

Designing Automated Customer Experiences with the new Webex AI Agent

cisco Live !

Speaker Name
Preetham Kademada

Session ID: BRKCCT-2555

Cisco Webex App

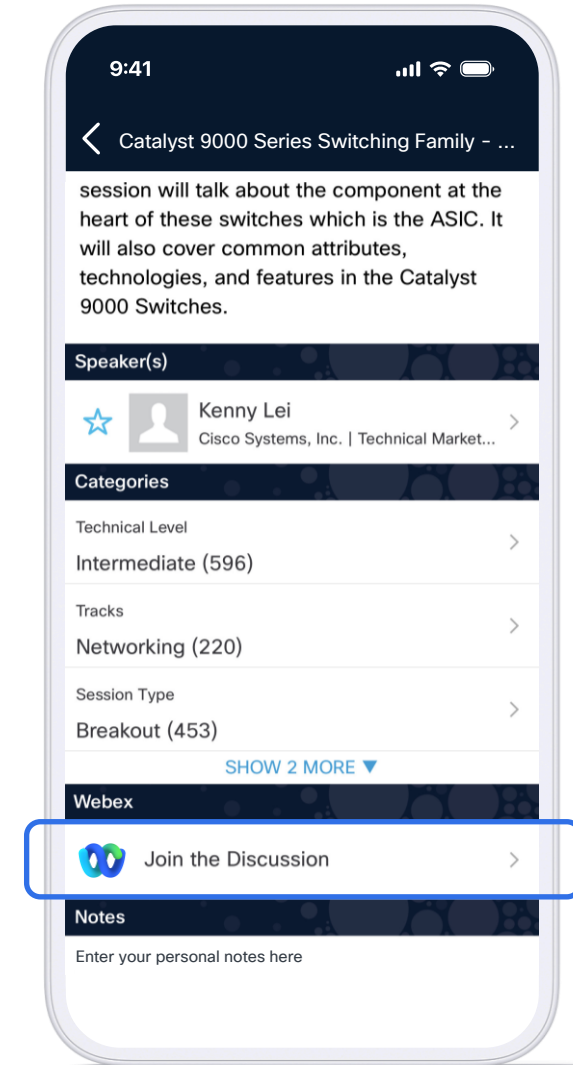
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKCCT-2555>

Agenda

- 01 Introduction
- 02 The game of cricket
- 03 Earn the Right!
- 04 Webex AI Agent introduction
- 05 Scripted AI Agent
- 06 Autonomous AI Agent
- 07 Cisco AI Security & Guardrails
- 08 Run time visibility
- 09 System-Level Guardrails
- 10 Roadmap

Let's talk Cricket!

Winning with Webex AI Agent

A Cricket Game Analogy



Opponent Analysis: Cricket Strategy & Webex AI ROI

The Cricket Playbook

 **Opponent Analysis:** Meticulous study of batting weaknesses, bowling patterns, and fielding gaps.

 **Targeting Weaknesses:** Bowlers exploit weak footwork; captains adjust to conditions.

 **Strategic Adjustments:** Dynamic play based on real-time match flow to secure victory.

Unlocking ROI

 **Precision Assessment:** Identify workflow bottlenecks, pain points, and collaboration gaps.

 **Targeted Solutions:** Identify actionable insights for measurable ROI and efficiency gains.

 **Business Optimization:** Transforms challenges into clear competitive advantages.



The Cricket Pitch & Business Outcomes



Fast Pitch

Pace bowlers dominate
Aggressive strategy needed



Spin-Friendly

Turn and grip matter
Technical precision wins



Balanced Surface

All-round capability
Adaptability is key



Selecting Your Winning Team

Optimizing for peak performance in any environment

Cricket Team Selection

A captain handpicks the ideal XI, balancing individual prowess with team synergy for victory.



Captain's Vision

Selecting the best XI players.



Specialized Skills

Batsmen, bowlers, wicket-keepers.



Strategic Positioning

Based on pitch and opponent.

AI Agent Selection

Deploying the right AI capabilities, precisely tailored to achieve business objectives.



Capability Mapping

Selecting the right AI functions.



Specific Functions

Automation, analytics, security.



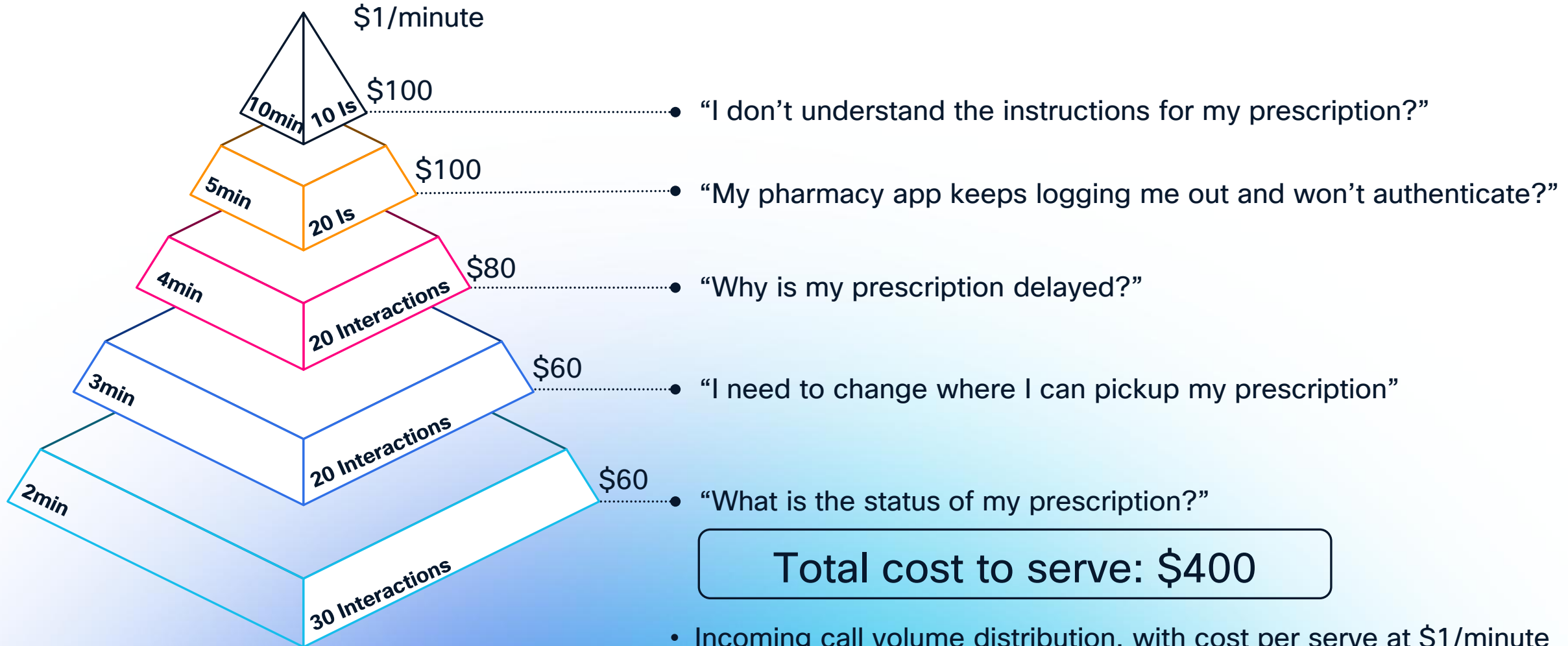
Strategic Deployment

Based on business needs and ROI.



Earn the Right!

Use case: Pharmacy prescription



AI is embedded across everything we do

Developers & ecosystem

AI assistant for developers | BYO virtual agent



Proactive journeys

Campaign management
AI agent linking

Webex Connect



AI agents

Omnichannel, multimodal, & multilingual
Scripted & autonomous modes
Execute actions & fulfill in

Webex Connect



Human agents

Summarization | Responses / answers
Wellbeing | Performance management

Webex Contact Center
Contact Center Enterprise

Customer experience foundation

Code generation | Insights & analytics

Webex platform

Noise removal | Prediction | Sentiment | Translation | Summarization

Cisco security

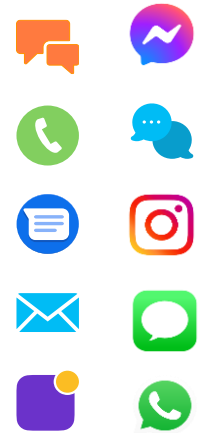
Use case: Pharmacy prescription

Outbound notifications and proactive messaging



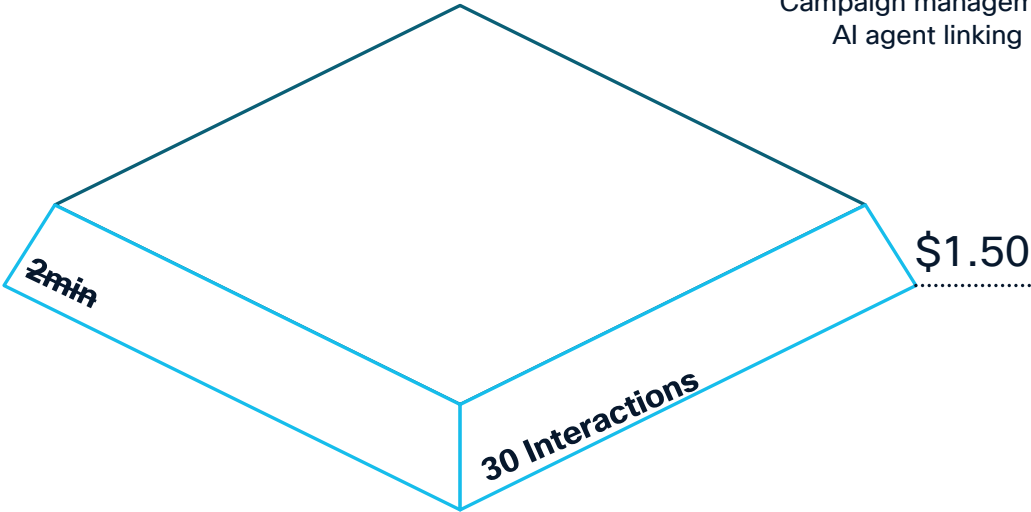
Proactive journeys

Campaign management
AI agent linking



The fulfillment of your prescription has been delayed.

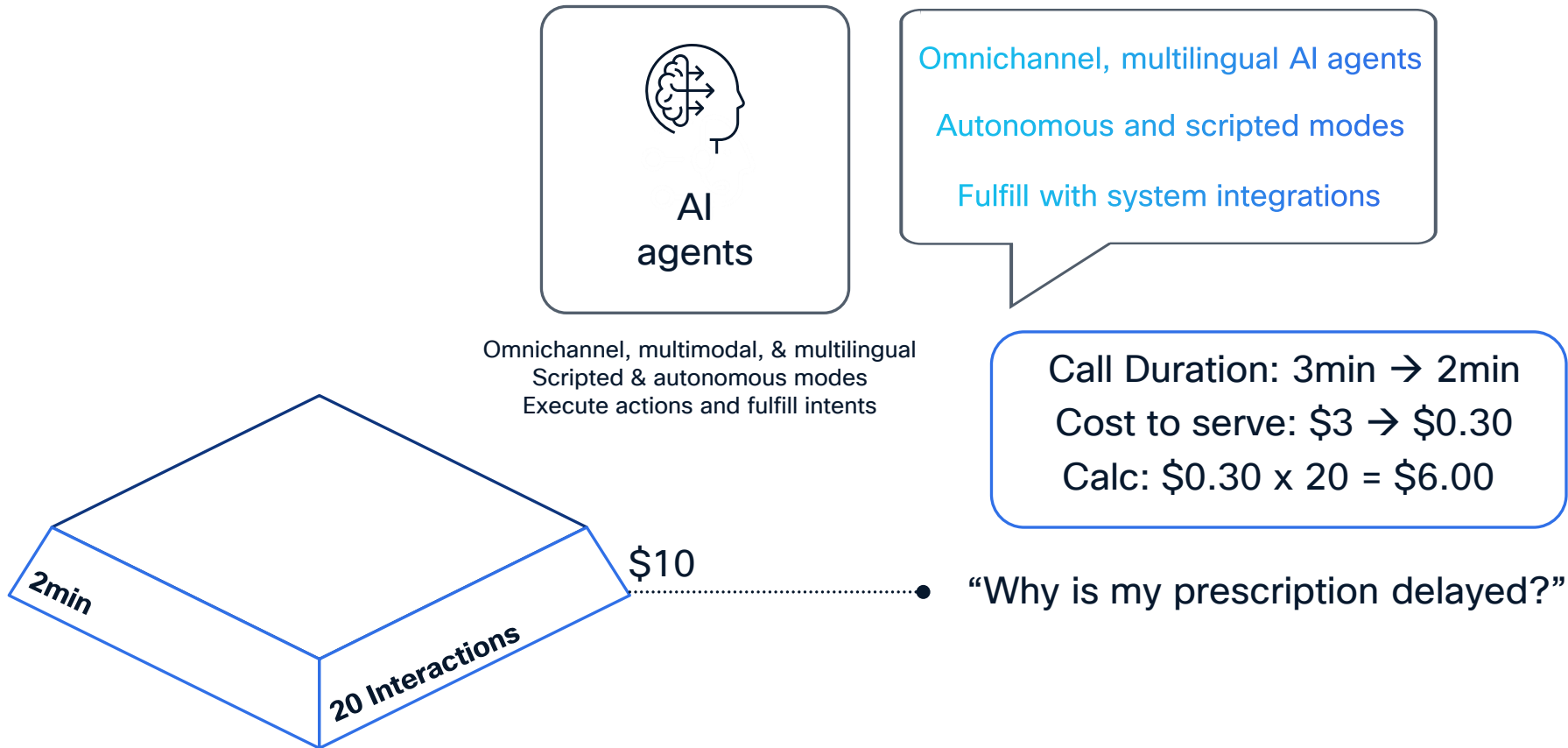
Cost per serve: \$2/min → \$0.05
Calc: \$0.05 x 30 = \$1.50



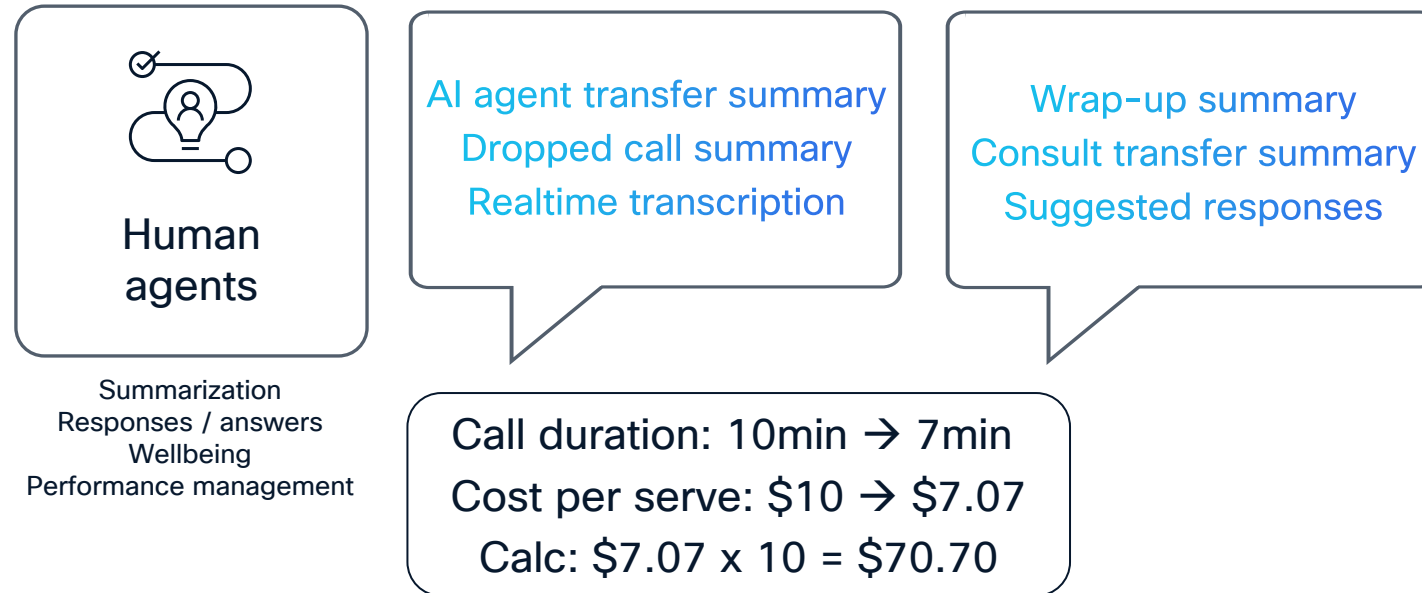
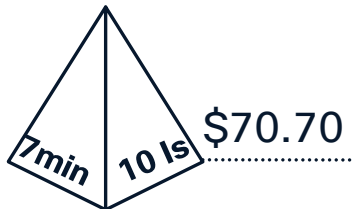
“Where is my prescription, why is it delayed?”

Use case: Pharmacy prescription

Conversational automation

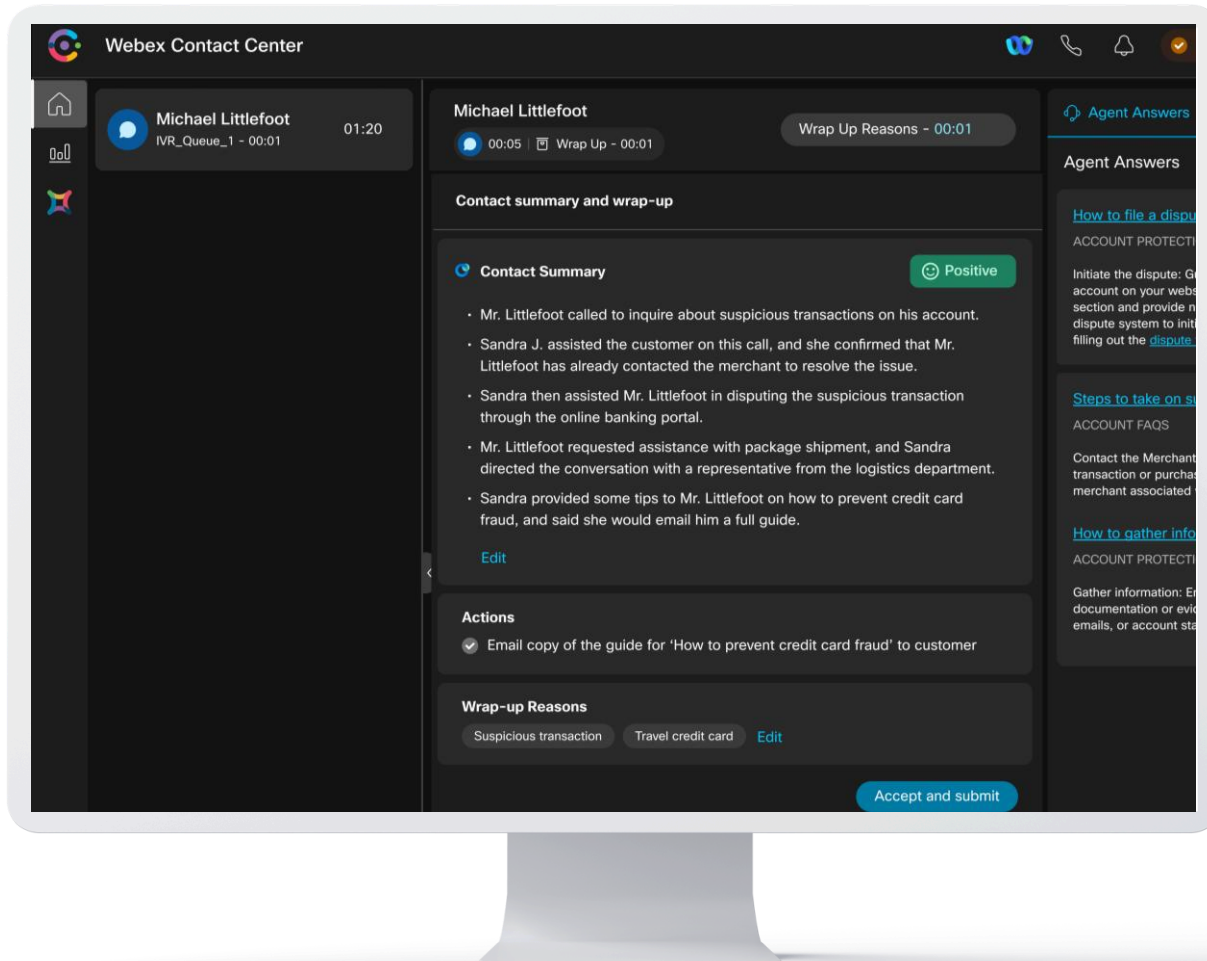


Use case: Pharmacy prescription

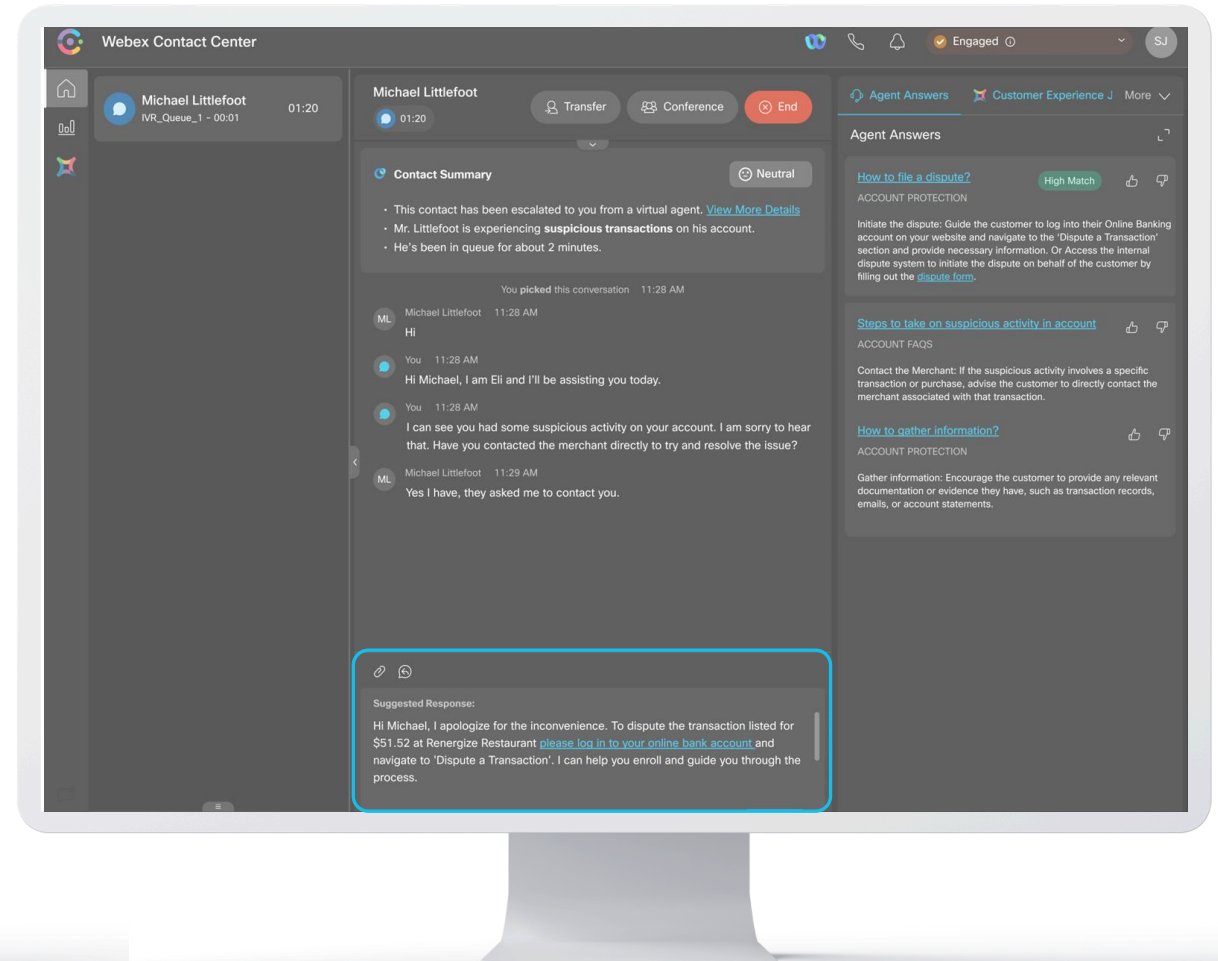


● "I don't understand the instructions for my prescription."

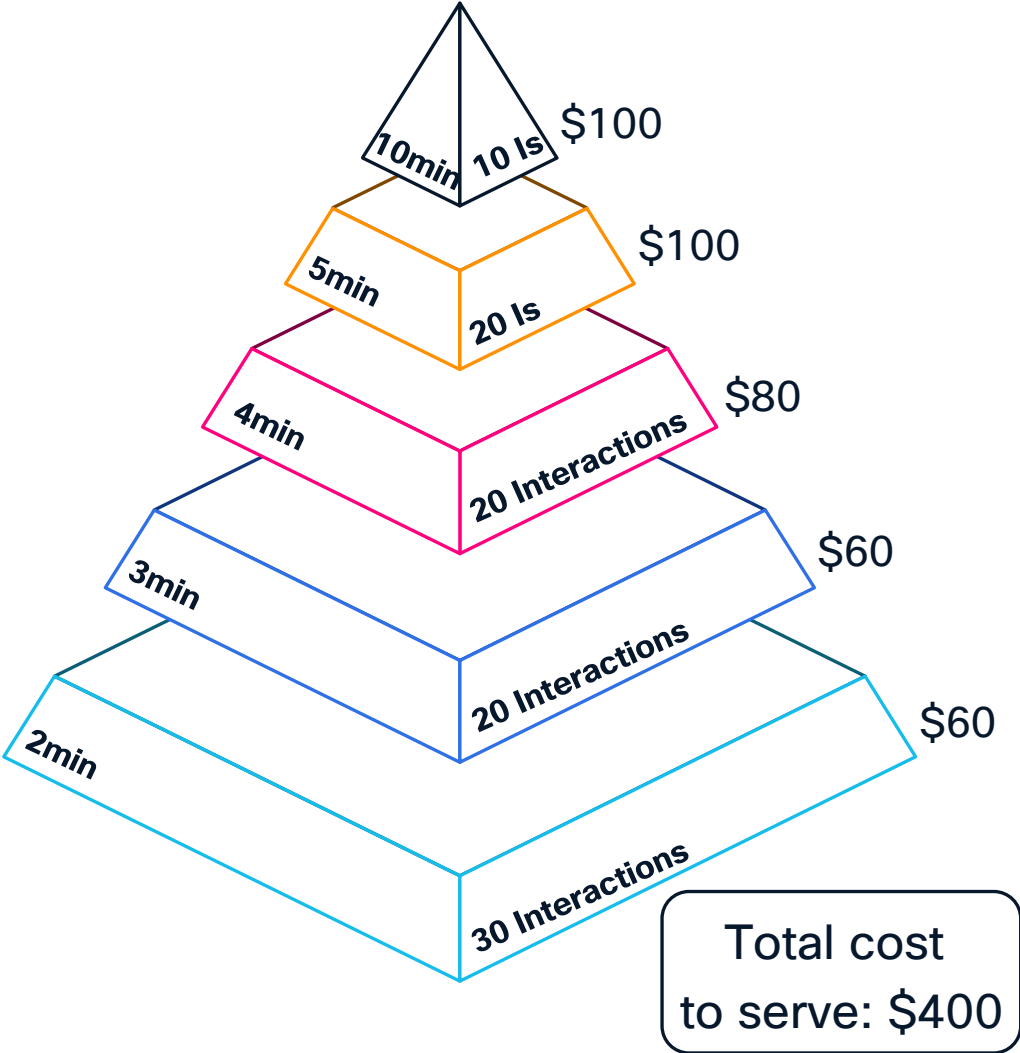
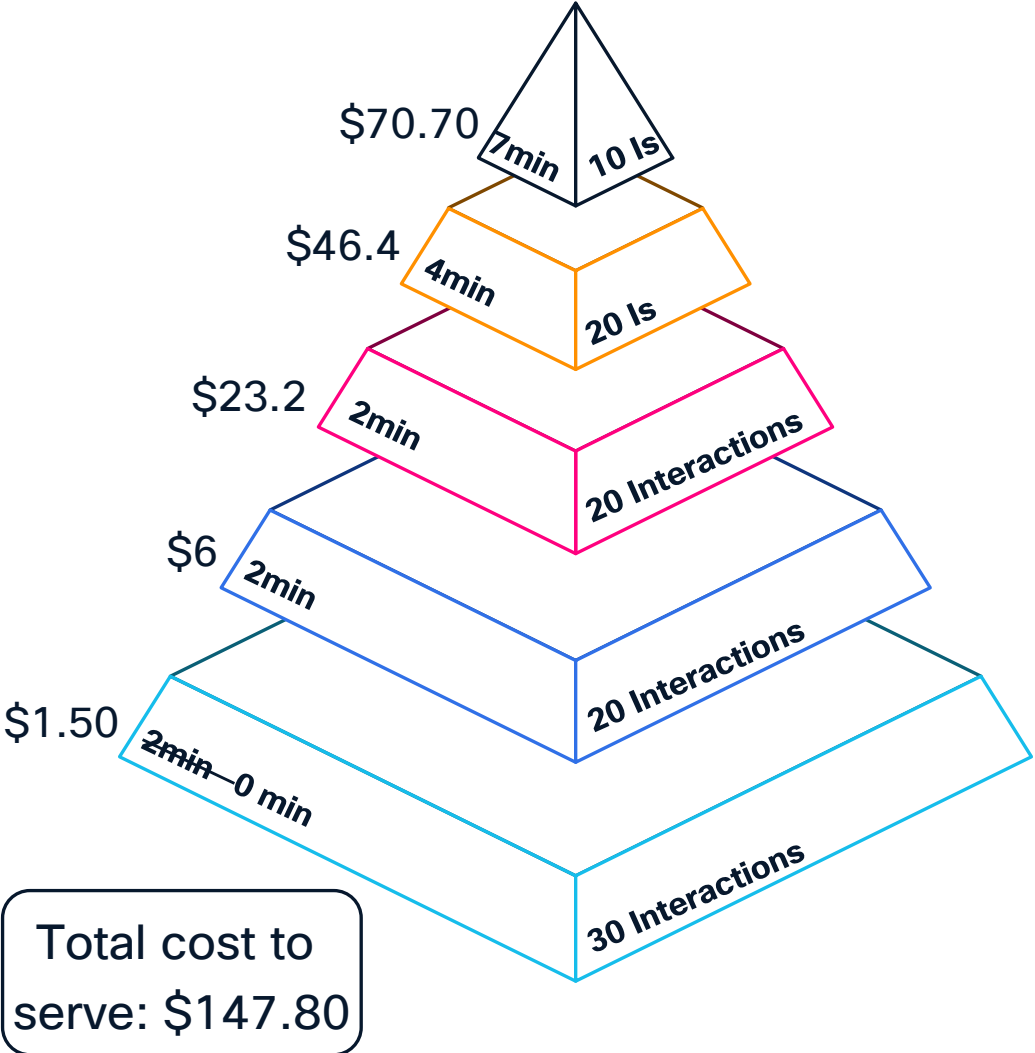
An AI assistant that wraps up calls



An AI assistant that suggests responses



Use case: Pharmacy prescription

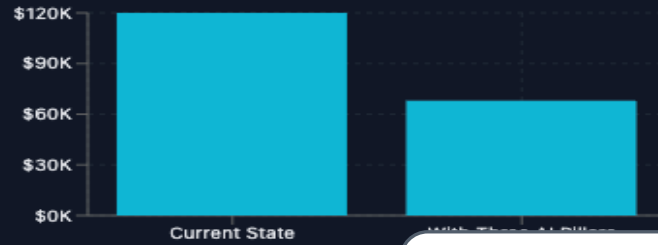


NEW Incoming call volume distribution, with cost per serve at \$1/minute

ROI: Pharmacy Prescription Analysis

Three AI Pillars Implementation - The Efficiency Breakthrough

Before vs After



Efficiency Breakthrough

Manual Only

150 interactions = \$60K

AI + Manual

300 interactions = \$68K

ROI Summary

Investment: **\$644K**
Payback: **0.4 months**
Year 1 ROI: **2,351%**

Implementation

Setup: **\$350K**
WxConnect: **\$55K/yr**
AI Platform: **\$64K/yr**
Support: **\$25K/yr**

Current:

With Three AI Pillars:

Savings:

\$15.8M annually (303 operating days)

\$52k
per day

Savings

86.8%

Cost
reduction

12
days

Payback

50%

Containment
rate

50%

More
interactions

ists - it makes them incredibly more efficient.

43%

Lower costs

100%

More
clinical time



Earn the Right !

Webex AI Agent Introduction!

Webex AI Agent

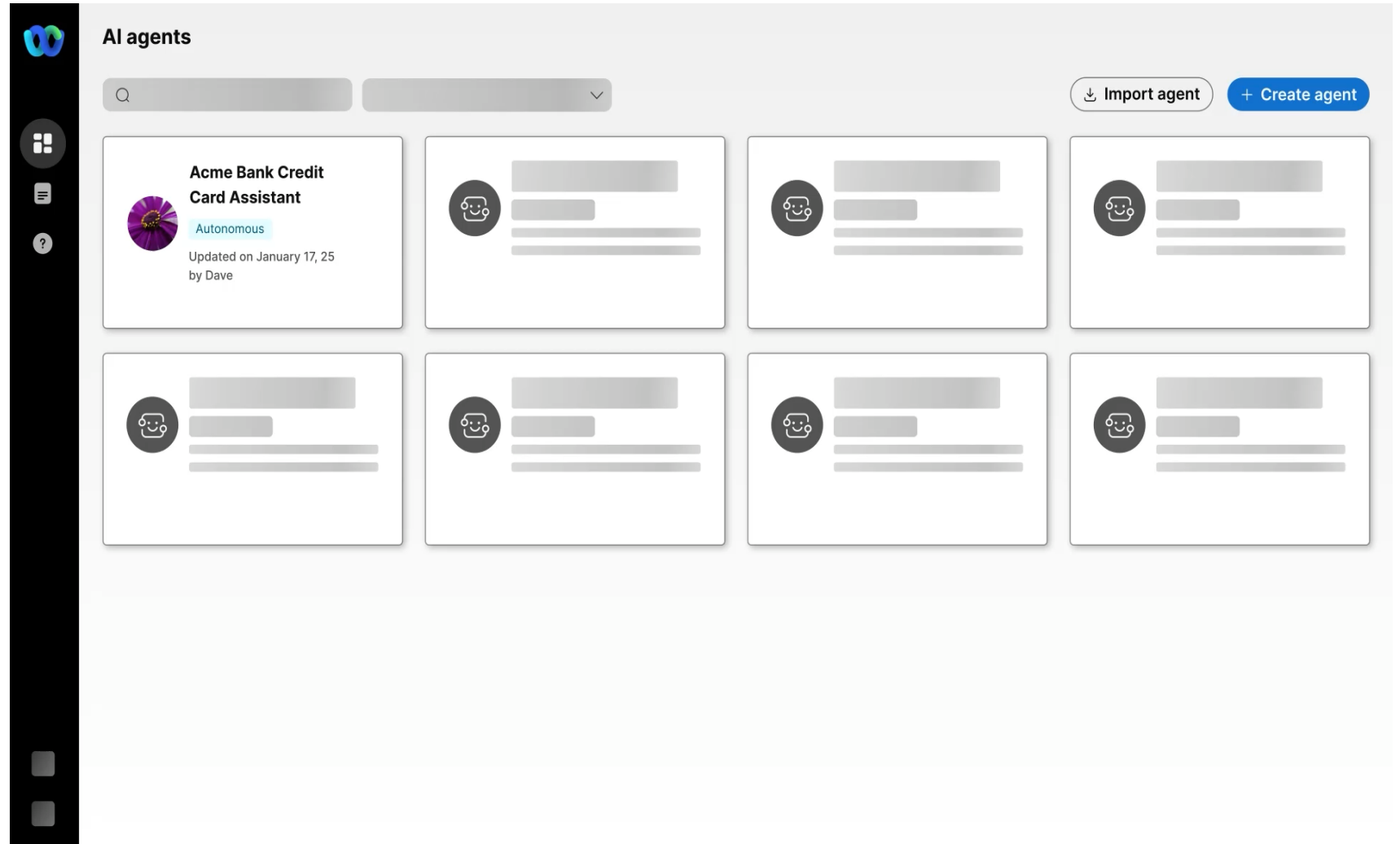
Powering human-like interactions across voice and digital channels

- | Omnichannel, multilingual AI agents
- | Autonomous and scripted modes
- | Fulfill with system integrations
- | Integrate with contact centers
- | 9 languages supported



Webex AI Agent Studio

- Create and Manage AI Agents
- Create Knowledgebases
- Set Up Guardrails, Actions and Scripts
- Languages
- Preview



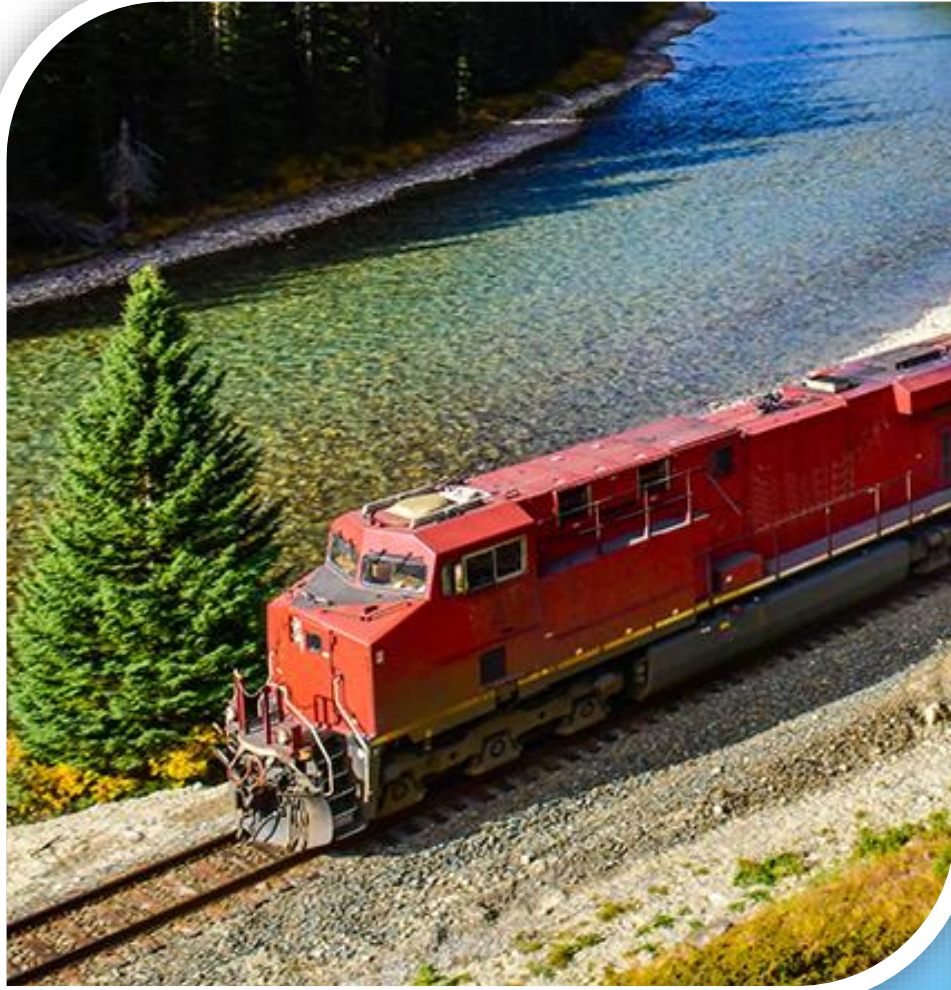
Technical Differences

	Scripted	Autonomous
Training	<ul style="list-style-type: none">Needs training data – the more, the better	<ul style="list-style-type: none">No training – only instructions & examples
Inference	<ul style="list-style-type: none">Classical ML algos for intent classification	<ul style="list-style-type: none">Taken care of by the LLM
Slot filling	<ul style="list-style-type: none">NLU frameworks	<ul style="list-style-type: none">Taken care of by the LLM
State & context management	<ul style="list-style-type: none">Highly reliant on developer	<ul style="list-style-type: none">Shared by app framework + LLM
Responses	<ul style="list-style-type: none">Pre-defined by the developer	<ul style="list-style-type: none">Generated by the LLM at runtime

Practical differences

	Scripted	Autonomous
Benefits	<ul style="list-style-type: none">Higher controlCheaper to runFaster at runtime	<ul style="list-style-type: none">Faster and easier to buildVery natural IXScope changes are easier
Drawbacks	<ul style="list-style-type: none">Effort intensive to buildBrittle and rigid IX	<ul style="list-style-type: none">Slower and more expensiveLower control, hallucinations, etcLack of high explainability

Technical Differences



Scripted AI Agent!

Scripted AI Agent Configuration

What the customer wants

What details to collect

How to respond

AI Agent Studio Voice Script

Last Updated at 15 Feb, 25 by rtmstestus1

Settings

Testing

Curation

Sessions

History

Analytics

AI agent configurations

Ready to preview

Change the agent configurations

Profile

Script

Handover

Language

Intents

Entities

Responses

Intent name

Utterances

Response name

Last update

Actions

Talk to an agent	6	Agent handover	15 Feb 25, 1:17 PM	
Thank you	10	Thank you	15 Feb 25, 1:17 PM	
Not helpful	28	Not helpful	15 Feb 25, 1:17 PM	
Greetings	24	Greetings	15 Feb 25, 1:17 PM	
Default fallback intent	0	Fallback message	15 Feb 25, 1:17 PM	
Goodbye	15	Goodbye	15 Feb 25, 1:17 PM	
Help	5	Help message	15 Feb 25, 1:17 PM	

Publish changes

Name this version so that it can be tracked in History.

Version name *

Version name

Required

Cancel

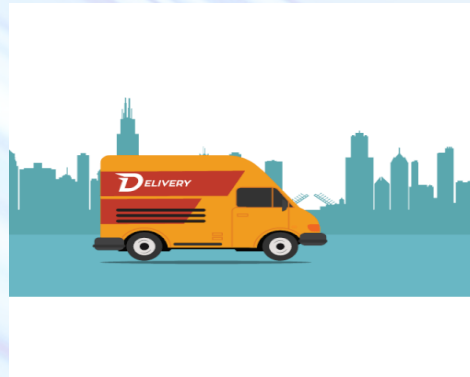
Publish

Preview

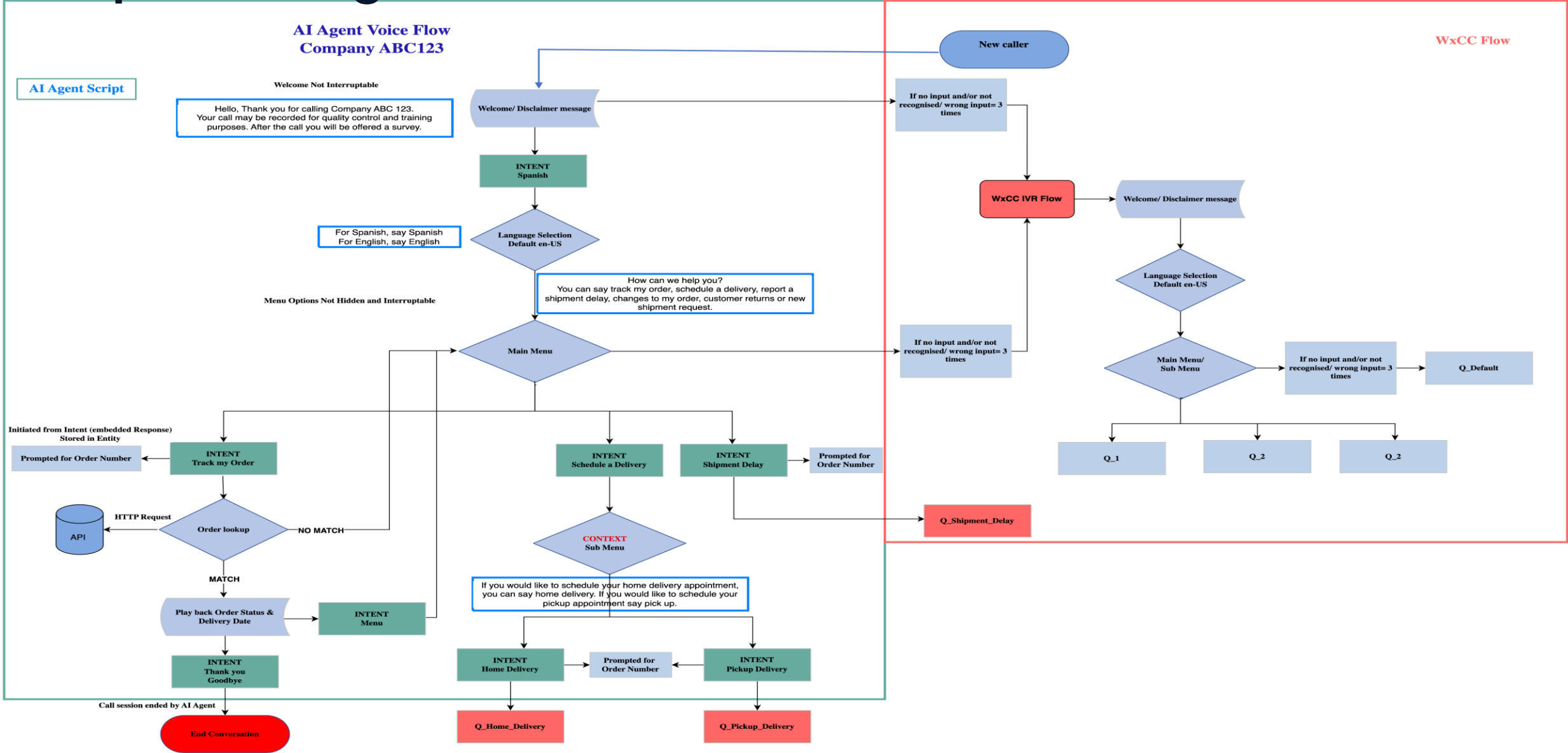
Publish

Create intent

Use Case: Company ABC123



Scripted AI Agent Voice Flow

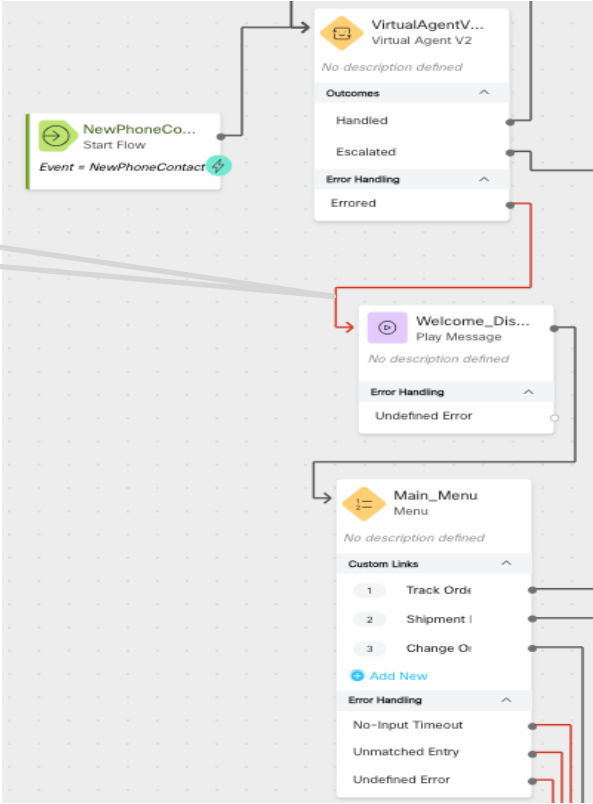


Scripted AI Agent Voice - Conditions

Flow Conditions

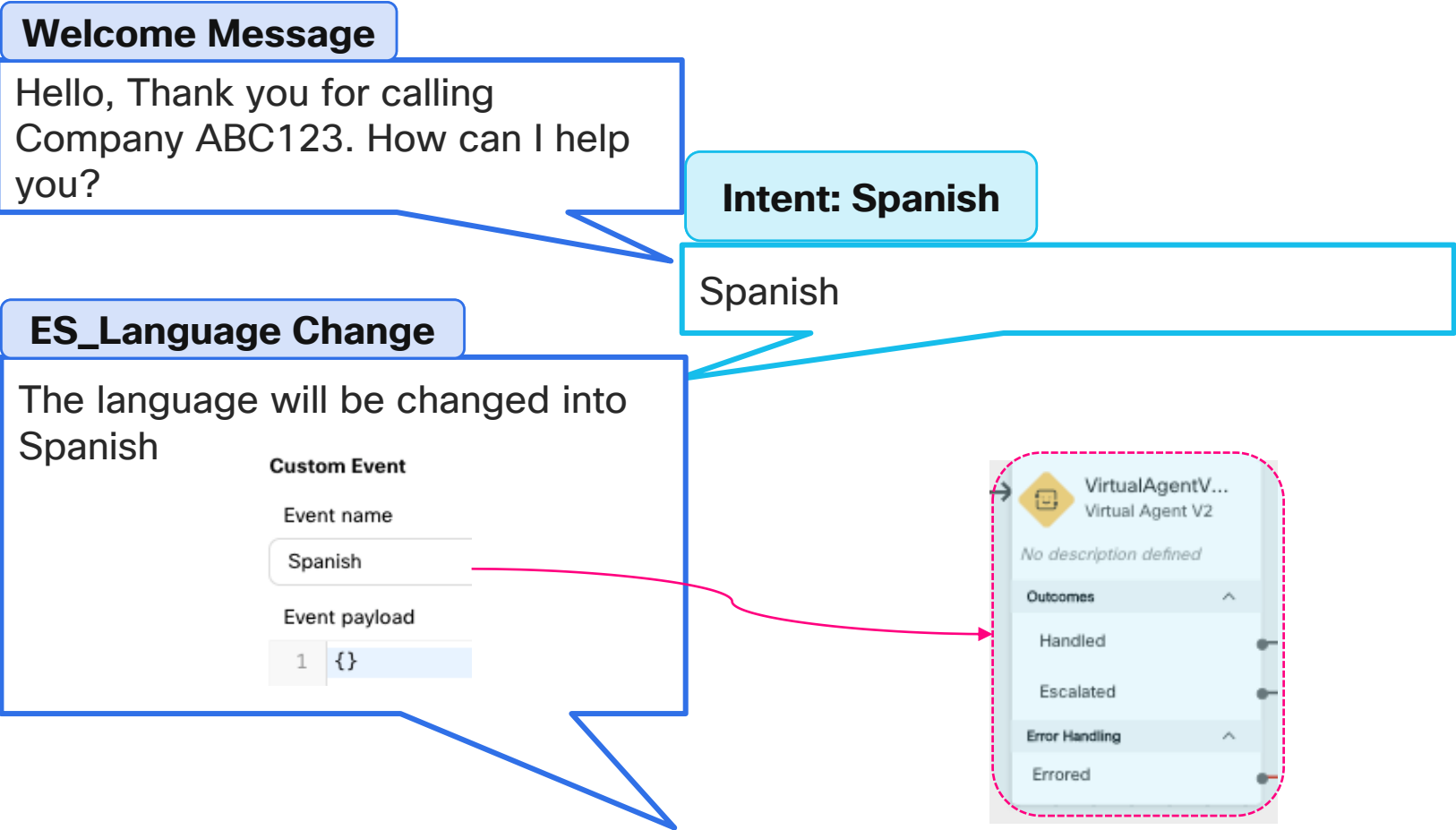
- ✓ Errored Scripted AI Agent Voice should overflow to WxCC Flow IVR.
- ✓ Default Language is English. User can change the language any time.

Errored Scripted AI Agent



Interactions		c1bd9378-d2a2-4a05-9378-dcf131be9bc0	
Sequence	Activity Name	Outcome	
1	NewPhoneContact	Success	
2	PlayMessage_jgv	Success	
3	VirtualAgentV2_pv2_3s0	Error	

Scripted AI Agent Voice – Change Language



Scripted AI Agent Voice – Change Language

The image displays two side-by-side screenshots of the Cisco AI Agent configuration interface, illustrating the setup for a scripted AI agent voice to change the language.

Left Screenshot (Spanish Intent Configuration):

- Spanish** (Header): Configure intent recognition for the agent and link a response.
- General information and settings**
 - Intent name ***: Spanish (highlighted with a pink box)
 - Settings**
 - ☐ Reset slots after completion
 - ☐ End conversation ⓘ
 - Context**
 - Entry**: Add input context
 - 0 items
- English (en) Default 4** | **Spanish (es) 7** (Tabs)
- Intent and utterances**
 - Add utterances to determine the intent. Link entities for collecting information. Make sure you don't use real customer data.
 - Add utterance** (Text input) | **+ Add** | **Generate**
 - Intent Identifier ⓘ**: Spanish
 - Spanish language** (Link)
 - Speaking Spanish** (Link)
 - Spanish
- Response**
 - Response name ***: ES_Language Change (highlighted with a pink box)

Right Screenshot (ES_Language Change Response Configuration):

- ES_Language Change** (Header): Configure channel-specific responses. Avoid using real customer data.
- Response Name ***: ES_Language Change (highlighted with a pink box)
- English (en) Default** | **Spanish (es)** (Tabs)
- Default response**
 - Conditions ⓘ** | **+ New**
 - Default (web)** | **Voice ⓘ** | **+ Add**
 - Please configure your timeout response
 - ☐ Allow barge-in ⓘ
 - ☐ DTMF input ⓘ
- Text**
 - Variant 1**: The language will be changed into Spanish (highlighted with a pink box)
 - + Add variant**
- Custom Event**
 - Event name**: Spanish
 - Event payload**: 1 {} (highlighted with a pink box)
- Default response**: Triggered when no condition is added or fulfilled

Annotations and Flow:

- A curved arrow points from the **Spanish** intent (Left Screenshot) to the **ES_Language Change** response (Right Screenshot).
- A blue box at the bottom of the right screenshot contains the text: **Event Name - String** and **Event Data - JSON**.
- A blue arrow points from the **Text** variant to the **Custom Event** section.
- A dashed pink box on the far right highlights the **VirtualAgentV... Virtual Agent V2** configuration, showing **Outcomes** (Handled, Escalated) and **Error Handling** (Errored).

Scripted AI Agent Voice – Change Language

Session ID: c20735e2-3dd6-4939-a862-143835659609 Consumer ID: 9860bd28-db52-46c4-be87-8e63520d42a2 Total Messages: 17 Last updated at: Feb 18 '25 3:40 PM

Search

Transaction info

Expand all

Intents identified

Spanish

Slots

No slots available

Entities identified

Algorithm results

Other info

Processed query: spanish

Language detection provider: fastText

Language detected: English (en)

Agent handover

Agent handover by rules

Response name: ES_Language Change

Response type: Conditional response

Response condition: default

AI Engine: Swiftmatch

Multi-lingual model: Polymatch

Min threshold score: 0.3

Partial match score difference: 0.05

Debug logs

Hello, Thank you for calling Company ABC 123. How can I help you?

3:09:04 PM, Feb 18, 2025

Txn ID: 550fb354420e410e8065c7caa8150482

Spanish

3:09:14 PM, Feb 18, 2025

The language will be changed into Spanish

```
1 {
2   "Data": {
3     "Params": {}
4   },
5   "Event_Name": "Spanish"
6 }
```

3:09:14 PM, Feb 18, 2025

Txn ID: 84d8347a970a443382b65a167e3aee71

Hola, gracias por llamar a la empresa ABC 123. ¿Le puedo ayudar en algo?

3:09:18 PM, Feb 18, 2025

VirtualAgentV...
Virtual Agent V2

No description defined

Outcomes

Handled

Escalated

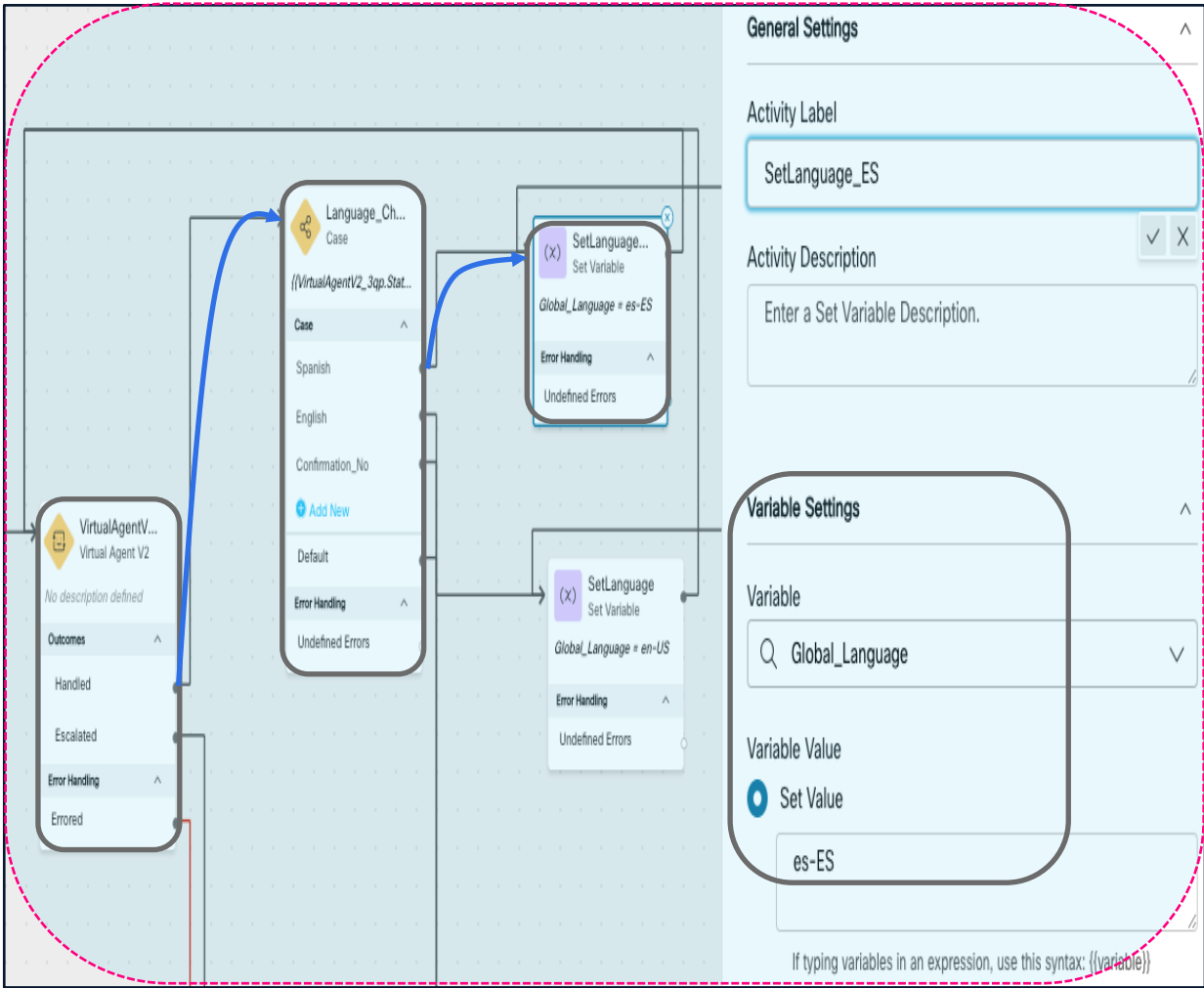
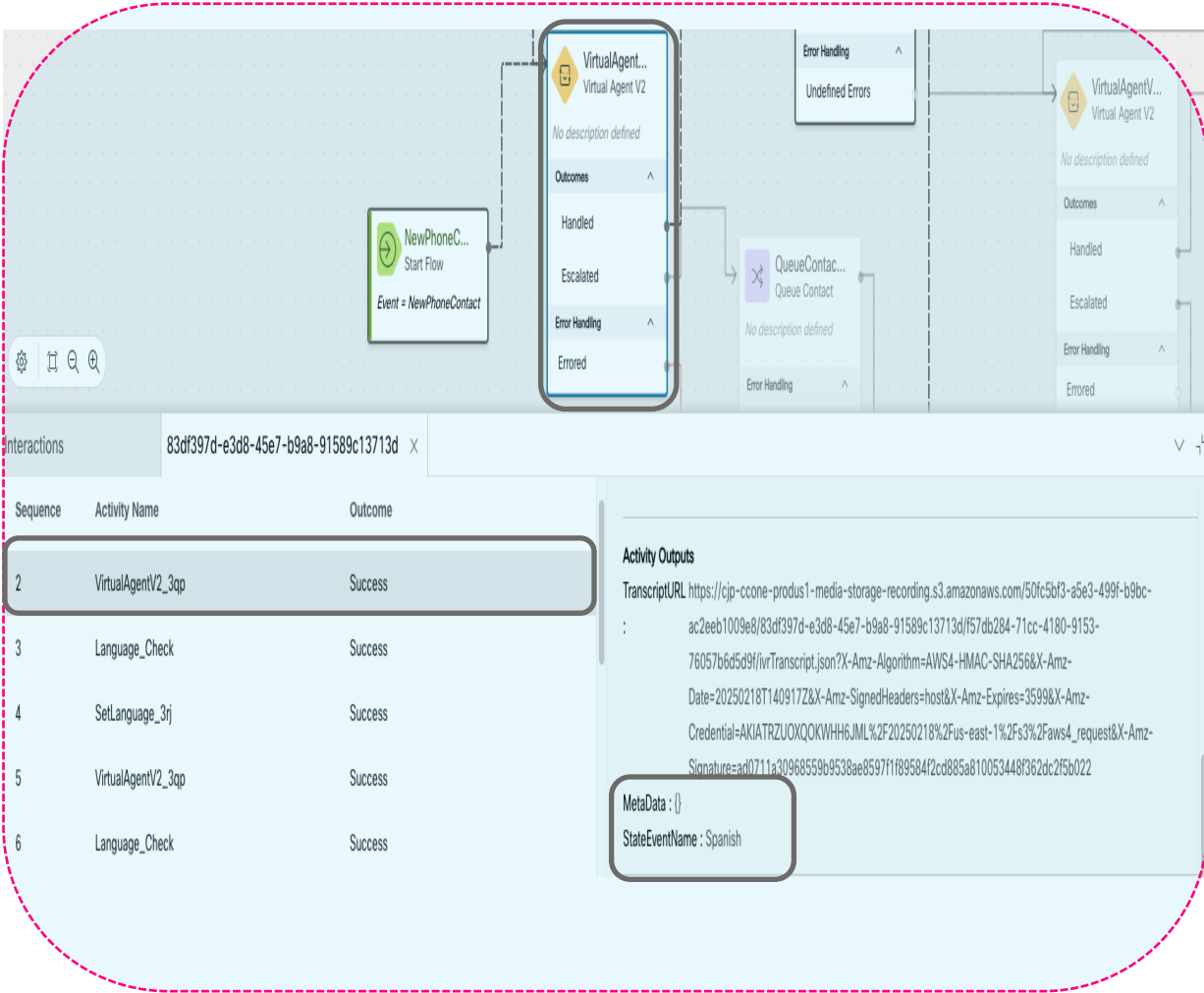
Error Handling

Errored

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKCCT-2555

Scripted AI Agent Voice – Change Language



Scripted AI Agent Configuration - Language

AI Agent Studio Voice Script

Last Updated at 24 Feb, 25 by rtmstestus1

Settings

Testing

Curation

Sessions

History

Analytics

AI agent configuration

Draft

Change the agent configuration

Profile

Script

Handover

Language

Choose agent supported languages

Language	Language code	Enabled	Actions
English	EN	☒	
Spanish	ES	☐	

Add new languages

Select language and locale

Select language

Danish da

Dutch nl

English en

French fr

German de

Italian it

Add

languages

Save changes

+ Add language

Scripted AI Agent Configuration - Language

Main Menu
Configure intent recognition for the agent and link a response.

General information and settings

Intent name *

Main Menu

Settings

☐ Reset slots after completion

☐ End conversation ⓘ

Context

Entry

Add input context

0 items

English (en) Default 9

Spanish (es) 6

Intent and utterances
Add utterances to determine the intent. Link entities for collecting information. Make sure you don't use real customer data.

Add utterance

+ Add

⚡ Generate

Intent identifier ⓘ

menú principal

askTrackingNum
Configure channel-specific responses. Avoid using real customer data.

Response Name *

askTrackingNum

English (en) Default

Spanish (es)

Default response

Conditions ⓘ + New

Default (web)

Voice ⓘ ⓘ +

Incoming event name ⓘ

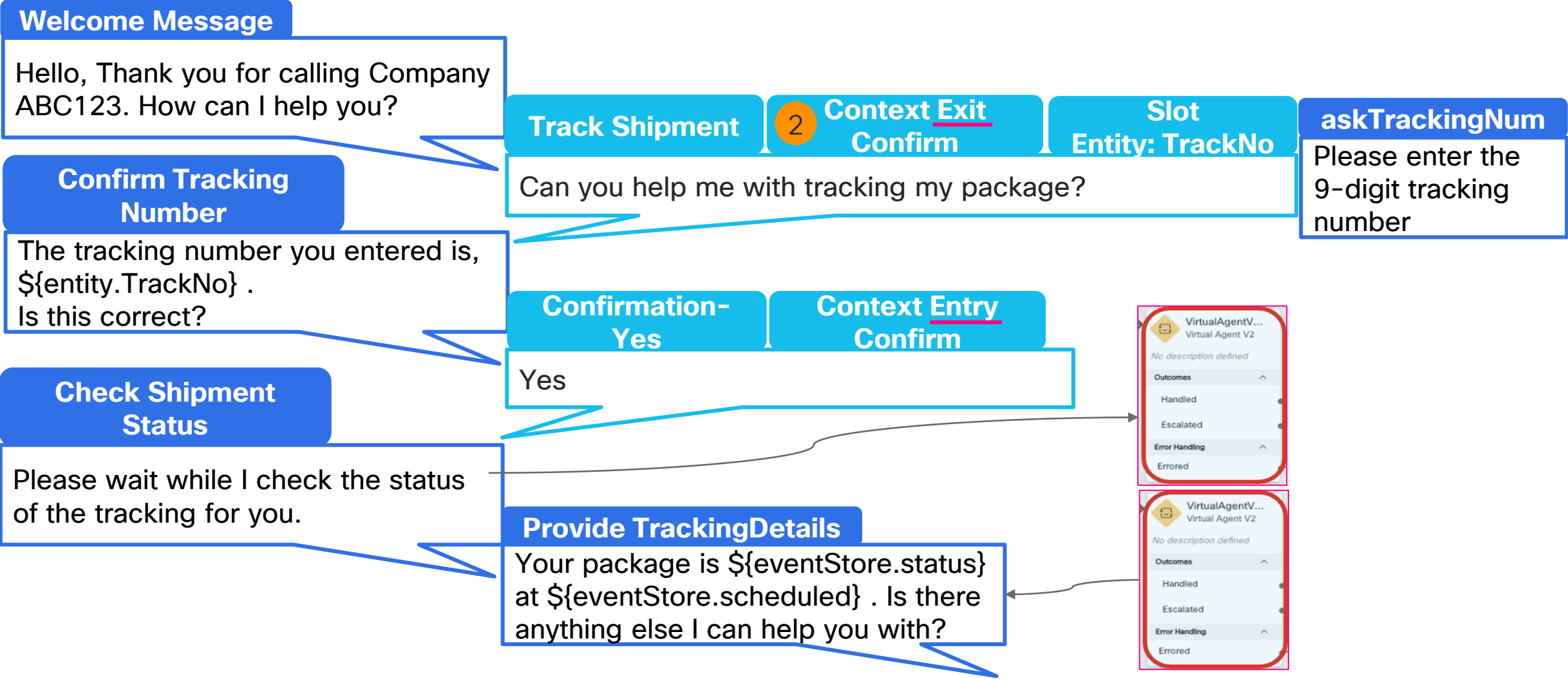
Incoming event name

Voice settings

Text
Variant 1
Please say or enter the 9-digit tracking number

No conditions added

Scripted AI Agent Voice – Shipment Order Status



Scripted AI Agent Voice – Shipment Order Status

Check Shipment Status

Configure channel-specific responses. Avoid using real customer data.

Response Name *

Check Shipment Status

English (en) Default

Spanish (es)

Default response

Conditions ⓘ + New

Default (web)

Voice ⓘ

+

Text

Variant 1

Please wait while I check the status of the tracking for you.

+ Add variant

Custom Event

Event name

shipment_status

Event payload

1 {"trackingNum":"\${entity.TrackNo}"}

Default response

Triggered when no condition is added or fulfilled

VirtualAgentV...

Virtual Agent V2

No description defined

Outcomes

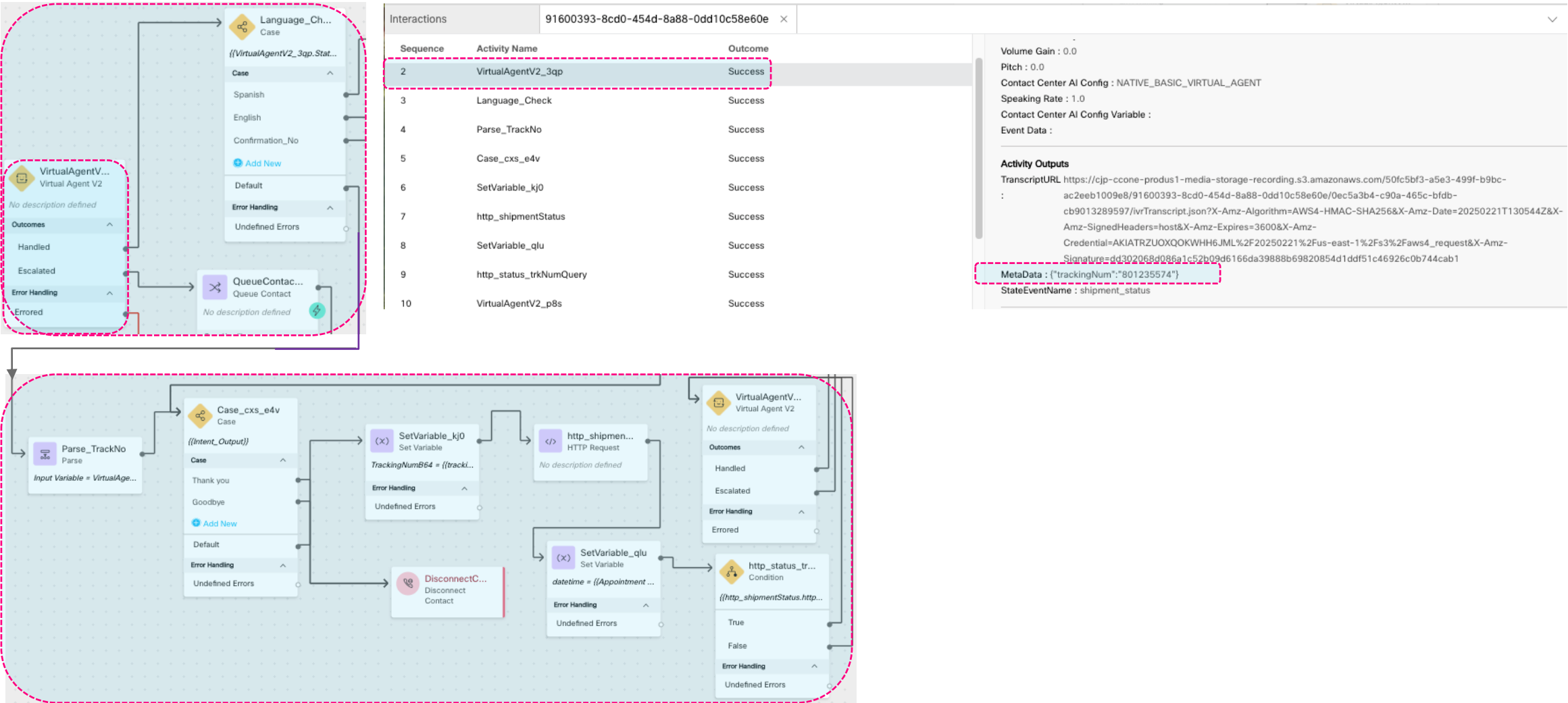
Handled

Escalated

Error Handling

Errored

Scripted AI Agent Voice – Shipment Order Status



Scripted AI Agent Voice – Shipment Order Status

Interactions

Sequence	Activity Name	Outcome
2	VirtualAgentV2_3qp	Success
3	Language_Check	Success
4	Parse_TrackNo	Success
5	Case_cxs_e4v	Success
6	SetVariable_kj0	Success
7	http_shipmentStatus	Success
8	SetVariable_qlu	Success
9	http_status_trkNumQuery	Success

Case_cxs_e4v Configuration

General Settings

- Activity Label: Parse_TrackNo
- Activity Description: Enter a Description

Parse Settings

- Input Variable: VirtualAgentV2_3qp.Metadata
- Content Type: JSON
- Output Variable: trackingNum
- Path Expression: \$.trackingNum

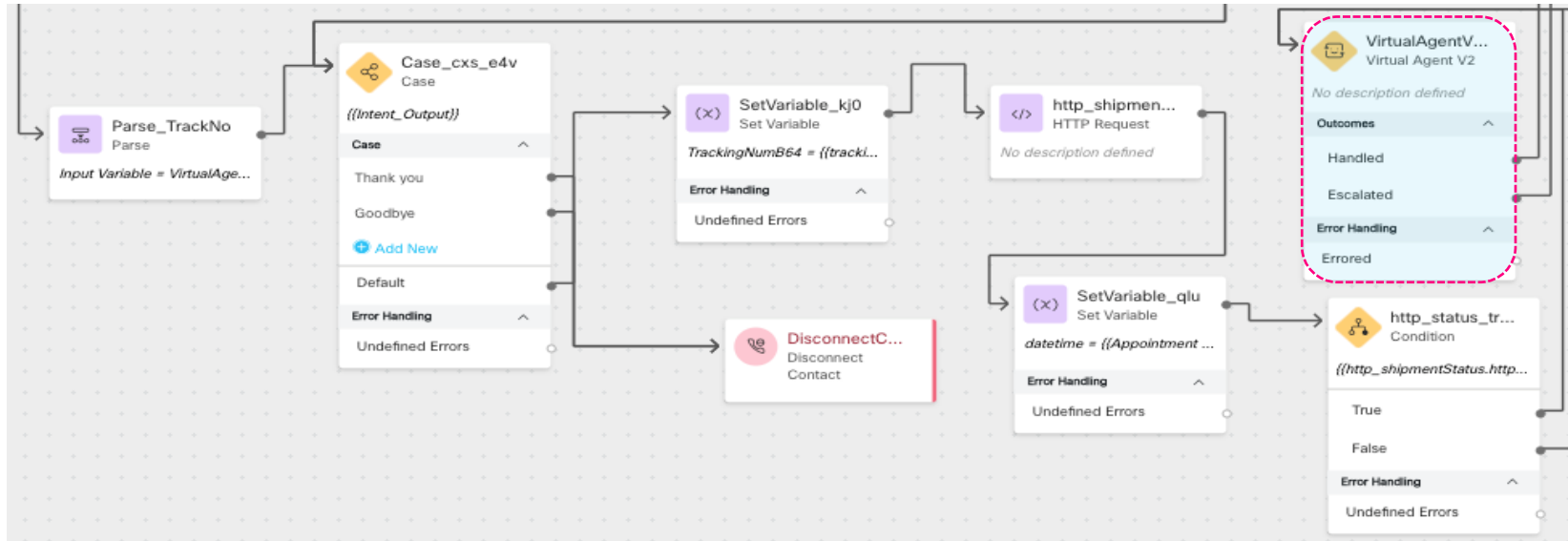
Activity Outputs

```
TranscriptURL https://cjp-ccone-produs1-media-storage-reco:499f-b9bc-ac2eeb1009e8/91600393-8cd0-454d-8a88-0dd10c58e60e/465c-bfdb-cb9013289597/ivrTranscript.json?X-SHA256&X-Amz-Date=20250221T130544Z&X-Amz-Expires=3600&X-Amz-Credential=AKIATRZUOX1%2Fs3%2Faws4_request&X-Amz-Signature=dd302068d086a1c52b09d6166da39f
```

Metadata : {"trackingNum": "801235574"}

StateEventName : shipment_status

Scripted AI Agent Voice – Shipment Order Status



General Settings

Activity Label
VirtualAgentV2_p8s

Activity Description
Enter a Description

Conversational Experience

Choose a Contact Center AI Config from those configured in Control Hub for the conversational experience. Use Global Variables such as Global_Language and Global_VoiceName to override the default language and voice name.

☒ Static Contact Center AI Config
☐ Variable Contact Center AI Config

Contact Center AI Config
Webex AI Agent (Scripted)

Virtual Agent
CompanyABC_Test_AIScript(CompanyABC_AIScri)

[Configure selected Virtual Agent](#)

State Event

An event is a configurable event that can be optionally sent to a third-party AI platform to build the conversational logic. This event can be invoked to initiate a specific flow or to handle certain flow behaviours or error scenarios in the flow.

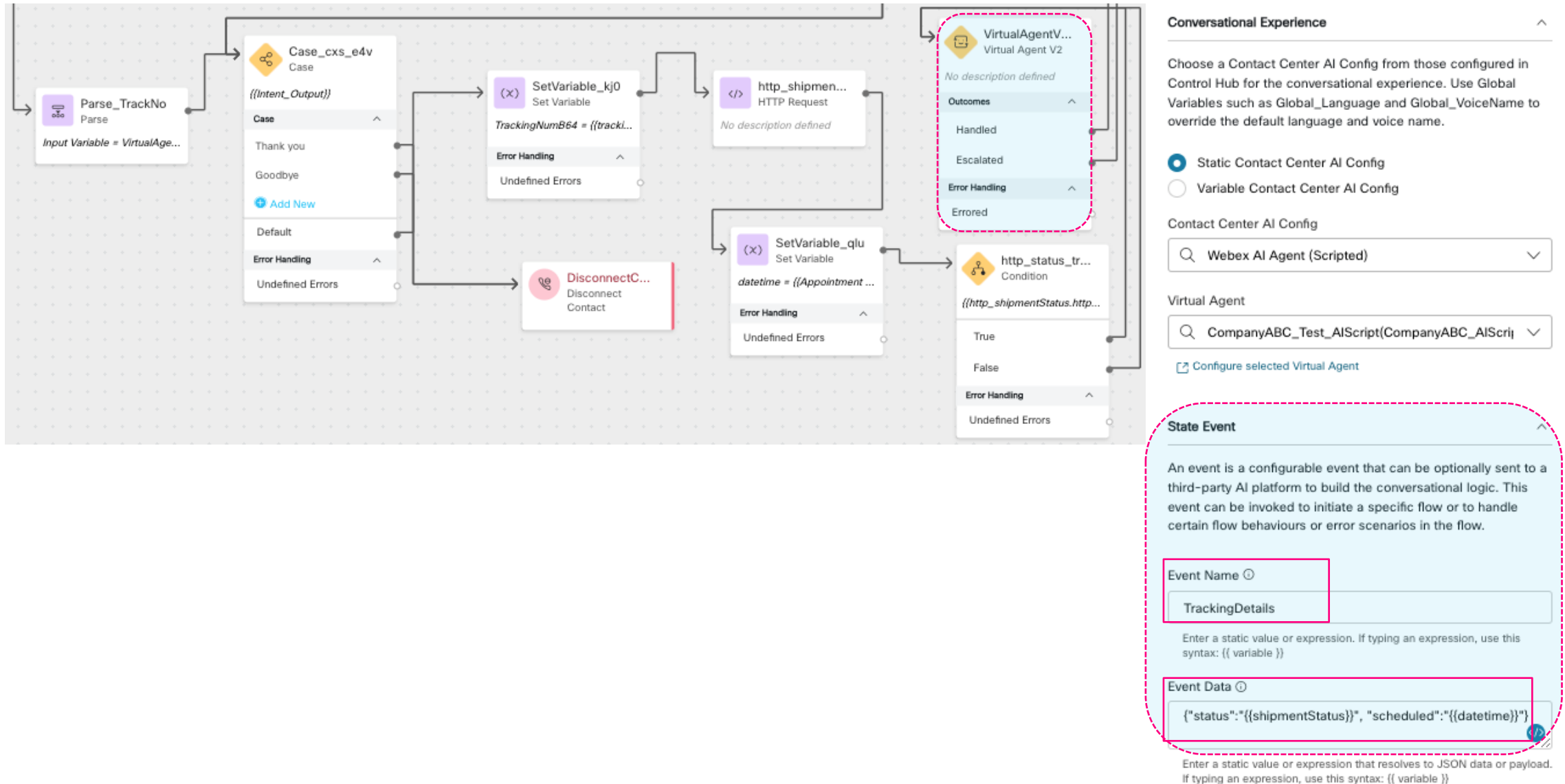
Event Name ⓘ
TrackingDetails

Enter a static value or expression. If typing an expression, use this syntax: {{ variable }}

Event Data ⓘ
{"status": "{{shipmentStatus}}", "scheduled": "{{datetime}}"}
[View](#)

Enter a static value or expression that resolves to JSON data or payload. If typing an expression, use this syntax: {{ variable }}

Scripted AI Agent Voice - Shipment Order Status



Scripted AI Agent Voice – Shipment Order Status

Provide TrackingDetails

Configure channel-specific responses. Avoid using real customer data.

Response Name *

Provide TrackingDetails

English (en) Default

Spanish (es)

Default response

Conditions ⓘ + New

Default (web)

Voice ⓘ

+

No conditions added

Incoming event name ⓘ

TrackingDetails

Voice settings

Text

Variant 1

Your package is \${eventStore.status} at \${eventStore.scheduled} . Is there anything else I can help you with?

+ Add variant

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKCCT-2555

Scripted AI Agent Voice – Shipment Order Status

Session ID: 67da3418-e56c-42b6-970d-b189d74a4672Consumer ID: 89c25999-5177-4a70-a5cb-04e58e7873f8Total Messages: 11Last updated at: Feb 21 '25 1:11 PM

Search

Hello, Thank you for calling Company ABC 123. How can I help you?

1:11:05 PM, Feb 21, 2025

Txn ID: bef1bc8c69fb49bbaf8b44e6ac4eb088

Check my shipment

1:11:15 PM, Feb 21, 2025

Please say or enter the 9-digit tracking number

1:11:15 PM, Feb 21, 2025

Txn ID: e9bb9d736dd64e07e13aaaaac09a110c

801235574

1:11:25 PM, Feb 21, 2025

The tracking number you entered is, 801235574 . Is this correct?

1:11:25 PM, Feb 21, 2025

Txn ID: 22168083d8a544adu6693b7e2e8234ab

Yes

Transaction info

Expand all

Intents identified

Confirmation-Yes1

Slots

No slots available

Entities identified

TrackNo: 801235574

Algorithm results

Other info

Processed query: yes

Language detection provider: google

Language detected: English (en)

Agent handover

Agent handover by rules

Response name: Check Shipment Status

Response type: Conditional response

Response condition: default

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKCCT-2555

Scripted AI Agent Voice – Shipment Order Status

Txn ID: 22168083d8a544ada6693b7e2e8234ab

Yes

1:11:36 PM, Feb 21, 2025

Please wait while I check the status of the tracking for you.

```
1 {
2   "Data": {
3     "Params": {
4       "trackingNum": "801235574"
5     }
6   },
7   "Event_Name": "shipment_status"
8 }
```

Debug logs

Log @ | appserver

VirtualAgentV...
Virtual Agent V2

No description defined

Outcomes

Handled

Escalated

Error Handling

Errored

Txn ID: 2bf07e9ca60041cbbbc012cb24e549df5

Incoming event name
TrackingDetails

```
1 {
2   "scheduled": "Friday 17 January 2025 at 2 36",
3   "status": "APPOINTMENT SCHEDULED"
4 }
```

1:11:42 PM, Feb 21, 2025

Your package is APPOINTMENT SCHEDULED at Friday 17 January 2025 at 2 36 . Is there anything else I can help you with?

1:11:42 PM, Feb 21, 2025

Debug logs

Log @ | appserver

VirtualAgentV...
Virtual Agent V2

No description defined

Outcomes

Handled

Escalated

Error Handling

Errored

Txn ID: d803def9da6e418dbc2f4f891363a08a

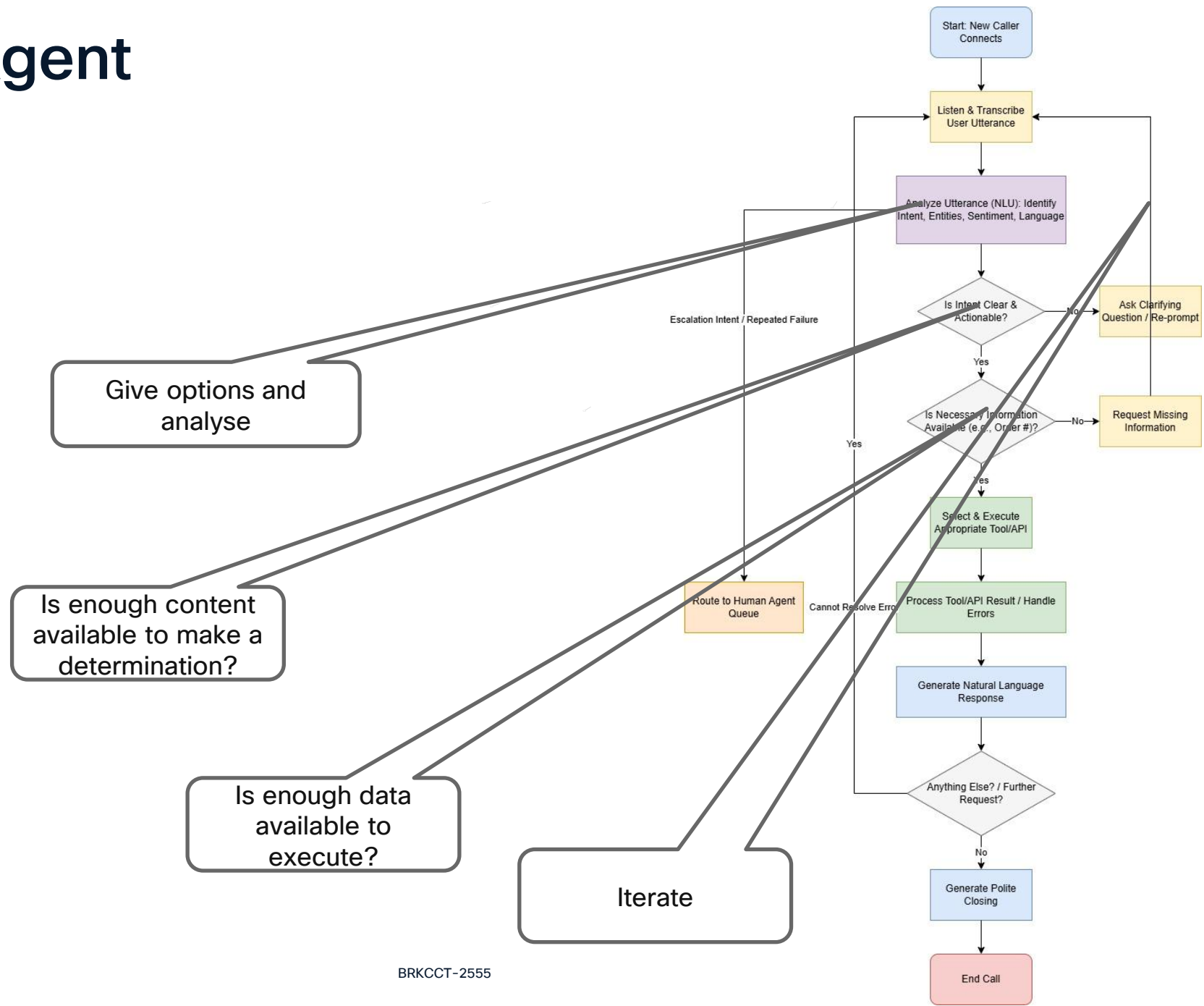
No goodbye

1:11:55 PM, Feb 21, 2025

Goodbye and take care!

Autonomous AI Agent!

Autonomous Agent



Let's Create One...

Create an AI agent

Choose how you want to get started



Start from scratch

Build a new AI agent from the ground up.

Start from the beginning

Or select a template for a quick setup.



Banking

Scripted

Updated on 9 Aug, 24



Airlines

Scripted

Updated on 6 Aug, 24



Telecom

Scripted

Updated on 3 Feb, 25

Agent Selection

Autonomous it is

Create an AI agent

Select the agent type and add the essential details

Select the type of agent you are building

Autonomous

Uses generative AI to create dynamic responses.

Scripted

Uses natural language processing to follow your set logic and responses.

💡

What to expect from your agent selection

▪ Customer experience:

Natural, flowing conversations that adapt flexibility to different needs. Occasional inaccuracies can happen because of how generated AI works.

▪ Setup:

Define your agent's goal using natural language. Add actions to connect your agent with external systems, and link a knowledge base to help it answer questions.

Add the essential details

Agent name *

Enter customer-facing name

×

System ID *

Enter unique system ID

×

AI engine *

Webex AI Pro 1.0

▼

Agent's goal * ⓘ

What is your agent's main purpose?

Insert example

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKCT-2555

Define AI Agent Personality

←

hoesser-auton

Last Updated at 4 Apr, 25 by admin

Configuration

Sessions

History

Analytics

AI agent configuration Draft

Change the agent configuration

Profile

Knowledge

Actions

Language

Agent name *

hoesser-auton

System ID *

hoesser-auton-GGOkmQMK

Agent's goal * ⓘ

Insert example

You are a friendly and efficient AI Agent. You are focused on answering product questions, providing answers to general FAQs and managing orders for the Cisco Store.

Instructions ⓘ

Insert example

Answer any questions from the user in a friendly and professional manner, referring to the relevant Knowledge sources as appropriate. You will also be able to manage any existing orders as follows: Collect an Order ID Number ("orderId") to be able to determine what order is being referenced. These are your available actions, once the "orderId" is known:
1. [fetch_status] - use the "orderId" to fetch the status of the order.
2. [change_date] - change the desired delivery date.
3. [safe_area] - add or update the specified safe area for the courier to leave the package.

URL for agent profile image *

https://aiagent.webexbotbuilder.com/static/assets/img/...

AI engine *

Webex AI Pro 1.0

Welcome message *

Hi there, how can I help you?

Give it a resume

Detailed Instructions

Do's and Don'ts when writing goals

Do's

- Keep the goal short and concise.
- Focus on the overall function or purpose of the AI Agent.
- Consider the end result or benefit for the user.
- Use clear and concise language.
- Ensure the goal aligns with the actions and capabilities of the AI Agent.

Don'ts

- Don't include specific details like dates or user information.
- Avoid mentioning particular actions or implementation methods.
- Don't use technical jargon.
- Avoid long and complicated goal statements.
- Avoid using ambiguous or vague language.

Detailed Instructions

Define the Entity

Point to the WxConnect Service/Flow to execute the action

Update action

Enable your AI agent to connect with external systems and perform more complex tasks.

General information

Action name *

change_Date

Action description *

Collect the orderId (if not already known) and ask the user for their new preferred delivery date. The delivery date will be used to overwrite the "deliveryETA" value in this action. Note that the user can change the delivery date, even if the order has already been shipped.

Action scope *

Slot filling and fulfillment

Slot filling

Add input entities in a table or define input parameters in JSON for slot filling to ensure the AI agent gathers all necessary information.

Input entities

Entity Name	Type	Value	Description	Example	Required	Controls
new_deliveryETA	string	-	delivery date in us date format	-	Yes	 
orderId	string	-	orderId used to change the the ETA	-	Yes	 

Webex Connect Flow Builder Fulfillment

Determine how to handle customer requests or resolve issues.

[Learn more about Webex Connect Flow Builder for fulfillment](#)

Select service *

My First Service

Select a flow *

changeDate

WxConnect as the Orchestrator

Please attend BRKCCT-2557 Implementing automation using AI Agent and AI Assistant actions.

Create the action with AI Agent as the trigger

Dashboard

Flows

Rules

API

Settings

Create Flow

Flow Builder

Flow builder is a visual designer with a library of nodes that you can drag and drop to create and test interactive customer journeys with little to no code.

[Check out our guide to building flows here.](#)

If you've got more questions after reading through it, just ask. We're always here to help.

Create Flow

Search Flows

Sort By Newest

Flow execution data shown below is for last 30 days

Trigger	Flow	Status	State	Executions	Actions
	v2Auto Flow Id:56720	Live		3	
	safe_area Flow Id:56718	Live		0	
	changeDate Flow Id:56715	Live		1	
	FetchStatus Flow Id:56712	Live		3	
	SMS Ingress Flow Id:56666	Live		2	
	V1 Flow Id:56517	Live		27	

Data Handling

Data sent to AI Agent

Entity Name	Type
new_deliveryETA	string
orderid	string

Payload

AI Agent initiated flow execution outcome are notified to AI Agent. The default notification payload is configured in the flow settings. If you want to include additional information in the notification payload, refer to the flow outcome settings. Waiting operations such as Delay, Social Hour, and Receive nodes are not permitted in AI Agent flows.

End Point URL

https://hooks.us.webexconnect.io/flows/56715/trigger/aiage

PROVIDE SAMPLE JSON

```
1 {
2   "new_deliveryETA": "",
3   "orderId": ""
4 }
```

OUTPUT VARIABLES

PARSED VARIABLES(2)

new_deliveryETA:

orderId:

Data returned to AI Agent

HTTP Request

Configuration

Transition Actions (Optional)

Make GET, POST, PUT, PATCH and DELETE requests to your application

Method

GET

Endpoint URL

https://cjpdata.wbx.ninja/?number= \${n2.aiAgent.orderId}

Header

Authorization

Bearer hoesser@cisco.com

Connection Timeout

Request Timeout

Output Variables

JSON

Output Variable Name

consentSMS

safeLocation

name

phoneNumber

orderId

deliveryAddress

timeZone

altDate2

altDate1

productName

deliveryETA

deliveryStatus

Response Entity

Body

Body

Body

Body

Body

Body

Body

Body

Body

Body

Body

Response Path

\$.consentSMS

\$.safeLocation

\$.name

\$.phoneNumber

\$.orderId

\$.deliveryAddress

\$.timeZone

\$.altDate2

\$.altDate1

\$.productName

\$.deliveryETA

\$.deliveryStatus

HTTP Request

Configuration

Transition Actions (Optional)

Make GET, POST, PUT, PATCH and DELETE requests to your application

Method

PATCH

Endpoint URL

https://cjpdata.wbx.ninja?number= \${n2.aiAgent.orderId}

Header

Content-Type

application/json

Authorization

hoesser@cisco.com

Body

{
 "deliveryETA": "\${n2.aiAgent.new_deliveryETA}"
}

Connection Timeout

Request Timeout

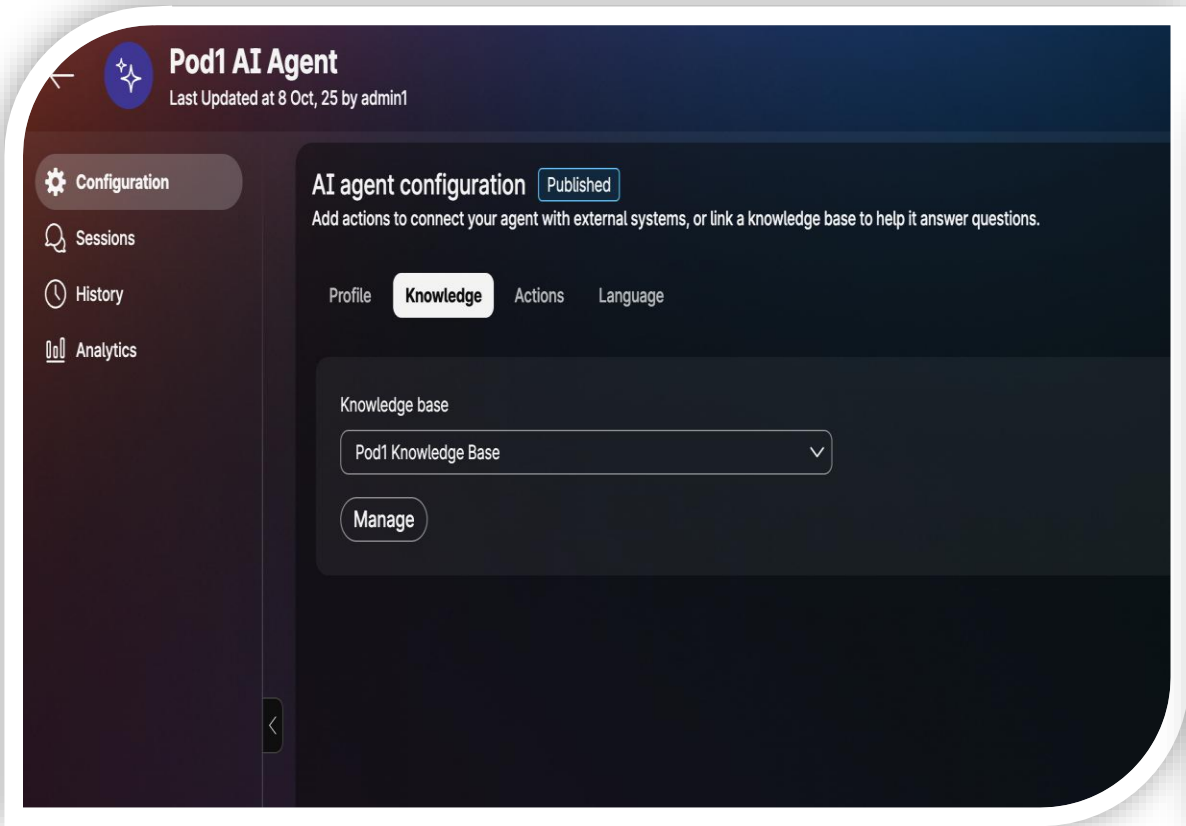
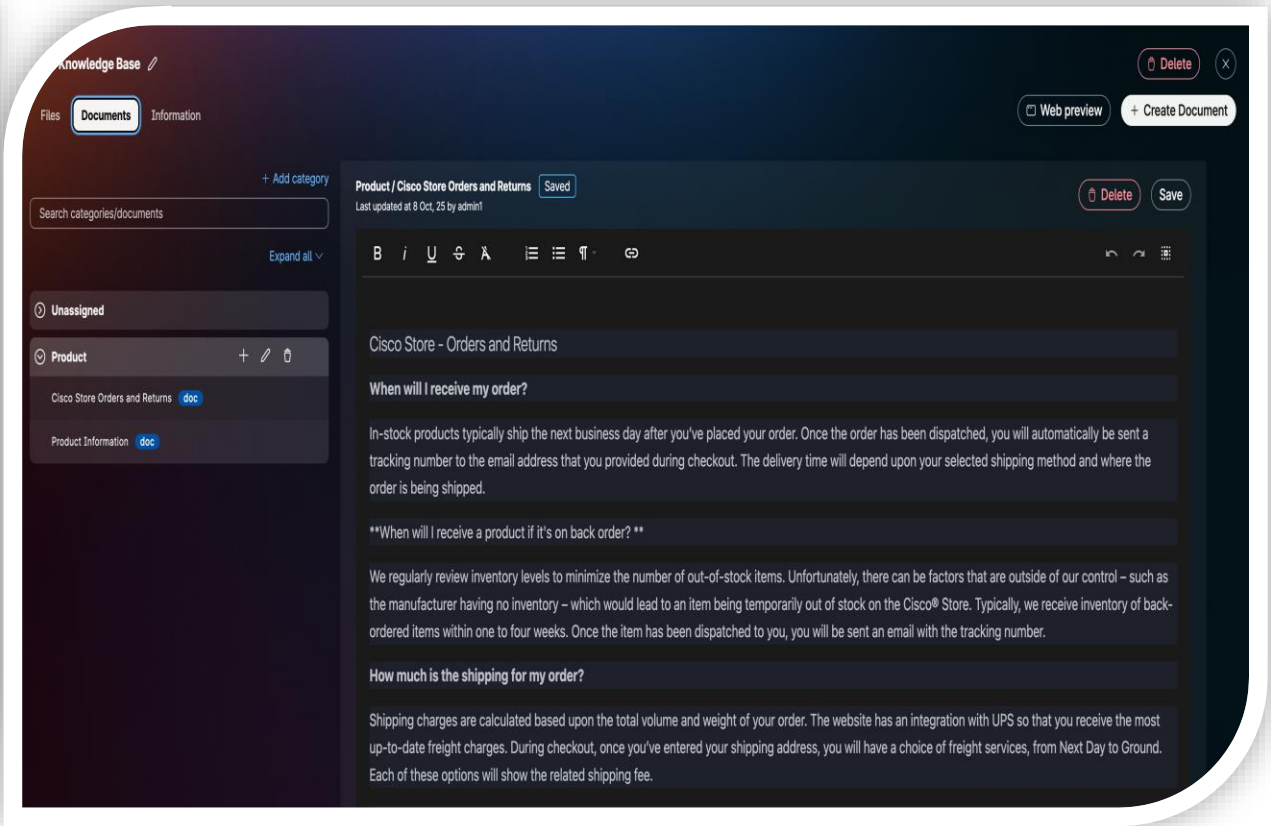
Proxy Address (Optional)

Output Variables

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKCCT-2555

Boost the AI Agent with Knowledge

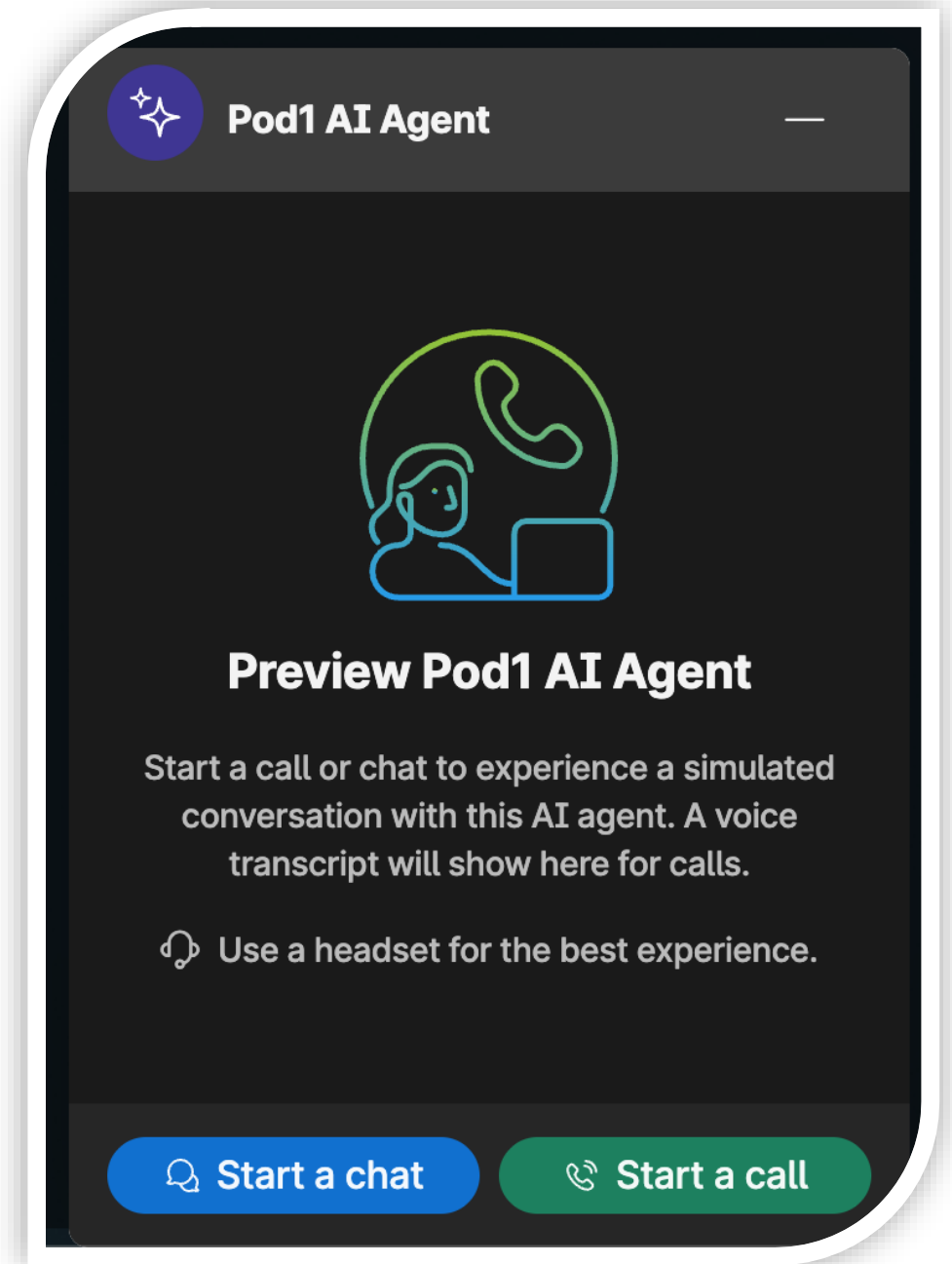


Recommendations for managing the Knowledge Bases

- Keep it precise and tailored to the purpose of AI Agent
- Organize content logically. Use categories when creating the KB document in AI Agent studio.
- When uploading files, avoid any conflicting or duplicate information across documents.
- Check the quality of the document before uploading
- Split larger files into smaller if needed for better performance.
- Periodically review the knowledge and update whenever required.

Preview AI Agent

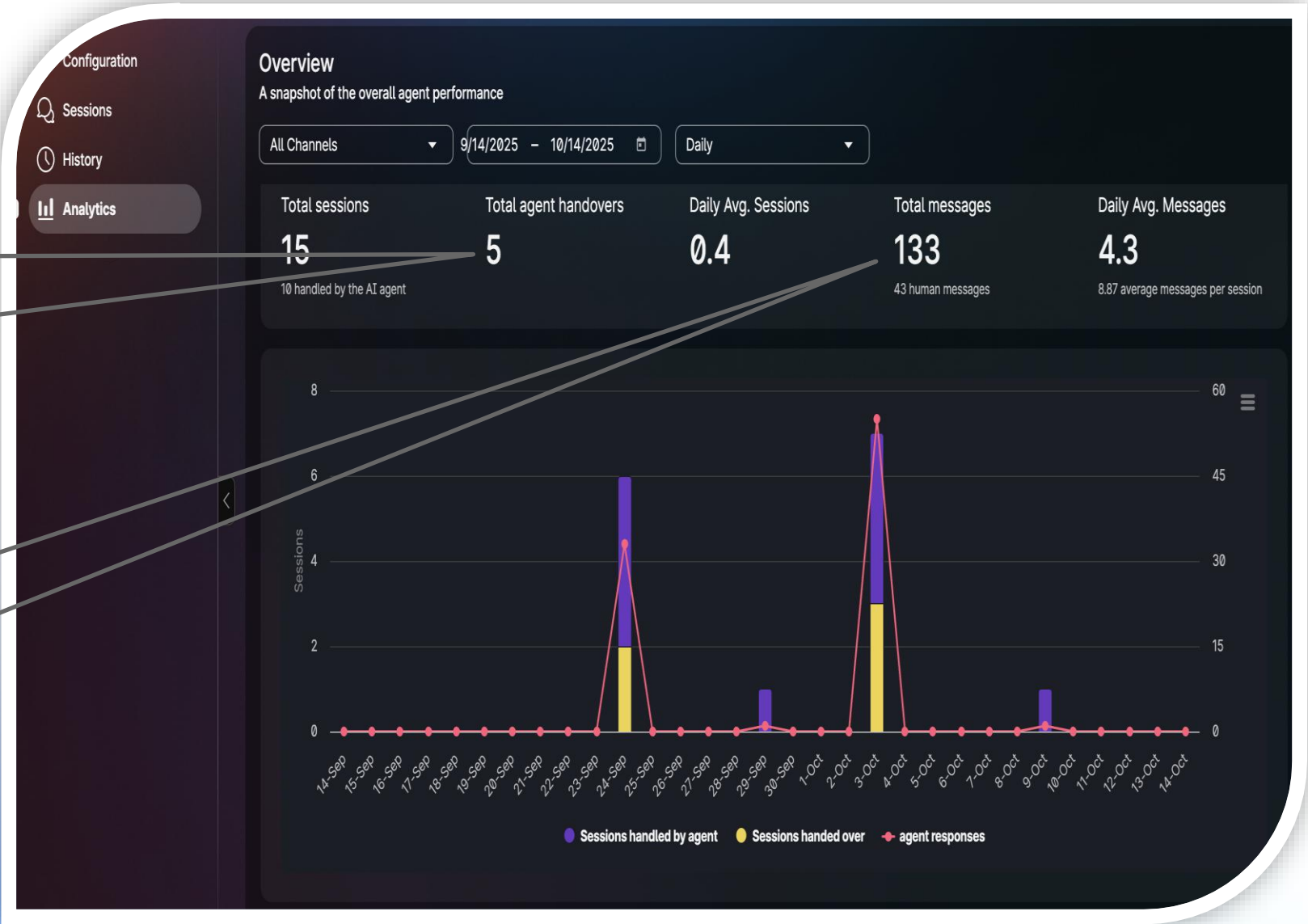
- Preview allows you to test the AI Agent within the studio
- AI Agent preview provides mechanism to test using both voice and digital medium.
- Actions are executed as part of the preview testing.



Analytics

Sessions handed over as agent escalations

AI Agent responses to Users Intent



Troubleshooting

Pod04 AI Agent

Last Updated at 14 Oct, 25 by admin4

Preview

Configuration

Sessions

History

Analytics

Sessions

Sessions capture all interactions with your AI agent, providing insight into what happens behind the scenes.

Refresh

Refine Results

Session ID

Consumer ID

Interaction ID

Filter Channels

Select channels to display

Last updated

Metadata

Hide test sessions

Agent handover happened

Error occurred

Submit

Clear

Channels	Session ID	Messages	Updated at	Metadata
	003750eb-9d19-4ebc-8508-274c9cd317af	8	14 Oct 25, 12:54 PM	
	0bd6c46c-e7a2-4c11-b54c-d20443595d0b	2	14 Oct 25, 11:10 AM	
	605e8b2f-c125-4916-847c-0bada2b69263	13	14 Oct 25, 10:46 AM	
	21c79107-11c3-4ee4-b566-6fa05008569b	11	14 Oct 25, 10:20 AM	

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKCCT-2555

Troubleshooting

Session ID: 605e8b2f-c125-4916-847c-0bada2b69263

Consumer ID: 9d263bd5-4112-46d5-9304-8038eb3a5226 • Total Messages: 13

Last updated at: Oct 14 '25 10:46 AM

Search

You do not need to include the country code in your Order ID. Please provide the Order ID in the phone number format, and I will check the status for you.

10:44:30 AM, Oct 14, 2025

Txn ID: 883cbbbfa0d145dd9ddacddd9eeb2e37

12163332790

10:44:40 AM, Oct 14, 2025

Performing action "fetch_status"

Hello Mark, thank you for providing your Order ID: 12163332790. Your order for the Core Trio QI Charger is currently being processed. The estimated delivery date is November 1, 2025. You will be notified with a tracking number once your order has shipped.

Is there anything else I can assist you with regarding your order?

10:44:45 AM, Oct 14, 2025

Txn ID: 9fd4a51624e848748293647b7a5f05f4

Collapse all

Action performed

fetch_status

Slot filling:

actionName: fetch_status

Required: true

Entity Type: string

Entity description: The value is set to "fetch_status" when this action is called.

orderId: 12163332790

Required: true

Entity Type: string

Entity description: The "orderId" is used to fetch the user's order status from the connected Order Management Platform.

Fulfillment:

Success (0.9s)

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKCCT-2555

Troubleshooting

Session ID: 605e8b2f-c125-4916-847c-0bada2b69263

Consumer ID: 9d263bd5-4112-46d5-9304-8038eb3a5226 • Total Messages: 13

Last updated at: Oct 14 '25 10:46 AM

Search

You do not need to include the country code in your Order ID. Please provide the Order ID in the phone number format, and I will check the status for you.

10:44:30 AM, Oct 14, 2025

Txn ID: 883cbbbfa0d145dd9ddacddd9eeb2e37

12163332790

10:44:40 AM, Oct 14, 2025

Performing action "fetch_status"

Hello Mark, thank you for providing your Order ID: 12163332790. Your order for the Core Trio QI Charger is currently being processed. The estimated delivery date is November 1, 2025. You will be notified with a tracking number once your order has shipped.

Is there anything else I can assist you with regarding your order?

10:44:45 AM, Oct 14, 2025

Txn ID: 9fd4a51624e848748293647b7a5f05f4

Entity type: string

Entity description: The "orderId" is used to fetch the user's order status from the connected Order Management Platform.

Fulfillment:

Success (0.9s)

Service and flow info:

Service: Pod 04

Flow: Pod04 All Actions Flow

Fulfillment output:

Transaction ID: b757cfef-6bbc-49eb-b028-bde08a12b3ee

Size: 494

Output:

1 {

2 "Outcome": "success",

3 "altDate1": "12/01/2025",

4 "altDate2": "1/02/2026",

5 "consentSMS": "true",

6 "deliveryAddress": "300 N

Commons Blvd, Mayfield

Heights, OH 44143",

7 "deliveryETA": "11/1/2025",

8 "deliveryStatus":

"*success*"

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKCCT-2555

Troubleshooting

Session ID: 605e8b2f-c125-4916-847c-0bada2b69263

Consumer ID: 9d263bd5-4112-46d5-9304-8038eb3a5226 • Total Messages: 13

Last updated at: Oct 14 '25 10:46 AM

Search

You do not need to include the country code in your Order ID. Please provide the Order ID in the phone number format, and I will check the status for you.

10:44:30 AM, Oct 14, 2025

Txn ID: 883cbbbfa0d145dd9ddacddd9eeb2e37

12163332790

10:44:40 AM, Oct 14, 2025

Performing action "fetch_status"

Hello Mark, thank you for providing your Order ID: 12163332790. Your order for the Core Trio QI Charger is currently being processed. The estimated delivery date is November 1, 2025. You will be notified with a tracking number once your order has shipped.

Is there anything else I can assist you with regarding your order?

10:44:45 AM, Oct 14, 2025

Txn ID: 9fd4a51624e848748293647b7a5f05f4

Knowledge utilized

Pod04 Knowledge Base

Orders and Returns 0.79

Page 1: Cisco Store - Orders and Returns When will I receive my order? In-stock products typically ship the next business day after you've placed your order. Once the order has been dispatched, you will automatically be sent a tracking number to the email address that you provided during checkout. The delivery time will depend upon your selected shipping method and where the order is being shipped. **When will I receive a product if it's on back order? ** We regularly review inventory levels to minimize the number of out-of-stock items. Unfortunately, there can be factors that are outside of our control – such as the manufacturer having no inventory – which would lead to an item being temporarily out of stock on the Cisco® Store. Typically, we receive inventory of back-ordered items within one to four weeks. Once the item has been dispatched to you, you will be sent an email with the tracking number. How much is the shipping for my order? Shipping charges are calculated based upon the total volume and weight of your order. The website has an integration with UPS so that you receive the most up-to-date freight charges. During checkout, once you've entered your shipping address, you will have a choice of freight services, from Next Day to Ground. Each of these options

© 2025 Cisco and/or its affiliates. All rights reserved.

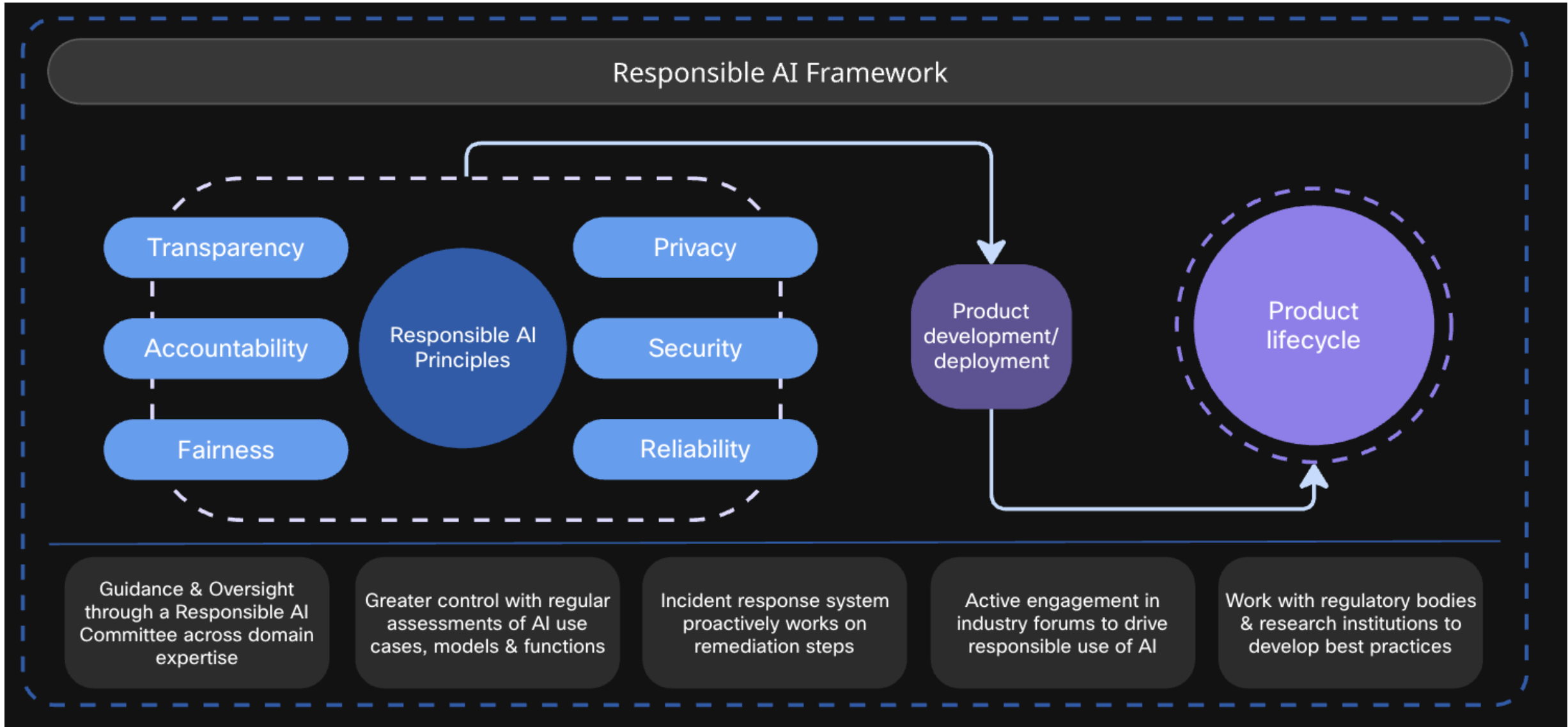
BRKCCT-2555

Cisco's AI Security Protocols & Guardrails Service!

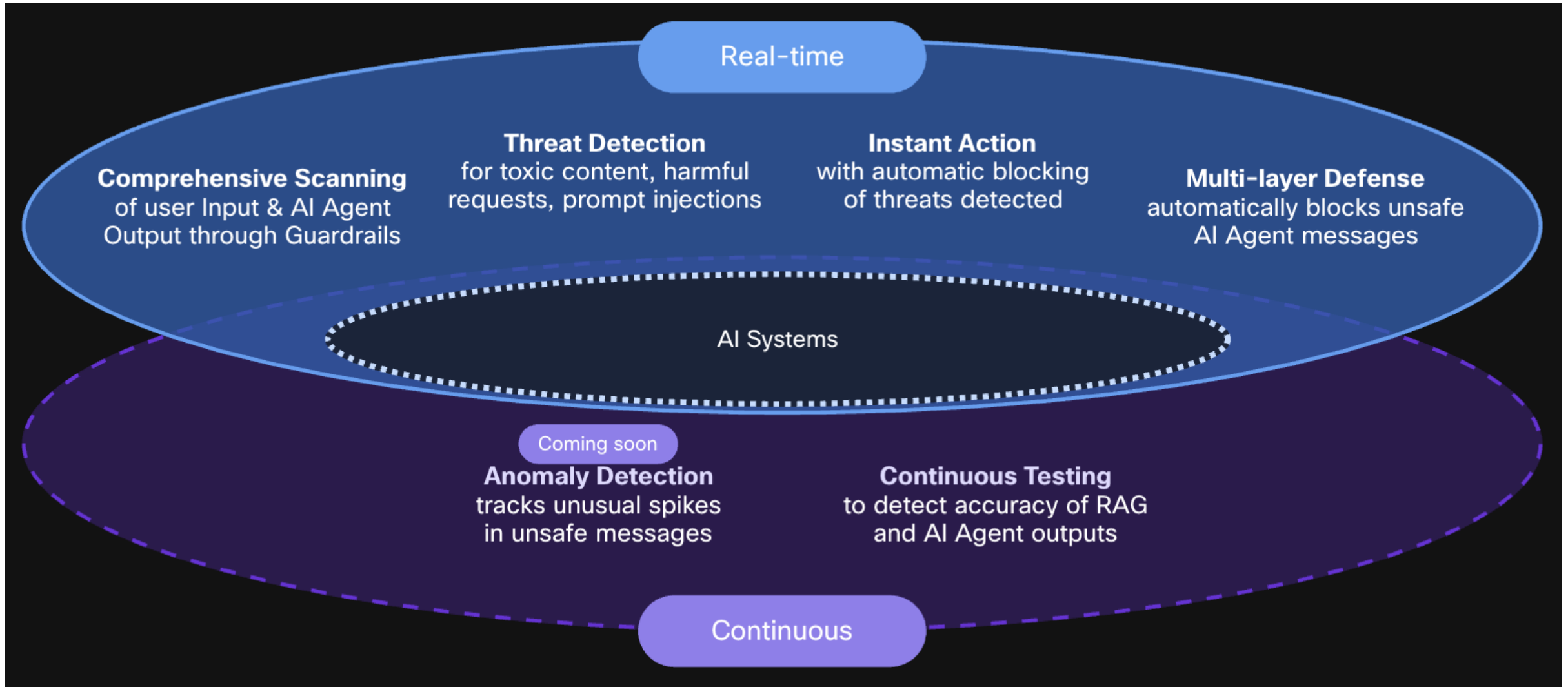
**While AI unlocks new possibilities,
trust is not optional.**

**That's why every agent we deploy
is governed by
Cisco's Responsible AI framework
designed for real-world risk.**

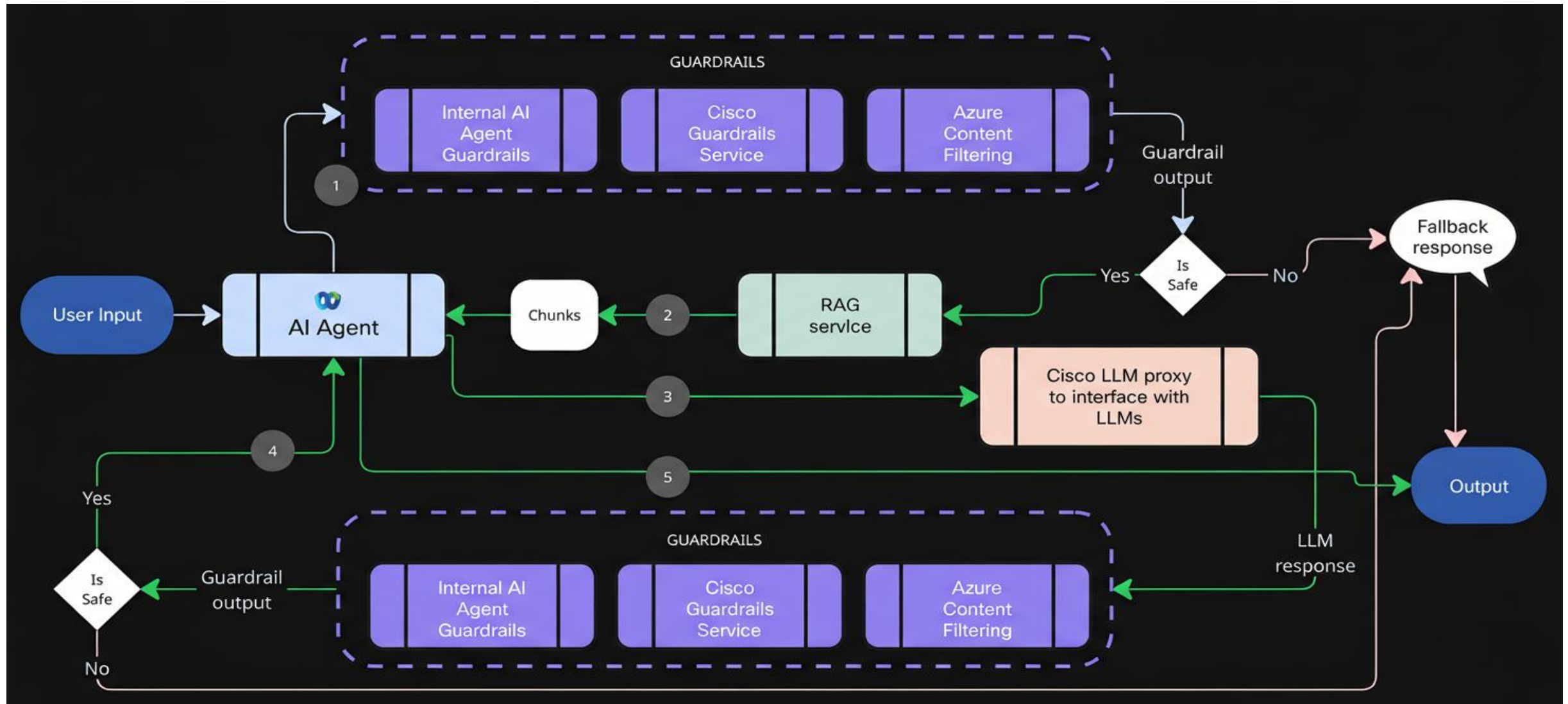
Each feature powered by AI undergoes an AI Impact Assessment to ensure adherence to the framework



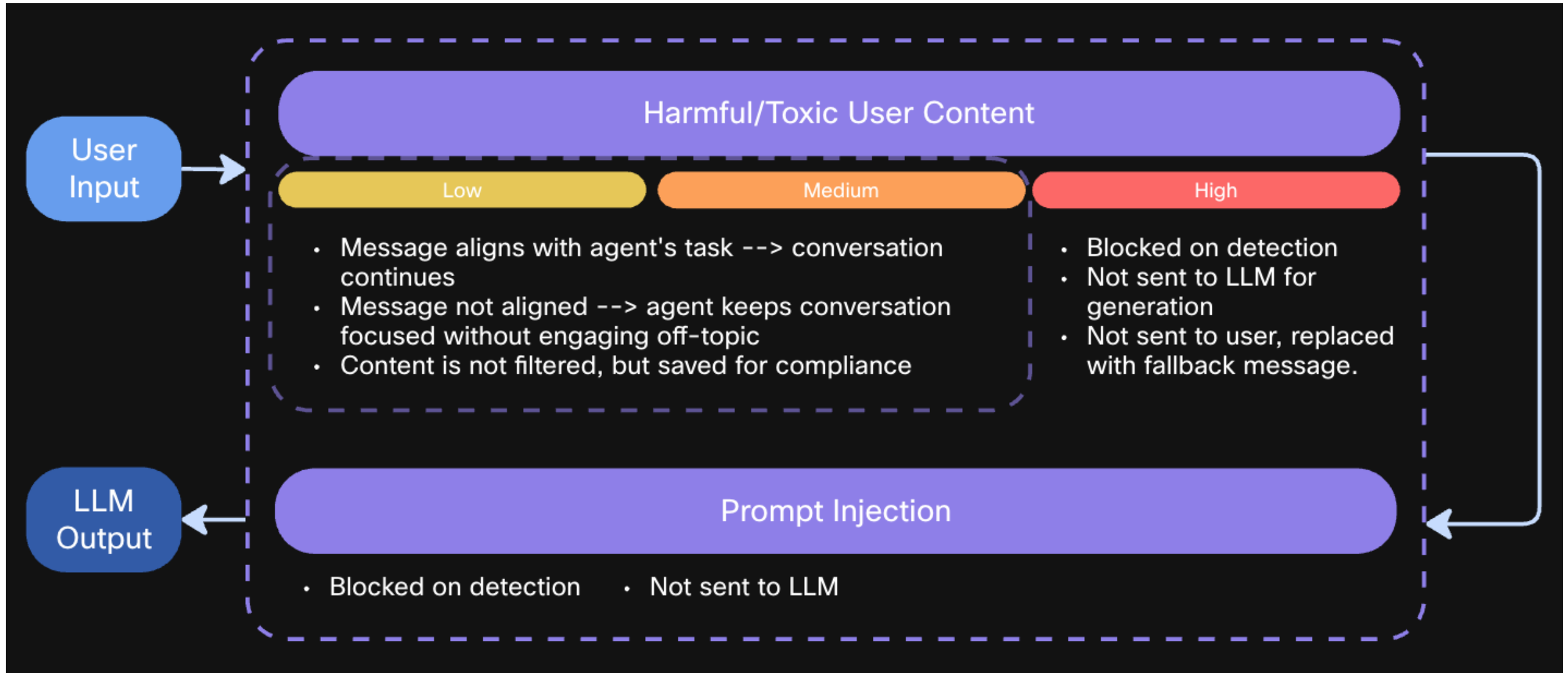
This is not a one-time exercise, we take an always-on approach with real-time and background monitoring.



Every message is validated by three lines of defense within our secure AI Agent framework



Together, these guardrails protect every exchange between the user and LLM



Rails available today

Toxicity - Default

Basic toxic speech detection focused on clearly harmful content. Detects toxic speech with a limited set of classes:

- toxic
- obscene
- threat
- insult
- identity hate

Toxicity - Expanded

Enhanced protection including demographic and identity-based harmful content. An expanded toxic speech detector, including additional classes beyond those in toxicity_default:

- male
- female
- homosexual, gay or lesbian
- christian
- jewish
- muslim
- black
- white
- psychiatric or mental illness

Harm

Identifies content that may lead to harm, such as:

- violent crimes
- non-violent crimes
- sex-related crimes
- child sexual exploitation
- specialized advice
- privacy violations
- intellectual property
- indiscriminate weapons
- hate
- suicide and self harm
- sexual content

Jailbreak

Preventing attempts to manipulate the LLM's behavior.

Detecting attempts to override the LLM's core functions and safety features.

Cisco Guardrails are built for enterprise trust

Built-in enforcement

Guardrails are wired directly into agent logic — monitoring input, output, and tool use as it happens.

Red-Team Validated

Defense is tested continuously with real-world threat scenarios, not one-time checks.

Real-Time Blocking

Guardrails act immediately — blocking risk before it can cause exposure or impact.

Audit-Ready Logging

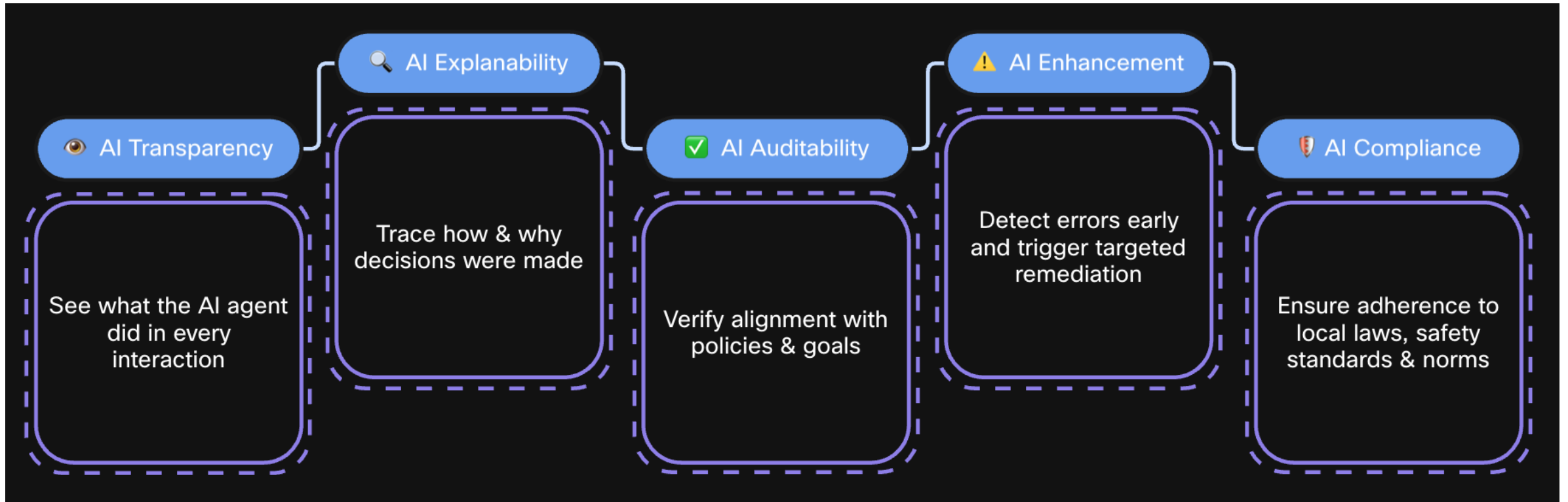
Customers have traceability for every guardrail event, making oversight and reporting simple.

Benchmarking Assessment

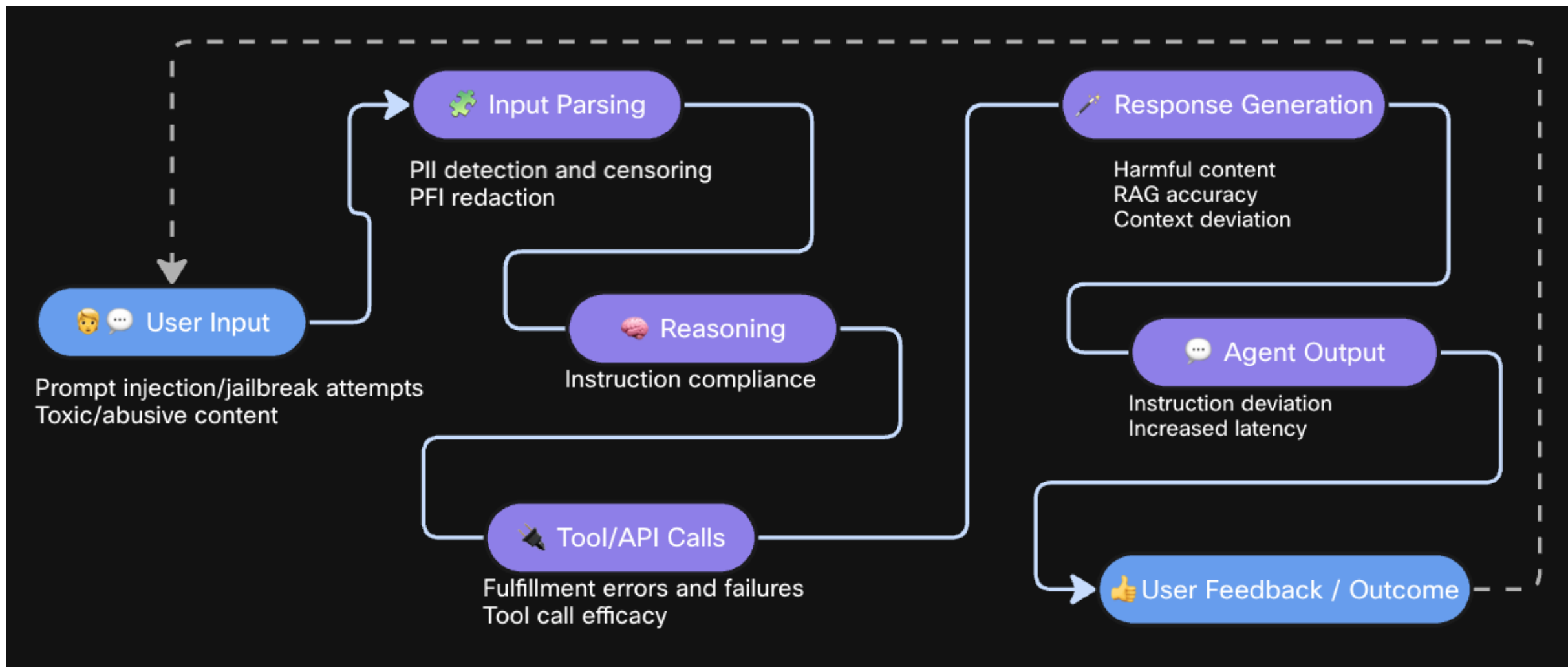
**Ranks higher on Jailbreaking
than Azure
& scores above 92% for recall
& precision on hate data**

Run-Time Visibility

Building trust in AI systems starts with full visibility



We already monitor every stage of the AI Agent lifecycle

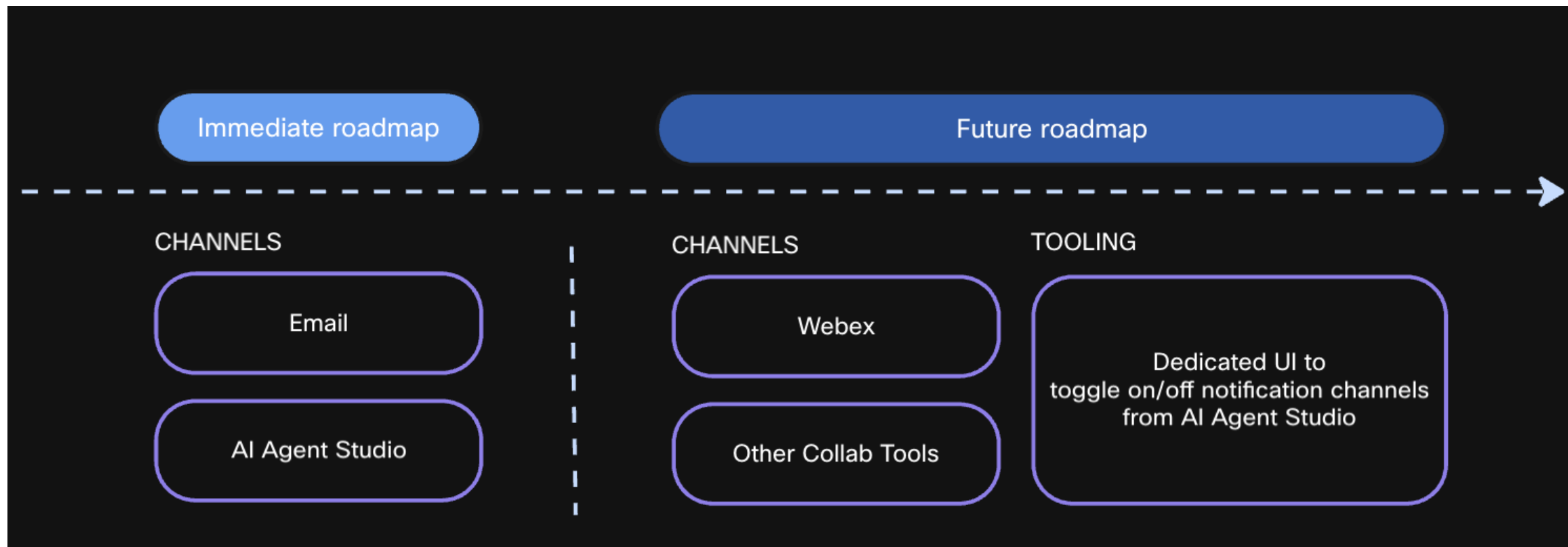


Run-time intelligence available today

Security		
Prompt injection/jailbreak attempts	User message attempting to override agent instructions	
PII detection	User or AI agent messages potentially contain personal info	
Toxic/abusive content	User or AI agent messages contain toxic or abusive content	
Harmful content	User or AI agent messages contain the intent to cause harm	
General		
Total sessions	Flagged sessions	Latency
Total messages	Flagged messages	Sentiment

Performance	
Instruction deviation	Agent not adhering to configured goals and instructions. LLM as judge used to detect this.
Context deviation	AI agent output not relevant to the last user query and conversation context.
Tool call efficacy	How often AI Agents are invoking tools as needed. $100 - (\text{false positives} + \text{false negatives})/\text{total tool calls}$
RAG accuracy	Correct answers/total answers provided using RAG
Fulfillment error	Error while making a fulfillment request to connect
Fulfillment failure	AI agent flow didn't proceed forward due to fulfillment output - either due to API errors or due to the user providing invalid details

Pro-active notifications to alert admins of critical issues in real-time



Validating Guardrails at System-Level

Planned system-level testing will further strengthen guardrails against evolving production threats.

PyRIT - *Python Risk Identification Toolkit*



Automate adversarial prompt generation to probe LLMs for vulnerabilities like jailbreaks, bias, and data leakage.

→ Used for continuous regression testing and policy stress-testing across model versions.

GOAT - *Generative Offensive Agent Tester*



Simulate realistic attack conversations, mimicking user behavior to uncover evasion paths and safety weaknesses.

→ Helps test how guardrails behave under real-world, multi-turn misuse.

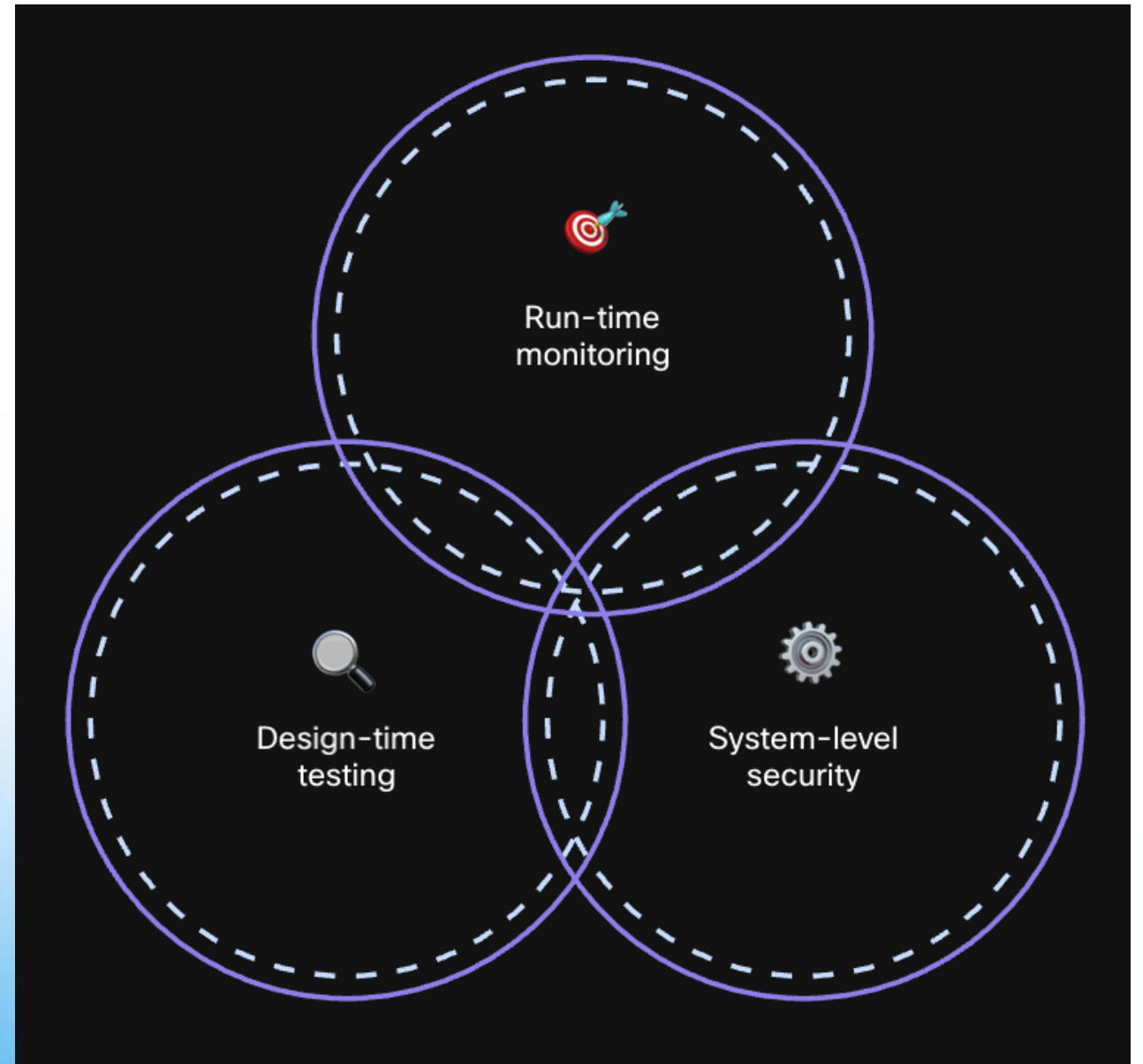
Crescendo Attacks



Chain multiple steps in a conversation to gradually bypass safety mechanisms.

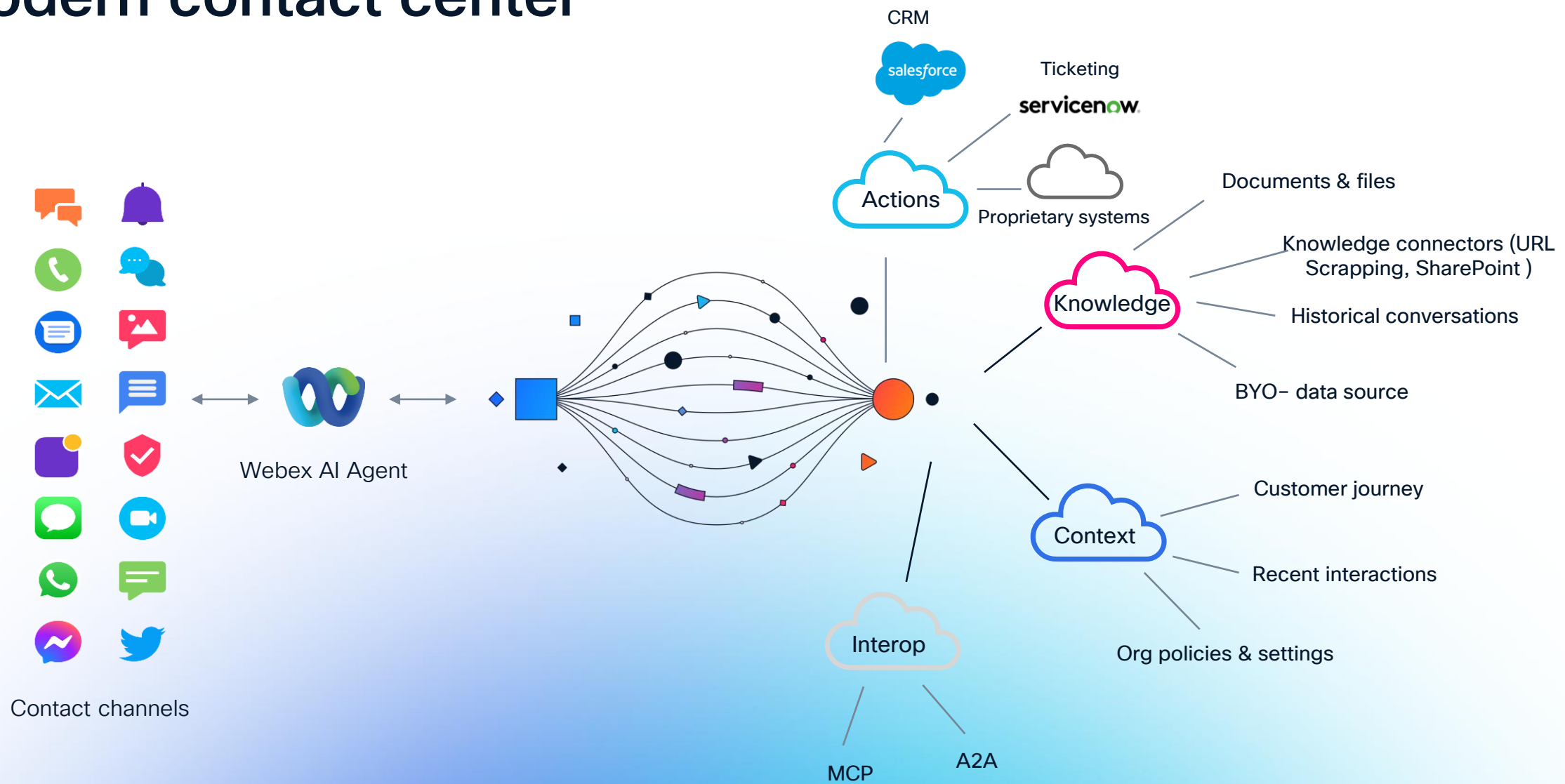
→ Reveals how threats can escalate across longer conversations.

Together, these will give full-spectrum oversight of AI agent risk & reliability – protecting your AI agents before, during, and beyond deployment.

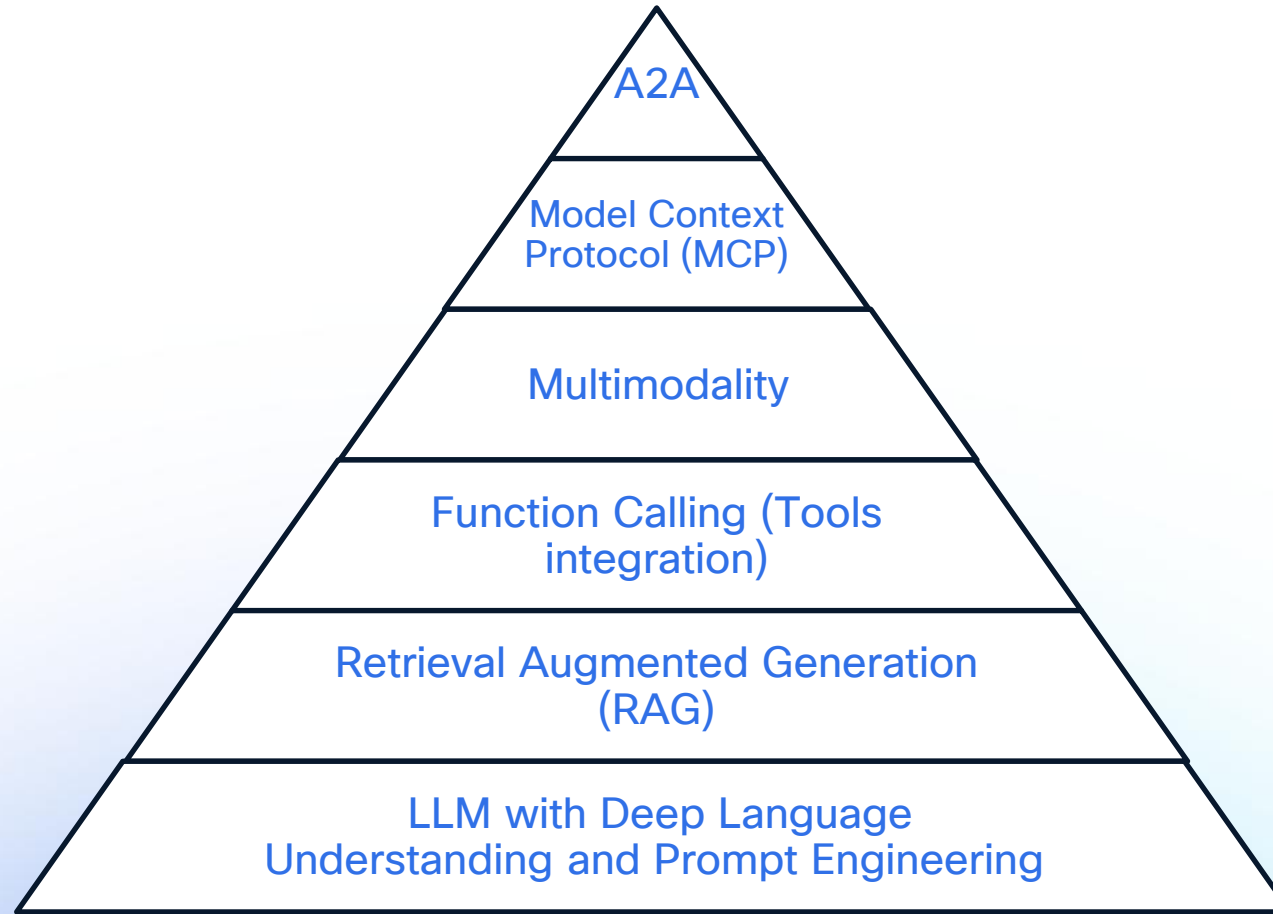


Roadmap

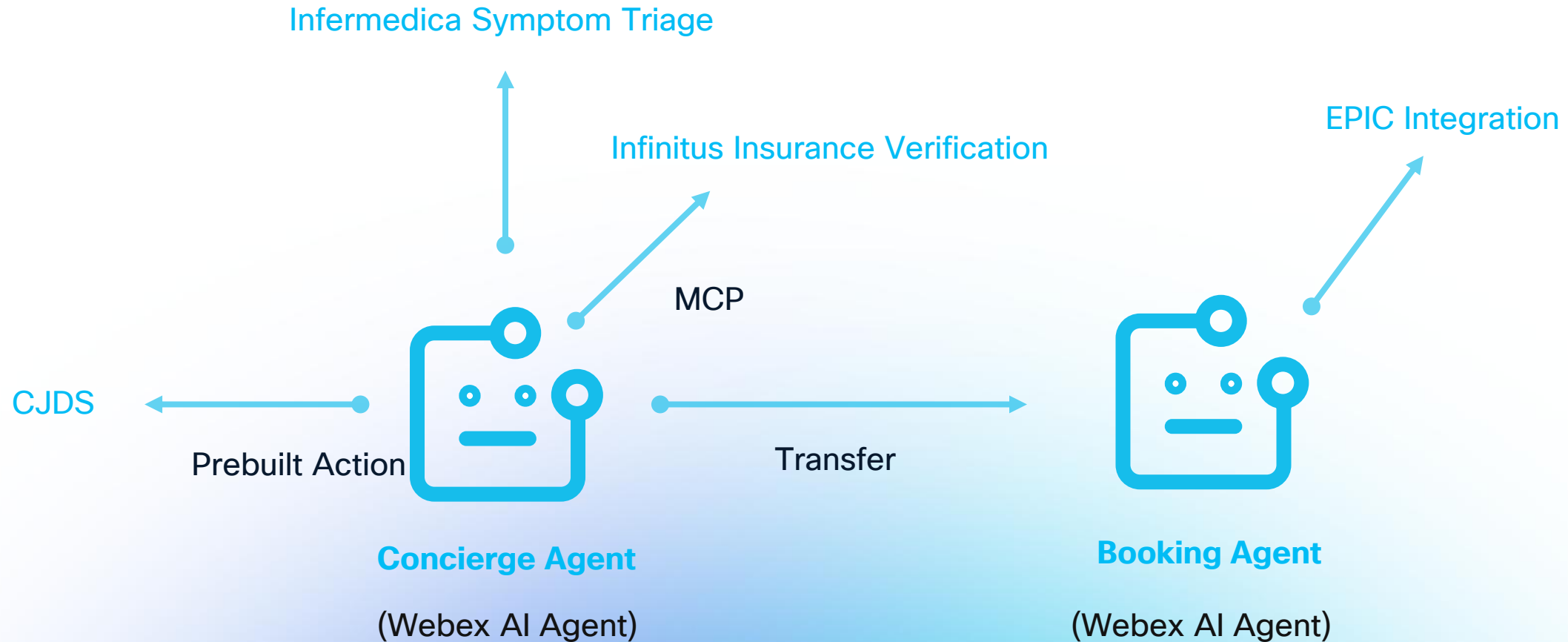
An agentic and intelligent front door for the modern contact center



Tech behind AI Agents

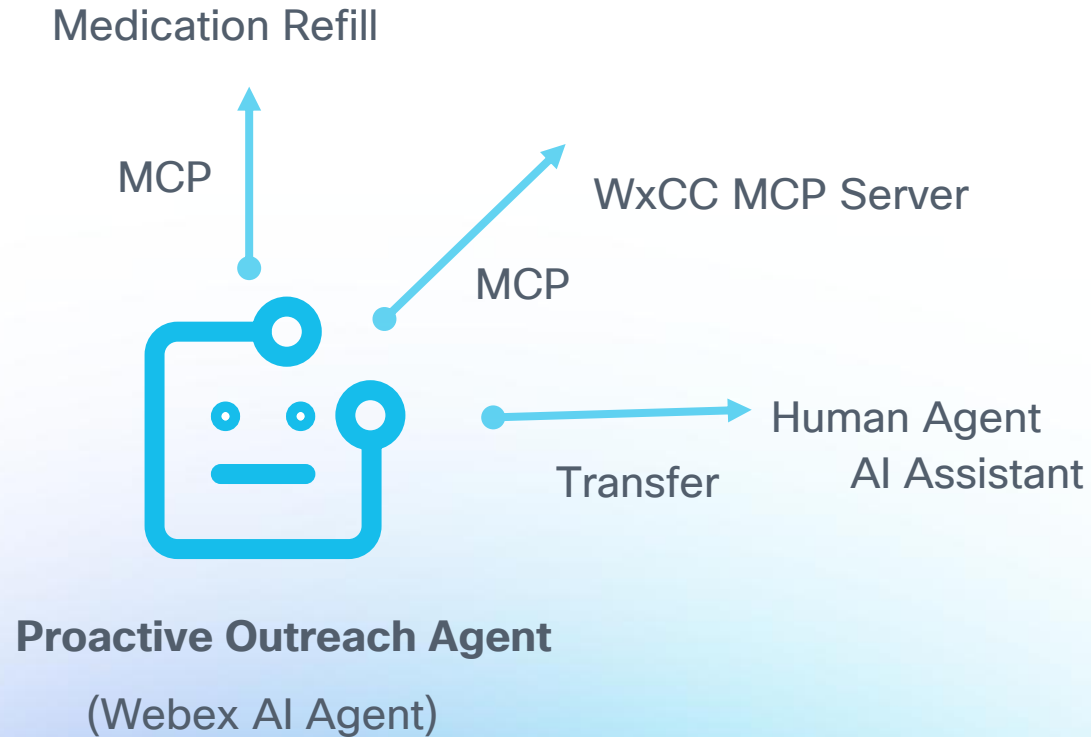


Engage via Contact Center



Proactive Engagement

Refer to the session recording BRKCCT-2556 for more information on MCP/A2A



New Webex AI Agent Studio: AI Agent Configuration

webex AI Agent Studio

Dashboard

AI Agents

AI Assistant Skills

Knowledge

Integrations

AI Engine

Renegize Healthcare Assistant

Draft

Last updated on 05/25/2025 by Henry Riggs

Preview

Configuration

Sessions

History

Analytics

Profile

Knowledge

Actions

Languages

Profile

Essential details

Agent name *

Renegize Healthcare Assistant

System ID *

RenegizeHealthcareAssistant-uah13as

URL for agent profile image *

https://us.webexbotbuilder.com/static/assets/default_logo

Instruction

Choose your AI engine and refine the goal and instructions to boost your agent's accuracy.

AI engine *

Webex AI Pro 1.0

Agent's goal *

Assist users with doctor appointments by efficiently guiding them through the necessary steps.

Instructions

Enter step-by-step instructions for your agent to accomplish its goal.

Welcome message *

Hi there, how can I help you?

Renegize Healthcare

New Webex AI Agent Studio: Pre-Interaction

webex AI Agent Studio

Dashboard

AI Agents

AI Assistant Skills

Knowledge

Integrations

AI Engine

Renegize Healthcare Assistant

Draft

Last updated on 05/25/2025 by Henry Riggs

Configuration

Sessions

History

Analytics

Profile

Knowledge

Actions

Languages

Pre-interaction

Mid-interaction

Post-interaction

Pre-Interaction actions

Add actions

Action name	Created by	Description	Last updated	Action type	Provider type	Controls
<div>Find record</div>	Henry Riggs	Search and locate specific customer records across connected databases and systems using MCP server integration.	10/13/25, at 1:29 PM	Fulfillment	MCP	<div></div> <div></div>

Add pre-interaction actions

Search by action name, description, or provider name

Create new

All

Integration

MCP

A2A

CJDS: Get customer detail

From Webex | Integration

Find record

From Salesforce | MCP

Send one-time PIN

From Duo | Integration

Verify one-time PIN

From Duo | Integration

Cancel

Add

New Webex AI Agent Studio: Mid-Interaction

webex AI Agent Studio

Dashboard

AI Agents

AI Assistant Skills

Knowledge

Integrations

AI Engine

Renegize Healthcare Assistant

Draft

Last updated on 05/25/2025 by Henry Riggs

Configuration

Sessions

History

Analytics

Profile

Knowledge

Actions

Languages

Pre-interaction

Mid-interaction

Post-interaction

Mid-interaction actions

Add actions

Action name	Created by	Description	Last updated	Action type	Provider type	Controls
Create case	Henry Riggs	Generate new customer service cases in connected CRM systems using MCP server framework.	10/13/25, at 1:10 PM	Fulfillment	MCP	

Add mid-interaction actions

Search by action name, description, or provider name

Create new

All

Integration

MCP

A2A

☐ Cancel reservation ⓘ
From Airbnb | MCP

☐ Check availability ⓘ
From Google Calendar | MCP

☐ Consult with "Symptom Triage" agent ⓘ
From Infermedica | A2A

☐ Create case ⓘ
From Salesforce | MCP

Cancel

Add

New Webex AI Agent Studio: Post-Interaction

webex AI Agent Studio

Dashboard

AI Agents

AI Assistant Skills

Knowledge

Integrations

AI Engine

Renegize Healthcare Assistant

Draft

Last updated on 05/25/2025 by Henry Riggs

Configuration

Sessions

History

Analytics

Profile

Knowledge

Actions

Languages

Pre-interaction

Mid-interaction

Post-interaction

Post-interaction actions

Add actions

Action name	Created by	Description	Last updated	Action type	Provider type	Controls
<div>AI Assistant: Generate AutoCSAT</div>	Henry Riggs	Enable intelligent assistant capabilities through connected AI service integrations.	10/13/25, at 1:38 PM	Fulfillment	Integration	<div></div> <div></div>
<div>AI Assistant: Analyze call sentiment</div>	Henry Riggs	Enable intelligent assistant capabilities through connected AI service integrations.	10/13/25, at 1:38 PM	Fulfillment	Integration	<div></div> <div></div>

Add post-interaction actions

Q Search by action name, description, or provider name

Create new

All

Integration

MCP

A2A

AI Assistant: Analyze call sentiment

From Webex | Integration

AI Assistant: Generate AutoCSAT

From Webex | Integration

AI Assistant: Generate summary

From Webex | Integration

CJDS: Update customer detail

From Webex | Integration

Cancel

Add

New Webex AI Agent Studio: Create a new transfer

Add pre-interaction actions

Search by action name, description, or provider name

Create new

All

Integration

MCP

A2A

CJDS: Get customer detail

From Webex | Integration

Find record

From Salesforce | MCP

Send one-time PIN

From Duo | Integration

Verify one-time PIN

From Duo | Integration

Cancel

Add

→ Transfer

⌚ Consult

⌚ Fulfillment

Create a transfer action

Set when to transfer, who to transfer to, and what to share with the next agent.

General information

Action name *

Agent transfer

Transfer condition * ⓘ

Add in custom condition to trigger agent transfer.

For example: If verification fails three times, transfer to an agent.

Select how you want to assign an agent *

Select an AI agent

Select an AI agent *

Select an agent from your organization

Transfer visibility

☒ Skip greetings and match voice ⓘ

☐ Set custom logic to assign a human or AI agent

Information to share

For faster, more accurate result, choose what to share with the next agent. If you skip this, we'll just include a summary of the conversation.

Entities

Entity name	Type	Value	Description	Example	Required
No entities added yet					

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKCCT-2555

New Webex AI Agent Studio: Create a new consult

Add pre-interaction actions

Search by action name, description, or provider name

Create new

All

Integration

MCP

A2A

CJDS: Get customer detail

From Webex | Integration

Find record

From Salesforce | MCP

Send one-time PIN

From Duo | Integration

Verify one-time PIN

From Duo | Integration

→ Transfer

Consult

Fulfillment

Cancel

Add

Create a consult action

Set when to consult, which agent to consult with, and what to share for collaborative decision making.

General information

Action name *

Agent consult

Consult condition *

Add in custom condition to trigger agent consultation.

For example: when patient symptom are complex, consult with specialist agent.

Consult with AI agent *

Select an agent *

Select an agent

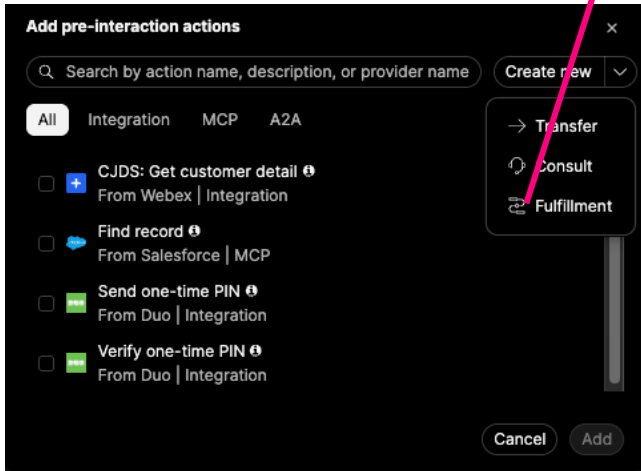
Information to share

For faster, more accurate result, choose what to share with the consulting agent. If you skip this, we'll just include a summary of the conversation.

Entities

Entity name	Type	Value	Description	Example	Required
No entities added yet					

New Webex AI Agent Studio: Create a new fulfillment



Update action

Enable your AI agent to connect with external systems and perform more complex tasks.

General Information

Action name *
Enter action name

Action description * ⓘ
Enter action description

Action scope *
☐ Slot filling ⓘ
☒ Fulfillment ⓘ

Fulfillment

Determine how to handle customer requests or resolve issues.

Select a fulfillment approach *
☒ **Webex Connect Flow Builder**
Build workflows using drag and drop interface with Webex Connect platform.
☐ **Custom server**
Connect to your own server or external API endpoint for custom logic processing.

Service *
Wrap up conversations

Flow *
Generate summary

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

CISCO Live !

