be aware of their limitations and use them as a tool rather than an infallible source of truth.

What Is LLM Training?

Training an LLM is like teaching a robot how to understand and use human language. And how do you train a robot to understand and use human language? Here's one way you could do it.

1. **Gather books and articles.** Imagine collecting a massive pile of books, articles, and other writings to teach the robot.
2. **Practice reading.** You make the robot read a sentence, and then ask it to guess the next word. At first, it might guess randomly since it's still learning.
3. **Check answers.** After the robot makes a guess, you show it the correct word from the actual text. If the robot's guess is wrong, you give it feedback, like saying, "Oops! That's not right."
4. **Repeat.** You keep doing this "guess and check" over and over, with tons of sentences. The robot starts getting better at guessing the next word as it reads more.
5. **Test.** Occasionally, you test the robot with sentences it hasn't seen before to see if it's really learning or just memorizing.
6. **Specialize.** If you want the robot to be especially good at, say, medical language, you might give it extra lessons with medical books.
7. **Graduate.** Once the robot gets really good at understanding and generating text, say, "Great job!" and let it help people with various language tasks.

And that's it! Training is like a mix of reading practice, quizzes, and special lessons until the robot becomes a language expert. The same basic idea applies to LLMs.

How Does Fine-Tuning Work?

Fine-tuning is the process of further training a pre-trained model on a new dataset that is smaller and more specific than the original training dataset.

Imagine you've taught a robot to cook dishes from all over the world using the world's biggest cookbook. That's the basic training. Now, let's say you want the robot to specialize in making just Italian dishes. You'd then give it a smaller, detailed Italian cookbook and have it practice those recipes. This specialized practice is like fine-tuning.

Fine-tuning is like taking a robot (or model) that knows a little bit about a lot of things, and then training it further on a specific topic until it becomes an expert in that area.

Why Is Fine-Tuning Important?

- **Transfer learning:** Pre-trained models have already learned a lot of generic features from their extensive training datasets. Fine-tuning allows these models to transfer that general knowledge to specific tasks with relatively small datasets.

- **Efficiency:** Training a deep learning model from scratch requires a lot of data and computational resources. With fine-tuning, you're starting with a model that already knows a lot, so you can achieve good performance with less data and time.
- **Better Performance:** Models fine-tuned on specific tasks often outperform models trained from scratch on those tasks, as they benefit from the broader knowledge captured during their initial training.

What's in a Version?

For each version, the underlying architecture might remain similar, but the scale, training data, or certain parameters can change. Each new version aims to improve upon the weaknesses of the previous one, handle a broader range of tasks, or reduce biases and errors.

Here's a simplified explanation.

Version 1 (for example, OpenAI's GPT-1 or Google's BERT-base)

- *The beginning:* The first release of the model. It works well, but it's like the first draft of a novel—there's room for improvement.
- *Size and data:* Uses a certain amount of data and has a particular number of parameters (like the “brain cells” of the model).

Version 2 (OpenAI's GPT-2)

- *Improvements:* Based on the learnings from the first version, adjustments are made. It's like editing your novel based on feedback.
- *Size and data:* Often bigger with more parameters. Might be trained on more diverse or larger datasets.

Version 3 (OpenAI's GPT-4)

- *Even better:* Incorporates more feedback, research, and technological advancements.
- *Size and data:* Much larger. For instance, GPT-4 has 1.76 trillion parameters, making it much more capable but also requiring more resources.

Fine-tuned versions:

- After the main versions are released, sometimes there are specialized versions fine-tuned for specific tasks. It's like taking a general novel and adapting it into a mystery, romance, or sci-fi version.

Other iterations:

- Models like BERT have variations (RoBERTa, DistilBERT, and so on) that are essentially different “versions” with tweaks in training strategy or architecture.
- Models like Claude have variations like Haiku, Sonnet, and Opus that are designed to optimize different levels of performance, capabilities, and reasoning skills.

LLM versions are like consecutive editions of a book series, with each new release aiming to be a more refined, expansive, and captivating read.

Next, let's look at how LLMs are being used by Salesforce.

Resources

- [Trailhead: Natural Language Processing Basics](#)
- [Trailhead: Model Fine-Tuning](#)
- [Trailhead: Retrieval Augmented Generation: Quick Look](#)
- [Trailhead: Generative AI Basics](#)
- [Salesforce News & Insights: Generative AI: 5 Guidelines for Responsible Development](#)

Quiz

To complete this unit, you need to answer all the quiz questions correctly.

+100 Points

1

What are the variables that the model learns during its training process?

A

Versions

B

Placeholders

C

Books

D

Parameters

2

Which is a benefit of increasing parameters used in large language models?

A

To reduce the computing resources required for training the model

B

To improve the model's ability to generate human-like text

C

To allow less complexity in the model

D

To increase biases and errors in the model

Learn How Salesforce Uses Large Language Models

Learning Objectives

After completing this unit, you'll be able to:

- Explain how Salesforce brings trust to LLMs
- Choose the correct LLM option for your business.
- Describe the limitations of the available LLM options.

Trailcast

If you'd like to listen to an audio recording of this module, please use the player below. When you're finished listening to this recording, remember to come back to each unit, check out the resources, and complete the associated assessments.

Leading with Trust

Trust is the number one value at Salesforce. So it makes sense that Salesforce uses Large Language Models (LLMs) in a secure and trusted way. The key to maintaining this trust is through the [Einstein Trust Layer](#). The Einstein Trust Layer ensures generative AI is secure by using data and privacy controls that are seamlessly integrated into the Salesforce end-user experience. These controls let Einstein deliver AI that securely uses retrieval augmented generation (RAG) to ground responses with your customer and company data, without introducing potential security risks. In its simplest form, the Einstein Trust Layer is a sequence of gateways and retrieval mechanisms that work together to enable trusted and open generative AI.

Trusted Salesforce Agents

Agentforce agents use leading LLMs through the Einstein Trust Layer by using RAG to build secure prompts with Salesforce and Data 360 data. This creates a rich and secure environment to use AI agents capable of supporting employees and customers. These agents don't just offer suggestions—they can complete tasks independently. For example, they can handle customer inquiries, troubleshoot issues, and even make sales recommendations without human intervention. All while using the Trust Layer to secure the data and provide confident responses.

Choose the Best Large Language Model

All Agentforce reasoning engine calls use OpenAI GPT-4o, and in some cases Azure OpenAI GPT-4o, as the default model. However, you can choose from other models that support your business needs. It's important to note that ensuring you have the right model for the right task will help you get started with generative AI faster and achieve the results you expect. Salesforce provides deployment capabilities for many different LLMs while also helping companies maintain their data privacy, security, residency, and compliance goals.

Many businesses use different LLM's to handle specific types of use cases, like coding, sentiment analysis, or content generation. When choosing a model for a use case, keep the model capabilities, cost, response quality, and speed in mind. You can also choose models that are geo-aware. These models automatically route LLM requests to a nearby data center based on where Data 360 is provisioned for your org. This gives you greater control over data residency and reduces latency.

The Right LLM for the Right Task



Shared Trust

Data retained in Salesforce with joint moderation



Salesforce Hosted

Globally on Hyperforce



Bring Your Own Model

Your model, your infrastructure



Use Salesforce-Managed LLMs

Salesforce-managed LLMs are a great way to access LLMs across the internet and get started using generative AI quickly. You can customize your AI implementation with different Salesforce-managed models using the Models API or Prompt Builder. Salesforce offers a variety of models that are enabled by default to help speed up the configuration process.

For a list of current Salesforce-managed models, visit the [Large Language Model Support](#) help documentation.

Use Salesforce Hosted Third-Party LLMs

You can also host models inside of Salesforce. As part of Salesforce's commitment to an open ecosystem, Einstein is designed to host LLMs from Amazon, Anthropic, Cohere, and others—entirely within the Salesforce infrastructure. Einstein will help maintain customer prompts and responses in the Salesforce infrastructure. In addition, Salesforce and OpenAI have established a shared trust partnership to securely deliver content through the Einstein Trust Layer.

Bring Your Own Large Language Model (BYOLLM)

If you're already investing in your own LLM, you can connect it to Salesforce to use within custom Prompt Builder templates. You can benefit from Einstein even if you've trained your own domain-specific models outside of Salesforce while storing data on your own infrastructure. When you execute a prompt through an external LLM you've connected, it works just the same as an internally connected LLM and routes the request through the LLM Gateway and the Einstein Trust Layer before sharing content with your users.

The BYOLLM options are changing and fast! Keep an eye on the resources for new updates.

Resources

- [Trailhead: The Einstein Trust Layer](#)
- [Trailhead: Large Language Model Data Masking in the Einstein Trust Layer](#)
- [Salesforce Help: Einstein Trust Layer: Designed for Trust](#)
- [Salesforce Help: Bring Your Own Model](#)

- [Trailhead: Prepare Your Data for AI](#)
- [Salesforce: What are LLMs \(Large Language Models\)?](#)
- [News and Insights: Salesforce Launches BYOM to Make It Easy for Businesses to Use Proprietary Data to Build and Deploy AI Models](#)
- [Developers' Blog: Bring Your Own AI Models to Data Cloud](#)

Quiz

To complete this unit, you need to answer all the quiz questions correctly.

+100 Points

1

True or false? You may need to use more than one LLM to meet your organization's use cases.

A

True

B

False

2

What is a benefit of using a geo-aware model?

A

Reduced control over data residency.

B

Greater latency.

C

Greater control over data residency.

D

It skips the Einstein Trust Layer.

Second attempt earns 50 points. Three or more earns 25 points.

Autonomous Agents:

[Get to Know Autonomous Agents](#)

~10 mins

[Incomplete](#)

[Establish Trust with Autonomous Agents](#)

~5 mins

Incomplete

Transform Your Business with Autonomous Agents

~10 mins

Get to Know Autonomous Agents

Learning Objectives

After completing this unit, you'll be able to:

- Define what an autonomous agent is and how it works.
- List some real-world examples of autonomous agents in different industries.

Trailcast

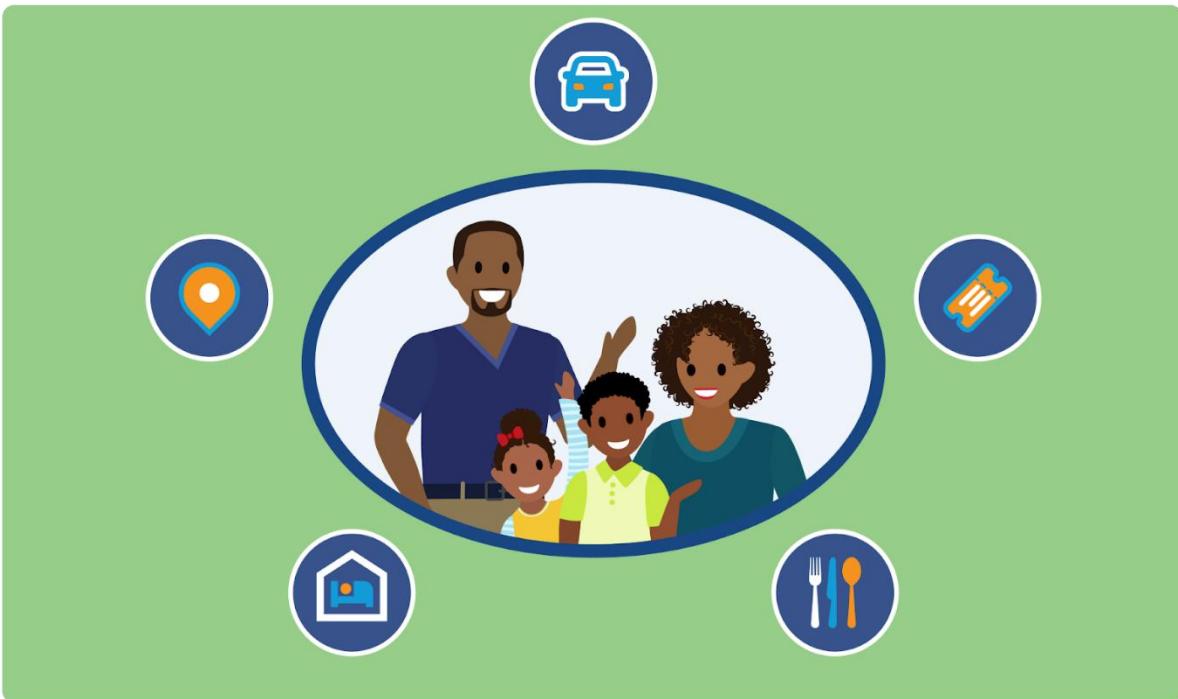
If you'd like to listen to an audio recording of this module, please use the player below. When you're finished listening to this recording, remember to come back to each unit, check out the resources, and complete the associated assessments.

The Power of Autonomous Agents

The Rodriguez family is eager for a stress-free vacation. Luckily, they discover Coral Cloud Resorts, which has an autonomous AI assistant that helps them set up every aspect of their trip.

They use the resort's AI-powered concierge agent to seamlessly book flights, secure a hotel, arrange transportation, and even select the best Coral Cloud experiences and dining reservations based on their preferences. The agent customizes an itinerary to suit each family member's interests and provides a detailed packing list with helpful reminders.

With the agent managing all the logistics and curating what's sure to be a magical experience, the Rodriguez family arrives at Coral Cloud Resorts relaxed and ready to create unforgettable memories.



How Do Autonomous Agents Work?

Autonomous agents like Coral Cloud's understand and respond to requests, and then act without human intervention. Give the agent a goal, and it generates tasks for itself, completes them, and moves on to the next one until the goal is achieved. Unlike traditional chatbots that follow predefined rules, autonomous agents operate in dynamic environments, making them perfect for complex tasks in customer service, marketing, commerce, sales, and more.

While autonomous agents don't need human help to complete their tasks, they still need you to describe the ideal goals and main objectives you want to achieve. Once in action, the agent can save your business significant time and resources and allow you to focus on improving the overall customer experience and driving growth—just like at Coral Cloud Resorts.

You might think setting up an agent takes a lot of time, but autonomous agents require less time to build compared with traditional bots. And they can do more when you set them up with the right data and actions. Let's take a look at the key components that make them effective.

Data

Data is the foundation of an autonomous agent's functionality. It's what enables an agent to make informed decisions and execute tasks autonomously. At Coral Cloud Resorts, the concierge agent analyzes opt-in data about the Rodriguez family, including family member profiles, past travel history, and more, to gain a deeper understanding of their preferences. With these insights, the agent can personalize every aspect of their trip and provide a seamless and enjoyable vacation.

Decision-Making

When an autonomous agent analyzes data, it uses advanced decision-making algorithms to prioritize and execute tasks efficiently. For the concierge agent at Coral Cloud Resorts, that means evaluating various options and scenarios to ensure that every decision aligns with the Rodriguez family's preferences and goals.

Action Execution

After making data-driven decisions, the agent seamlessly transitions to executing the planned actions. For the concierge agent, those planned actions might be autonomously reserving hotel rooms, arranging transportation, and more. This not only enhances the customer experience but also allows the business to save an immense amount of time and focus on other critical tasks that provide even better customer service.

Learning and Adaptation

Over time, the agent continuously learns from each interaction and adapts to improve future performance. It analyzes feedback and outcomes to refine its algorithms and decision-making processes to better meet the customer's needs.

In addition, autonomous agents are adaptable to various situations and can provide data-driven solutions to simplify and improve efficiency in a wide range of areas. Let's take a look at that next.

Autonomous Agents in Action

Autonomous agents are becoming increasingly universal and offer support in a wide range of fields. Here are some industries where they bring significant benefits and support to CRM platforms.

Healthcare

An autonomous agent can engage with patients, providers, and payers to resolve inquiries, provide summaries, and take action. For example, a patient services agent can answer simple patient questions, help schedule appointments with the best physician, review coverage benefits, generate medical history summaries, and approve care requests.

Example: A patient needs to schedule a follow-up appointment with a specialist. They use the healthcare provider's agent to request the appointment. The autonomous agent checks the availability of the best-suited specialist, confirms the patient's insurance coverage, and schedules the appointment. The agent also generates a summary of the patient's medical history and sends it to the specialist in advance. This streamlined process ensures that the patient receives timely care and reduces the administrative burden on healthcare staff.

Financial Services

Banks can autonomously manage transaction disputes through various channels such as the banking app, SMS, website, or phone. Prebuilt service flows allow agents to file complaints, meet regulatory reporting requirements, verify transaction history, alert merchants, and even issue provisional credits or new cards. These autonomous agents only escalate to a human for final authorizations, saving time and allowing human experts to focus on more complex interactions.

Example: A customer notices a fraudulent transaction on their bank statement and reports it through the banking app. The autonomous agent verifies the transaction history, files the complaint, and issues a provisional credit to the customer's account. The agent also alerts the merchant and schedules a follow-up with a human representative for final authorization. This process, which used to take several days, is now completed within hours, significantly improving customer satisfaction and reducing the workload on human service reps.

Insurance

Insurance companies can autonomously update coverage, extend better pricing to qualified policyholders, update beneficiaries, schedule and deploy claims adjusters, and even issue claims checks or policy renewals—all without human intervention. Wealth advisors reported that 67% of their daily work is non-value-added administrative work. Autonomous agents can reduce this by

planning, scheduling, and summarizing client meetings, drafting client communications, and ensuring compliance by routing communications to the proper licensed supervisors.

Example: An insurance policyholder wants to update their beneficiary information. They use the insurance company's mobile app to make the change. The autonomous agent verifies the policyholder's identity, updates the beneficiary's information, and sends a confirmation email. The agent also ensures that the change is compliant with regulatory requirements by routing the communication to a licensed supervisor for a final review. This process, which previously required a phone call and manual processing, is now completed in seconds, freeing up the policyholder's time and reducing administrative workload.

Retail

Autonomous agents can share campaign insights, proactively manage customer outreach, and resolve cases for retailers. A personal shopper autonomous agent acts like a digital concierge for online shoppers, using generative AI to help customers on ecommerce sites, chat, or messaging apps like WhatsApp. While basic chatbots only solve predefined questions, autonomous AI agents learn from shoppers' behavior and preferences and can provide natural language searches, conversational responses, and quick cart additions for instant checkout.

Example: A customer is shopping for a new pair of shoes on an ecommerce site. The personal shopper autonomous agent, integrated into the chat feature, engages with the customer and analyzes their past purchases and preferences. Using this information, the agent recommends a pair of shoes that perfectly match the customer's style and size. The customer can then add the shoes to their cart and complete the purchase with a single click. To further enhance the experience, the agent follows up with a personalized thank-you message and suggests complementary accessories. This thoughtful approach not only delights the customer but also increases the likelihood of repeat business.



In this unit, you learned that autonomous agents are like intelligent digital assistants that can operate independently without direct human supervision. They can reason, plan, and take action to achieve specific tasks or goals once you equip them with the relevant data and the knowledge and experience

of human experts. Next, learn how to provide a safe and trusted autonomous agent experience for your customers.

Resources

- [Salesforce Blog: What are Autonomous Agents? A Complete Guide](#)

Quiz

To complete this unit, you need to answer all the quiz questions correctly.

+100 Points

1

What is the primary function of an autonomous agent?

A

It replaces human employees entirely.

B

It saves time and resources and enhances the customer experience.

C

It handles all customer service inquiries.

D

It performs only tasks that are too complex for human employees.

2

Which of these features distinguish autonomous agents from chatbots?

A

Autonomous agents follow predefined rules.

B

Autonomous agents take longer to build than chatbots.

C

Autonomous agents need human help to complete tasks.

D

Autonomous agents can execute tasks independently.

Second attempt earns 50 points. Three or more earns 25 points.

Establish Trust with Autonomous Agents

Learning Objectives

After completing this unit, you'll be able to:

- Explain why it's important to implement safety precautions with autonomous agents.
- List seven guardrails that keep autonomous agents safe and trusted.

Trailcast

If you'd like to listen to an audio recording of this module, please use the player below. When you're finished listening to this recording, remember to come back to each unit, check out the resources, and complete the associated assessments.

Make Safety Your #1 Priority

Implementing autonomous agents into your workflow brings great benefits, but it's crucial to ensure that they operate safely and maintain customer trust. Let's explore a common example.

Today, there's increasing demand for medical services and patient support. Providing support when it's most needed makes a significant difference in patient outcomes and satisfaction. Autonomous agents can help, but they must be safe and trusted when managing patient data or providing medical advice.

For example, an autonomous agent that helps patients schedule appointments or follow up on prescriptions must keep personal health information (PHI) confidential and comply with HIPAA regulations. If the agent recommends that a patient should be seen by a doctor based on their symptoms, it must cross-check against up-to-date medical guidelines to ensure an accurate assessment of the severity and urgency of the condition.

Also, the agent must clearly communicate its limitations so that patients understand that it's not a replacement for a doctor's consultation. Trust and safety are critical in this environment to ensure that the agent provides accurate, secure, and reliable assistance in managing healthcare needs.

Guardrails for Safe and Trusted Autonomous Agents

No matter what industry you're in, it's important to take safety precautions when using autonomous agents for your business. Here are some key guardrails to consider when you build and integrate autonomous agents.

Define Clear Boundaries

Set clear boundaries for what your autonomous agents can and can't do. For example, you might limit an agent's ability to make financial transactions above a certain amount or to access sensitive personal information without explicit permission. Clear boundaries help prevent misuse and ensure that agents stay within safe and ethical limits.

Implement Robust Security Measures

Autonomous agents handle a lot of customer data, so security is paramount. Use encryption, secure data storage, access controls, and regular security audits to protect customer information. Ensure that your agents comply with data protection regulations, such as GDPR or CCPA, to maintain customer trust and avoid legal issues.

Monitor and Audit

Regularly monitor the performance of your autonomous agents, and audit your agent's actions. This helps you catch any errors or inappropriate behavior early and make necessary adjustments.

Monitoring also allows you to gather feedback from users and continuously improve the agents' performance.

Integrate Human Oversight

While autonomous agents handle many tasks independently, it's important to have human oversight for more complex or sensitive interactions. Create clear guidelines for when and how human representatives should step in to assist. This provides a safety net and ensures that customers receive the best possible service.

Ensure Transparency

Be transparent with your customers about how your organization uses autonomous agents. Inform them when they are interacting with an autonomous agent, and provide options to speak with a human representative if needed. Transparency builds trust, helps customers feel more comfortable with AI interactions, and ensures compliance with [bots disclosure regulations](#).

Test Thoroughly

Before deploying autonomous agents, test them thoroughly to identify and address any potential issues. Use a variety of scenarios and edge cases to ensure that agents can handle unexpected situations gracefully. Testing helps you catch bugs and ensure that agents perform as expected.

Continuous Learning and Improvement

Autonomous agents should continuously learn and improve. However, this learning process must be controlled and monitored to make sure that the agents don't develop harmful behaviors. Use reinforcement learning with clear positive and negative feedback to guide the agents' development.

Resources

- [Trailhead: Trusted Agentic AI](#)
- [Salesforce Help: Einstein Generative AI and Trust](#)

Quiz

To complete this unit, you need to answer all the quiz questions correctly.

+100 Points

1

Which of the following is an important guardrail to consider when building and integrating autonomous agents?

A

After successfully testing your agent, keep it from evolving any further.

B

Provide human oversight for more complex or sensitive interactions.

C

Limit your agent's ability to communicate directly with customers.

D

Never allow your agent to handle financial transactions.

2

When you deploy an autonomous agent to interact with customers, it's important to be transparent about what?

A

How and when customers are interacting with an autonomous agent

B

The agent's name

C

The large language model the agent uses

D

The agent's testing mechanism

Second attempt earns 50 points. Three or more earns 25 points.

Transform Your Business with Autonomous Agents

Learning Objectives

After completing this unit, you'll be able to:

- Explain how autonomous agents can transform business operations.
- Describe what the Agentforce platform is.
- List four best practices for implementing autonomous agents.

Trailcast

If you'd like to listen to an audio recording of this module, please use the player below. When you're finished listening to this recording, remember to come back to each unit, check out the resources, and complete the associated assessments.

How Autonomous Agents Help Your Business

Earlier, you explored how a wide range of industries can seamlessly integrate and tailor autonomous agents to different use cases. You learned how they can handle a variety of tasks and situations across different fields because they are built to manage complex challenges and to consider previous patterns and insights to refine their solutions.

Autonomous agents can be the key differentiator for boosting almost any business or workflow. They're always on, ready to chat with customers across all channels. Plus, they resolve issues super fast by sticking to the facts. These agents are transformative in many ways.

Still not sure how they could impact your organization? Here are some common use cases where autonomous agents can help.

- **Customer support:** They can handle a wide range of customer queries, from simple FAQs to more complex issues that do not require human oversight. This frees up your human representatives to focus on the trickier stuff that needs a personal touch.
- **Order management:** They can process orders, track shipments, handle returns, and even send automated updates to keep customers in the loop.
- **Lead generation:** They can engage with potential customers, gather contact information, and qualify leads. This helps you capture more leads and convert them into sales.

- **Personalized recommendations:** By analyzing customer data, they can offer personalized product or service recommendations, enhancing the customer experience and boosting sales.
- **Scheduling and reservations:** They can manage appointments, reservations, and bookings, making it easier for customers to schedule their time and reducing the workload on your staff.
- **Feedback collection:** They can collect and analyze customer feedback, helping you identify areas for improvement and make data-driven decisions.
- **Internal processes:** They can streamline internal tasks like HR inquiries, IT support, and employee onboarding, making your team more efficient and productive.

No matter the team or industry, autonomous agents can help your company become more efficient. By delegating tedious, time-consuming tasks to autonomous agents, your employees can focus on what matters most: your customers.



Meet Agentforce

Ready to give autonomous agents a try? At Salesforce, we've got just the thing for you. Our advanced conversational AI, Agentforce, is designed to boost productivity and lighten your team's workload. These smart agents can handle routine tasks with ease and even lend a hand with more complex ones, all while operating independently within the parameters you set. They can be deployed across various customer channels to enhance engagement and efficiency.

The best part? Agentforce is seamlessly integrated into the Salesforce interface, making it a breeze to set up and launch agents right within your workflow. Imagine your team getting business tasks done with the help of a super-smart assistant, right where they work. Agents can also be deployed in your company's support channels to give your customers the same level of awesome assistance. Whether it's your employees or your customers, Agentforce is there to make everyone's life easier and more efficient.

Trusted and Secure

Agentforce ensures that your data remains secure and private. The Einstein Trust Layer uses a secure gateway and zero-retention agreements to protect your company data. Additionally, it includes toxicity detection and audit trail logging to ensure that the agents' responses are safe and compliant.

Powerful and Versatile

Agentforce uses industry-leading Salesforce applications to deliver transformative experiences across sales, service, commerce, marketing, and industries. By combining the language and reasoning capabilities of large language models (LLMs) with granular actions, these agents can handle a wide range of tasks and provide personalized experiences at scale.

Grounded in Unified Data

To deliver accurate and relevant outcomes, Agentforce is grounded in Salesforce data and unified data from Data 360. This ensures that these agents have access to the most up-to-date and relevant information, leading to better decision-making and more effective actions.

Agentforce is the perfect solution for integrating autonomous agents into your Salesforce Platform. With a comprehensive suite of tools, you can get up and running quickly and start improving your business processes faster than ever before. Experience the power of automation and watch your business thrive!

A Beginner's Roadmap to Integrating Salesforce Autonomous Agents

Getting started with autonomous agents can seem daunting, but it's quite simple once you know what you want to achieve. Here are some helpful tips to keep in mind when you start the process.

Think Big, Start Smart: Plan Your Strategy

Define the goals and scope of your autonomous agents, and pinpoint the areas where they can make the biggest impact. For example, a retail company sees that a lot of customer service inquiries are about order tracking and returns. It decides to use Agentforce to automate these tasks. They want an autonomous agent to handle text-based interactions on the company's website and mobile app, pulling customer order data from the CRM to provide real-time updates.

Design with Flair: Build Your Agent

Design and configure your autonomous agents to perform specific tasks and interactions. Using Agentforce to create the autonomous agent, the customer service team at the retail company creates a topic called Order Management that includes actions such as Check Order Status, Initiate Return, and Provide Tracking Information. They design the agent to handle these tasks autonomously, using natural language processing (NLP) to understand and respond to customer inquiries.

Put It to the Test: Test Your Agent

Conduct thorough testing to ensure your agent performs as expected, and resolve any issues before deploying it. The team's customer service manager sets up a testing phase for their new agent. They simulate common customer inquiries and edge cases to make sure the agent can handle them like a pro. They collect user feedback through a survey and use this data to fine-tune the agent's responses and actions. During testing, they see that the agent struggles with handling return requests, so the manager adjusts the instructions for the Initiate Return action and quickly resolves the issue.

Go Live and Celebrate: Launch Your Agent

After deploying the agent, the team monitors its performance and notices a significant reduction in the time it takes to resolve order tracking and return requests. They share this success with leadership and stakeholders, highlighting the efficiency gains and improved customer satisfaction. This success story helps build confidence and encourages further investment in time-saving autonomous agents. It's like watching your agent ace its first big challenge and earn a gold star!

Wrap It Up

You've learned that effectively integrating autonomous agents into your workflow can save you significant time and resources while dramatically improving the overall customer experience. These smart agents are your secret weapon for boosting efficiency, allowing you to focus on other important tasks that propel your business forward.

Ready to transform your business with Agentforce? Start your journey today and see the difference for yourself.

Resources

- [Trailhead: AI Strategy](#)
- [Trailhead: Agentforce: Quick Look](#)
- [Trailhead: AI + Data: Project Planning](#)
- [Trailhead: The Einstein Trust Layer](#)
- [Trailhead: Agentforce: Agent Planning](#)
- [Salesforce Help: AI Project Success](#)
- [Salesforce Help: Design and Implement Agents](#)

Quiz

To complete this unit, you need to answer all the quiz questions correctly.

+100 Points

1

What is a key benefit of using autonomous agents in customer support?

A

They can send customers all of the company's FAQs.

B

Human representatives can focus on more complex issues.

C

They can handle all customer issues without any human intervention.

D

They can create new products and services for customers.

2

What ensures that Agentforce protects your company's data and detects toxicity?

A

Data 360

B

Einstein Trust Layer

C

External APIs

D

External human audits

Explore Agentforce

Learning Objectives

After completing this unit, you'll be able to:

- Define what topics and actions are.
- Explain the difference between standard versus custom topics and actions.

A Look Under the Hood

Before Linda sets up Agentforce, she wants to explore its different components and learn what makes Agentforce tick.

How Agentforce Works

Agentforce has four basic components: the agent, topics, actions, and the reasoning engine.

Agent

Previously, you learned that Agentforce includes tools for creating, customizing, and testing AI agents that perform tasks and business interactions. Currently, you can customize and launch agents for your employees and customers. See [Agent Types and Considerations](#) to learn about the different agent types and default templates for specific clouds and use cases. Here are a few examples:

- **Agentforce Employee Agent:** Help your employees across a wide range of workflows and tasks by giving them access to the Employee Agent, which is seamlessly built into the Salesforce interface.
- **Agentforce Sales Coach:** Offer personalized coaching to help your sales reps handle challenging conversations and improve performance.
- **Agentforce for Service:** Support your customers intelligently by resolving common inquiries autonomously and processing incoming cases.
- **Agentforce SDR:** Scale your sales team and make the most of your pipeline by handling new or updated leads, sending customized intro emails, responding to replies, and connecting qualified leads with sales reps.

These AI agents are goal-oriented and autonomous, and they can perform business tasks and make data-driven decisions. But how exactly does that happen? That's where topics and actions come in.

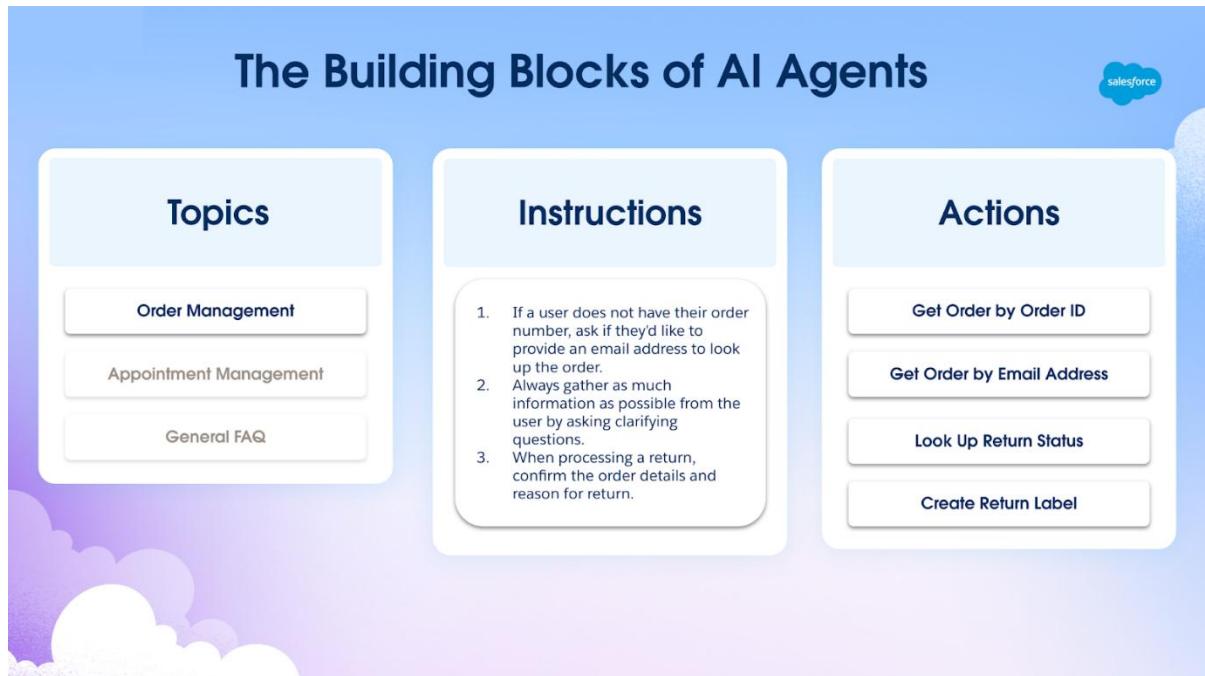
Topics and Actions

Agents are made up of topics, which define the different jobs an agent can do. Topics include natural-language [instructions](#) that tell the agent how to make decisions and what it should and shouldn't do.

Topics also contain a set of actions, which are the tools the agent uses to do its job.

For example, an Order Management topic might include these actions.

- Get Order by Order ID
- Get Order by Email Address
- Look Up Return Status
- Create Return Label



Like topics, actions also include a set of instructions. [Action instructions](#) are crucial because they tell the agent what the action does. The names, instructions, inputs, and outputs for agent actions determine when and how an action is used. The better the instructions, the more predictably the action performs, which leads to more reliable interactions.

The Importance of Topics

Just like it's important to establish a topic in a person-to-person conversation, topics help an agent recognize and organize how to behave and respond. When you define topics, you set clear boundaries and context. This helps your agent focus on specific tasks, which leads to more consistent and appropriate interactions.

When a user asks a question or makes a request, your agent picks the relevant topic and launches the appropriate actions within that topic. This focuses your agent on the most relevant actions and data for the current conversation.

Standard Versus Custom

Salesforce provides some standard topics and actions for Agentforce out of the box, so you can get up and running quickly. But you can also create custom topics and actions to give your AI agent the ability to perform tasks specific to your business. Let's look at both, so you can decide when to use standard versus custom topics and actions.

Standard and Custom Topics

First, let's go over standard and custom topics.

Standard Topics

Salesforce offers a library of standard topics for common use cases. Standard topics are predefined and come with a set of commonly used actions for various business scenarios. They're a great starting point for many organizations: They cover a wide range of tasks and are perfect for quick implementation.

Here are a few examples of topics provided by Salesforce, along with a brief description.

Topic Name	What It Does
General CRM	Handles user requests that are related to Salesforce CRM data, such as identifying, summarizing, or refining emails, aggregating data, and finding Salesforce objects.
Close Deals	Provides sellers with recommendations to close deals based on past deals won, conversation signals, and more. Sellers also get answers to product-related pricing questions and suggestions for plans to help them close deals faster.
Marketing Campaigns	Drafts compelling, branded briefs and campaigns in Marketing Cloud.

Keep in mind that some topics are tailored for specific clouds or licenses, so they might need additional permissions or licenses. To learn more about standard topics, see the Resources section.

Custom Topics

Custom topics help you tailor an agent to meet specific business needs. Define a topic, actions, and instructions that align with your unique processes and requirements.

Let's check back in with Linda to see how Cloud Kicks might use custom topics. Cloud Kicks offers a wide range of custom sneakers, and the order fulfillment process is quite complex. Linda decides to create a Shipping Management custom topic.

For example, a customer might ask, "Do you have the blue custom sneakers in stock? And can I get them next week?"

The custom topic and its assigned actions guide the agent to check the inventory, review shipping options, and confirm the delivery date.

To learn more about custom topics, see the Resources section.

Standard and Custom Actions

Now that you're an expert on topics, let's dive into standard and custom actions. Actions are the tools that an agent uses to get things done.

Standard Actions

Standard actions handle general use cases and perform a variety of functional tasks from simple queries to complex operations. Similar to standard topics, Salesforce offers a library of standard actions. Some are available to all users with Agentforce access, while others require additional licenses for specific clouds or products.

The table shows a few standard actions provided by Salesforce, along with a brief description. Some of these actions are system actions, which are critical and can't be removed.

Action Name	What It Does
Query Records (Beta)	Finds and retrieves Salesforce records based on the user's request and specific conditions, such as: "Find all open opportunities set to close this quarter sorted by created date."

Action Name	What It Does
Summarize Record	Summarizes a single Salesforce CRM record. For example: “Create a summary for the Acme account.”
Draft or Revise Email	Creates an email draft or revises the latest version of a generated email based on the user’s input. For example: “Write an intro email to Steve from Acme.”
Answer Questions with Knowledge	Answers a question from a user based on information from relevant knowledge articles. For example: “What happens if a customer returns an item for returns over 30 days?” (Requires a Knowledge license.)

To see all the available standard actions, check out the [documentation](#).

Custom Actions

If you need to customize your agent for business-specific processes and workflows, create custom actions for your topics. The best part? You don’t have to start from scratch. Custom actions use Salesforce technologies you already know and love.

When you create a custom action, you build it on top of existing platform features, like invocable and REST Apex classes, autolaunched flows, prompt templates, and external services.

For example, you can use flows to connect to MuleSoft APIs or Apex and flows to connect to third-party APIs. You can also use Apex or flows to access engagement data, website data, or third-party data through Data 360. By making this functionality available in Agentforce, you unlock a ton of value and use cases.

If you want to get hands on with agent actions, check out the [Quick Start: Agent Actions](#) badge.

The Final Building Block of Agentforce

Now that Linda understands how topics and actions work, it’s time to introduce the powerful component of Agentforce that orchestrates everything behind the scenes: the reasoning engine.

Resources

- [Salesforce Help: What Are Agents?](#)
- [Salesforce Help: Best Practices for Writing Topic Instructions](#)
- [Salesforce Help: Best Practices for Agent Action Instructions](#)
- [Salesforce Help: Agent Actions](#)
- [Salesforce Help: Standard Agent Topic Reference](#)
- [Salesforce Help: Create a Custom Topic](#)
- [Video: Get Started with Agent Actions for Developers](#)
- [Video: How to Use Prompt Templates as Agent Actions](#)
- [Video: Build Custom Agent Actions Using Apex](#)

Quiz

To complete this unit, you need to answer all the quiz questions correctly.

+100 Points

What's the primary difference between standard and custom actions in Agentforce?

A

Standard actions are predefined and available to all users, while custom actions are built to meet specific business needs.

B

Standard actions can only be used with internal agents, while custom actions are for customer-facing agents.

C

Standard actions are more complex and require additional licenses, while custom actions are simpler, and do not.

D

Standard actions are used for data retrieval, while custom actions are used for data manipulation.

2

Which of the following best describes the role of topics in Agentforce?

A

Topics are predefined scripts that the agent follows without deviation.

B

Topics provide the agent with a set of actions and instructions to perform specific tasks.

C

Topics are used to store user data and preferences.

D

Topics are templates for creating new AI agents.

Second attempt earns 50 points. Three or more earns 25 points

Meet the Reasoning Engine

Learning Objectives

After completing this unit, you'll be able to:

- Define what the reasoning engine is.
- Explain how the reasoning engine works.

Putting It All Together

Topics and actions are the building blocks of an agent, and they're pretty powerful, right? But how does an agent know when to launch these topics during conversations? Let's meet the reasoning engine behind Agentforce.

What's a Reasoning Engine?

Think of the reasoning engine as the conductor of an orchestra. Just like a conductor keeps time and guides musicians, the reasoning engine orchestrates how topics and actions handle a user's request.

Here's the breakdown.

- **Interpret the user's request.** When a user starts a conversation, the reasoning engine interprets the request and classifies it into a specific topic. For example, if you ask, "When will my order be delivered?", the engine classifies it as the Order Management topic.
- **Build a plan for accomplishing the goal.** The reasoning engine then processes each step to accomplish the goal. It considers the context, previous interactions, and available data when breaking the problem down.
- **Use data to change behavior and respond to the user.** When the agent finds and reviews the data from topics and actions, the results can provide a wealth of additional information. This empowers the agent to respond dynamically and make better decisions. The insights the agent gains can show potential pathways and significantly influence the next steps of the plan.

Remember that scenario at the beginning of the module with Alex and Agentforce? Let's analyze it and see the reasoning engine in action.

Customer (Alex): "Hi, I just placed an order for a pair of custom sneakers. Can you tell me when it will be delivered?"

Agentforce: "Hello, Alex! Your order will be shipped within the next 2 to 3 business days and should arrive at your address within 5 to 7 business days after shipping. Is there anything else you'd like to know about your order?"

- **Interpret the user's request:** The reasoning engine classifies this as the Order Management topic.
- **Build a plan for accomplishing the goal:** It queries the order database to confirm the shipping timeline and provides a clear response.
- **Find and launch the right topics and actions:** The agent retrieves the shipping information and provides a detailed response.

Alex: "Thanks! Do you have any stores in New York City?"

Agentforce: "We don't have any physical stores in New York City, but we have a popup shop opening next month at 123 Fashion Avenue from October 1 to October 15. You can also shop online for the latest styles."

- **Interpret the user's request:** The reasoning engine classifies this as the Store Locations custom topic.
- **Build a plan for accomplishing the goal:** It takes the next step of searching the company's store locations and upcoming events to solve requests.
- **Find and launch the right topics and actions:** Given the lack of stores, the agent provides alternative information about the popup shop and online shopping options.

Alex: "Awesome, thanks! One more thing—do you have any recommendations for a good running trail in New York City?"

Agentforce: "Certainly! For a great running trail, I recommend Central Park's Reservoir Loop, which is 1.58 miles and offers beautiful views. For a longer run, try the Hudson River Greenway, which stretches for about 13 miles. Enjoy your run!"

- **Interpret the user's request:** The reasoning engine classifies this as the Local Recommendations custom topic.
- **Build a plan for accomplishing the goal:** It accesses a database of local recommendations and selects the most relevant options.
- **Finds and launches the right topics and actions:** The agent provides detailed recommendations for running trails in New York City.

Alex: "That's perfect, thanks so much for all the information!"

Agentforce: "You're welcome, Alex! If you have any more questions, feel free to reach out. Have a great day!"

In this scenario, the reasoning engine handles the initial request about order delivery then seamlessly transitions to other topics like store locations and local recommendations. The reasoning engine can tackle topic changes and complex situations, ensuring a smooth and satisfying experience for the customer.

Time for Action

Linda's feeling more confident now that she knows how Agentforce works, and she's ready to take it for a spin. We suggest you do the same! Here are some suggested Trailhead badges to continue learning about Agentforce.

- [Agentforce Builder Basics](#)
- [Quick Start: Build Your First Agent with Agentforce](#)
- [Connect Data 360 to Agentforce and Prompt Builder](#)

Now that you have a solid grasp of both standard and custom topics and actions and the reasoning engine, you're ready to plan, build, and customize your own agents with Agentforce. Explore our resources to learn more about Agentforce and get hands on with Trailhead badges.

Resources

- [Trailhead: Agentforce: Agent Planning](#)
- [Trailhead: Be an Agentblazer](#)
- [Video Playlist: Agentforce Decoded](#)

Quiz

To complete this unit, you need to answer all the quiz questions correctly.

+100 Points

1 What is the primary role of the reasoning engine in Agentforce?

A

To store user data

B

To interpret user requests and classify them into topics

C

To design the user interface

D

To manage the agent's schedule

2

What does the reasoning engine do when it finds and launches the right topics and actions?

A

It stops the conversation

B

It provides a static response

C

It retrieves and provides detailed, relevant information

D

It redirects the user to a representative

Second attempt earns 50 points. Three or more earns 25 points.

5) Explore Multi-Agent Interoperability

Learning Objectives

After completing this unit, you'll be able to:

- Explain how interoperability protocols enable agents to share context and work together effectively.
- Determine when to apply the Agent API to support complex, multi-agent solutions.

Key Topics

This unit prepares you for the Multi-Agent Interoperability section of the Salesforce Agentforce Specialist exam, which makes up 5% of the overall exam. This section of the exam tests these topics.

- Explain the purpose of Model Context Protocol (MCP) and its use cases.
- Explain the purpose of agent to agent protocol.
- Given a scenario, identify when it's appropriate to use Agent API.

Like the previous units, this unit contains practice scenario-based questions and flashcards.

Exam Practice Questions

Ready to jump in? The sample tool is not scored—it's just an easy way to quiz yourself. To use it, read the scenario, then click the answer you think is correct. Some questions can have more than one

correct answer. Click **Submit** to learn whether the answer you chose is correct or incorrect, and why. When you reach the end, you can review the answers or retake the questions.

Study Materials

Did you choose an incorrect answer? Check out the table for related study materials.

Questions	Study Materials
1	Learn how MuleSoft Model Context Protocol (MCP) can result in richer context, and more intelligent, secure experiences across the business.
2	Study the importance and benefits of agent-to-agent interoperability in the context of AI agents.
3	Explore how Agent API can be used to communicate with AI agents directly from a REST API.
4	Read more on how to use the Agent API to programmatically interact with Salesforce agents.

Exam Topic Flashcards

The following flashcards cover key Multi-Agent Interoperability terms and concepts. Use these interactive flashcards to brush up on some of the key topics you'll find on this part of the exam.

Read the question or term on each card, then click or tap the card to reveal the correct answer. Click the right-facing arrow to move to the next card and the left-facing arrow to return to the previous card.

Study Materials

Did you choose an incorrect answer? Check out the table for related study materials.

Flashcards	Study Materials
1-2	Review how agent-to-agent interoperability protocol provides the foundation for cross-vendor collaboration.
3	Learn more about how Model Context Protocol (MCP) helps simplify the development workflow.
4	Study up on using Agent API to communicate with AI agents directly from a REST API.

Congratulations! You've covered 100% of the Salesforce Agentforce Specialist Certification exam material in this badge.

You've reviewed these sections.

- Review AI Agents
- Study Up on Prompt Engineerings
- Review Data Cloud for Agentforce
- Examine the Development Lifecycle
- Explore Multi-Agent Interoperability

Good luck on your exam!

Quiz

To complete this unit, you need to answer all the quiz questions correctly.

+100 Points

1

The Multi-Agent Interoperability section makes up what percentage of the Salesforce Agentforce Specialist certification exam?

A

5%

B

10%

C

15%

D

20%

2

Which key topic does the Multi-Agent Interoperability section of the exam cover?

A

Identify the considerations for deploying an agent from sandbox to production.

B

Explain the purpose of Model Context Protocol (MCP) and its use cases.

C

Explain the process for creating, activating, and executing prompt templates.

D

Given a use case, manage deterministic behavior for the agent using filters and variables.

Second attempt earns 50 points. Three or more earns 25 points.
