aws

Administrator Guide

Amazon Connect Decisions

Amazon Connect Decisions: Administrator Guide

Table of Contents

What is Amazon Connect Decisions

Amazon Connect Decisions is a supply chain planning and intelligence solution with AI teammates that work alongside your team harmonizing demand signals into consensus forecasts, generating constraint-aware supply plans, and actively monitoring your operations to prevent problems, resolve issues, and identify root causes for continuous improvement.

AI teammates adapt to how you work: driven by your operating procedures and rules, integrating with your existing systems and learning from your practitioners' decisions. It leverages Amazon supply chain expertise to deliver effective plans and recommendations from day one.

You lead a team of AI agents that handle coordination and execute actions, freeing you to focus on strategic decisions that drive service levels and working capital efficiency.

Benefits

Adapt with your business

AI teammates adapt to your business, systems, and decisions, quickly delivering transformation within your existing workflows. Driven by your operating procedures and business rules, teammates work with your existing planning and ERP systems. They learn from planners' decisions, aligning with your priorities and institutionalizing knowledge so your operations get better over time, and every team member is more effective.

Stay ahead of what's coming

Lead a team of AI agents that handle coordination work 24/7—harmonizing demand signals, generating constraint-aware plans, and executing approved actions. Teammates also detect patterns invisible to manual analysis, like cascading supplier disruptions or inventory misalignment across thousands of SKUs, and surface what matters before it becomes a problem. Planners shift from reactive firefighting to proactive planning, running more effective operations and improving service levels through strategic decisions that drive business outcomes.

Build trust from day one

AI teammates are backed by science refined over 30 years of overseeing 400M+ Amazon SKUs and equipped with specialized supply chain tools. Your team benefits from domain expertise honed by one of the world's most complex supply chain networks, delivering actionable insights and recommendations out-of-the-box with clear, explainable reasoning you can trust and verify.

Capabilities

Adaptive intelligence

AI teammates learn from every plan and decision through a continuous loop: observing patterns, detecting what matters, recommending actions, and executing approved decisions. This institutionalizes knowledge—when planners leave, expertise stays; new members are productive from day one, improving outcomes without manual retraining.

Demand intelligence

AI teammates dynamically orchestrate 18+ forecasting tools and foundation models trained on Amazon data, autonomously optimizing at the SKU level. Generate accurate forecasts from day one, even with limited history. Harmonize statistical forecasts, customer commitments, and cross-functional inputs through consensus planning while continuously monitoring accuracy.

Supply intelligence

AI teammates generate forward-looking supply plans (preview) and intelligently cluster exceptions into strategic decisions ranked by impact. Run optimization models for constraint-aware planning across your network. Monitor operations 24/7, surface what matters, then execute approved decisions directly in existing systems—reducing cycles from weeks to hours.

Agentic onboarding

AI-powered onboarding agents guide you through setup via natural language conversation. Connect fragmented data through JDBC or Amazon S3, prepare it for Connect Decisions, and automatically flag issues before they affect forecasts. Configure business rules and policies in plain language with real-time previews—getting operational in weeks, not months.

Getting Started

In this section, you can learn to create an Amazon Connect Decisions instance, grant user permission roles, and log into the Amazon Connect Decisions web application.

Prerequisites to use Amazon Connect Decisions

Before you create an Amazon Connect Decisions instance, make sure that you complete the following steps:

- You have an AWS account. To create an AWS account, see Setting up an AWS account.
- Make sure IAM Identity Center is enabled. To enable IAM Identity Center, see Enabling IAM Identity Center.
- An IAM Identity Center instance must be activated in the same region where you want to create your Amazon Connect Decisions instance. Amazon Connect Decisions is only supported in US East (N. Virginia) and Europe (Ireland) Region.
- If the Amazon Connect Decisions instance is not in the same region as your existing IAM Identity Center region, contact us for further assistance.
- You must have at least one user in the IAM Identity Center instance to assign as the Amazon Connect Decisions administrator. You can connect your active directory to IAM Identity Center. For more information, see Connect to a Microsoft AD directory.
- Add any additional users who need access to Amazon Connect Decisions to IAM Identity Center.
- You need AWS Key Management Service (AWS KMS) to create an instance. Amazon Connect Decisions uses this AWS KMS key to encrypt all the data that comes into Amazon Connect Decisions. For information about AWS KMS Keys, see Creating keys.
- If you intend to enable the actions feature, you will need to configure a connection to the system you use to maintain the relevant data, and provide credentials for Amazon Connect Decisions to use. Please contact us for further assistance.

Browsers supported by Amazon Connect Decisions

Before you work with Amazon Connect Decisions, verify that your browser is supported using the following table.

Browser	Supported Versions
Google Chrome	Latest three versions.
Mozilla Firefox ESR	Versions are supported until their Firefox end-of-life date. For details, see the Firefox ESR release calendar.
Mozilla Firefox	Latest three versions.
Microsoft Edge and Edge Chromium	Version 84 and later.
Safari	Safari 10 or later on macOS.

Languages supported by Amazon Connect Decisions

Amazon Connect Decisions supports the following languages:

- English (US)

Setting up an AWS account

Use this section to create an AWS account and create an IAM user. For information on best practices to create an AWS account, see Establishing your best practice AWS environment.

Sign up for an AWS account

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account

1. Open https://portal.aws.amazon.com/billing/signup.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call or text message and entering a verification code on the phone keypad.

When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to a user, and use only the root user to perform tasks that require root user access.

AWS sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to https://aws.amazon.com/ and choosing **My Account**.

Create a user with administrative access

After you sign up for an AWS account, secure your AWS account root user, enable AWS IAM Identity Center, and create an administrative user so that you don't use the root user for everyday tasks.

Secure your AWS account root user

1. Sign in to the AWS Management Console as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.

   For help signing in by using root user, see Signing in as the root user in the *AWS Sign-In User Guide*.

2. Turn on multi-factor authentication (MFA) for your root user.

   For instructions, see Enable a virtual MFA device for your AWS account root user (console) in the *IAM User Guide*.

Create a user with administrative access

1. Enable IAM Identity Center.

   For instructions, see Enabling AWS IAM Identity Center in the *AWS IAM Identity Center User Guide*.

2. In IAM Identity Center, grant administrative access to a user.

   For a tutorial about using the IAM Identity Center directory as your identity source, see Configure user access with the default IAM Identity Center directory in the *AWS IAM Identity Center User Guide*.

Sign in as the user with administrative access

- To sign in with your IAM Identity Center user, use the sign-in URL that was sent to your email address when you created the IAM Identity Center user.

  For help signing in using an IAM Identity Center user, see Signing in to the AWS access portal in the *AWS Sign-In User Guide*.

Assign access to additional users

1. In IAM Identity Center, create a permission set that follows the best practice of applying least-privilege permissions.

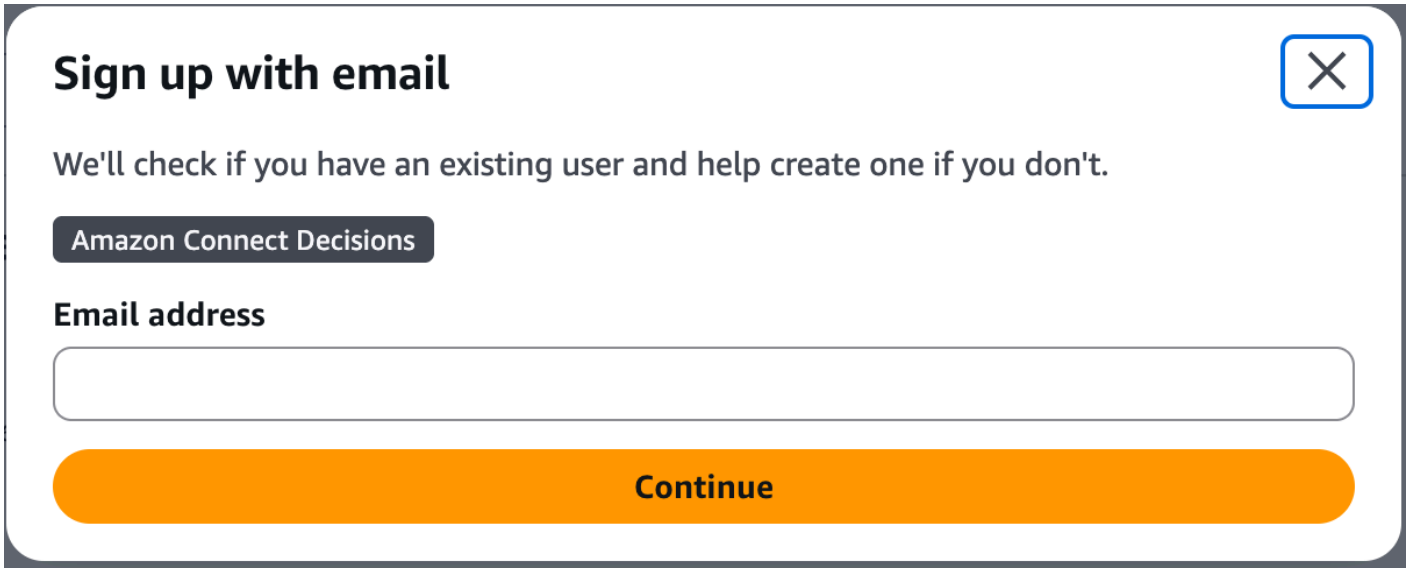
   For instructions, see Create a permission set in the *AWS IAM Identity Center User Guide*.
2. Assign users to a group, and then assign single sign-on access to the group.

   For instructions, see Add groups in the *AWS IAM Identity Center User Guide*.

Configuring AWS Identity Center Integration

To create an instance and use the Amazon Connect Decisions service, you need to either connect an existing IAM Identity Center user profile or create a new one.

1. Open the Amazon Connect Decisions console. You can also search for "Amazon Connect Decisions" from the main AWS Management Console.
2. If necessary, change the **AWS Region** by selecting **Select a Region** located at the top of the console. Choose your Region from the drop-down list.
3. Select **Create Amazon Connect Decisions instance**. A notification will appear.



4. Enter your email address and select **Continue**. IdC will verify if the email matches an existing user.
5. Do one of the following:
   - **If IdC matches the email address to a user** – Select **Connect your identity source and onboard your team**.

     > **Note**
     >
     > This can be used if your organization has an established IdC instance that you would like to use for Amazon Connect Decisions.

   - **If IdC does not find a match to an existing user** – A **Create a New User** notification appears. Proceed to the next step.
6. In the notification, enter the following then select **Continue**:
   - Email address
   - First name
   - Last name

   IdC creates the user automatically and adds them as the Amazon Connect Decisions administrator.
7. Do one of the following:
   - **To create an instance using standard configuration** – Select **Create**. See Use standard configuration.

- **To create an instance using a custom configuration** – Select **Edit in advanced setup**. See Use advanced configuration.

When used in conjunction with IAM Identity Center, Amazon Connect Decisions retrieves the 'username' and 'email' fields from IAM Identity Center directory. None of these attributes are stored natively in your Amazon Connect Decisions instance and are always retrieved at runtime. Amazon Connect Decisions encrypts these identity attributes at rest using an AWS owned KMS key by default. Customer managed KMS keys are not supported in Amazon Connect Decisions. If you delete a user in your AWS IAM Identity Center instance, Amazon Connect Decisions deletes that user from your instance as well.

Managing your Amazon Connect Decisions instance

Creating an instance in Amazon Connect Decisions establishes a dedicated environment for supply chain management and analytics. To set up an instance, you configure basic details, establish settings, and define initial user access permissions.

Only the AWS Management Console administrator can create an instance. The AWS Management Console administrator who creates the Amazon Connect Decisions instance should have all permissions listed under Identity-based policy examples. This administrator should invite an IAM user as an Amazon Connect Decisions administrator to manage Amazon Connect Decisions.

The following pages describe the process of creating and deleting an instance in detail.

Creating Your Instance

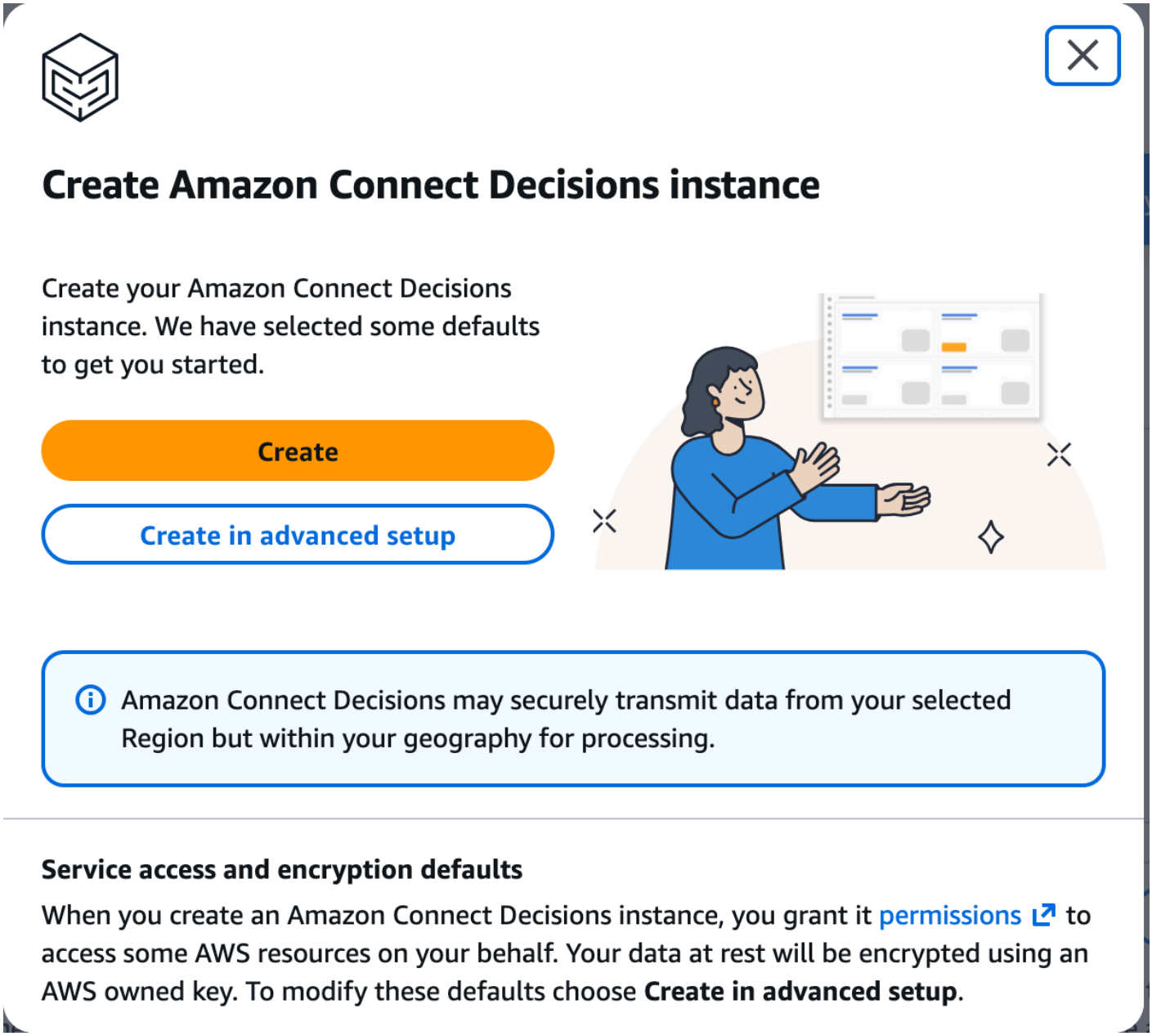
You create an instance using one of two methods, Standard configuration or Advanced configuration. Standard configuration uses an automated process that creates your instance quickly using preset parameters. Advanced configuration allows you to customize your instance by setting your own parameters.

Using standard configuration

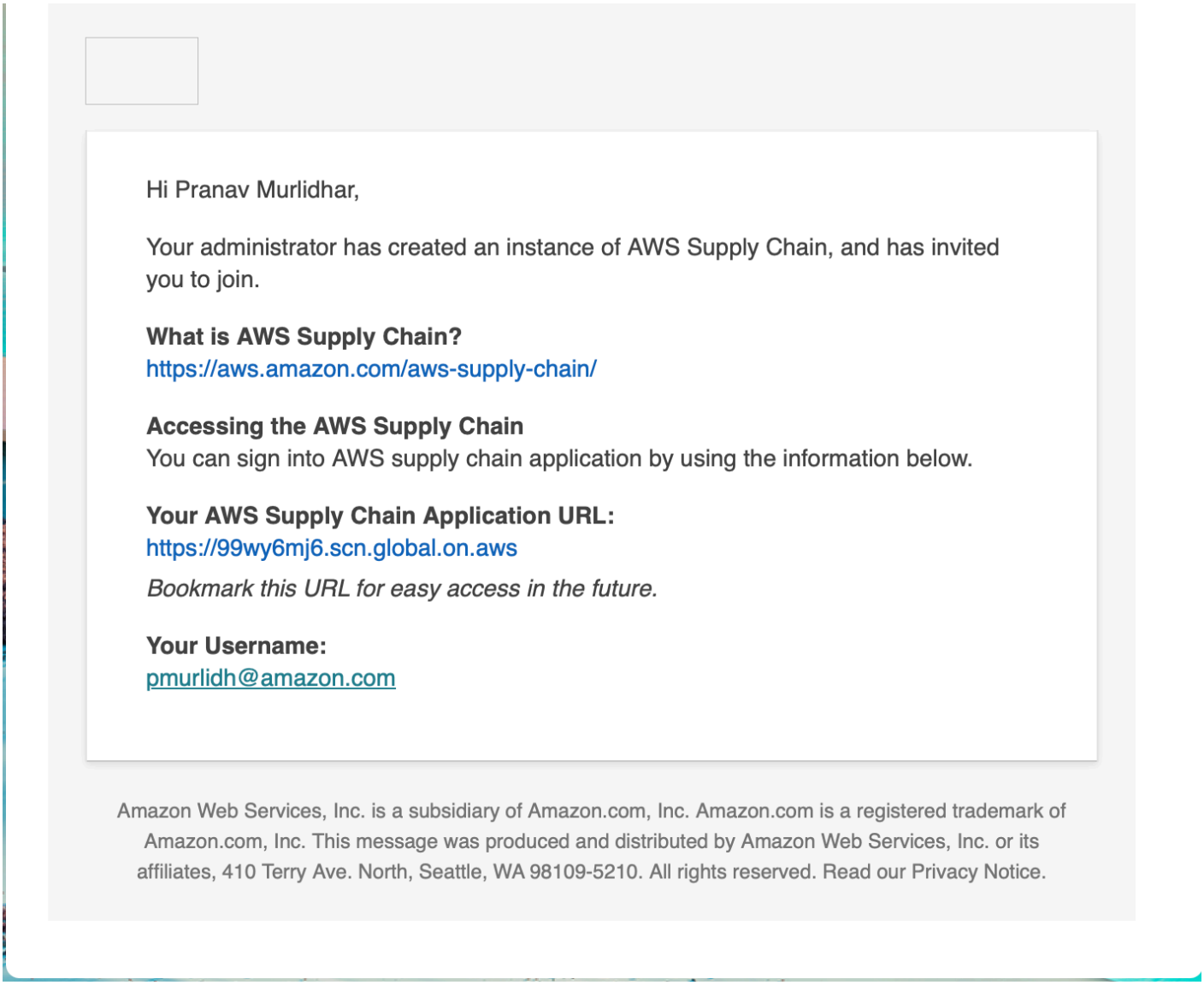
Standard configuration creates your Amazon Connect Decisions instance using default security and encryption settings. Instances operate in AWS geographic regions. For more information about regions, see Regions and endpoints in the *IAM User Guide* and Regional endpoints in the *AWS General Reference*.

To create an Amazon Connect Decisions instance using a standard configuration of preset parameters, follow these steps.

1. Select **Create**.



2. Check your email for the following:
   - An email from the IdC team.
   - An email from Identity Management team.

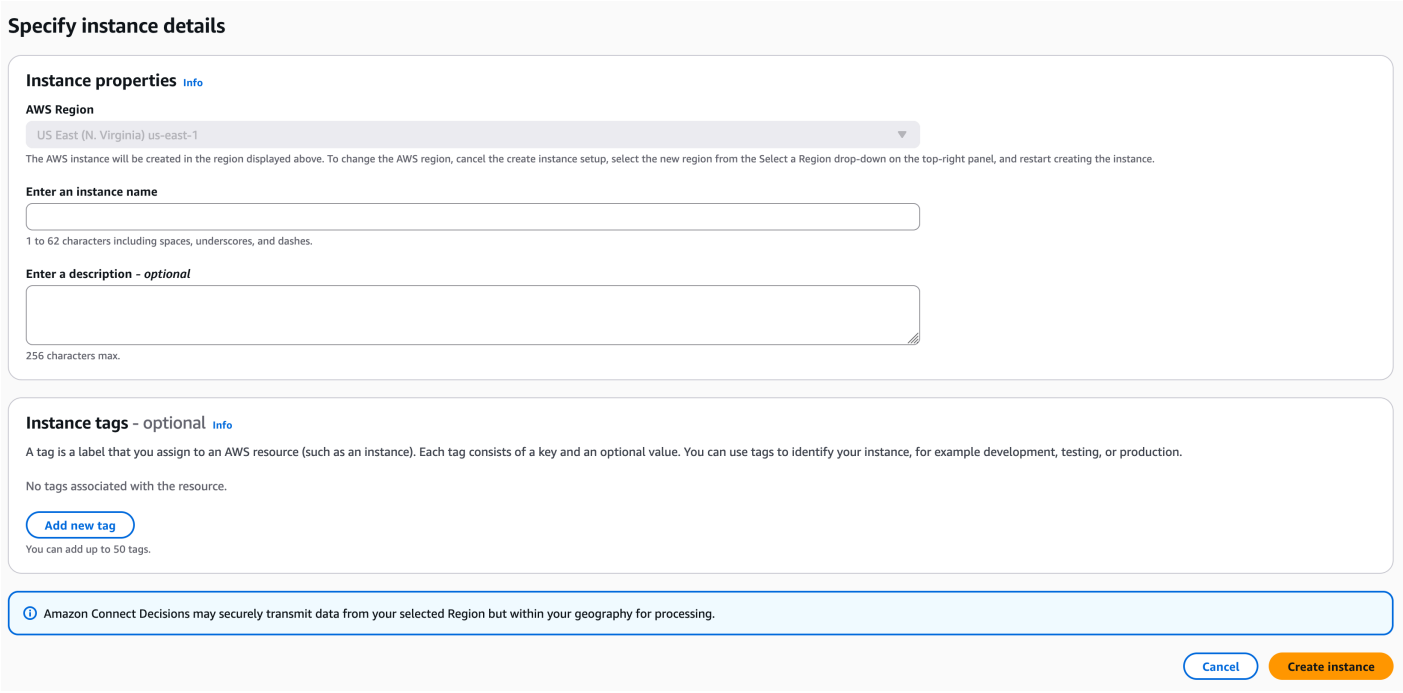


3. Once you receive the invite email, log on to Amazon Connect Decisions. See Log on to Amazon Connect Decisions web application .

Using advanced configuration

Advanced configuration allows you to customize your instance by setting your own parameters. To create an Amazon Connect Decisions instance using an advanced configuration of preset parameters, follow these steps.

1. Select **Create in advanced setup**.
2. The **Instance properties** page will appear.



3. Enter the following on the **Instance properties** page:
   - **Name** – Enter an instance name.
   - **Description** – Enter a description of your Amazon Connect Decisions instance (e.g., production instance, test instance, etc.).
   - **Instance tags** – You can add tags to your instance that can be used for identification. For example, you can add a tag to define the type of instance you are creating (e.g., production, test, UAT, etc.).
4. Select **Create instance**.

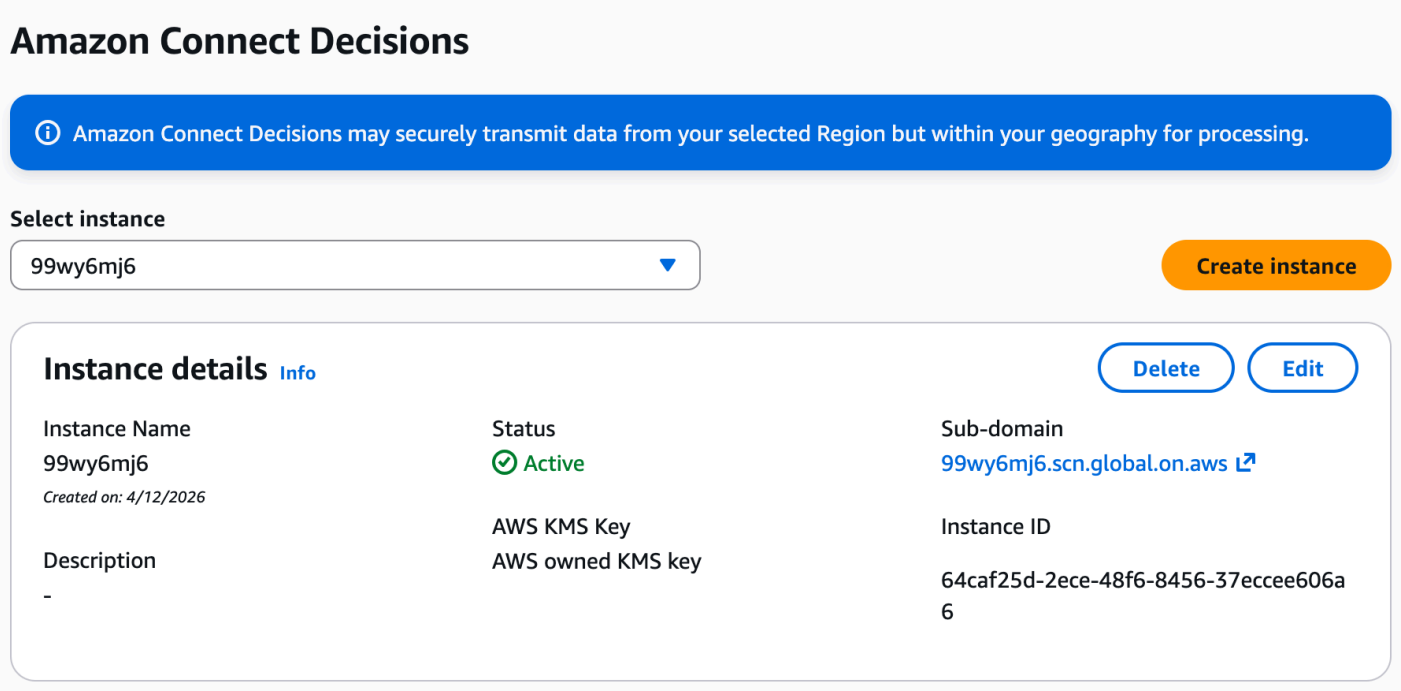
Deleting an instance

To delete an instance, follow these steps.

> **Note**
>
> When you delete an instance, information from the Amazon S3 bucket is not automatically deleted.

1. Open the Amazon Connect Decisions console at https://console.aws.amazon.com/scn/home.

2. On the Amazon Connect Decisions console dashboard, from the dropdown, select the instance that you want to delete.



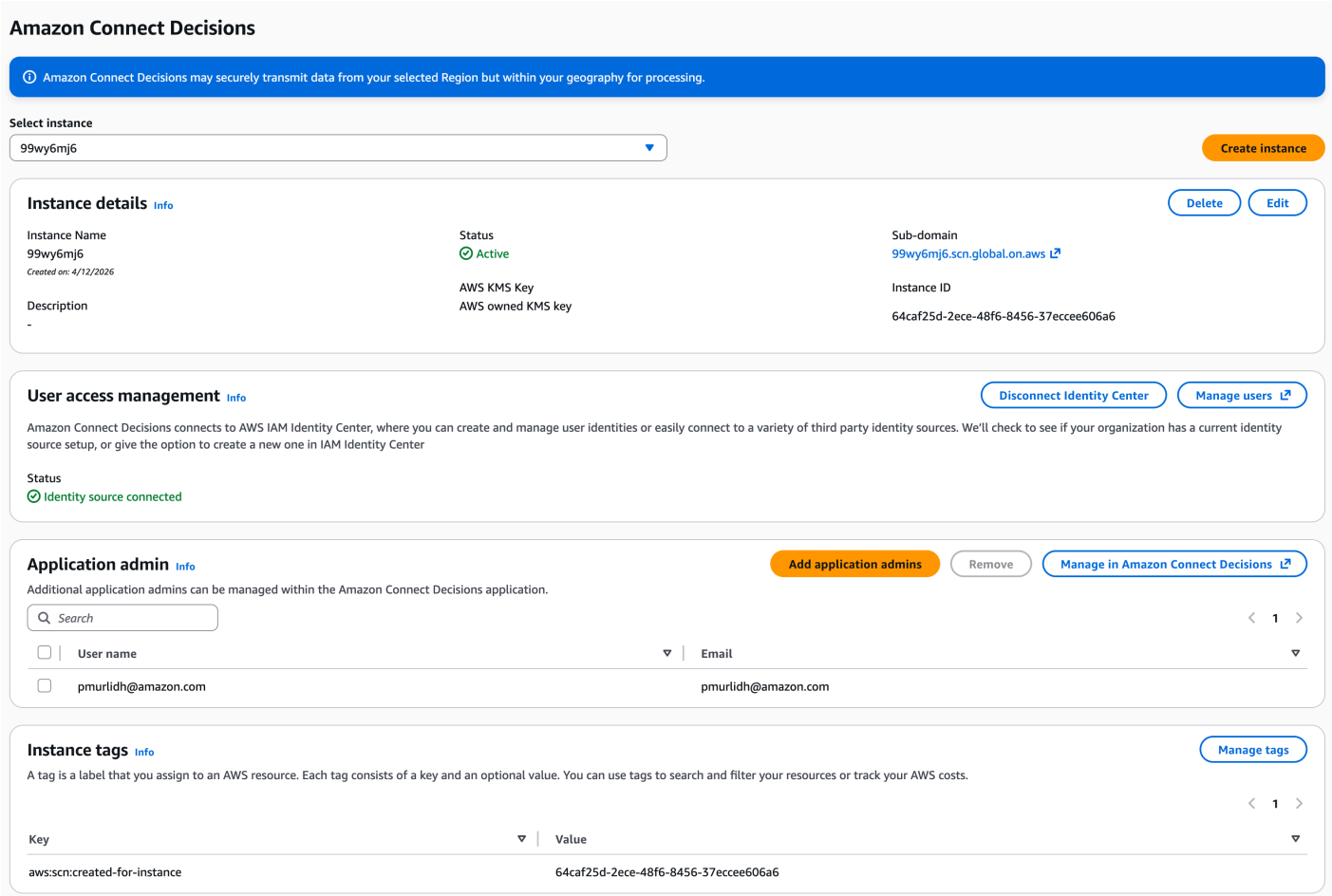
3. Choose **Delete**.
4. On the **Delete Amazon Connect Decisions Instance** page, under **Confirmation**, type `delete` to confirm that you want to delete the instance.
5. Choose **Delete**. The instance deletion starts and once the instance is deleted, you will see a confirmation message.

Choose an application admin

As an AWS console administrator, you choose an Amazon Connect Decisions application admin to manage the Amazon Connect Decisions web application access. The Amazon Connect Decisions application admin can add or remove user permission roles to the Amazon Connect Decisions web application.

After the instance is created and an identity source is connected, follow these steps to choose an Amazon Connect Decisions application admin.

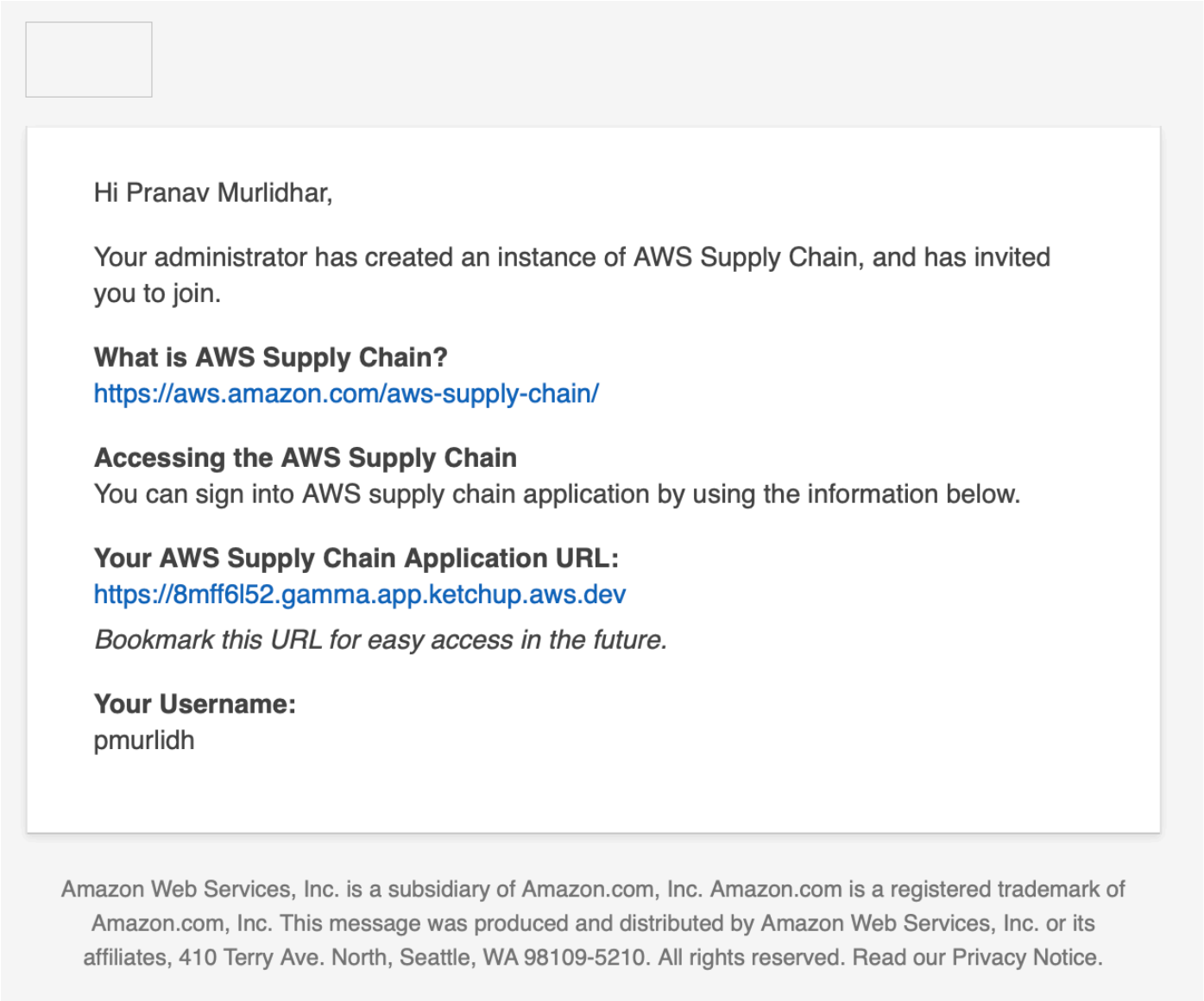
1. Open the Amazon Connect Decisions console dashboard.
2. Go to **Select application admin** and select a user to be an Amazon Connect Decisions application admin. Search results only show users matching the search criteria.



3. (Optional) Choose **Go to IAM Identity Center** to add more users. For more information on adding users, see Manage your identity source in *AWS IAM Identity Center User Guide* and for more information on user permission roles, see User permission roles.

> **Note**
>
> You can only add one user at a time from the Amazon Connect Decisions Console. You cannot add a group as an application admin in Amazon Connect Decisions.

4. Choose **Send Invite**. An email is sent to the web application administrator. Once the web application administrator receives the invite email, they will be able to select the application URL and log into the Amazon Connect Decisions.



Hi Pranav Murlidhar,

Your administrator has created an instance of AWS Supply Chain, and has invited you to join.

What is AWS Supply Chain?
https://aws.amazon.com/aws-supply-chain/

Accessing the AWS Supply Chain
You can sign into AWS supply chain application by using the information below.

Your AWS Supply Chain Application URL:
https://8mff6l52.gamma.app.ketchup.aws.dev
Bookmark this URL for easy access in the future.

Your Username:
pmurlidh

Amazon Web Services, Inc. is a subsidiary of Amazon.com, Inc. Amazon.com is a registered trademark of Amazon.com, Inc. This message was produced and distributed by Amazon Web Services, Inc. or its affiliates, 410 Terry Ave. North, Seattle, WA 98109-5210. All rights reserved. Read our Privacy Notice.

In the Amazon Connect Decisions webapp, you will see the user listed under **Application admin**.

Accessing your instance

Using the console is the easiest way to manage your service resources and configurations. The console provides an intuitive web-based interface where you can view, create, modify, and monitor your resources.

To access the Amazon Connect Decisions console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the Amazon Connect Decisions resources in your AWS account. If you create an identity-based policy that is more restrictive than

the minimum required permissions, the console won't function as intended for entities (users or roles) with that policy.

You don't need to allow minimum console permissions for users that are making calls only to the or the AWS API. Instead, allow access to only the actions that match the API operation that they're trying to perform.

As an Amazon Connect Decisions administrator, you should have received an email invite to the Amazon Connect Decisions web application.

1. You can either choose the link in the email or on the Amazon Connect Decisions console dashboard, under **Sub-domain**, choose **web URL**.
2. The **Amazon Connect Decisions** web application login page appears.
3. Enter the AWS IAM Identity Center user credentials and choose **Sign in**.
4. Each user that you added receives an email message with a link that goes to Amazon Connect Decisions, or you can choose **Copy link** and send the link to the users.

After successfully logging in, you will land at your personalized Home Page. Refer to Understanding your Homepage in the user guide to understand your home page better.

Access Control

Amazon Connect Decisions provides enterprise-grade access management that gives you precise control over who can access what data and perform which actions within your instance. This ensures your users see only the information relevant to their responsibilities while maintaining the security and compliance standards your organization requires.

Overview of roles and permissions

As an Amazon Connect Decisions administrator, you can either use the default user permission roles or create custom permission roles. Amazon Connect Decisions has the following default user permission roles:

- **Administrator** – Access to create, view, and manage all data and user permissions.

Admin

Role name
Admin

Description
Maximum privilege role for the Supply Chain Instance

Permissions details

Insights
Grant access to insights and exceptions, specifying the actions that authorized individuals are permitted to take.

Access	All	Create	Read	Update	Delete
Insights			☑	☑	
Configuration	☑	☑	☑	☑	☑

Plans
Grant access to plans, specifying the actions that authorized individuals are permitted to take.

Access	All	Create	Read	Update	Delete
Plans	☑	☑	☑	☑	☑

Management
Grant access to management functions, including data, access control, and user access.

Access	All	Create	Read	Update	Delete
Data	☑	☑	☑	☑	☑
Access Control		☑	☑	☑	
User Access	☑	☑	☑	☑	☑

- **Manager** – Access to create, view, and manage the following.

Manager

Role name
Manager

Description
Users managing inventory or demand planning teams within the organization

Permissions details

Insights
Grant access to insights and exceptions, specifying the actions that authorized individuals are permitted to take.

Access	All	Create	Read	Update	Delete
Insights			☑	☑	
Configuration	☑	☑	☑	☑	☑

Plans
Grant access to plans, specifying the actions that authorized individuals are permitted to take.

Access	All	Create	Read	Update	Delete
Plans	☑	☑	☑	☑	☑

Management
Grant access to management functions, including data, access control, and user access.

Access	All	Create	Read	Update	Delete
Data					
Access Control					
User Access					

- **Planner** – Access to create, view and manage the following.

Planner

Role name
Planner

Description
Users planning inventory or demand within the organization

Permissions details

Insights

Grant access to insights and exceptions, specifying the actions that authorized individuals are permitted to take.

Access	All	Create	Read	Update	Delete
Insights			☑	☑	
Configuration		☑	☑	☑	

Plans

Grant access to plans, specifying the actions that authorized individuals are permitted to take.

Access	All	Create	Read	Update	Delete
Plans		☑	☑	☑	

Management

Grant access to management functions, including data, access control, and user access.

Access	All	Create	Read	Update	Delete
Data					
Access Control					
User Access					

Note

As an Amazon Connect Decisions administrator, before you add users, note the following:

- Each default user permission role is defined with a set of permissions. You can add users to default user permission roles or create custom permission roles.
- A user can only be assigned to one user permission role.
- You cannot edit or delete default user permission roles.
- When you edit a custom permission role you created, the permissions for all the users under the custom permission role are updated.
- When you delete a custom permission role you created, all the users under the custom permission role will lose access to Amazon Connect Decisions.
- Adding groups is not supported in Amazon Connect Decisions.

Managing user permission roles

Adding users

As an Amazon Connect Decisions administrator, you can add users to access the Amazon Connect Decisions web application. Users first must be added to IAM Identity Center (IdC), and then they can be added to Amazon Connect Decisions. For more information about adding users to IdC, see Assign user access.

Once users have been added to IdC, follow these steps to add a user.

1. Choose the **Settings** left-hand side drawer
2. Select **Users**. Select Assign users
3. Search to identify the user. You can search using Display Name, Email, First name, Last name, Username
4. Select **the users that you want to add**.
5. Assign them a role. View Overview of roles and permissions to learn more about User roles in Amazon Connect Decisions.
6. Select Assign. Confirm that your selections are accurate.

Updating user permissions

To update the user permission role for the current Amazon Connect Decisions users, follow these steps.

1. Choose the **Settings** left-hand side drawer
2. Select **Users**. Select Assign users
3. In the **Users** list, select the user to open the **User details** page.
4. Use the role dropdown to update the role permissions for the user.
5. Confirm that you want to change the role by clicking the change role button

Deleting users

As an Amazon Connect Decisions administrator, you can delete users from the Amazon Connect Decisions web application. Follow these steps to delete users.

1. Choose the **Settings** left-hand side drawer
2. Select **Users**. Select Assign users
3. In the **Users** list, select the user to open the **User details** page.
4. Select Delete
5. Confirm that you want to delete the user by clicking the **Delete** button

Setting up attribute-level access

Attribute-Based Access Control (ABAC) adds an additional layer of precision by restricting access based on business context. Using product and site attributes, you can ensure that planners only see details for the specific products and locations they manage, while managers maintain visibility across their teams' areas of responsibility.

Any user with the 'Admin' role can configure access by product and sites for other users:

1. Navigate to the Users page from the left navigation bar.
2. From the list of users in that instance, select the user that needs configuration.
3. By default, in the Data access section, users will have "Grant full access to all products and sites" enabled. When this toggle is on, it provides access to all products and sites (how it worked prior to this launch).

4. Toggle off "Grant full access to all products and sites" and the product and sites configuration section will become visible. No products or sites will be assigned when first accessed.
5. Click the Add/Remove button for either products or sites based on what you need to configure. Use the search to find and select the items needed for that user.
6. Multiple users can have the same product or site assigned to them. A user can have a maximum of 1,000 product-site combinations.
7. Previously configured products or sites can be removed using the same interface.
8. Review and confirm the full list of additions and removals in the final page of the wizard to complete the access configuration.

Once product and site access has been configured, access for that user will be restricted based on these assignments:

- All users can view any exception or recommendation page, regardless of whether it was generated for a product or site included in their access control.
- To perform mutate actions (such as dismissing an exception or changing status from In Progress to Complete), users must have the appropriate product OR site configured in their access control.
- Users with configured access control can also use User Assignment and the Access View Toggle.

User Assignment

User Assignment is a feature that makes it easier to balance insights between multiple users. Using User Assignment, customers can assign specific insights to users to better reflect how these tasks are shared in real life. It works as follows:

- Whenever an exception is created, the system checks the product and site for which the exception is created against all users that have the same product OR site configured for their access control
- If the system finds a user that matches, the Assigned To field for that exception is updated with the username. In cases where more than one user has products or sites that match with the exception, it is assigned randomly to one of them
- Only one user can be assigned to each exception, but an exception can be reassigned to another user if needed. It can only be reassigned to a user with product or site access

- Auto-assignment for insights occurs when the exception is first created. Previously created insights will not be reassigned automatically. Further, if a user is deleted or their access control is updated, the user assignment is not automatically updated
- In the insights listing page, a user can filter by the Assigned To dimension to easily identify all insights assigned to them. They can also use this same filter to view unassigned insights. User Assignment is currently available only for insights

Data Onboarding

Connecting your data

Prerequisites

Before starting data onboarding, ensure you have:

- Amazon Connect Decisions Instance
  - Your instance should already be created with an associated S3 bucket
- Data Prepared
  - Work with your Amazon Customer Success counterpart to determine which data you need based on how you plan to use Amazon Connect Decisions. Base data requirements include:
    - Sales/Order History: 12+ months of transaction records
    - Product Details: Complete product catalog with specifications
    - Site/Location Information: Warehouses, distribution centers, retail locations
    - Current Inventory Holdings: On-hand inventory at each location
  - All source data in CSV format with UTF-8 encoding

First Time Login: Onboarding Questionnaire

When you log in to Amazon Connect Decisions for the first time, the system presents a guided Onboarding Questionnaire. This personalization wizard helps the Decisions teammates contextualize the capabilities most relevant to your business. The questionnaire collects information about your industry, primary business challenges, and preferred approach for planning. Your responses will help optimize the onboarding steps based on your selection, allowing the system to streamline subsequent setup workflows and surface the most relevant configuration paths for your business. You must complete all steps before accessing the full application. The Decisions Teammate is available throughout the onboarding process via the right sidebar to answer questions in real time.

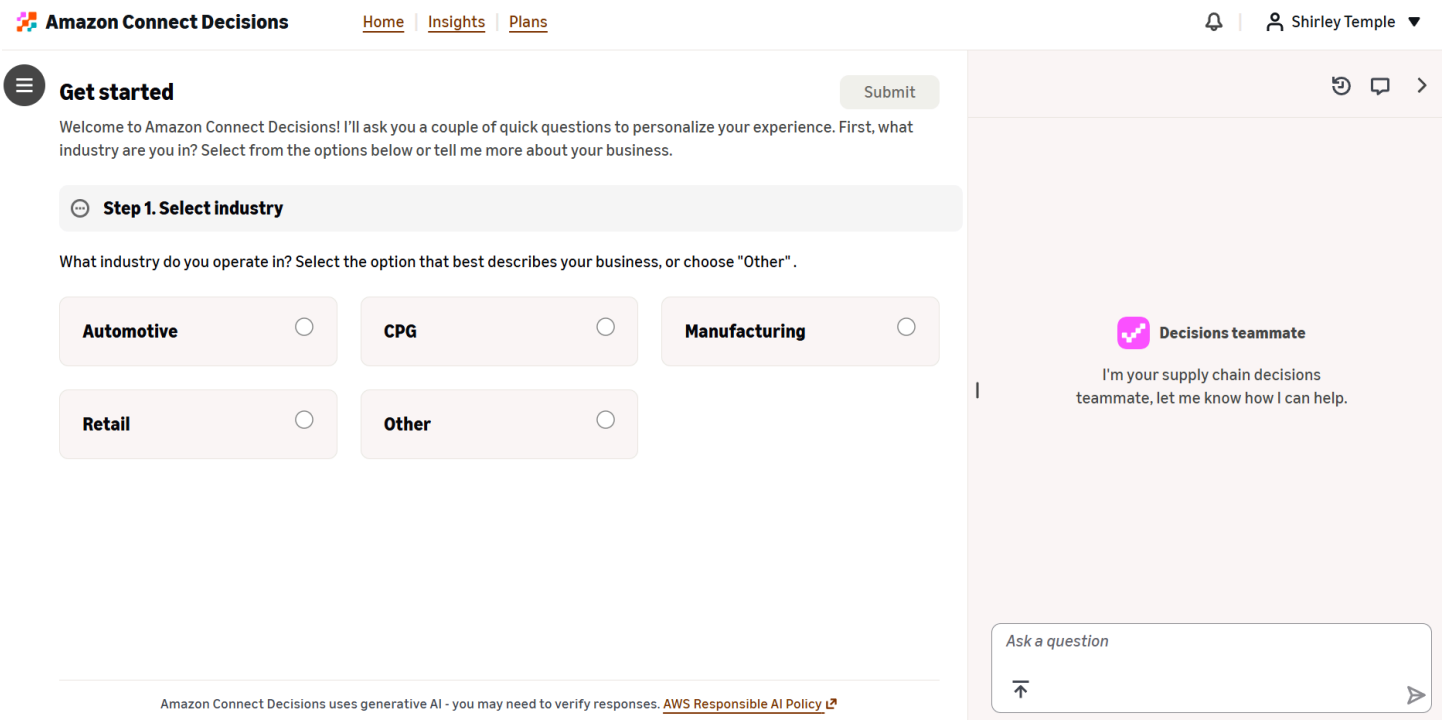
Note

This is a onetime selection on first login only. Your responses provide additional context to optimize subsequent onboarding steps and help agents understand your business environment. All capabilities remain fully accessible regardless of your selections.

Step 1: Select Industry

What you see: A welcome message and a set of radio buttons prompting you to select the industry that best describes your business.

1. Select the radio button that best represents your business.
2. If none of the predefined options apply, select **Other**.



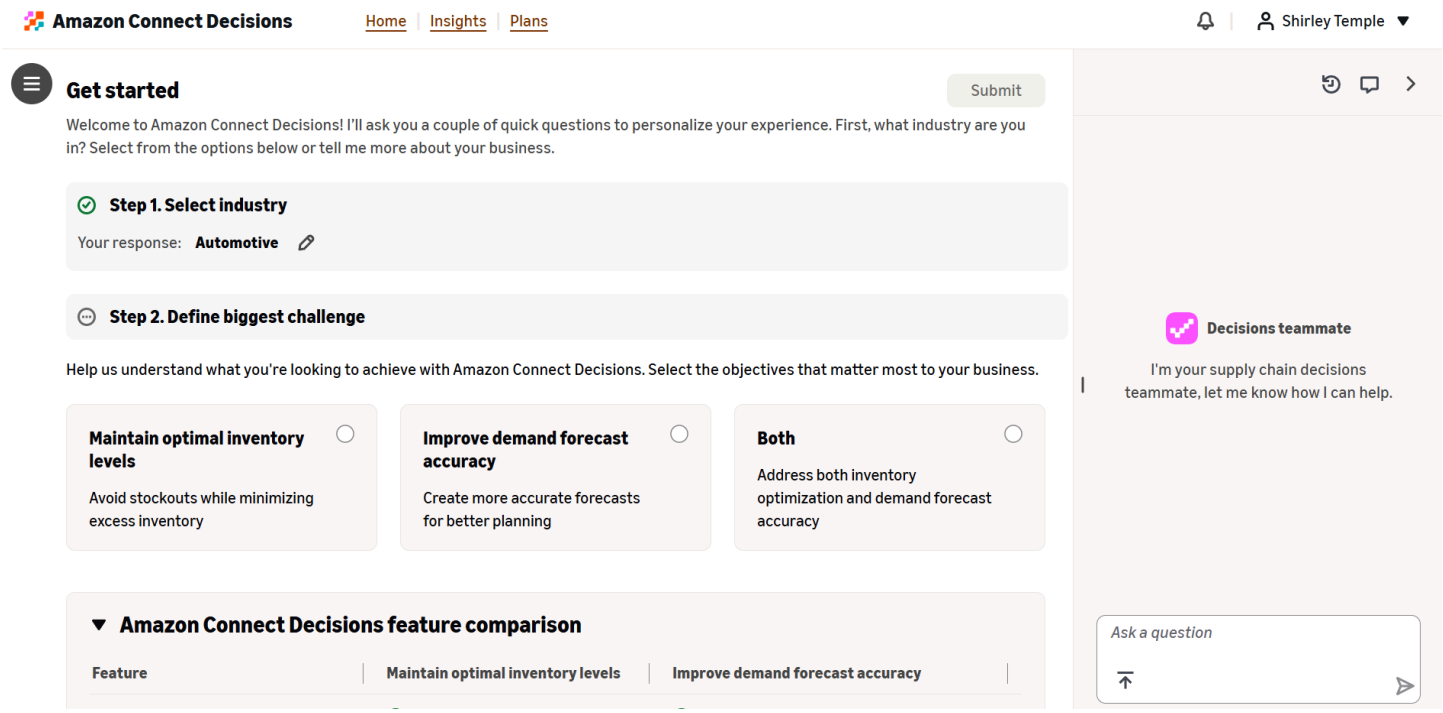
Step 2: Define Your Biggest Challenge

What you see: Your Step 1 response is displayed with an edit option. Below it, you are asked to identify your primary business challenge from three options. A feature comparison table is displayed to help you understand which capabilities are associated with each selection.

1. Review the options. See the following table for the available options and what they mean.
2. Select the radio button that represents your most pressing challenge.
3. Optionally, review the feature comparison table below the options to understand what is included with each selection.

Business challenge options

Option	Description	Key Features Enabled
Maintain optimal inventory levels	Choose this if your primary challenge is avoiding stockouts while minimizing excess inventory.	Inventory optimization; Stockout prevention; Excess inventory reduction; Supply planning; Vendor lead time tracking
Improve demand forecast accuracy	Choose this if your primary challenge is creating more accurate forecasts for better planning decisions.	Baseline forecasting; Consensus planning; Forecast accuracy tracking
Both	Choose this if you need to address both inventory optimization and demand forecast accuracy simultane ously.	All supply specific and demand specific features are enabled



Step 3: Choose Your Inventory Planning Approach

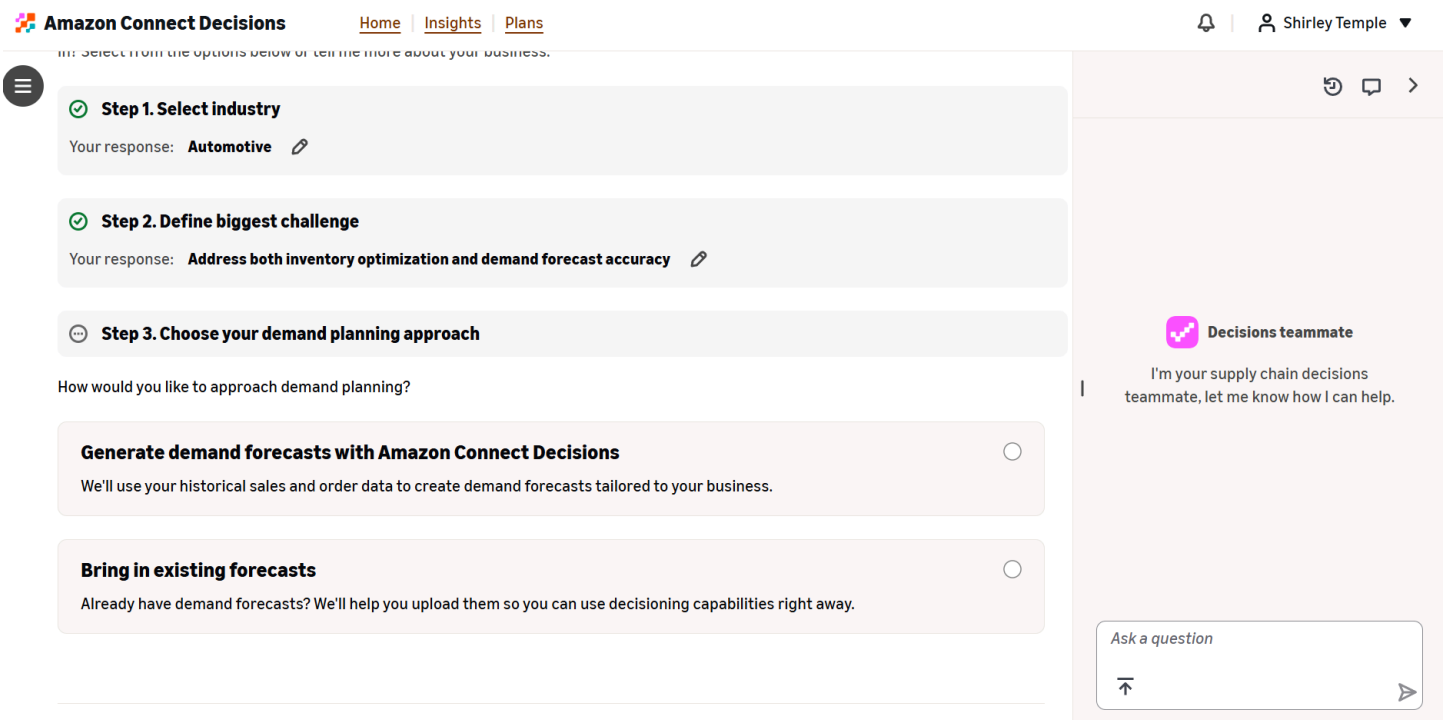
What you see: Steps 1 and 2 are displayed as completed (indicated by green checkmarks) with your responses shown and editable. Step 3 asks how you would like to approach inventory planning, with two options highlighted.

1. Review the two inventory planning options. See the following table for the available options and what they mean.
2. Select the radio button for the approach that matches your current state.

Inventory planning approach options

Option	Description	Best For
Generate inventory plans with Amazon Connect Decisions	The system uses your historical sales and inventory data to create plans tailored to your business.	Organizations that do not have an existing planning solution or want to leverage AI generated plans from their historical data.
Bring in existing inventory projections or plans	Upload your existing inventory plans or projectio	Organizations that already have established planning

Option	Description	Best For
	ns so you can use decisioning capabilities immediately. The system will help you upload and map your data.	processes and want to leverage monitoring, insight generation, and recommend ation capabilities without changing their plan source.



Step 4: Choose Your Demand Planning Approach

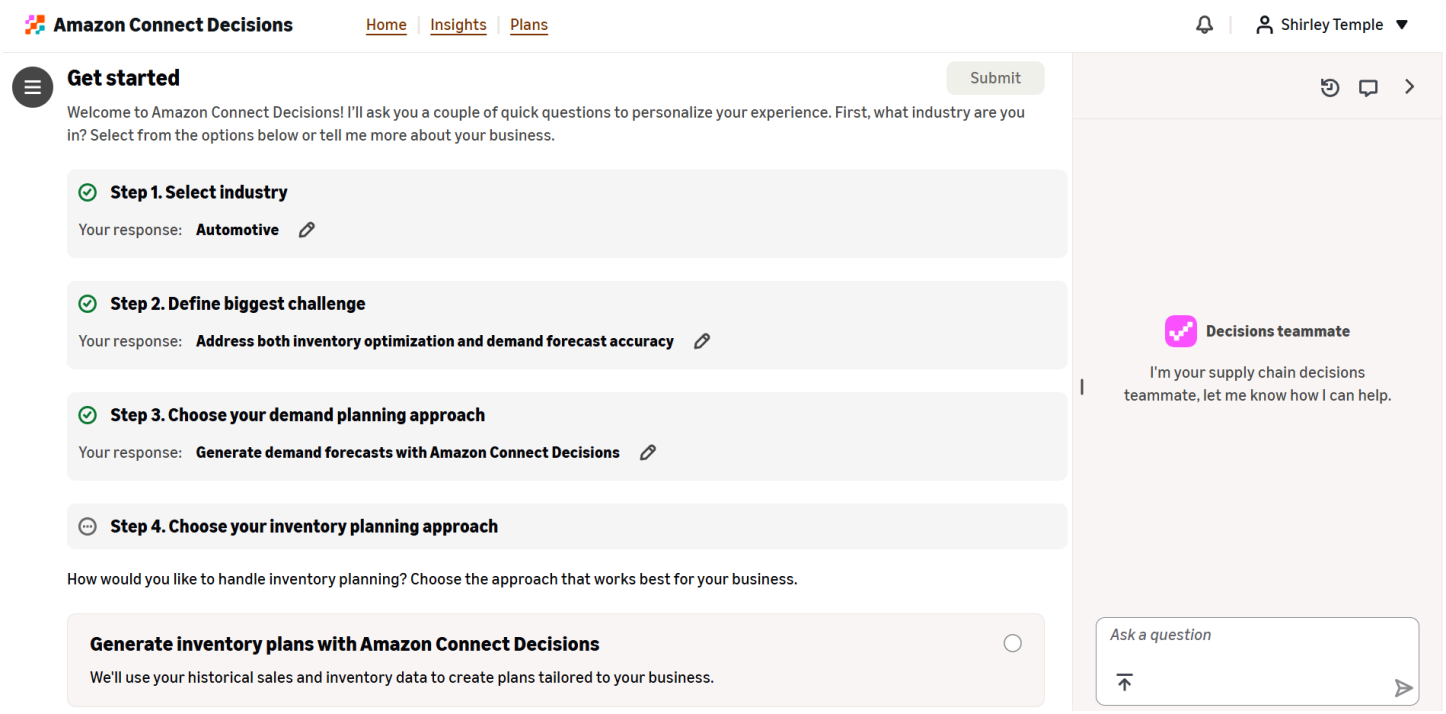
What you see: Steps 1 through 3 are displayed as completed. Step 4 asks how you would like to approach demand planning.

1. Review the two demand planning options. See the following table for the Available Options and What They Mean.
2. Select the radio button for the approach that matches your current state.
3. Click **Submit** to finalize the onboarding questionnaire.

Remember: This onboarding questionnaire is a onetime contextual input that helps optimize the onboarding steps based on your selections. It does not alter agent behavior or restrict access to any capabilities. All features of Amazon Connect Decisions remain fully available to you.

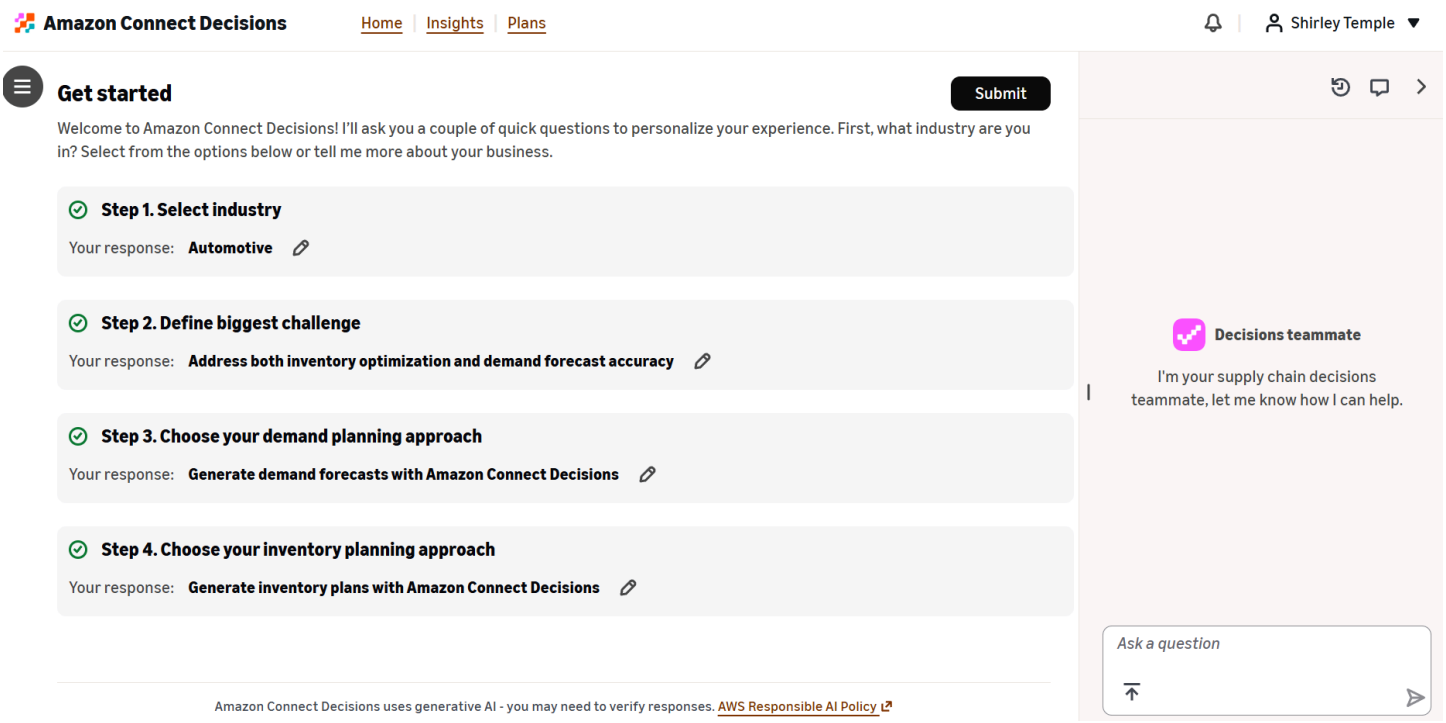
Demand planning approach options

Option	Description	Best For
Generate demand forecasts with Amazon Connect Decisions	The system uses your historical sales and order data to create demand forecasts tailored to your business. Amazon Connect Decisions orchestrates 18+ forecasti ng tools to produce accurate baseline forecasts.	Organizations that do not have an existing forecasting solution or want to replace their current approach with AI generated forecasts.
Bring in existing forecasts	Upload your existing demand forecasts so you can use decisioning capabilities immediately. The system will help you map and import your forecast data.	Organizations that already have established forecasti ng processes and want to leverage the monitoring, insight generation, and recommendation capabilit ies without changing their forecast source.



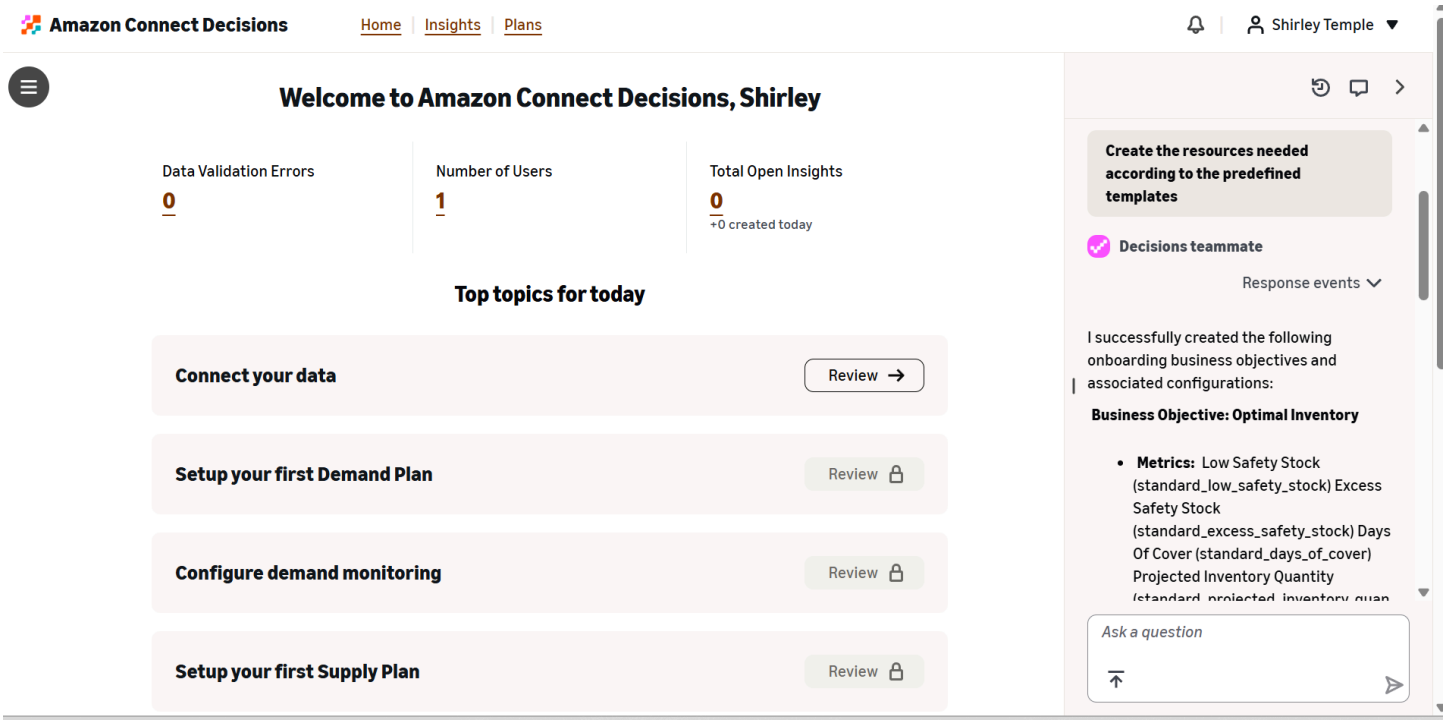
After Completing the Questionnaire

Click **Submit** after completing all four steps:



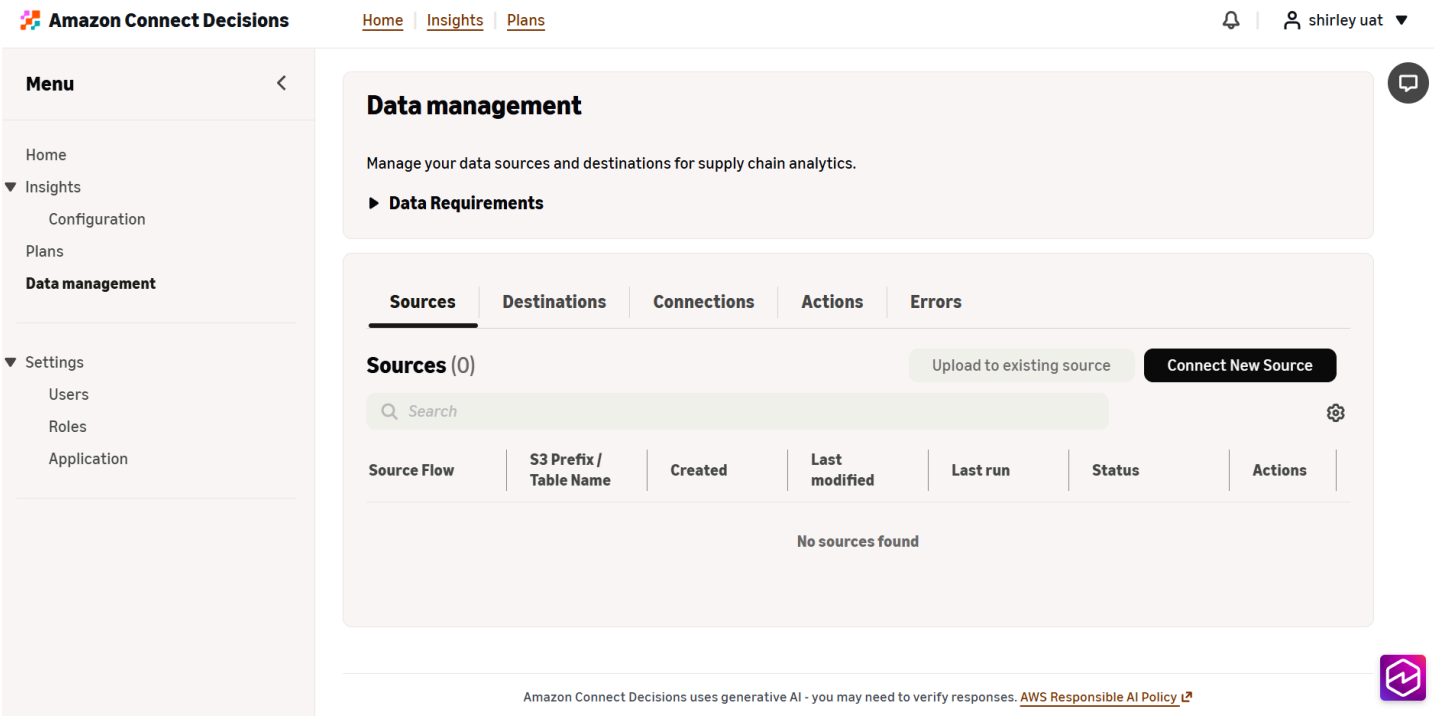
- You will be **redirected to the Homepage** with dashboard and topic cards designed to guide you through the remaining onboarding steps.

- The system will **auto create metrics and rules** within the application based on your selections. These are created in **Draft status** and are not immediately active.
- You can review the auto created metrics and rules, then **activate them** if they meet your needs, or **create your own** metrics and rules tailored to your specific business requirements.



Creating Your First Source Flow

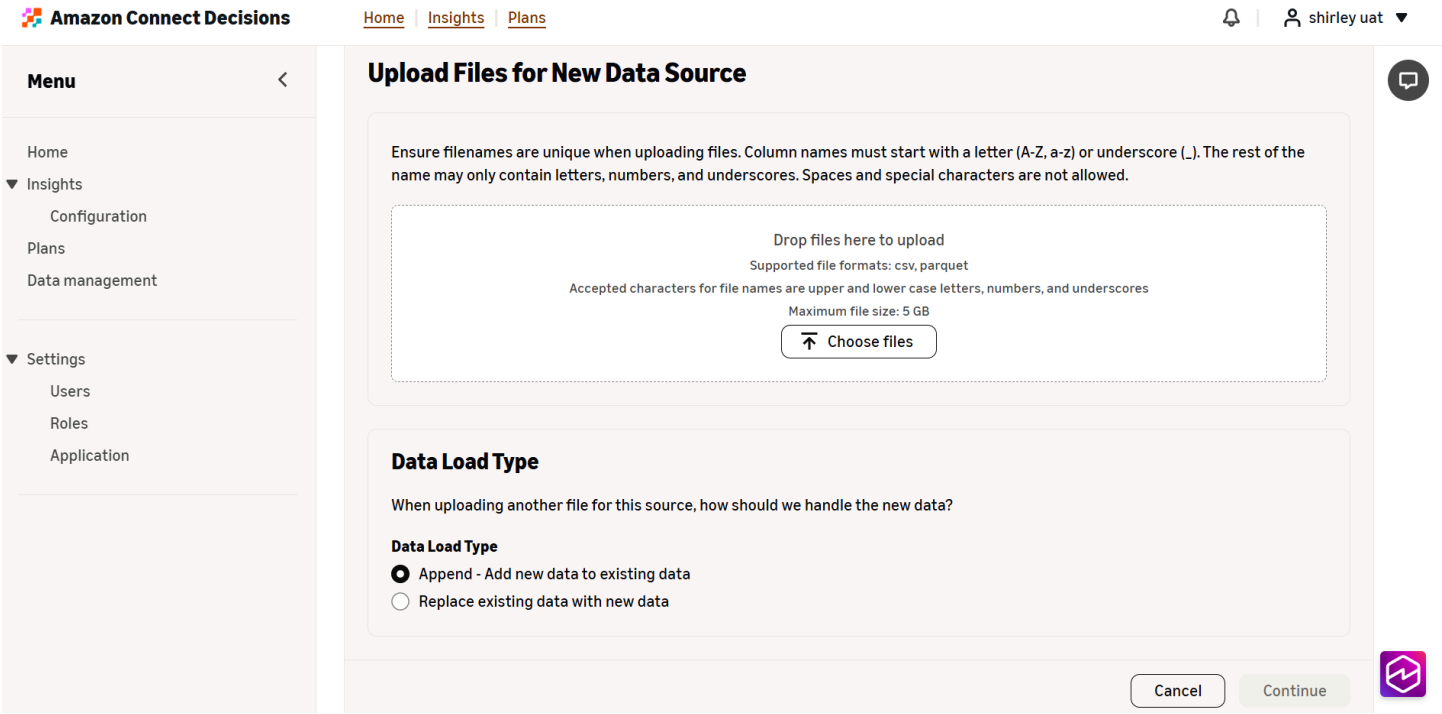
To start onboarding your data, click on **Review** for the **Connect your data** topic card or navigate to the **Data Management** tab in the 'Hamburger Menu' in Amazon Connect Decisions. Here you can see all of your existing source flows. If you have not set one up yet, click **"Connect New Source"** to begin.



Upload Your Source Data

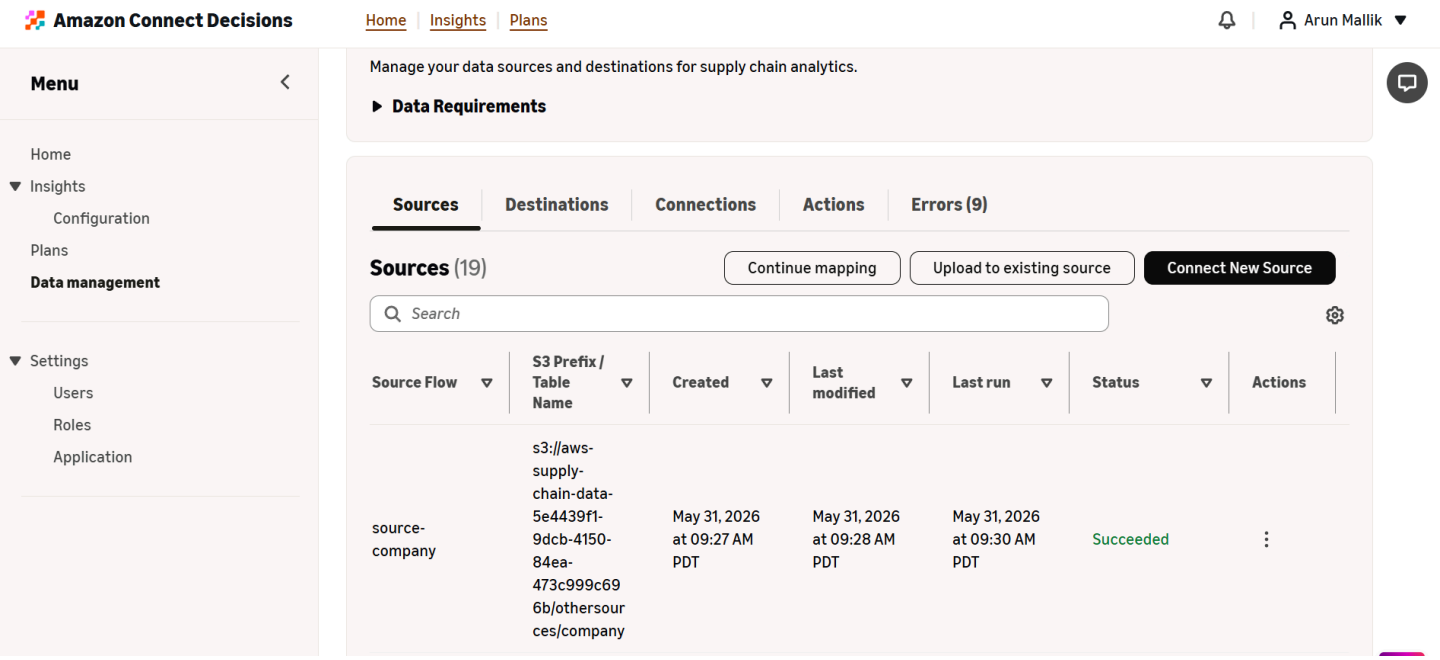
Upload your CSV files containing source data based on the required CDM tables for your use case. You can choose how you want to handle data updates:

- **Append**: Add new data to existing data
- **Replace**: Replace existing data with new data



When you upload files, Amazon Connect Decisions automatically creates a folder structure in S3 for that data including:

- A parent folder named after your selected source system
- A subfolder named after your selected source table name
- All files under a subfolder are saved against the same source table
- This file structure is also used to create the Amazon S3 folder path

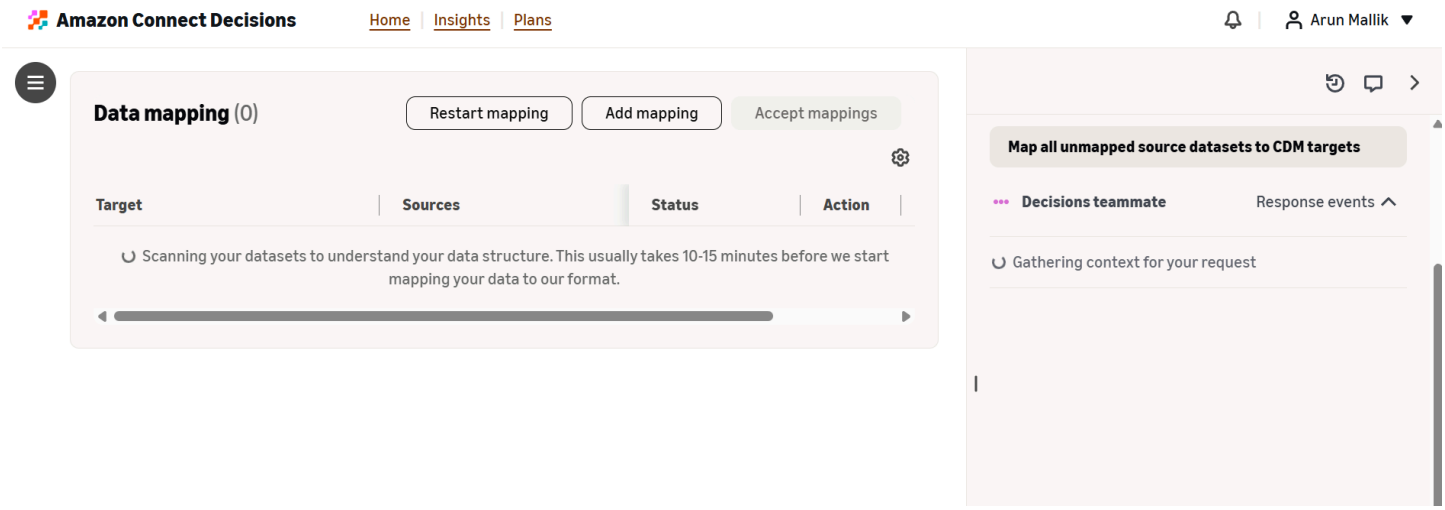


Source-to-CDM Destination Mapping

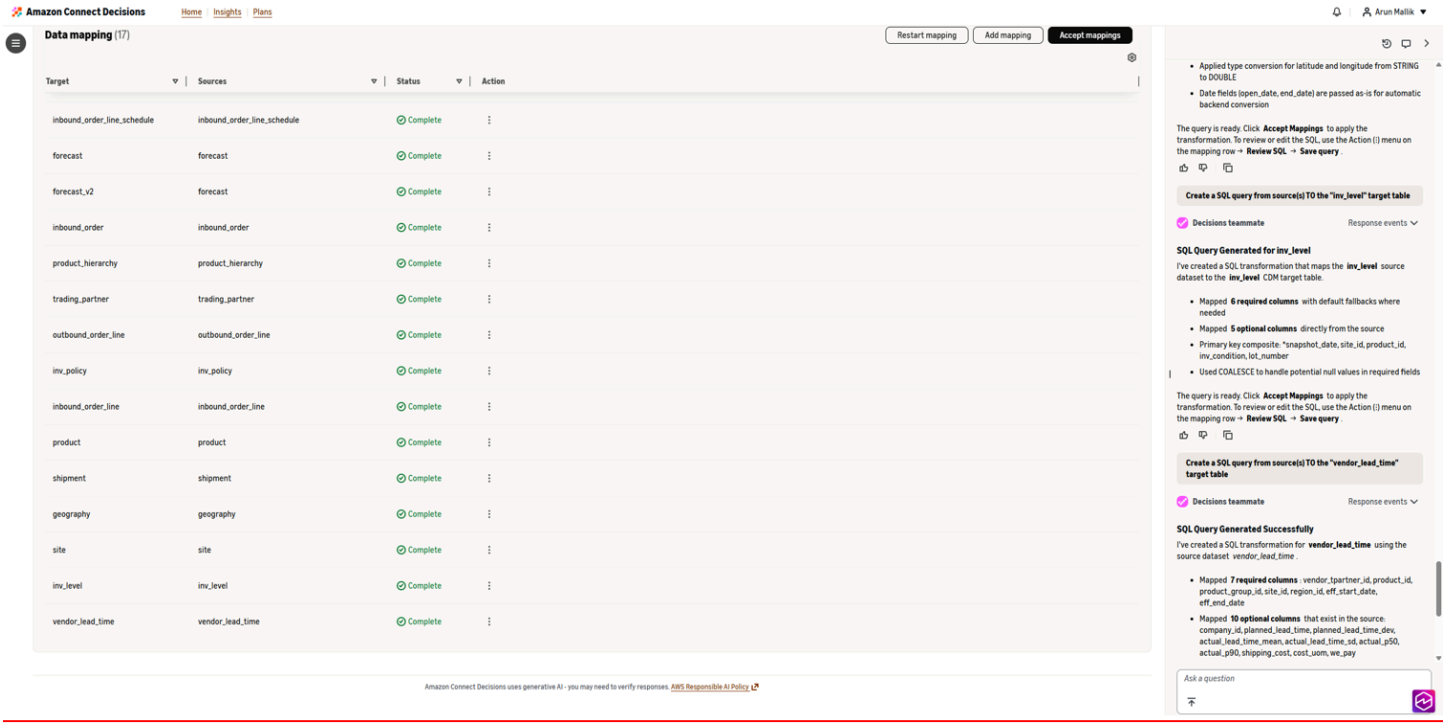
Once your files are uploaded, Amazon Connect Decisions begins analyzing your data and map it automatically to one or many of Amazon Connect Decisions's CDM destination tables.

What to Expect

- This step can take between 10-15 minutes depending on the amount of data uploaded
- The Data Agent works in the background to identify the best CDM destination datasets for your source data.
- *Navigating away from this page will cause automated mappings to fail.* While waiting, please keep the Amazon Connect Decisions and Data Management tab open to ensure automated mapping completes.

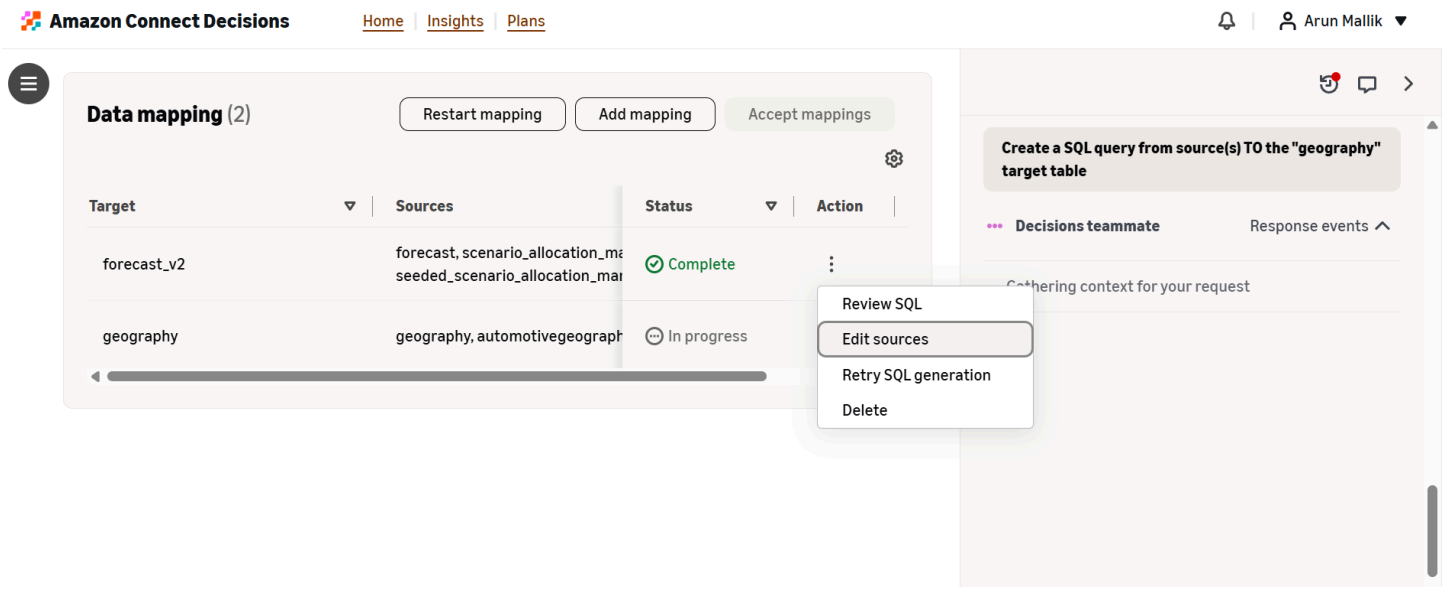


Once complete, the Data Agent provides rationale on source-to-destination mappings based on overlapping data which you can review and ask questions to the agent on any mapping results.



To review and edit source mappings, you can:

- Interact directly with the Data Agent using natural language to update source-destination mappings.
- Click on the **Actions** and select **"Edit Sources"**.



Editing Mappings

From here, you can:

- Update source and destination mapping manually if needed
- Ask questions using the Data Agent on the right-hand side of the screen to confirm the mappings
- Reference user guides to learn more about specific datasets

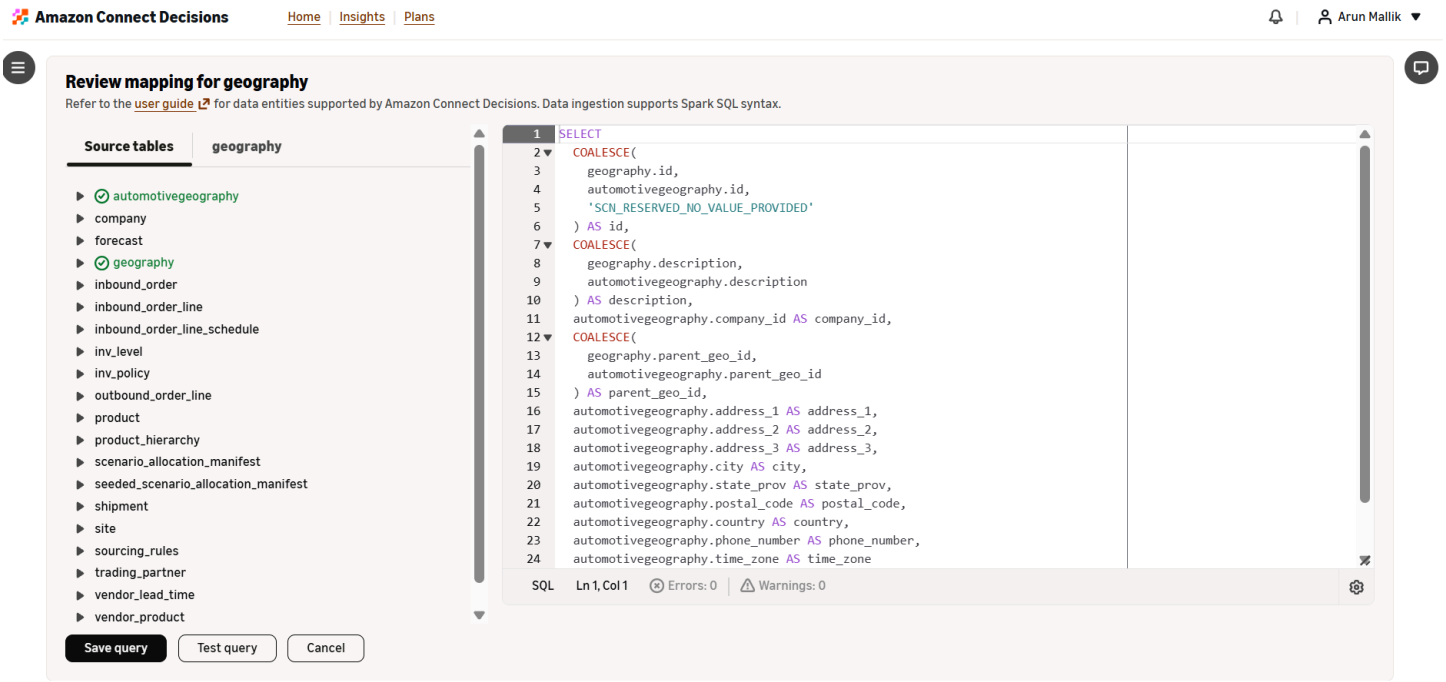
Column/Data Mapping

After source-to-destination mapping is complete, Amazon Connect Decisions will automatically create SQL transformation queries from your source dataset to CDM destination. After any of your mappings complete, you will receive a notification from the Data Agent detailing the result of the mapping.

From here, you should review the SQL generated for mappings by selecting **"Review SQL"** from the Action menu.

Reviewing the mapping (SQL), you'll see:

- Source dataset columns you've added
- Destination CDM table columns for reference
- The transformation SQL connecting them
- Rationale for mapping provided by the Data Agent



Editing Mappings

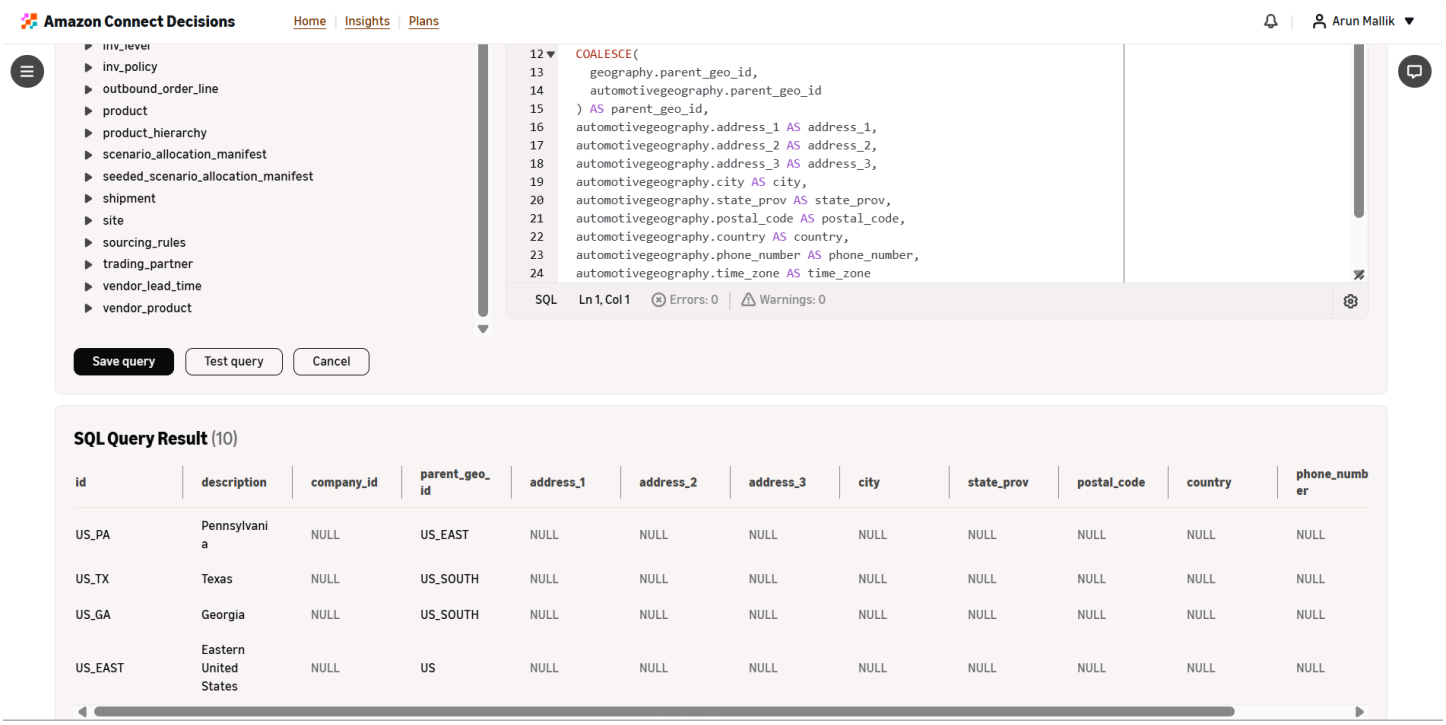
You have two options for editing any mappings:

- **Work with Data Agent**: Use natural language to ask questions, manage, and update the mappings
- **Edit SQL Directly**: If you're familiar with SQL, you can modify the query directly

Testing Your Changes

As you edit the mapping query, continue to test it using the **"Test Query"** functionality which will give you a scrollable preview of how a sample of how your data is being transformed into destination CDM. Use this to ensure your transformation runs properly and to validate any appropriate updates from your source-to-destination CDM.

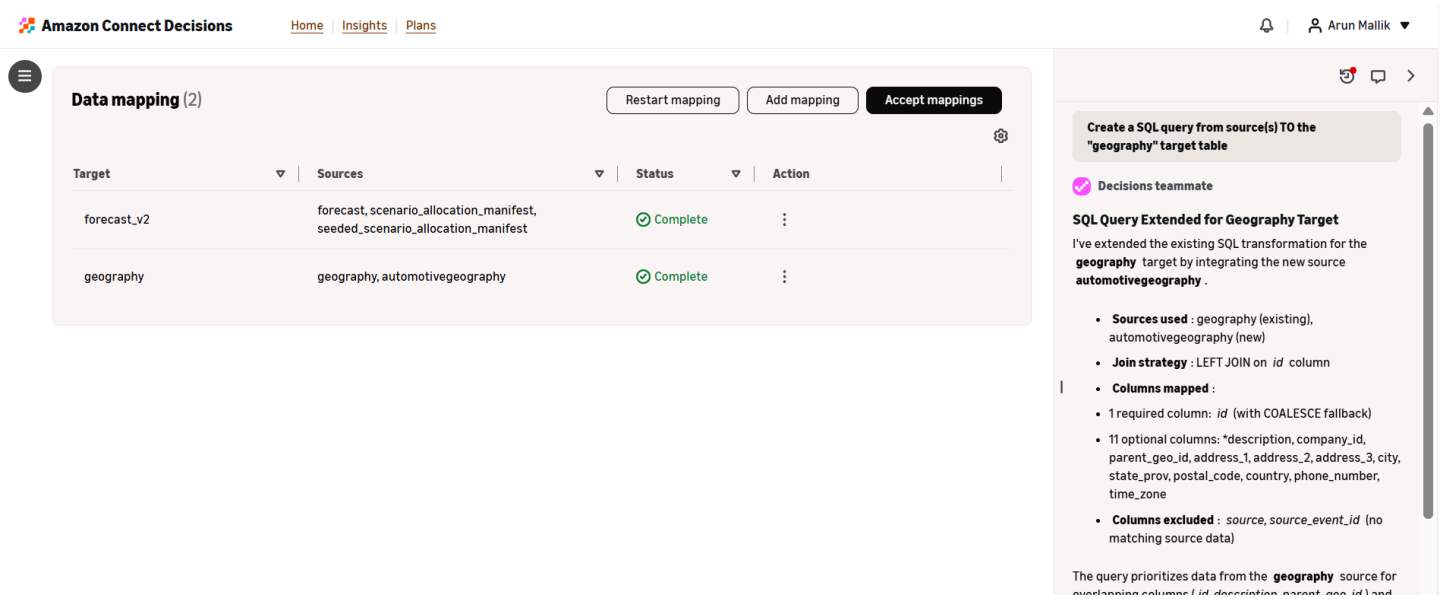
Once you are satisfied with the mapping output, select "**Save Query**" to save the transformation query for that source-destination pair.



Review and Accept Mappings

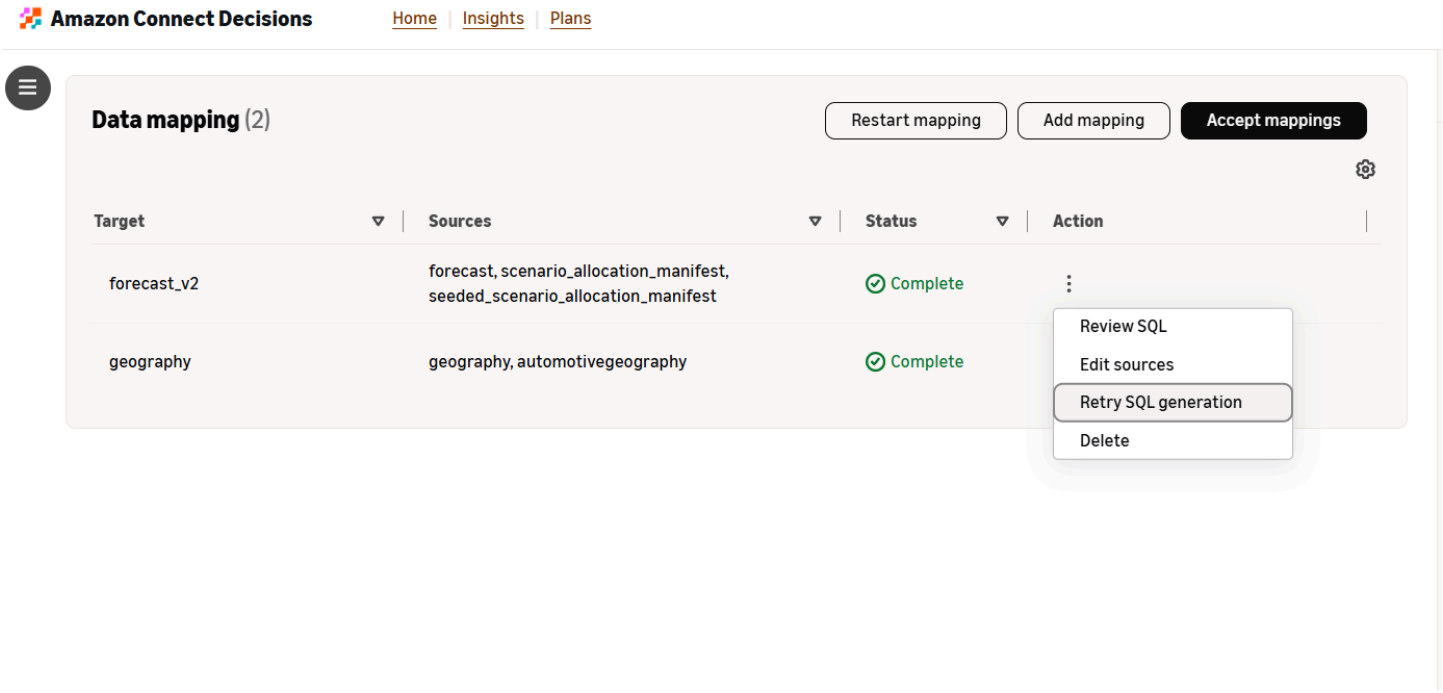
Review the remaining mappings for each of your source datasets. The Data Agent remains persistent on the right-hand side of the screen for questions or troubleshooting help.

Once you're satisfied with all mappings, accept them to complete data onboarding by clicking on **Accept mappings.**



Handle Failed Mappings

If any mappings failed, you can select **"Restart mapping"** to restart all mappings, or manually retry a single mapping from the Actions menu via **"Retry SQL generation"**. The Data Agent can also retry mappings using natural language and will continue to help you identify and resolve issues if errors continue to persist.

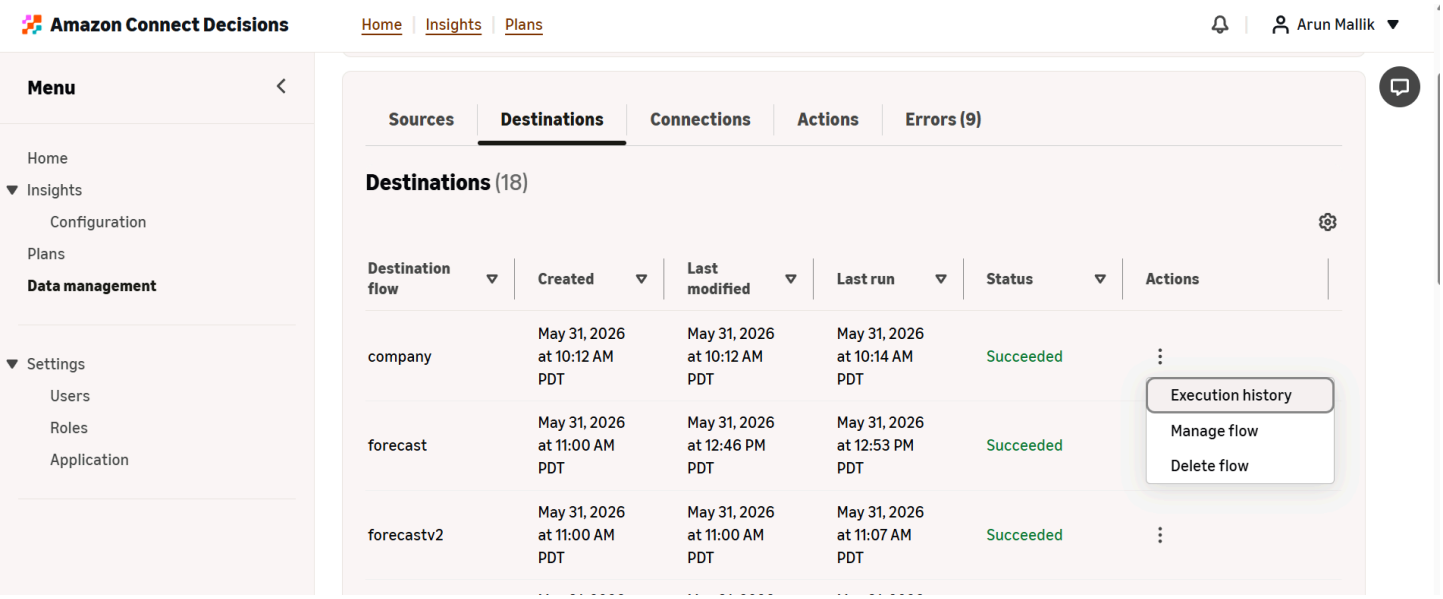


Monitor Your Flows

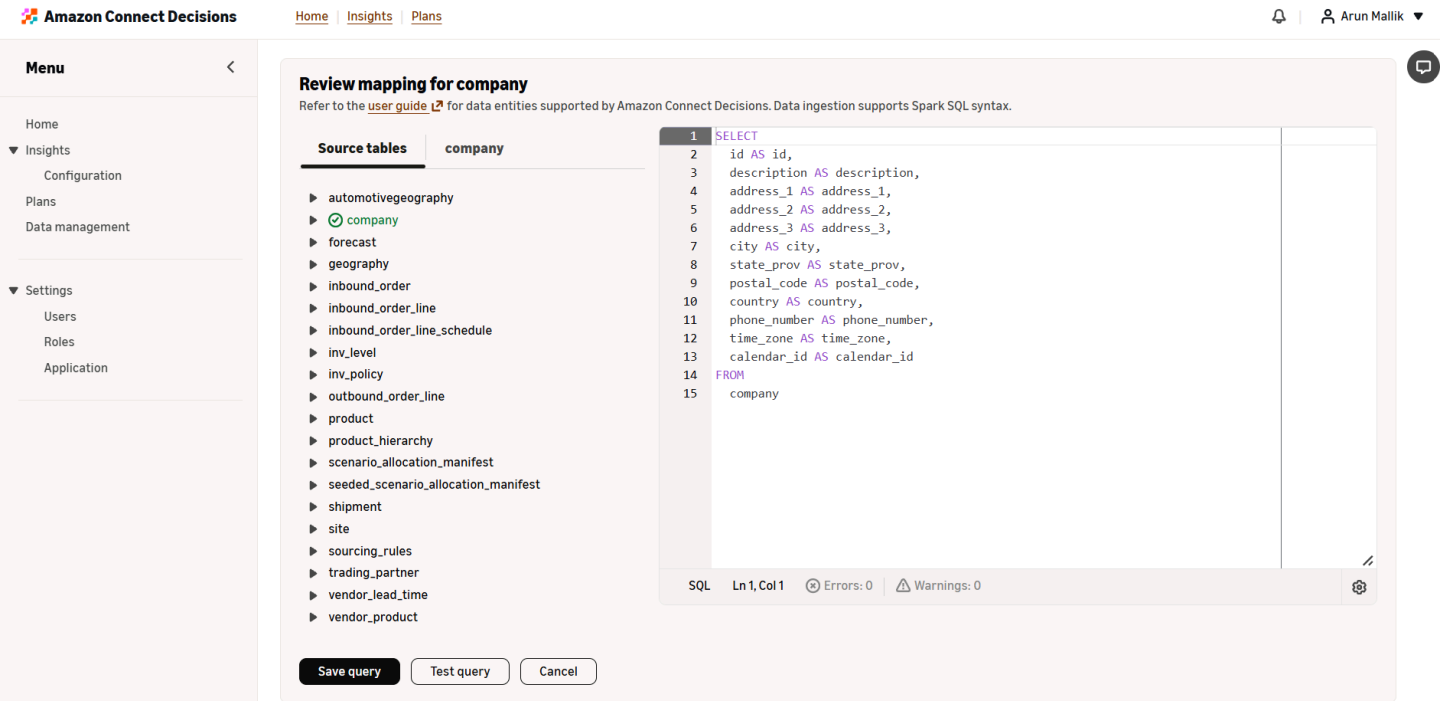
Destinations Tab

Upon accepting mappings, you'll be navigated to the **Destinations** tab within **Data Management** where you can:

- Review destination flows
- Manage and edit mappings ("Manage Flow")
- Delete obsolete flows
- Review execution status for these flows



Selecting **"Manage Flow"** will bring you back to the Data Mapping experience where you can continue to work with the Data Agent to refine mappings over time.



Sources Tab

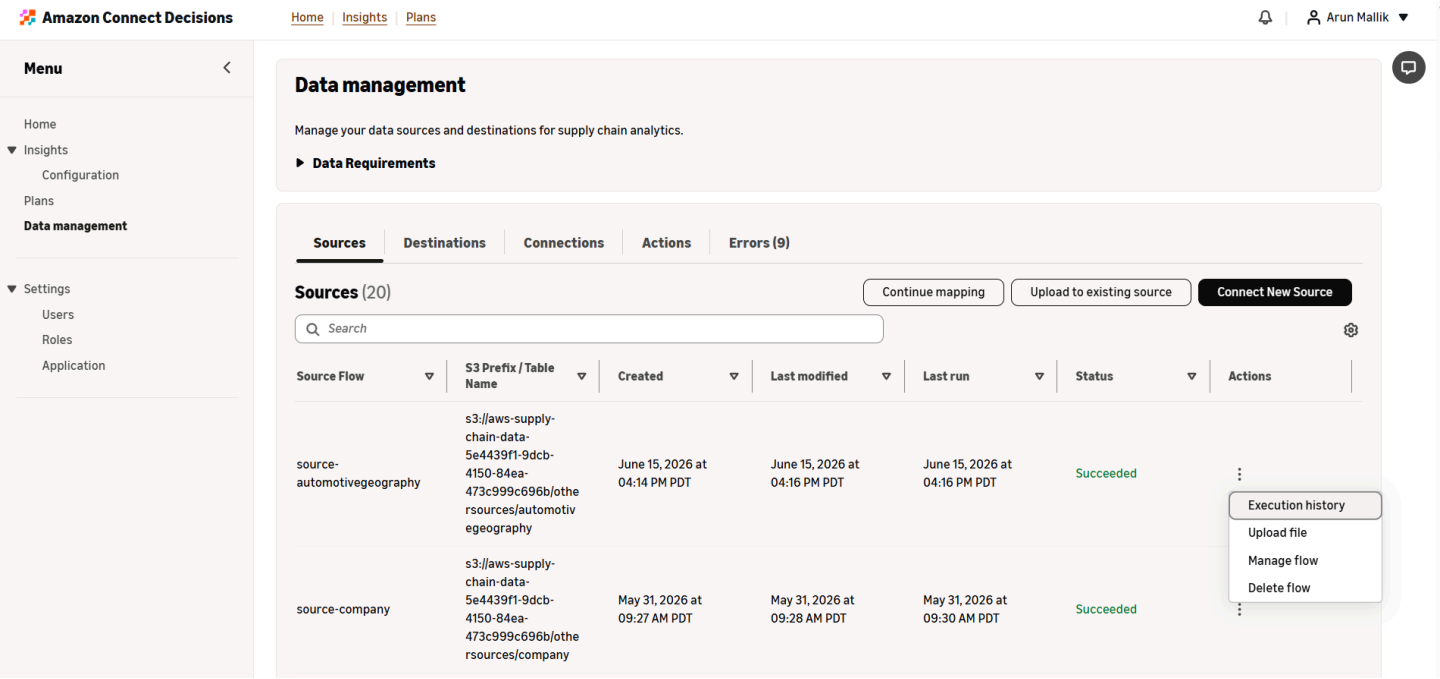
Navigating back to the **Sources** tab you can find:

- The source dataset that has been created
- Its associated S3 bucket

- Options to:
  - Append more source data via another file upload
  - Manage the flow
  - Delete the flow
  - Review executions

Selecting **"Manage Flow"** will bring you back to the Data Mapping experience where you can continue to work with the Data Agent to refine mappings over time.

You also have access to **Create a New Source** as needed to restart the Data Onboarding process for any new data sources.



Best Practices

Data Preparation

- Follow steps in the Prerequisites section
- Use UTF-8 encoding for all CSV files
- Ensure filenames are unique
- Validate data quality before uploading

Working with Data Agent

- Be specific in your requests
- Ask for explanations when you don't understand any of its decisions
- Test all SQL changes before accepting
- Use the Preview feature to verify transformations

Ongoing Maintenance

- Keep your source data updated
- Monitor flow execution regularly
- Address data errors promptly when notified
- Document custom transformations for your team

Connecting to Your Database with JDBC

This guide walks you through connecting your database to Amazon Connect Decisions using **Java Database Connectivity** (JDBC). You'll set up secure encryption for your database credentials and establish a connection that Amazon Connect Decisions can use to access your data.

What is JDBC Connection and When Should You Use It?

JDBC connection allows Amazon Connect Decisions to connect to your existing database to read data, rather than requiring you to export and upload CSV files or set up your own Extraction, Transformation, Load (ETL) pipelines to S3. This approach is ideal when:

- Your data is already stored in an AWS Glue-compatible relational database. Refer to this guide for compatible databases and versions.
- You want real-time or near-real-time data access without manual file exports
- Your data volume is large and frequently updated
- You prefer to keep your data in its current location rather than duplicating it
- If you're working with smaller datasets or prefer file-based uploads, the standard CSV upload process may be simpler for your needs. Refer to Data Onboarding User Guide for more details on this process.

Prerequisites

Before you begin, ensure you have:

- An AWS account with permissions to create KMS keys and Secrets Manager resources
- Your AWS account ID and the region where Amazon Connect Decisions will operate
- Database connection details: hostname, port, database name, and credentials
- Administrative access to your database to verify connectivity
- Your database configured to accept connections from AWS services

Create a Customer-Managed KMS Key

Before connecting your database to Amazon Connect Decisions, you'll need to set up encryption for your database credentials. AWS Key Management Service (KMS) provides this security layer, ensuring your connection details remain protected.

Create Your KMS Key

1. **Navigate to AWS KMS Console**
   - Open the AWS Management Console in your browser
   - In the search bar at the top, type "KMS" and select "Key Management Service" from the results
   - This opens the KMS dashboard where you'll manage encryption keys
2. **Initiate key creation**
   - On the KMS dashboard, locate and click the **Create key** button in the upper right
   - This starts the key creation wizard that will guide you through the setup process
3. **Configure key type and usage**
   - On the "Configure key" page, select **Symmetric** as the key type (this is the default and recommended option)
   - Keep "Encrypt and decrypt" selected under key usage
4. **Set key identification details**
   - In the "Alias" field, enter a descriptive name for your key, such as `aws-supply-chain-database-key`
   - In the "Description" field, add context like "Encryption key for Amazon Connect Decisions database credentials"

- Optionally, add tags to help organize and track your AWS resources (e.g., Key: "Project", Value: "Amazon Connect Decisions")

5. **Define key administrative permissions**
   - Select the IAM users or roles who should be able to manage this key (create, delete, modify policies)
   - At minimum, include your own Admin role to ensure you can modify the key later if needed
   - These administrators can manage the key but won't automatically have permission to use it for encryption/decryption
   - On the "Key Deletion" section, Allow key administrators to delete this key. (this is the default and recommended option)
6. **Define key usage permissions**
   - On this page, you'll see options to select IAM users and roles that can use the key
   - Skip selecting specific users here, you'll configure service permissions in the next step
7. **Configure the key policy for Amazon Connect Decisions services**
   - You'll see a policy editor with default JSON
   - In the KMS key policy editor, append the following statement to your existing "Statement" array
   - This policy grants your account full control and allows Amazon Connect Decisions's services (Secrets Manager and Glue) to decrypt your database credentials

```
{
  "Sid": "Allow GDIS service to decrypt",
  "Effect": "Allow",
  "Principal": {
    "Service": "scn.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey",
    "kms:CreateGrant",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*"
}
```

8. **Review and finalize**

- Review all your configuration settings on the summary page
- Verify that your alias, description, and policy are correct
- Click **Finish** to create the key
- Once created, you'll be returned to the KMS dashboard where your new key will appear in the list

What to Expect

Key creation is immediate. Once created, you'll see your new key listed in the KMS console with a status of "Enabled." The key is now ready to encrypt your database credentials in Secrets Manager.

Configure AWS Secrets Manager

Now that you have a KMS key, you'll create a secret in AWS Secrets Manager to securely store your database credentials, then configure a resource policy that allows Amazon Connect Decisions to access this secret.

Create Your Secret

1. **Navigate to AWS Secrets Manager**
   - In the AWS Management Console search bar, type "Secrets Manager"
   - Select "Secrets Manager" from the results to open the service dashboard
2. **Start creating a new secret**
   - Click the **Store a new secret** button
   - On the "Choose secret type" page, select **Other type of secret** (this gives you flexibility to structure your credentials)
3. **Enter your database credentials**
   - In the key-value pairs section, add your database connection details as **strings**:

```
Key: username, Value: your database username
Key: password, Value: your database password
Key: host, Value: your database hostname (e.g., database.example.com)
Key: port, Value: your database port (e.g., 3306 for MySQL)
Key: database, Value: your database name
```

4. **Select your encryption key**

- Under "Encryption key," select **Choose an AWS KMS key**
- From the dropdown, select the KMS key you created in Step 1 (e.g., `aws-supply-chain-database-key`)
- This ensures your credentials are encrypted with your customer-managed key

5. **Name your secret**
   - Enter a descriptive name for your secret, such as `aws-supply-chain-production-database`
   - Optionally, add a description like "Database credentials for Amazon Connect Decisions production environment"
   - Add tags if desired for organization (e.g., Key: "Environment", Value: "Production")
6. **Add Resource Permissions**
   - Click "Edit Permissions". In the policy editor, paste the following policy. This policy allows Amazon Connect Decisions's services to read your secret

```
{
  "Version" : "2012-10-17",
  "Statement" : [ {
    "Effect" : "Allow",
    "Principal" : {
      "Service" : "scn.amazonaws.com"
    },
    "Action" : [ "secretsmanager:GetSecretValue", "secretsmanager:DescribeSecret" ],
    "Resource" : "<COPY-THE-SECRET-ARN-HERE-AFTER-CREATING>"
  } ]
}
```

7. **Save the policy**
   - Click **Save** to apply the resource policy
   - The policy is now active and allows Amazon Connect Decisions to retrieve your database credentials
8. **Configure rotation (optional)**
   - For this setup, you can skip automatic rotation by selecting **Disable automatic rotation**
   - You can enable rotation later if your security policies require it
9. **Review and create**
   - Review all your secret details

- Click **Store** to create the secret
- You'll be returned to the Secrets Manager dashboard

10 **Save your Secret ARN**

- Find your newly created secret in the secrets list
- Click on the secret name to open its details page
- At the top, you'll see the Secret ARN
- Copy and save this ARN
- The ARN format looks like: `arn:aws:secretsmanager:us-east-1:123456789012:secret:aws-supply-chain-production-database-AbCdEf`

11 **Edit Resource Permissions**

- Click "Edit permissions"
- Paste the copied Secret ARN and replace `<COPY-THE-SECRET-ARN-HERE-AFTER-CREATING>` with your copied ARN
- Click **Save** to attach the policy

What to Expect

Your secret is now securely stored and encrypted with your KMS key. Amazon Connect Decisions's services have permission to retrieve the credentials when establishing a database connection, but the credentials remain encrypted at rest and in transit.

Connect Your Database to Amazon Connect Decisions

With your KMS key and secret configured, you're ready to establish the JDBC connection in Amazon Connect Decisions.

Configure Your JDBC Connection

1. **Navigate to Amazon Connect Decisions > Data Management**
   - Log into your Amazon Connect Decisions instance
   - From the main navigation, select "Data Management"
   - Within the tab navigation, navigate to "Connections"
   - Select "New Connection" to create a new Connection
2. **Enter your connection details**

- **Connection name (required):** Enter a unique identifier for this connection (e.g., "production-database")
- **Description (optional):** Add details about the purpose and usage of this connection to help your team understand what data it accesses
- **JDBC URL (required):** Enter your full JDBC connection string in the format: `jdbc:<database-type>://<hostname>:<port>/<database>` (e.g., `jdbc:postgresql://db.example.com:5432/mydb`)
- **Schema name (optional):** Specify the database schema if needed (e.g., "public", "dbo", "myschema"). Leave blank to use your database's default schema
- **Secret ARN (required):** Paste the Secret ARN you saved from Step 2. This allows Amazon Connect Decisions to securely retrieve your database credentials from Secrets Manager.
- **Enforce SSL connection:** Keep this checkbox selected (recommended) to require SSL/TLS encryption for your database connection
- **VPC endpoint service name (required):** Enter your VPC endpoint service name for private connectivity via AWS PrivateLink (format: `com.amazonaws.vpce.<region>.vpce-svc-xxxxxxxxx`)

3. **Connect to your database**

- Click "Connect" to test and establish the connection. Amazon Connect Decisions will verify that it can successfully connect to your database using the provided credentials. This step can take up to 2 minutes, so please do not leave this screen during connection.
- If the connection succeeds, you'll be automatically navigated to table selection
- If the connection fails:
  - Review your connection details to ensure all fields are accurate:
    - Verify your Secret ARN is correct
    - Confirm your database credentials are accurate
    - Check that your JDBC URL format is correct
    - Ensure your database is configured to accept connections from AWS services
    - Verify your KMS key and Secrets Manager policies are correctly configured
  - You can also use the chat experience to help troubleshoot connection issues by asking questions like "Why is my database connection failing?" or "Help me debug my JDBC connection"

4. **Select tables to ingest**

- Once connected, you'll see the Select Tables screen showing all available tables from your database
- Select the checkbox next to each table you want to ingest

5. **Configure table refresh schedule**
   - For each selected table, click the three-dot menu in the Action column and select "Schedule refresh"
   - In the Configure load details dialog, set:
     - **Cadence:** How often to refresh (Hourly, Daily, Weekly, or Custom)
     - **Start hour:** The time for refresh to begin (displayed in UTC with your timezone offset)
     - **Refresh type:** Choose Complete refresh (replace all data) or Incremental update (add new data to existing; requires selecting a Record timestamp column)
     - Repeat for each table as needed
   - Click Start mapping when all tables are configured
6. **Continue with data mapping**
   - From this point forward, the experience is identical to our Data Onboarding flow
   - Follow the Data Mapping section of the Data Onboarding User Guide to complete your setup

What to Expect

Once your connection is established and tables are selected, Amazon Connect Decisions can read data from your database. The connection remains active and secure, with credentials encrypted and managed through AWS Secrets Manager. You won't need to manually update credentials in Amazon Connect Decisions, any changes you make in Secrets Manager will automatically be reflected.

Best Practices

Security and Access Management

- **Store credentials securely**: Always use AWS Secrets Manager to store database credentials, never hardcode credentials in connection strings or configuration files
- **Enable SSL/TLS encryption**: Keep the "Enforce SSL connection" option enabled to ensure data is encrypted in transit

- **Review KMS and Secrets Manager policies regularly**: Ensure only authorized services and accounts have access to your encryption keys and secrets
- **Use least-privilege access**: Grant only the minimum necessary permissions to database users that Amazon Connect Decisions will use for connections

Connection Configuration

- **Use descriptive connection names**: Choose clear, meaningful names that indicate the environment and purpose (e.g., "production-inventory-db" rather than "db1")
- **Document your connections**: Use the Description field to note what data the connection accesses, who owns it, and any special considerations
- **Test connections before proceeding**: Always verify your connection works before selecting tables and configuring refresh schedules
- **Validate JDBC URL format**: Double-check your JDBC URL syntax matches your database type to avoid connection errors

Data Refresh Strategy

- **Choose appropriate refresh cadence**: Select refresh frequency based on how often your source data changes and your business needs
- **Schedule refreshes during low-activity periods**: Configure refresh times when your database has lower load to minimize performance impact
- **Use incremental updates when possible**: For large datasets with frequent changes, incremental updates are more efficient than complete refreshes
- **Select meaningful timestamp columns**: When using incremental updates, choose columns that accurately reflect when records were created or modified

Working with the chat for troubleshooting

- **Be specific in your requests**: Provide clear context when asking for help troubleshooting connection or mapping issues
- **Ask for explanations**: If you don't understand the recommendations or generated SQL queries, ask for clarification

- **Test all SQL changes before accepting**: Use the preview feature to verify transformations work as expected with your actual data
- **Leverage the chat for troubleshooting**: When connections fail or refreshes encounter errors, ask diagnostic questions like "Why is my connection failing?" or "Help me understand this refresh error"

Ongoing Maintenance

- **Monitor refresh execution regularly**: Check the Destinations and Sources tabs in Data Management to ensure refreshes are completing successfully
- **Address errors promptly**: When Amazon Connect Decisions alerts you to refresh failures, investigate and resolve issues quickly to avoid data gaps
- **Update credentials securely**: When database passwords change, update them in AWS Secrets Manager, Amazon Connect Decisions will automatically use the new credentials
- **Document custom configurations**: Keep notes about any special refresh schedules, transformation logic, or connection requirements for your team's reference
- **Review table selections periodically**: As your data needs evolve, revisit which tables you're ingesting and whether refresh schedules still align with business requirements

Understanding the Canonical Data Model (CDM)

The Canonical Data Model (CDM) is the standardized data structure used by . When you onboard your supply chain data, it must be transformed into CDM format so that can process it for planning, forecasting, and operational insights.

This topic explains what the CDM is, why it matters, and which data entities are available.

What is the CDM?

The CDM defines a common set of data entities and fields that represent supply chain concepts such as products, sites, orders, shipments, and inventory. Regardless of the format or structure of your source data, the CDM provides a single, consistent schema that uses across all of its features.

During data onboarding, your source data is mapped to CDM destination tables. The Data Agent can automatically suggest mappings between your source fields and CDM fields, and generate SQL transformation queries to convert your data.

Why the CDM matters

- **Consistency** — All features in operate on the same data structure, ensuring uniform behavior across demand planning, inventory optimization, and lead time insights.
- **Interoperability** — Data from different source systems (ERP, WMS, TMS) is normalized into a single model, enabling cross-system analysis.
- **Simplified onboarding** — The Data Agent uses the CDM as the target schema when generating automated mappings, reducing manual effort.
- **Data quality** — Validation checks run against CDM definitions to catch issues before data is used in production.

Data entity categories

CDM data entities fall into two categories:

- **Non-transactional data** — Reference or master data that changes infrequently, such as products, sites, trading partners, and geographies.
- **Transactional data** — Operational data that changes frequently, such as forecasts, inventory levels, orders, and shipments.

Supported data entities

The following table lists all data entities supported in the CDM.

Supported CDM data entities

Data entity	Type of data	Required
Company	Non-transactional data	Yes
Product	Non-transactional data	Yes
Trading partner	Non-transactional data	Yes
Vendor product	Non-transactional data	Yes
Geography	Non-transactional data	Yes

Data entity	Type of data	Required
Product hierarchy	Non-transactional data	Yes
Transportation lane	Non-transactional data	Yes
Vendor lead time	Non-transactional data	Yes
Site	Non-transactional data	Yes
Vendor holiday	Non-transactional data	Yes
Forecast	Transactional data	Yes
Inventory	Transactional data	Yes
Inbound order (PO/STO)	Transactional data	Yes
Outbound order line	Transactional data	Yes
Shipment	Transactional data	Yes
Inventory policy	Transactional data	Yes
Inbound order line (PO/STO)	Transactional data	Yes
Outbound shipment	Transactional data	Yes
Inbound order line schedule	Transactional data	Yes

Entities required by feature

Not every feature in requires all CDM entities. The following sections describe which entities are required, optional, or not applicable for each feature.

Inventory visibility

CDM entities for inventory visibility

Data entity	Type of data	Required
Company	Non-transactional	Optional
Product	Non-transactional	Yes
Trading partner	Non-transactional	Optional
Vendor product	Non-transactional	Not applicable
Geography	Non-transactional	Optional
Product hierarchy	Non-transactional	Optional
Transportation lane	Non-transactional	Optional
Vendor lead time	Non-transactional	Not applicable
Site	Non-transactional	Yes
Vendor holiday	Non-transactional	Not applicable
Forecast	Transactional	Optional
Inventory	Transactional	Yes
Inbound order (PO/STO)	Transactional	Optional
Outbound order line	Transactional	Optional
Shipment	Transactional	Optional
Inventory policy	Transactional	Yes
Inbound order line	Transactional	Optional
Outbound shipment	Transactional	Optional
Inbound order line schedule	Transactional	Optional

Lead time insights

CDM entities for lead time insights

Data entity	Type of data	Required
Company	Non-transactional	Optional
Product	Non-transactional	Yes
Trading partner	Non-transactional	Yes
Vendor product	Non-transactional	Yes
Geography	Non-transactional	Optional
Product hierarchy	Non-transactional	Optional
Transportation lane	Non-transactional	Yes
Vendor lead time	Non-transactional	Yes
Site	Non-transactional	Yes
Vendor holiday	Non-transactional	Optional
Forecast	Transactional	Not applicable
Inventory	Transactional	Not applicable
Inbound order (PO/STO)	Transactional	Yes
Outbound order line	Transactional	Not applicable
Shipment	Transactional	Yes
Inventory policy	Transactional	Not applicable
Inbound order line	Transactional	Yes
Outbound shipment	Transactional	Not applicable
Inbound order line schedule	Transactional	Yes

Demand planning

CDM entities for demand planning

Data entity	Type of data	Required
Company	Non-transactional	Optional
Product	Non-transactional	Yes
Trading partner	Non-transactional	Not applicable
Vendor product	Non-transactional	Not applicable
Geography	Non-transactional	Optional
Product hierarchy	Non-transactional	Optional
Transportation lane	Non-transactional	Not applicable
Vendor lead time	Non-transactional	Not applicable
Site	Non-transactional	Yes
Vendor holiday	Non-transactional	Not applicable
Forecast	Transactional	Not applicable
Inventory	Transactional	Not applicable
Inbound order (PO/STO)	Transactional	Not applicable
Outbound order line	Transactional	Yes
Shipment	Transactional	Not applicable
Inventory policy	Transactional	Not applicable
Inbound order line	Transactional	Not applicable
Outbound shipment	Transactional	Not applicable
Inbound order line schedule	Transactional	Not applicable

How the CDM relates to data onboarding

When you onboard data into , the process follows these steps:

1. **Upload** — You upload your source data as CSV files to Amazon S3.
2. **Map** — The Data Agent analyzes your source datasets and suggests which CDM destination tables best match your data.
3. **Transform** — SQL transformation queries convert your source data format into CDM format.
4. **Validate** — Quality checks run against the transformed data to verify it conforms to CDM requirements.
5. **Activate** — Once validated, the data flows into and becomes available for features.

For step-by-step instructions on onboarding your data, see the Data Onboarding topic.

Data Validation and Quality Checks

Overview

Data validation ensures your data meets quality requirements before Amazon Connect Decisions capabilities execute. The system validates data based on your configured plans, metrics, and rules to identify issues that could block or degrade performance.

How Data Validation Works

Validation Triggers

Data validation runs automatically at the following times:

- **Insights configuration changes**: When you create or modify metrics, rules, or other configurations
- **Plan creation**: When you create an ad-hoc plan or at each scheduled plan run
- **Data refresh**: After each data refresh to your Destination flows
- **Capability execution**: Before or during AI teammate operations (e.g., when root-causing an exception or determining recommendations)

Validation Types

Amazon Connect Decisions performs two types of validation:

Data Presence Validation verifies that required datasets and fields are loaded based on your configured resources (metrics, rules, plans).

Data Quality Validation validates that provided data meets quality requirements based on your setup configuration, including:

- **Setup Criteria Validation**: Confirms products and sites match your rule criteria (e.g., product categories, site locations)
- **Hierarchy Validation**: Identifies missing hierarchical relationships if you use hierarchies in your setup
- **Scope Validation**: Confirms all necessary data exists for identified products and sites
- **Quality Assessment**: Evaluates data quality and usability for operational requirements

Progressive Validation

Amazon Connect Decisions enables capabilities for products and sites with valid data rather than blocking functionality for your entire dataset. When validation issues affect specific products or sites, the system continues processing products and sites with valid data, identifies products or sites with data issues, and alerts you to the specific items requiring attention. This allows you to begin using capabilities while resolving the remaining data issues.

Accessing Data Validation Errors

You can view data validation errors through three entry points:

1. "Data Validation Errors" metric on the home page
2. Data validation errors topic card on the home page
3. "Data Management" in the left navigation > "Errors" tab

Reviewing Validation Errors

The Errors page displays all open and resolved validation errors. You can search and filter by any of the following columns:

- **ID**: Unique identifier for the validation error
- **Status**
  - **Open**: Error has not been resolved
  - **Resolved**: Error has been fixed and validated
- **Description**: Explanation of the data quality issue
- **Issue Type**
  - **Missing required data**: Mandatory data is not provided to trigger an operation (e.g., no outbound_order_line source table for Supply Plan)
  - **Invalid data values**: Data exists but contains incorrect values (e.g., negative product cost)
  - **Missing relationships**: Required hierarchical or reference relationships are missing (e.g., missing product hierarchies)
  - **Insufficient data**: Not enough data available to perform required operations (e.g., demand plan requires 12 months of historical order data but only 3 months exist)
- **Capability**: The affected capability or resource
  - Supply Plan
  - Demand Plan
  - Insight (includes Exceptions, Recommendations, and RCA for Supply or Demand)
- **Destination**: Impacted destination flow
- **Priority**
  - **Critical**: At least one capability is fully blocked and cannot execute
  - **High**: At least one capability is partially blocked (some products or sites cannot be processed)
  - **Medium**: At least one capability has reduced accuracy (will run but with degraded results)
- **Created at**: Timestamp showing when the error was first detected

Viewing Error Details

Select any error to view detailed information. The detail screen displays the above information along with a Last Occurred On timestamp, related resource and link (the metric, rule, or plan representing the capability impacted by the issue), and a preview of up to 100 rows of impacted data showing how the data validation error is manifesting.

Available Actions

From the error detail screen, you can:

- **Troubleshoot**: Launch the AI teammate to assist with troubleshooting the issue in natural language and receive detailed remediation guidance
- **Resolve Error**: Manually mark the error as resolved if you have fixed the underlying issue
- **Download**: Download the complete affected dataset for detailed analysis and correction

Resolving Data Validation Errors

Resolution Workflow

1. Review the error description and priority to understand the impact
2. Check the impacted data preview to see which specific records are affected
3. Follow the specific recommendation provided for remediation
4. Choose an appropriate action:
   - **For configuration issues**: Work with your managers and planners to adjust the metric, rule, or plan configuration
   - **For mapping issues**: Correct uploaded source data or update data transformations and mappings
   - **For missing or invalid data**: Upload corrected data
5. Manually mark the error as resolved once you have addressed the underlying issue

Working with the AI Teammate

Use the Troubleshoot option to ask questions like "What errors should I focus on first?" or "Which errors are blocking my demand plan?", receive detailed explanations of the issue and its impact, get step-by-step guidance on resolution approaches, and understand how the error affects your specific configuration. The AI teammate can act as a guide to resolving the issue within Amazon Connect Decisions and within your source data systems.

Best Practices

- **Prioritize by severity**: Focus on Critical errors first, as they fully block capabilities from executing. Then address High priority errors that partially block processing, followed by Medium priority issues that reduce accuracy.
- **Review recommendations carefully**: Each error includes specific, actionable guidance tailored to the issue based on your configuration.
- **Use progressive validation to your advantage**: Don't wait to resolve every error before using capabilities. The system enables functionality for valid products and sites while you work on resolving issues for others.
- **Monitor after data refreshes**: Check for new validation errors after each data update to catch issues early before they impact production workflows.
- **Download impacted data strategically**: Use the download option when you need to analyze all affected records beyond the preview, or when you need to provide the complete dataset to your data team.
- **Use the AI teammate for complex issues**: The Troubleshoot option provides contextual assistance that adapts to your specific situation and configuration.
- **Verify resolution**: After fixing data issues, manually mark errors as resolved to confirm your fix was successful and remove them from the Open list.

System Configuration

Settings in Amazon Connect Decisions are organized by scope and audience. Some settings are personal, allowing each user to tailor their own experience. Others are instance-level configurations managed by administrators that affect how the system behaves for all users or how it connects to your broader technology environment.

User-level settings let individuals manage their account information, notification preferences, and how their data access scope is applied to their views.

Instance-level settings allow administrators to configure the access control filter behavior across the organization, establish connections to your ERP and other external systems, and define how the system handles recommended actions.

Together, these settings give your organization the flexibility to adapt Amazon Connect Decisions to your specific operational context while maintaining consistency across your team.

User Profile Settings

Users can access their profile settings by selecting their name in the top right corner of the application and choosing **Profile** from the dropdown menu. The Profile page allows users to manage their account information, notification preferences, and data access settings.

Accessing Profile Settings

To access your profile settings:

1. Select your name in the top right corner of the page
2. Choose **Profile** from the dropdown menu
3. The Profile page displays your account information and settings

Profile Information

The Profile page displays the following account details:

User: Your username

Role: Your assigned role (Admin, Manager, or Planner)

Time zone: Select your preferred time zone from the dropdown menu. This setting determines how dates and times are displayed throughout Amazon Connect Decisions.

Email: Your email address associated with your Amazon Connect Decisions account

Created: The date and time your account was created

Updated: The date and time your profile was last modified

Select **Save** in the top right corner to save any changes to your profile information.

Notification Preferences

The Notification Preferences tab allows you to configure how you receive notifications for various system events. You can choose to receive notifications in the application, via email, or both.

Plans

Plan Generation Success: Choose how you want to be notified when plan generation completes successfully. Options include in-app notifications and email notifications.

Plan Generation Failure: Choose how you want to be notified when plan generation fails. Options include in-app notifications and email notifications.

Insights Configurations

Insights Configurations Succeeded: Choose how you want to be notified when insights configuration completes successfully. Options include in-app notifications.

Insights Configurations Failed: Choose how you want to be notified when insights configuration fails. Options include in-app notifications.

Data Ingestion

Data Ingestion Failed: Choose how you want to be notified when data ingestion fails. Options include in-app notifications and email notifications.

Admin Settings

Admins can configure system-wide notification settings that apply to all users.

Notification retention: Set the number of days after which notifications are automatically removed from the system. Enter a numeric value to specify the retention period.

Select **Save** to apply your notification preferences.

Assigned Scope

The Assigned Scope tab displays your data access permissions and allows you to configure how data views are filtered based on your assigned scope.

Data Access

This section displays your current data access level. If you have access to all sites and products, you will see the message "You have access to all sites and products."

Default View Filter

Filter views by my assigned scope: When enabled, data views automatically filter to show only items within your assigned products and sites. Toggle this setting on or off based on your preference.

When this filter is enabled, you will only see exceptions, plans, and other data relevant to your assigned scope. When disabled, you may see data outside your assigned scope depending on your role permissions.

Select **Save** to apply your filter preferences.

Access Control Filter Toggle

As stated earlier, all users can view all exceptions, irrespective of whether they have the appropriate products and sites configured (mutate actions still require appropriate access). While this makes it easier to share knowledge, users that are focused on only specific products and sites can get overwhelmed by exceptions or recommendations for other products and sites. To help users focus on the exceptions and recommendations that matter to them, they can use the access view toggle as follows:

- First, a user with the 'Admin' role must enable the feature on that instance. Navigate to the Instance Settings page from the left navigation bar
- By default, they will see a toggle which sets the default access view filter for the entire instance. The 'Admin' can either decide to have one unified setting for all users in the instance, or let users decide their preferences

- If they choose unified access view toggle setting, the 'Admin' can also decide if the toggle should be enabled or disabled for all users
- If they choose to let each user select their own preferences, each user will have the option to toggle the access view filter for themselves. Each user can navigate to the User Preferences page from the User dropdown from the top-right corner of the screen

Change the access control toggle for your instance:

1. Choose the **Settings** left-hand side drawer
2. Select **Application**
3. Update the toggle and click save settings

If the setting is enabled, the system will auto-filter exceptions and recommendations listing pages to only show those which have been generated for a product OR site that matches with the access control configuration

For users that have the "Grant full access to all products and sites" enabled, the access view toggle will still show all exceptions and recommendations. If a user has that toggle disabled but has no products or sites configured, the system interprets that as having access to no product and site and so the user will see nothing

The access view filter is considered a different type of filter, and so will not show in the filter chips in the exception and recommendation page. Users can still apply other filters the same way as before, including other product and sites filters

Users can still access exceptions and recommendations for other products OR sites if they turn off the access view toggle, or they have the direct hyperlink to them

Configuring Connections to your ERP

To enable Amazon Connect Decisions to perform operations on your behalf in your Enterprise Resource Planning (ERP) system, you must configure a Connection that specifies the necessary connection parameters and the credentials Amazon Connect Decisions should use during the operation.

Supported ERP systems:

- SAP S/4HANA

Configure the Credentials in Secrets Manager

1. Using your account, use Secrets Manager to Create an Secrets Manager secret
   - When entering the credentials in Secrets Manager, replace the placeholder values below (<username> and <password>) with the actual username and password that Amazon Connect Decisions should use
   - If using the console, choose `Other type of secret` for the `Secret Type`
   - If entering the details through the `Key/value pairs` tab in the console, enter 2 pairs:
     - Key: `username`; Value: <*username*>
     - Key: `password`; Value: <*password*>
   - If using the `Plaintext` tab to enter the secret in the console, enter a JSON object with the two pairs:

```
{
  "Username": "<username>",
  "Password": "<password>"
}
```

2. Encrypt your secret with an AWS KMS Key, take note of the Key's id, as you will need it in subsequent steps
3. Once your secret is created, take note of its Amazon Resource Name (ARN), as you will need it in subsequent steps
   - e.g.: `arn:aws:secretsmanager:<Region>:<AccountId>:secret:<SecretName>-<SixRandomCharacters>`

Configure permissions on the KMS Key

You need to provide the permissions necessary for Amazon Connect Decisions to access and use it.

1. Update your KMS policy to allow Amazon Connect Decisions to access your key through the instance role
   - Note: Replace <YourAccountNumber> and <YourInstanceID> with your AWS account and Amazon Connect Decisions Instance ID.

```
{
    "Sid": "Allow Amazon Connect Decisions to access the AWS KMS Key",
```

```
    "Effect": "Allow",
    "Principal": {
       "Service": "scn.amazonaws.com",
        "AWS": "arn:aws:iam::YourAccountNumber:role/service-role/scn-instance-
role-YourInstanceID"
    },
    "Action": [
       "kms:DescribeKey",
       "kms:CreateGrant",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey",
       "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*"
}
```

2. Update the inline policy for your instance role to grant permission on the key

- Note: Replace <YourSecretArn>, <YourAccountNumber> and <YourInstanceID> with your Secret ARN, AWS account and AWS Supply Chain Instance ID.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": "secretsmanager:*",
            "Resource": "YourSecretArn"
        },
        {
            "Sid": "AllowKmsForSecretsManager",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws:kms:us-east-1:YourAccountNumber:key/YourKeyId"
        }
    ]
}
```

Update the Secrets Manager resource policy for your Secret

1. Update the Secrets Manager resource Policy for your Secret
   - Note: Replace <YourSecretArn> with the ARN of your Secret

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"scn.amazonaws.com"
         },
         "Action":[
            "secretsmanager:GetSecretValue",
            "secretsmanager:DescribeSecret"
         ],
         "Resource":"YourSecretArn"
      }
   ]
}
```

Configure the Amazon Connect Decisions Connection

1. In your instance of Amazon Connect Decisions, navigate to the Data Management page
2. Select the Connections tab
3. Click the Create Connection button
4. In the Create Connector page, click the Select button on the row for SAP S/4HANA connector type
5. In the Configure SAP S/4HANA API Connector page enter the necessary information:
   - Connection Name: unique connection name
   - API Endpoint URL: the OData API endpoint URL of your SAP S/4HANA instance (e.g.: https://<hostname>:<port>)
   - Client Number: the 3-digit SAP client number (e.g.: 100)
   - Secret ARN: the Amazon Resource Name (ARN) of the secret in Secrets Manager where the credentials to be used by Amazon Connect Decisions are stored

6. Click on the `Create Connector` button

Configuring Action Settings

Amazon Connect Decisions allows you to control for which action types it should offer to perform operations on your behalf in your Enterprise Resource Planning (ERP) system. By default, all action types are disabled, and you must enable this feature for each desired action type.

> **Note**
>
> Enabling support for a given action type controls whether the option of Amazon Connect Decisions performing the action on your behalf will be presented throughout the system (e.g.: when reviewing an Insight with a recommendation of the given type). Amazon Connect Decisions will not perform these actions (even when support is enabled) until you accept the specific recommendation.

Supported action types:

- Create Purchase Order
- Update Purchase Order
- Cancel Purchase Order

Configure actions support for each action type:

1. In your instance of Amazon Connect Decisions, navigate to the Data Management page
2. Select the `Actions` tab
3. Find the action type you wish to configure in the listing
4. To enable support for the action type:
   - Select one of the connections listed in the dropdown menu for that action type
   - Note: the dropdown will display only the available connections that have been configured of a type supporting the `Actions` capability (e.g.: `SAP S/4HANA`)
5. To disable support for the action type:
   - Select `No connection` in the dropdown menu for that action type
6. Click `Save` to save your changes

Security

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security *of* the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS compliance programs. To learn about the compliance programs that apply to Amazon Connect Decisions, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Amazon Connect. The following topics show you how to configure Amazon Connect Decisions to meet your security and compliance objectives.

Data Protection

The AWS shared responsibility model applies to data protection in Amazon Connect Decisions. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. You are also responsible for the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the *AWS Security Blog*.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual users with AWS Identity and Access Management (IAM). That way each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We recommend TLS 1.2 or later.
- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon Simple Storage Service.
- If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-2.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a **Name** field. This includes when you work with Amazon Connect Decisions or other AWS services using the AWS Management Console, API, AWS Command Line Interface (AWS CLI), or AWS SDKs. Any data that you enter tags or free-form text fields used for names may be used for billing or diagnostic logs.

Data Encryption

This topic provides information specific to Amazon Connect Decisions about encryption in transit and encryption at rest.

Encryption in transit

All communication between customers and Amazon Connect Decisions and between Amazon Connect Decisions and its downstream dependencies is protected using TLS 1.2 or higher connections.

Encryption at rest

Amazon Connect Decisions stores data at rest using DynamoDB and Amazon Simple Storage Service (Amazon S3). The data at rest is encrypted using AWS encryption solutions by default. Amazon Connect Decisions encrypts your data using AWS owned encryption keys from AWS Key Management Service (AWS KMS). You don't have to take any action to protect the AWS managed keys that encrypt your data. For more information, see AWS owned keys in the *AWS KMS Developer Guide*.

If you change the KMS key used to encrypt data on your Amazon Connect Decisions instance in the AWS console, you must create a new instance to begin using the new key to encrypt your data. Any

data that were encrypted with the previous key won't be retained, and only data will be encrypted with the updated key. If you want to maintain your data from a previous encryption method, you can revert to the key you were using during those conversations.

Your conversations with Amazon Connect Decisions on the webapp and in chat applications are only encrypted with AWS-owned keys.

Cross-region processing

Amazon Connect Decisions is powered by Amazon Bedrock and uses cross-region inference (CRIS) to distribute traffic across different AWS Regions to enhance large language model (LLM) inference performance and reliability. With cross-region inference, you get:

- Increased throughput and resilience during high demand periods
- Improved performance
- Access to newly launched Amazon Connect Decisions capabilities and features that rely on the most powerful LLMs hosted on Amazon Bedrock

Cross-region inferencing works differently based on the AWS Region in which your Amazon Connect Decisions instance is created in.

For all instances created in the US geographical region, Amazon Connect Decisions will use Global CRIS. This means that inference requests will be routed to supported commercial AWS Regions worldwide, optimizing available resources and enabling higher model throughput. Refer to Amazon Bedrock user guide to learn more about Global CRIS.

For all instances created in the EU geographical region, Amazon Connect Decisions will use Geographic CRIS. This means that inference requests are kept within the AWS Regions that are part of the geography where the data originally resides. Refer to Amazon Bedrock user guide to learn more about Geographic CRIS.

For example, a request made from an Amazon Connect Decisions instance created in the US East (N. Virginia) (us-east-1) region can be routed to any AWS Region globally such as Asia Pacific (Sydney) (ap-southeast-2). However, for a request made from an Amazon Connect Decisions instance created in the Europe (Ireland) (eu-west-1) region is routed to an AWS Regions within the EU such as Europe (Frankfurt) (eu-central-1). For more information, see Supported regions for Amazon Connect Decisions.

Although cross-region inferencing doesn't change where your data is stored, your requests and output results may move outside of the Region where the data originally resides. All data is encrypted while transmitted across Amazon's secure network. There's no additional cost for using cross-region inference. For information on where data is stored when you use Amazon Connect Decisions, see Data protection in Amazon Connect Decisions.

IAM for Amazon Connect Decisions

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use Amazon Connect Decisions resources. IAM is an AWS service that you can use with no additional charge.

How does IAM work with Amazon Connect Decisions

Before you use IAM to manage access to Amazon Connect Decisions, learn what IAM features are available to use with Amazon Connect Decisions. To get a high-level view of how Amazon Connect Decisions and other AWS services work with most IAM features, see AWS services that work with IAM in the *IAM User Guide*.

Identity-based policies for Amazon Connect Decisions

Supports identity-based policies: Yes

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Define custom IAM permissions with customer managed policies in the *IAM User Guide*.

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. To learn about all of the elements that you can use in a JSON policy, see IAM JSON policy elements reference in the *IAM User Guide*.

Resource-based policies within Amazon Connect Decisions

Supports resource-based policies: No

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that

support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

To enable cross-account access, you can specify an entire account or IAM entities in another account as the principal in a resource-based policy. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

Policy actions for Amazon Connect Decisions

Supports policy actions: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Include actions in a policy to grant permissions to perform the associated operation.

Policy actions in Amazon Connect Decisions use the following prefix before the action:

```
scn
```

To specify multiple actions in a single statement, separate them with commas.

```
"Action": [
      "scn:action1",
      "scn:action2"
         ]
```

Policy resources for Amazon Connect Decisions

Supports policy resources: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Resource` JSON policy element specifies the object or objects to which the action applies. As a best practice, specify a resource using its Amazon Resource Name (ARN). For actions that don't

support resource-level permissions, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

Policy condition keys for Amazon Connect Decisions

Supports service-specific policy condition keys: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Condition` element specifies when statements execute based on defined criteria. You can create conditional expressions that use condition operators, such as equals or less than, to match the condition in the policy with values in the request. To see all AWS global condition keys, see AWS global condition context keys in the *IAM User Guide*.

Using temporary credentials with Amazon Connect Decisions

Supports temporary credentials: Yes

Temporary credentials provide short-term access to AWS resources and are automatically created when you use federation or switch roles. AWS recommends that you dynamically generate temporary credentials instead of using long-term access keys. For more information, see Temporary security credentials in IAM and AWS services that work with IAM in the *IAM User Guide*.

Forward access sessions for Amazon Connect Decisions

Supports forward access sessions (FAS): Yes

Forward access sessions (FAS) use the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. For policy details when making FAS requests, see Forward access sessions.

Service roles for Amazon Connect Decisions

Supports service roles: Yes

A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Create a role to delegate permissions to an AWS service in the *IAM User Guide*.

Warning

Changing the permissions for a service role might break Amazon Connect Decisions functionality. Edit service roles only when Amazon Connect Decisions provides guidance to do so.

Identity-based policy examples

By default, users and roles don't have permission to create or modify Amazon Connect Decisions resources. They also can't perform tasks by using the AWS Management Console, AWS Command Line Interface (AWS CLI), or AWS API. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

To learn how to create an IAM identity-based policy by using these example JSON policy documents, see Creating IAM policies in the IAM User Guide.

Instance Management IAM Policy

Below is the IAM policy needed to create, update, or delete instances through the console or public API (excludes all Webapp operations).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "scn:*",
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:PutBucketVersioning",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutEncryptionConfiguration",
                "s3:PutBucketPolicy",
```

```
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketPublicAccessBlock",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutBucketOwnershipControls",
                "s3:PutBucketNotification",
                "s3:PutAccountPublicAccessBlock",
                "s3:PutBucketLogging",
                "s3:PutBucketTagging"
            ],
            "Resource": "arn:aws:s3:::aws-supply-chain-*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "cloudtrail:CreateTrail",
                "cloudtrail:PutEventSelectors",
                "cloudtrail:GetEventSelectors",
                "cloudtrail:StartLogging"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "events:DescribeRule",
                "events:PutRule",
                "events:PutTargets"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "cloudwatch:PutMetricData",
                "cloudwatch:Describe*",
                "cloudwatch:Get*",
                "cloudwatch:List*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
```

```
                "organizations:CreateOrganization",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "kms:ListAliases"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:CreateRole",
                "iam:CreatePolicy",
                "iam:GetRole",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "sso:AssociateDirectory",
                "sso:AssociateProfile",
                "sso:CreateApplication",
                "sso:CreateApplicationAssignment",
                "sso:CreateInstance",
                "sso:CreateManagedApplicationInstance",
                "sso:DeleteApplication",
                "sso:DeleteApplicationAssignment",
                "sso:DeleteManagedApplicationInstance",
                "sso:DescribeApplication",
                "sso:DescribeDirectories",
                "sso:DescribeInstance",
                "sso:DescribeRegisteredRegions",
                "sso:DescribeTrusts",
```

```
                "sso:DisassociateProfile",
                "sso:GetManagedApplicationInstance",
                "sso:GetPeregrineStatus",
                "sso:GetProfile",
                "sso:GetSharedSsoConfiguration",
                "sso:GetSsoConfiguration",
                "sso:GetSSOStatus",
                "sso:ListApplicationAssignments",
                "sso:ListApplicationTemplates",
                "sso:ListDirectoryAssociations",
                "sso:ListInstances",
                "sso:ListProfileAssociations",
                "sso:ListProfiles",
                "sso:PutApplicationAuthenticationMethod",
                "sso:PutApplicationGrant",
                "sso:RegisterRegion",
                "sso:SearchDirectoryGroups",
                "sso:SearchDirectoryUsers",
                "sso:SearchGroups",
                "sso:SearchUsers",
                "sso:StartPeregrine",
                "sso:StartSSO",
                "sso:UpdateSsoConfiguration",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Policy best practices

Identity-based policies determine whether someone can create, access, or delete Amazon Connect Decisions resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies

that are specific to your use cases. For more information, see AWS managed policies or AWS managed policies for job functions in the *IAM User Guide*.

- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see Policies and permissions in IAM in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as CloudFormation. For more information, see IAM JSON policy elements: Condition in the *IAM User Guide*.
- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see Validate policies with IAM Access Analyzer in the *IAM User Guide*.
- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see Secure API access with MFA in the *IAM User Guide*.

For more information about best practices in IAM, see Security best practices in IAM in the *IAM User Guide*.

Troubleshooting IAM

Use the following information to help you diagnose and fix common issues that you might encounter when working with Amazon Connect Decisions and IAM.

I'm not authorized to perform an action in Amazon Connect Decisions

If the AWS Management Console that you're not authorized to perform an action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password.

The following example error occurs when the `mateojackson` IAM user tries to use the console to view details about a fictional `my-example-widget` resource but doesn't have the fictional `scn:GetWidget` permissions.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 scn:GetWidget on resource: my-example-widget
```

In this case, Mateo asks his administrator to update his policies to allow him to access the `my-example-widget` resource using the `scn:GetWidget` action.

I'm not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, your policies must be updated to allow you to pass a role to Amazon Connect Decisions.

Some AWS services allow you to pass an existing role to that service instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in Amazon Connect Decisions. However, the action requires the service to have permissions that are granted by a service role. Mary does not have permissions to pass the role to the service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In this case, Mary's policies must be updated to allow her to perform the `iam:PassRole` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I want to allow people outside of my AWS account to access my Amazon Connect Decisions resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Amazon Connect Decisions supports these features, see How Amazon Connect Decisions works with IAM.
- To learn how to provide access to your resources across AWS accounts that you own, see Providing access to an IAM user in another AWS account that you own in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see Providing access to AWS accounts owned by third parties in the *IAM User Guide*.
- To learn how to provide access through identity federation, see Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see Cross account resource access in IAM in the *IAM User Guide*.

Third-party subprocessors

Amazon Connect Decisions uses Boomi, a third-party API, to enable actions to be taken on your behalf in external systems. When you use a feature of Amazon Connect Decisions that connects to your third-party systems, you authorize us to use Boomi as our integration middleware to transmit and process your encrypted data; your data is not stored separately within Boomi.

To learn more about Boomi and how it works, refer to Boomi's public documentation.

Supported Regions

This page describes the AWS Regions where you can use Amazon Connect Decisions. For more information about AWS Regions, see Specify which AWS Regions your account can use in the *AWS Account Management Reference Guide*.

Your data may be processed in a different Region from the Region where you use Amazon Connect Decisions. For information on cross-region processing in Amazon Connect Decisions, see Cross-region processing. For information on where data is stored during processing, see Data protection.

Supported Regions

Amazon Connect Decisions is available in the AWS Management Console, AWS Console Mobile Application, AWS website, AWS Documentation website in the following AWS Regions. These

Regions are enabled by default, meaning you don't need to enable them before use. For more information, see Regions that are enabled by default.

You use Amazon Connect Decisions in the following Regions.

AWS Region Name	Code Name	Geography (US, EU, etc.)
US East (N. Virginia)	us-east-1	US
Europe (Ireland)	eu-west-1	EU

Troubleshooting

When issues arise during setup or day-to-day use of Amazon Connect Decisions, this section provides guidance to help you diagnose and resolve the most common problems. Start by identifying the category that best matches the issue you are experiencing, then follow the troubleshooting steps on the relevant page. If you are unsure which category applies, begin with Common Setup Issues, which covers the broadest range of initial configuration problems.

Common Setup Issues

Referential integrity errors: "product_id values do not match any id in Product dataset"

The most common cause is trailing whitespace in ID fields. Source systems that export from fixed-width databases often pad string fields with spaces. The product master may have clean IDs ("MAT604") while the order line file has padded IDs ("MAT604 "). The system does a strict string match, so these won't join.

Fix: Add TRIM() to all string ID fields in your data flow SQL transforms. Apply it to product_id, ship_from_site_id, customer_tpartner_id, and any other join key. Also check for quoting inconsistencies between files. When re-exporting CSVs, use QUOTE_ALL to prevent type inference issues where numeric-looking IDs (e.g., "111613") get treated as integers in one file and strings in another.

Prevention: Always TRIM all ID fields in your SQL transforms as a default practice, even if you don't see the issue today. Source data can change between exports.

Products in order history missing from product master

Your order history will often contain products that aren't in the current product master (discontinued products, one-time items, test SKUs). The system will reject the entire order file if any product_id doesn't have a matching product master record.

Fix: Either (a) create stub rows in the product master for missing products with minimal required fields (id, description, base_uom), or (b) filter the order history to only include products present in the product master. Option (a) is preferred because it preserves demand history that may be useful for lineage and trend detection.

CSV parsing errors on product master upload

Product descriptions containing commas, quotes, or special characters can break CSV parsing. You may see errors like "Expected 17 fields, saw 19" on specific rows.

Fix: Re-export the file with proper quoting (QUOTE_ALL). Check the specific failing rows for embedded commas in description fields.

Data not appearing after upload

- Verify your file format hasn't changed (extension, column headers, encoding).
- Check that file names and extensions match the expected pattern — renaming .csv to .csv000 or similar will break ingestion.
- Allow up to 30 minutes for data ingestion to complete after upload.
- If column headers change between loads (e.g., columns named by month/year), a pre-processing step is required before upload.

PIV not updating after data refresh

- PIV triggers approximately 15 minutes after ingestion completes and takes ~20-30 minutes to run.
- End-to-end from data upload to fresh PIV: approximately 1–1.5 hours.
- If PIV hasn't updated in 24+ hours, contact support.

Exception counts seem too high or too low

- **Too high:** Threshold may be too loose, or a single product+site may be generating multiple exceptions for different dates. Contact support to review rule configuration.
- **Too low:** Threshold may be too restrictive, or required data (e.g., forecast, inventory levels) may be missing for some products.

Spot-check a few products you know well and compare what the system shows vs your source system.

No financial impact showing on exceptions

Financial impact requires unit cost to be populated in the product data. If cost is missing or zero for a product, no dollar value will display. Check with your support team on cost data coverage — a waterfall approach across multiple cost fields typically provides the best coverage.