

User Guide

Amazon Q Developer



Amazon Q Developer: User Guide

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

What is Amazon Q Developer?	1
Key features of Amazon Q	1
Get started	2
Amazon Q Developer pricing	3
Features	3
Get answers in context to your conversation	4
Diagnose common console errors	4
Develop software	4
Chat about code	4
Get inline code suggestions	4
Transform code	4
Scan your code for security vulnerabilities	5
Contact AWS Support	5
Use Amazon Q in AWS Chatbot	5
Use Amazon Q in the AWS Console Mobile Application	5
Tiers of service	6
Professional tier	6
Free tier	6
Setting up	7
Setting up your AWS account	7
Sign up for an AWS account	7
Create a user with administrative access	8
Setting up authentication for Amazon Q Developer	9
Access options	9
Authorize an Amazon Q subscriptions administrator	13
Authorize an Amazon Q profile administrator	13
Set up an organization instance of Amazon Q	13
Set up an account instance of Amazon Q Developer	15
Set up Amazon Q Developer with IAM	16
Managing subscriptions	16
Prerequisites for subscribing to Amazon Q Developer	16
Subscribing to Amazon Q Developer	17
Enabling trusted access	19
Unsubscribing	20

Troubleshooting subscriptions	21
On AWS	23
Chatting about AWS	23
Working with Amazon Q on AWS websites	24
Example questions	25
Chatting about your resources	25
Chatting about your costs	27
Diagnosing console errors	29
Diagnose common errors in the console	30
Chatting with AWS Support	30
Prerequisites	30
Specify the right service	31
Create a support case	31
Leave feedback	34
Chatting with Amazon Q in AWS Chatbot	34
Add Amazon Q to a chat channel	34
Ask Amazon Q questions in your channel	27
In your IDE	36
Supported IDEs	36
Installing Amazon Q	37
Choose a supported version of your IDE	38
In JetBrains IDEs	39
In Visual Studio Code	40
In Visual Studio	41
IAM principals in your AWS console	43
Understanding AWS coding environments	43
Chatting about code	43
Working with Amazon Q in your IDE	44
Example topics and questions	45
Reporting issues with responses	45
Explaining and updating code	46
Adding workspace context	46
Generating inline suggestions	48
Pausing suggestions	49
Amazon Q code completion in action	53
Suggestions in AWS coding environments	59

Using shortcut keys	68
Using code references	74
Code examples	82
Transforming your code	103
Step 1: Prerequisites	104
Step 2: Configure your project	105
Step 3: Transform your code	106
How it works	108
Troubleshooting	109
Developing software	120
Develop features with <i>/dev</i>	121
Best practices	122
Example tasks	123
Quotas	124
Troubleshooting	124
Scanning your code	125
Types of scans	126
Quotas	124
Starting a scan	127
Addressing findings	132
Supported languages	134
Inline suggestions	134
Code Transformation	135
Security scans	135
On your command line	137
Installing	137
Supported environments	138
Verifying	138
Uninstalling	139
Chat	139
Context integration	139
Context modifiers	139
Usage	140
CLI Completions	140
Popular settings	141
Over SSH	142

Inline	147
Usage	148
Limitations	149
Translating	149
Debugging	150
Expected output	150
Contributing	151
Customizing	152
Preparing	152
Creating	156
Connecting to your data source	156
Customizations and your data	158
Troubleshooting	158
Deleting	159
Evaluating	159
Evaluating	159
Optimizing	160
Troubleshooting	161
Setting up log delivery	161
Understanding Amazon CloudWatch Logs	161
Understanding console error messages	163
Activating	165
Activating a version	165
Updating	167
Creating a new version	168
Adding users and groups	169
Using	170
Dashboard	171
User activity	172
Code impact	172
Security scans	172
Amazon Q and other services	174
Amazon SageMaker Studio	174
Amazon Q Business	175
Amazon Q in AWS Chatbot	175
Amazon Q in Amazon CodeCatalyst	175

Amazon Q in Amazon Connect	175
Amazon Q in Amazon EC2	175
Amazon Q in AWS Glue	176
Amazon Q in VPC Reachability Analyzer	176
Amazon Q in Amazon QuickSight	176
Security	177
Data protection	177
Data encryption	179
Service improvement	180
Opt out of data sharing in the IDE	181
Cross-Region calls	186
Identity and access management	187
Audience	187
Authenticating with identities	188
Managing access using policies	191
How Amazon Q works with IAM	193
Manage access to Amazon Q	200
Amazon Q permissions reference	222
AWS managed policies for Amazon Q	225
Using service-linked roles	231
Compliance validation	239
Resilience	240
Infrastructure security	240
VPC endpoints (AWS PrivateLink)	241
Considerations for Amazon Q VPC endpoints	241
Prerequisites	241
Creating an interface VPC endpoint for Amazon Q	242
Using an on-premises computer to connect to a Amazon Q endpoint	242
Using an in-console coding environment to connect to a Amazon Q endpoint	243
Connecting to Amazon Q through AWS PrivateLink from a third-Party IDE on an Amazon EC2 instance	243
Monitoring	245
CloudTrail logs	245
Amazon Q Developer information in CloudTrail	245
Understanding Amazon Q Developer log file entries	246
Monitoring with CloudWatch	251

Across your organization	252
Expenses per user	253
Accessing Amazon CloudWatch Logs	253
Supported Regions	255
Opt-in Regions	256
Amazon Q Developer service rename	257
Document history	258

What is Amazon Q Developer?

Note

Powered by Amazon Bedrock: AWS implements [automated abuse detection](#). Because Amazon Q Developer is built on Amazon Bedrock, users can take full advantage of the controls implemented in Amazon Bedrock to enforce safety, security, and the responsible use of artificial intelligence (AI).

Amazon Q Developer is a generative artificial intelligence (AI) powered conversational assistant that can help you understand, build, extend, and operate AWS applications. You can ask questions about AWS architecture, your AWS resources, best practices, documentation, support, and more. Amazon Q is constantly updating its capabilities so your questions get the most contextually relevant and actionable answers.

When used in an integrated development environment (IDE), Amazon Q provides software development assistance. Amazon Q can chat about code, provide inline code completions, generate new code, scan your code for security vulnerabilities, and make code upgrades and improvements, such as language updates, debugging, and optimizations.

Amazon Q is powered by [Amazon Bedrock](#), a fully managed service that makes foundation models (FMs) available through an API. The model that powers Amazon Q has been augmented with high quality AWS content to get you more complete, actionable, and referenced answers to accelerate your building on AWS.

Note

This is the documentation for Amazon Q Developer. If you are looking for documentation for Amazon Q Business, see the [Amazon Q Business User Guide](#).

Key features of Amazon Q Developer

Amazon Q Developer includes the following capabilities:

- **Chat** – Amazon Q answers natural language questions in English about AWS, including questions about AWS service selection, AWS Command Line Interface (AWS CLI) usage, documentation,

best practices, and your AWS resources. Amazon Q responds with information summaries or step-by-step instructions, and includes links to its information sources.

- **Conversation memory** – Amazon Q uses the context of your conversation to inform future responses for the duration of your conversation.
- **Code improvements and advice** – Within IDEs, Amazon Q can answer questions about software development, improve your code, and generate new code.
- **Code completion** – As you write code, Amazon Q automatically generates suggestions, in real time, based on your existing code and comments.
- **Troubleshoot and support** – Amazon Q can help you understand errors in the AWS Management Console and provides access to live AWS Support agents to address your AWS questions and issues.

For more information about these and other Amazon Q features, see [Understanding Amazon Q Developer features](#).

Get started with Amazon Q Developer

To quickly get started using Amazon Q, you can access it in the following ways:

AWS apps and websites

Add the [necessary permissions](#) to your IAM identity, and then choose the Amazon Q icon to start chatting in the AWS Management Console, AWS Documentation website, AWS website, or AWS Console Mobile Application. For more information, see [Using Amazon Q Developer on AWS apps and websites](#).

IDEs

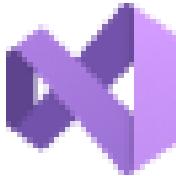
Download the Amazon Q extension and use your AWS Builder ID (no AWS account required) to sign in for free.



[Download Amazon Q in Visual Studio Code](#)



[Download Amazon Q in JetBrains IDEs](#)



[Download Amazon Q in the AWS Toolkit for Visual Studio](#)

From the Amazon Q extension, choose **Open Chat Panel** to start chatting or initiate a development workflow. For more information, see [Installing the Amazon Q Developer extension or plugin in your IDE](#).

Command line

Download [Amazon Q for the macOS command line](#). For more information, see [Using Amazon Q Developer on the command line](#).

AWS Chatbot for Microsoft Teams and Slack

Add the [AmazonQFullAccess](#) managed policy to your IAM identity and channel guardrails for Microsoft Teams or Slack channels configured with AWS Chatbot. For more information, see [Chatting with Amazon Q Developer in AWS Chatbot](#).

Amazon Q Developer pricing

Amazon Q Developer is available through a Free Tier and the Amazon Q Developer Pro subscription. For more information, see [Amazon Q Developer pricing](#).

Understanding Amazon Q Developer features

This section describes the different features of Amazon Q Developer that you might encounter across your AWS experience. The availability of these features depends on whether you're using Amazon Q on AWS apps and websites or in an integrated development environment (IDE).

Get answers in context to your conversation

Amazon Q uses the context of your current conversation to inform its responses. You can ask follow-up questions or refer to its response when you ask a new question.

Diagnose common console errors

With Amazon Q, you can diagnose console error messages directly in the AWS Management Console. Amazon Q provides information about the error and an overview of a potential solution. For more information, see [Diagnosing common errors in the console with Amazon Q Developer](#).

Develop software

After you explain, in natural language, the feature that you want to develop, Amazon Q can use the context of your current project to generate an implementation plan and the accompanying code. Amazon Q can help you build AWS projects or your own applications. For more information, see [Developing software with the Amazon Q Developer Agent for software development](#).

Chat about code

Within integrated development environments (IDEs), Amazon Q can answer questions related to the software development process, including conceptual questions about programming and how specific code works. You can also ask Amazon Q to update and improve code snippets from the chat panel. For more information, see [Chatting with Amazon Q Developer about code](#).

Get inline code suggestions

Amazon Q provides you with code recommendations in real time. As you write code, Amazon Q automatically generates suggestions based on your existing code and comments. For more information, see [Generating inline suggestions with Amazon Q Developer](#).

Transform code

Within IDEs, Amazon Q can update the language version of your code files. Currently, Amazon Q Code Transformation supports updating Java 8 and Java 11 code to Java 17. For more information, see [Upgrading language versions with the Amazon Q Developer Agent for code transformation](#).

Scan your code for security vulnerabilities

Within IDEs, Amazon Q scans your code for security vulnerabilities and code quality issues. You can get security recommendations as you code or scan entire projects to monitor the security posture of your applications throughout development. For more information, see [Scanning your code with Amazon Q](#).

Contact AWS Support

You can create AWS Support cases and chat with a live support agent within Amazon Q to address issues you're having with AWS services. You can access AWS Support with Amazon Q in the AWS Management Console. For more information, see [Using Amazon Q Developer to chat with AWS Support](#).

Use Amazon Q in AWS Chatbot

You can add Amazon Q to your Slack and Microsoft Teams channels that are configured with AWS Chatbot. Amazon Q in AWS Chatbot can answer questions about building at AWS, including those about best practices for building solutions, troubleshooting issues, and identifying next steps. For more information, see [Chatting with Amazon Q Developer in AWS Chatbot](#).

Use Amazon Q in the AWS Console Mobile Application

Amazon Q is integrated with the AWS Console Mobile Application to answer questions about AWS. You configure access the same way that you get access to Amazon Q in the AWS Management Console. For more information, see [Setting up Amazon Q Developer](#).

Understanding tiers of service for Amazon Q Developer

When you use Amazon Q Developer, you either use Amazon Q Developer Pro, which is a paid subscription service, or you use Amazon Q Developer at the free tier. This page explains the difference.

Understanding the Amazon Q Developer Pro tier

To use Amazon Q Developer Pro, you must be a user in IAM Identity Center, and your administrator must subscribe you to Amazon Q Developer Pro. As a user with an Amazon Q Developer Pro subscription, your limits are based on an individual user level in the Amazon Q Console, Q in the IDE, and Q in Code Catalyst.

Subscriptions are not available in the AWS Console Mobile App (ACMA), AWS Chatbot, or on AWS marketing pages. Interactions with Amazon Q through those channels are governed exclusively by free tier limits.

Understanding the free tier

Amazon Q Developer offers a perpetual free tier with monthly limits available to anyone logged in as an AWS Identity and Access Management user or AWS Builder ID user. Exactly which features you can use depends on your interface, and on how you authenticate.

To see the capabilities and limits for Amazon Q Developer Pro and the Amazon Q Developer free tier, visit the [Amazon Q Developer pricing page](#).

Setting up Amazon Q Developer

The following sections describe the steps you need to take before using Amazon Q the first time. If you are an IAM Identity Center administrator who is setting up Amazon Q Pro for your organization, see [Set up an organization instance of Amazon Q](#).

If you are not an administrator, see [Get started with Amazon Q Developer](#).

Topics

- [Setting up your AWS account](#)
- [Setting up authentication for Amazon Q Developer](#)
- [Managing subscriptions](#)

Setting up your AWS account

This page is for customers who are new to AWS. The following sections will help you set up an AWS account and create an administrative user.

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 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*.

Setting up authentication for Amazon Q Developer

There are different ways to authenticate and access Amazon Q Developer features. Choose how you want to get started with Amazon Q.

Topics

- [Access options for Amazon Q Developer](#)
- [Authorize an Amazon Q subscriptions administrator](#)
- [Authorize an Amazon Q profile administrator](#)
- [Set up an organization instance of Amazon Q](#)
- [Set up an account instance of Amazon Q Developer](#)
- [Set up Amazon Q Developer with IAM](#)

Access options for Amazon Q Developer

There are different ways to authenticate and access Amazon Q features. Understanding how your situation differs from the situation of other customers may help you understand issues related to authentication, IDE choices, and billing. You can review the different types of Amazon Q Developer features and security requirements to help you choose how you want to get started with Amazon Q Developer.

			IAM Identity Center	
	Works with AWS Builder ID	Works with IAM principals	Account instances	Organization instances
Amazon Q Developer in the IDE				
Amazon Q Developer on the command line				
Amazon Q in Amazon CodeCatalyst				
Amazon Q on AWS websites				

For information about Amazon Q Business, see [Getting started with Amazon Q Business](#) in the Amazon Q Business User Guide.

AWS Builder ID

If you want to get started quickly with some Amazon Q Developer features, you can create a [Builder ID](#) to use Amazon Q Developer in the IDE. Builder ID is separate from any AWS account or sign in credential. You might use a workforce identity in IAM Identity Center to represent your work-self and a Builder ID to represent your private-self. These identities operate independently. To get started with a Builder ID, see [Install the Amazon Q Developer extension or plugin in your IDE](#).

IAM Principles

Depending on how you use AWS, you may be accustomed to using your [IAM credentials](#) to sign in to the console for all AWS services. With IAM principals, you can use some features of Amazon Q Developer. IAM principals cannot use Amazon Q Developer in the IDE or Amazon Q on the command line. You must authenticate with credentials from either IAM Identity Center or Builder ID. To get started with IAM, see [Add IAM permissions for Amazon Q on AWS websites](#).

 **Note**

Some Amazon Q features are limited for IAM principals. For a list of interaction limits, refer to the Free pricing tier on [the Amazon Q Developer pricing page](#).

IAM Identity Center instances

You can keep managing your workforce access to AWS accounts in the way you always have, while managing Amazon Q subscriptions through IAM Identity Center.

 **Warning**

For compatibility with Amazon Q Pro, you cannot set up IAM Identity Center in an [opt-in Region](#).

Organization instances of IAM Identity Center

An organization instance of IAM Identity Center is the primary form of deploying IAM Identity Center, and in most cases, an organization instance is recommended. If you want access to all Amazon Q Developer features, including enterprise access controls across multiple AWS accounts, then you should use an organization instance.

 **Note**

Identity-aware sessions require an organization instance of IAM Identity Center and are required to enable the full set of Amazon Q Developer features on AWS websites. For more information, see [Enabling identity-aware console sessions](#) in the *IAM Identity Center User Guide*.

Warning

Depending on the structure of your enterprise, you may want to create multiple profiles of Amazon Q Developer across multiple AWS accounts within your organization, and to associate each of those profiles with your organization instance of IAM Identity Center. In such cases, do not add subscriptions for the same IAM Identity Center users to multiple Amazon Q profiles. If you do this, and your users sign in to Amazon Q in the IDE, you will not be able to reliably anticipate with which Amazon Q Developer profile their sessions will be associated.

Account instances of IAM Identity Center

If you don't have plans to adopt IAM Identity Center for your entire organization, you can use an [account instance](#) of IAM Identity Center to manage user and group access to Amazon Q Developer features. With an account instance of IAM Identity Center, you can create an isolated deployment of Amazon Q in a single AWS account. To get started with an account instance of IAM Identity Center, see [Set up an account instance of Amazon Q Developer](#).

Note

Some Amazon Q Developer features are limited for account instances. For a list of interaction limits, refer to the Free pricing tier on [the Amazon Q Developer pricing page](#).

Use cases for account instances with Amazon Q Developer Pro

Although AWS recommends that you use an organization instance of IAM Identity Center with Amazon Q Developer Pro, there are a few situations in which it might make sense to use account instances. These situations include:

- You are trying out Amazon Q Developer Pro, and you haven't yet decided that you want to deploy it to your entire organization.
- You are the administrator of a single AWS account within an organization. Instead of waiting for the administrator of your organization to implement Amazon Q Developer Pro, you want to go ahead and do it just for the AWS account that you control.
- Your enterprise is large, and does not have a single identity provider, or a single identity store, containing the entire user base that you want to give access to Amazon Q Developer.

Disadvantages to using an account instance include:

- The dashboard will only provide information about users and groups associated with the one account.
- The administrative settings (such as whether to include suggestions with code references) will only be available for the one account.
- When chatting with Amazon Q on AWS websites, a monthly question limit will be imposed across all users.

Learn more about how to manage organization and account instances of IAM Identity Center.

Authorize an Amazon Q subscriptions administrator

When you set up subscriptions for Amazon Q, you are acting as an Amazon Q subscriptions administrator.

To authorize a Amazon Q subscriptions administrator, use the policy under [Allow an administrator to use the Amazon Q service management console](#).

Authorize an Amazon Q profile administrator

When you configure the settings on your Amazon Q Developer profile, you are acting as an Amazon Q Developer administrator.

To authorize a Amazon Q Developer administrator, use the policy under [Allow an administrator to configure the Amazon Q Developer Pro console](#).

Set up an organization instance of Amazon Q

AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage.

For help creating an organization instance in IAM Identity Center, [see Enabling AWS IAM Identity Center](#) in the *IAM Identity Center User Guide*.

Note

When you enable IAM Identity Center in your Organizations management account to manage application access, you can add a service control policy (SCP) to block all interaction with permission sets. This ensures that IAM Identity Center is used only for

access to applications. If an account instance of IAM Identity Center is enabled, IAM Identity Center account access is unavailable by default. For more information, see [Manage access with service control policies \(SCPs\)](#).

For more information, refer to [What is Organizations](#) in The Organizations User Guide.

1. Sign in to the AWS Management Console and open [the Amazon Q subscriptions console](#).

 **Note**

To set up subscriptions for Amazon Q Developer, your AWS management console must be set to US East (N. Virginia).

2. If you are new to IAM Identity Center, choose **Create organization instance**.

 **Note**

If you are an IAM Identity Center administrator who is setting up Amazon Q Developer for your existing organization, the **Connect to Identity Center** section displays **Organization instance of Identity Center connected to Amazon Q**.

3. (optional) In the **Enable identity-aware sessions** section, choose **Enable**. An identity-aware session for the console enhances a user's AWS console session by providing some additional user context to personalize that user's experience. For more information about identity-aware console sessions, see [Enabling identity-aware console sessions](#) in the AWS IAM Identity Center User Guide.
4. In the **Enable identity-aware sessions** dialog box, Choose **Enable**.
5. Under **Select a bundle to get started**, under Amazon Q Developer Pro, choose **Subscribe**.
6. (optional) **Share settings profile with member accounts**. This option is selected by default to provide access to Amazon Q Developer to all associated member accounts. Choose this setting to manage user and group subscriptions on the **Subscriptions** page in the Amazon Q Developer console.

Changing this setting requires authorization as the Amazon Q Developer Pro administrator. You may also change this setting as part of the [Managing subscriptions](#) workflow.

7. Choose whether you want to subscribe users and groups to Amazon Q Developer.

If you are not ready to subscribe, you can choose **Create only**, which will save the Amazon Q Developer managed application that you have been setting up with this process.

If you are ready to subscribe, choose **Create and subscribe to Amazon Q Developer Pro**.

Next step: [Managing subscriptions](#).

Set up an account instance of Amazon Q Developer

Amazon Q Developer and Amazon Q Business both allow you to use account instances of IAM Identity Center. Account instances can manage access to AWS applications without managing access to AWS accounts.

For help creating an account instance in IAM Identity Center, see [Enable account instances in the IAM Identity Center console](#) in the IAM Identity Center User Guide.

1. Sign in to the AWS Management Console and open [the Amazon Q console](#).
2. If you don't have plans to adopt IAM Identity Center for your entire organization, choose **Create account instance**.

 **Note**

If you are an existing IAM Identity Center user who is setting up Amazon Q Developer for your account instance, the **Connect to Identity Center** section displays **Account instance of Identity Center connected to Amazon Q**.

3. Under **Select a bundle to get started**, under Amazon Q Developer Pro, choose **Subscribe**.
4. Choose whether you want to subscribe users and groups to Amazon Q Developer.

If you are not ready to subscribe, you can choose **Create only**, which will save the Amazon Q Developer managed application that you have been setting up with this process.

If you are ready to subscribe, choose **Create and subscribe to Amazon Q Developer Pro**.

Next step: [Manage subscriptions](#).

Set up Amazon Q Developer with IAM

By default, IAM users and roles don't have permission to use Amazon Q Developer in the console. IAM administrators can manage access to Amazon Q Developer and its features by granting permissions to IAM identities. For more information, see [Identity-based policy examples for Amazon Q Developer](#).

 **Note**

IAM principals cannot be assigned to Amazon Q Developer subscriptions, and they do not have access to Amazon Q Developer in the IDE or Amazon Q on the command line.

Managing subscriptions

This section provides instructions for managing Amazon Q Developer subscriptions. It details the prerequisites for subscribing, how to assign users and groups to subscriptions, and the steps to manage your Amazon Q Developer settings. Additionally, it includes troubleshooting tips for common subscription issues to ensure smooth and effective use of Amazon Q Developer services.

Prerequisites for subscribing to Amazon Q Developer

Before you begin, be sure that you've [authorized an Amazon Q Developer subscriptions administrator](#), [authorized an Amazon Q Developer profile administrator](#), and set up either an [organization instance](#) or an [account instance](#) of Amazon Q Developer.

Topics

- [Subscribing to Amazon Q Developer](#)
- [Enabling trusted access](#)
- [Unsubscribing](#)
- [Troubleshooting subscriptions](#)

Subscribing to Amazon Q Developer

Note

If you are using an organization instance of IAM Identity Center, then AWS recommends that you manage your Amazon Q Developer profile from the organization management account.

If you choose to manage it from some other account within the same organization (including a delegated admin account), then you will not be able to change the default profile settings. These include:

- You will receive suggestions with code references.
- All Amazon Q Developer features will be enabled.
- Your data will be encrypted with a AWS KMS key that AWS owns and manages for you.

1. Sign in to the AWS Management Console, and open [the Amazon Q Developer subscriptions console](#).
2. Choose **Subscriptions**.
3. You can view users and groups in your organization's member accounts on the Subscriptions page by enabling **View subscriptions from member accounts** in Settings. When this option is not enabled, the Subscriptions page only displays users and groups in your AWS account.
4. On the Amazon Q subscriptions page, select the users and groups that should be end users of Amazon Q Developer, and choose **Assign**.

It is necessary to search for each user whom you want to add by name. The names of the users registered to your IAM Identity Center will not appear automatically. Also, you must search by display name (usually the user's first and last name), and not by the one-word username used to sign in to the AWS account.

Note

When you add a group, as defined in IAM Identity Center, to a subscription, or add a user to a subscribed group, it may take up to 24 hours for that user, or users in that group, to be subscribed.

Assign users and groups



People

- Alice Jackson
- Bob Thompson
- Anna Ellington
- David Wilson
- Aaron Collins
- Chris Evans

Groups

Accounting

Group description

A-Team

Group description

Analytics

Group description

[Cancel](#)

[Assign](#)

- Open the Amazon Q Developer console.
- Manage your Amazon Q Developer settings.

On this page, you can select the features of Amazon Q Developer that will be available to your users.

[Amazon Q Developer](#) > Settings

Settings Info

[Delete profile](#)

Q Developer account details

[Edit](#)

Enabled Amazon Q Developer features

Q in the IDE

Amazon Q code transformation
Amazon Q task assistance
Amazon Q completions
Amazon Q feature dev
Amazon Q conversations
Amazon Q analysis

Q in the AWS Console

Amazon Q assistant
Amazon Q troubleshooting
Amazon Q actions

Amazon CodeCatalyst

Amazon Q feature dev
Pull request comment summary

Q ChatBots

AWS console mobile application
AWS chatbot in Slack and Teams

Include suggestions with code references

True

Encryption key

Default AWS managed key

Region

US East (N. Virginia)

Start URL

Give this URL to your users. This is required for them to access Amazon Q Developer in their IDEs. [Learn more](#)

<https://b-5632de3745.awsapps.com/start>

Member account settings

[Edit](#)

Q Developer managed application and settings profile

To share Q Developer Settings Profile set in the Management account with your Member accounts, ensure this is turned on.

On (default)

Tags Info

[Manage tags](#)

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

 Find tags

Key

Value

7. Copy the Start URL.

Pass the Start URL along to your developers, and direct them to [Using Amazon Q Developer in the IDE](#).

Enabling trusted access

Amazon Q Developer uses trusted access to share the settings made in the Organizations management account with member accounts in the same organization.

For example, the Amazon Q Developer Pro administrator, working in the Organizations management account, may enable suggestions with code references. If trusted access is enabled,

then suggestions with code references will also be enabled for all member accounts in that organization.

When you subscribe to Amazon Q Developer Pro with an AWS Organizations management account, you are given the option to share settings with member accounts. You may also share or un-share those settings after subscribing.

To enable or disable trusted access after subscribing, use the following procedure.

1. On the Amazon Q Developer **Settings** page, under **Member account settings**, choose **Edit**.
2. In the pop-up window, select **On** or **Off**.
3. Choose **Save**.

To learn more about trusted access, refer to [Enabling trusted access for AWS Account Management](#) in the *AWS Organizations User Guide*.

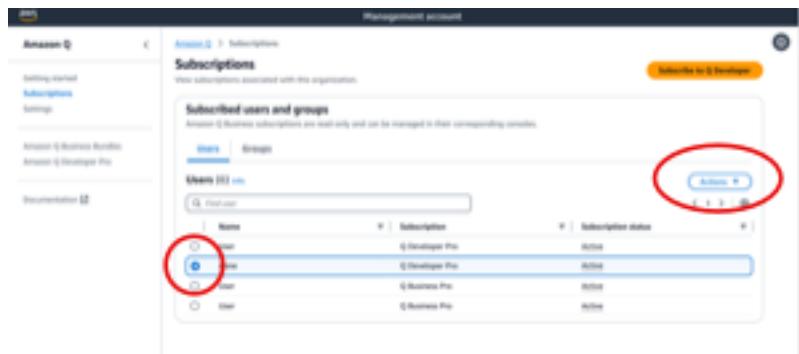
Unsubscribing

Unsubscribing from Amazon Q Developer Pro

Administrators can unsubscribe users from Amazon Q Developer Pro subscriptions through the subscriptions page in the console by de-selecting user names in the Amazon Q console.

To unsubscribe a user:

1. Go to the Subscriptions page of the Amazon Q Developer console.
2. Select the user.
3. Under Actions, choose **Unsubscribe**.
4. A pop-up window will ask you to confirm. Choose **Unsubscribe**.



However, the process varies based on the creator of the subscription:

- *Member account administrators* can only view and unsubscribe users subscribed within their account, and only if they created that specific subscription.
- *Organization management account administrators* can unsubscribe users if they created that subscription. They can also view other accounts the user is subscribed through (by selecting **Share settings profile with member accounts** on the **Settings** page), allowing them to coordinate with respective member account admins for unsubscription. Alternatively, they can log in as a member account administrator and unsubscribe the user directly.

For more information, refer to [Managing AWS accounts in your organization](#).

Unsubscribing from Amazon Q Business

To unsubscribe from Amazon Q Business, see Section 2.c., **Unsubscribe and remove**, under [Adding user access and subscriptions to an Amazon Q application](#) in the *Amazon Q Business User Guide*.

Unsubscribing from Amazon QuickSight Q

To unsubscribe from Amazon QuickSight, see [Unsubscribing from Amazon QuickSight Q](#) in the *Amazon QuickSight User Guide*.

Note

If a user is using both Amazon QuickSight and Amazon Q Business as part of Amazon Q Business Pro, then you must remove the user from both services in order to avoid further billing for that user.

Troubleshooting subscriptions

You may encounter the following error message when trying to access Amazon Q Developer in the AWS Management Console and on the AWS Documentation website:

An error occurred when attempting to access Amazon Q
Review the Amazon Q in console common errors documentation for potential solutions.

This could be due to one of the following reasons:

- **You were recently added to a group, and your subscription is not yet active.**

If your administrator manages Amazon Q subscription access using identity provider groups, there might be a delay when they add users to the group. You might need to wait up to 24 hours for access to be activated.

- **You don't have an active subscription.**

Try refreshing the page to use the Amazon Q Developer Free Tier.

- **Your access to the Amazon Q Developer Pro managed application was revoked.**

You still have an active subscription, but your access to the Amazon Q Developer Pro managed application was revoked or the managed application was deleted. Contact your administrator to restore your access.

- **You don't have sufficient IAM permissions.**

You or your AWS administrator must update your IAM permissions to allow the use of Amazon Q Developer. For more information, see [Identity-based policy examples for Amazon Q Developer](#).

After you obtain the necessary permissions, reload the console page to access Amazon Q.

Using Amazon Q Developer on AWS apps and websites

Use Amazon Q Developer in the AWS Management Console, AWS Console Mobile Application, AWS Marketing website, AWS Documentation website, and chat channels integrated with AWS Chatbot to ask questions about AWS. You can ask Amazon Q about AWS architecture, best practices, support, and documentation. Amazon Q can also help with code that you're writing with the AWS SDKs and AWS Command Line Interface (AWS CLI).

In the AWS Management Console, you can ask Amazon Q about your AWS resources and costs, contact AWS Support directly, and diagnose common console errors.

Topics

- [Chatting with Amazon Q Developer about AWS](#)
- [Diagnosing common errors in the console with Amazon Q Developer](#)
- [Using Amazon Q Developer to chat with AWS Support](#)
- [Chatting with Amazon Q Developer in AWS Chatbot](#)

Chatting with Amazon Q Developer about AWS

Chat with Amazon Q in the AWS Management Console, AWS Console Mobile Application, AWS website, AWS Documentation website, and chat channels integrated with AWS Chatbot to learn about AWS services. You can ask Amazon Q about best practices, recommendations, step-by-step instructions for AWS tasks, and architecting your AWS resources and workflows.

You can also ask Amazon Q about your AWS resources and account costs. Amazon Q also generates short scripts or code snippets to help you get started using the AWS SDKs and AWS CLI.

Topics

- [Working with Amazon Q on AWS websites](#)
- [Example questions](#)
- [Chatting about your resources](#)
- [Chatting about your costs](#)

Working with Amazon Q on AWS websites

To chat with Amazon Q Developer in the AWS Management Console, choose the Amazon Q icon in the right sidebar. To chat on the AWS website or any AWS service's documentation page, choose the Amazon Q icon in the bottom right corner.

To ask Amazon Q a question, enter your question into the text bar in the Amazon Q panel. Amazon Q generates a response to your question with a sources section that links to its references.

After you receive a response, you can optionally leave feedback by using the thumbs-up and thumbs-down icons. You can also copy the response to your clipboard by choosing the copy icon.

Conversation history

Amazon Q maintains context of your conversation within a given session as context to inform future responses. You can ask follow-up questions or refer to previous questions and responses throughout the duration of your session.

If you're using Amazon Q in the console, your current conversation and associated context are maintained when you navigate to another place in the console or to another browser or tab. If you're using Amazon Q on the AWS website, Documentation website, or Console Mobile Application, a new conversation starts without any context when you navigate to a new page, browser, or tab.

If you want to restart your conversation and clear the context provided by previous questions and responses, choose **New conversation**. Your previous conversation will no longer be used to inform responses from Amazon Q.

Chat settings

To update your chat settings in Amazon Q, choose the gear icon in the top right corner of the chat panel.

You can specify the following settings:

- **Region** — Amazon Q defaults to the AWS Region set in the AWS Management Console when you open the chat panel. To update the Region used by Amazon Q, change your console Region.
- **Cross-region calls** — To provide some features, such as listing your AWS resources in the chat, Amazon Q might need to make cross-region calls to retrieve information about your resources

in other Regions. Enable cross-region calls to grant Amazon Q permission to make calls to other Regions.

Example questions

You can ask Amazon Q questions about AWS and AWS services, such as finding the right service or understanding best practices.

You can also ask about software development with the AWS SDKs and AWS CLI. Amazon Q in the console can generate short scripts or code snippets to help you get started using the AWS SDKs and AWS CLI.

The following are example questions that demonstrate how Amazon Q can help you build on AWS:

- What's the maximum runtime for a Lambda function?
- When should I put my resources in a VPC?
- What's the best container service to use to run my workload if I need to keep my costs low?
- How do I list my Amazon S3 buckets?
- How do I create and host a website on AWS?

Chatting about your resources

In the AWS Management Console, you can ask Amazon Q about your AWS account resources. In the chat panel, ask Amazon Q to list a type of resource in your account, for details about a specific resource, or to list resources based on a criteria such as region or state.

Amazon Q can perform get, list, and describe actions to retrieve your AWS resources. For example, you can ask “List my S3 buckets” or “Show my running EC2 instances in us-east-1”. Amazon Q can't answer questions about the data stored in your resources, such as listing objects in an Amazon S3 bucket, or questions related to your account security, identity, credentials, or cryptography.

Amazon Q lists up to 6 resources in the chat panel, and the response includes details about each resource, a resource ARN that you can copy, and, if applicable, a link to the service console. When you ask about one resource, the response also includes the resource information in JSON format.

Topics

- [Prerequisites](#)

- [Ask Amazon Q about resources](#)

Prerequisites

For Amazon Q to show your resources, the following prerequisites must be met.

Add permissions

To chat about your resources, you need the following permissions:

- q:SendMessage to chat with Amazon Q
- q:StartConversation to chat with Amazon Q
- q:GetConversation to chat with Amazon Q
- q>ListConversations to chat with Amazon Q
- q:PassRequest to allow Amazon Q to call the APIs required to view your resources
- Permissions to perform the actions required to view your resources

Your IAM identity must have permissions to perform the actions required to access resources you ask about. For example, if you ask Amazon Q to list your Amazon S3 buckets, you must have the s3>ListAllMyBuckets permission. Amazon Q will never perform an action that you don't have permission to perform yourself.

For an example IAM policy that grants the necessary permissions, see [Allow Amazon Q to perform actions on your behalf](#). For more information about the q:PassRequest action, see [Using q:PassRequest](#).

Important

Normal fees apply when you ask Amazon Q to perform read, list, or describe actions. For more information, see the pricing page for the AWS service you are asking Amazon Q about.

Cross-Region consent

Amazon Q chat makes calls from US East (N. Virginia), so it might have to make cross-Region calls to access your resources in another Region, including to opt-in Regions. Amazon Q requires cross-

region consent to retrieve resources. To consent to cross-Region calls, complete the following steps:

1. Open the AWS Management Console and choose the Amazon Q icon.
2. If you haven't consented already, a notification about cross-region calls appears above the text bar. Choose **Continue** to consent to Amazon Q making cross-region calls to access your resources. If you choose **Don't allow**, you won't be able to ask Amazon Q about your AWS resources.
3. If you want to modify your cross-Region settings, choose the gear icon in the top right corner of the chat panel.

Ask Amazon Q about resources

You can ask Amazon Q to list your resources or get details about a specific resource or group of resources.

When you ask Amazon Q about your resources, you can specify the Region that Amazon Q calls to locate your resources. If no Region is specified, Amazon Q uses your current console Region, or the most recent console Region if you are using a global console Region. If no Region is found, it defaults to calling US East (N. Virginia).

Amazon Q might need additional information to retrieve your resources, such as the name of a resource or a resource ARN. When Amazon Q asks a follow up, reply with the requested details.

Following are example questions you can ask Amazon Q about your resources:

- Describe the encryption settings for S3 bucket <name>
- List my EC2 instances in us-west-2
- Get the configuration for my lambda function <name>

Chatting about your costs

Amazon Q's cost analysis capability is in preview and can make mistakes. Please verify your cost data with AWS Cost Explorer. Use the thumb icon in Amazon Q to provide feedback and help us improve.

You can ask Amazon Q about your AWS bill and account costs in the AWS Management Console. Amazon Q can retrieve your cost data, explain costs, and analyze cost trends, so you can understand your costs without referring to documentation or interrupting your workflow.

When you ask Amazon Q about your costs, its response includes information about the requested cost figure, including the metric, time period and granularity, and any groups or filters applied to retrieve the cost data. It also provides a link to an AWS Cost Explorer view with the same specifications, so you can see visualizations or download the data for your own analysis.

Prerequisites

Permissions

To chat about your costs, you need the following permissions:

- q:SendMessage to chat with Amazon Q
- q:StartConversation to chat with Amazon Q
- q:GetConversation to chat with Amazon Q
- q>ListConversations to chat with Amazon Q
- q:PassRequest to allow Amazon Q to call the APIs required to view your resources
- ce:GetCostAndUsage to get Cost Explorer data

For more information about the q:PassRequest action, see [Using q:PassRequest](#).

Enable AWS Cost Explorer

To chat about your costs with Amazon Q, you must enable AWS Cost Explorer in your AWS account.

To enable Cost Explorer, open the Cost Explorer console. For more information, see [Enabling Cost Explorer in the AWS Cost Management User Guide](#).

Example questions

Following are example questions about costs that you can ask Amazon Q:

- How much did we spend on SageMaker in January?
- What are the top contributing services to my AWS bill in the 'eu-central-1' region?
- What were my Amazon EC2 costs by instance type last week?

- What was my cost breakdown by service for the past three months?
- Which linked accounts increased their spend the most from January to February?
- Which linked accounts spent the most on DynamoDB last month?
- What were my cost trends by region over the last three months?

Diagnosing common errors in the console with Amazon Q Developer

In the AWS Management Console, Amazon Q Developer can diagnose common errors you receive while working with AWS services, such as insufficient permissions, incorrect configuration, and exceeding service limits. This feature is available for errors that arise while using the following services in the AWS Management Console:

- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon Simple Storage Service (Amazon S3)
- AWS Lambda

You can diagnose most common console errors with Amazon Q, except for simple validation errors. Amazon Q doesn't maintain a history of previous error diagnosing sessions.

If you're unable to diagnose your error with Amazon Q, you can use Amazon Q to create a support case with AWS Support. For more information, see [Using Amazon Q Developer to chat with AWS Support](#). If you have an issue specific to the Amazon Q error diagnosing feature, you can use the thumbs-down icon to report an issue.

Note

Diagnosing console errors with Amazon Q is currently available in the US West (Oregon) and US East (N. Virginia) AWS Regions.

You might need additional permissions to access this feature. For more information, see [Allow users to diagnose console errors with Amazon Q](#).

Diagnose common errors in the console

To use Amazon Q to diagnose an error in the AWS Management Console, use the following procedure.

1. If you receive an error that Amazon Q can help you with, a **Diagnose with Amazon Q** button appears in the error message. If you want to use Amazon Q to diagnose the error, choose **Diagnose with Amazon Q** to proceed.
2. A window appears where Amazon Q provides information about the error and an overview of how to resolve it. To see detailed steps for how to resolve the error, choose **Help me resolve**.
3. It can take several seconds for Amazon Q to generate instructions. After they appear, follow the instructions to resolve the error.
4. To provide feedback, you can use the thumbs-up and thumbs-down icons. To provide detailed feedback, choose the **Tell me more** button that appears after you select an icon.

Using Amazon Q Developer to chat with AWS Support

You can use Amazon Q Developer to create a support case and contact AWS Support from anywhere in the AWS Management Console, including the AWS Support Center Console. Amazon Q uses the context of your conversation to draft a support case on your behalf automatically. It also adds your recent conversation to the support case description. After creating the case, Amazon Q can transfer you to a support agent in the method of your choice, including live chat in the same interface.

When you create a support case in Amazon Q, the case is also updated in the Support Center Console. To track updates on cases created with Amazon Q, use the Support Center Console.

The type of AWS Support available to you depends on the support plan for your AWS account. All AWS users have access to account and billing support as part of the Basic Support plan. For technical support questions, only users with support plans other than the Basic Support plan can contact AWS Support with Amazon Q. For more information about AWS Support, see [Getting started with AWS Support](#) in the *AWS Support User Guide*.

Prerequisites

To create cases in Amazon Q, you must meet the following requirements:

- You have permissions to start conversations with Amazon Q. For more information, see [Allow users to chat with Amazon Q](#).
- You have permissions to create AWS Support cases. For more information, see [Manage access to AWS Support Center](#).

Specify the right service

When you create a support case with Amazon Q, it populates the service field based on your question. If Amazon Q chooses the wrong service, update the case with the correct service. If your question has to do with multiple services, specify the service that's most applicable.

To contact AWS Support about an Amazon Q feature that is part of another AWS service, create a support case for the other AWS service, not for Amazon Q. For example, if you're using Amazon Q network troubleshooting in Amazon VPC Reachability Analyzer, choose Amazon VPC for the service in the support case.

To contact AWS Support about features in either Amazon Q Developer or Amazon Q Business, create a support case for Amazon Q.

Create a support case

To create an AWS Support case with Amazon Q, use the following steps.

1. You can create an AWS Support case through Amazon Q in one of two ways:
 - a. Ask for help directly by entering a question such as "I want to speak to someone" or "Get support".

To provide more context for Amazon Q to create the support case, you can add more information when requesting support directly. Following is an example of providing more information in a request:

"I am unable to connect to my bastion instance. I have tried restarting it and generating new key pairs but still nothing works. This started this morning after a planned deployment. I can confirm that no other network related changes were made. Can I talk to someone?"
 - b. If an Amazon Q response didn't help you, choose the thumbs-down icon on the response and then choose a reason that you're providing the feedback. To contact AWS Support, choose **Create a support case**.

The following image shows the **Create a support case** button in the Amazon Q chat panel that appears after you leave feedback.

[3] Troubleshoot instances with failed status checks - Amazon Elastic Compute Cloud



Thank you for your feedback. If you need further assistance related to this issue, you may contact support.

Create a support case

2. A support case appears in the chat panel. If you had a conversation with Amazon Q before requesting support, it will use the context of your conversation to autopopulate the fields in the case. To update any field in the support case, choose **Edit**. You can also attach files that help explain your issue.

If you didn't chat with Amazon Q before requesting support or Amazon Q otherwise can't complete the fields in the support case, you can input your support case information into the case manually.

The following image is an example of a filled-out support case in the Amazon Q chat panel.

Sure, I've drafted the following support case for you. Review details and make required changes before continuing. I will also add our recent conversation to the case description once submitted.

Support Level	Enterprise Support	Change 
Description	The customer is unable to connect to their instance after a recent deployment. They have tried restarting the instance and generating new key pairs but are still unable to connect. No other changes were made to the network configuration. The issue is problematic and the customer would like to chat with support.	
Case type	Technical	
Service	Elastic Compute Cloud (EC2 - Linux)	
Category	Instance Issue	
Severity	General guidance	
Additional Contacts	None	
Attachments	<a data-bbox="497 1024 677 1066" href="#"> Attach Files You can attach up to 3 files. Each file can be up to 5 MB.	
<a data-bbox="236 1151 318 1182" href="#">Cancel <a data-bbox="856 1151 922 1182" href="#">Edit <a data-bbox="1003 1151 1101 1182" href="#">Submit		

3. After confirming that the support case describes your needs, choose **Submit** to create the support case. If you no longer want to create the case, choose **Cancel**.
4. To contact AWS Support, choose the method that you want to use. Depending on your case details, you can chat, email, or request a phone call from a live support agent:
 - a. **Chat** – If you choose to chat with an agent, a live support agent will enter the conversation. To end the chat with the support agent, choose **End this chat** at any time during the chat.

If you refresh your page, navigate to a different console, or get signed out of the console because of session expiration, the conversation will end.

- If you minimize the chat panel or leave the page, you might miss notifications and be disconnected because of inactivity. We recommend that you keep the chat panel open throughout the duration of your support chat.
- b. **Email** – If you choose to send an email message to an agent, a support agent will contact you at the email address that's associated with your AWS account.
 - c. **Call** – If you choose to call an agent, enter your phone number when prompted, and choose **Submit**. You will be added to the call queue.
5. You can leave feedback or choose **Skip** to return to the Amazon Q chat panel.

Leave feedback

After the support chat has ended, you can optionally leave feedback.

Rate your experience, enter any additional feedback, and then choose **Submit feedback**.

Chatting with Amazon Q Developer in AWS Chatbot

You can chat with Amazon Q Developer in Microsoft Teams and Slack messaging platforms that are configured with AWS Chatbot. Amazon Q in AWS Chatbot can answer questions about best practices for building solutions, troubleshooting issues, and identifying next steps.

To add Amazon Q to a Microsoft Teams or Slack channel that is already configured with AWS Chatbot, complete the following steps. To set up AWS Chatbot in your channels for the first time and allow users to use Amazon Q, see [Get started with Microsoft Teams](#) and [Get started with Slack](#) in the *AWS Chatbot Administrator Guide*.

Add Amazon Q to a chat channel

You can add Amazon Q to a Microsoft Teams or Slack channel that is already configured with AWS Chatbot. First, update your AWS Identity and Access Management (IAM) role settings to include the [AmazonQFullAccess](#) managed policy, and then add the policy as a channel guardrail.

1. Add the `AmazonQFullAccess` managed policy to your IAM role:
 - a. Sign in to the AWS Management Console and open the [IAM console](#).
 - b. In the navigation pane of the IAM console, choose **Roles**.
 - c. Choose the name of the role that you want to modify.

- d. In **Permissions policies**, choose **Add permissions** and **Attach policies**.
 - e. Enter **AmazonQFullAccess** in the search.
 - f. Select **AmazonQFullAccess**.
 - g. Choose **Add permissions**.
2. Add the AmazonQFullAccess managed policy to your channel guardrails:
 - a. Open the [AWS Chatbot console](#).
 - b. Choose a configured client.
 - c. Select a configured channel.
 - d. Choose **Set guardrails**.
 - e. Enter **AmazonQFullAccess** in the search.
 - f. Select **AmazonQFullAccess**.
 - g. Choose **Save**.

Ask Amazon Q questions in your channel

To check that your configuration was successful, ask Amazon Q a question. Enter @aws followed by your question. For example, you can enter @aws what is fargate?

Following are some examples of questions that you can ask Amazon Q from your configured channel:

- @aws how do I troubleshoot lambda concurrency issues?
- @aws what are the best practices for securing S3 buckets?
- @aws what is the maximum zipped file size for a lambda?

Using Amazon Q Developer in the IDE

Use Amazon Q Developer in integrated development environments (IDEs) to learn about AWS and get assistance with your software development needs. In IDEs, Amazon Q includes capabilities to provide guidance and support across various aspects of software development, such as answering questions about building on AWS, generating and updating code, security scanning, and optimizing and refactoring code.

To install Amazon Q in your IDE, see [Installing the Amazon Q Developer extension or plugin in your IDE](#).

Topics

- [Supported IDEs and available features](#)
- [Installing the Amazon Q Developer extension or plugin in your IDE](#)
- [Chatting with Amazon Q Developer about code](#)
- [Generating inline suggestions with Amazon Q Developer](#)
- [Upgrading language versions with the Amazon Q Developer Agent for code transformation](#)
- [Developing software with the Amazon Q Developer Agent for software development](#)
- [Scanning your code with Amazon Q](#)
- [Supported languages for Amazon Q Developer in the IDE](#)

Supported IDEs and available features

The features you have access to depend on the IDE where you use Amazon Q. The following table describes the IDEs supported by Amazon Q and the availability and limitations of features in each IDE.

If no language support is specified, the IDE supports languages listed in the [Supported languages](#) topic.

IDE	Supported features
JetBrains IDEs	Chat Workspace context in chat

IDE	Supported features
	Inline suggestions Agent for code transformation Agent for software development Security scanning Customizations
Visual Studio Code	Chat Workspace context in chat Inline suggestions Agent for code transformation Agent for software development Security scanning Customizations
Visual Studio	Chat Inline suggestions – C, C++, and C# Security scanning – C#
AWS coding environments	Inline suggestions

Installing the Amazon Q Developer extension or plugin in your IDE

To set up Amazon Q Developer in your integrated development environment (IDE), complete the following steps. After installing the Amazon Q extension or plugin, authenticate through IAM

Identity Center or AWS Builder ID. You can use Amazon Q for free, without an AWS account, by authenticating with Builder ID.

To get started, download the Amazon Q extension or plugin for your IDE:

- [Download Amazon Q in Visual Studio Code](#)
- [Download Amazon Q in JetBrains IDEs](#)
- [Download Amazon Q in the AWS Toolkit for Visual Studio](#)

 **Note**

In general, the default duration for a session that is authenticated through IAM Identity Center is 8 hours. However, in the case of Amazon Q, the default session lasts 90 days (if you set up IAM Identity Center on April 18, 2024 or later). For more information refer to [How to extend the session duration for Amazon Q in the IDE](#) in the *IAM Identity Center User Guide*.

To sign in and authenticate, complete the steps in this section.

Steps

- [Prerequisite: Choose a supported version of your IDE](#)
- [Authenticating in JetBrains IDEs](#)
- [Authenticating in Visual Studio Code](#)
- [Authenticating in Visual Studio](#)
- [Using an IAM principal in your AWS console](#)
- [Understanding AWS coding environments](#)

Prerequisite: Choose a supported version of your IDE

Amazon Q is available as an extension in Visual Studio Code and a plugin in JetBrains. Amazon Q is also available in the AWS Toolkit for Visual Studio.

- The minimum version of Visual Studio Code supported by Amazon Q is 1.85.0.
- The minimum version of JetBrains IDEs (including IntelliJ and PyCharm) supported by Amazon Q is 232.1. JetBrains versions 232, 233 and 241 are also supported.

- Only Visual Studio for Windows is supported by Amazon Q. The minimum version of Visual Studio supported is Visual Studio 2022 version 17.7. All Visual Studio 2022 editions are supported.

Authenticating in JetBrains IDEs

You can authenticate for free with AWS Builder ID or with IAM Identity Center with a Amazon Q Developer Pro subscription. Choose your authentication method to see steps to start using Amazon Q in your JetBrains IDE.

Builder ID

This procedure does not require you to have Builder ID. If you have not yet signed up for Builder ID, you will have the opportunity to do so during the sign-in process.

1. Install the [Amazon Q IDE plugin](#) in your JetBrains IDE.
2. Choose the Amazon Q icon in your IDE.

The icon will be on the side of the interface by default.

3. Follow the instructions in your browser to authenticate with Builder ID.
4. To begin using Amazon Q, choose the Amazon Q icon to chat with Amazon Q, or choose **Amazon Q** from the navigation bar at the bottom of your IDE.

Amazon Q Developer Pro license

Before you begin this procedure, your administrator should have:

- Created an identity for you in IAM Identity Center
- Subscribed that identity to Amazon Q Developer Pro

After your identity has been subscribed to Amazon Q Developer Pro, complete the following steps to authenticate:

1. Install the [Amazon Q IDE plugin](#) in your JetBrains IDE.
2. Choose the Amazon Q icon in your IDE.

The icon will be on the side of the interface by default.

3. Choose **Use with Pro license**.
4. Fill in the **Start URL** that your administrator got from [the Amazon Q subscription console](#).
5. Fill in the AWS Region in which your administrator set up your IAM Identity Center [account instance](#).
6. Choose **Continue**. The focus will switch to your web browser.
7. Follow the instructions in your browser to authenticate with IAM Identity Center.
8. To begin using Amazon Q, choose the Amazon Q icon to chat with Amazon Q, or choose **Amazon Q** from the navigation bar at the bottom of your IDE.

Authenticating in Visual Studio Code

You can authenticate for free with AWS Builder ID or with IAM Identity Center with a Amazon Q Developer Pro subscription. Choose your authentication method to see steps to start using Amazon Q in VS Code.

Builder ID

This procedure does not require you to have Builder ID. If you have not yet signed up for Builder ID, you will have the opportunity to do so during the sign-in process.

1. Install the [Amazon Q IDE extension](#) in VS Code.
2. Choose the Amazon Q icon in your IDE.

The icon will be on the side of the interface by default.

3. Follow the instructions in your browser to authenticate with Builder ID.
4. To begin using Amazon Q, choose the Amazon Q icon to chat with Amazon Q, or choose **Amazon Q** from the navigation bar at the bottom of your IDE.

Amazon Q Developer Pro license

Before you begin this procedure, your administrator should have:

- Created an identity for you in IAM Identity Center
- Subscribed that identity to Amazon Q Developer Pro

After your identity has been subscribed to Amazon Q Developer Pro, complete the following steps to authenticate:

1. Install the [Amazon Q IDE extension](#) in VS Code.
2. Choose the Amazon Q icon in your IDE.

The icon will be on the side of the interface by default.

3. Choose **Use with Pro license**.
4. Fill in the **Start URL** that your administrator got from [the Amazon Q subscription console](#).
5. Fill in the AWS Region in which your administrator set up your IAM Identity Center [account instance](#).
6. Choose **Continue**. The focus will switch to your web browser.
7. Follow the instructions in your browser to authenticate with IAM Identity Center.
8. To begin using Amazon Q, choose the Amazon Q icon to chat with Amazon Q, or choose **Amazon Q** from the navigation bar at the bottom of your IDE.

Authenticating in Visual Studio

To connect to your AWS accounts from the Toolkit for Visual Studio, open the **Getting Started with the AWS Toolkit** User Interface (connection UI) by completing the following procedure.

1. From the Visual Studio main menu, expand **Extensions** then expand the **AWS Toolkit**.
2. From the **AWS Toolkit** menu options choose **Getting Started**.
3. The **Getting Started with the AWS Toolkit** connection UI opens in Visual Studio.

You can authenticate for free with AWS Builder ID or with IAM Identity Center with a Amazon Q Developer Pro subscription. Choose your authentication method to see steps to start using Amazon Q in Visual Studio.

Builder ID

1. From the **Getting Started with the AWS Toolkit** connection UI, select the **Amazon Q Developer** radial to expand the Amazon Q Developer authentication options.
2. From the **I'm using Amazon Q Developer on my own** section, choose the **Sign up or Sign in** button to open the **Log in with AWS Builder ID** dialog.

3. Choose the **Proceed to Browser** button to open the AWS **Authorize request** site in your default web browser.
4. Follow the prompts in your default web browser. You're notified when the authorization process is complete, and it's safe to close your browser and return to Visual Studio.

Amazon Q Developer Pro license

1. From the **Getting Started with the AWS Toolkit** connection UI, select the **Amazon Q Developer** radial to expand the Amazon Q Developer authentication options.

 **Note**

If no stored credentials exist, proceed to **Step 3** to add or update your IAM Identity Center credentials.

2. From the **My organization has enabled Amazon Q Developer** section, expand the **Choose from an existing Profile or add new** drop-down menu to choose from your list of stored credentials.
3. From the **Profile Type** drop-down menu, choose **AWS IAM Identity Center**.
4. In the **Profile Name** text field, enter the **Profile Name** of the IAM Identity Center profile you want to authenticate with.
5. In the **Start URL** text field, enter the **Start URL** that's attached to your IAM Identity Center credentials.
6. From the **Profile Region (defaults to us-east-1)** drop-down menu, choose the **Profile Region** that's defined by the IAM Identity Center user profile you're authenticating with.
7. From the **SSO Region (defaults to us-east-1)** drop-down menu, choose the **SSO Region** that's defined by your IAM Identity Center credentials, then choose the **Connect** button to open the **Log in with AWS IAM Identity Center** dialog.
8. From the **Log in with AWS IAM Identity Center** dialog, choose the **Proceed to Browser** button to open the AWS **Authorize request** site in your default web browser.
9. Follow the prompts in your default web browser. You're notified when the authorization process is complete, and it's safe to close your browser and return to Visual Studio.

For more information about authenticating in the Toolkit for Visual Studio, see [Getting Started](#) in the *AWS Toolkit for Visual Studio User Guide*.

Using an IAM principal in your AWS console

Depending on how you use AWS, you may be accustomed to using your IAM credentials to sign in to the console for all AWS services. However, you cannot use Amazon Q Developer in the IDE as an IAM principal, or with an IAM role. You must authenticate with credentials from either IAM Identity Center or Builder ID.

Understanding AWS coding environments

If you're developing software, then the way to get the most out of Amazon Q Developer is to subscribe to Amazon Q Developer Pro, and to use Amazon Q through the Amazon Q extension in Visual Studio or Visual Studio Code, or the plugin in a JetBrains IDE. Most of the features described in this chapter pertain to that setup.

However, there are many other aspects of your AWS experience in which you might end up writing code. For example, you might write code directly in the AWS Lambda interface. In some such cases, inline code suggestions from Amazon Q can be available to you.

Environments in which you may enable code suggestions include:

- Amazon SageMaker Studio Classic
- JupyterLab
- Amazon EMR Studio
- AWS Glue Studio
- AWS Lambda
- AWS Cloud9

To enable code suggestions in coding environments within the AWS console, your administrator must assign you [the appropriate permissions](#).

Chatting with Amazon Q Developer about code

Chat with Amazon Q Developer in your integrated development environment (IDE) to ask questions about building at AWS and for assistance with software development. Amazon Q can explain coding concepts and code snippets, generate code and unit tests, and improve code, including debugging or refactoring.

Topics

- [Working with Amazon Q in your IDE](#)
- [Example topics and questions](#)
- [Reporting issues with responses from Amazon Q](#)
- [Explaining and updating code with Amazon Q Developer](#)
- [Adding workspace context to Amazon Q Developer chat in the IDE](#)

Working with Amazon Q in your IDE

You can ask Amazon Q questions, update your code, and initiate actions with quick commands all from the Amazon Q chat panel in your IDE.

To start chatting with Amazon Q in JetBrains and Visual Studio Code, choose the Amazon Q icon from the navigation bar in your IDE and enter your question in the text bar. To start chatting with Amazon Q in Visual Studio, choose **View** from the main menu and then choose **Amazon Q chat**.

When you ask Amazon Q a question, it uses the current file that is open in your IDE as context, including the programming language and the file path.

If Amazon Q includes code in its response, you can copy the code or insert it directly into your file by choosing **Insert at cursor**. Amazon Q might include inline references to its sources in its response. To view a list of sources, expand the **Sources** section at the bottom of a response.

Amazon Q maintains the context of your conversation within a given session inform future responses. You can ask follow up questions or refer to previous questions and responses throughout the duration of your session. To start a new conversation with Amazon Q, open a new tab in the panel. You can open up to 10 tabs at a time. Amazon Q doesn't retain context across different conversations.

Chat commands

You can enter the following commands in the chat panel to access Amazon Q features, depending on your IDE. For information about what Amazon Q features are available in your IDE, see [Supported IDEs](#).

- **/transform** - Use this command to update the code language version of an entire project. For more information, see [Transforming your code](#).

- **/dev** - Use this command to get an implementation plan to develop a feature with Amazon Q. For more information, see [Developing software](#).
- **/clear** - Use this command to clear a current conversation. This removes all previous conversation from the chat panel and clears the context that Amazon Q has about your previous conversation.
- **/help** - Use this command to see an overview of what Amazon Q can and can't do, example questions, and quick commands.

Example topics and questions

Within IDEs, Amazon Q can answer questions about AWS services and software development, in addition to generating code. Amazon Q is particularly useful for answering questions related to the following subject areas:

- Building on AWS, including AWS service selection, limits, and best practices
- General software development concepts, including programming language syntax and application development
- Writing code, including explaining code, debugging code, and writing unit tests

Following are some example questions that you can ask to get the most out of Amazon Q in your IDE:

- How do I debug issues with my Lambda functions locally before deploying to AWS?
- How do I choose between AWS Lambda and Amazon EC2 for a scalable web application backend?
- What is the syntax of declaring a variable in TypeScript?
- How do I write an app in React?
- Provide me a description of what this [*selected code or application*] does and how it works.
- Generate test cases for [*selected code or function*].

Reporting issues with responses from Amazon Q

You can optionally leave feedback for every response Amazon Q generates by using the thumbs-up and thumbs-down icons. To report an issue with a response, choose the thumbs-down icon, and enter information in the feedback window that appears.

Explaining and updating code with Amazon Q Developer

Amazon Q Developer can explain and update specific lines of code in your integrated development environment (IDE). To update your code, ask Amazon Q to make changes to a given line or block of code, and it will generate new code that reflects the changes that you asked it to make. Then, you can insert the updated code directly into the file where the code originated.

You can choose from the following options:

- **Explain** – Get your code explained in natural language.
- **Refactor** – Improve code readability or efficiency, among other improvements.
- **Fix** – Debug code.
- **Optimize** – Enhance code performance.
- **Send to prompt** – Send the highlighted code to the Amazon Q chat panel, and ask questions that you have about the code.

Send code to Amazon Q

To get your code explained or updated by Amazon Q, complete the following steps.

1. Highlight a section of a code file in your IDE.
2. Right-click your highlighted code to open a context window. Choose **Amazon Q**, and then choose **Explain**, **Refactor**, **Fix**, **Optimize**, or **Send to prompt**.

If you choose **Send to prompt**, Amazon Q copies the highlighted code to the chat panel, where you can enter questions that you have about the code.

3. To replace the highlighted code with the newly generated code, you can copy the code or insert it directly into your file by choosing **Insert code**. Amazon Q replaces the original code with the updated code.

Adding workspace context to Amazon Q Developer chat in the IDE

When you chat with Amazon Q in the integrated development environment (IDE), you can add **@workspace** to your question to automatically include the most relevant chunks of your workspace code as context. Amazon Q Developer determines relevance based on an index that is updated periodically.

With workspace context, Amazon Q has enhanced capabilities, including locating files, understanding how code is used across files, and generating code that leverages multiple files, including files that aren't opened.

Topics

- [Setup](#)
- [Ask questions with workspace context](#)

Setup

Before you continue, make sure you have the latest version of your IDE installed. You can then complete the following setup steps.

Enable indexing

To use your workspace as context, Amazon Q creates a local index of your workspace repository, including code files, configuration files, and project structure. During indexing, non-essential files like binaries or those specified in `.gitignore` files are filtered out.

It can take 5 to 20 minutes to index a new workspace. During this time, you can expect elevated CPU usage in your IDE. After initial indexing, the index is incrementally updated when you make changes to your workspace.

The first time you add workspace context, you must enable indexing in your IDE. Complete the following steps to enable indexing:

1. Add **@workspace** to your question in the Amazon Q chat panel.
2. Amazon Q prompts you to enable indexing. Choose **Settings** to be redirected to Amazon Q settings in your IDE. You can also choose **Open Settings** from the Amazon Q task bar.
3. Select the box under **Amazon Q: Local Workspace Index**.

Configure indexing (optional)

No configuration is necessary for the indexing process, however you can choose to specify the number of threads dedicated to indexing. If you increase the number of threads used, indexing will complete faster, and it will use more of your CPU. To update the indexing configuration, specify the number of threads in Amazon Q settings under **Amazon Q: Local Workspace Index Threads**.

Ask questions with workspace context

To add your workspace as context to your conversation with Amazon Q, open the workspace you want to ask questions about, and then add `@workspace` to your question in the chat panel.

If you want to start chatting about a different workspace, open the workspace, and then open a new chat tab. Include `@workspace` in your question to add the new workspace as context.

You can ask Amazon Q about any file in your workspace, including unopened files. Amazon Q can explain files, locate code, and generate code across files, in addition to existing conversational coding capabilities.

Following are example questions you can ask Amazon Q that leverage workspace context in the chat:

- `@workspace where is the code that handles authorization?`
- `@workspace what are the key classes with application logic in this project?`
- `@workspace explain main.py`
- `@workspace add auth to this project`
- `@workspace what third-party libraries or packages are used in this project, and for what purpose?`
- `@workspace add unit tests for function <function name>`

Generating inline suggestions with Amazon Q Developer

Amazon Q can provide you with code recommendations in real time. As you write code, Amazon Q automatically generates suggestions based on your existing code and comments. Your personalized recommendations can vary in size and scope, ranging from a single line comment to fully formed functions.

When you start typing out single lines of code or comments, Amazon Q makes suggestions based on your current and previous inputs.

Inline suggestions are automatically enabled when you download the Amazon Q extension. To get started, start writing code, and Amazon Q will begin generating code suggestions.

You can also customize the suggestions Amazon Q generates to your software development team's internal libraries, proprietary algorithmic techniques, and enterprise code style. For more information on customizing suggestions, see [Customizing suggestions](#).

Topics

- [Pausing suggestions with Amazon Q](#)
- [Amazon Q code completion in action](#)
- [Generating inline suggestions in AWS coding environments](#)
- [Using shortcut keys](#)
- [Using code references](#)
- [Code examples](#)

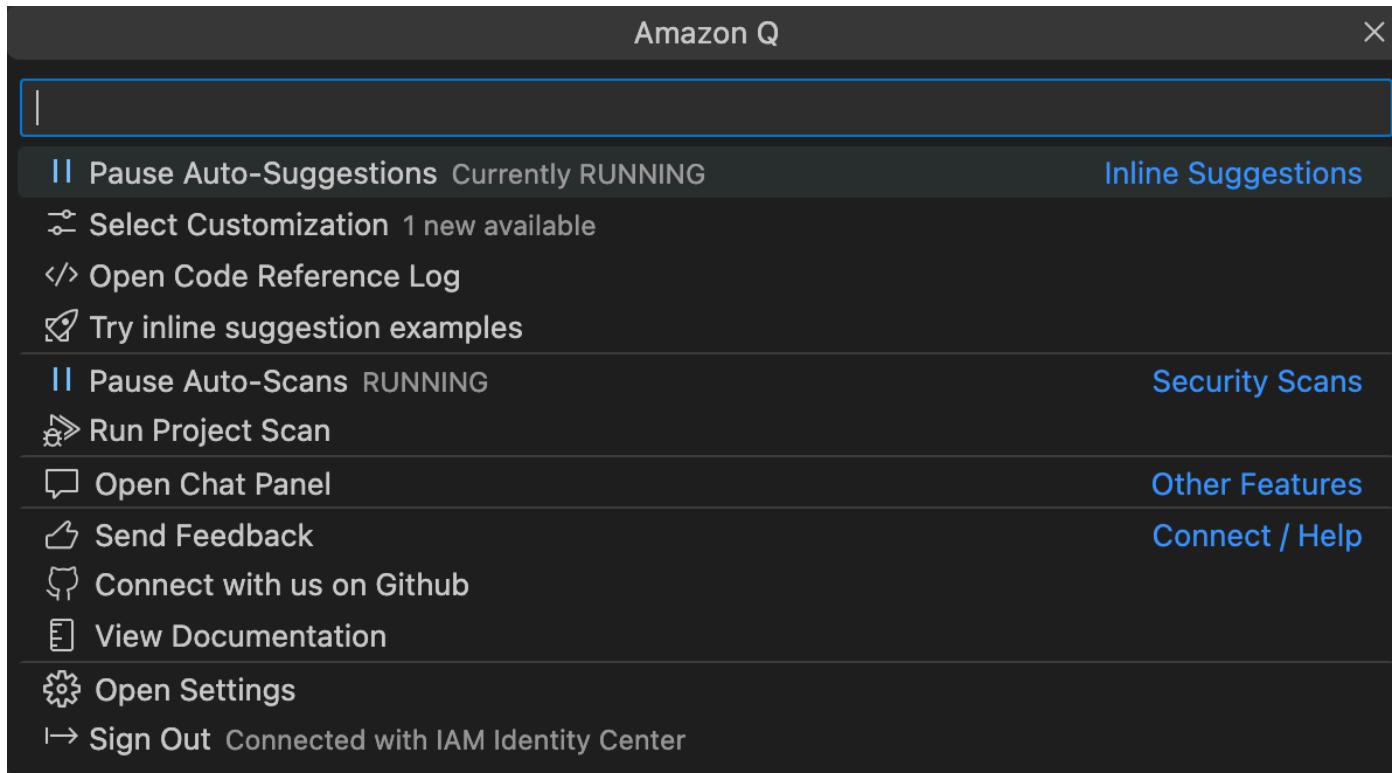
Pausing suggestions with Amazon Q

Choose your IDE to see steps for pausing and resuming inline code suggestions in Amazon Q.

Visual Studio Code

1. In VS Code, choose **Amazon Q** from the component tray at the bottom of the IDE window.
The Amazon Q task bar opens at the top of the IDE window.
2. Choose **Pause Auto-Suggestions** or **Resume Auto-Suggestions**.

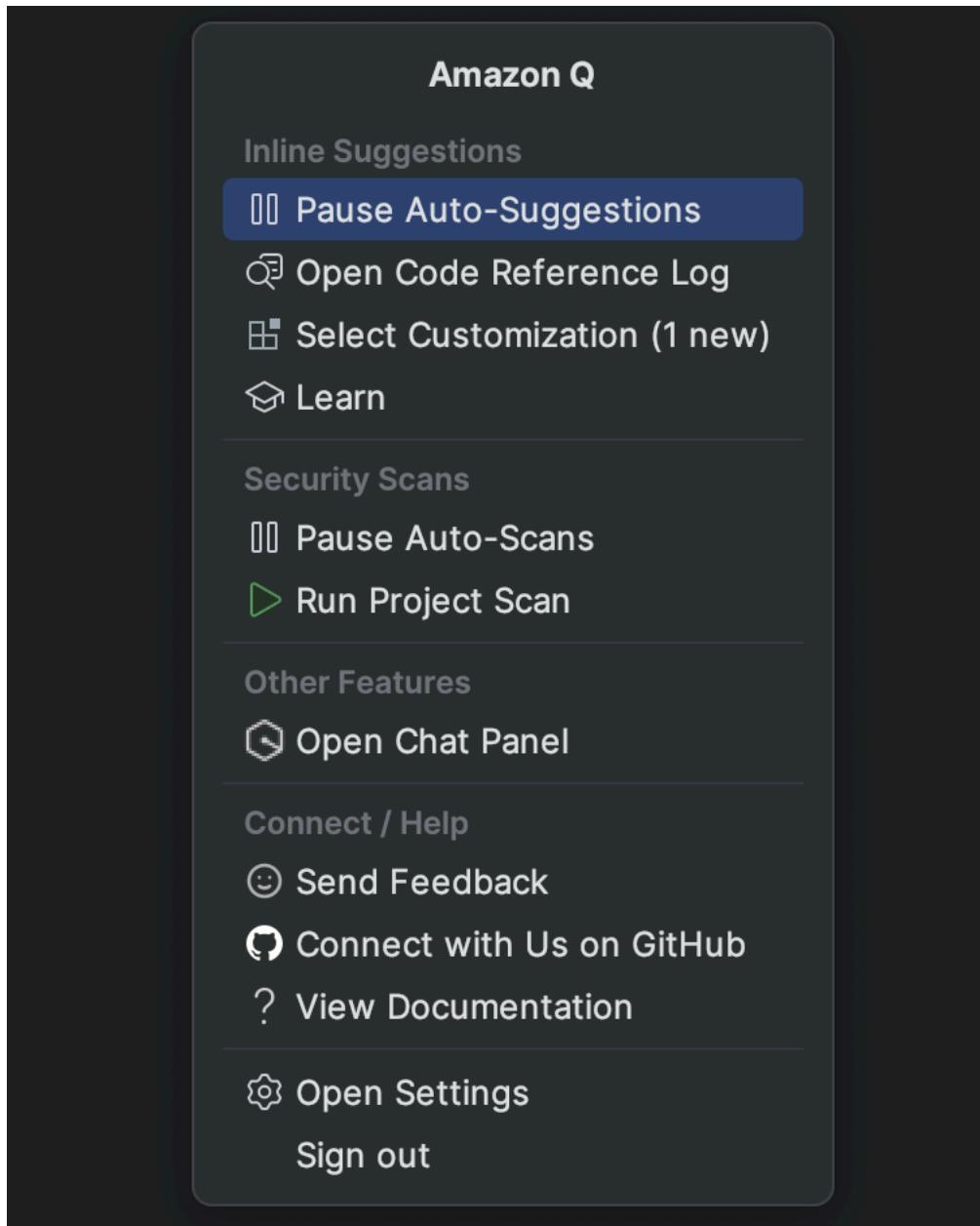
The following image shows the Amazon Q task bar in VS Code.



JetBrains

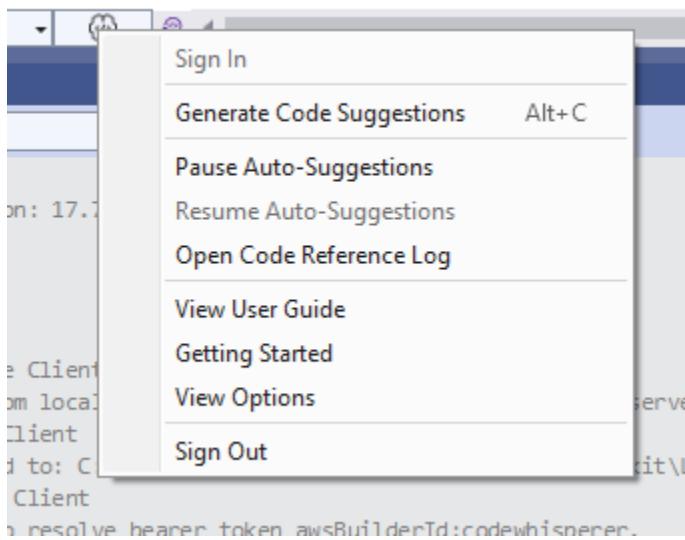
1. In JetBrains, choose **Amazon Q** from the status bar at the bottom of the IDE window.
The Amazon Q task bar opens above the status bar.
2. Choose **Pause Auto-Suggestions** or **Resume Auto-Suggestions**.

The following image shows the Amazon Q task bar in JetBrains.



Visual Studio

1. From the edge of the window, choose the Amazon Q icon.
2. Select **Pause Auto-Suggestions** or **Resume Auto-Suggestions**



AWS Cloud9

Amazon Q does not support toggling suggestions on and off in AWS Cloud9.

To stop receiving Amazon Q suggestions in AWS Cloud9, remove the IAM policy that gives Amazon Q access to AWS Cloud9 from the role or user that you are using to access AWS Cloud9.

Lambda

To deactivate or re-activate Amazon Q code suggestions in Lambda:

1. In the Lambda console, open the screen for a particular Lambda function.
2. In the **Code source** section, from the toolbar, choose **Tools**.
3. From the dropdown menu, choose **Amazon Q Code Suggestions**.

Amazon SageMaker Studio

1. In the SageMaker Studio console, choose Amazon Q from the bottom of the window.

The Amazon Q panel will open.

2. Choose **Pause Auto-Suggestions** or **Resume Auto-Suggestions**.

JupyterLab

1. In the JupyterLab console, choose Amazon Q from the bottom of the window.

The Amazon Q panel will open.

2. Choose **Pause Auto-Suggestions** or **Resume Auto-Suggestions**.

AWS Glue Studio Notebook

1. In the AWS Glue Studio Notebook console, choose Amazon Q from the bottom of the window.

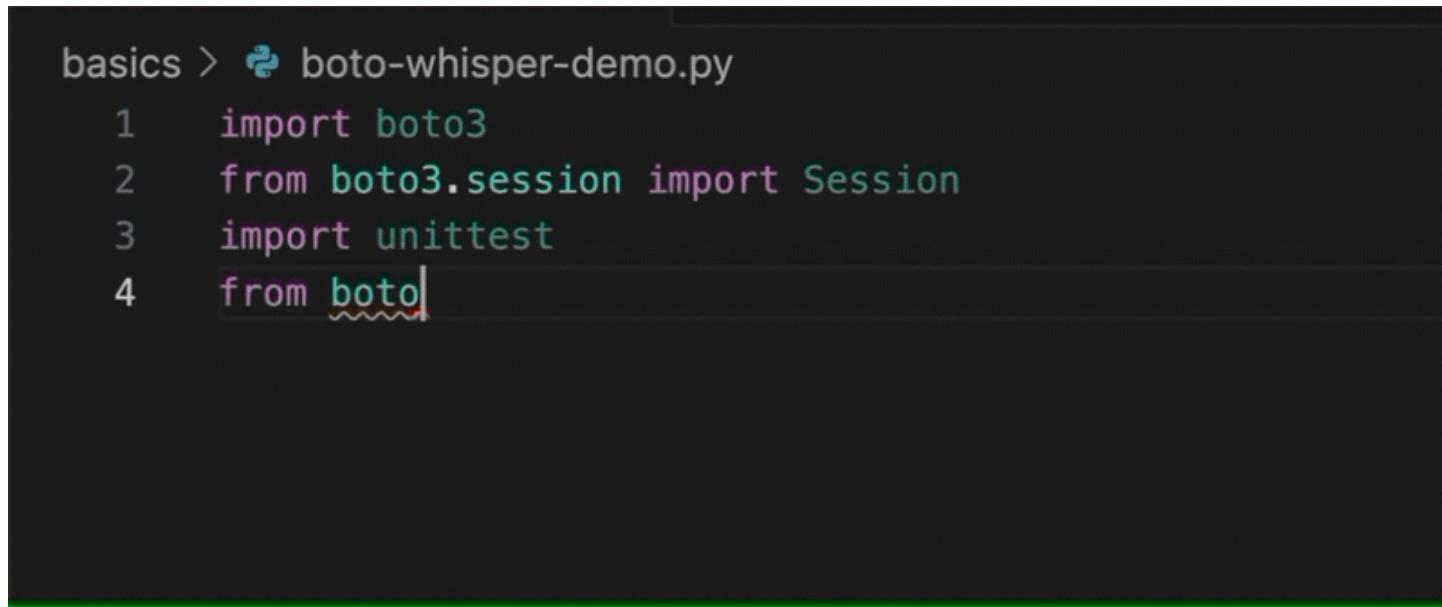
The Amazon Q panel will open.

2. Choose **Pause Auto-Suggestions** or **Resume Auto-Suggestions**.

Amazon Q code completion in action

This section demonstrates how Amazon Q can help you write a complete application. This application creates an Amazon S3 bucket and a Amazon DynamoDB table, plus a unit test that validates both tasks.

Here, Amazon Q helps the developer choose which libraries to import. Using the arrow keys, the developer toggles through multiple suggestions.



basics > `boto-whisper-demo.py`

```
1  import boto3
2  from boto3.session import Session
3  import unittest
4  from boto
```

Here, the developer enters a comment, describing the code they intend to write on the next line.

Amazon Q correctly anticipates the method to be called. The developer can accept the suggestion with the tab key.

```
basics > 🐍 boto-whisper-demo.py  
1 import boto3  
2 from boto3.session import Session  
3 import unittest  
4 from botocore.exceptions import ClientError  
5 import logging  
6 import time  
7  
8 # set up logging  
9 logging.basicConfig(level=logging.INFO)
```

Here, the developer prepares to define constants.

Amazon Q correctly anticipates that the first constant will be REGION and that its value will be us-east-1, which is the default.

```
basics > 🐍 boto-whisper-demo.py > ...  
8 # set up logging  
9 logging.basicConfig(level=logging.INFO)  
10  
11 #Create a new session  
12 session = Session()  
13  
14 # define constants  
15 DEFAULTREGION = 'us-east-1'
```

Here, the developer prepares to write code that will open sessions between the user and both Amazon S3 and DynamoDB.

Amazon Q, familiar with AWS APIs and SDKs, suggests the correct format.

```
8 # set up logging
9 logging.basicConfig(level=logging.INFO)
10
11 #Create a new session
12 session = Session()
13
14 # define constants
15 DEFAULT_REGION = 'us-east-1'
16 TEST_BUCKET_NAME = 'my-test-bucket' + str(int(time.time()))
17 TEST_TABLE_NAME = 'my-test-table' + str(int(time.time()))
18
19 # AWS Clients with session
20 s3 = session.client('s3', region_name=DEFAULT_REGION)
    dynamodb = session.client('dynamodb', region_name=DEFAULT_REGION)
```

The developer has merely written the name of the function that will create the bucket. But based on that (and the context), Amazon Q offers a full function, complete with try/except clauses.

Notice the use of TEST_BUCKET_NAME, which is a constant declared earlier in the same file.

```
18
19 # AWS Clients with session
20 s3_client = session.client('s3', region_name=us-east-1)
21 dynamodb_client = session.client('dynamodb', region_name=us-east-1)
22
23 def create_s3_bucket():
    """
    Creates a new S3 bucket
    """
    try:
        s3_client.create_bucket(Bucket=TEST_BUCKET_NAME)
    except ClientError as e:
        logging.error(e)
        return False
    return True
```

The developer has only just begun to type in the name of the function that will create a DynamoDB table. But Amazon Q can tell where this is going.

Notice that the suggestion accounts for the DynamoDB session created earlier, and even mentions it in a comment.

```
40  def create_dynamodb_table(table_name, region=None):
    # global dynamodb # Use the global dynamodb client created with the session
    print(f"Using region: {region}")
    print(f"DynamoDB endpoint URL: {dynamodb.meta.endpoint_url}") # Print the end
    try:
        print(f"Creating table in region: {region}") # Add this line to debug
        if region is None or region.lower() == 'us-east-1':
            response = dynamodb.create_table(
                TableName=table_name,
                KeySchema=[
                    {
                        'AttributeName': 'id',
                        'KeyType': 'HASH' # Partition key
                    }
                ],
            )
    
```

The developer has done little more than write the name of the unit test class, when Amazon Q offers to complete it.

Notice the built-in references to the two functions created earlier in the same file.

The developer has only just begun to type in the name of the function that will create a DynamoDB table. But Amazon Q can tell where this is going.

Notice that the suggestion accounts for the DynamoDB session created earlier, and even mentions it in a comment.

```
69 # Unit test class
70 class TestBotoWhisper(unittest.TestCase):
71     def setUp(self):
72         self.s3 = session.client('s3', region_name=DEFAULT_REGION)
73         self.dynamodb = session.client('dynamodb', region_name=DEFAULT_REGION)
74         self.s3_resource = session.resource('s3', region_name=DEFAULT_REGION)
75         self.dynamodb_resource = session.resource('dynamodb', region_name=DEFAULT_REGION)
76
77     def tearDown(self):
78         self.s3.delete_bucket(Bucket=TEST_BUCKET_NAME)
79         self.dynamodb.delete_table(TableName=TEST_TABLE_NAME)
80
81     def test_create_s3_bucket(self):
82         self.assertTrue(create_s3_bucket(TEST_BUCKET_NAME, DEFAULT_REGION))
83
84     def test_create_dynamodb_table(self):
85         self.assertTrue(create_dynamodb_table(TEST_TABLE_NAME, DEFAULT_REGION))
```

Based only on a comment and the context, Amazon Q supplies the entire main function.

```
basics > 🐍 boto-whisper-demo.py > ...
80     def test_create_dynamodb_table(self):
81         create_dynamodb_table('my-test-table')
82         client = boto3.client('dynamodb', region_name='us-east-1')
83         response = client.list_tables()
84         self.assertIn('my-test-table', response['TableNames'])
85
86     # Main function to create bucket and table
87     def main():
88         create_s3_bucket(TEST_BUCKET_NAME, region='us-east-1')
89         create_dynamodb_table(TEST_TABLE_NAME, region='us-east-1')
```

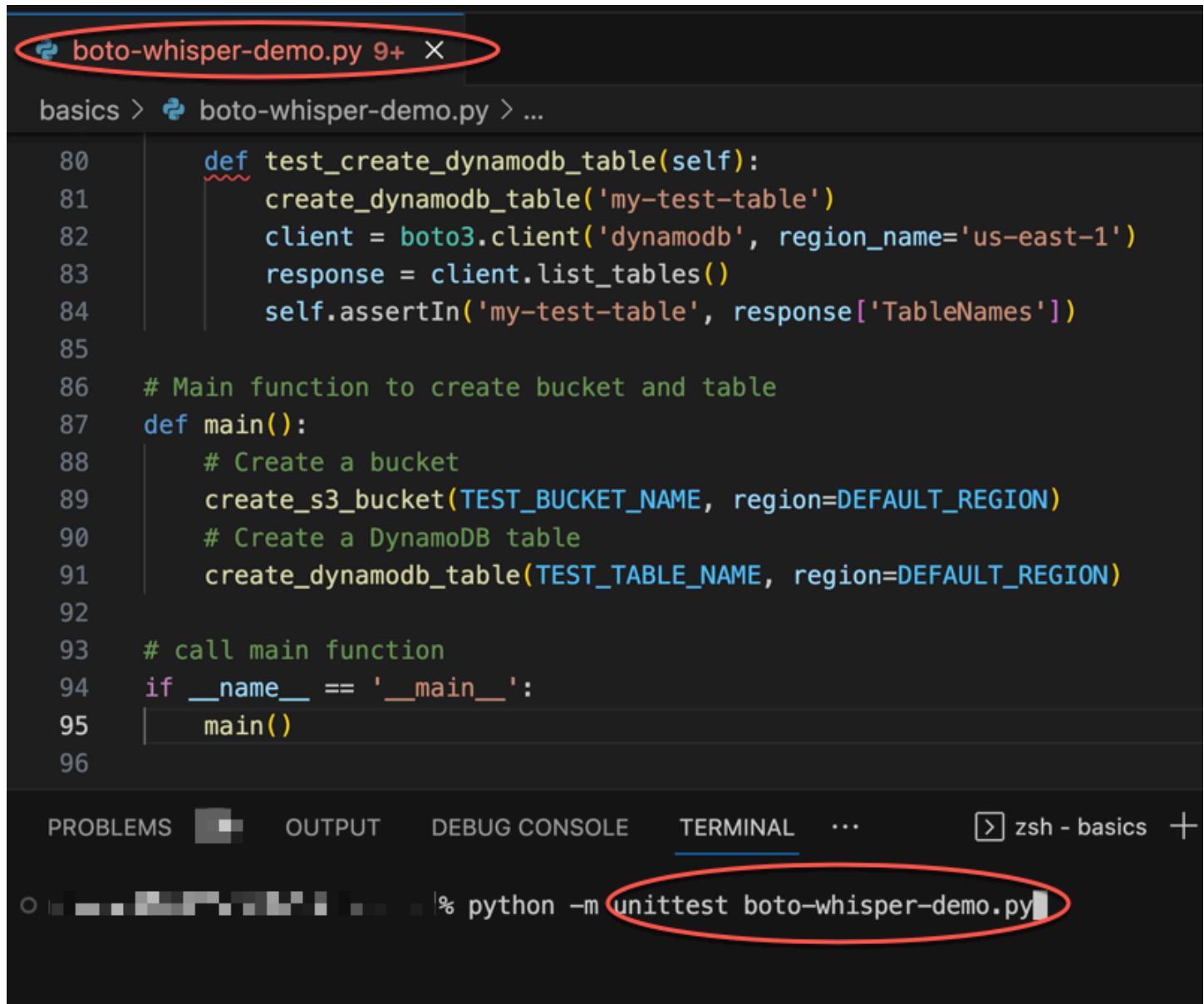
All that's left is the main guard, and Amazon Q knows it.

Based only on a comment and the context, Amazon Q supplies the entire main function.

```
# Main function to create bucket and table
def main():
    # Create a bucket
    create_s3_bucket(TEST_BUCKET_NAME, region=DEFAULT_REGION)
    # Create a DynamoDB table
    create_dynamodb_table(TEST_TABLE_NAME, region=DEFAULT_REGION)

# call| main function
if __name__ == '__main__':
    main()
```

Finally, the developer runs the unit test from the terminal of the same IDE where the coding took place.



```
80     def test_create_dynamodb_table(self):
81         create_dynamodb_table('my-test-table')
82         client = boto3.client('dynamodb', region_name='us-east-1')
83         response = client.list_tables()
84         self.assertIn('my-test-table', response['TableNames'])
85
86     # Main function to create bucket and table
87     def main():
88         # Create a bucket
89         create_s3_bucket(TEST_BUCKET_NAME, region=DEFAULT_REGION)
90         # Create a DynamoDB table
91         create_dynamodb_table(TEST_TABLE_NAME, region=DEFAULT_REGION)
92
93     # call main function
94     if __name__ == '__main__':
95         main()
96
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL ... zsh - basics +

```
% python -m unittest boto-whisper-demo.py
```

Generating inline suggestions in AWS coding environments

In addition to third-party IDEs, Amazon Q Developer can generate inline suggestions within AWS services that provide their own coding environments.

The following sections describe how to set up Amazon Q inline code suggestions within integrated AWS services.

Note

If you are using Amazon Q as part of an enterprise, then you are using Amazon Q Developer Pro. In that case, administrators at your organization must complete additional steps before you can start coding. For more information, see [Setting up Amazon Q Developer](#).

Topics

- [Using Amazon Q Developer with Amazon SageMaker Studio](#)
- [Using Amazon Q Developer with JupyterLab](#)
- [Using Amazon Q Developer with Amazon EMR Studio](#)
- [Using Amazon Q Developer with AWS Glue Studio](#)
- [Using Amazon Q Developer with AWS Lambda](#)
- [Using Amazon Q Developer with AWS Cloud9](#)
- [Using Amazon Q Developer with other services](#)

Using Amazon Q Developer with Amazon SageMaker Studio

You can chat with Amazon Q inside Amazon SageMaker Studio. You can also make code recommendations automatically as you write your code.

To set up and activate Amazon Q for Amazon SageMaker Studio, see [Set up Amazon Q Developer for your users](#) in the *Amazon SageMaker User Guide*.

To use Amazon Q Developer with Amazon SageMaker Studio, you must Add the Amazon Q-related permissions to your SageMaker execution role.

Create an IAM policy containing the following statement. Then attach that policy to the execution role (IAM) or permission set (IAM Identity Center) associated with your user profile.

Note

The `codewhisperer` prefix is a legacy name from a service that merged with Amazon Q Developer. For more information, see [Amazon Q Developer rename - Summary of changes](#).

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AmazonQDeveloperPermissions",  
      "Effect": "Allow",  
      "Action": ["codewhisperer:GenerateRecommendations"],  
      "Resource": "*"  
    }  
  ]  
}
```

For more information about policies, see [Creating IAM policies](#) and [Adding and removing IAM identity permissions](#) in the *IAM User Guide*.

Using Amazon Q Developer with JupyterLab

This page describes how to set up and activate Amazon Q Developer for JupyterLab. Once activated, Amazon Q can make code recommendations automatically as you write your code.

Note

Python is the only programming language that Amazon Q supports in JupyterLab.

Installing JupyterLab

Install [JupyterLab](#) on your computer or if you already have JupyterLab installed, check its version by running the following command.

```
pip show jupyterlab
```

Note the version in the response, and follow the use the corresponding directions in one of the following sections.

Installation using pip for Jupyter Lab version >= 4.0

You can install and enable the Amazon Q extension for JupyterLab 4 with the following commands.

```
# JupyterLab 4
```

```
pip install amazon-q-developer-jupyterlab-ext
```

Installation using pip for Jupyter Lab version >= 3.6 and < 4.0

You can install and enable the Amazon Q extension for JupyterLab 3 with the following commands.

```
# JupyterLab 3
pip install amazon-q-developer-jupyterlab-ext~=1.0
jupyter server extension enable amazon-q-developer-jupyterlab-ext
```

Authenticating with AWS Builder ID

In the following procedure, you will set up Builder ID, which you will use to authenticate when you enable Amazon Q.

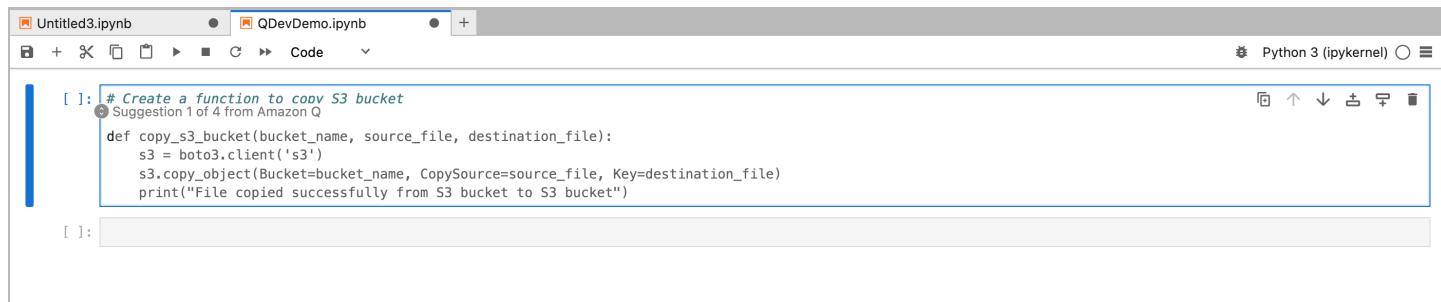
1. Refresh the browser tab on which you are using JupyterLab.
2. From the Amazon Q panel at the bottom of the window, choose **Start Amazon Q**.
3. From the pop-up window, choose **Copy Code and Proceed**.
4. On the **Create AWS Builder ID** page, if you don't have a Builder ID, enter a personal email address and choose **Next**.

If you already have a Builder ID, skip to the step about the **Authorize request** page.

5. On the next **Create your AWS Builder ID** page, enter a name and choose **Next**.
6. After you receive your email verification code, enter it in the blank field and choose **Verify**.
7. On the next screen, choose and confirm a password, then choose **Create AWS Builder ID**
8. On the next page choose **Allow** to allow Amazon Q to access your data.

Now you should be logged into Amazon Q in JupyterLab with Builder ID.

To begin coding, see [Using shortcut keys](#).



The screenshot shows the JupyterLab interface with two notebooks open: 'Untitled3.ipynb' and 'QDevDemo.ipynb'. A code cell in the 'Untitled3.ipynb' notebook contains the following Python code:

```
[ ]: # Create a function to copy S3 bucket
Suggestion 1 of 4 from Amazon Q
def copy_s3_bucket(bucket_name, source_file, destination_file):
    s3 = boto3.client('s3')
    s3.copy_object(Bucket=bucket_name, CopySource=source_file, Key=destination_file)
    print("File copied successfully from S3 bucket to S3 bucket")
```

Using Amazon Q Developer with Amazon EMR Studio

This page describes how to set up and activate Amazon Q Developer for Amazon EMR Studio. Once activated, Amazon Q can make code recommendations automatically as you write your ETL code.

Note

Amazon Q supports Python, which can be used to code ETL scripts for Spark jobs in Amazon EMR Studio.

Use the following procedure to set up Amazon EMR Studio to work with Amazon Q.

1. Set up [Amazon EMR Studio Notebook](#).
2. Attach the following policy to the IAM user role for Amazon EMR Studio Notebook.

Note

The codewhisperer prefix is a legacy name from a service that merged with Amazon Q Developer. For more information, see [Amazon Q Developer rename - Summary of changes](#).

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AmazonQDeveloperPermissions",  
            "Effect": "Allow",  
            "Action": [  
                "codewhisperer:GenerateRecommendations"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

3. Open the [Amazon EMR console](#).
4. Under Amazon EMR Studio, choose **Workspaces (Notebooks)**.

5. Select your desired Workspace and choose **Quick launch**.

Using Amazon Q Developer with AWS Glue Studio

This page describes how to set up and activate Amazon Q Developer for [AWS Glue Studio Notebook](#). Once activated, Amazon Q can make code recommendations automatically as you write your ETL code.

 **Note**

Amazon Q supports both Python and Scala, the two languages used for coding ETL scripts for Spark jobs in AWS Glue Studio.

In the following procedure, you will set up AWS Glue to work with Amazon Q.

1. [Set up AWS Glue Studio Notebook](#).
2. Attach the following policy to your IAM role for Glue Studio notebook

 **Note**

The codewhisperer prefix is a legacy name from a service that merged with Amazon Q Developer. For more information, see [Amazon Q Developer rename - Summary of changes](#).

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AmazonQDeveloperPermissions",  
            "Effect": "Allow",  
            "Action": [  
                "codewhisperer:GenerateRecommendations"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

3. Open the [Glue console](#)
4. Under **ETL jobs**, choose **Notebooks**.
5. Verify that **Jupyter Notebook** is selected. Choose **Create**.
6. Enter a **Job name**.
7. For IAM role, select the role that you configured to interact with Amazon Q
8. Choose **Start notebook**.

Using Amazon Q Developer with AWS Lambda

This document describes how to set up and activate Amazon Q Developer for the Lambda console. Once activated, Amazon Q can make code recommendations on demand in the Lambda code editor as you develop your function.

 **Note**

In the Lambda console, Amazon Q only supports functions using the Python and Node.js runtimes.

AWS Identity and Access Management permissions for Lambda

For Amazon Q to provide recommendations in the Lambda console, you must enable the correct IAM permissions for either your IAM user or role. You must add the `codewhisperer:GenerateRecommendations` permission, as outlined in the sample IAM policy below:

 **Note**

The `codewhisperer` prefix is a legacy name from a service that merged with Amazon Q Developer. For more information, see [Amazon Q Developer rename - Summary of changes](#).

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {
```

```
        "Sid": "AmazonQDeveloperPermissions",
        "Effect": "Allow",
        "Action": ["codewhisperer:GenerateRecommendations"],
        "Resource": "*"
    }
]
}
```

It is best practice to use IAM policies to grant restrictive permissions to IAM principals. For details about working with IAM for AWS Lambda, see [Identity and access management in AWS Lambda](#) in the *AWS Lambda Developer Guide*.

Activating Amazon Q Developer with Lambda

To activate Amazon Q in the Lambda console code editor, complete these steps.

 **Note**

Amazon Q for Lambda is only supported in US East (N. Virginia).

1. Open the [Functions page](#) of the Lambda console, and choose the function that you want to edit.
2. In the code editor under **Code source**, choose **Tools** in the top menu bar.
3. Choose **Amazon Q code suggestions**. This immediately activates the Amazon Q service, and a check mark appears next to this option. To deactivate, choose this option again.

For shortcut keys, see [Using shortcut keys](#).

Using Amazon Q Developer with AWS Cloud9

AWS Identity and Access Management permissions for AWS Cloud9

For Amazon Q to provide recommendations in AWS Cloud9 console, you must enable the correct IAM permissions for either your IAM user or role. You must add the `codewhisperer:GenerateRecommendations` permission, as outlined in the sample IAM policy below:

Note

The codewhisperer prefix is a legacy name from a service that merged with Amazon Q Developer. For more information, see [Amazon Q Developer rename - Summary of changes](#).

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AmazonQDeveloperPermissions",  
      "Effect": "Allow",  
      "Action": ["codewhisperer:GenerateRecommendations"],  
      "Resource": "*"  
    }  
  ]  
}
```

It is best practice to use IAM policies to grant restrictive permissions to IAM principals. For details about working with IAM for AWS Cloud9, see [Identity and access management in AWS Cloud9](#) in the *AWS Cloud9 user guide*.

Activating Amazon Q with AWS Cloud9

To activate Amazon Q in the AWS Cloud9 console code editor, complete these steps.

1. From inside your existing AWS Cloud9 environment, choose the AWS logo on the left edge of the window. A panel will expand rightward.
2. In the lower part of the panel, under **Developer tools**, open the **Amazon Q** dropdown.
3. Choose **Resume Auto-Suggestions**.

For examples of how Amazon Q integrates with AWS Cloud9 and displays code suggestions in the AWS Cloud9 IDE, see [Code examples](#).

Using Amazon Q Developer with other services

AWS Identity and Access Management permissions for other services

For Amazon Q to provide recommendations in the context of another service, you must enable the correct IAM permissions for either your IAM user or role. You must add the

`codewhisperer:GenerateRecommendations` permission, as outlined in the sample IAM policy below:

 **Note**

The `codewhisperer` prefix is a legacy name from a service that merged with Amazon Q Developer. For more information, see [Amazon Q Developer rename - Summary of changes](#).

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AmazonQDeveloperPermissions",  
            "Effect": "Allow",  
            "Action": ["codewhisperer:GenerateRecommendations"],  
            "Resource": "*"  
        }  
    ]  
}
```

It is best practice to use IAM policies to grant restrictive permissions to IAM principals. For details about working with IAM, see [Security best practices](#) in the *IAM user guide*.

Using shortcut keys

While getting inline suggestions from Amazon Q, you can use keyboard shortcuts for common actions you take, such as initiating Amazon Q or accepting a recommendation.

Choose the integrated development environment (IDE) where you are developing code to see keyboard shortcuts for your IDE.

Toolkit for Visual Studio

Action	Keyboard shortcut
Manually initiate Amazon Q	MacOS: Option + C
<code>AWSToolkit.CodeWhisperer.GetSuggestion</code> in the keybindings	Windows: Alt + C

Action	Keyboard shortcut
Accept a recommendation	Tab
Next recommendation Edit.NextSuggestion in the keybindings	MacOS: Option + . Windows: Alt + .
Previous recommendation Edit.PreviousSuggestion in the keybindings	MacOS: Option + , Windows: Alt + ,
Reject a recommendation	ESC, backspace, or keep typing and the recommendation will disappear as soon as there is a character mismatch.

See also Microsoft's [Visual Studio default keyboard shortcuts](#).

To change keybindings in Visual Studio, use Tools -> Options -> Keyboard.

AWS Toolkit for Visual Studio Code

Action	Keyboard shortcut
Manually initiate Amazon Q	MacOS: Option + C Windows: Alt + C
Accept a recommendation	Tab
Next recommendation	Right arrow
Previous recommendation	Left arrow
Reject a recommendation	ESC, backspace, or keep typing and the recommendation will disappear as soon as there is a character mismatch.

Action	Keyboard shortcut
Accept next word	Option + right arrow

To change keybindings in VS Code, see [Key Bindings for Visual Studio Code](#) on the VS Code website.

 **Note**

The inline suggestions toolbar in VS Code is disabled by default. For more information, see [Redesigned inline suggestions toolbar](#) on the VS Code website.

AWS Toolkit for JetBrains

Action	Keyboard shortcut
Manually initiate Amazon Q	MacOS: Option + C Windows: Alt + C
Accept a recommendation	Tab
Next recommendation	Right arrow
Previous recommendation	Left arrow
Reject a recommendation	ESC, backspace, or keep typing and the recommendation will disappear as soon as there is a character mismatch.

To change keybindings in IntelliJ, see [IntelliJ IDEA keyboard shortcuts](#) on the JetBrains website.

Amazon SageMaker

Action	Keyboard shortcut
Manually initiate Amazon Q	MacOS: Option + C

Action	Keyboard shortcut
	Windows: Alt + C
Accept a recommendation	Tab
Next recommendation	Down arrow
Previous recommendation	Up arrow
Reject a recommendation	ESC

JupyterLab

Action	Keyboard shortcut
Manually initiate Amazon Q	MacOS: Option + C Windows: Alt + C
Accept a recommendation	Tab
Next recommendation	Down arrow
Previous recommendation	Up arrow
Reject a recommendation	ESC

AWS Glue Studio Notebook

Action	Keyboard shortcut
Manually initiate Amazon Q	MacOS: Option + C Windows: Alt + C
Accept a recommendation	Tab
Next recommendation	Down arrow

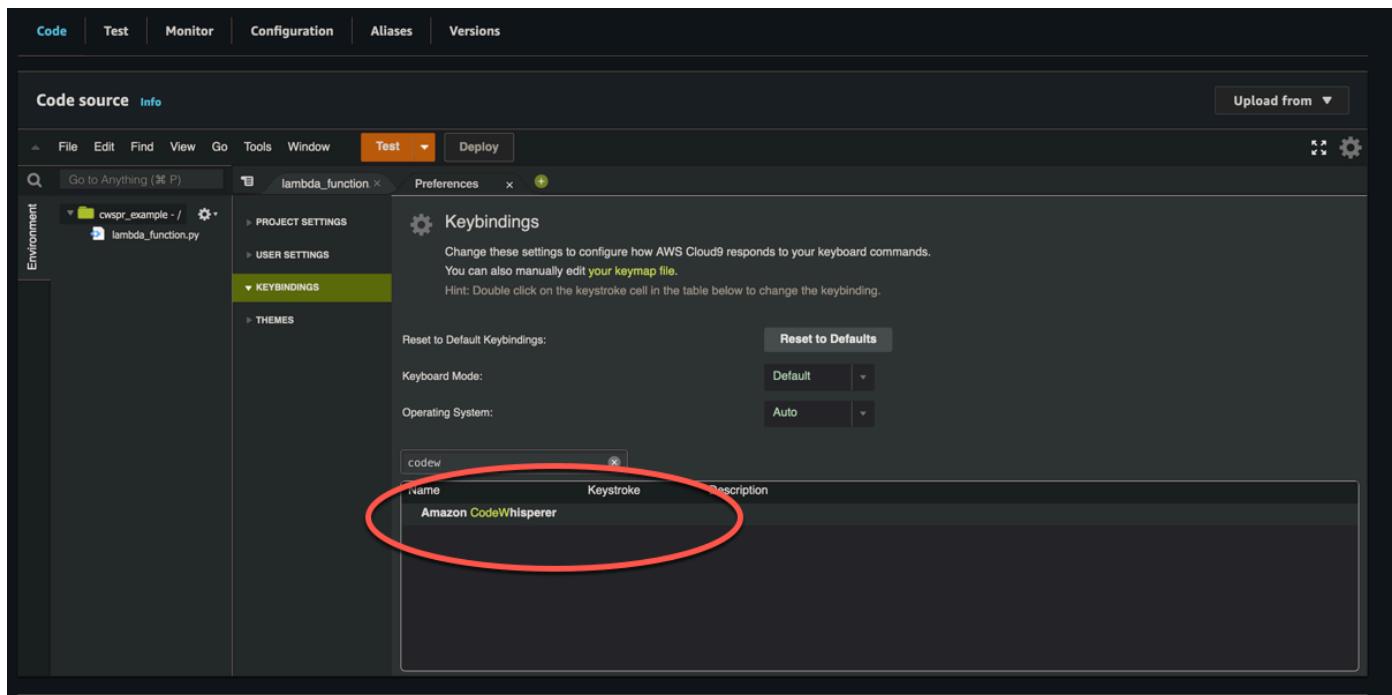
Action	Keyboard shortcut
Previous recommendation	Up arrow
Reject a recommendation	ESC

Lambda

Action	Keyboard shortcut
Manually fetch a code suggestion	MacOS: Option + C Windows: Alt + C
Accept a suggestion	Tab
Reject a suggestion	ESC, Backspace, scroll in any direction, or keep typing and the recommendation automatically disappears.

To change the key bindings, use the following procedure.

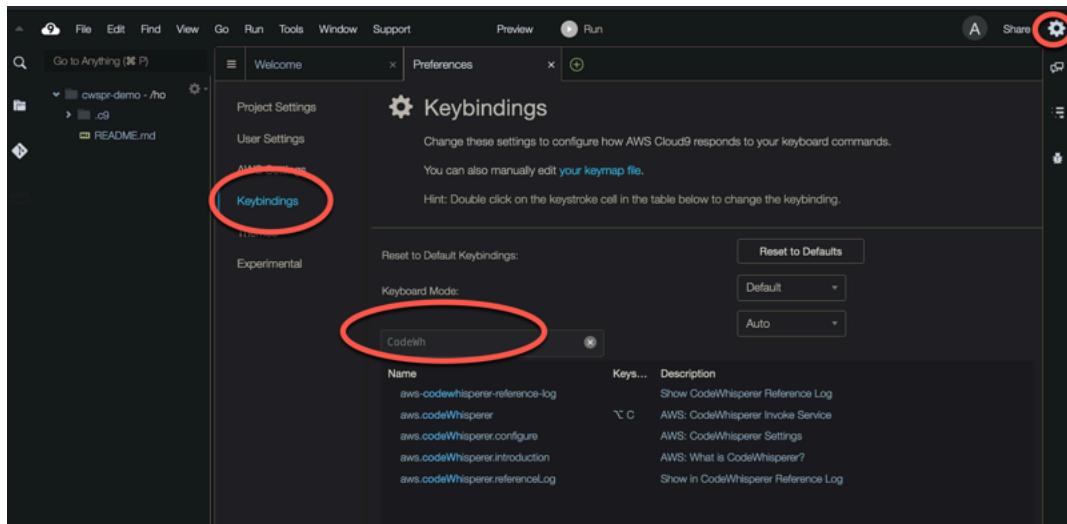
1. While viewing a particular function, choose the gear icon to open the **Preferences** tab.
2. On the **Preferences** tab, select **Keybindings**.
3. In the keybindings search box, enter Amazon Q.



AWS Cloud9

Action	Keyboard shortcut
Manually fetch a code suggestion	MacOS: Option + C Windows: Alt + C
Accept a suggestion	Tab
Reject a suggestion	ESC, Backspace, scroll in any direction, or keep typing and the recommendation automatically disappears.

1. While viewing a particular environment, choose the gear icon to open the **Preferences** tab.
2. On the **Preferences** tab, select **Keybindings**.
3. In the keybindings search box, enter Amazon Q.
4. In the Keystroke column, double-click the space corresponding to the function you're interested in.
5. Enter the keys that you want to bind the function to.



Using code references

Amazon Q learns, in part, from open-source projects. Sometimes, a suggestion it's giving you may be similar to a specific piece of training data. Code references include information about the source Amazon Q used to generate a recommendation.

Topics

- [View and update code references](#)
- [Turn code references off and on](#)
- [Opt out of code with references](#)

View and update code references

With the reference log, you can view references to code recommendations that are similar to training data. You can also update and edit code recommendations suggested by Amazon Q.

Choose your IDE to see steps for how to view and update code references.

Visual Studio Code

To display the Amazon Q reference log in VS Code, use the following procedure.

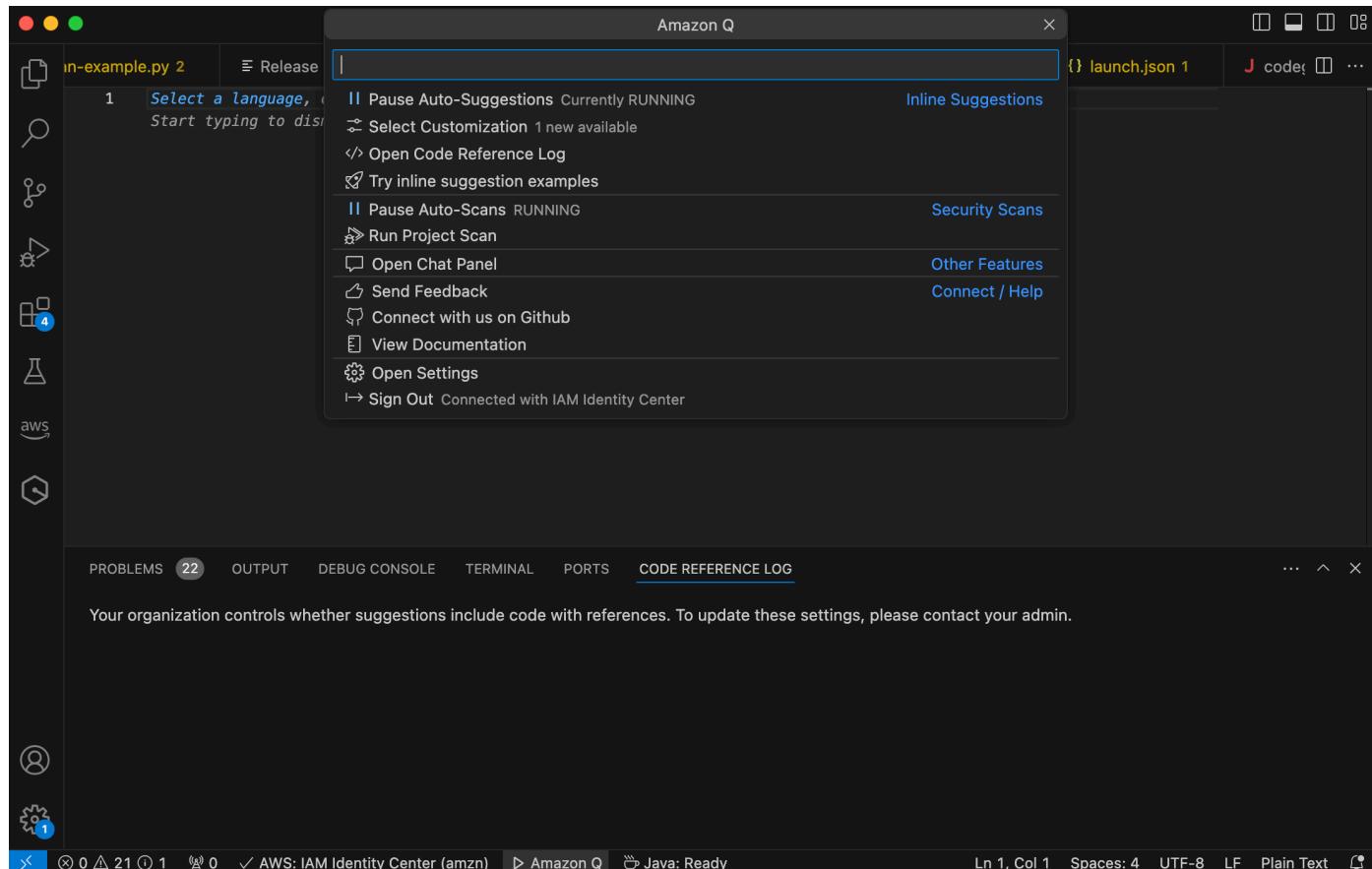
1. Make sure you are using the latest version of both VS Code and the Amazon Q extension.
2. In VS Code, choose **Amazon Q** from the component tray at the bottom of the IDE window.

The Amazon Q task bar opens at the top of the IDE window.

3. Choose **Open Code Reference Log**.

The code reference log tab opens. Any references to code recommendations are listed.

The following image shows the open Amazon Q task bar and code reference log tab.



JetBrains

To display the Amazon Q reference log in JetBrains IDEs, use the following procedure.

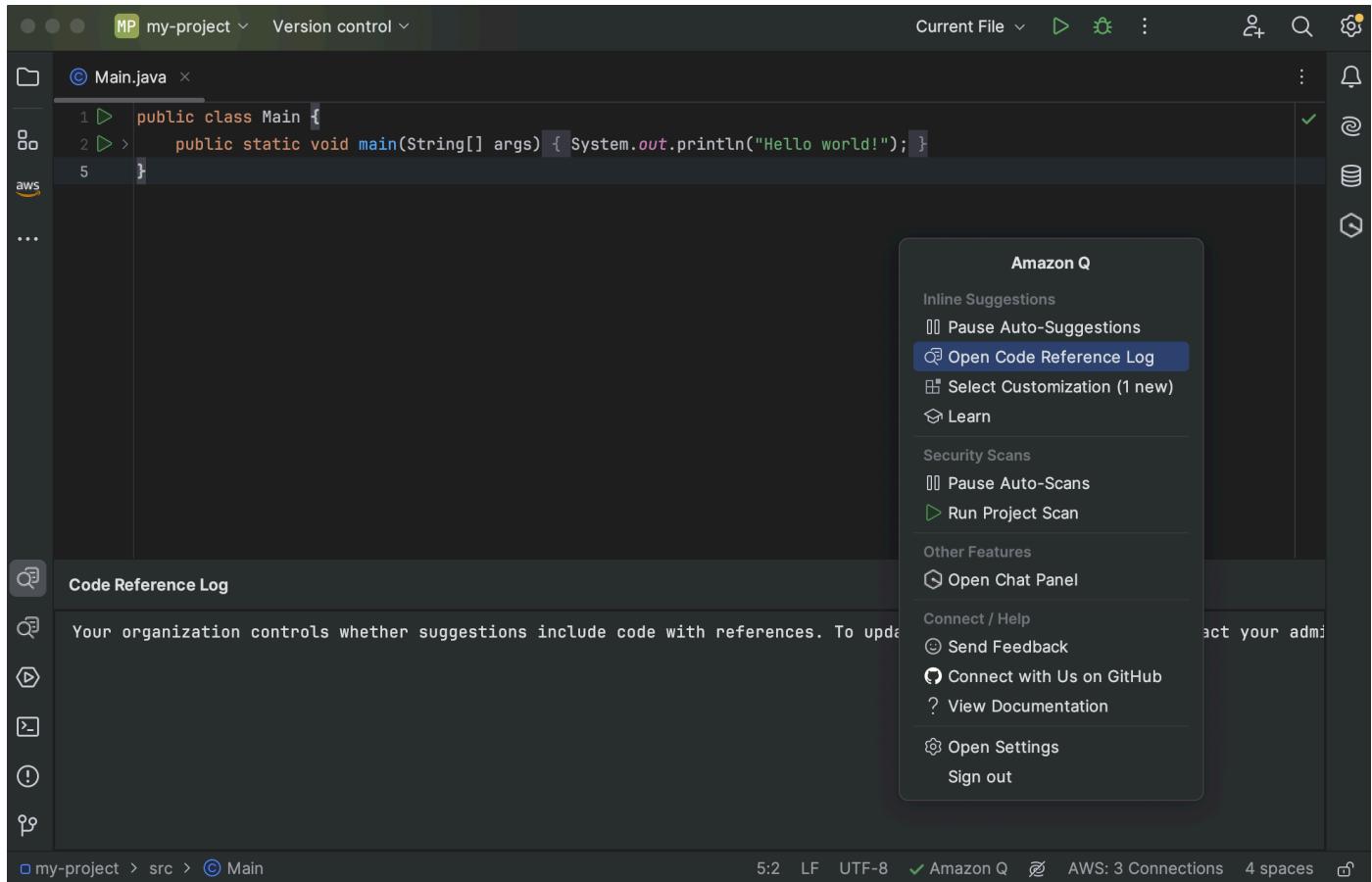
1. Make sure you are using the latest version of both your JetBrains IDE and the Amazon Q plugin.
2. In JetBrains, choose **Amazon Q** from the status bar at the bottom of the IDE window.

The Amazon Q task bar opens above the status bar.

3. Choose **Open Code Reference Log**.

The code reference log tab opens. Any references to code recommendations are listed.

The following image shows the open Amazon Q task bar and code reference log tab.



Toolkit for Visual Studio

When Amazon Q suggests code that contains a reference in the Toolkit for Visual Studio, the reference type appears in the suggestion description.

```
# Create function to create a DynamoDB Table
def Suggestion (License: MIT) 1 / 1 | Tab to accept | ⚙️
    table = dynamodb.create_table(
        TableName='Products',
        KeySchema=[
            {
                'AttributeName': 'id',
                'KeyType': 'HASH'
            },
            {
                'AttributeName': 'name',
                'KeyType': 'RANGE'
            }
        ],
        AttributeDefinitions=[{
            'AttributeName': 'id',
            'AttributeType': 'S

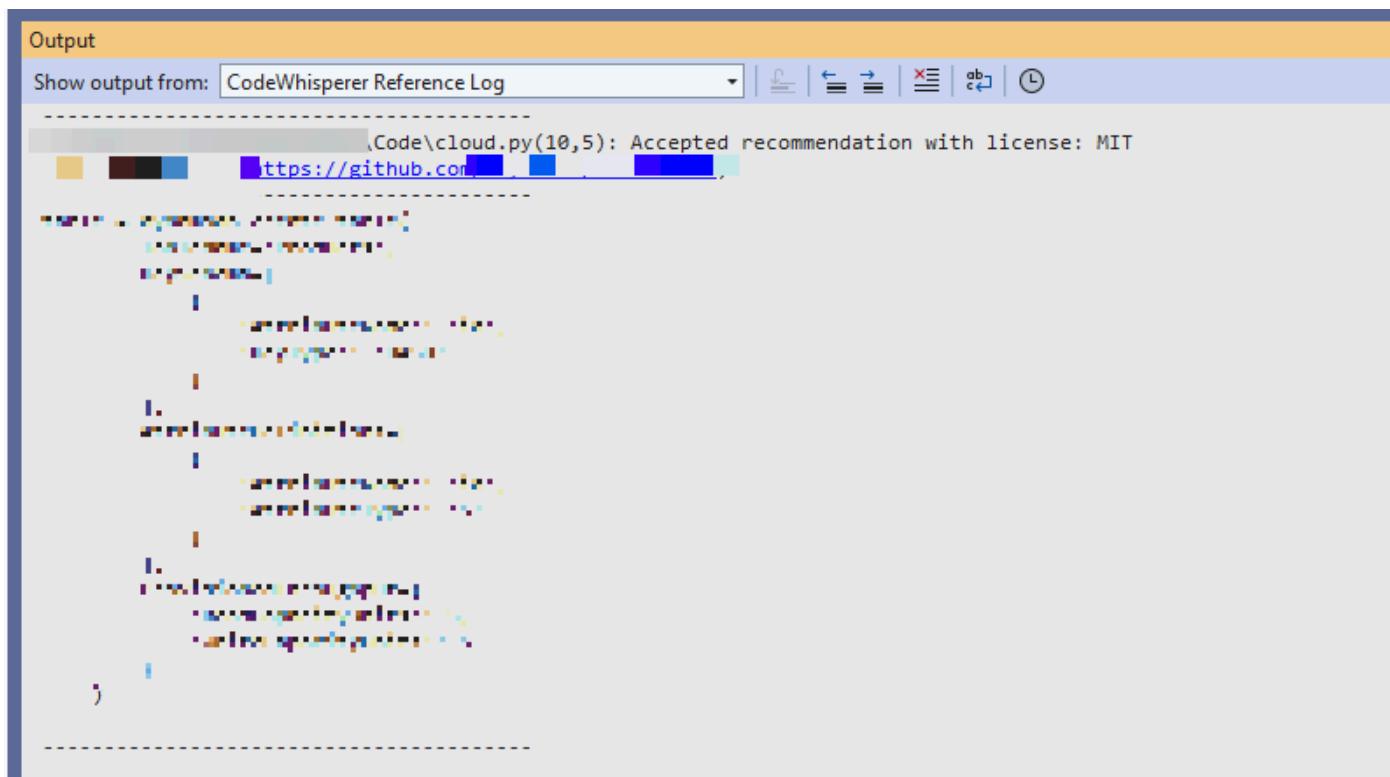
```

All accepted suggestions that contain references are captured in the reference log.

To access the reference log, choose the AWS icon, then select **Open Code Reference Log**.

A list of accepted suggestions that contain references will appear. This list includes:

- The location where the suggestion was accepted. Double clicking on this will take you to that location in your code.
- The associated license
- The referenced source code
- The fragment of code attributed to the reference



The screenshot shows the AWS Cloud 9 interface with the 'Output' tab selected. The 'Show output from' dropdown is set to 'CodeWhisperer Reference Log'. The log displays a series of code snippets and their corresponding GitHub URLs, indicating accepted recommendations with MIT licenses. The code snippets are part of a Python file named 'cloud.py'.

```
Code\cloud.py(10,5): Accepted recommendation with license: MIT
https://github.com/.../cloud.py#L10
def get_weather_forecast(city):
    response = requests.get(f"https://api.openweathermap.org/data/2.5/weather?q={city}&appid=...&units=metric")
    weather_data = response.json()
    forecast = weather_data['weather'][0]['description']
    return forecast
    
```

AWS Cloud 9

When you use Amazon Q with AWS Cloud 9, code references are on by default.

To turn them off, or to turn them back on later, use the following procedure.

1. On the AWS Cloud 9 console, in the upper left corner, choose the AWS Cloud 9 logo.
2. From the dropdown menu, choose **Preferences**.

On the right side of the console, the **Preferences** tab will open.

3. On the **Preferences** tab, under **Project Settings**, under **Extensions**, select **AWS Toolkit**.
4. Select or deselect **Amazon Q: Include Suggestions With Code References**.

Lambda

Amazon Q in Lambda does not support code references. When you use Amazon Q with Lambda, any code suggestions with references are omitted.

SageMaker Studio

To display the Amazon Q reference log in SageMaker Studio, use the following procedure.

1. At the bottom of the SageMaker Studio window, open the Amazon Q panel.
2. Choose **Open Code Reference Log**.

JupyterLab

To display the Amazon Q reference log in JupyterLab, use the following procedure.

1. At the bottom of the JupyterLab window, open the Amazon Q panel.
2. Choose **Open Code Reference Log**.

AWS Glue Studio Notebook

To display the Amazon Q reference log in AWS Glue Studio Notebook, use the following procedure.

1. At the bottom of the AWS Glue Studio Notebook window, open the Amazon Q panel.
2. Choose **Open Code Reference Log**.

Turn code references off and on

In most IDEs, code references are on by default. Choose your IDE to see steps for how to turn code references off or on.

Visual Studio Code

When you use Amazon Q with VS Code, code references are on by default.

To turn them off, or to turn them back on later, use the following procedure.

1. Make sure you are using the latest version of both VS Code and the Amazon Q extension.
2. In VS Code, choose **Amazon Q** from the component tray at the bottom of the IDE window.

- The Amazon Q task bar opens at the top of the IDE window.
3. Choose **Open Settings**. The settings tab opens with the options related to Amazon Q displayed.
 4. Select or deselect the box next to **Show Inline Code Suggestions with Code References**.

JetBrains

When you use Amazon Q with your JetBrains IDE, code references are on by default.

To turn them off, or to turn them back on later, use the following procedure.

1. Make sure you are using the latest version of both your JetBrains IDE and the Amazon Q plugin.
2. In JetBrains, choose **Amazon Q** from the status bar at the bottom of the IDE window.

The Amazon Q task bar opens above the status bar.
3. Choose **Open Settings**. The settings window opens with the options related to Amazon Q displayed.
4. Select or deselect the box next to **Include suggestions with code references**.

AWS Cloud 9

When you use Amazon Q with AWS Cloud 9, code references are on by default.

To turn them off, or to turn them back on later, use the following procedure.

1. On the AWS Cloud 9 console, in the upper left corner, choose the AWS Cloud 9 logo.
2. From the dropdown menu, choose **Preferences**.

On the right side of the console, the **Preferences** tab will open.
3. On the **Preferences** tab, under **Project Settings**, under **Extensions**, select **AWS Toolkit**.
4. Select or deselect **Amazon Q: Include Suggestions With Code References**.

Lambda

Amazon Q in Lambda does not support code references. When you use Amazon Q with Lambda, any code suggestions with references are omitted.

SageMaker Studio

When you use Amazon Q with SageMaker Studio, code references are on by default.

To turn them off, or to turn them back on later, use the following procedure.

1. From the top of the SageMaker Studio window choose **Settings**.
2. From the **Settings** dropdown, choose **Advanced Settings Editor**.
3. In the Amazon Q dropdown, select or deselect the box next to **Enable suggestions with code references**.

JupyterLab

When you use Amazon Q with JupyterLab, code references are on by default.

To turn them off, or to turn them back on later, use the following procedure.

1. From the top of the JupyterLab window choose **Settings**.
2. From the **Settings** dropdown, choose **Advanced Settings Editor**.
3. In the Amazon Q dropdown, select or deselect the box next to **Enable suggestions with code references**.

AWS Glue Studio Notebook

1. From the bottom of the AWS Glue Studio Notebook window choose **Amazon Q**.
2. From the pop-up menu, toggle the switch next to **Code with references**.

Note

Pausing code references will be valid only for the duration of the current AWS Glue Studio Notebook.

Opt out of code with references

In some IDEs, you can opt out of receiving suggestions with references at the administrator level.

Choose your IDE to see steps for opting out as an administrator.

Visual Studio Code

If you are an enterprise administrator, you can opt out of suggestions with code references for your entire organization. If you do this, individual developers in your organization will not be able to opt back in through the IDE. Those developers will be able to select and deselect the box discussed in the previous section, but it will have no effect if you have opted out at the enterprise level.

To opt out of suggestions with references at the enterprise level, use the following procedure.

1. In the Amazon Q Developer console, choose **Settings**.
2. In the **Amazon Q Developer account details** pane, choose **Edit**.
3. On the Edit details page, in the **Advanced settings** pane, deselect **Include suggestions with code references**.
4. Choose **Save changes**.

JetBrains

If you are an enterprise administrator, you can opt out of suggestions with code references for your entire organization. If you do this, individual developers in your organization will not be able to opt back in through the IDE. Those developers will be able to select and deselect the box discussed in the previous section, but it will have no effect if you have opted out at the enterprise level.

To opt out of suggestions with references at the enterprise level, use the following procedure.

1. In the Amazon Q Developer console, choose **Settings**.
2. In the **Amazon Q Developer account details** pane, choose **Edit**.
3. On the Edit details page, in the **Advanced settings** pane, deselect **Include suggestions with code references**.
4. Choose **Save changes**.

Toolkit for Visual Studio

To opt out of suggestions with references at the enterprise level, use the following procedure.

1. You can get to the code references setting in one of two ways:

- a. Choose the Amazon Q icon at the edge of the window, and then choose **Options...**
 - b. Go to **Tools -> AWS Toolkit -> Amazon Q**
2. Change the toggle to **True or False**, depending on whether you want to include suggestions with references.

AWS Cloud 9

Amazon Q in AWS Cloud 9 does not support opting out of code suggestions with references at the enterprise level.

To opt out at the individual developer level, see [Toggling code references](#).

Lambda

Amazon Q in Lambda does not support code references. When you use Amazon Q with Lambda, any code suggestions with references are omitted.

SageMaker Studio

Amazon Q does not support opting out of code suggestions with references at the enterprise level in SageMaker Studio.

JupyterLab

Amazon Q does not support opting out of code suggestions with references at the enterprise level in JupyterLab.

AWS Glue Studio Notebook

Amazon Q does not support opting out of code suggestions with references in AWS Glue Studio Notebook.

Code examples

Amazon Q can suggest code in different scenarios. To understand how it can help you as you write code in your programming language of choice, view the following code examples.

Topics

- [Using Amazon Q Developer for single-line code completion](#)
- [Using Amazon Q Developer for full function generation](#)
- [Using Amazon Q Developer for block completion](#)

- [Using Amazon Q Developer for Docstring, JSDoc, and Javadoc completion](#)
- [Using Amazon Q Developer for line-by-line recommendations](#)

Using Amazon Q Developer for single-line code completion

When you start typing out single lines of code, Amazon Q makes suggestions based on your current and previous inputs.

C++

A screenshot of a C++ code editor interface. The code shown is:

```
17 int main(int argc, char **argv) {
18     Aws::SDKOptions options;
19     Aws::InitAPI(options); // Should only be called once.
20     {
21         Aws::Client::ClientConfiguration clientConfig;
22
23         clientConfig.region = "us-east-1";
24
25         Aws::SQS::SQSClient sqsClient(clientConfig);
26
27         Aws::Vector<Aws::String> allQueueUrls;
28         Aws::String nextToken; // Next token is used to handle a paginated response.
29         do {
30             Aws::SQS::Model::ListQueuesRequest request;
31
32             [Completion Suggestion Bar]
33
34         } while (!nextToken.empty());
35     }
36 }
```

The code editor displays a completion suggestion bar above the cursor at line 32, indicating potential completions for the current context.

JavaScript

In this example, Amazon Q completes a line of code that the developer begins.

A screenshot of a JavaScript code editor interface. The code shown is:

```
1  /*
2  * Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
3  * SPDX-License-Identifier: Apache-2.0
4  */
5
6 // Upload an object to Amazon S3 bucket.
7 
```

The code editor displays a completion suggestion bar above the cursor at line 7, indicating potential completions for the current context.

TypeScript

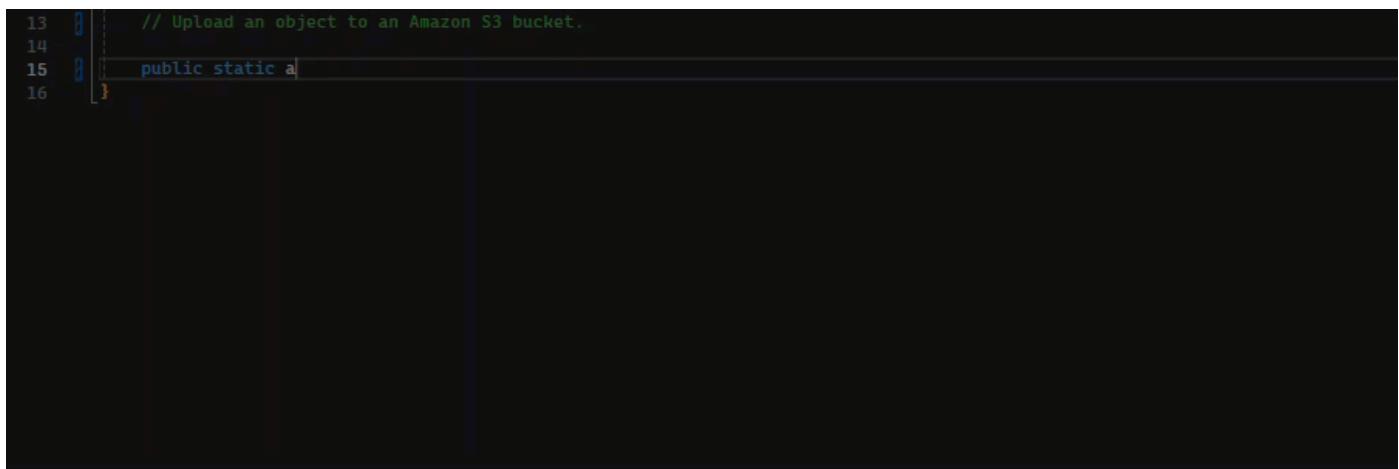
In this example, the user enters a full comment, and then Amazon Q supplies the code that goes with it.



```
TS index.ts  X
TS index.ts > ...
1   import {S3Client} from "@aws-sdk/client-s3";
2
3   const client = new S3Client({});
4
5   |
```

C#

In this example, Amazon Q provides a single-line recommendation based on a comment.



```
13 // Upload an object to an Amazon S3 bucket.
14
15 public static a
16 }
```

Shell

In the image below, Amazon Q offers recommendations on how to complete a single line of code.

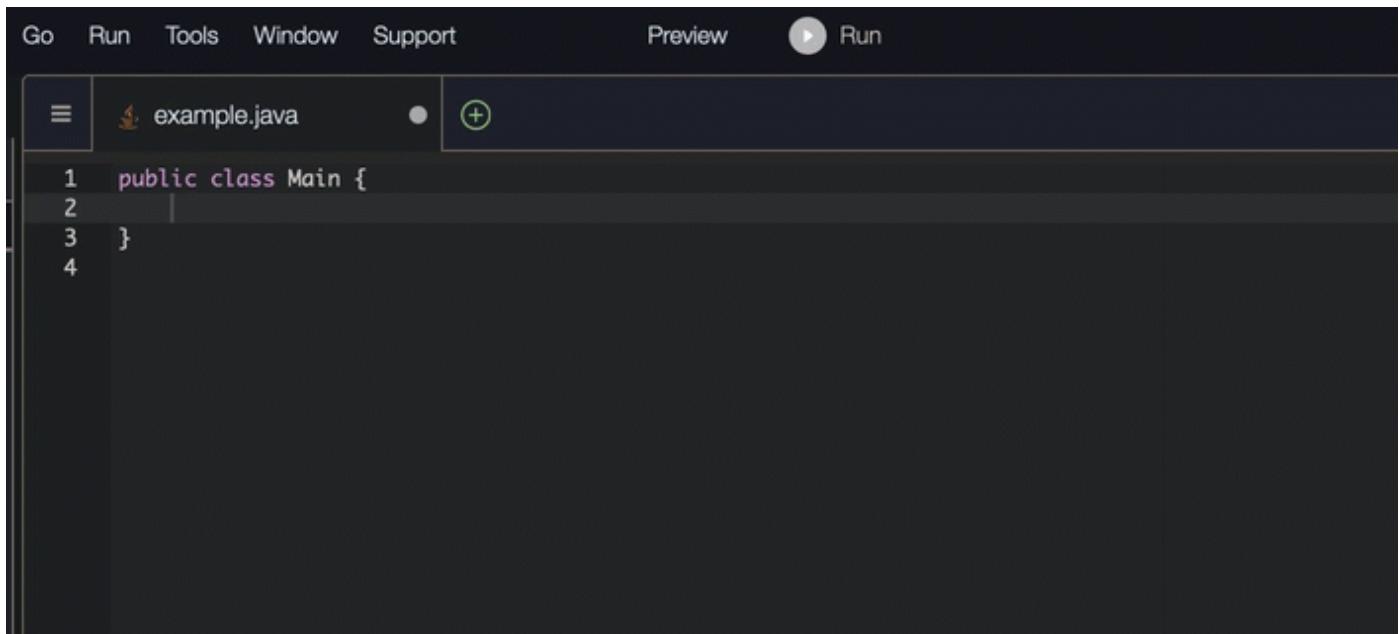
```
local access_key_response
access_key_response=$(iam_create_user_access_key -u "$user_name")
# shellcheck disable=SC2181
if [[ ${?} != 0 ]]; then
    errecho "The access key failed to create. This demo will exit."
    clean_up "$user_name"
    return 1
fi
```

Java

When you start typing out single lines of code, Amazon Q makes suggestions based on your current and previous inputs.

In the example below, in Java, a user enters the string `public` into an existing class.

Based on the input, Amazon Q generates a suggestion for the signature of the main method.



The screenshot shows a Java code editor interface. The menu bar includes 'Go', 'Run', 'Tools', 'Window', 'Support', 'Preview', and 'Run'. A file named 'example.java' is open. The code currently visible is:

```
1 public class Main {  
2  
3 }  
4
```

A cursor is positioned at the end of the first line. A green circular icon with a plus sign (+) is located to the right of the code editor window, indicating an AI suggestion or completion feature.

Python

In this example, Amazon Q recommends a single line of code, based on the developer's comment.

```
sagemaker_session = sage.Session()
bucket = sagemaker_session.default_bucket()
runtime = boto3.client("runtime.sagemaker")
s3 = boto3.resource("s3")

# Create a prefix called sampledata.
prefix = "sampledata"

# Create a filename called rawdata.csv
filename = "rawdata.csv"
```

Using Amazon Q Developer for full function generation

Amazon Q can generate an entire function based on a comment that you've written. As you finish your comment Amazon Q will suggest a function signature. If you accept the suggestion, Amazon Q automatically advances your cursor to the next part of the function and makes a suggestion. Even if you enter an additional comment or line of code in between suggestions, Amazon Q will refactor based on your input.

C

```
32
33     bool AwsDoc::SQS::createQueue(const Aws::String &queueName,
34                                     const Aws::Client::ClientConfiguration &clientConfigurat
```

C++

A screenshot of a code editor showing a partial C++ function definition. The code is as follows:

```
32     bool AwsDoc::SQS::createQueue(const Aws::String &queueName,
33                                     const Aws::Client::ClientConfiguration &clientConfigurat
```

JavaScript

In the following example, the user generates, and then edits, a full function based on a set of comments.

A screenshot of a code editor showing a generated AWS Lambda handler function named index.js. The code is as follows:

```
1 /**
2  * AWS Lambda handler
3  *
4  * Exports a single function that takes the "operand" property from the event
5  * input, squares it, and returns it.
6 */
7 |
8 |
9 |
10
```

In the following image, a user has written a function signature for reading a file from Amazon S3. Amazon Q then suggests a full implementation of the `read_from_s3` method.

A screenshot of a code editor showing a function signature and an AI-generated implementation. The code is as follows:

```
def read_from_s3(bucket, key):
    import boto3
    s3 = boto3.client('s3')
    obj = s3.get_object(Bucket=bucket, Key=key)
    return obj['Body'].read().decode('utf-8')
```

Note

Sometimes, as in the previous example, Amazon Q includes import statements as part of its suggestions. As a best practice, manually move these import statements to the top of your file.

As another example, in the following image, a user has written a function signature. Amazon Q then suggests a full implementation of the quicksort method.

```
def quicksort(a):
    if len(a) <= 1:
        return a
    else:
        pivot = a[0]
        less = [i for i in a[1:] if i <= pivot]
        greater = [i for i in a[1:] if i > pivot]
        return quicksort(less) + [pivot] + quicksort(greater)
```

Amazon Q considers past code snippets when making suggestions. In the following image, the user in the previous example has accepted the suggested implementation for quicksort above. The user then writes another function signature for a generic sort method. Amazon Q then suggests an implementation based on what has already been written.

```
def quicksort(a):
    if len(a) <= 1:
        return a
    else:
        pivot = a[0]
        less = [i for i in a[1:] if i <= pivot]
        greater = [i for i in a[1:] if i > pivot]
        return quicksort(less) + [pivot] + quicksort(greater)

def sort(a):
    return quicksort(a)
```

In the following image, a user has written a comment. Based on this comment, Amazon Q then suggests a function signature.

```
# Binary search function
```

```
def binary_search(arr, l, r, x):
```

In the following image, the user in the previous example has accepted the suggested function signature. Amazon Q can then suggest a complete implementation of the `binary_search` function.

```
# Binary search function
```

```
def binary_search(arr, l, r, x):
```

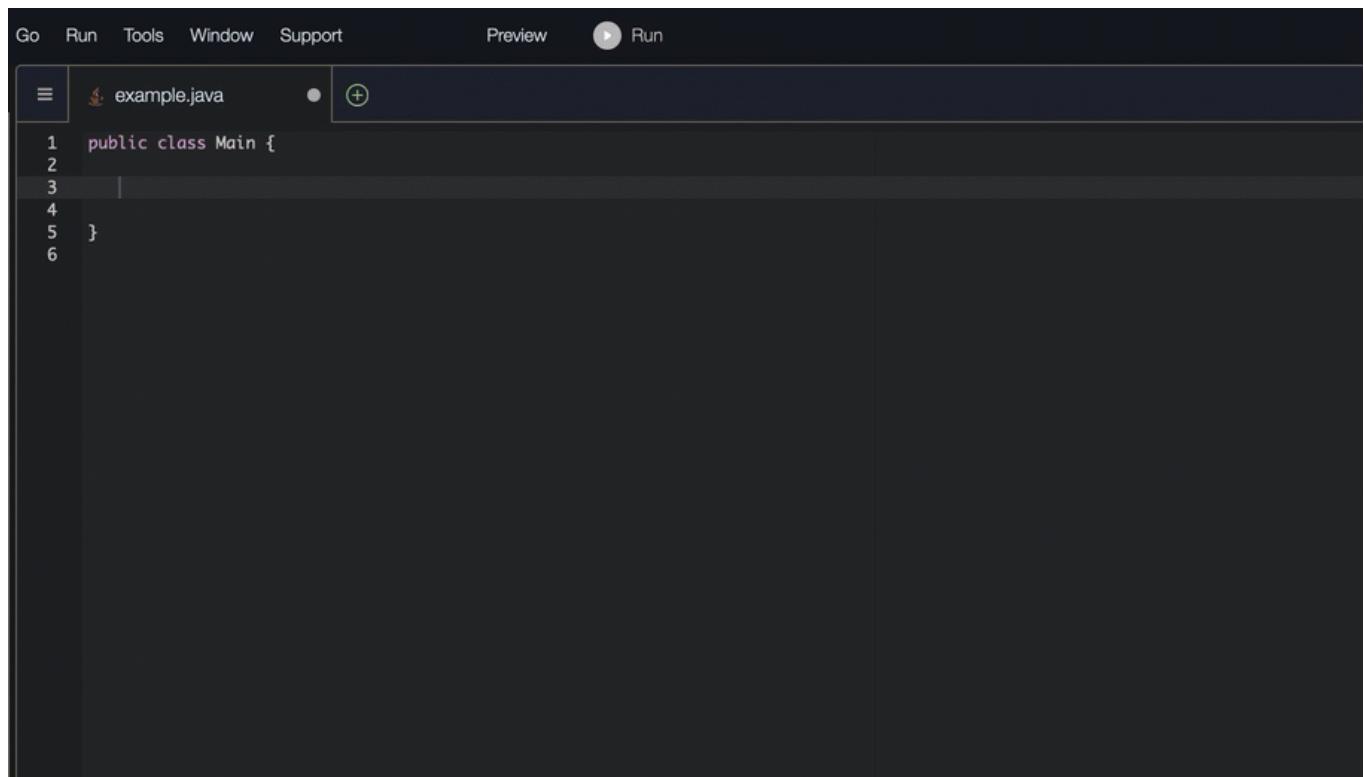
```
    while l <= r:
        mid = l + (r - l) // 2
        if arr[mid] == x:
            return mid
        elif arr[mid] < x:
            l = mid + 1
        else:
            r = mid - 1
```

Java

The following list contains examples of how Amazon Q makes suggestions and advances you through the entire process of creating a function.

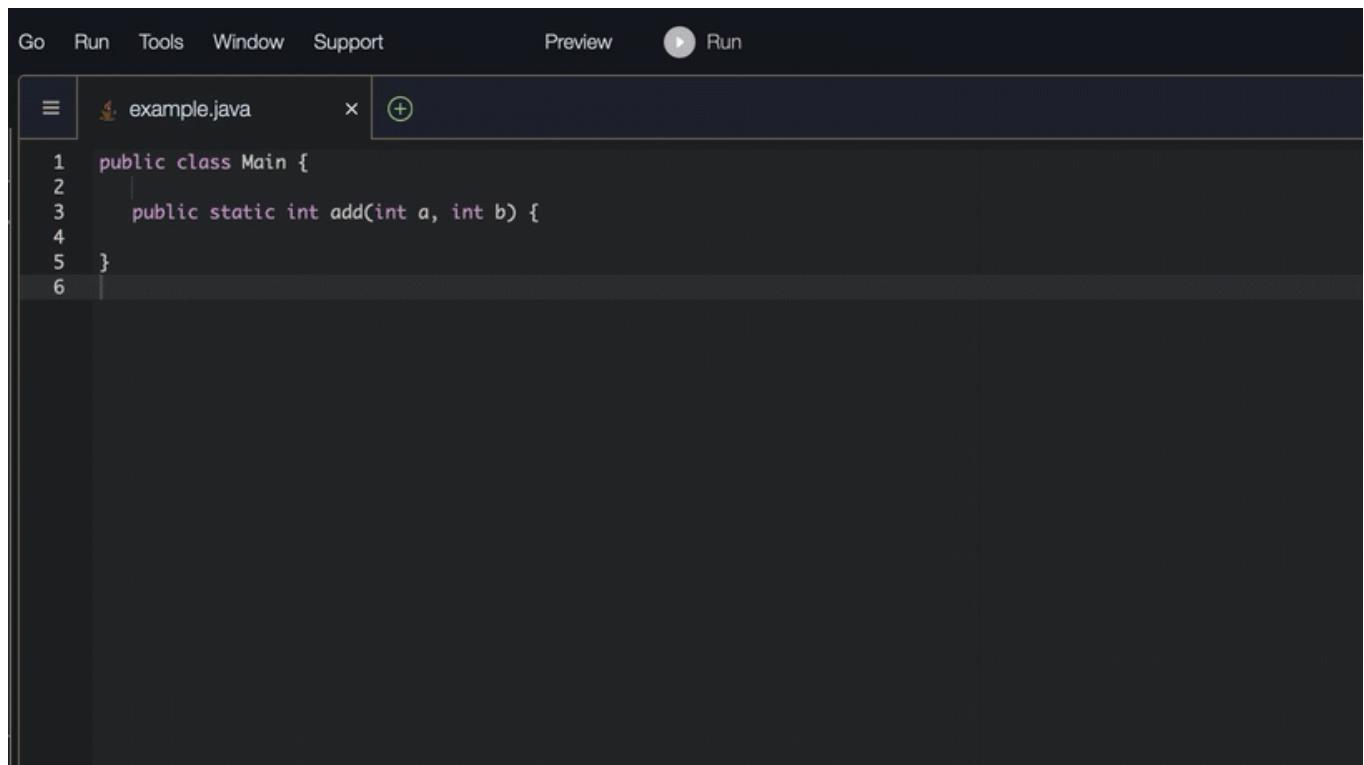
1. In the following example, a user inputs a comment. Amazon Q suggests a function signature.

After the user accepts that suggestion, Amazon Q suggests a function body.



```
1 public class Main {  
2     // This is a test.  
3 }  
4  
5 }
```

2. In the image below, a user inputs a comment in the body of the function prior to accepting a suggestion from Amazon Q. On the following line, Amazon Q generates a suggestion based on the comment.



```
1 public class Main {  
2     // Add two numbers.  
3     public static int add(int a, int b) {  
4         return a + b;  
5     }  
6 }
```

C#

In the following example, Amazon Q recommends a full function.

```
15  // Create a function that outputs DynamoDB table names
16
17  public static async Task ListTables(AmazonDynamoDBClient |
18 }
```

TypeScript

In the following example, Amazon Q generates a function based on the user's docstrings.

```
/** 
 * Upload a large file to an S3 bucket in multiple parts.
 * @param {string} fileName -- The name of the file to upload.
 * @param {string} bucketName -- The name of the bucket to upload to.
 */
```

Python

Amazon Q can generate an entire function based on a comment that you've written. As you finish your comment, Amazon Q will suggest a function signature. If you accept the suggestion, Amazon Q automatically advances your cursor to the next part of the function and makes a suggestion. Even if you enter an additional comment or line of code in between suggestions, Amazon Q will refactor based on your input.

In the following example, Amazon Q generates both a full function and the corresponding unit test.

```
1 import boto3
2 ddb_client = boto3.client('dynamodb')
3
```

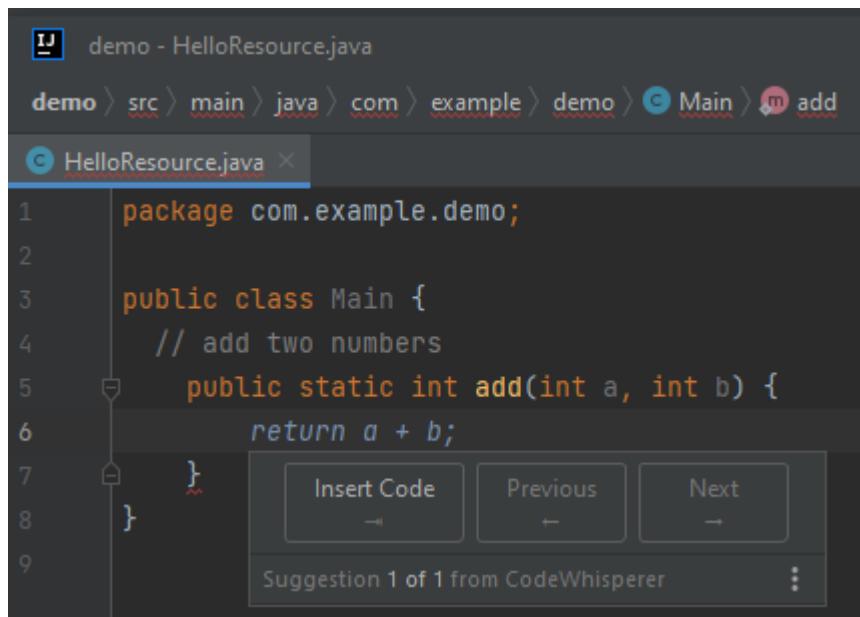
The following list contains examples of how Amazon Q makes suggestions and advances you through the entire process of creating a function.

1. In the image below, a user has input a comment. The function signature, located below the comment, is a suggestion from Amazon Q.

A screenshot of a Java code editor showing a file named `HelloResource.java`. The code defines a class `Main` with a static method `add`. A tooltip or suggestion box is overlaid on the code editor, containing three buttons: `Insert Code`, `Previous`, and `Next`. Below the buttons, the text `Suggestion 2 of 2 from CodeWhisperer` is visible. The code in the editor is:

```
1 package com.example.demo;
2
3 class Main {
4     //add two numbers
5     public static int add(int a, int b) {
6     }
7 }
```

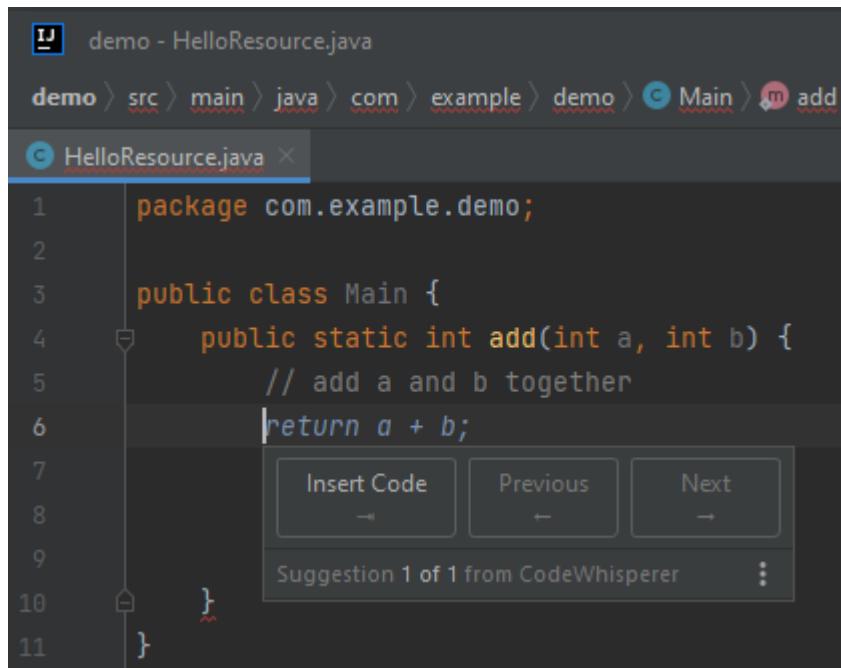
2. In the image below, the user has accepted the Amazon Q suggestion for a function signature. Accepting the suggestion automatically advanced the cursor and Amazon Q has made a new suggestion for the function body.



A screenshot of a Java code editor showing a file named `HelloResource.java`. The code defines a class `Main` with a static method `add` that returns the sum of two integers. A tooltip from Amazon Q is displayed over the closing brace of the `add` method, containing three buttons: `Insert Code`, `Previous`, and `Next`. Below the buttons, it says "Suggestion 1 of 1 from CodeWhisperer".

```
1 package com.example.demo;
2
3 public class Main {
4     // add two numbers
5     public static int add(int a, int b) {
6         return a + b;
7     }
8 }
9
10
11 }
```

3. In the image below, a user input a comment in the body of the function prior to accepting a suggestion from Amazon Q. On the following line, Amazon Q has generated a new suggestion based on the content of the comment.



A screenshot of a Java code editor showing the same `HelloResource.java` file. The user has added a comment `// add a and b together` before the `return` statement. A tooltip from Amazon Q is displayed over the `return` statement, containing three buttons: `Insert Code`, `Previous`, and `Next`. Below the buttons, it says "Suggestion 1 of 1 from CodeWhisperer".

```
1 package com.example.demo;
2
3 public class Main {
4     public static int add(int a, int b) {
5         // add a and b together
6         return a + b;
7     }
8 }
9
10
11 }
```

In this example, Amazon Q recommends a full function after the user types part of the signature.

```
examplebucketname = "example-bucket-1"
```

Using Amazon Q Developer for block completion

Block completion is used to complete your if/for/while/try code blocks.

C

```
9
10 // function to pop the stack
11 int pop(Stack *stack) {
12     if (stack->top == -1) {
13         printf("Stack is empty\n");
14         return -1;
15     }
16     return stack->array[stack->top--];
17 }
18
19 // function to push the stack
20 void push(Stack *stack, int data) {
21 }
```

C++

A screenshot of a code editor showing a C++ file. The code is as follows:

```
33     bool AwsDoc::RDS::describeDBInstance(const Aws::String &dbInstanceIdentifier,
34                                         Aws::RDS::Model::DBInstance &instanceResult,
35                                         const Aws::RDS::RDSClient &client) {
36
37     }
38
39 }
```

The cursor is at the end of the closing brace on line 38. A dropdown menu is open above the cursor, showing suggestions for the completion of the if statement. The suggestions include:

- if (dbInstanceIdentifier == "my-instance") {
- if (dbInstanceIdentifier != "my-instance") {
- if (dbInstanceIdentifier == "my-instance") {
- if (dbInstanceIdentifier != "my-instance") {

Java

In the example below, a user enters the signature of an `if` statement. The body of the statement is a suggestion from Amazon Q.

A screenshot of a code editor showing a Java file named `example.java`. The code is as follows:

```
1 public class Main {
2
3     |
4
5     }
6
```

The cursor is at the end of the opening brace on line 5. A dropdown menu is open above the cursor, showing suggestions for the completion of the if statement. The suggestions include:

- if (true) {
- if (false) {
- if (true) {
- if (false) {

C#

In the image below, Amazon Q recommends a way to complete the function.

A screenshot of a code editor showing a portion of a TypeScript file. The code is as follows:

```
8     public int CalculateFibonacci(int n)
9     {
10    }
11 }
12 }
```

TypeScript

In the image below, Amazon Q recommends a way to complete the function.

A screenshot of a code editor showing a portion of a TypeScript file named index.ts. The code is as follows:

```
ts index.ts 2 ×
```

```
ts index.ts > [?] uploadFile
1 import { S3Client } from "@aws-sdk/client-s3";
2
3 const client = new S3Client({});
4
5 /**
6  * Upload local file to bucket
7 */
8 export const uploadFile = async (
```

AWS Toolkit for JetBrains

In the image below, a user has input the signature of an `if` statement. The body of the statement, `System.out.println("negative");` is a suggestion from Amazon Q.

The screenshot shows a Java code editor with a file named `HelloResource.java`. The code defines a `Main` class with an `if` statement. A code completion suggestion box is open at the end of the `if` block, containing the line `System.out.println("Number is negative")`. Below the suggestion are buttons for "Insert Code", "Previous", and "Next". A message at the bottom of the box says "Suggestion 1 of 3 from CodeWhisperer".

```
demo - HelloResource.java
demo > src > main > java > com > example > demo > Main

HelloResource.java ×

1 package com.example.demo;
2
3 class Main {
4     if(number< 0)
5
6         {
7             System.out.println("Number is negative")
8         }
9     }
10 }
```

Python

In this example, Amazon Q recommends a block of code, based on the context.

The screenshot shows a Python code editor with a function definition for `print_bucket_contents`. The function prints the contents of an S3 bucket. A code completion suggestion box is open at the end of the `for` loop, containing the line `print(obj)`. Below the suggestion are buttons for "Insert Code", "Previous", and "Next". A message at the bottom of the box says "Suggestion 1 of 3 from CodeWhisperer".

```
examplebucketname = "example-bucket-1"

def print_bucket_contents(bucket_name):
    ...
    Print the contents of a bucket.
    ...
    print(f"Printing bucket contents for bucket {bucket_name}")
    for obj in s3.Bucket(bucket_name).objects.all():
        print(obj)
```

Using Amazon Q Developer for Docstring, JSDoc, and Javadoc completion

Amazon Q can help you generate or complete documentation inside your code.

C++

```

7  /// <summary>
8  /// This example shows how to attach a policy to an IAM role.
9  /// </summary>
10 //> <param name="roleName">
11 <bool AwsDoc::IAM::putRolePolicy(
12     const Aws::String &roleName,
13     const Aws::String &policyName,
14     const Aws::String &policyDocument,
15     const Aws::Client::ClientConfiguration &clientConfig) {
16     Aws::IAM::IAMClient iamClient(clientConfig);
17     Aws::IAM::Model::PutRolePolicyRequest request;
18
19     request.SetRoleName(roleName);
20     request.SetPolicyName(policyName);
21     request.SetPolicyDocument(policyDocument);
22
23     Aws::IAM::Model::PutRolePolicyOutcome outcome = iamClient.PutRolePolicy(request);
24     if (!outcome.IsSuccess()) {
25         std::cerr << "Error putting policy on role. " <<
26             outcome.GetError().GetMessage() << std::endl;

```

Javascript

In this example, Amazon Q fills in JSDoc parameters based on existing constants.

```

1 import {PutObjectCommand, S3Client} from "@aws-sdk/client-s3";
2
3 const client = new S3Client({});
4
5 /**
6 * @param {Object} params
7 */
8 export const putObject = async (bucketName, key, body) => {
9     const params = {
10         Bucket: bucketName,
11         Key: key,
12         Body: body,
13     };
14     return client.send(new PutObjectCommand(params));

```

C#

In this example, Amazon Q fills in JSDoc parameters based on existing constants.

```
6     /// <summary>
7     /// Shows how to create a new Amazon S3 bucket.
8     /// </summary>
9     public static async Task<bool> CreateBucketAsync(IAmazonS3 client, string bucketName)
10    {
11        try
12        {
13            var request = new PutBucketRequest
14            {
15                BucketName = bucketName,
16                UseClientRegion = true,
17            };
18
19            var response = await client.PutBucketAsync(request);
20            return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
21        }
22        catch (AmazonS3Exception ex)
```

Java

The following example is adapted from [an example on the Oracle website](#).

In the image below, the user has entered a docstring. Amazon Q has suggested a function to complete the docstring.

A screenshot of a Java IDE interface. The title bar says "demo - HelloResource.java". The file path in the title bar is "demo > src > main > java > com > example > demo > Main". The current file is "HelloResource.java". The code shown is:

```
1 package com.example.demo;
2
3 public class Main {
4     /**
5      * @param url an absolute URL giving the base location of the resource
6      * @param name the location of the resource
7      * @return the resource at the specified location
8      * @see IMAGE
9     */
10    public static String getResource(String url, String name) {
```

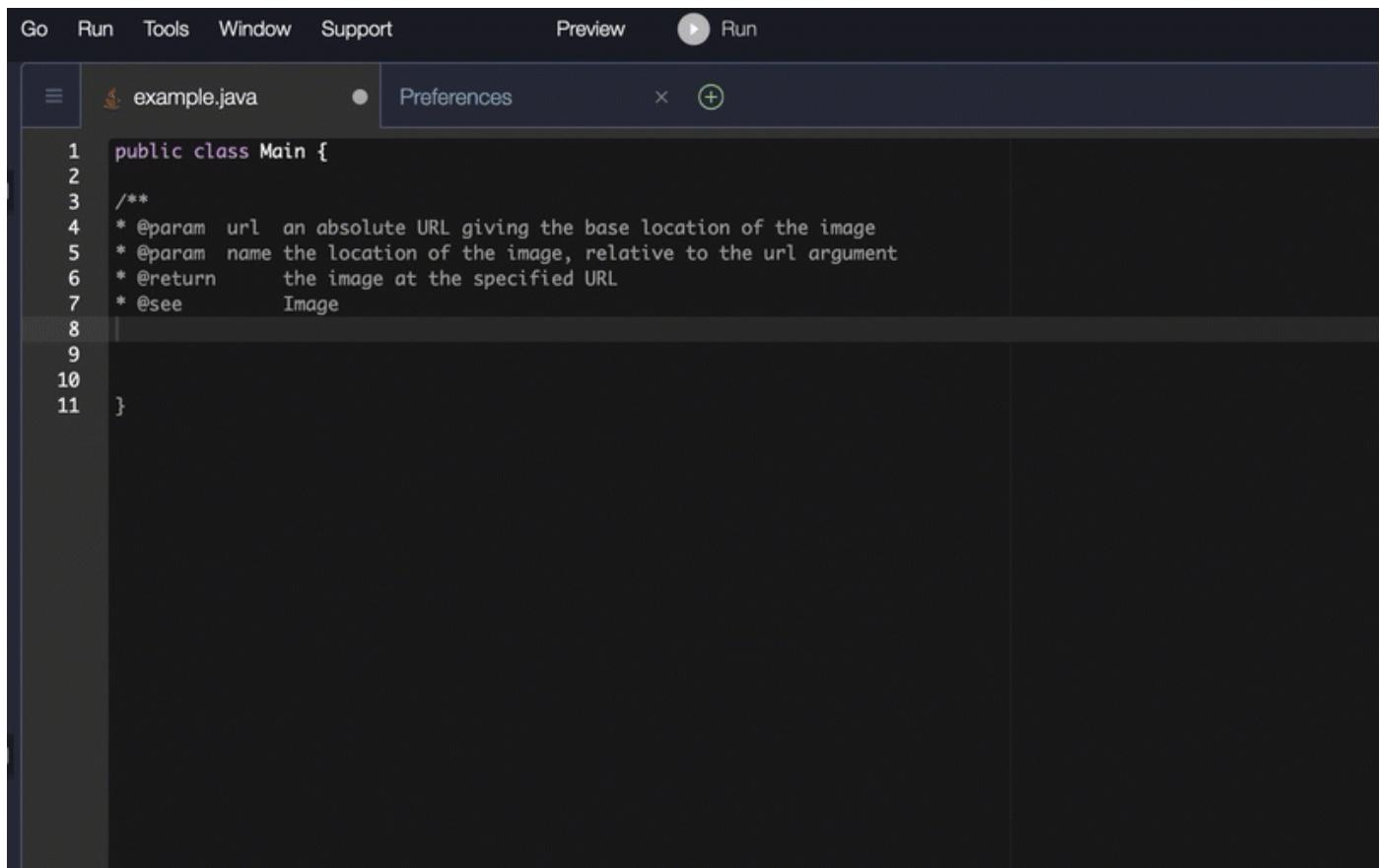
Below the code, there is a suggestion box from "CodeWhisperer" with the following options:

- Insert Code
- Previous
- Next

The message "Suggestion 1 of 2 from CodeWhisperer" is displayed.

The following example is adapted from [an example on the Oracle website](#).

In the example below, in Java, the user enters a docstring. Amazon Q suggests a function to process the docstring.

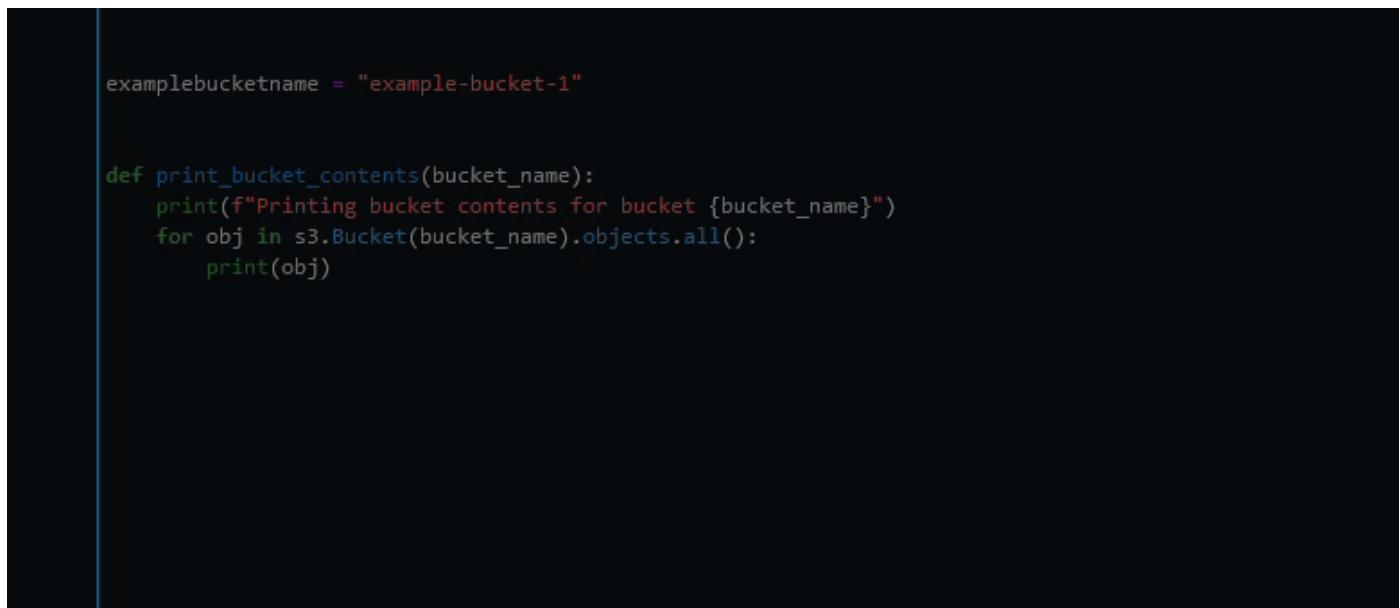


The screenshot shows the Amazon Q developer interface with a dark-themed code editor. At the top, there's a navigation bar with 'Go', 'Run', 'Tools', 'Window', and 'Support' buttons. To the right of the navigation bar are 'Preview' and 'Run' buttons. Below the navigation bar, the title bar displays 'example.java' and 'Preferences'. The main area is a code editor with the following Java code:

```
1 public class Main {  
2  
3     /**  
4      * @param url an absolute URL giving the base location of the image  
5      * @param name the location of the image, relative to the url argument  
6      * @return the image at the specified URL  
7      * @see Image  
8  
9  
10 }  
11 }
```

Python

In this example, Amazon Q recommends a Docstring, based on the surrounding context.



The screenshot shows the Amazon Q developer interface with a dark-themed code editor. The code editor contains the following Python script:

```
examplebucketname = "example-bucket-1"  
  
def print_bucket_contents(bucket_name):  
    print(f"Printing bucket contents for bucket {bucket_name}")  
    for obj in s3.Bucket(bucket_name).objects.all():  
        print(obj)
```

Using Amazon Q Developer for line-by-line recommendations

Depending on your use case, Amazon Q may not be able to generate an entire function block in one recommendation. However, Amazon Q can still provide line-by-line recommendations.

Go and GoLand

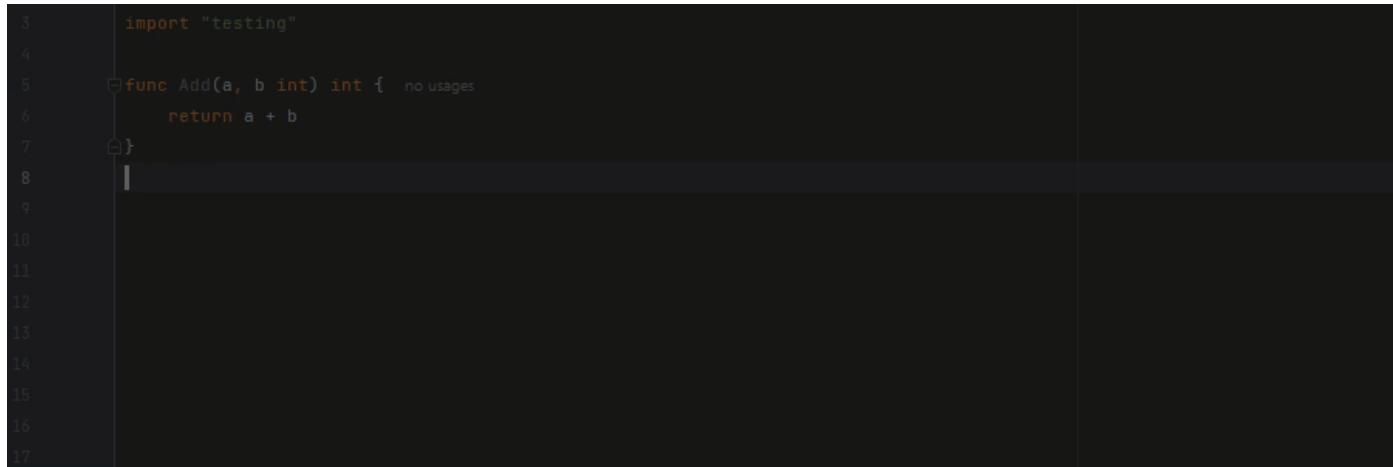
In this example, Amazon Q provides line-by-line recommendations.



The screenshot shows a Go code editor window. Line 15 contains the code: `s3Client := s3.NewFromConfig(cfg)`. A yellow lightbulb icon is positioned above the cursor, indicating a code completion or recommendation is available. The code editor has a dark theme with syntax highlighting for Go keywords and comments.

```
10 func ListBuckets() { no usages
11     var err error
12     cfg, err := config.LoadDefaultConfig(context.TODO())
13     if err != nil {
14         panic("configuration error, " + err.Error())
15     }
16     s3Client := s3.NewFromConfig(cfg)
17 }
```

Here is another example of line-by-line recommendations, this time with a unit test.



The screenshot shows a C++ code editor window. Line 6 contains the code: `return a + b`. A vertical bar with a small arrow at the top is positioned to the left of the cursor, indicating a code completion suggestion is being displayed. The code editor has a dark theme with syntax highlighting for C++ keywords and comments.

```
3 import "testing"
4
5 func Add(a, b int) int { no usages
6     return a + b
7 }
8
9
10
11
12
13
14
15
16
17
```

C++ and CLion

In this example, Amazon Q provides line-by-line recommendations.

```
34  
35     bool CreateBucket(const Aws::String &bucketName,  
36                           const Aws::Client::ClientConfiguration &clientConfig) {  
37         |  
38     }  
39  
40  
41  
42  
43  
44  
45  
46
```

Python

In the following image, the customer has written an initial comment indicating that they want to publish a message to an Amazon CloudWatch Logs group. Given this context, Amazon Q is only able to suggest the client initialization code in its first recommendation, as shown in the following image.

```
# Publish a message to a CloudWatch Logs Group
```

```
client = boto3.client('logs')
```

However, if the user continues to request line-by-line recommendations, Amazon Q also continues to suggest lines of code based on what's already been written.

```
# Publish a message to a CloudWatch Logs Group  
client = boto3.client('logs')  
response = client.put_log_events(  
    |
```

```
        logGroupName='VPCFlowLogs',
```

Note

In the example above, VPCFlowLogs may not be the correct constant value. As Amazon Q makes suggestions, remember to rename any constants as required.

Amazon Q can eventually complete the entire code block as shown in the following image.

```
# Publish a message to a CloudWatch Logs Group
client = boto3.client('logs')
response = client.put_log_events(
    logGroupName='VPCFlowLogs',
    logStreamName='VPCFlowLogs',
    logEvents=[
        {
            'timestamp': int(round(time.time() * 1000)),
            'message': json.dumps(event)
        }
    ]
)
```

No recommendations

In this example, Amazon Q provides recommendations, one line at a time.

```
role = get_execution_role()

sagemaker_session = sage.Session()
bucket = sagemaker_session.default_bucket()
runtime = boto3.client("runtime.sagemaker")
s3 = boto3.resource("s3")
```

Upgrading language versions with the Amazon Q Developer Agent for code transformation

The Amazon Q Developer Agent for code transformation can upgrade the code language version of your files in place. You can transform a module in JetBrains and a project or entire workspace in Visual Studio Code.

Amazon Q first builds your code in the source language version and verifies that it has the information necessary to transform your code. After Amazon Q successfully transforms your code, you verify and accept the changes in your integrated development environment (IDE). For more information, see [How the Amazon Q Developer Agent for code transformation works](#).

Currently, Amazon Q can upgrade Java 8 and Java 11 code to Java 17 code.

Topics

- [Step 1: Prerequisites](#)
- [Step 2: Configure your project](#)
- [Step 3: Transform your code](#)
- [How the Amazon Q Developer Agent for code transformation works](#)
- [Troubleshooting issues with the Amazon Q Developer Agent for code transformation](#)

Step 1: Prerequisites

Before you continue, make sure you've completed the steps in [Set up Amazon Q in your IDE](#).

Make sure that the following prerequisites are met before you begin a Code Transformation job:

- Your project is a Java 8 or Java 11 project built on Maven.
- Your project successfully builds with Maven in your IDE. Amazon Q Developer Agent for code transformation supports Maven 2.8, but we recommend Maven 3.9.5 or later.
- Your project source JDK is available locally and is the version of your source code. For example, if you are transforming Java 8 code, your local JDK installation should be JDK 8.
- Your project builds in 55 minutes or less.
- Your project is configured correctly, and the correct JDK version is specified. For more information, see [Step 2: Configure your project](#).
- Your project doesn't require access to resources on your private network, including a virtual private cloud (VPC) or on-premise network. For example, if your project contains unit tests that connect to a database in your network, the transformation will fail.
- Your project doesn't use plugins that package languages other than Java in your Java project. For example, if your project uses the [frontend-maven-plugin](#) for executing front-end JavaScript code in addition to your Java source code, the transformation will fail.
- Your project doesn't use pom.xml file dependency version ranges. For example, if your pom.xml file includes <version>[1.0.0,)</version>, the transformation will fail. For more information, see [Version Range Specification](#) in the Apache Maven Project documentation.
- Your local network allows uploads to Amazon S3 buckets that Amazon Q uses to transform your code. For more information, see [Allow access to Amazon S3 buckets in data perimeters](#).
- Your minimum compiler version for the maven-compiler-plugin is v13.13.0.

Step 2: Configure your project

To configure your project, use the following information for the IDE you're using.

Configure a project in JetBrains

To configure your project in JetBrains, you might need to specify the following Project Structure settings:

- Project SDK – The JDK used to compile your project. This must be specified in order to build your project.
- Project language level – The Java language used in your project. This must be specified if the Java version used in your project is different from your JDK version.
- Module language level – The Java language used in your module. This must be specified if the Java version used in your modules is different from your project or JDK version.

You might need to adjust these settings if you are using an unsupported JDK, but your project or modules use a supported language version. For example, if you're transforming a Java 8 project, but you're using JDK 18, you must set your project language level to Java 8.

Additionally, if your project contains multiple modules that use different language versions, you must set the language level for the module you're transforming.

Update project settings

To update your project SDK, project language, or module language settings, complete the following steps:

1. From your JetBrains IDE, choose **File** and then **Project Structure**.
2. The Project Structure window opens. Under **Project Settings**, choose **Project**.
 - a. To update your JDK, choose from the dropdown menu next to **SDK**.
 - b. To update your project language, choose from the dropdown next to **Language level**.
3. Under **Project Settings**, choose **Modules**.
 - To update your module language, choose from the dropdown next to **Language level**.

For more information, see [Project structure settings](#) and [Module structure settings](#) in the JetBrains documentation.

Configure a project in VS Code

To configure your project in VS Code, your project must contain the following:

- A pom.xml file in the project root folder
- A .java file in the project directory

If your project contains a Maven wrapper executable (mvnw for macOS or mvnw.cmd for Windows), make sure it's at the root of your project. Amazon Q will use the wrapper, and no other Maven configuration is necessary.

If you aren't using a Maven wrapper, install Maven. For more information, see [Installing Apache Maven](#) in the Apache Maven documentation.

After installing Maven, add it to your PATH variable. For more information, see [How do I add Maven to my PATH?](#) Your Java runtime variable should also be pointing to a JDK and not to a JRE. To confirm your configuration is correct, run mvn -v. The output should show your Maven version and the runtime variable pointing to the path to your JDK.

Step 3: Transform your code

Before you transform your own code, you might want to test that your IDE is setup correctly by transforming a sample project. Following is a sample GitHub project that is eligible for code transformation: <https://github.com/aws-samples/aws-appconfig-java-sample>.

To test your IDE setup, download and unzip the sample project, and complete the following steps for your IDE. If you are able to view the proposed changes and transformation summary, you are ready to transform your own code project. If the transformation fails, your IDE is not configured correctly. To address configuration issues, review [Step 2: Configure your project](#) and [Troubleshooting](#).

Note

If you navigate away from your IDE before the transformation starts, the transformation will fail and you will have to restart.

To upgrade the language version of your code project or module, complete the following steps for your IDE.

JetBrains

1. Open the module that you want to upgrade in JetBrains. Make sure you've successfully built your project in the IDE.
2. Choose the Amazon Q logo, and then enter **/transform** in the Amazon Q chat panel that opens.
3. A **Transform your application** pop-up appears. Choose the project that you want to upgrade from the dropdown menu, and then choose **Transform**.
4. Amazon Q begins the transformation. You can view progress on the **Transformation details** tab.
5. After the transformation is complete, you can verify the upgraded code before updating your project. To view the new code, go to the **Transformation details** tab and then choose **View diff**. In the **Apply patch** window that appears, choose a file to open a diff view with your source code and upgraded code.
6. To accept the changes that Amazon Q made, choose **View diff** to open the **Apply patch** window. Select all the updated files, and choose **OK** to update your project in place.
7. To get details about how your code was upgraded and suggested next steps, on the **Transformation details** tab, choose **View transformation summary**.

Visual Studio Code

1. Open the project or workspace that you want to upgrade in VS Code. Make sure that you've successfully built your project in the IDE.
2. Choose the Amazon Q logo, and then enter **/transform** in the Amazon Q chat panel that opens.
3. Choose the project that you want to upgrade from the search bar at the top of the IDE.
4. If Amazon Q can't find the version of your source code, it prompts you to choose your code version. Choose the version that your source code is written in, and then choose **Transform** in the pop-up to proceed.
5. If prompted, enter the JAVA_HOME path to your JDK. For more information, see [Configure your VS Code project](#).

6. Amazon Q begins the transformation. You can view progress on the **Transformation Hub** tab.
7. After the transformation is complete, the **Proposed Changes** tab opens. To verify the upgraded code before updating your project, choose **Download proposed changes**. Choose a file to open a diff view with your source code and upgraded code.
8. To accept the changes Amazon Q made, go to the **Proposed Changes** tab and choose **Accept**.
9. To get details about how your code was upgraded and suggested next steps, on the **Transformation Hub**, choose the **Views and More Actions** ellipsis button, and then choose **Show Transformation Summary**.

How the Amazon Q Developer Agent for code transformation works

To transform your code, the Amazon Q Developer Agent for code transformation generates a transformation plan that it uses to upgrade the code language version of your project. After transforming your code, it provides a transformation summary and a file diff for you to review changes before accepting them. The following sections provide more details on how Amazon Q performs the transformation.

Building your code and creating a transformation plan

To begin transforming your code, Amazon Q builds your project locally and generates a build artifact that contains your source code, project dependencies, and build logs. This build artifact must be under 1 GB for Amazon Q to transform your code.

After generating the build artifact, Amazon Q builds your code in a secure build environment and creates a transformation plan, which is customized to the project or module you're upgrading. The transformation plan outlines the specific changes Amazon Q will attempt to make, including new dependency versions, major code changes, and suggested replacements for deprecated code. These changes are based on the preliminary build of your code, and might change during the transformation.

Transforming your code

To transform your code, Amazon Q attempts to upgrade your code based on the proposed changes in the transformation plan. As it makes changes, it re-builds and runs existing unit tests in your source code to iteratively fix any encountered errors.

Amazon Q attempts to make the following changes when upgrading your code:

- Upgrade popular libraries and frameworks to a version compatible with Java 17. This includes updating Spring, Spring Boot, Junit, JakartaEE, Mockito, Hibernate, and Log4j to their latest available major versions.
- Update deprecated code components according to Java 17 recommendations

Reviewing the transformation summary and accepting changes

After the transformation is complete, Amazon Q provides a transformation summary with details about the changes it made, including the status of the final build which indicates whether your entire project was upgraded. You can also view a build log summary to understand any issues that prevented Amazon Q from building your code in the upgraded version.

The transformation summary additionally includes the differences between the changes proposed in the transformation plan and the changes Amazon Q ultimately made to upgrade your code, and any additional changes that weren't in the original plan.

After you review the transformation summary, you can view the changes Amazon Q is proposing in a file diff view. Any code changes Amazon Q suggests will not affect your current project files until you accept the changes. The transformed code is available up to 24 hours after the transformation completes.

Troubleshooting issues with the Amazon Q Developer Agent for code transformation

The following information can help you troubleshoot common issues with the Amazon Q Developer Agent for code transformation.

Topics

- [Why can't Amazon Q upload my project?](#)
- [Why are my Maven commands failing?](#)
- [How do I add Maven to my PATH?](#)
- [Why did my transformation fail after 55 minutes?](#)
- [Why can't I download my transformed code?](#)
- [How do I access code transformation logs?](#)
- [How do I find my transformation job ID?](#)

Why can't Amazon Q upload my project?

If your project fails to upload, it's likely due to one of the following issues. See the topic that corresponds to the error you see from Amazon Q.

Topics

- [Reduce project size](#)
- [Configure proxy settings in your IDE](#)
- [Allow access to Amazon S3](#)

Reduce project size

To transform your code, Amazon Q generates a project artifact, which includes your source code, project dependencies, and build logs. The maximum project artifact size for a transformation job is 2 GB. If you get an error related to project artifact size, you must decrease the size of your project or try transforming a smaller project. You can view the size of your project artifact file in the code transformation logs. For more information, see [How do I access code transformation logs?](#)

Configure proxy settings in your IDE

To transform your code, Amazon Q uploads your project artifact to a service-owned Amazon S3 bucket. Part of the upload process involves using SSL or TLS certificates to establish communication between Amazon S3 and your IDE. If you are using a proxy server, the SSL or TLS certificates used by your proxy server must be trusted, otherwise Amazon Q is not able to upload your project.

If you receive an error related to your proxy or certificates, you likely need to configure your IDE or operating system to trust your certificates or update other proxy settings.

Note

You might also encounter issues unrelated to certificates if you are behind your organization's proxy server or firewall. If you complete the following procedures to configure your certificates and still have issues, contact your network administrator to ensure you are allowed to communicate with Amazon S3 from your IDE. For more information, see [Allow access to Amazon S3](#).

Configure certificates in JetBrains

To configure your JetBrains IDE Java Runtime Environment (JRE) to trust the SSL or TLS certificates used by your proxy server, you must import the SSL or TLS certificates to the `cacerts` file in the JRE. The `cacerts` file is a file that contains trusted root certificates for secure connections such as HTTPS and SSL, and it's part of the JRE's security settings. To import a certificate, complete the following procedure.

Note

We recommend making a backup of the `cacerts` file before modifying it, as any mistakes can cause issues with secure connections.

1. Determine the path to the `cacerts` file in your JRE. The path of the `cacerts` file in the internal JRE shipped with your JetBrains IDE depends on the operating system and the version of the JetBrains IDE you're using.

Following are examples of paths to the `cacerts` file in common operating systems. Choose your operating system to see examples.

Note

`<JetBrains Installation Folder>` refers to the directory where JetBrains products are installed. This directory is typically chosen during the installation process. The `jbr` folder represents the JRE bundled with JetBrains IDEs, which is a specific version of the JRE tailored for use with JetBrains IDEs.

Windows

The `cacerts` file path for a JetBrains IDE installed on Windows is:

```
<JetBrains Installation Folder>\jbr\bin\cacerts
```

For example, if you installed a JetBrains IDE on Windows in the default location, the path might be:

```
C:\Program Files\JetBrains\jbr\bin\cacerts
```

macOS

The cacerts file path for a JetBrains IDE installed on macOS is:

```
/Applications/JetBrains Toolbox/<version>/JetBrains Toolbox.app/Contents/jbr/  
Contents/Home/lib/security/cacerts
```

For example, if you installed a JetBrains IDE on macOS in the default location, the path might be:

```
/Applications/JetBrains Toolbox/2022.3.4/JetBrains Toolbox.app/Contents/jbr/  
Contents/Home/lib/security/cacerts
```

Linux

The cacerts file path for a JetBrains IDE installed on Linux is:

```
/opt/jetbrains/jbr/lib/security/cacerts
```

2. Determine the certificate you need to import to the cacerts file. The certificate file typically has a .cer, .crt, or .der file extension. If you aren't sure which certificates you need to add, contact your network administrator.
3. Import the certificate to the cacerts keystore. You can do this with the Java keytool command.
 - a. Open a command prompt and enter the following command:

```
keytool -import -alias <alias> -file <certificate_file> -keystore  
<path_to_cacerts>
```

- b. For <alias>, you can add a name for the certificate you are importing to refer to it later. This option is optional.
- c. For <certificate_file>, specify the path to the certificate you are importing. This should be a path to the .cer, .crt, or .der file containing the certificate.
- d. For <path_to_cacerts>, specify the path to the cacerts keystore file you saved in step 1. This is the file where you are importing the certificate.

For example, if you want to import a certificate named `my_certificate.cer` into the `cacerts` keystore of the bundled JRE in IntelliJ IDEA on Windows, and you want to give the alias `myalias` to the certificate, the command might be:

```
keytool -import -alias myalias -file my_certificate.cer -keystore "C:\Program Files \JetBrains\IntelliJ IDEA 2022.3.2\jbr\bin\cacerts"
```

4. During the import process, you'll be prompted to enter the keystore password. The default password for the `cacerts` keystore is `changeit`.
5. After running the command, you'll be asked to trust the certificate. To confirm the certificate is trusted and complete the import, enter `yes`.
6. You might also need to add the certificates to the IDE itself, in addition to the JRE. For more information, see [Server Certificates](#) in the JetBrains documentation.

Configure certificates in Visual Studio Code

Note

The following information only pertains to troubleshooting proxy issues with Visual Studio Code on macOS.

To configure Visual Studio Code to trust the SSL or TLS certificates used by your proxy server, make sure you have configured the following proxy settings.

Add certificates to your keychain

If you haven't already, you must add the certificates used by your proxy server to your macOS keychain. For information on adding certificates to your keychain, see [Add certificates to a keychain using Keychain Access on Mac](#) in the Keychain Access User Guide.

Install the Mac CA VSCode extension

The [Mac CA VSCode extension](#) allows Amazon Q to access the certificates you added to Keychain Access on your Mac.

To install the extension:

1. Search for mac-ca-vscode in the VS Code extensions pane, and choose **Install**.
2. Restart VS Code.

Update proxy settings in VS Code

Update the following settings to make sure VS Code is configured properly for your proxy.

1. Open settings in VS Code.
2. Enter proxy in the search bar.
3. In the **Http: Proxy** field, add your proxy URL.
4. Deselect **Http: Proxy Strict SSL**.
5. In the **Http: Proxy Support** dropdown menu, choose **on**.
6. In the settings search bar, enter `http.experimental.systemCertificatesV2`. Select **Http > Experimental: System Certificates V2**.

Allow access to Amazon S3

During a transformation, the Amazon Q Developer Agent for code transformation uploads your code to a service-owned Amazon S3 bucket. If your network or organization hasn't configured access to Amazon S3, Amazon Q isn't able to upload your project.

To ensure Amazon Q can upload your project, make sure your proxy configuration and other network components, such as Data Loss Prevention (DLP) policies, are configured to allow access to Amazon S3. You might also need to allowlist the Amazon S3 bucket where Amazon Q uploads your project. For more information, see [Data perimeters for Amazon Q resources](#).

If you transform a large project, DLP policies or other network components might cause delays and prevent a successful upload if they aren't configured to allowlist the Amazon S3 bucket. If you choose not to allowlist the bucket, you might need to transform a smaller project so that Amazon Q can upload it.

Why are my Maven commands failing?

Following are Maven configuration issues that you might see in the JetBrains and Visual Studio Code IDEs. If you address the issues and still see Maven errors, there might be an issue with your project. Use the information in the error logs to address any issues with your project, and then try transforming your project again.

Update Maven configuration in JetBrains

If a transformation fails in JetBrains due to Maven command issues, the error logs appear on the **Run** tab. Use the information in the logs to address the issue. Following are some issues that you might need to address:

- Make sure that your Maven home path is set to **Bundled**. Go to **Settings**, and then expand the **Build, Execution, Deployment** section. Expand the **Build Tools** section and then expand **Maven**. In the **Maven home path** dropdown menu, choose **Bundled**.
- Make sure that the Java runtime environment (JRE) is using your project JDK. Go to **Settings**, and then expand the **Build, Execution, Deployment** section. Expand **Maven** and choose **Runner**. In the **JRE** dropdown menu, choose **Use Project JDK**.
- Make sure that Maven is enabled. Go to **Settings** and choose **Plugins**. Search for Maven and choose the Maven plugin. If you see an **Enable** button, choose it to enable Maven.

Update Maven configuration in Visual Studio Code

If a transformation fails in VS Code because of Maven command issues, a text file that contains the error logs opens in a new tab. Use the information in the logs to address the issue.

Make sure that you have configured either one of the following options:

- Your project contains a Maven wrapper in the project root folder
- A version of Maven supported by Amazon Q is available on your PATH

For more information, see [How do I add Maven to my PATH?](#)

How do I add Maven to my PATH?

To transform your code in VS Code without using a Maven wrapper, you must install Maven and add it to your PATH variable.

To check if you have Maven installed correctly already, run `mvn -v` in a new OS terminal outside of Visual Studio Code. You should see an output with your Maven version.

If you get an output in your Visual Studio Code terminal but not in your OS terminal, or if the command isn't found, you need to add Maven to your PATH.

To add Maven to your PATH, follow the instructions for your machine.

macOS

To add Maven to your macOS PATH, complete the following steps.

1. Locate your Maven installation directory, or the folder where you installed Maven, and save the path to that folder.
2. Open the configuration file for your shell in an editor of your choice. For recent macOS versions, the default shell is zsh and the default configuration file is located at `~/.zshrc`.

Add the following lines to the bottom of the configuration file. Set the value of `M2_HOME` to the path you saved in step 1:

```
export M2_HOME="your Maven installation directory"
export PATH = "${M2_HOME}/bin:${PATH}"
```

These commands make the `mvn` command available in all terminals.

3. Close all OS terminal windows and quit all Visual Studio Code instances.
4. To verify that Maven was added to your PATH, open a new OS terminal and run the following command:

```
mvn -v
```

You should see an output with your Maven version.

5. After seeing your Maven output, restart Visual Studio Code. You might also need to restart your machine. Open a new Visual Studio Code terminal and run the following command:

```
mvn -v
```

The output should be identical to the output in step 4. If the Visual Studio Code output is different, try the following to make sure your setup is correct:

- Check your PATH variable in Visual Studio Code. An IDE extension might be altering the PATH such that it differs from your local PATH variable. Uninstall the extension to remove it from your PATH.
- Check your default shell in Visual Studio Code. If it's set to something other than zsh, repeat these steps for your shell.

Windows

To add Maven to your Windows PATH, complete the following steps:

1. Locate your Maven installation directory, or the folder where you installed Maven, and save the path to that folder.
2. Open the Environment Variables window:
 - a. Choose the Windows button to open the search bar.
 - b. Enter **Edit environment variables for your account** and choose it.
3. In the **Environment Variables** window, look for the Path variable. If you have a Path variable already, choose **Edit...** to update it. If you don't see a Path variable, choose **New...** to add one.
4. In the **Edit environment variable** window that appears, double click the existing path to edit it, or choose **New** to add a new path entry.

Replace the existing Maven path entry with the path you saved in step 1, or add the path as a new entry. At the end of the path, add \bin as a suffix, as in the following example:

```
C:\Users\yourusername\Downloads\apache-maven-3.9.6-bin\apache-maven-3.9.6\bin
```

5. Choose **OK** to save the path entry, and then choose **OK** again in the **Environment Variables** window.
6. Open a new Command Prompt and run the following command:

```
mvn -v
```

You should see an output with your Maven version.

Why did my transformation fail after 55 minutes?

If your code transformation job fails after 55 minutes, your code build time likely exceeds the build time limit. There is currently a time limit of 55 minutes for building your code.

If your local build time takes 55 minutes or longer, reduce your project's build time to transform your code. If your local build is faster than the build with Code Transformation, check your project for tasks that might be failing or take a longer time in a different environment. Consider disabling

long-running test cases. Also consider using timeouts for attempts to access resources that might not be available from the secure IDE environment or the internet.

Why can't I download my transformed code?

If you aren't able to download your code after your transformation is complete, it's likely due to one of the following issues. See the topic that corresponds to the error you see from Amazon Q.

Topics

- [Reduce project size](#)
- [Download code diff within 24 hours](#)
- [Configure proxy settings in your IDE](#)
- [Remove wildcard characters in JetBrains proxy settings](#)

Reduce project size

After the transformation is complete, Amazon Q generates an output artifact that contains a diff with your upgraded code and a transformation summary with information about the changes it made. The output artifact must be 1 GB or less in order for the IDE to download it.

If the output artifact exceeds the limit, you will not be able to download your upgraded code or transformation summary. Try transforming a smaller project to prevent a large output artifact. If the issue persists, contact AWS Support. For information about contacting AWS Support with Amazon Q, see [Using Amazon Q Developer to chat with AWS Support](#).

Download code diff within 24 hours

The code diff file with your upgraded code is only available for 24 hours after the transformation is complete. If it's been over 24 hours since the transformation completed, restart the transformation to download the diff file.

Configure proxy settings in your IDE

The Amazon Q Developer Agent for code transformation downloads your upgraded code from a service-owned Amazon S3 bucket. Part of the download process involves using SSL or TLS certificates to establish communication between Amazon S3 and your IDE. If you are using a proxy server, the SSL or TLS certificates used by your proxy server must be trusted, otherwise Amazon Q is not able to upload your project.

To download your code, you might need to configure your IDE to trust certificates or update other proxy settings. For more information on updating your proxy settings, see [Configure proxy settings in your IDE](#).

Remove wildcard characters in JetBrains proxy settings

If you have configured proxy settings in your JetBrains IDE, you might see the following error when downloading your upgraded code:

```
software.amazon.awssdk.core.exception.SdkClientException:  
Unable to execute HTTP request: Dangling meta character '*' near index 0
```

This is likely caused by the presence of a wildcard character (*) in the **No proxy for** field of your IDE's proxy settings. The Java SDK used by the Amazon Q Developer Agent for code transformation doesn't support wildcard entries in this field.

To download your code, remove any wildcards from the **No proxy for** field, and then restart your IDE. If you need to specify hosts that should bypass the proxy, use a regular expression instead of a wildcard. To update proxy settings in your JetBrains IDE, see [HTTP Proxy](#) in the JetBrains documentation.

How do I access code transformation logs?

Access logs in JetBrains

For information about how to access JetBrains log files, see [Locating IDE log files](#) in the JetBrains documentation.

To find logs emitted by the Amazon Q Developer Agent for code transformation in JetBrains, search the IDE logs for the following string:

```
software.aws.toolkits.jetbrains.services.codemodernizer
```

Code transformation logs start with the preceding string. Logs generated by Maven are displayed on the **Run** tab and have the preceding string before and after the log entry.

Access logs in Visual Studio Code

To find logs emitted by the Amazon Q Developer Agent for code transformation in VS Code, complete the following steps:

1. Choose **View** in the top navigation bar, and then choose **Command Palette**.
2. Search Amazon Q: View Logs in the command palette that appears.
3. The logs open in the IDE. To search the log files for CodeTransformation, use CMD + F or Control + F.

Code transformation logs in VS Code are prefixed with CodeTransformation:. Following is an example of a log generated in VS Code for a Maven copy dependencies error:

```
2024-02-12 11:29:16 [ERROR]: CodeTransformation: Error in running Maven copy-dependencies command mvn = /bin/sh: mvn: command not found
```

How do I find my transformation job ID?

Find your job ID in JetBrains

To find a transformation job ID in JetBrains, go to the **Transformation details** tab in the **Transformation Hub** and choose the **Show Job Status** (clock) icon.

Find your job ID in Visual Studio Code

To find a transformation job ID in VS Code, go to the **Transformation Hub** and choose the **Show Job Status** (clock) icon.

Developing software with the Amazon Q Developer Agent for software development

The Amazon Q Developer Agent for software development can help you develop code features or make code changes to projects in your integrated development environment (IDE). You explain the feature you want to develop, and Amazon Q uses the context of your current project to generate an implementation plan and the accompanying code to implement the feature. Amazon Q can help you build AWS projects or your own applications.

You can start an entirely new project, or work on an open project in your IDE. When you develop in an existing project, Amazon Q uses all relevant files in your workspace root as context to develop a plan and generate code. Amazon Q filters out files or folders defined in a .gitignore file, and only uses supported file types to generate code. For a list of supported file types, see the following GitHub links for your IDE:

- Supported file types for JetBrains IDEs – <https://github.com/aws/aws-toolkit-jetbrains/blob/main/plugins/core/jetbrains-community/src/software/aws/toolkits/jetbrains/services/amazonq/QConstants.kt>
- Supported file types for Visual Studio Code – <https://github.com/aws/aws-toolkit-vscode/blob/master/packages/core/src/shared/filetypes.ts>

To get started, open up a new or existing project and enter **/dev** in the Amazon Q chat panel. A new chat tab opens where you interact with Amazon Q to generate an implementation plan and new code for your feature.

Topics

- [Develop features with /dev](#)
- [Best practices](#)
- [Example tasks](#)
- [Quotas](#)
- [Troubleshooting issues with the Amazon Q Developer Agent for software development](#)

Develop features with **/dev**

To develop a feature in your IDE, complete the following steps.

1. In your IDE, open a new or existing project or workspace where you want to develop features.
2. Choose the Amazon Q extension, and then choose **Open Chat Panel**. Enter **/dev** in the Amazon Q chat panel that opens. You can also type your feature description directly after **/dev**.
3. A new tab opens. Enter a description of the feature that you want to develop or the issue that you want to resolve. You can provide a brief overview of a task, or add more details. Amazon Q uses your description and the code in your project to come up with an implementation plan.

Following is an example of a code change you can ask Amazon Q to implement:

Create a new REST API endpoint /api/authenticate to handle user authentication. This endpoint should accept POST requests with user credentials and return a JWT token upon successful authentication. Additionally, update the user management system to integrate with the

new authentication endpoint and enforce authentication for relevant API endpoints.

4. Amazon Q responds with an implementation plan, including the code updates that it would make to complete the task you described.
5. Review the implementation plan that Amazon Q generates. If you want to change anything about the plan, enter modifications or more details to clarify what you want to achieve.
6. When you're satisfied with the implementation plan, choose **Generate code**. Amazon Q generates new code and proposes updates to your files based on the implementation plan. This might take a few minutes.
7. After Amazon Q has generated the code for your feature, it provides a list of files with proposed changes. Choose a file to view a file diff with the changes.
8. To accept the changes and update your file, choose **Accept**. To reject the changes to the file, choose **Reject**.

If you aren't satisfied with the proposed changes, you can provide feedback in the chat panel on what can be improved. Amazon Q generates new code based on your feedback. When the generated code meets your requirements, choose **Accept** to update the code in your workspace.

9. To develop another feature with Amazon Q in the same chat tab, choose **Discuss a new plan** and repeat these steps. Your previous conversation and implementation plan aren't used as context for the new plan.

Best practices

To make the most out of the Amazon Q Developer Agent for software development, follow these best practices:

- Provide a detailed description of the new feature or code changes you want to make, including the specifics of what the code should achieve. This allows Amazon Q to create a comprehensive implementation plan and code changes that can be implemented. For examples, see [Example tasks](#).
- Your feature shouldn't require updates to more than 5 files at a time. Asking Amazon Q to make larger changes might impact the quality and manageability of the implementation of your feature. If your file diff includes changes to many files, try reducing the scope of your feature description.

Example tasks

Following are example feature development tasks you can ask the Amazon Q Developer Agent for software development to perform, with the corresponding description you might provide.

- **Update CSS Styles for Responsive Layout:** Enhance the responsiveness of the application's layout by updating CSS styles. Focus on adjusting the layout for different screen sizes, ensuring optimal display across various devices.
- **Fix User Profile Image Upload:** Resolve the issue preventing users from uploading profile images. Investigate the file upload process, ensure proper file type validation, and address any server-side errors preventing successful uploads.
- **Refactor Code for Code Readability:** Improve the readability of a specific code module by refactoring it. Break down complex functions into smaller, more manageable units, and apply meaningful variable and function names for better clarity.
- **Implement Input Validation for Contact Form:** Add client-side and server-side input validation to the contact form to prevent submission of empty or invalid data. Display appropriate error messages to users for any validation failures.
- **Resolve Broken Links in Navigation Menu:** Investigate and fix broken links in the navigation menu of the application. Update the URLs or routes to ensure all navigation links lead to the correct pages.
- **Optimize Image Loading for Faster Page Loads:** Optimize image loading on key pages of the application to reduce page load times. Implement lazy loading or asynchronous loading techniques to prioritize the display of visible content.
- **Add Error Logging for Critical API Endpoints:** Enhance error handling by implementing logging for critical API endpoints. Log relevant error details such as request parameters and stack traces to facilitate debugging and troubleshooting.
- **Update Documentation for API Endpoints:** Review and update the documentation for existing API endpoints to reflect recent changes or additions. Ensure accuracy and completeness of information for developers consuming the API.
- **Refactor Database Queries for Efficiency:** Analyze and optimize database queries to improve efficiency and reduce resource consumption. Identify and eliminate redundant queries, optimize indexing, and consider caching strategies where applicable.

Quotas

The Amazon Q Developer Agent for software development maintains the following quotas:

- **Implementation plans per task** – The number of implementation plans the Amazon Q Developer Agent for software development can create for a given development task, including the initial plan.
- **Code generations per task** – The number of times the Amazon Q Developer Agent for software development can generate code for a given development task, including the initial code generation.
- **Code project size** – The maximum size of the code file or folder that the Amazon Q Developer Agent for software development can use as context to generate new code.

Amazon Q Developer Agent for software development Quotas

Resource	Quota
Implementation plans per task	10
Code generations per task	3
Code project size	200 MB uncompressed
	50 MB compressed

Troubleshooting issues with the Amazon Q Developer Agent for software development

The following information can help you troubleshoot common issues with the Amazon Q Developer Agent for software development.

How do I find my conversation ID?

You might need your conversation ID to get support for issues with the Amazon Q Developer Agent for software development. For some error messages, the conversation ID appears in the message from Amazon Q. If you don't see it, use the following steps to find the conversation ID in your IDE.

Visual Studio Code

1. Open the Command Palette, and run the following command:

Amazon Q: View Logs.

2. An output console opens in the VS Code terminal. Search for the following string:

Amazon Q Developer Agent for software development Conversation ID:

The conversation ID is listed after the colon. Confirm that the timestamp corresponds to the conversation that you need the ID for.

JetBrains

1. At the top of the IDE, choose **Help**, and then **Show Log in Finder**.

Depending on your JetBrains IDE and operating system, the logs menu text might look different. For more information, see [Locating IDE log files](#) in the IntelliJ IDEA documentation.

2. Your file finder opens. Choose **idea.log** to open the log file.
3. Search for the following string:

Amazon Q Developer Agent for software development Conversation ID:

The conversation ID is listed after the colon. Confirm that the timestamp corresponds to the conversation that you need the ID for.

Scanning your code with Amazon Q

Amazon Q can scan your codebase for security vulnerabilities and code quality issues to improve the posture of your applications throughout the development cycle. You can initiate a scan of an entire codebase, analyzing all files in your local project or workspace, or enable auto scans that assess your code as you write it.

When Amazon Q discovers a potential security vulnerability or quality issue in your code, it generates a finding with a description of the issue and a recommended fix. Some findings include an automatic fix, which updates your code files in-place.

Scans are powered by [security detectors](#) that are informed by years of AWS and Amazon.com security best practices. As security policies are updated and detectors are added, scans automatically incorporate new detectors to ensure your code is compliant with the most up-to-date policies.

Topics

- [Types of scans](#)
- [Quotas](#)
- [Starting a scan](#)
- [Addressing findings](#)

Types of scans

Amazon Q performs code security and code quality analysis in every scan. The following sections explain the types of security and quality issues Amazon Q detects.

Code security scanning

Amazon Q detects security policy violations and vulnerabilities in your code with static application security testing (SAST), secrets detection, and infrastructure as code (IaC) scanning. For a complete list of the detectors Amazon Q uses to scan your code, see the [Detector Library](#).

- **SAST scanning — Detect security vulnerabilities in your source code.** Amazon Q identifies various security issues, such as resource leaks, SQL injection, and cross-site scripting.
- **Secrets scanning — Prevent the exposure of sensitive or confidential information in your codebase.** Amazon Q scans your code and text files for secrets such as hardcoded passwords, database connection strings, and usernames. Secrets findings include information about the unprotected secret and how to protect it.
- **IaC scanning — Evaluate the security posture of your infrastructure files.** Amazon Q can scan your infrastructure as code (IaC) code files to detect misconfiguration, compliance, and security issues.

Code quality scanning

Amazon Q detects quality and maintainability issues in your code to ensure your codebase is meeting quality and efficiency best practices. Amazon Q generates findings related to various

quality issues, including but not limited to performance, machine learning rules, and AWS best practices.

Quotas

Amazon Q security scans maintain the following quotas:

- **Input artifact size** – The size of all the files within an IDE project workspace, including third-party libraries, build JAR files, and temporary files.
- **Source code size** – The size of the source code that Amazon Q scans after filtering all third-party libraries and unsupported files.

The following table describes the quotas maintained for auto scans and full project scans.

Resource	Auto scans	Project scans
Maximum input artifact size	200 KB	500 MB
Maximum source code size	200 KB	50 MB

Starting a scan

Amazon Q can scan your entire codebase, or auto-scan your code as you write it.

Topics

- [Scan as you code](#)
- [Scan your project](#)

Scan as you code

Note

The following steps assume that you have already [installed the Amazon Q plugin in your IDE](#), and that you have [subscribed to Amazon Q Developer Pro](#).

Amazon Q auto-scans are only available with a Amazon Q Developer Pro subscription in JetBrains and Visual Studio Code.

Amazon Q automatically scans the file you are actively coding in, generating findings as soon as they are detected in your code. Auto-scans are enabled by default when you use Amazon Q.

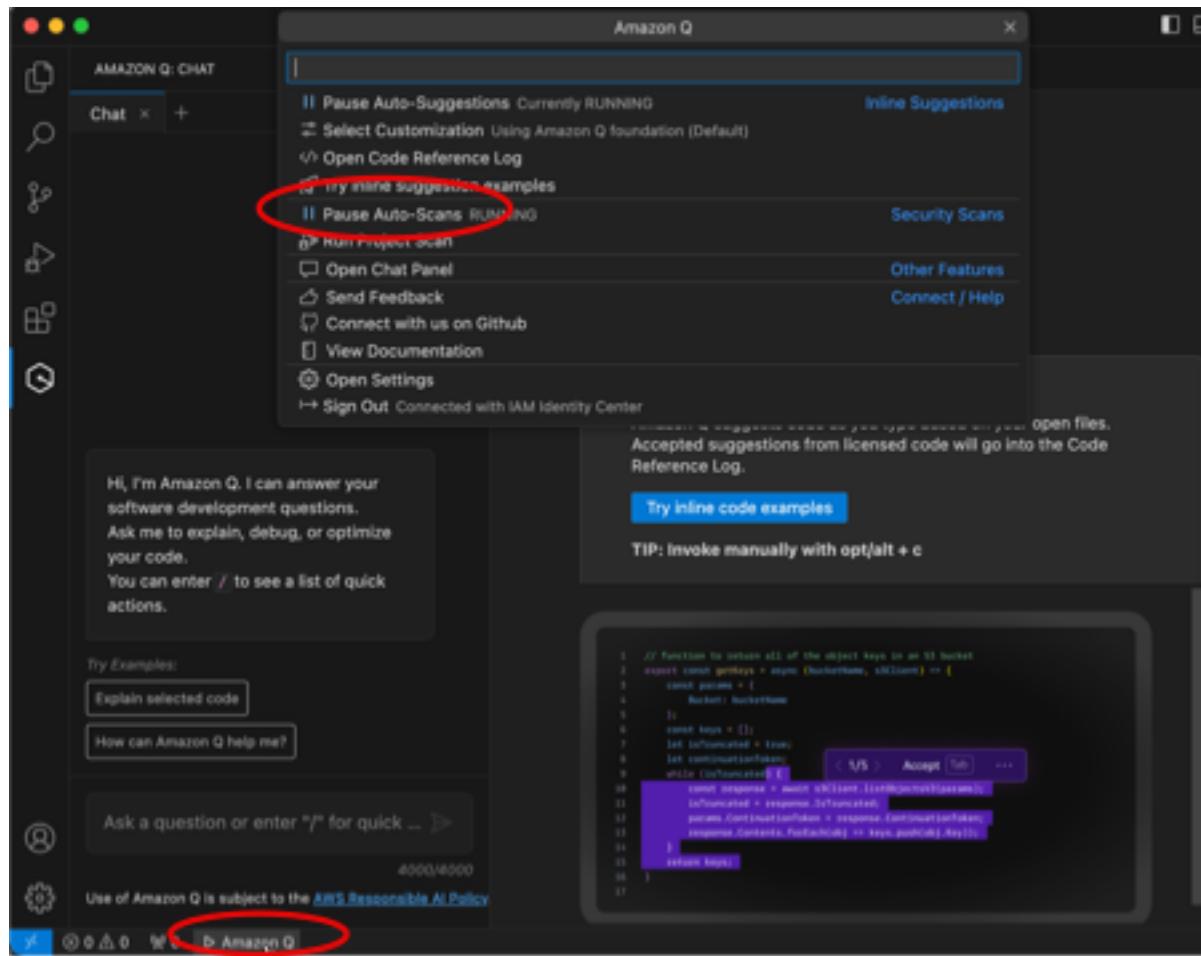
Pausing auto-scans

To pause auto scans, complete the following steps.

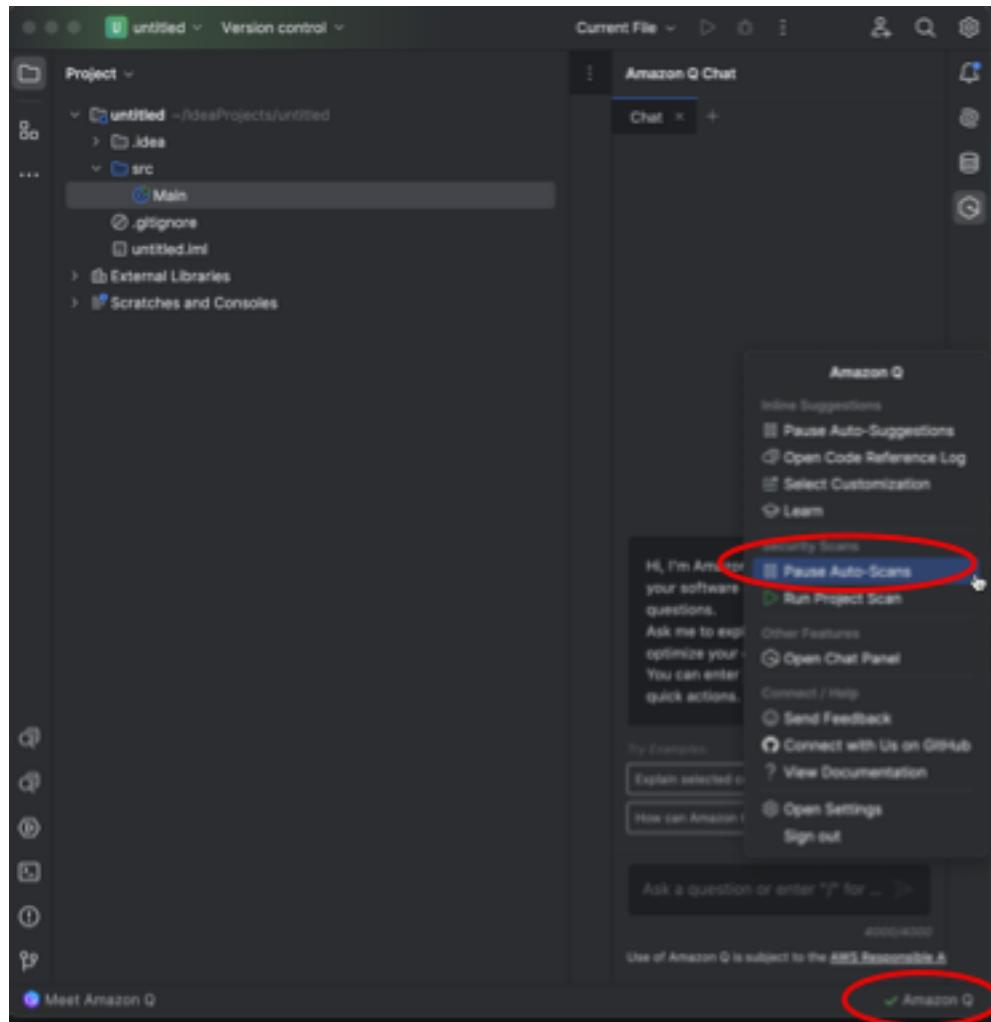
1. Choose the text, **Amazon Q**, from the rectangular area at the bottom of the IDE window. In VS Code, this area is called the *component tray*. In JetBrains IDEs, this area is called the *status bar*.

After you choose the Amazon Q text the Amazon Q task bar opens at the top of the IDE window.

In the following image, in Visual Studio Code, the user chooses the text **Amazon Q** at the bottom of the interface, prompting a drop-down window from which the user may choose **Pause Auto-Scans**.



In the following image, in IntelliJ (a JetBrains IDE), the user chooses the text **Amazon Q** at the bottom of the interface, prompting a drop-down window from which the user may choose **Pause Auto-Scans**.



2. Choose **Pause Auto-Scans**.

Scan your project

You can scan a project to evaluate the security posture of your entire codebase at once.

To manually run a scan, complete the following steps for your IDE.

JetBrains

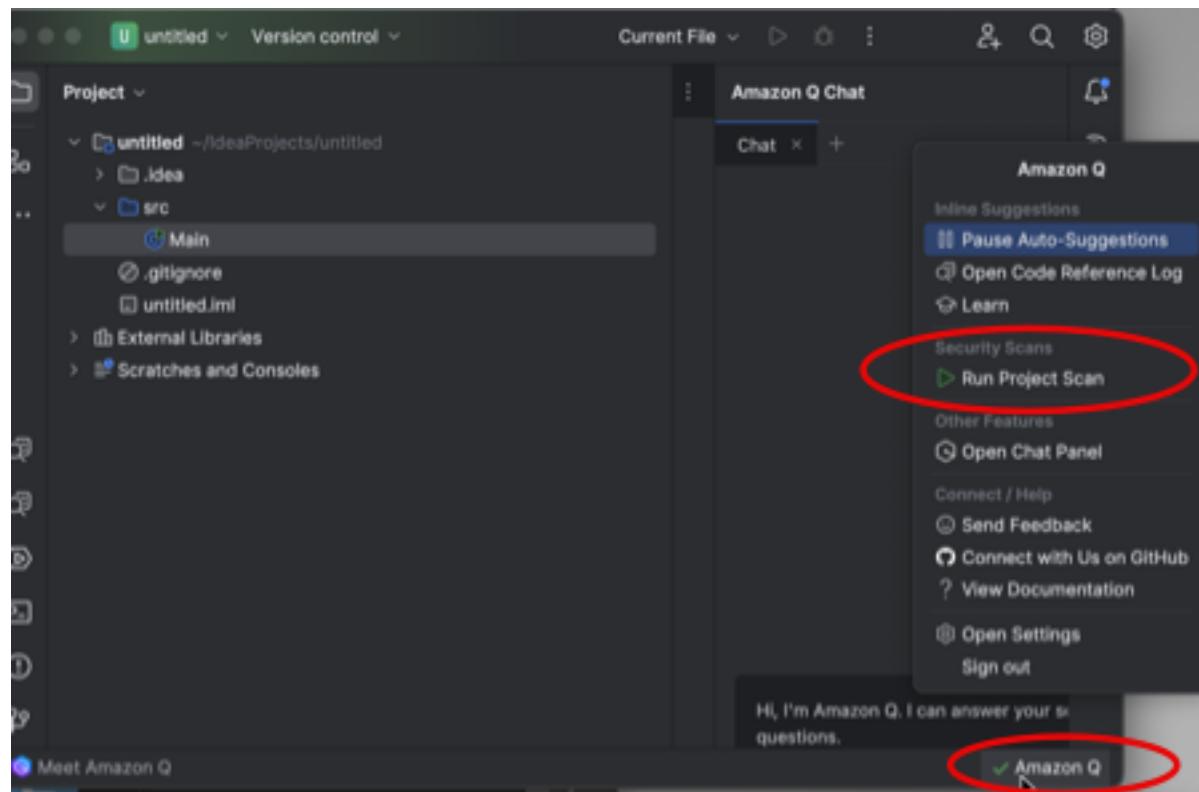
To scan a project in a JetBrains IDE:

1. Open up a file from the project you want to scan in your JetBrains IDE.
2. Choose **Amazon Q** from the status bar at the bottom of the IDE window.

The Amazon Q task bar opens on the right of the IDE window.

3. Choose **Run Project Scan** from the task bar. Amazon Q begins scanning your project.

In the following image, in IntelliJ (a JetBrains IDE), the user chooses **Amazon Q** from the status bar, prompting a task bar from which the user may choose **Run Project Scan**.



4. When the scan is complete, the findings Amazon Q generated appear in the **Problems** tab. You can choose individual findings to be redirected to the specific area of the file where the vulnerability or low-quality code was detected.
5. Hover your cursor over the underlined code to view details about the finding. For information about addressing findings, see [Addressing findings](#).

Visual Studio Code

To scan a project in a VS Code:

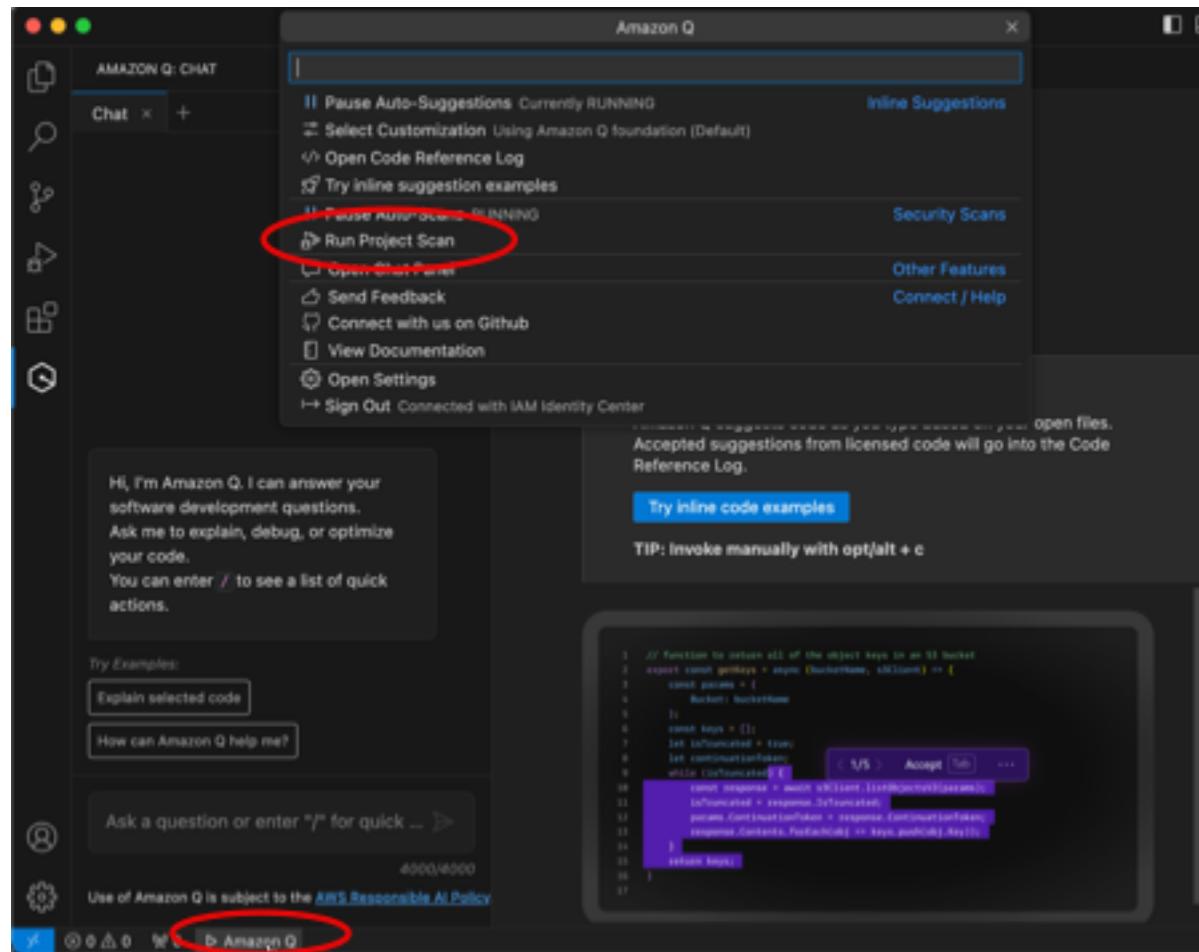
1. Open up a file from the project you want to scan in VS Code.

2. Choose **Amazon Q** from the component tray at the bottom of the IDE window.

The Amazon Q task bar opens at the top of the IDE window.

3. Choose **Run Project Scan**. Amazon Q begins scanning your project.

In the following image, in VS Code, the user chooses **Amazon Q** from the component tray, prompting a task bar from which the user may choose **Run Project Scan**.



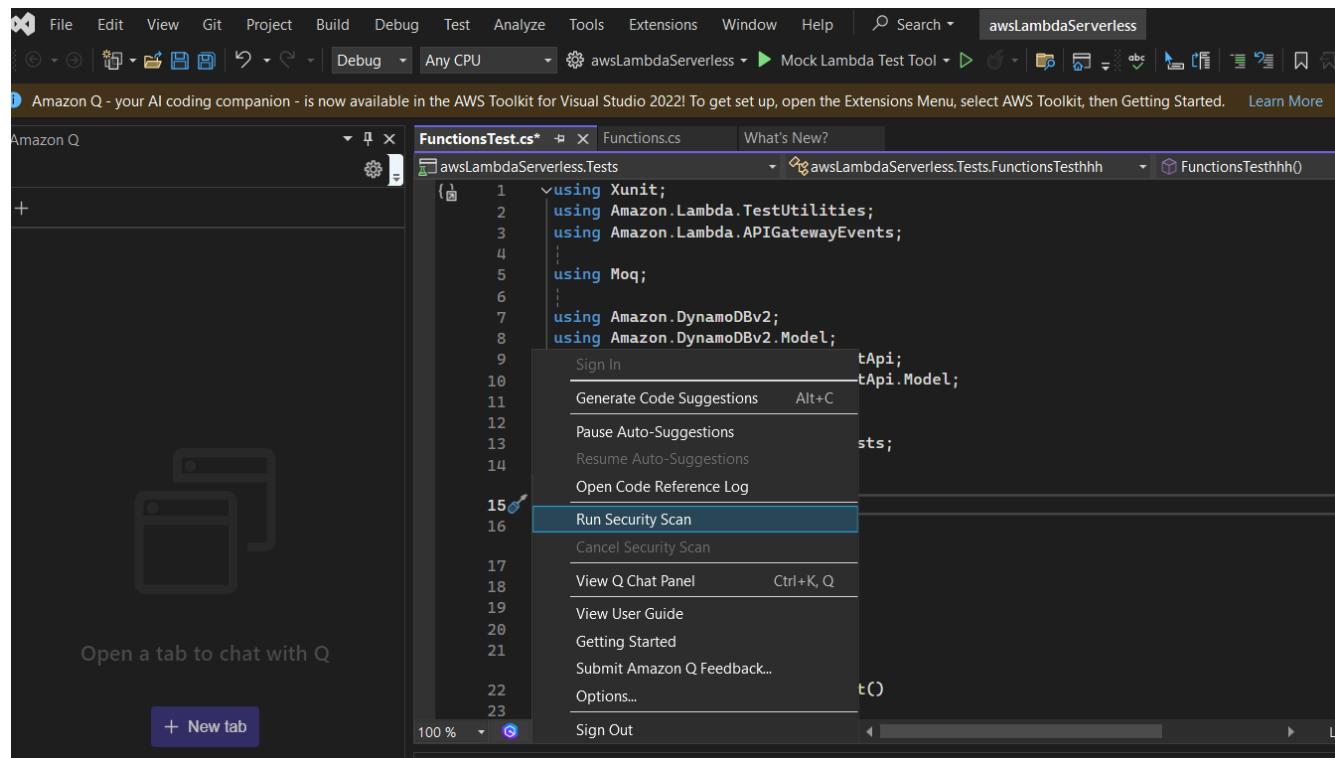
4. When the scan is complete, the findings Amazon Q generated appear in the **Problems** tab. You can choose individual findings to be redirected to the specific area of the file where the vulnerability or low-quality code was detected.
5. Hover your cursor over the underlined code to view details about the finding. For information about addressing findings, see [Addressing findings](#).

Visual Studio

To scan a project in a Visual Studio:

1. Open up a file from the project you want to scan in Visual Studio.
2. Choose the Amazon Q icon at the bottom of your file to open the Amazon Q task bar.
3. From the task bar, choose **Run Security Scan**. Amazon Q begins scanning your project.

In the following image, in Visual Studio, the user chooses the **Amazon Q** icon, prompting a task bar from which the user may choose **Run Security Scan**.



4. The status of your scan is updated in the Visual Studio output pane. You're notified when the scan is complete.

For information about viewing and addressing findings, see [Addressing findings](#).

Addressing findings

When Amazon Q generates a finding, it underlines the vulnerable or low-quality code. Findings include details about the security or quality issue and how to address it in your code.

Topics

- [Address findings in JetBrains and Visual Studio Code](#)
- [Address findings in Visual Studio](#)

Address findings in JetBrains and Visual Studio Code

You can view a list of detected findings in the **Problems** tab. Choose a finding to be redirected to the specific area of the file where the vulnerability or low-quality code was detected. To see a pop-up with information about the finding, hover your cursor over the underlined code.

From the pop-up, you have a few options to address a finding:

- **Automatic fix** — This option appears for some vulnerabilities. Choose **Fix** to update your code in-place and address the finding.
- **Explain with Q** — Amazon Q explains the finding and recommends how to fix it. In the pop-up, choose **Explain** to send the finding and associated code to the Amazon Q chat panel.
- **Learn more about the finding** — The finding describes how you can approach remediating the vulnerability. Use this information to replace the code with improved code.

Address findings in Visual Studio

To view findings in Visual Studio, open the Visual Studio **Error List** by expanding the **View** heading in the Visual Studio main menu and choosing **Error List**.

You can use the information in the finding to update your code. After updating your code, scan your code again to see if the findings were addressed.

By default, the Visual Studio **Error List** displays all of the warnings and errors for your code base. To filter your Amazon Q findings from the Visual Studio **Error List**, create a filter by completing the following procedure.

Note

Scan findings are only visible after you've run a security scan in which Amazon Q detected issues.

Findings appear as warnings in Visual Studio. In order to view findings from your **Error List**, the **Warnings** option in the **Error List** heading must be selected.

Filter findings in the Error List

1. From the Visual Studio main menu, choose **view** and then **Error List** to open the **Error List** pane.

2. From the **Error List** pane, right-click the header row to open the context menu.
3. From the context menu, expand **Show Columns**, and then select **Tool** in the expanded menu.
4. The **Tool** column is added to your **Error List**.
5. From the **Tool** column header, select the **Filter** icon and choose **Amazon Q** to filter for Amazon Q security scan findings.

Supported languages for Amazon Q Developer in the IDE

Amazon Q Developer provides support for a wide range of programming languages across its various features and capabilities. This page outlines the languages and versions supported for inline code suggestions, code transformation, security scans, and automatic code fixes.

Language support for inline suggestions

Amazon Q supports inline code suggestions for multiple programming languages. The accuracy and quality of the code generation for a programming language depends on the size and quality of the training data.

In terms of the quality of the training data, the programming languages with the most support are:

- Java
- Python
- JavaScript
- TypeScript
- C#
- Go
- PHP
- Rust
- Kotlin
- SQL
- C++
- C

The Infrastructure as Code (IaC) languages with the most support are:

- JSON (AWS CloudFormation)
- YAML (AWS CloudFormation)
- HCL (Terraform)
- CDK (TypeScript, Python)

Amazon Q also supports code generation for:

- Ruby
- Shell
- Scala

Language support for Code Transformation

The Amazon Q Developer Agent for code transformation supports upgrading code from Java 8 or Java 11 to Java 17.

Language support for security scans

Amazon Q security scans supports the following language versions:

- **Java** - Java 17 and earlier
- **JavaScript** - ECMAScript 2021 and earlier
- **Python** - Python 3.11 and earlier, within the Python 3 series
- **C#** - All versions (.NET 6.0 and later recommended)
- **TypeScript** - All versions
- **Ruby** - Ruby 2.7 and 3.2
- **Go** - Go 1.18
- **C** - C11 and earlier
- **C++** - C++17 and earlier
- **PHP** - PHP 8.2 and earlier
- **Kotlin** - Kotlin 2.0.0 and earlier
- **Scala** - Scala 3.2.2 and earlier
- **JSX** - React 17 and earlier

- **Infrastructure as Code (IaC) languages**
 - **AWS CloudFormation** - 2010-09-09
 - **Terraform** - 1.6.2 and earlier
 - **AWS CDK** - TypeScript and Python

Automatic code fixes are available for scans in the following languages and versions:

- **Java** - Java 17 and earlier
- **JavaScript** - ECMAScript 2021 and earlier
- **Python** - Python 3.11 and earlier, within the Python 3 series
- **C#** - All versions (.NET 6.0 and later recommended)
- **TypeScript** - All versions
- **Infrastructure as Code (IaC) languages**
 - **AWS CloudFormation** - 2010-09-09
 - **Terraform** - 1.6.2 and earlier
 - **AWS CDK** - TypeScript and Python

Using Amazon Q Developer on the command line

This chapter explains how you can use Amazon Q Developer to enable IDE-style completions for hundreds of popular CLIs like git, npm, docker, and aws. Start typing, and Amazon Q populates contextually relevant subcommands, options and arguments.

Topics

- [Installing Amazon Q for command line](#)
- [Chatting with Amazon Q in the CLI](#)
- [Generating CLI completions](#)
- [Amazon Q inline on the command line](#)
- [Translating from natural language to bash](#)
- [Debugging Amazon Q Developer for the command line](#)
- [Contributing completion specs to Amazon Q Developer](#)

Installing Amazon Q for command line

To install Amazon Q for command line, complete the following steps.

1. [Download Amazon Q for command line \(macOS only\)](#)
2. Authenticate with [Builder ID](#), or with [IAM Identity Center](#) using the start URL given to you by your account administrator.
3. Follow the instructions to install the shell integrations, and to grant macOS accessibility permissions.

The screenshot shows the 'Automated checks' section with two items: 'Shell integrations' (green checkmark) and 'Enable accessibility' (red X). A red oval highlights the 'Enable accessibility' item. Below this, the 'Still having issues?' section lists steps to run 'q doctor' and 'q issue'. It also provides a link to the 'User manual'.

Getting started

Help & support

Features

CLI Completions

Chat

Translate

Inline

Settings

Keybindings

Integrations

Preferences

Automated checks

Shell integrations ✓

Enable accessibility ✗

Still having issues?

- Run `q doctor` to automatically debug
- Run `q issue` to create an auto-populated issue

You can also check out the following:
[User manual →](#)

Supported command line environments

Amazon Q for command line integrates with the following environments:

- Operating systems: macOS
- Shells: bash, zsh, fish
- Terminal emulators: iTerm2, macOS terminal, Hyper, Alacritty, Kitty, wezTerm
- IDEs: VS Code terminal, Jetbrains terminals (except Fleet)
- CLIs: 500+ of the most popular CLIs such as git, aws, docker, npm, yarn

Verifying your download

After you download Amazon Q for command line, you can verify its code signature as follows:

```
codesign -v /Applications/Amazon\ Q.app
```

If there is no output, then the app's code signature is valid, and it has not been tampered with since it was signed.

For more verbose information about the app signature, run:

```
codesign -dv --verbose=4 /Applications/Amazon\ Q.app
```

To learn more about the macOS codesign utility, see the [Code Signing Guide](#) on the Apple developer website.

Uninstalling Amazon Q for command line

To uninstall Amazon Q for command line, complete the following steps.

1. Open a terminal window.
2. Run the following command:

```
q uninstall
```

Chatting with Amazon Q in the CLI

The Amazon Q CLI is a command-line interface that allows you to interact with the Amazon Q. With the Amazon Q CLI, you can engage in natural language conversations, ask questions, and receive responses from Amazon Q, all within your terminal environment.

Context integration

One of the powerful features of the Amazon Q CLI is its ability to integrate contextual information from your local development environment. By using context modifiers, you can provide the Amazon Q with relevant context, such as your git repository status, local shell environment variables, and shell command history. This context integration enhances the AI model's understanding of your specific use case, enabling it to provide more relevant and context-aware responses.

Context modifiers

The Amazon Q CLI supports the following context modifiers:

- **@git:** This modifier allows you to pass information about your git repository status, including the current branch, staged and unstaged changes, and commit history.

- **@env:** By using this modifier, you can provide the Amazon Q with your local shell environment variables, which can be useful for understanding your development setup and configuration.
- **@history:** The **@history** modifier allows you to share your recent shell command history with Amazon Q, giving it insights into the actions you've taken and the context in which you're working.

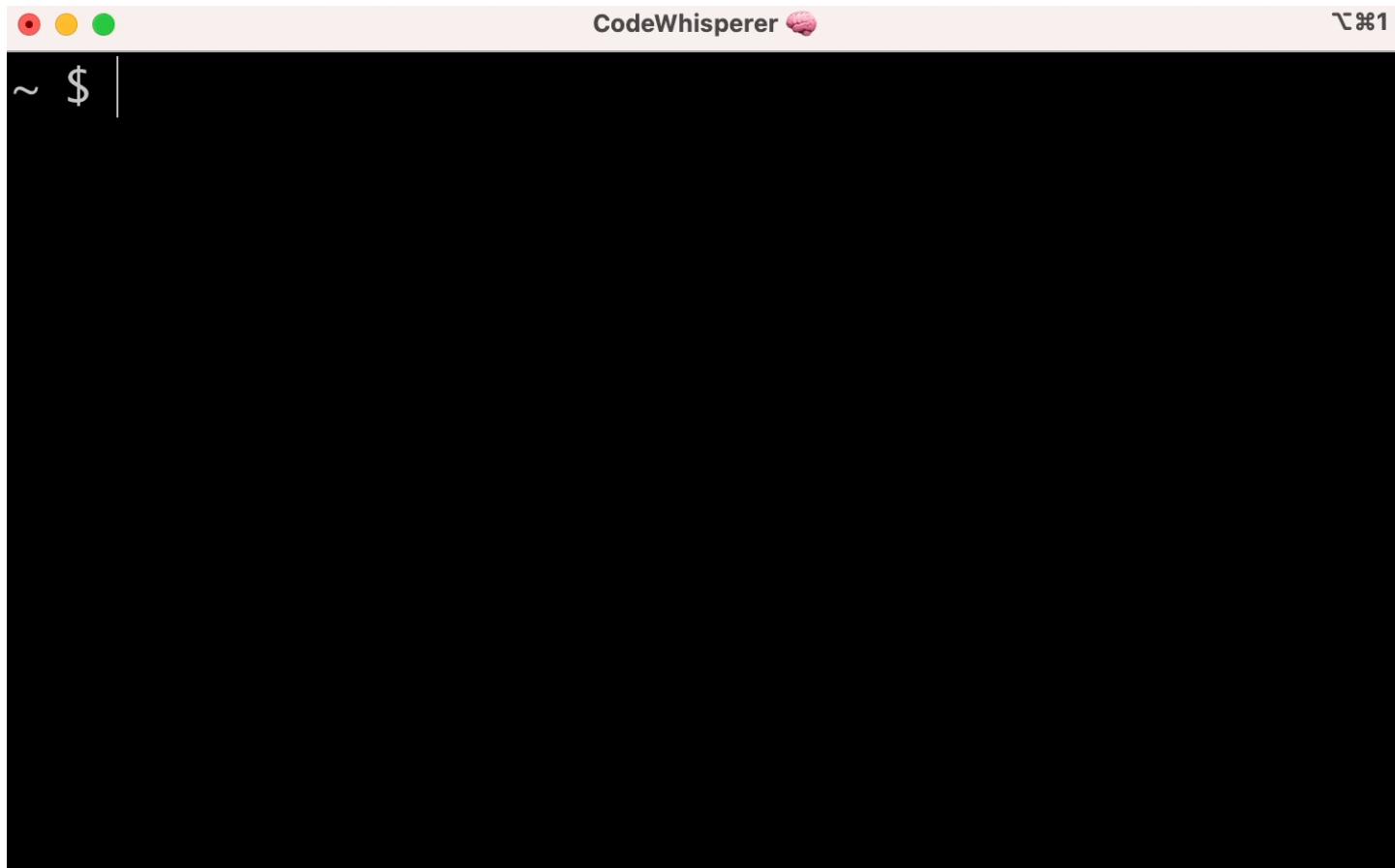
Usage

To start using the Amazon Q CLI, follow these steps:

1. [Install the Amazon Q CLI.](#)
2. Open your terminal or command prompt.
3. Run the `q chat` command to initiate a conversation with Q.
4. Optionally, include any context modifiers (for example, `@git`, `@env`, `@history`) in your input to provide additional context to the model.
5. Type your query or input, and press **Enter**.
6. The Amazon Q will process your input, considering any provided context, and respond with its output.
7. Continue the conversation by providing additional input or asking follow-up questions.

Generating CLI completions

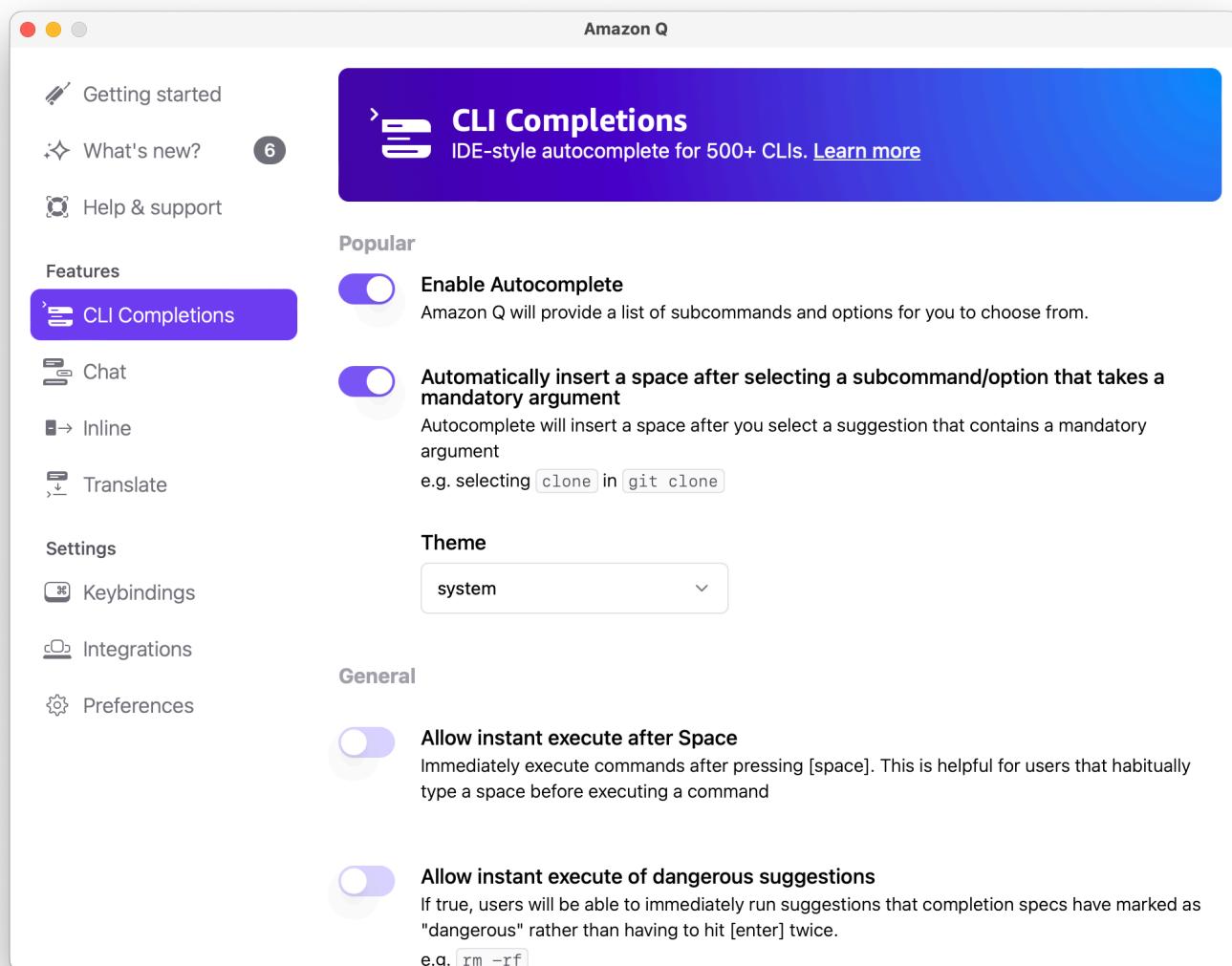
You can use Amazon Q Developer to add IDE-style completions to hundreds of popular CLIs like `git`, `npm`, `docker`, and `aws`. Start typing, and Amazon Q will pop up contextually relevant subcommands, options and arguments.



Popular settings

The default settings provided by Amazon Q for command line may not "feel right," and may disrupt your existing workflow. You can customize your settings at any time by running `q` to open the settings dashboard. Here are a few popular settings:

- Keybindings – Changing the tab keybinding to "Insert common prefix or navigate" may make CLI Completions feel more like traditional shell completions while "Insert common prefix or insert" will feel more like an IDE.
- Theme – You know what this is. Choose your favorite.
- Instant execute after space – A lot developers habitually type a space character just before they execute it. Enable this setting to avoid Amazon Q blocking you.
- First token completion – Enable this setting to get completions for CLIs themselves, not just the subcommands, options, and arguments.



Using CLI Autocomplete on a remote machine with SSH

When you install Amazon Q for the command line locally, it adds autocomplete for over 500 CLI tools to your existing terminal in your local environment. By enabling SSH integration, you can make CLI autocomplete accessible on remote machines as well.

Local macOS Integration

To enable SSH integration enable the local SSH integrations by running the following command:

```
q integrations install ssh
```

Remote Linux Integration

Install and update requirements

- You must be able to extract or "unzip" the downloaded package. If your operating system doesn't have the built-in unzip command, use an equivalent.
- The Amazon Q CLI uses glibc 2.34 or newer. It is included by default in most major distributions of Linux released since 2021.
- We support the Amazon Q CLI on 64-bit versions of recent distributions of Fedora, Ubuntu, and Amazon Linux 2023.
- Because AWS doesn't maintain third-party repositories, we can't guarantee that they contain the latest version of the Q CLI.

Install the Amazon Q CLI

1. Download the installation file in one of the following ways:

Linux x86-64

```
curl --proto '=https' --tlsv1.2 -sSF "https://desktop-release.codewhisperer.us-east-1.amazonaws.com/latest/q-x86_64-linux.zip" -o "q.zip"
```

Linux ARM (aarch64)

```
curl --proto '=https' --tlsv1.2 -sSF "https://desktop-release.codewhisperer.us-east-1.amazonaws.com/latest/q-aarch64-linux.zip" -o "q.zip"
```

2. (Optional) Verifying the integrity of your downloaded zip file

If you chose to manually download the Amazon Q CLI installer package .zip in the above steps, you can use the following steps to verify the signatures by using the GnuPG tool.

The Amazon Q CLI installer package .zip files are cryptographically signed using PGP signatures. If there is any damage or alteration of the files, this verification fails and you should not proceed with installation.

- a. Download and install the gpg command using your package manager. For more information about GnuPG, see the GnuPG website.

- b. To create the public key file, create a text file and paste in the following text.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----  
  
mDMEZig60RYJKwYBBAHaRw8BAQdAy/+G05U5/E0A72W1cD4WkYn5SInri8pc4Z6D  
BKNNNG0m0JEfTYXpvbiBRIENMSSBUZWFTIDxxLWNsaUBhbWF6b24uY29tPoiZBBMW  
CgBBFiEEmvYEF+gnQskUPgPsUNx6jcJMVmcFAmYo0tECGwMFCQPCZwAFCwkIBwIC  
IgIGFQoJCAAsCBYCAwECHgcCF4AACgkQUNx6jcJMVmf5QD/QWWEGG/c0nbDnp68  
SJXuFkwiNwlH2rPw9ZRIQMnfAS0A/0V6ZsGB4k0y1Bfc7CNfzRGtovdBBgHqA6P  
zQ/PNscGuDgEZig60RIKKwYBBAGXVQEFAQEHQC4qle0NMBCq3+wJwbZSr0vbuRba  
D1xr4wUPn4Avn4AnAwEIB4h+BBgWCGAmFiEEmvYEF+gnQskUPgPsUNx6jcJMVmcF  
AmYo0tECGwwFCQPCZwAACgkQUNx6jcJMVmcFchMgEA6l3RveCM0YHAGQaSFMkguoAo  
vK6Fg0kDawgP0NPIP2oA/jIA04gsAntuQgM0sPunEdDeji2t+AhV02+DQIsXZpoB  
=f8yY  
-----END PGP PUBLIC KEY BLOCK-----
```

- c. Import the Amazon Q CLI public key with the following command, substituting public-key-file-name with the file name of the public key you created.

```
gpg --import public-key-file-name  
gpg: directory '/home/username/.gnupg' created  
gpg: keybox '/home/username/.gnupg/pubring.kbx' created  
gpg: /home/username/.gnupg/trustdb.gpg: trustdb created  
gpg: key 50DC7A8DC24C5667: public key "Amazon Q CLI Team <q-cli@amazon.com>"  
    imported  
gpg: Total number processed: 1  
gpg:                      imported: 1
```

- d. Download the Amazon Q CLI signature file for the package you downloaded. It has the same path and name as the .zip file it corresponds to, but has the extension .sig. In the following examples, we save it to the current directory as a file named q.zip.sig.

Linux x86-64

For the latest version of the Amazon Q CLI, use the following command block:

```
curl --proto '=https' --tlsv1.2 -sSf "https://desktop-release.codewhisperer.us-  
east-1.amazonaws.com/latest/q-x86_64-linux.zip.sig" -o "q.zip.sig"
```

For a specific version of the Amazon Q CLI, replace the latest with the version number. For this example the path for version 1.1.0 would be /1.1.0/q-linux-x86_64.zip.sig resulting in the following command:

```
q curl --proto '=https' --tlsv1.2 -sSf "https://desktop-release.codewhisperer.us-east-1.amazonaws.com/1.1.0/q-x86_64-linux.zip.sig" -o "q.zip.sig"
```

Linux ARM (aarch64)

For the latest version of the Amazon Q CLI, use the following command block:

```
curl --proto '=https' --tlsv1.2 -sSf "https://desktop-release.codewhisperer.us-east-1.amazonaws.com/latest/q-aarch64-linux.zip.sig" -o "q.zip.sig"
```

For a specific version of the Amazon Q CLI, replace the latest with the version number. For this example the path for version 1.1.0 would be /1.1.0/q-linux-aarch64.zip.sig resulting in the following command:

```
curl --proto '=https' --tlsv1.2 -sSf "https://desktop-release.codewhisperer.us-east-1.amazonaws.com/1.1.0/q-aarch64-linux.zip.sig" -o "q.zip.sig"
```

For a specific version of the Amazon Q CLI, replace the latest with the version number. For this example the path for version 1.1.0 would be /1.1.0/q-linux-aarch64.zip.sig resulting in the following command:

```
curl --proto '=https' --tlsv1.2 -sSf "https://desktop-release.codewhisperer.us-east-1.amazonaws.com/1.1.0/q-aarch64-linux.zip.sig" -o "q.zip.sig"
```

- e. Verify the signature, passing both the downloaded .sig and .zip file names as parameters to the gpg command.

```
gpg --verify q.zip.sig q.zip
```

The output should look similar to the following.

```
gpg: Signature made Wed 24 Apr 2024 12:08:49 AM UTC
gpg: using EDDSA key 9AF60417E82742C9143E03EC50DC7A8DC24C566
```

```
gpg: Good signature from "Amazon Q CLI Team <q-cli@amazon.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:                 There is no indication that the signature belongs to the owner.
Primary key fingerprint: 9AF6 0417 E827 42C9 143E  03EC 50DC 7A8D C24C 5667
```

Note

The warning in the output is expected and doesn't indicate a problem. It occurs because there isn't a chain of trust between your personal PGP key (if you have one) and the Amazon Q for command line PGP key. For more information, see [Web of trust](#).

3. Unzip the installer. If your Linux distribution doesn't have a built-in unzip command, use an equivalent to unzip it. The following example command unzips the package and creates a directory named q under the current directory.

```
unzip q.zip
```

4. Run the install program. The installation command uses a file named install in the newly unzipped q directory. By default, the files are all installed to `~/.local/bin`.

```
./q/install.sh
```

5. Install ssh config integrations. To do this you must edit your `sshd_config` to add the `AcceptEnv` and `AllowStreamLocalForwarding` setting. To edit the `sshd_config` run:

```
sudo -e /etc/ssh/sshd_config
```

Once you are editing the `sshd_config` add the following to the end of the config file:

```
AcceptEnv Q_SET_PARENT
AllowStreamLocalForwarding yes
```

Note, you must also restart the `sshd` process after installing, if you are using `systemd` you may run:

```
sudo systemctl restart sshd
```

6. To finish setting up the integrations you must disconnect from the SSH instance and reconnect. Once you do you can login to Q by running:

```
q login
```

To check for any other installation issues run:

```
q doctor
```

Known limitations

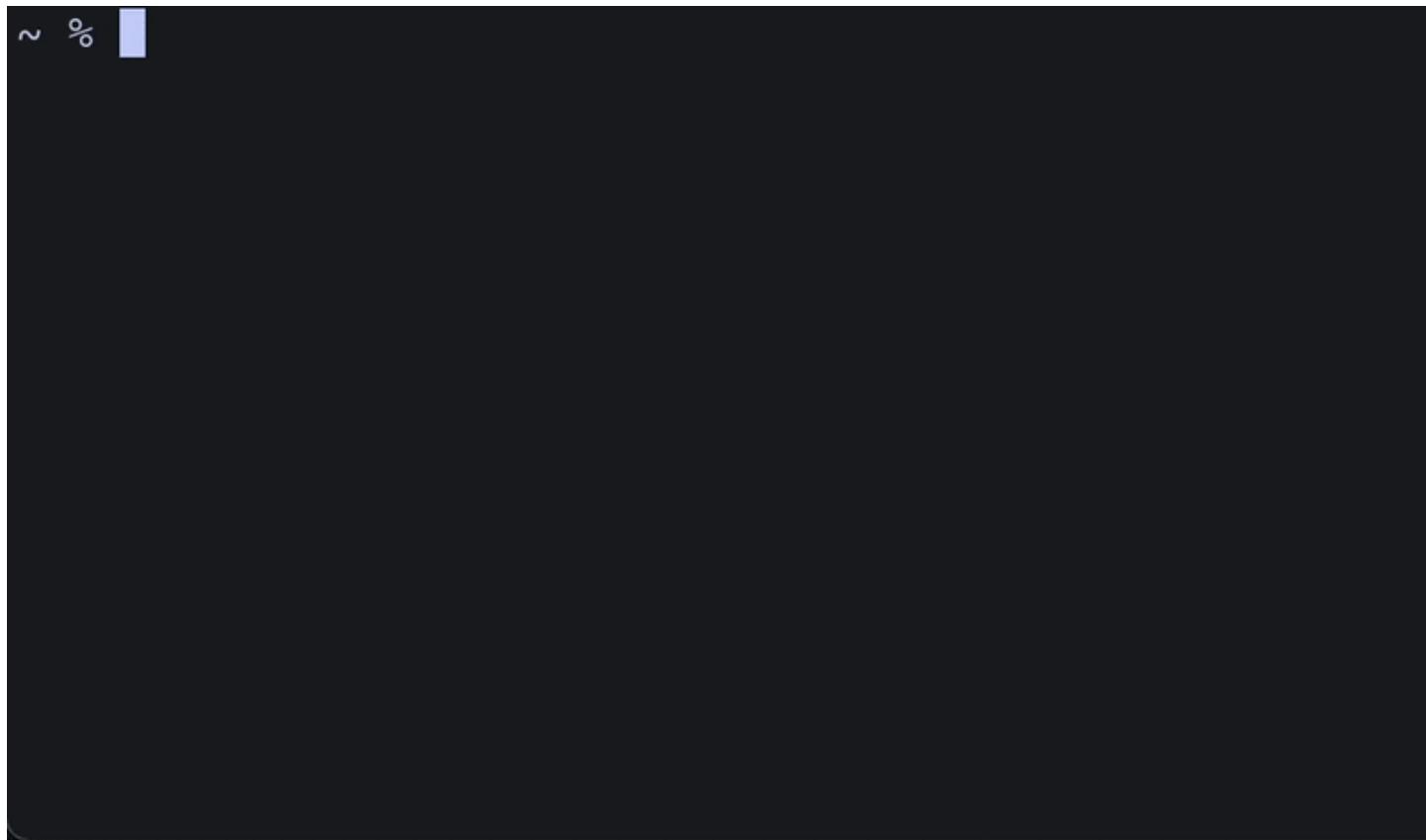
A known limitation is that if the Amazon Q desktop client is quit while connected to a remote machine via SSH, an error message will print repeatedly by SSH. For example:

```
connect to /var/folders/tg/u1vx4xfmvqav0oxfa4zfknaxiwmbbsbr/T/cwrun/remote.sock port -2  
failed: Connection refused
```

To get rid of the error message, either exit the SSH session and reconnect or restart the Amazon Q desktop client.

Amazon Q inline on the command line

The Amazon Q CLI provides AI-generated completions as you type in the command line.



Using Amazon Q inline

To start using the Amazon Q CLI:

1. [Install the Amazon Q CLI.](#)
2. Open a new terminal or command prompt.
3. When you start typing Amazon Q will make suggestions based on your current input and previous commands. To accept a suggestion, press the right arrow key. The suggestion will be inserted into your shell.

To disable the inline feature for new terminal sessions, run the following command:

```
q inline disable
```

This command will only affect new terminal sessions, and the inline feature will remain enabled in any existing terminal windows.

Amazon Q inline Limitations

Currently, inline is only supported in zsh on macOS, and on Linux via the SSH integration.

The inline feature is known to conflict with some popular shell extensions, including zsh-autosuggestions. If you have zsh-autosuggestions installed, you must disable it to use Amazon Q inline in the command line.

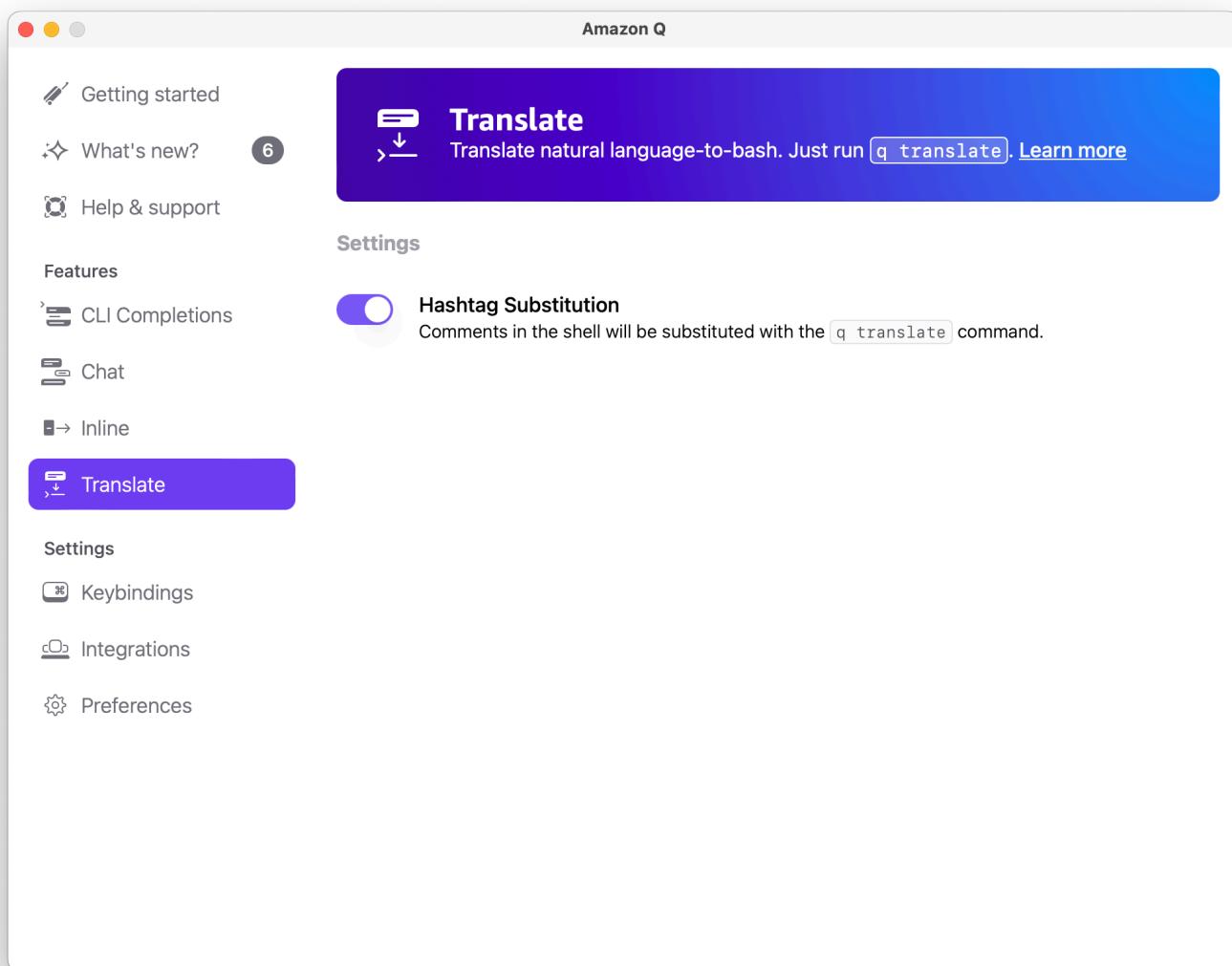
Translating from natural language to bash

The `q translate` command lets you write a natural language instruction such as “copy all files in my current directory to Amazon S3”. Amazon Q will then translate it to an instantly executable shell code snippet. The `q translate` command is useful in those common situations where the correct bash syntax is easy to forget. Examples include reversing a git commit, finding strings inside files with `grep`, or compressing files with `tar`.

To get started, run either of the following

- `q translate prompt`
- `# prompt`

To opt out of using `#` to invoke Amazon Q, go to **Settings -> Translate** and toggle off **Hashtag substitution**.



Debugging Amazon Q Developer for the command line

If you're having a problem with Amazon Q Developer for command line, run `q doctor`.

`q doctor` identifies and fixes common issues. Most of the time, you won't need to do anything else.

Expected output

```
$ q doctor
```

```
# Everything looks good!
```

Amazon Q still not working? Run `q issue` to let us know!

If your output doesn't look like the output above, follow the prompts to resolve your issue. If it's still not working, run `q issue` to report the bug.

Contributing completion specs to Amazon Q Developer

A completion spec is a declarative schema that specifies the subcommands, options and arguments for a CLI tool. Amazon Q Developer for command line uses these schemas to generate suggestions.

You can contribute a completion spec to the open source repository to improve the quality of completions. To add your spec, see the [Amazon Q Developer for command line GitHub repository..](#)

Customizing suggestions

Note

Customizations are supported for the following features of Amazon Q Developer:

- [Generating inline suggestions](#)
- (Preview) [Chatting about code](#)

With customizations, Amazon Q Developer can assist with software development in ways that conform to your team's internal libraries, proprietary algorithmic techniques, and enterprise code style.

An Amazon Q customization is a set of elements that enables Amazon Q to provide you with suggestions based on your company's codebase. You connect a data source that contains your code base, and Amazon Q uses your content to provide assistance that caters to the style of your organization's developers.

Topics

- [Prerequisites for Amazon Q customizations](#)
- [Creating your customization](#)
- [Deleting your customization](#)
- [Evaluating and optimizing your customization](#)
- [Logging and troubleshooting](#)
- [Activating your Amazon Q customizations](#)
- [Updating your Amazon Q customizations](#)
- [Adding users and groups to your Amazon Q customizations](#)
- [Using Amazon Q customizations](#)

Prerequisites for Amazon Q customizations

Amazon Q customizations build upon the foundation of Amazon Q Developer Pro, and uses its features.

To use Amazon Q customizations you must first follow the Amazon Q Developer Pro setup process under [Setting up Amazon Q Developer](#). This includes adding any users to your Amazon Q Developer Pro profile that you also wish to grant access to Amazon Q Customizations.

When you use Amazon Q Customizations, your Amazon Q administrator must be authorized to access your codebase, which you may store on Amazon S3 or through AWS CodeConnections. However, during the standard setup process for Amazon Q Developer Pro, your AWS Organizations administrator does not provide the Amazon Q administrator with access to those services.

 **Note**

If you are using GitHub as your data source, you can restrict usage to certain repositories. See [Create a connection to GitHub](#) in the Developer Tools Console User Guide.

Therefore, before you use Amazon Q Customizations, you must add the following permissions to your Amazon Q administrator's role:

 **Note**

The `codewhisperer` prefix is a legacy name from a service that merged with Amazon Q Developer. For more information, see [Amazon Q Developer rename - Summary of changes](#).

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": [  
            "sso-directory:DescribeUsers"  
        ],  
        "Resource": [  
            "*"  
        ]  
    },  
    {  
        "Effect": "Allow",  
        "Action": [  
            "codewhisperer>CreateCustomization",  
            "codewhisperer>DeleteCustomization",  
            "codewhisperer>GetCustomization",  
            "codewhisperer>ListCustomizations",  
            "codewhisperer>UpdateCustomization"  
        ]  
    }  
}]
```

```
        "codewhisperer>ListCustomizations",
        "codewhisperer>UpdateCustomization",
        "codewhisperer>GetCustomization",
        "codewhisperer>ListCustomizationPermissions",
        "codewhisperer>AssociateCustomizationPermission",
        "codewhisperer>DisassociateCustomizationPermission"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "codeconnections>ListConnections",
        "codeconnections>ListOwners",
        "codeconnections>ListRepositories",
        "codeconnections>GetConnection"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": "codeconnections>UseConnection",
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "codeconnections>ProviderAction": [
                "GitPull",
                "ListRepositories",
                "ListOwners"
            ]
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject*",
        "s3:GetBucket*",
        "s3>ListBucket*"
    ],

```

```
    "Resource": [
        "*"
    ]
}
```

Note

The encryption key that you set up for Amazon Q Developer Pro is also used for customizations.

It's important to create your customization using the best possible source material. When preparing your data source, add code containing patterns that are encouraged on your team. Avoid code containing anti-patterns, bugs, security vulnerabilities, performance issues, and so forth.

Your data source must contain at least 2 MB, and at most 20 GB, of source code files from supported languages. Any file larger than 10 MB will be ignored. There is no limit on the number of files, but you must include at least 10 files for each language that you want your customization to support. In the Amazon S3 data source, ensure that all source code is placed within a directory and not at the root level. Any files at the root level will be ignored.

Note

Amazon Q Customizations supports the following languages and file extensions:

- Java (.java)
- JavaScript (.js, .jsx)
- Python (.py)
- TypeScript (.ts, .tsx)

You can store information about the creation of your customizations in Amazon CloudWatch Logs. For more information, see [Accessing customization-related messages in Amazon CloudWatch Logs](#).

Creating your customization

This section explains how to create a customization with Amazon Q.

To create your customization, follow this procedure:

1. Complete your setup of Amazon Q Developer Pro. This includes enabling IAM Identity Center and authorizing an administrator to Amazon Q Developer, and activating the Amazon Q Developer console.
2. Open the Amazon Q Developer console.
3. From the navigation pane on the left, choose **Customizations**.
4. The customizations page will appear.
5. Choose **Create customization**.
6. Enter a customization name and (optional) description.

 **Note**

Use both names and descriptions that will be informative to your developers. Developers from your organization who are authorized to use Amazon Q Developer Pro will be able to see them in VS Code or JetBrains through the AWS plugin.

Connecting to your data source

The Amazon Q Customizations feature is in preview, and is subject to change.

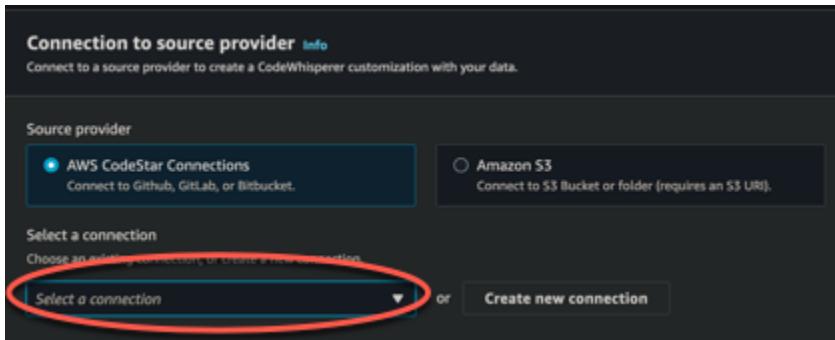
Before you create a customization, you must connect to the data source that contains your codebase. How you do this depends on where your data source is.

If your data source is in Github, GitLab, or Bitbucket, then you must connect to it with AWS CodeConnections. Otherwise, use Amazon S3.

To learn more about CodeConnections, see [What are connections?](#) in the *Developer Tools console User Guide*

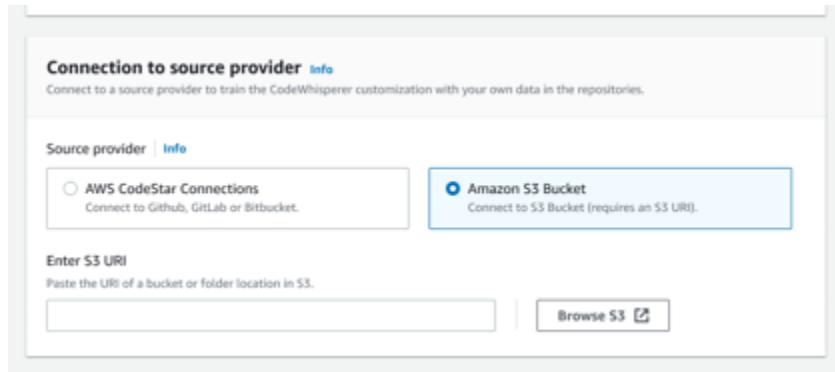
To connect to your data source through CodeConnections, follow this procedure:

1. Under **Connection to source provider**, select CodeConnections.
2. If you are using an existing connection, choose **Select existing connection**. Then, under **Select a connection**, select your connection from the dropdown.



Otherwise, choose **Create a new connection**.

3. In the pop-up window that opens, navigate to your data source and follow the instructions in the console.
4. After you create your data source, return to the **Create customization** page.
5. Under **Select a connection**, select your connection from the dropdown.



To connect to your data source through Amazon S3, follow this procedure:

1. Under **Connection to source provider**, select Amazon S3.
2. Choose **Browse Amazon S3**.
3. Navigate to the bucket or folder containing your codebase and make a note of the URI.

For more information, see [Creating, configuring, and working with Amazon S3 buckets](#) and [Access control best practices](#) in the [Amazon S3 User Guide](#).

4. Paste the URL into the field labeled **Enter Amazon S3 URI**.

Before you create your customization, you have the option of adding tags to it.

To learn more about tags, see [the Tagging your AWS resources User Guide](#).

After following the procedures above, choose **Create customization**.

Customizations and your data

Amazon Q customizations use your content to present suggestions to you in the style of your organization's developers.

However, AWS will not store or use your content in any context that does not directly serve your enterprise.

AWS will not use your content to provide code suggestions to other customers.

Amazon Q will not reference [security scans](#) for other customers (or for you).

For more information, see [Amazon Q Developer service improvement](#).

Troubleshooting the creation of your customization

- You may receive the error: Total size of the provided repositories exceeds the maximum allowed size of *number* for a customization.
In that case, remove a repository from your data source and try again.
- You may receive the error: Insufficient data to create a customization. Add more files from supported languages and retry.

In order for code written in a particular language to be used to create a customization, there must be at least 10 files containing code in that language in your data source. Your data source must contain at least 2 MB, while it is recommended to have close to 20MB, and at most 20 GB, of source code files from supported languages.

Some files, even if they are in the relevant language, will not count toward the 10 MB. For example, duplicate files and files in an unsupported format will not be counted.

If you receive this error, add more files containing the programming language that is the focus of your customization, and try again.

Deleting your customization

This section explains how to delete a customization with Amazon Q.

Warning

Deleting a customization will delete all versions associated with the resource.

To delete your customization, follow this procedure:

1. Open the Amazon Q Developer console.
2. From the navigation pane on the left, choose **Customizations**.
3. The customizations page will appear.
4. If the customization that you want to delete is still active, choose **Deactivate**.
5. Choose **Delete**.

Note

You can also delete a customization from the page that gives the details of that customization.

To do that, just choose **Delete** from the upper right corner of the customization detail page.

Evaluating and optimizing your customization

This page explains how to evaluate and optimize your customization.

Evaluating your customization

This section explains how to evaluate your customization.

1. In the Amazon Q Developer console, from the navigation panel, choose **Customizations**.
2. Choose the name of the customization to examine.
3. The right side of the window will display an evaluation score. This score indicates Amazon Q's evaluation of how effective your customization may be.

With your evaluation score in mind, you must now consider whether or not to activate your customization. In making this decision, take the following factors into consideration.

- **Very good 8-10:** Amazon Q recommends that you activate this customization.
- **Fair 5-7:** Amazon Q recommends that you activate this customization.

If you do not see significant improvement, consider the optimization suggestions below. If those are not effective, consider switching to a different code source.

- **Poor 1-4:** The customization may not be effective. To improve the quality of customization, consider the optimization suggestions below. If those are not effective, consider switching to a different code source.

Optimizing your customization

This section contains suggestions for optimizing your suggestion in order to achieve a higher evaluation score.

- Consider expanding your data source to include more code repositories.
- If you primarily included data from limited programming languages, consider expanding to more languages.
- Remove auto-generated files and repositories, or those generated from templates. Training a customization to generate or complete such files is typically not valuable, and tends to just add noise.

 **Note**

Amazon Q automatically filters out non-code files, such as configuration files and text files.

- It is possible that your codebase does not frequently use internal libraries. If you know this to be true, then the core Amazon Q model may already have been performing as well as possible.

Optimizing for the languages you use

In order for code in a particular language to be used in a customization, you must include at least 20 data files containing that language, and all of your source files together must come to at least 10 MB. If your developers write code in a language that is not supported by your

customization, Amazon Q's recommendations in that language will come from the Amazon Q base model (not your customization). In other words, they will be the same recommendations that you would receive if you did not have a customization. This, in turn, could affect the metrics on your dashboard. For example, the "Lines of code generated by Amazon Q" may be less than what it would have been if the language commonly used by your developers had been included in your customization.

Logging and troubleshooting

Setting up log delivery

Amazon Q can provide you with log files that will help you understand and troubleshoot issues with your customization.

You can have your log files sent to a [Amazon CloudWatch Logs](#) group, an [Amazon S3](#) bucket, an [Amazon Data Firehose](#), or any combination.

To set up log delivery, select the Log deliveries tab on the console page for your customization. Follow the instructions in the interface to configure your log deliveries. Then choose **Create log deliveries**.

The prefix of logs delivered to an Amazon S3 bucket will be: AWSLogs/*account_id*/codeWhispererCustomizationLogs/*region*/*customization_id*/*year*/*month*/*day*/*hour*/

The files will be zipped, with the naming format:

*account_id*_codeWhispererCustomizationLogs_*customization_id_date_file_id.log.gz*

Warning

In order to get the most use out of customization logs, it's best to set up log delivery within five minutes of creating the customization.

To learn more about the permissions required to delivery logs to multiple resources, see [Logging that requires additional permissions \[V2\]](#) in the *Amazon CloudWatch Logs User Guide*.

Understanding customization-related log messages

The following table lists log messages that may help you understand issues with your customization.

Log message	Log level
Starting to ingest <i>number</i> repos from source <i>source</i>	Info
Downloading data from repo: <i>repo name</i>	Info
Received <i>amount</i> MB of supported data. <i>amount</i> MB required. Add more data and retry.	Error
The provided CodeStar Connection ARN: <i>Arn</i> is invalid.	Error
Access denied when attempting to reach the provided CodeStar Connection: <i>Arn</i>	Error
Failed to download with AWS CodeStar Connection: <i>Arn</i> probably deleted by customer	Error
ProviderThrottlingException from CodeStar Connection: <i>Arn</i> while cloning repository: <i>repository</i>	Error
Processing data from S3: <i>S3 URI</i>	Info
Invalid S3 path specified: <i>S3 Directory</i>	Error
Unable to access the provided S3 bucket: <i>bucket name</i>	Error
The provided S3 bucket: <i>bucket name</i> does not exist.	Error

Log message	Log level
The provided S3 key <i>S3 URI</i> does not exist.	Error
Failed to ingest <i>number of failed repos / total number of repos</i> repositories	Error
Unable to process repository: <i>repo name</i> , with a size of <i>repo size</i> GB, exceeds the limit of <i>max size</i> GB.	Warn
Unable to process file: <i>file name</i> , with a size of <i>file size</i> , which exceeds the limit of <i>max file size</i> MB	Error
Unable to process collection: <i>collection name</i> , with total size of <i>total repo size</i> MB, which exceeds the limit of <i>max total repo size</i> MB	Error
The following languages will be used for customization: <i>list of languages</i> . Languages may be excluded from customization if they are not sufficiently represented in your files.	Info

Understanding customization-related error messages in the console

The following table will help you understand customization-related messages in the Amazon Q console.

Error message	Suggested action
You have activated the maximum number of customizations.	Deactivate an active customization and try again.
You have exceeded the maximum number of group permissions limit of <i>limit</i> .	Remove a group and retry.
You have exceeded the maximum number of user permissions limit of <i>limit</i> .	Remove a user and retry.
Maximum active jobs reached.	Wait until an in-progress job in the same account has finished. Retry the operation.
Encountered an unexpected error when processing the request.	Retry the operation. If it continues to fail, contact customer support.
Access denied when attempting to reach the provided AWS CodeConnections connection.	Validate permissions on your connection and on your third-party provider. Then retry the operation.
One or more repositories not found while accessing the provided AWS CodeConnections connection.	Validate permissions and list of repos from the third-party provider. Then retry the operation.
The provided AWS CodeConnections connection ARN is invalid.	Update the customization with a corrected Connection ARN.
The Host associated with the provided AWS CodeConnections connection is unavailable.	Try again in 5 minutes.
Invalid Amazon S3 path specified.	Update the customization with a valid Amazon S3 URI.
Unable to access the provided Amazon S3 bucket.	Validate permissions for the admin's role. Retry after fixing any permission issues.
The provided Amazon S3 bucket does not exist.	Update the customization with a valid Amazon S3 URI.

Error message	Suggested action
The provided Amazon S3 key does not exist.	Update the customization with a valid Amazon S3 URI.
Insufficient data to create a customization. Add more files from supported languages and retry.	Add more data to the same data source, and update the customization with the same reference.
Total size of the provided repositories exceeds the maximum allowed size of <i>size</i> for a customization.	Remove some data from the provided data source. Update the customization with the same reference.
You have created the maximum number of customizations. Delete an existing customization and try again.	Delete the current customization and retry.
Customizations exist within the account. You must delete all customizations prior to deleting the profile.	Delete all customizations associated with the account and retry.

Activating your Amazon Q customizations

Activating a version

This section describes how to activate and deactivate a version of your customization.

You can activate a new version of a customization, even while developers from your organization are using the previous version. After you activate the new version, the developers will seamlessly begin using it, with no adjustments needed on the development side.

You can also roll your customization back to a previously active state. However, Amazon Q does not actually re-activate a previously activated version. Instead, it creates a new version by copying a previous version and then activating the copy.

For example, suppose that you have three versions: 1, 2, and 3. The active version is 3. You decide to go back to version 1. But "re-activating" version 1 is actually just copying version 1 and creating version 4. That's the version you use: version 4, the new copy of the old version.

To activate a version of your customization, follow this procedure:

1. Open the Amazon Q Developer console.
2. From the navigation pane on the left, choose **Customizations**.

The customizations page will appear.

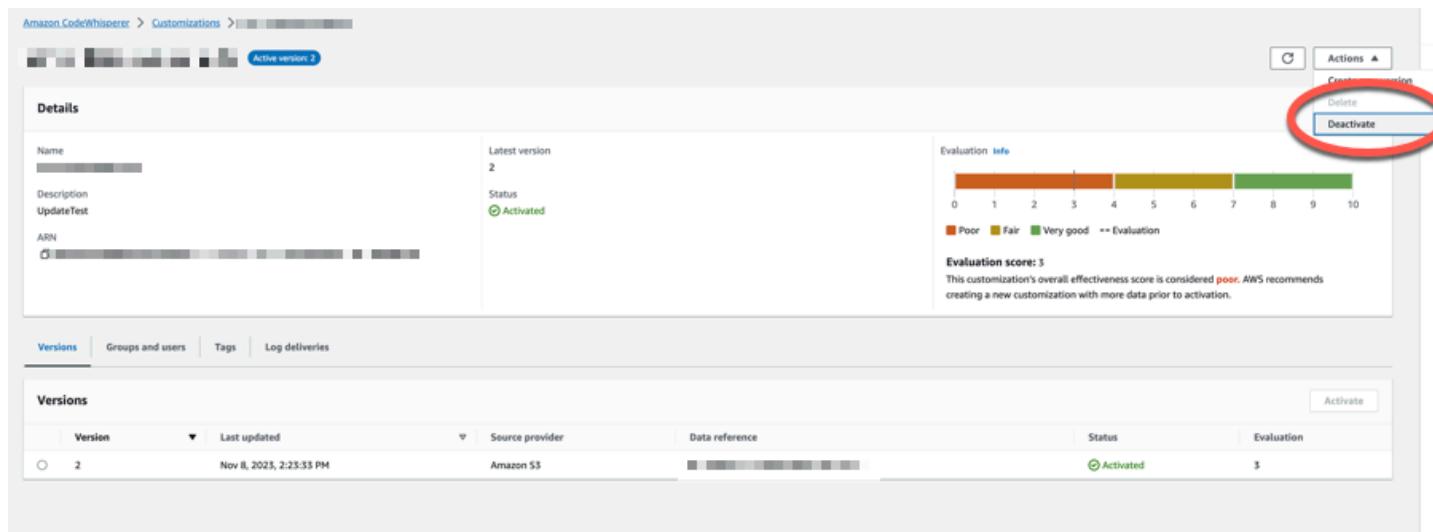
3. Choose the customization you want to activate a version for.

The customization details page will appear.

4. Choose the version you want to activate from the **Versions** table.
5. Choose **Activate**.

The screenshot shows the Amazon Q Developer Customizations page. At the top, there's a breadcrumb trail: Amazon CodeWhisperer > Customizations. Below it, a navigation bar with 'Active version: 2' and 'Actions' dropdown. The main area has two tabs: 'Details' (selected) and 'Versions'. In the 'Details' tab, there are sections for Name, Description, and ARN, along with a 'Latest version' (3), 'Status' (Updated), and an 'Evaluation' chart (score 4). The chart has three segments: orange (Poor), yellow (Fair), and green (Very good). Below the chart, it says 'Evaluation score: 4' and provides a note about the overall effectiveness score being considered 'fair'. In the 'Versions' tab, there's a table with columns: Version, Last updated, Source provider, Data reference, Status, and Evaluation. It lists two versions: Version 3 (Nov 8, 2023, 2:40:30 PM, Amazon S3, status Updated, evaluation 4) and Version 2 (Nov 8, 2023, 2:23:33 PM, Amazon S3, status Activated, evaluation 3). An 'Activate' button is located at the top right of the 'Versions' table.

To deactivate a customization, choose **Deactivate** from the dropdown.



The screenshot shows the 'Customizations' section of the Amazon CodeWhisperer console. A customization named 'UpdateTest' is selected, showing its details. The 'Status' is 'Activated'. An 'Evaluation' bar indicates a score of 3, labeled as 'Fair'. The 'Actions' menu includes 'Delete' and 'Deactivate', with 'Deactivate' circled in red. Below the details, there are tabs for 'Versions', 'Groups and users', 'Tags', and 'Log deliveries'. The 'Versions' tab lists one version (Version 2, Last updated Nov 8, 2023, 2:23:33 PM, Source provider: Amazon S3, Status: Activated, Evaluation: 3).

Updating your Amazon Q customizations

This section explains how to update a customization with Amazon Q.

A customization can have multiple versions.

Amazon Q administrators have access to a maximum of three versions for each customization:

- the latest version
- the currently active version
- the most recently active version that is not currently active

Creating a new version

The screenshot shows the 'Customizations' page in the Amazon Q Developer console. A customization named 'ABIS...' is selected. The 'Actions' dropdown menu is open, with 'Create new version' highlighted. The 'Evaluation' section displays a score of 6 (Fair) with a bar chart ranging from 0 to 10. The 'Versions' section shows one version (Version 1, Last updated Nov 21, 2023, 4:03:47 PM, Source provider: Amazon S3, Status: Created, Evaluation: 6).

To create a new version of your customization, follow this procedure:

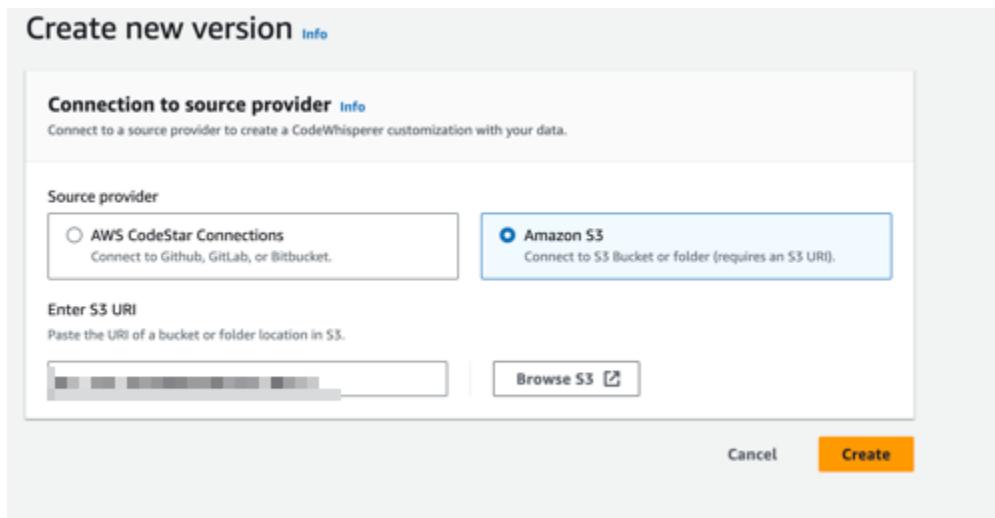
1. Open the Amazon Q Developer console.
2. From the navigation pane on the left, choose **Customizations**.

The customizations page will appear.

3. Choose the customization for which you want to create a new version.

The customization details page will appear.

4. Select **Create new version** from the **Actions** dropdown.
5. If applicable, change the data source.



6. Choose **Create**.

If you receive error messages, see [Troubleshooting the creation of your customization](#).

Adding users and groups to your Amazon Q customizations

This section contains information about how to add users and groups to customizations.

Note

You must activate a customization before you can add users to it.

Note

You can only add a user or group to a customization if you have already added the user or group to your Amazon Q Developer Pro profile. For more information, see [Managing subscriptions](#).

1. In the Amazon Q Developer console, from the navigation panel, choose **Customizations**.
2. Choose the name of the customization to which you want to add users or groups.
3. In the bottom half of the window, if necessary, select the **Users and groups** tab. and then the **Users or Groups** sub-tab.
4. Select the users or groups that require access to your customization.

5. Choose **Add users** or **Add groups**.

Using Amazon Q customizations

This section contains information about how to use customizations as a developer.

Amazon Q only supports customizations in VS Code and JetBrains IDEs.

AWS Toolkit for Visual Studio Code

To use customizations with VS Code:

1. Authenticate to Amazon Q Developer Pro with IAM Identity Center using the steps under [Installing the Amazon Q Developer extension or plugin in your IDE](#).
2. In the **Developer Tools** pane, under Amazon Q, choose **Select Customization**.
3. At the top of the window, from the dropdown menu, select the appropriate customization.

AWS Toolkit for JetBrains

To use customizations with JetBrains:

1. Authenticate to Amazon Q Developer Pro with IAM Identity Center using the steps under [Installing the Amazon Q Developer extension or plugin in your IDE](#).
2. In the **Developer Tools** pane, under Amazon Q, choose **Select Customization**.
3. In the pop-up window, select the appropriate customization.
4. Choose **Connect**.

Dashboard

Available only for Amazon Q Developer administrators, the Amazon Q Developer dashboard summarizes useful data about how your developers use the service. Among the useful metrics is the acceptance rate, which indicates how often you take inline suggestions from Amazon Q.

Note

As a feature in Preview, Amazon Q Developer may answer your questions in the IDE using data provided by an active customization. However, such interactions are not tracked in the dashboard.

AWS Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia MyRole/AWSUser @ 0123-4567-8901

Amazon Q in the IDE > Dashboard

Dashboard Info

Amazon Q in the IDE dashboard provides metrics illustrating how your developers use the service.

Active customization Data range

Programming language All 2023-10-27 — 2023-11-10

All Clear filters

User activity

Count

10/29/2023 11/02/2023 11/06/2023 11/10/2023

— Active subscriptions — Daily active users

Code impact

Lines of code generated by Amazon Q in the IDE
144.85 million

Acceptance rate
45.32%

Accepted recommendations with references
4.83 million

Security scans

Language	Number of scans
Java	1.2 million
Javascript	-
Python	-

Dashboard User activity Code impact Security scans

The User activity section indicates how many Amazon Q in the IDE seats you are paying for, and how many of those seats are being used on a daily basis. The difference between the two is the number of subscriptions you are paying for that are not being used.

The Lines of code generated by Amazon Q in the IDE simply indicates how many lines of code were suggested by Amazon Q and accepted by your developers.

Accepted recommendations with references indicates the number of suggestions from Amazon Q that are based on open-source projects, the references to which Amazon Q makes available to you.

Amazon Q in the IDE security scan is a tool that helps identify security vulnerabilities in your developers' code.

The data shown indicates how many scans your developers have successfully run in their IDEs.

Learn more [Amazon Q in the IDE dashboard](#) [Security scan](#) [Code references](#)

CloudShell Feedback Language © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

You can filter the data in the dashboard by date range. The minimum range is two weeks and the maximum is one year. You can also filter by programming language.

To view metrics on the dashboard, you must have the `cloudwatch:GetMetricData` and `cloudwatch:listMetrics` permissions. This permission is granted to administrators as part of [assigning Amazon Q administration rights](#).

User activity

The **User activity** section indicates how many Amazon Q seats you are paying for, and how many of those seats are being used on a daily basis. The difference between the two is the number of subscriptions you are paying for that are not being used.

Code impact

The Lines of code generated by Amazon Q simply indicates how many lines of code were suggested by Amazon Q and accepted by your developers.

Accepted recommendations with references indicates the number of suggestions from Amazon Q that are based on open-source projects, the references to which Amazon Q makes available to you.

If you use Amazon Q very little over a two-week period, the **Code impact** section will be affected as follows:

- If no recommendations are invoked for two weeks, then no data will appear in the **Code impact** section.
- If recommendations are invoked, but none are accepted or rejected, then no data will appear in the **Code impact** section.
- If recommendations are invoked, and none are accepted, but some are rejected, then the **Acceptance rate (0%)** will be displayed, but no data will appear for **Lines of code generated by Amazon Q** or **Accepted recommendations with references**.

Security scans

Amazon Q security scans identify security vulnerabilities in your developers' code.

The data shown indicates how many scans your developers have successfully run in their IDEs.

Amazon Q Developer and other AWS services

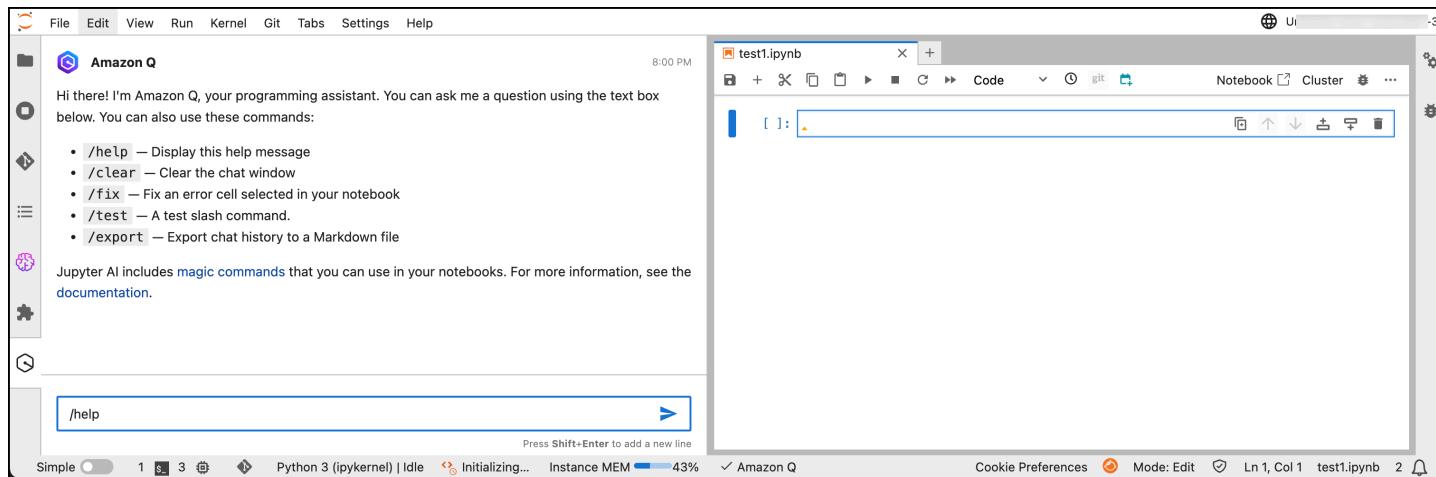
Amazon Q Developer is available as a feature in several other AWS services. This section explains some of the ways you can access Amazon Q within AWS.

AWS services

- [Amazon SageMaker Studio](#)
- [Amazon Q Business](#)
- [Amazon Q in AWS Chatbot](#)
- [Amazon Q in Amazon CodeCatalyst](#)
- [Amazon Q in Amazon Connect](#)
- [Amazon Q in Amazon EC2](#)
- [Amazon Q in AWS Glue](#)
- [Amazon Q in VPC Reachability Analyzer](#)
- [Amazon Q in Amazon QuickSight](#)

Amazon SageMaker Studio

Amazon SageMaker Studio is a web-based experience for running ML workflows. You can chat with Amazon Q Developer, and receive coding suggestions from it, inside Studio.



For more information, see [Use Amazon Q Developer to expedite your machine learning workflows](#) in the *Amazon SageMaker Developer Guide*.

Amazon Q Business

Amazon Q Business is a fully managed, generative AI-powered enterprise chat assistant that you can deploy within your organization. For more information, see the [Amazon Q Business User Guide](#).

Amazon Q in AWS Chatbot

You can activate Amazon Q in your Slack and Microsoft Teams channels that are configured with AWS Chatbot to ask questions about building at AWS. To add Amazon Q to your channels, see [Chatting with Amazon Q Developer in AWS Chatbot](#). For more information, see [Get started with Slack](#) and [Get started with Microsoft Teams](#) in the *AWS Chatbot Administrator Guide*.

Amazon Q in Amazon CodeCatalyst

Amazon Q feature development capability in Amazon CodeCatalyst is a generative AI assistant to which you can assign issues. After an issue is assigned to Amazon Q, it analyzes the issue based on its title and description and reviews the code in the specified repository. If Amazon Q can create an approach, it creates a draft solution for users to evaluate in a pull request. For more information, see [Tutorial: Using CodeCatalyst generative AI features to speed your development work](#) in the *Amazon CodeCatalyst User Guide*.

Amazon Q in Amazon Connect

Amazon Q in Amazon Connect is a generative AI customer service assistant that is a large language model (LLM)-enhanced evolution of Amazon Connect Wisdom. Amazon Q in Amazon Connect delivers real-time recommendations to help contact center agents resolve customer issues quickly and accurately. For more information, see [Use Amazon Q in Amazon Connect](#) in the *Amazon Connect Administrator Guide*.

Amazon Q in Amazon EC2

In the Amazon Elastic Compute Cloud (Amazon EC2) console, you can use the Amazon Q EC2 instance type selector to provide guidance and suggestions for EC2 instance types that are best suited to your new workloads. For more information, see [Get instance type recommendations for a new workload](#) in the *Amazon EC2 User Guide*.

Amazon Q in AWS Glue

Amazon Q data integration in AWS Glue is a generative AI-powered assistant that enables you to build data integration jobs in AWS Glue using natural language. With Amazon Q data integration, you can author data integration jobs, troubleshoot issues, and get answers to AWS Glue data integration questions. For more information, see [Amazon Q data integration in AWS Glue](#) in the *AWS Glue User Guide*.

Amazon Q in VPC Reachability Analyzer

When you ask Amazon Q to help you fix a network connectivity problem, it works with VPC Reachability Analyzer to check your connections, inspect your network configuration, and identify potential issues. Then Amazon Q provides guidance on how to resolve or further diagnose the issue. Using the conversational capabilities of Amazon Q and Reachability Analyzer together creates an intuitive way for you to fix network connectivity problems quickly. For more information, see [Amazon Q network reachability analysis](#) in the *Reachability Analyzer User Guide*.

Amazon Q in Amazon QuickSight

Amazon Q in Amazon QuickSight is optimized to understand natural language that you use to ask questions about your data. You can ask Amazon Q questions that use common phrases related to sales, marketing, and retail to meet your business needs quickly. For more information, see [Amazon Q in Amazon QuickSight](#) in the *Amazon QuickSight User Guide*.

Security in Amazon Q Developer

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 Q, 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 Q Developer. It shows you how to configure Amazon Q to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Amazon Q resources.

Topics

- [Data protection in Amazon Q Developer](#)
- [Identity and access management for Amazon Q Developer](#)
- [Compliance validation for Amazon Q Developer](#)
- [Resilience in Amazon Q Developer](#)
- [Infrastructure security in Amazon Q Developer](#)
- [Amazon Q Developer and interface VPC endpoints \(AWS PrivateLink\)](#)

Data protection in Amazon Q Developer

The AWS [shared responsibility model](#) applies to data protection in Amazon Q Developer. 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 S3.
- 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 Q or other AWS services using the AWS Management Console, API, AWS Command Line Interface (AWS CLI), or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs.

Regardless of where you use Amazon Q Developer, data is sent to and stored in an AWS Region in the US. Your conversations with Amazon Q are stored in the US East (N. Virginia) Region even if the AWS Management Console is set to a different AWS Region. Data processed during troubleshooting console error sessions is stored in the US West (Oregon) Region. Data processed during interactions with Amazon Q in integrated development environments (IDEs) is stored in the US East (N. Virginia) Region.

Amazon Q stores your questions, its responses, and additional context, such as console metadata and code in your IDE, to generate responses to your questions. For information about how AWS

may use some questions that you ask Amazon Q and its responses to improve our services, see [Amazon Q Developer service improvement](#).

Topics

- [Data encryption in Amazon Q Developer](#)
- [Amazon Q Developer service improvement](#)
- [Opt out of data sharing in the IDE](#)
- [Cross-Region calls in Amazon Q Developer](#)

Data encryption in Amazon Q Developer

This topic provides information specific to Amazon Q Developer about encryption in transit and encryption at rest.

Encryption in transit

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

Encryption at rest

Amazon Q stores data at rest using Amazon DynamoDB and Amazon Simple Storage Service (Amazon S3). The data at rest is encrypted using AWS encryption solutions by default. Amazon Q 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 Key Management Service Developer Guide*.

For data stored by Amazon Q in integrated development environments (IDEs), you can create your own customer managed AWS KMS key to encrypt your data at rest. Customer managed keys are KMS keys in your AWS account that you create, own, and manage to directly control access to your data by controlling access to the KMS key. For information on creating your own KMS key, see [Creating keys](#) in the *AWS Key Management Service Developer Guide*.

Encryption with the Amazon Q Developer Agent for code transformation

When you begin a transformation with the [Amazon Q Developer Agent for code transformation](#), your code is sent to a service-owned Amazon S3 bucket over an encrypted TLS connection. Your code is encrypted at rest with a customer managed key if you provide one, and otherwise with

an AWS-owned key. During the transformation, your code is stored in memory in a secure build environment. After the transformation has completed, the build environment is deleted and any artifacts are flushed from memory. Your encrypted code remains in the service-owned Amazon S3 bucket for up to 24 hours, and then is permanently deleted.

Encryption with Customizations

When you create a [customization](#), Amazon Q uploads your files to a service-owned Amazon S3 bucket. Your files are encrypted in transit with HTTPS and TLS. They are encrypted at rest with a customer managed key if you provide one, and otherwise with an AWS-owned key. Once your customization has been created, AWS permanently deletes your data from the bucket, and purges it from memory.

Your customizations are fully isolated from each other within your account. They are also isolated from the data of other customers. Only users [specified by a Amazon Q Developer administrator](#) have access to any specific customization. Before a Amazon Q administrator can specify which users can access which customizations, you must authorize that administrator permission to do so. For more information, see [Prerequisites for Amazon Q customizations](#).

Amazon Q Developer service improvement

To help Amazon Q Developer provide the most relevant information, we may use certain content from Amazon Q, such as questions that you ask Amazon Q and its responses, for service improvement. This page explains what content we use and how to opt out.

Amazon Q Developer Free Tier content used for service improvement

We may use certain content from Amazon Q Developer Free Tier for service improvement. Amazon Q may use this content, for example, to provide better responses to common questions, fix Amazon Q operational issues, for de-bugging, or for model training.

Content that AWS may use for service improvement includes, for example, your questions to Amazon Q and the responses and code that Amazon Q generates.

We do not use content from Amazon Q Developer Pro or Amazon Q Business for service improvement.

How to opt out

The way you opt out of Amazon Q Developer Free Tier using content for service improvement depends on the environment where you use Amazon Q.

For the AWS Management Console, AWS Console Mobile Application, AWS websites, and AWS Chatbot, configure an AI services opt-out policy in AWS Organizations. For more information, see [AI services opt-out policies](#) in the *AWS Organizations User Guide*.

In the IDE, for Amazon Q Developer Free Tier, adjust your settings in the IDE. For more information, see [Opt out of data sharing in the IDE](#).

Opt out of data sharing in the IDE

This page explains how to opt out of sharing your data in the IDE where you use Amazon Q, including third-party IDEs and AWS coding environments. For information on how Amazon Q uses this data, see [Amazon Q Developer service improvement](#).

Opting out of sharing your client-side telemetry

Your client-side telemetry quantifies your usage of the service. For example, AWS may track whether you accept or reject a recommendation. Your client-side telemetry does not contain actual code, and does not contain personally identifiable information (PII) such as your IP address.

Choose an environment for instructions on opting out of sharing your client-side telemetry.

Visual Studio Code

To opt out of sharing your telemetry data in VS Code, use this procedure:

1. Open **Settings** in VS Code.
2. If you are using VS Code workspaces, switch to the **Workspace** sub-tab. In VS Code, workspace settings override user settings.
3. In the Settings search bar, enter **Amazon Q: Telemetry**.
4. Deselect the box.

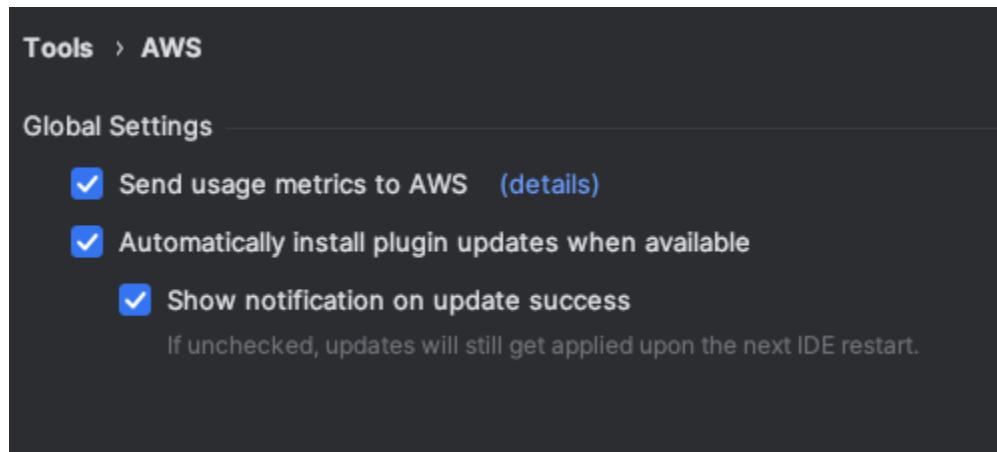
Note

This is a decision for each developer to make inside their own IDE. If you are using Amazon Q as part of an enterprise, your administrator will not be able to change this setting for you.

JetBrains

To opt out of sharing your telemetry data in JetBrains, use this procedure:

1. In your JetBrains IDE, open **Preferences** (on a Mac, this will be under **Settings**).
2. In the left navigation bar, choose **Tools**, and then choose **AWS**.
3. Deselect **Send usage metrics to AWS**.



Note

This is a decision for each developer to make inside their own IDE. If you are using Amazon Q as part of an enterprise, your administrator will not be able to change this setting for you.

Visual Studio

To opt out of sharing your telemetry data in the AWS Toolkit for Visual Studio, use this procedure:

1. Under **Tools**, choose **Options**.
2. In the **Options** pane, choose **AWS Toolkit**, and then choose **General**.
3. Deselect **Allow AWS Toolkit to collect usage information**.

Note

This is a decision for each developer to make inside their own IDE. If you are using Amazon Q as part of an enterprise, your administrator will not be able to change this setting for you.

AWS Cloud9

1. From inside your AWS Cloud9 IDE, choose the AWS Cloud9 logo at the top of the window, then choose **Preferences**.
2. On the **Preferences** tab choose **AWS Toolkit**.
3. Next to **AWS: client-side telemetry**, toggle the switch to the off position.

Note

This setting affects whether or not you share your AWS Cloud9 client-side telemetry in general, not just for Amazon Q.

Lambda

When you use Amazon Q with Lambda, Amazon Q does not share your client-side telemetry with AWS.

SageMaker Studio

1. From the top of the SageMaker Studio window choose **Settings**.
2. From the **Settings** dropdown, choose **Advanced Settings Editor**.
3. In the Amazon Q dropdown, select or deselect the box next to **Share usage data with Amazon Q**.

JupyterLab

1. From the top of the JupyterLab window choose **Settings**.
2. From the **Settings** dropdown, choose **Advanced Settings Editor**.

3. In the Amazon Q dropdown, select or deselect the box next to **Share usage data with Amazon Q**.

AWS Glue Studio Notebook

1. From the bottom of the AWS Glue Studio Notebook window choose **Amazon Q**.
2. From the pop-up menu, toggle the switch next to **Share telemetry with AWS**.

 **Note**

Pausing the sharing of client-side telemetry will be valid only for the duration of the current AWS Glue Studio Notebook.

Command line

In the command line tool, under **Preferences**, toggle **Telemetry**.

Opting out of sharing your content

For information on content AWS uses, see [Amazon Q Developer service improvement](#).

Visual Studio Code

At the Amazon Q Developer Pro Tier, Amazon Q does not collect your content.

At the Amazon Q Developer Free Tier, to opt out of sharing your content in VS Code, use the following procedure.

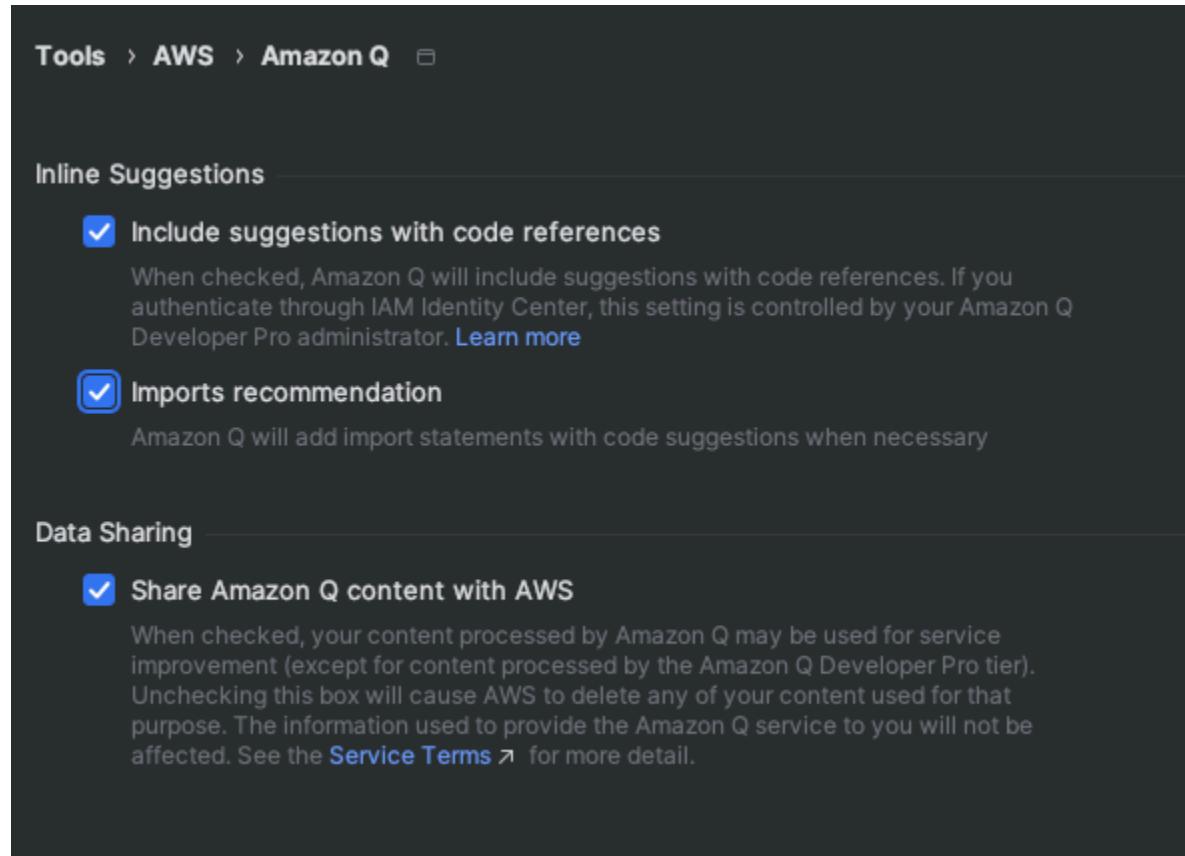
1. Open **Settings** in VS Code.
2. If you are using VS Code workspaces, switch to the **Workspace** sub-tab. In VS Code, workspace settings override user settings.
3. In the Settings search bar, enter **Amazon Q: Share Content**.
4. Deselect the box.

JetBrains

At the Amazon Q Developer Pro Tier, Amazon Q does not collect your content.

At the Amazon Q Developer Free Tier, to opt out of sharing Amazon Q data in JetBrains, use the following procedure.

1. Make sure you are using the latest version of JetBrains.
2. In your JetBrains IDE, open **Preferences** (on a Mac, this will be under **Settings**).
3. In the left navigation bar, choose **Tools --> AWS --> Amazon Q**.
4. Under **Data sharing**, deselect **Share Amazon Q content with AWS**.



Visual Studio

At the Amazon Q Developer Pro Tier, Amazon Q does not collect your content.

At the Amazon Q Developer Free Tier, to opt out of sharing your content in Visual Studio, use the following procedure.

Bring up the Amazon Q options menu one of two ways:

- Choose the AWS Toolkit icon from the edge of the window, then choose **Options...**
- Go to **Tools -> Options -> AWS Toolkit -> Amazon Q**

Toggle **Share Amazon Q Content with AWS** to True or False.

AWS Cloud9

When you use Amazon Q with AWS Cloud9, Amazon Q does not share your content with AWS.

Note

The AWS Cloud9 settings do contain a toggle switch for sharing Amazon Q content with AWS, but that switch is non-functional.

Lambda

When you use Amazon Q with Lambda, Amazon Q does not share your content with AWS.

SageMaker Studio

When you use Amazon Q with SageMaker Studio, Amazon Q does not share your content with AWS.

JupyterLab

1. From the top of the JupyterLab window choose **Settings**.
2. From the **Settings** dropdown, choose **Advanced Settings Editor**.
3. In the Amazon Q dropdown, select or deselect the box next to **Share content with Amazon Q**.

AWS Glue Studio Notebook

When you use Amazon Q with AWS Glue Studio Notebook, Amazon Q does not share your content with AWS.

Command line

In the command line tool, under **Preferences**, toggle **Share Amazon Q content with AWS**.

Cross-Region calls in Amazon Q Developer

While using Amazon Q Developer, you might be asked to consent to cross-Region calls. Cross-Region calls are API calls made by Amazon Q from one AWS Region to another AWS Region.

Amazon Q Developer is hosted in US East (N. Virginia), but can make calls to Regions listed on the Supported Regions page, including opt-in Regions. You must consent to cross-Region calls to use Amazon Q Developer features that access your AWS resources, since Amazon Q Developer might have to make calls to other Regions to access your resources.

You must consent to cross-Region calls for each feature that requires consent. If you don't provide consent, Amazon Q Developer will not make cross-Region calls.

When you use a feature of Amazon Q Developer that requires consent to cross-Region calls, you will be prompted to give consent. The way you update cross-Region consent settings depends on the feature you're using. See the topic for the feature you're using for information about updating your cross-Region preferences.

Identity and access management for Amazon Q Developer

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 Q Developer resources. IAM is an AWS service that you can use with no additional charge.

Topics

- [Audience](#)
- [Authenticating with identities](#)
- [Managing access using policies](#)
- [How Amazon Q Developer works with IAM](#)
- [Manage access to Amazon Q Developer with policies](#)
- [Amazon Q Developer permissions reference](#)
- [AWS managed policies for Amazon Q Developer](#)
- [Using service-linked roles for Amazon Q Developer and User Subscriptions](#)

Audience

How you use IAM differs, depending on the work you do in Amazon Q.

Service user – If you use the Amazon Q service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Amazon Q features to do

your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator.

Service administrator – If you’re in charge of Amazon Q resources at your company, you probably have full access to Amazon Q. It’s your job to determine which Amazon Q features and resources your service users should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Amazon Q, see [How Amazon Q works with IAM](#).

IAM administrator – If you’re an IAM administrator, you might want to learn details about how you can write policies to manage access to Amazon Q. If you’re an IAM administrator, consider learning the details about how you can write policies to manage IAM user access to services. For information that’s specific to Amazon Q, see [AWS Regions managed policies for Amazon Q](#).

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be *authenticated* (signed in to AWS) as the AWS account root user, an IAM user, or by assuming an IAM role.

You can sign in to AWS as a federated identity by using credentials provided through an identity source. AWS IAM Identity Center (IAM Identity Center) users, your company’s single sign-on authentication, and your Google or Facebook credentials are examples of federated identities. When you sign in as a federated identity, your administrator previously set up identity federation using IAM roles. When you access AWS by using federation, you are indirectly assuming a role.

Depending on the type of user you are, you can sign in to the AWS Management Console or the AWS access portal. For more information about signing in to AWS, see [How to sign in to your AWS account](#) in the *AWS Sign-In User Guide*.

Regardless of the authentication method that you use, you might also be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see [Multi-factor authentication](#) in the *AWS IAM Identity Center User Guide* and [Using multi-factor authentication \(MFA\) in AWS](#) in the *IAM User Guide*.

AWS account root user

When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see [Tasks that require root user credentials](#) in the *IAM User Guide*.

Federated identity

As a best practice, require human users, including users that require administrator access, to use federation with an identity provider to access AWS services by using temporary credentials.

A federated identity is a user from your enterprise user directory, a web identity provider, the AWS Directory Service, the Identity Center directory, or any user that accesses AWS services by using credentials provided through an identity source. When federated identities access AWS accounts, they assume roles, and the roles provide temporary credentials.

For centralized access management, we recommend that you use AWS IAM Identity Center. You can create users and groups in IAM Identity Center, or you can connect and synchronize to a set of users and groups in your own identity source for use across all your AWS accounts and applications. For information about IAM Identity Center, see [What is IAM Identity Center?](#) in the *AWS IAM Identity Center User Guide*.

IAM users and groups

An [IAM user](#) is an identity within your AWS account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see [Rotate access keys regularly for use cases that require long-term credentials](#) in the *IAM User Guide*.

An [IAM group](#) is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. For more information, see [When to create an IAM user \(instead of a role\)](#) in the *IAM User Guide*.

IAM roles

An [IAM role](#) is an identity within your AWS account that has specific permissions. An IAM role is similar to an IAM user but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by [switching roles](#). You can assume a role by calling an AWS Command Line Interface (AWS CLI) or AWS API operation or by using a custom URL. For more information about methods for using roles, see [Using IAM roles](#) in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see [Creating a role for a third-party Identity Provider](#) in the *IAM User Guide*. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permissions sets, see [Permission sets](#) in the *AWS IAM Identity Center User Guide*.
- **Temporary IAM user permissions** – An IAM user can assume an IAM role to temporarily take on different permissions for a specific task.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). For more information about the difference between roles and resource-based policies for cross-account access, see [How IAM roles differ from resource-based policies](#) in the *IAM User Guide*.
- **Cross-service access** – Some AWS services use features in other AWS services. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
 - **Principal permissions** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions.

- **Service role** – 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 [Creating a role to delegate permissions to an AWS service](#) in the *IAM User Guide*.
- **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view but not edit the permissions for service-linked roles.
- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an Amazon EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the Amazon EC2 instance. To assign an IAM role to an Amazon EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the Amazon EC2 instance to get temporary credentials. For more information, see [Using an IAM role to grant permissions to applications running on Amazon EC2 instances](#) in the *IAM User Guide*.

For more information about whether to use IAM roles, see [When to create an IAM role \(instead of a user\)](#) in the *IAM User Guide*.

Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when a principal (user, root user, or role session) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see [Overview of JSON policies](#) in the *IAM User Guide*.

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**.

Every IAM entity (user or role) starts with no permissions. By default, users can do nothing, not even change their own password. To give a user permission to do something, an administrator must attach a permissions policy to a user. Or the administrator can add the user to a group that has the intended permissions. When an administrator gives permissions to a group, all users in that group are granted those permissions.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, role, or group. These policies control what actions users and roles can perform, on which resources, and under what conditions. For more information about how to create an identity-based policy, see [Creating IAM policies](#) in the *IAM User Guide*.

Identity-based policies can be further categorized as *inline policies* or *managed policies*. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. For more information about how to choose between a managed policy or an inline policy, see [Choosing between managed policies and inline policies](#) in the *IAM User Guide*.

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource such as an Amazon S3 bucket. Service administrators can use these policies to define what actions a specified principal (account member, user, or role) can perform on that resource and under what conditions. Resource-based policies are inline policies. There are no managed resource-based policies.

Access control lists (ACLs)

Access control lists (ACLs) are a type of policy that controls which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format. Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. For more information about ACLs, see [Access Control List \(ACL\) overview](#) in the *Amazon S3 User Guide*.

Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of an entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the Principal field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see [Permissions boundaries for IAM entities](#) in the *IAM User Guide*.
- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply SCPs to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see [How SCPs work](#) in the *AWS Organizations User Guide*.
- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see [Session policies](#) in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see [Policy evaluation logic](#) in the *IAM User Guide*.

How Amazon Q Developer works with IAM

Before you use IAM to manage access to Amazon Q Developer, learn what IAM features are available to use with Amazon Q Developer.

IAM features you can use with Amazon Q Developer

IAM feature	Amazon Q support
Identity-based policies	Yes

IAM feature	Amazon Q support
Resource-based policies	No
Policy actions	Yes
Policy resources	No
Policy condition keys	No
ACLs	No
ABAC (tags in policies)	No
Temporary credentials	Yes
Principal permissions	Yes
Service roles	No
Service-linked roles	Yes

To get a high-level view of how Amazon Q 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 Q

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 [Creating IAM 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. You can't specify the principal in an identity-based policy because it applies to the user or role to which it is attached. 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*.

Identity-based policy examples for Amazon Q

To view examples of Amazon Q Developer identity-based policies, see [Identity-based policy examples for Amazon Q Developer](#).

Resource-based policies within Amazon Q

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. Adding a cross-account principal to a resource-based policy is only half of establishing the trust relationship. When the principal and the resource are in different AWS accounts, an IAM administrator in the trusted account must also grant the principal entity (user or role) permission to access the resource. They grant permission by attaching an identity-based policy to the entity. However, if a resource-based policy grants access to a principal in the same account, no additional identity-based policy is required. For more information, see [Cross account resource access in IAM](#) in the *IAM User Guide*.

Policy actions for Amazon Q

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. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as *permission-only actions* that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called *dependent actions*.

Include actions in a policy to grant permissions to perform the associated operation.

To see a list of Amazon Q actions, see [Manage access to Amazon Q Developer with policies](#).

Policy actions in Amazon Q use the following prefix before the action:

q

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

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

You can specify multiple actions using wildcards (*). For example, to specify all actions that begin with the word Get, include the following action:

```
"Action": "q:Get*"
```

To view examples of Amazon Q Developer identity-based policies, see [Identity-based policy examples for Amazon Q Developer](#).

Policy resources for Amazon Q

Supports policy resources: No

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. Statements must include either a Resource or a NotResource element. As a best practice, specify a resource using its [Amazon Resource Name \(ARN\)](#). You can do this for actions that support a specific resource type, known as *resource-level permissions*.

For actions that don't support resource-level permissions, such as listing operations, use a wildcard (*) to indicate that the statement applies to all resources.

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

To view examples of Amazon Q Developer identity-based policies, see [Identity-based policy examples for Amazon Q Developer](#).

Policy condition keys for Amazon Q

Supports service-specific policy condition keys: No

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 (or Condition *block*) lets you specify conditions in which a statement is in effect. The Condition element is optional. 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.

If you specify multiple Condition elements in a statement, or multiple keys in a single Condition element, AWS evaluates them using a logical AND operation. If you specify multiple values for a single condition key, AWS evaluates the condition using a logical OR operation. All of the conditions must be met before the statement's permissions are granted.

You can also use placeholder variables when you specify conditions. For example, you can grant an IAM user permission to access a resource only if it is tagged with their IAM user name. For more information, see [IAM policy elements: variables and tags](#) in the *IAM User Guide*.

AWS supports global condition keys and service-specific condition keys. To see all AWS global condition keys, see [AWS global condition context keys](#) in the *IAM User Guide*.

To view examples of Amazon Q Developer identity-based policies, see [Identity-based policy examples for Amazon Q Developer](#).

ACLs in Amazon Q

Supports ACLs: No

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

ABAC with Amazon Q

Supports ABAC (tags in policies): No

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes. In AWS, these attributes are called *tags*. You can attach tags to IAM entities (users or roles) and to many AWS resources. Tagging entities and resources is the first step of ABAC. Then you design ABAC policies to allow operations when the principal's tag matches the tag on the resource that they are trying to access.

ABAC is helpful in environments that are growing rapidly and helps with situations where policy management becomes cumbersome.

To control access based on tags, you provide tag information in the [condition element](#) of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys.

If a service supports all three condition keys for every resource type, then the value is **Yes** for the service. If a service supports all three condition keys for only some resource types, then the value is **Partial**.

For more information about ABAC, see [What is ABAC?](#) in the *IAM User Guide*. To view a tutorial with steps for setting up ABAC, see [Use attribute-based access control \(ABAC\)](#) in the *IAM User Guide*.

Using temporary credentials with Amazon Q

Supports temporary credentials: Yes

Some AWS services don't work when you sign in using temporary credentials. For additional information, including which AWS services work with temporary credentials, see [AWS services that work with IAM](#) in the *IAM User Guide*.

You are using temporary credentials if you sign in to the AWS Management Console using any method except a user name and password. For example, when you access AWS using your company's single sign-on (SSO) link, that process automatically creates temporary credentials. You also automatically create temporary credentials when you sign in to the console as a user and then switch roles. For more information about switching roles, see [Switching to a role \(console\)](#) in the *IAM User Guide*.

You can manually create temporary credentials using the AWS CLI or AWS API. You can then use those temporary credentials to access AWS. AWS recommends that you dynamically generate

temporary credentials instead of using long-term access keys. For more information, see [Temporary security credentials in IAM](#).

Cross-service principal permissions for Amazon Q

Supports forward access sessions (FAS): Yes

When you use an IAM user or role to perform actions in AWS, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other AWS services or resources to complete. In this case, you must have permissions to perform both actions. For policy details when making FAS requests, see [Forward access sessions](#).

Service roles for Amazon Q

Supports service roles: No

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 [Creating 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 Q functionality. Edit service roles only when Amazon Q provides guidance to do so.

Service-linked roles for Amazon Q

Supports service-linked roles: Yes

A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

For details about creating or managing Amazon Q service-linked roles, see [Using service-linked roles for Amazon Q Developer and User Subscriptions](#).

Manage access to Amazon Q Developer with policies

Note

The information on this page pertains to accessing Amazon Q Developer. For information about managing access to Amazon Q Business, see [Identity-based policy examples for Amazon Q Business](#) in the *Amazon Q Business User Guide*.

The policies and examples in this topic are specific to Amazon Q in the AWS Management Console, AWS Console Mobile Application, AWS website, AWS Documentation, AWS Chatbot, and in IDEs. Other services integrated with Amazon Q might require different policies or settings. For more information, see the documentation for the service that contains an Amazon Q feature or integration.

By default, users and roles don't have permission to use Amazon Q. IAM administrators can manage access to Amazon Q Developer and its features by granting permissions to IAM identities.

The quickest way for an administrator to grant access to users is through an AWS managed policy. The `AmazonQFullAccess` policy can be attached to IAM identities to grant full access to Amazon Q Developer and its features. For more information about this policy, see [AWS managed policies for Amazon Q Developer](#).

To manage specific actions that IAM identities can perform with Amazon Q Developer, administrators can create custom policies that define what permissions a user, group, or role has. You can also use service control policies (SCPs) to control what Amazon Q features are available in your organization.

For a list of all Amazon Q permissions you can control with policies, see the [see the Amazon Q Developer permissions reference](#).

Topics

- [Policy best practices](#)
- [Assign permissions](#)
- [Manage access with service control policies \(SCPs\)](#)
- [Data perimeters for Amazon Q resources](#)
- [Identity-based policy examples for Amazon Q Developer](#)

Policy best practices

Identity-based policies determine whether someone can create, access, or delete Amazon Q Developer 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 AWS 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 [IAM Access Analyzer policy validation](#) 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 [Configuring MFA-protected API access](#) in the *IAM User Guide*.

For more information about best practices in IAM, see [Security best practices in IAM](#) in the *IAM User Guide*.

Assign permissions

To provide access, add permissions to your users, groups, or roles:

- Users and groups in AWS IAM Identity Center:

Create a permission set. Follow the instructions in [Create a permission set](#) in the *AWS IAM Identity Center User Guide*.

- Users managed in IAM through an identity provider:

Create a role for identity federation. Follow the instructions in [Creating a role for a third-party identity provider \(federation\)](#) in the *IAM User Guide*.

- IAM users:

- Create a role that your user can assume. Follow the instructions in [Creating a role for an IAM user](#) in the *IAM User Guide*.
- (Not recommended) Attach a policy directly to a user or add a user to a user group. Follow the instructions in [Adding permissions to a user \(console\)](#) in the *IAM User Guide*.

Manage access with service control policies (SCPs)

Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. You can control what Amazon Q Developer features are available in your organization by creating an SCP that specifies permissions for some or all Amazon Q actions.

For more information about using SCPs to control access in your organization, see [Creating, updating, and deleting service control policies](#) and [Attaching and detaching service control policies](#) in the *AWS Organizations User Guide*.

The following is an example of an SCP that denies access to Amazon Q. This policy restricts access to Amazon Q chat, console error troubleshooting, and network troubleshooting.

 **Note**

Denying access to Amazon Q will not disable the Amazon Q icon or chat panel in the AWS console, AWS website, AWS documentation pages, or AWS Console Mobile Application.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "DenyAmazonQFullAccess",  
      "Effect": "Deny",  
      "Action": [  
        "q:*"  
      ],  
      "Resource": "*"  
    }  
  ]  
}
```

Data perimeters for Amazon Q resources

For some features, Amazon Q uploads artifacts to AWS service-owned Amazon S3 buckets. If you are using data perimeters to control access to Amazon S3 in your environment, you might need to explicitly allow access to these buckets to use the corresponding Amazon Q features.

The following table lists the ARN and URL of each of the Amazon S3 buckets that Amazon Q requires access to, and the features that use each bucket. You can use the bucket ARN or bucket URL to allowlist these buckets, depending on how you control access to Amazon S3.

Amazon S3 bucket ARN	Amazon S3 bucket URL	Description
<code>arn:aws:s3:::amazonq-code-scan-us-east-1-29121b44f7b</code>	<code>https://amazonq-code-scan-us-east-1-29121b44f7b.s3.amazonaws.com/</code>	An Amazon S3 bucket used to upload artifacts for Amazon Q code scans
<code>arn:aws:s3:::amazonq-code-transformation-us-east-1-c6160f047e0</code>	<code>https://amazonq-code-transformation-us-east-1-c6160f047e0.s3.amazonaws.com/</code>	An Amazon S3 bucket used to upload artifacts for the Amazon Q Developer Agent for code transformation

Amazon S3 bucket ARN	Amazon S3 bucket URL	Description
arn:aws:s3:::amazonq-feature-development-us-east-1-a5b980054c6	https://amazonq-feature-development-us-east-1-a5b980054c6.s3.amazonaws.com/	An Amazon S3 bucket used to upload artifacts for the Amazon Q Developer Agent for software development

Identity-based policy examples for Amazon Q Developer

The following example IAM policies control permissions for various Amazon Q Developer actions. Use them to allow or deny Amazon Q Developer access for your users, roles, or groups.

For a list of all Amazon Q permissions you can control with policies, see the [Amazon Q Developer permissions reference](#).

Note

The following example policies grant permissions for features of Amazon Q Developer, but users might need additional permissions to access Amazon Q with an Amazon Q Developer Pro subscription. For more information, see [Allow users to access Amazon Q with an Amazon Q Developer Pro subscription](#).

You can use the policies below as written, or you can add permissions for the individual Amazon Q features you want to use. For examples of policies you can create to allow access to specific features, see [Identity-based policy examples for Amazon Q Developer](#).

For more information about configuring IAM permissions with Amazon Q, see [Manage access to Amazon Q Developer with policies](#).

For more information about what these permissions do, see the [Amazon Q Developer permissions reference](#).

Allow an administrator to use the Amazon Q service management console

The following policy empowers a user to use the Amazon Q service management console. This is the console where you configure Amazon Q's integration with IAM Identity Center and AWS Organizations, and where you choose which Amazon Q package to subscribe to.

To fully set up your Amazon Q Pro subscription, someone in your enterprise will also need access to the Amazon Q Pro console. For more information, see [Assigning permissions to use the Amazon Q Developer Pro console](#).

Note

The codewhisperer prefix is a legacy name from a service that merged with Amazon Q Developer. For more information, see [Amazon Q Developer rename - Summary of changes](#).

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "organizations>ListAWSAccessForOrganization",  
        "organizations>DisableAWSAccess",  
        "organizations>EnableAWSAccess",  
        "organizations>DescribeOrganization"  
      ],  
      "Resource": [  
        "*"  
      ]  
    },  
    {  
      "Effect": "Allow",  
      "Action": [  
        "sso>ListApplications",  
        "sso>ListInstances",  
        "sso>DescribeRegisteredRegions",  
        "sso>GetSharedSsoConfiguration",  
        "sso>DescribeInstance",  
        "sso>CreateApplication",  
        "sso>PutApplicationAuthenticationMethod",  
        "sso>PutApplicationAssignmentConfiguration",  
        "sso>PutApplicationAssignmentConfiguration"  
      ]  
    }  
  ]  
}
```

```
    "sso:PutApplicationGrant",
    "sso:PutApplicationAccessScope",
    "sso:DescribeApplication",
    "sso:DeleteApplication",
    "sso:GetSSOStatus",
    "sso>CreateApplicationAssignment",
    "sso>DeleteApplicationAssignment"
],
"Resource": [
    "*"
]
},
{
    "Effect": "Allow",
    "Action": [
        "sso-directory:DescribeUsers",
        "sso-directory:DescribeGroups",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers",
        "sso-directory:DescribeGroup",
        "sso-directory:DescribeUser",
        "sso-directory:DescribeDirectory"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "signin>ListTrustedIdentityPropagationApplicationsForConsole",
        "signin>CreateTrustedIdentityPropagationApplicationForConsole"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "codewhisperer>ListProfiles",
        "codewhisperer>CreateProfile",
        "codewhisperer>DeleteProfile"
    ],
    "Resource": [
        "*"
    ]
}
```

```
"Resource": [
    "*"
],
},
{
    "Effect": "Allow",
    "Action": [
        "user-subscriptions>ListClaims",
        "user-subscriptions>ListUserSubscriptions",
        "user-subscriptions>CreateClaim",
        "user-subscriptions>DeleteClaim",
        "user-subscriptions>UpdateClaim"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "q>CreateAssignment",
        "q>DeleteAssignment"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "iam>CreateServiceLinkedRole"
    ],
    "Resource": [
        "arn:aws:iam::*:role/aws-service-role/user-subscriptions.amazonaws.com/
AWSServiceRoleForUserSubscriptions"
    ]
}
]
```

Allow an administrator to configure the Amazon Q Developer Pro console

The following policy empowers a user to access the Amazon Q Developer Pro console. On that console, you can attach users and groups to subscriptions, and configure various aspects of Amazon Q Developer relating to specific features, such as code references.

To fully set up your Amazon Q Pro subscription, someone in your enterprise will also need access to the Amazon Q service management console. For more information, see [Allow an administrator to use the Amazon Q service management console](#).

Note

The `codewhisperer` prefix is a legacy name from a service that merged with Amazon Q Developer. For more information, see [Amazon Q Developer rename - Summary of changes](#).

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "sso-directory:GetUserPoolInfo"  
      ],  
      "Resource": [  
        "*"  
      ]  
    },  
    {  
      "Effect": "Allow",  
      "Action": [  
        "iam>ListRoles"  
      ],  
      "Resource": [  
        "*"  
      ]  
    },  
    {  
      "Effect": "Allow",  
      "Action": [  
        "sso:DescribeRegisteredRegions",  
        "sso:GetSSOStatus"  
      ]  
    }  
  ]  
}
```

```
],
  "Resource": [
    "*"
  ],
},
{
  "Effect": "Allow",
  "Action": [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization"
  ],
  "Resource": [
    "*"
  ],
},
{
  "Effect": "Allow",
  "Action": [
    "kms>ListAliases",
    "kms>CreateGrant",
    "kms>Encrypt",
    "kms>Decrypt",
    "kms>GenerateDataKey*",
    "kms>RetireGrant",
    "kms>DescribeKey"
  ],
  "Resource": [
    "*"
  ],
},
{
  "Effect": "Allow",
  "Action": [
    "codeguru-security:UpdateAccountConfiguration"
  ],
  "Resource": [
    "*"
  ],
},
{
  "Effect": "Allow",
  "Action": [
    "iam>CreateServiceLinkedRole"
  ],
}
```

```
"Resource": [
    "arn:aws:iam::*:role/aws-service-role/q.amazonaws.com/
AWSServiceRoleForAmazonQDeveloper"
]
},
{
    "Effect": "Allow",
    "Action": [
        "codewhisperer:UpdateProfile",
        "codewhisperer>ListProfiles",
        "codewhisperer:TagResource",
        "codewhisperer:UnTagResource",
        "codewhisperer>ListTagsForResource",
        "codewhisperer>CreateProfile"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "cloudwatch:GetMetricData",
        "cloudwatch>ListMetrics"
    ],
    "Resource": [
        "*"
    ]
}
]
```

For legacy Amazon CodeWhisperer profiles, the following policy will enable an IAM principal to administer a CodeWhisperer application.

 **Note**

The `codewhisperer` prefix is a legacy name from a service that merged with Amazon Q Developer. For more information, see [Amazon Q Developer rename - Summary of changes](#).

{

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "sso-directory:SearchUsers",
      "sso-directory:SearchGroups",
      "sso-directory:GetUserPoolInfo",
      "sso-directory:DescribeDirectory",
      "sso-directory>ListMembersInGroup"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam>ListRoles"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "pricing:GetProducts"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "sso:AssociateProfile",
      "sso:DisassociateProfile",
      "sso:GetProfile",
      "sso>ListProfiles",
      "sso>ListApplicationInstances",
      "sso:GetApplicationInstance",
      "sso>CreateManagedApplicationInstance",
      "sso:GetManagedApplicationInstance",
      "sso:DeleteManagedApplicationInstance"
    ]
  }
]
```

```
    "sso>ListProfileAssociations",
    "sso:GetSharedSsoConfiguration",
    "sso>ListDirectoryAssociations",
    "sso:DescribeRegisteredRegions",
    "sso:GetSsoConfiguration",
    "sso:GetSSOStatus"
],
"Resource": [
    "*"
]
},
{
    "Effect": "Allow",
    "Action": [
        "identitystore>ListUsers",
        "identitystore>ListGroups"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "organizations>DescribeAccount",
        "organizations>DescribeOrganization"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "kms>ListAliases",
        "kms>CreateGrant",
        "kms>Encrypt",
        "kms>Decrypt",
        "kms>GenerateDataKey*",
        "kms>RetireGrant",
        "kms>DescribeKey"
    ],
    "Resource": [
        "*"
    ]
}
```

```
        ],
    },
{
    "Effect": "Allow",
    "Action": [
        "codeguru-security:UpdateAccountConfiguration"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": [
        "arn:aws:iam::*:role/aws-service-role/q.amazonaws.com/
AWSServiceRoleForAmazonQDeveloper"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "codewhisperer:UpdateProfile",
        "codewhisperer>ListProfiles",
        "codewhisperer:TagResource",
        "codewhisperer:UnTagResource",
        "codewhisperer>ListTagsForResource",
        "codewhisperer>CreateProfile"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "cloudwatch:GetMetricData",
        "cloudwatch>ListMetrics"
    ],
    "Resource": [
        "*"
    ]
}
```

```
    }  
]  
}
```

Note

If you are using Customizations, then your Amazon Q Developer administrator will require additional permissions. For more information, see [Prerequisites for customizations](#).

To learn more about IAM policies, see [Access Management](#) in the *IAM User Guide*.

Add IAM permissions for Amazon Q on AWS websites

To use Amazon Q Developer features on AWS apps and websites, you must attach the appropriate AWS Identity and Access Management (IAM) permissions. Following is an example policy you can use to access most Amazon Q features on AWS apps and websites:

Note

The availability of Amazon Q features depends on the environment where you use Amazon Q. See the topic for the feature you want to use for more information about where you can access it and the specific permissions you need to use it.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "q:SendMessage",  
        "q:StartConversation",  
        "q:GetConversation",  
        "q>ListConversations",  
        "q:GetIdentityMetaData",  
        "q:StartTroubleshootingAnalysis",  
        "q:GetTroubleshootingResults",  
        "q:StartTroubleshootingResolutionExplanation",  
        "q:UpdateTroubleshootingCommandResult",  
      ]  
    }  
  ]  
}
```

```
    "q:PassRequest"
],
"Resource": [
  "*"
]
},
{
  "Effect": "Allow",
  "Action": [
    "ce:GetCostAndUsage"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "sts:setContext"
  ],
  "Resource": [
    "arn:aws:sts::*:self"
  ]
}
]
```

Allow users to access Amazon Q with an Amazon Q Developer Pro subscription

The following example policy grants permission to use Amazon Q with an Amazon Q Developer Pro subscription. Without these permissions, users can only access the Free Tier of Amazon Q. To chat with Amazon Q or use other Amazon Q features, users need additional permissions, such as those granted by the example policies in this section.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowGetIdentity",
      "Effect": "Allow",
      "Action": [
        "lambda:InvokeFunction"
      ],
      "Resource": [
        "arn:aws:lambda:us-east-1:123456789012:function:chatbot"
      ]
    }
  ]
}
```

```
        "q:GetIdentityMetaData"
    ],
    "Resource": "*"
},
{
    "Sid": "AllowSetTrustedIdentity",
    "Effect": "Allow",
    "Action": [
        "sts:SetContext"
    ],
    "Resource": "arn:aws:sts::*:self"
}
]
}
```

Allow users to chat with Amazon Q

The following example policy grants permissions to chat with Amazon Q in the console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAmazonQConversationAccess",
            "Effect": "Allow",
            "Action": [
                "q:StartConversation",
                "q:SendMessage",
                "q:GetConversation",
                "q>ListConversations"
            ],
            "Resource": "*"
        }
    ]
}
```

Allow users to diagnose console errors with Amazon Q

The following example policy grants permissions to diagnose console errors with Amazon Q.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
{  
    "Sid": "AllowAmazonQTroubleshooting",  
    "Effect": "Allow",  
    "Action": [  
        "q:StartTroubleshootingAnalysis",  
        "q:GetTroubleshootingResults",  
        "q:StartTroubleshootingResolutionExplanation",  
        "q:UpdateTroubleshootingCommandResult"  
    ],  
    "Resource": "*"  
}  
]  
}
```

Allow Amazon Q to perform actions on your behalf

The following example policy grants permission to chat with Amazon Q, and allows Amazon Q to perform actions on your behalf. Amazon Q only has permission to perform actions that your IAM identity has permission to perform.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowAmazonQPassRequest",  
            "Effect": "Allow",  
            "Action": [  
                "q:StartConversation",  
                "q:SendMessage",  
                "q:GetConversation",  
                "q>ListConversations",  
                "q:PassRequest"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

Deny Amazon Q permission to perform specific actions on your behalf

The following example policy grants permission to chat with Amazon Q, and allows Amazon Q to perform any action on your behalf that your IAM identity has permission to perform, except for

Amazon EC2 actions. This policy uses the [aws:CalledVia global condition key](#) to specify that Amazon EC2 actions are only denied when Amazon Q calls them.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "q:StartConversation",  
                "q:SendMessage",  
                "q:GetConversation",  
                "q>ListConversations",  
                "q:PassRequest"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Deny",  
            "Action": [  
                "ec2:*"  
            ],  
            "Resource": "*",  
            "Condition": {  
                "ForAnyValue:StringEquals": {  
                    "aws:CalledVia": ["q.amazonaws.com"]  
                }  
            }  
        }  
    ]  
}
```

Allow Amazon Q permission to perform specific actions on your behalf

The following example policy grants permission to chat with Amazon Q, and allows Amazon Q to perform any action on your behalf that your IAM identity has permission to perform, with the exception of Amazon EC2 actions. This policy grants your IAM identity permission to perform any Amazon EC2 action, but only allows Amazon Q to perform the ec2:describeInstances action. This policy uses the [aws:CalledVia global condition key](#) to specify that Amazon Q is only allowed to call ec2:describeInstances, and not any other Amazon EC2 actions.

```
{
```

```
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "q:StartConversation",
            "q:SendMessage",
            "q:GetConversation",
            "q>ListConversations",
            "q:PassRequest"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:)"
        ],
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringNotEquals": {
                "aws:CalledVia": ["q.amazonaws.com"]
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:describeInstances"
        ],
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:CalledVia": ["q.amazonaws.com"]
            }
        }
    }
]
```

Allow Amazon Q permission to perform actions on your behalf in specific regions

The following example policy grants permission to chat with Amazon Q, and allows Amazon Q to make calls to only the us-east-1 and us-west-2 Regions when performing actions on your behalf. Amazon Q can't make calls to any other Region. For more information on how to specify what Regions you can make calls to, see [aws:RequestedRegion](#) in the *AWS Identity and Access Management User Guide*.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "q:StartConversation",  
                "q:SendMessage",  
                "q:GetConversation",  
                "q>ListConversations",  
                "q:PassRequest"  
            ],  
            "Resource": "*",  
            "Condition": {  
                "StringEquals": {  
                    "aws:RequestedRegion": [  
                        "us-east-1",  
                        "us-west-2"  
                    ]  
                }  
            }  
        }  
    ]  
}
```

Deny Amazon Q permission to perform actions on your behalf

The following example policy prevents Amazon Q from performing actions on your behalf.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "DenyAmazonQPassRequest",  
            "Effect": "Deny",  
            "Action": "q:PassRequest",  
            "Resource": "*"  
        }  
    ]  
}
```

```
        "Effect": "Deny",
        "Action": [
            "q:PassRequest"
        ],
        "Resource": "*"
    }
]
}
```

Deny access to Amazon Q

The following example policy denies all permissions to use Amazon Q.

Note

Denying access to Amazon Q will not disable the Amazon Q icon or chat panel in the AWS console, AWS website, AWS documentation pages, or AWS Console Mobile Application.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAmazonQFullAccess",
            "Effect": "Deny",
            "Action": [
                "q:/*"
            ],
            "Resource": "*"
        }
    ]
}
```

Allow users to view their permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```
{
    "Version": "2012-10-17",
```

```
"Statement": [
    {
        "Sid": "ViewOwnUserInfo",
        "Effect": "Allow",
        "Action": [
            "iam:GetUserPolicy",
            "iam>ListGroupsForUser",
            "iam>ListAttachedUserPolicies",
            "iam>ListUserPolicies",
            "iam GetUser"
        ],
        "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
        "Sid": "NavigateInConsole",
        "Effect": "Allow",
        "Action": [
            "iam:GetGroupPolicy",
            "iam:GetPolicyVersion",
            "iam GetPolicy",
            "iam>ListAttachedGroupPolicies",
            "iam>ListGroupPolicies",
            "iam>ListPolicyVersions",
            "iam>ListPolicies",
            "iam>ListUsers"
        ],
        "Resource": "*"
    }
]
```

Amazon Q Developer permissions reference

Amazon Q Developer uses two types of APIs to provide the service:

- User and administrator permissions, which can be used in policies to control usage of Amazon Q
- Other APIs used to provide the service, which can't be used in policies to control usage of Amazon Q

This section provides information about the APIs used by Amazon Q Developer, and what they do.

Topics

- [Amazon Q Developer permissions](#)
- [Amazon Q User Subscriptions permissions](#)
- [Other Amazon Q Developer APIs](#)

Amazon Q Developer permissions

You can use the following permissions as a reference when you are setting up [Authenticating with identities in Amazon Q](#) and writing permissions policies that you can attach to an IAM identity (identity-based policies).

The following table shows the Amazon Q Developer permissions that you can allow or deny access to in policies.

Important

To chat with Amazon Q, an IAM identity needs permissions for the following actions:

- StartConversation
- SendMessage
- GetConversation (console only)
- ListConversations (console only)

If one of these actions isn't explicitly allowed by an attached policy, an IAM permissions error is returned when you try to chat with Amazon Q.

Note

The `codewhisperer` prefix is a legacy name from a service that merged with Amazon Q Developer. For more information, see [Amazon Q Developer rename - Summary of changes](#).

Using q:PassRequest

`q:PassRequest` is an Amazon Q permission that allows Amazon Q to call AWS APIs on your behalf. When you add the `q:PassRequest` permission to an IAM identity, Amazon Q gains permission to call any API that the IAM identity has permission to call. For example, if an IAM role

has the `s3>ListAllMyBuckets` permission and the `q:PassRequest` permission, Amazon Q is able to call the `ListAllMyBuckets` API when a user assuming that IAM role asks Amazon Q to list their Amazon S3 buckets.

You can create IAM policies that restrict the scope of the `q:PassRequest` permission. For example, you can prevent Amazon Q from performing a specific action, or only permit Amazon Q to perform a subset of actions for a service. You can also specify what regions Amazon Q can make calls to when performing actions on your behalf.

For examples of IAM policies that control the use of `q:PassRequest`, see the following identity-based policy examples:

- [Allow Amazon Q to perform actions on your behalf](#)
- [Deny Amazon Q permission to perform specific actions on your behalf](#)
- [Allow Amazon Q permission to perform specific actions on your behalf](#)
- [Allow Amazon Q permission to perform actions on your behalf in specific regions](#)
- [Deny Amazon Q permission to perform actions on your behalf](#)

Amazon Q User Subscriptions permissions

Amazon Q Developer administrators must have the following permissions to create and manage subscriptions for users and groups in their organization.

The following terminology is useful in understanding what subscriptions permissions do:

User

An individual user, represented within AWS IAM Identity Center by a unique user ID.

Group

A collection of users, represented within AWS IAM Identity Center by a unique group ID.

Subscription

A subscription is tied to a single Identity Center user, and entitles them to use Amazon Q features. A subscription does not authorize a user to use Amazon Q features. For example, if Adam is subscribed to Amazon Q Developer Pro, they are entitled to use Amazon Q Developer features, but they don't have access to those features until their administrator grants them the needed permissions.

Other Amazon Q Developer APIs

The following table shows the APIs that are used by features of Amazon Q in the IDE. These APIs aren't used to control access to features of Amazon Q, but they will appear in AWS CloudTrail logs in management accounts when users access the associated feature.

 **Note**

The `codewhisperer` prefix is a legacy name from a service that merged with Amazon Q Developer. For more information, see [Amazon Q Developer rename - Summary of changes](#).

AWS managed policies for Amazon Q Developer

An AWS managed policy is a standalone policy that is created and administered by AWS. AWS managed policies are designed to provide permissions for many common use cases so that you can start assigning permissions to users, groups, and roles.

The quickest way for an administrator to grant access to users is through an AWS managed policy. The following AWS managed policies for Amazon Q Developer can be attached to IAM identities:

- `AmazonQFullAccess` provides full access to enable interactions with Amazon Q Developer, including administrator access.
- `AmazonQDeveloperAccess` provides full access to enable interactions with Amazon Q Developer, without administrator access.

Keep in mind that AWS managed policies might not grant least-privilege permissions for your specific use cases because they're available for all AWS customers to use. We recommend that you reduce permissions further by defining [customer managed policies](#) that are specific to your use cases.

You cannot change the permissions defined in AWS managed policies. If AWS updates the permissions defined in an AWS managed policy, the update affects all principal identities (users, groups, and roles) that the policy is attached to. AWS is most likely to update an AWS managed policy when a new AWS service is launched or new API operations become available for existing services.

For more information, see [AWS managed policies](#) in the *IAM User Guide*.

AmazonQFullAccess

The AmazonQFullAccess managed policy provides administrator access to enable users in your organization to access Amazon Q Developer. It also provides full access to enable interactions with Amazon Q Developer, including logging in with IAM Identity Center to access Amazon Q through an Amazon Q Developer Pro subscription.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowAmazonQFullAccess",  
            "Effect": "Allow",  
            "Action": [  
                "q:StartConversation",  
                "q:SendMessage",  
                "q:GetConversation",  
                "q>ListConversations",  
                "q:PassRequest",  
                "q:StartTroubleshootingAnalysis",  
                "q:GetTroubleshootingResults",  
                "q:StartTroubleshootingResolutionExplanation",  
                "q:UpdateTroubleshootingCommandResult",  
                "q:GetIdentityMetadata",  
                "q>CreateAssignment",  
                "q>DeleteAssignment"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Sid": "AllowCloudControlReadAccess",  
            "Effect": "Allow",  
            "Action": [  
                "cloudformation:GetResource",  
                "cloudformation>ListResources"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Sid": "AllowSetTrustedIdentity",  
            "Effect": "Allow",  
            "Action": [  
                "sts:SetContext"  
            ]  
        }  
    ]  
}
```

```
        ],
        "Resource": "arn:aws:sts::*:self"
    }
]
}
```

AmazonQDeveloperAccess

The AmazonQDeveloperAccess managed policy provides full access to enable interactions with Amazon Q Developer, without administrator access. It includes access to log in with IAM Identity Center to access Amazon Q through an Amazon Q Developer Pro subscription.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAmazonQDeveloperAccess",
            "Effect": "Allow",
            "Action": [
                "q:StartConversation",
                "q:SendMessage",
                "q:GetConversation",
                "q>ListConversations",
                "q:PassRequest",
                "q:StartTroubleshootingAnalysis",
                "q:StartTroubleshootingResolutionExplanation",
                "q:GetTroubleshootingResults",
                "q:UpdateTroubleshootingCommandResult",
                "q:GetIdentityMetaData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowCloudControlReadAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:GetResource",
                "cloudformation>ListResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowSetTrustedIdentity",
            "Effect": "Allow",
            "Action": [
                "cloudformation:SetTrustedIdentity"
            ],
            "Resource": "*"
        }
    ]
}
```

```
"Effect": "Allow",
"Action": [
    "sts:SetContext"
],
"Resource": "arn:aws:sts::*:self"
}
]
}
```

AWSServiceRoleForAmazonQDeveloperPolicy

This AWS managed policy grants permissions commonly needed to use Amazon Q Developer. The policy is added to the AWSServiceRoleForAmazonQDeveloper service linked role that is created when you onboard to Amazon Q.

You can't attach AWSServiceRoleForAmazonQDeveloperPolicy to your IAM entities. This policy is attached to [a service-linked role](#) that allows Amazon Q to perform actions on your behalf. For more information, see [Using service-linked roles for Amazon Q Developer and User Subscriptions](#).

This policy grants **administrator** permissions that allows metrics to be published for Billing / Usage.

Permissions details

This policy includes the following permissions.

- **cloudwatch** – Allows principals to publish usage metrics to CloudWatch for Billing / Usage. This is required so that you can track your usage of Amazon Q in CloudWatch.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {

```

```
        "StringEquals": {
            "cloudwatch:namespace": [
                "AWS/Q"
            ]
        }
    }
]
```

To view this policy in the context of other AWS managed policies, see [AmazonQDeveloperPolicy](#).

AWSServiceRoleForUserSubscriptionPolicy

This AWS managed policy grants permissions commonly needed to use Amazon Q Developer. The policy is added to the AWSServiceRoleForUserSubscriptions service-linked role that is created when you create Amazon Q subscriptions.

You can't attach AWSServiceRoleForUserSubscriptionPolicy to your IAM entities. This policy is attached to [a service-linked role](#) that allows Amazon Q to perform actions on your behalf. For more information, see [Using service-linked roles for Amazon Q Developer and User Subscriptions](#).

This policy provides access for Amazon Q Subscriptions to your Identity Center resources to automatically update your subscriptions.

Permissions details

This policy includes the following permissions.

- **identitystore** – Allows principals to track Identity Center directory changes so that subscriptions can be automatically updated.
organizations – Allows principals to track AWS Organizations changes so that subscriptions can be automatically updated.
sso – Allows principals to track Identity Center instance changes so that subscriptions can be automatically updated.

{

```
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "identitystore:DescribeGroup",
            "identitystore:DescribeUser",
            "identitystore:IsMemberInGroups",
            "identitystore>ListGroupMemberships",
            "organizations:DescribeOrganization",
            "sso:DescribeApplication",
            "sso:DescribeInstance",
            "sso>ListInstances"
        ],
        "Resource": "*"
    }
]
```

To view this policy in the context of other AWS managed policies, see [AWS Service Role for User Subscription Policy](#).

Policy updates

View details about updates to AWS managed policies for Amazon Q Developer since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the [Document history for Amazon Q Developer User Guide](#) page.

Change	Description	Date
AmazonQFullAccess - Updated policy	Additional permissions have been added to enable Amazon Q to access downstream resources.	July 9, 2024
AmazonQDeveloperAccess - New policy	Provides full access to enable interactions with Amazon Q Developer, without administrator access.	July 9, 2024
AmazonQFullAccess - Updated policy	Additional permissions have been added to enable subscriptions checks for Amazon Q Developer.	April 30, 2024

Change	Description	Date
<u>AWSservic eRoleForU serSubscr ptionPolicy</u> - New policy	Allows Amazon Q Subscriptions to automatically update subscriptions from changes in AWS IAM Identity Center, AWS IAM Identity Center directory and AWS Organizations on your behalf.	April 30, 2024
<u>AWSservic eRoleForA mazonQDev eloperPolicy</u> - New policy	Allows Amazon Q to call Amazon CloudWatch and Amazon CodeGuru on your behalf.	April 30, 2024
<u>AmazonQFu llAccess</u> - New policy	Provides full access to enable interactions with Amazon Q Developer.	November 28, 2023
Amazon Q Developer started tracking changes	Amazon Q Developer started tracking changes to AWS managed policies.	November 28, 2023

Using service-linked roles for Amazon Q Developer and User Subscriptions

Amazon Q Developer uses AWS Identity and Access Management (IAM) [service-linked roles](#). A service-linked role is a unique type of IAM role that is linked directly to Amazon Q Developer. Service-linked roles are predefined by Amazon Q Developer and include all the permissions that the service requires to call other AWS services on your behalf.

Topics

- [Using service-linked roles for Amazon Q Developer](#)
- [Using service-linked-roles for User Subscriptions](#)

Using service-linked roles for Amazon Q Developer

Amazon Q Developer uses AWS Identity and Access Management (IAM) [service-linked roles](#). A service-linked role is a unique type of IAM role that is linked directly to Amazon Q Developer. Service-linked roles are predefined by Amazon Q Developer and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Amazon Q Developer easier because you don't have to manually add the necessary permissions. Amazon Q Developer defines the permissions of its service-linked roles, and unless defined otherwise, only Amazon Q Developer can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting their related resources. This protects your Amazon Q Developer resources because you can't inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see [AWS services that work with IAM](#) and look for the services that have **Yes** in the **Service-linked roles** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Learn about [AWS managed policies for Amazon Q Developer](#).

Service-linked role permissions for Amazon Q Developer

Amazon Q Developer uses the service-linked role named **AWSServiceRoleForAmazonQDeveloper** – This role grants permissions to Amazon Q to access data in your account to calculate billing, provides access to create and access security reports in Amazon CodeGuru, and emit data to CloudWatch.

The AWSServiceRoleForAmazonQDeveloper service-linked role trusts the following services to assume the role:

- q.amazonaws.com

The role permissions policy named **AWSServiceRoleForAmazonQDeveloperPolicy** allows Amazon Q Developer to complete the following actions on the specified resources:

- Action: `cloudwatch:PutMetricData` on AWS/Q CloudWatch namespace

You must configure permissions to allow your users, groups, or roles to create, edit, or delete a service-linked role. For more information, see [Service-linked role permissions](#) in the *IAM User Guide*.

Creating a service-linked role for Amazon Q Developer

You don't need to manually create a service-linked role. When you create a profile for Amazon Q in the AWS Management Console, Amazon Q Developer creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you update the settings, Amazon Q creates the service-linked role for you again.

You can also use the IAM console or AWS CLI to create a service-linked role with the `q.amazonaws.com` service name. For more information, see [Creating a service-linked role](#) in the *IAM User Guide*. If you delete this service-linked role, you can use this same process to create the role again.

Editing a service-linked role for Amazon Q Developer

Amazon Q Developer does not allow you to edit the `AWSServiceRoleForAmazonQDeveloper` service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see [Editing a service-linked role](#) in the *IAM User Guide*.

Deleting a service-linked role for Amazon Q Developer

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it.

Note

If the Amazon Q Developer service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS CLI, or the AWS API to delete the AWSServiceRoleForAmazonQDeveloper service-linked role. For more information, see [Deleting a service-linked role](#) in the *IAM User Guide*.

Supported Regions for Amazon Q Developer service-linked roles

Amazon Q Developer does not support using service-linked roles in every Region where the service is available. You can use the AWSServiceRoleForAmazonQDeveloper role in the following Regions. For more information, see [AWS Regions and endpoints](#).

Region name	Region identity	Support in Amazon Q Developer
US East (N. Virginia)	us-east-1	Yes
US East (Ohio)	us-east-2	No
US West (N. California)	us-west-1	No
US West (Oregon)	us-west-2	No
Africa (Cape Town)	af-south-1	No
Asia Pacific (Hong Kong)	ap-east-1	No
Asia Pacific (Jakarta)	ap-southeast-3	No
Asia Pacific (Mumbai)	ap-south-1	No
Asia Pacific (Osaka)	ap-northeast-3	No
Asia Pacific (Seoul)	ap-northeast-2	No
Asia Pacific (Singapore)	ap-southeast-1	No
Asia Pacific (Sydney)	ap-southeast-2	No
Asia Pacific (Tokyo)	ap-northeast-1	No
Canada (Central)	ca-central-1	No

Region name	Region identity	Support in Amazon Q Developer
Europe (Frankfurt)	eu-central-1	No
Europe (Ireland)	eu-west-1	No
Europe (London)	eu-west-2	No
Europe (Milan)	eu-south-1	No
Europe (Paris)	eu-west-3	No
Europe (Stockholm)	eu-north-1	No
Middle East (Bahrain)	me-south-1	No
Middle East (UAE)	me-central-1	No
South America (São Paulo)	sa-east-1	No
AWS GovCloud (US-East)	us-gov-east-1	No
AWS GovCloud (US-West)	us-gov-west-1	No

Using service-linked-roles for User Subscriptions

User Subscriptions uses AWS Identity and Access Management (IAM) [service-linked roles](#). A service-linked role is a unique type of IAM role that is linked directly to User Subscriptions. Service-linked roles are predefined by User Subscriptions and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up User Subscriptions easier because you don't have to manually add the necessary permissions. User Subscriptions defines the permissions of its service-linked roles, and unless defined otherwise, only User Subscriptions can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting their related resources. This protects your User Subscriptions because you can't inadvertently remove permissions required by the resources.

For information about other services that support service-linked roles, see [AWS services that work with IAM](#) and look for the services that have **Yes** in the **Service-linked roles** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for User Subscriptions

User Subscriptions uses the service-linked role named **AWSServiceRoleForUserSubscriptions**

- Provides access for User Subscriptions to your IAM Identity Center resources to automatically update your subscriptions.

The AWSServiceRoleForUserSubscriptions service-linked role trusts the following services to assume the role:

- `user-subscriptions.amazonaws.com`

The role permissions policy named AWSServiceRoleForUserSubscriptionPolicy allows User Subscriptions to complete the following actions on the specified resources:

- Action: `identitystore:DescribeGroup` on *
- Action: `identitystore:DescribeUser` on *
- Action: `identitystore:IsMemberInGroups` on *
- Action: `identitystore>ListGroupMemberships` on *
- Action: `organizations:DescribeOrganization` on *
- Action: `sso:DescribeApplication` on *
- Action: `sso:DescribeInstance` on *
- Action: `sso>ListInstances` on *

You must configure permissions to allow your users, groups, or roles to create, edit, or delete a service-linked role. For more information, see [Service-linked role permissions](#) in the *IAM User Guide*.

Creating a service-linked role for User Subscriptions

You don't need to manually create a service-linked role. When you create a User Subscription in the AWS Management Console, User Subscriptions creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you update the settings, User Subscriptions creates the service-linked role for you again.

You can also use the IAM console or AWS CLI to create a service-linked role with the `q.amazonaws.com` service name. For more information, see [Creating a service-linked role](#) in the *IAM User Guide*. If you delete this service-linked role, you can use this same process to create the role again.

Editing a service-linked role for User Subscriptions

User Subscriptions does not allow you to edit the `AWSServiceRoleForUserSubscriptions` service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see [Editing a service-linked role](#) in the *IAM User Guide*.

Deleting a service-linked role for User Subscriptions

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it.

Note

If the User Subscriptions service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS CLI, or the AWS API to delete the `AWSServiceRoleForUserSubscriptions` service-linked role. For more information, see [Deleting a service-linked role](#) in the *IAM User Guide*.

Supported Regions for User Subscriptions service-linked roles

Amazon Q Developer Subscriptions supports using service-linked roles in all of the Regions where the service is available. For more information, see [AWS Regions and endpoints](#).

Amazon Q Developer Subscriptions does not support using service-linked roles in every Region where the service is available. You can use the AWSServiceRoleForUserSubscriptions role in the following Regions.

Region name	Region identity	Support in User Subscriptions
US East (N. Virginia)	us-east-1	Yes
US West (Oregon)	us-west-2	Yes
US East (N. Virginia)	us-east-1	Yes
US East (Ohio)	us-east-2	Yes
US East (Ohio)	us-east-2	Yes
US West (N. California)	us-west-1	Yes
Asia Pacific (Mumbai)	ap-south-1	Yes
Asia Pacific (Osaka)	ap-northeast-3	Yes
Asia Pacific (Seoul)	ap-northeast-2	Yes
Asia Pacific (Singapore)	ap-southeast-1	Yes
Asia Pacific (Sydney)	ap-southeast-2	Yes
Asia Pacific (Tokyo)	ap-northeast-1	Yes
Canada (Central)	ca-central-1	Yes
Europe (Frankfurt)	eu-central-1	Yes
Europe (Ireland)	eu-west-1	Yes

Region name	Region identity	Support in User Subscriptions
Europe (London)	eu-west-2	Yes
Europe (Paris)	eu-west-3	Yes
Europe (Stockholm)	eu-north-1	Yes
South America (São Paulo)	sa-east-1	Yes

Compliance validation for Amazon Q Developer

For a list of AWS services in scope of specific compliance programs, see [AWS services in Scope by Compliance Program](#). For general information, see [AWS Compliance Programs](#).

You can download third-party audit reports using AWS Artifact. For more information, see [Downloading Reports in AWS Artifact](#) in the *AWS Artifact User Guide*.

Your compliance responsibility when using Amazon Q Developer is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- [Security and Compliance Quick Start Guides](#) – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- [Architecting for HIPAA Security and Compliance Whitepaper](#) – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.
- [AWS Compliance Resources](#) – This collection of workbooks and guides might apply to your industry and location.
- [Evaluating Resources with Rules](#) in the *AWS Config Developer Guide* – AWS Config assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- [AWS Security Hub](#) – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

Resilience in Amazon Q Developer

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see [AWS Global Infrastructure](#).

Infrastructure security in Amazon Q Developer

As a managed service, Amazon Q is protected by AWS global network security. For information about AWS security services and how AWS protects infrastructure, see [AWS Cloud Security](#). To design your AWS environment using the best practices for infrastructure security, see [Infrastructure Protection](#) in *Security Pillar AWS Well-Architected Framework*.

You use AWS published API calls to access Amazon Q Developer through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.
- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the [AWS Security Token Service](#) (AWS STS) to generate temporary security credentials to sign requests.

Amazon Q Developer and interface VPC endpoints (AWS PrivateLink)

Note

Amazon Q Developer supports VPC endpoints for features available [in your IDE](#). Chatting with Amazon Q [on AWS apps and websites](#) is not supported.

You can establish a private connection between your VPC and Amazon Q Developer by creating an *interface VPC endpoint*. Interface endpoints are powered by [AWS PrivateLink](#), a technology that enables you to privately access Amazon Q APIs without an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC don't need public IP addresses to communicate with Amazon Q APIs. Traffic between your VPC and Amazon Q does not leave the Amazon network.

Each interface endpoint is represented by one or more [Elastic Network Interfaces](#) in your subnets.

For more information, see [Interface VPC endpoints \(AWS PrivateLink\)](#) in the *Amazon VPC User Guide*.

Considerations for Amazon Q VPC endpoints

Before you set up an interface VPC endpoint for Amazon Q, ensure that you review [Interface endpoint properties and limitations](#) in the *Amazon VPC User Guide*.

Amazon Q supports making calls to all of its API actions from your VPC, in the context of services that are configured to work with Amazon Q.

Prerequisites

Before you begin any of the procedures below, ensure that you have the following:

- An AWS account with appropriate permissions to create and configure resources.
- A VPC already created in your AWS account.
- Familiarity with AWS services, especially Amazon VPC and Amazon Q.

Creating an interface VPC endpoint for Amazon Q

You can create a VPC endpoint for the Amazon Q service using either the Amazon VPC console or the AWS Command Line Interface (AWS CLI). For more information, see [Creating an interface endpoint](#) in the *Amazon VPC User Guide*.

Create a VPC endpoint for Amazon Q using the following service name:

- com.amazonaws.*region*.q

Warning

If you are [Connecting to Amazon Q through AWS PrivateLink from a third-Party IDE on an Amazon EC2 instance](#), then you will also creating the following endpoint:

- com.amazonaws.*region*.codewhisperer

If you enable private DNS for the endpoint, you can make API requests to Amazon Q using its default DNS name for the Region, for example, q.us-east-1.amazonaws.com.

For more information, see [Accessing a service through an interface endpoint](#) in the *Amazon VPC User Guide*.

Note

Currently, you can only create an interface endpoint for Amazon Q Developer in the US East (N. Virginia) Region.

Using an on-premises computer to connect to a Amazon Q endpoint

This section describes the process of using an on-premises computer to connect to Amazon Q through a AWS PrivateLink endpoint in your AWS VPC.

1. [Create a VPN connection between your on-premises device and your VPC.](#)
2. [Create an interface VPC endpoint for Amazon Q.](#)
3. [Set up an inbound Amazon Route 53 endpoint.](#) This will enable you to use the DNS name of your Amazon Q endpoint from your on-premises device.

Using an in-console coding environment to connect to a Amazon Q endpoint

This section describes the process of using an in-console coding environment to connect to a Amazon Q endpoint.

In this context, an in-console IDE is an IDE that you access inside the AWS console, and authenticate to with IAM. Examples include AWS Cloud9, SageMaker Studio, and AWS Glue Studio.

1. [Create an interface VPC endpoint for Amazon Q.](#)
2. Set up Amazon Q with the in-console coding environment
 - [AWS Cloud9](#)
 - [SageMaker Studio](#)
 - [AWS Glue Studio](#)
3. Configure the coding environment to use the Amazon Q endpoint.
 - [AWS Cloud9](#)
 - [SageMaker Studio](#)
 - [AWS Glue Studio](#)

Connecting to Amazon Q through AWS PrivateLink from a third-Party IDE on an Amazon EC2 instance

This section will walk you through the process of installing a third-party Integrated Development Environment (IDE) like Visual Studio Code or JetBrains on an Amazon EC2 instance, and configuring it to connect to Amazon Q using AWS PrivateLink.

1. [Create an interface VPC endpoint for Amazon Q.](#)
2. Launch an Amazon EC2 instance in your desired subnet within your VPC. You can choose an Amazon Machine Image (AMI) that is compatible with your third-party IDE. For example, you can select an Amazon Linux 2 AMI.
3. Connect to the Amazon EC2 instance.
4. Install and Configure the IDE (Visual Studio Code or JetBrains).
5. [Install the Amazon Q extension or plugin.](#)

6. Configure the IDE to connect via AWS PrivateLink.

- [Network connections in Visual Studio Code](#)
- [JetBrains remote development](#)

Monitoring Amazon Q Developer

Monitoring is an important part of maintaining the reliability, availability, and performance of Amazon Q Developer and your other AWS solutions. AWS provides the following monitoring tools to watch Amazon Q Developer, report when something is wrong, and take automatic actions when appropriate:

- *AWS CloudTrail* captures API calls and related events made by or on behalf of your AWS account and delivers the log files to an Amazon Simple Storage Service (Amazon S3) bucket that you specify. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred. For more information, see the [AWS CloudTrail User Guide](#).
- *Amazon CloudWatch* monitors your AWS resources and the applications you run on AWS in real time. You can collect and track metrics, create customized dashboards, and set alarms that notify you or take actions when a specified metric reaches a threshold that you specify. For example, you can have CloudWatch track the number of times that Amazon Q has been invoked on your account, or the number of daily active users. For more information, see the [Amazon CloudWatch User Guide](#).

Logging Amazon Q Developer API calls using AWS CloudTrail

Amazon Q Developer is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Amazon Q. CloudTrail captures all API calls for Amazon Q as events. The calls captured include calls from the Amazon Q console and code calls to the Amazon Q API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Amazon Q. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to Amazon Q, the IP address from which the request was made, who made the request, when it was made, and additional details.

For more information about CloudTrail, see the [AWS CloudTrail User Guide](#).

Amazon Q Developer information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Amazon Q Developer, that activity is recorded in a CloudTrail event along with other AWS service

events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see [Viewing Events with CloudTrail Event History](#) in the *AWS CloudTrail User Guide*.

For an ongoing record of events in your AWS account, including events for Amazon Q, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following topics in the *AWS CloudTrail User Guide*:

- [Overview for creating a trail](#)
- [CloudTrail supported services and integrations](#)
- [Configuring Amazon SNS notifications for CloudTrail](#)
- [Receiving CloudTrail log files from multiple Regions](#)
- [Receiving CloudTrail log files from multiple accounts](#)

All Amazon Q Developer actions are logged by CloudTrail and generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials
- Whether the request was made with temporary security credentials for a role or federated user
- Whether the request was made by another AWS service

For more information, see [CloudTrail userIdentity element](#) in the *AWS CloudTrail User Guide*.

Understanding Amazon Q Developer log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

Amazon Q Developer also makes API calls with a `dryRun` parameter to verify that you have the necessary permissions for the action, without actually making the request. Calls to Amazon Q Developer APIs with the `dryRun` parameter are captured as events and recorded in a CloudTrail log with `"dryRun" : true` in the `requestParameters` field.

The following example shows a CloudTrail log entry that demonstrates the `SendMessage` action.

```
{  
    "eventVersion": "1.08",  
    "userIdentity": {  
        "type": "AssumedRole",  
        "principalId": "AROAXD12ABCDEF3G4HI5J:aws-user",  
        "arn": "arn:aws:sts::123456789012:assumed-role/PowerUser/aws-user",  
        "accountId": "123456789012",  
        "accessKeyId": "ASIAAB12CDEFG34HIJK",  
        "sessionContext": {  
            "sessionIssuer": {  
                "type": "Role",  
                "principalId": "AROAXD12ABCDEF3G4HI5J",  
                "arn": "arn:aws:iam::123456789012:role/PowerUser",  
                "accountId": "123456789012",  
                "userName": "PowerUser"  
            },  
            "webIdFederationData": {},  
            "attributes": {  
                "creationDate": "2023-11-28T10:00:00Z",  
                "mfaAuthenticated": "false"  
            }  
        }  
    },  
    "eventTime": "2023-11-28T10:00:00Z",  
    "eventSource": "q.amazonaws.com",  
    "eventName": "SendMessage",  
    "awsRegion": "us-east-1",  
    "sourceIPAddress": "123.456.789.012",  
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/115.0",  
    "requestParameters": {  
        "Origin": "https://conversational-experience-worker.widget.console.aws.amazon.com",  
        "conversationId": "a298ec0d-0a49-4d2e-92bd-7d6e629b4619",  
        "source": "CONSOLE",  
        "conversationToken": "***",  
    }  
}
```

```
        "utterance": "***"
    },
    "responseElements": {
        "result": {
            "content": {
                "text": {
                    "body": "***",
                    "references": []
                }
            },
            "format": "PLAINTEXT",
            "intents": {},
            "type": "TEXT"
        },
        "Access-Control-Expose-Headers": "x-amzn-RequestId, x-amzn-ErrorType, x-amzn-ErrorMessage, Date",
        "metadata": {
            "conversationExpirationTime": "2024-02-25T19:31:38Z",
            "conversationId": "a298ec0d-0a49-4d2e-92bd-7d6e629b4619",
            "conversationToken": "***",
            "utteranceId": "3b87b46f-04a9-41ef-b8fe-8abf52d2c053"
        },
        "resultCode": "LLM"
    },
    "requestID": "19b3c30e-906e-4b7f-b5c3-509f67248655",
    "eventID": "a552c487-7d97-403a-8ec4-d49539c7a03d",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

The following example shows a CloudTrail log entry that demonstrates the PassRequest action.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDA60N6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::555555555555:user/Mary",
        "accountId": "555555555555",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    }
}
```

```
"sessionContext": {  
    "sessionIssuer": {  
        "type": "Role",  
        "principalId": "AIDA60N6E4XEGIEXAMPLE",  
        "arn": "arn:aws:iam::555555555555:user/Mary",  
        "accountId": "555555555555",  
        "userName": "Mary"  
  
    },  
    "attributes": {  
        "creationDate": "2024-04-10T20:03:01Z",  
        "mfaAuthenticated": "false"  
    },  
    "invokedBy": "q.amazonaws.com"  
},  
"eventTime": "2024-04-10T20:04:42Z",  
"eventSource": "q.amazonaws.com",  
"eventName": "PassRequest",  
"awsRegion": "us-east-1",  
"sourceIPAddress": "q.amazonaws.com",  
"userAgent": "q.amazonaws.com",  
"requestParameters": null,  
"responseElements": null,  
"requestID": "2d528c76-329e-410b-9516-EXAMPLE565dc",  
"eventID": "ba0801a1-87ec-4d26-be87-EXAMPLE75bbb",  
"readOnly": false,  
"eventType": "AwsApiCall",  
"managementEvent": true,  
"recipientAccountId": "555555555555",  
"eventCategory": "Management"  
}
```

The following example shows a CloudTrail log entry that demonstrates Amazon Q calling the `s3>ListBuckets` action on your behalf.

```
{  
    "eventVersion": "1.09",  
    "userIdentity": {  
        "type": "AssumedRole",  
        "principalId": "AIDA60N6E4XEGIEXAMPLE",  
        "arn": "arn:aws:iam::555555555555:user/Paulo",  
        "accountId": "555555555555",  
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",  
        "sessionContext": {  
            "sessionIssuer": {  
                "type": "Role",  
                "principalId": "AIDA60N6E4XEGIEXAMPLE",  
                "arn": "arn:aws:iam::555555555555:user/Paulo",  
                "accountId": "555555555555",  
                "userName": "Paulo"  
            },  
            "attributes": {  
                "creationDate": "2024-04-10T20:03:01Z",  
                "mfaAuthenticated": "false"  
            },  
            "invokedBy": "q.amazonaws.com"  
        },  
        "eventTime": "2024-04-10T20:04:42Z",  
        "eventSource": "q.amazonaws.com",  
        "eventName": "PassRequest",  
        "awsRegion": "us-east-1",  
        "sourceIPAddress": "q.amazonaws.com",  
        "userAgent": "q.amazonaws.com",  
        "requestParameters": null,  
        "responseElements": null,  
        "requestID": "2d528c76-329e-410b-9516-EXAMPLE565dc",  
        "eventID": "ba0801a1-87ec-4d26-be87-EXAMPLE75bbb",  
        "readOnly": false,  
        "eventType": "AwsApiCall",  
        "managementEvent": true,  
        "recipientAccountId": "555555555555",  
        "eventCategory": "Management"  
    }  
}
```

```
"sessionContext": {
    "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDA60N6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::555555555555:user/Paulo",
        "accountId": "555555555555",
        "userName": "Paulo"
    },
    "attributes": {
        "creationDate": "2024-04-10T14:06:08Z",
        "mfaAuthenticated": "false"
    }
},
"invokedBy": "q.amazonaws.com"
},
"eventTime": "2024-04-10T14:07:55Z",
"eventSource": "s3.amazonaws.com",
"eventName": "ListBuckets",
"awsRegion": "us-east-1",
"sourceIPAddress": "q.amazonaws.com",
"userAgent": "q.amazonaws.com",
"requestParameters": {
    "Host": "s3.amazonaws.com"
},
"responseElements": null,
"additionalEventData": {
    "SignatureVersion": "SigV4",
    "CipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "bytesTransferredIn": 0,
    "AuthenticationMethod": "AuthHeader",
    "x-amz-id-2": "ExampleRequestId123456789",
    "bytesTransferredOut": 4054
},
"requestID": "ecd94349-b36f-44bf-b6f5-EXAMPLE9c463",
"eventID": "2939ba50-1d26-4a5a-83bd-EXAMPLE85850",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "555555555555",
"vpcEndpointId": "vpce-EXAMPLE1234",
"eventCategory": "Management"
}
```

Monitoring Amazon Q Developer with Amazon CloudWatch

Note

The metrics discussed here only pertain to using [Amazon Q in your IDE](#).

You can monitor Amazon Q Developer using CloudWatch, which collects raw data and processes it into readable, near real-time metrics. These statistics are kept for 15 months, so that you can access historical information and gain a better perspective on how Amazon Q is performing. You can also set alarms that watch for certain thresholds, and send notifications or take actions when those thresholds are met. For more information, see the [Amazon CloudWatch User Guide](#).

The Amazon Q Developer service reports the following metrics in the AWS/CodeWhisperer namespace.

Dimensions	Metric	Use case or explanation
Count	Invocations	You want to determine how many invocations have been counted over time.
UserCount	DailyActiveUserTrend	You want to determine the number of active users per day.
SubscriptionUserCount	SubscriptionCount	You want to determine the number of users with paying subscriptions.
UniqueUserCount	MonthlyActiveUniqueUsers	You want to determine the number of users who are active in a given month.
ProgrammingLanguage, SuggestionState,	GeneratedLineCount	You want to determine the number of lines generated by CodeWhisperer.

Dimensions	Metric	Use case or explanation
CompletionType		
ProgrammingLanguage, SuggestionState, CompletionType	SuggestionReferenceCount	You want to determine the number of recommendation triggers with references that have taken place.
ProgrammingLanguage	CodeScanCount	You want to determine the number of code scans that have taken place.
ProgrammingLanguage	TotalCharacterCount	The number of characters in your file, including all suggestions from CodeWhisperer.
ProgrammingLanguage	CodeWhispererCharacterCount	The number of characters generated by CodeWhisperer.

To aggregate Invocations, use the Sum statistic.

To aggregate DailyActiveUserTrend, use the Sum statistic, and use "1 Day" as the period.

To aggregate SubscriptionCount, use the Sum statistic.

To aggregate MonthlyActiveUniqueUsers use the Sum statistic, and use "30 Days" as the period.

Tracking Amazon Q Developer usage across your organization

Your business may operate many different AWS accounts that are all part of one AWS organization. In that case, you may want to create a separate Amazon Q Developer instance for each of your

AWS accounts. Then, you can assign a different Amazon Q administrator, and a different (or overlapping) set of developers to each account.

When a Amazon Q administrator views the dashboard, they will only see information about the account to which they have been assigned.

Billing for Amazon Q Developer Pro usage is per AWS organization. If the same developer uses Amazon Q Developer in multiple accounts within the same organization, you will not be double-billed.

Tracking subscription expenses per user

You can identify the cost of Amazon Q subscriptions for specific users with resource IDs through AWS Billing and Cost Management.

To do so, in the Billing and Cost Management console under [Data Exports](#), create either a standard data export or a legacy CUR export with the **Include resource IDs** option selected.

To learn more, refer to [Creating data exports](#) in the AWS Data Exports user guide.

Accessing customization-related messages in Amazon CloudWatch Logs

You can store information about the creation of your [customization](#) in [Amazon CloudWatch Logs](#).

You can authorize your CodeWhisperer administrator to view those logs with the following permission set.

To learn more about the permissions required to delivery logs to multiple resources, see [Logging that requires additional permissions \[V2\]](#) in the *Amazon CloudWatch Logs User Guide*.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AllowLogDeliveryActions",  
      "Effect": "Allow",  
      "Action": [  
        "logs:PutDeliverySource",  
        "logs:GetDeliverySource",  
      ]  
    }  
  ]  
}
```

```
        "logs>DeleteDeliverySource",
        "logs>DescribeDeliverySources",
        "logs>PutDeliveryDestination",
        "logs>GetDeliveryDestination",
        "logs>DeleteDeliveryDestination",
        "logs>DescribeDeliveryDestinations",
        "logs>CreateDelivery",
        "logs>GetDelivery",
        "logs>DeleteDelivery",
        "logs>DescribeDeliveries",
        "firehose>ListDeliveryStreams",
        "firehose>DescribeDeliveryStream",
        "s3>ListAllMyBuckets",
        "s3>ListBucket",
        "s3>GetBucketLocation"
    ],
    "Resource": [
        "arn:aws:logs:us-east-1:account number:log-group:/*",
        "arn:aws:firehose:us-east-1:account number:deliverystream/*",
        "arn:aws:s3:::/*"
    ]
}
]
```

Supported Regions for Amazon Q Developer

Note

If you have enabled cross-region calls in Amazon Q, Amazon Q might make calls to opt-in Regions that aren't listed on this page. To manage access to Regions Amazon Q can make calls to, see [Allow Amazon Q permission to perform actions on your behalf in specific regions](#).

Regardless of where you use Amazon Q Developer, data is sent to and stored in an AWS Region in the US. Your conversations with Amazon Q are stored in the US East (N. Virginia) Region even if the AWS Management Console is set to a different AWS Region. Data processed during troubleshooting console error sessions is stored in the US West (Oregon) Region. Data processed during interactions with Amazon Q in integrated development environments (IDEs) is stored in the US East (N. Virginia) Region.

Note

To set up Amazon Q Developer, your AWS management console must be set to US East (N. Virginia).

Amazon Q Developer in the AWS Management Console, AWS Console Mobile Application, AWS website, AWS Documentation website, and AWS Chatbot is available in the following AWS Regions. Even if you set your console to one of these Regions, your data will still be processed in a US Region.

- US East (Ohio)
- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- Asia Pacific (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)

- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Europe (Paris)
- Europe (Stockholm)
- South America (São Paulo)

Opt-in Regions

At [the free tier](#), you can chat with Amazon Q Developer [on AWS apps and websites](#) in an [*opt-in Region*](#) (Region that is disabled by default). To use an opt-in Region with Amazon Q Developer, you must enable the Region manually. For more information about AWS Regions, see [Specify which AWS Regions your account can use](#) in the *AWS Account Management Reference Guide*. The following opt-in Regions are supported. Even if you set your console to one of these Regions, your data will still be processed in a US Region.

- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- Asia Pacific (Hyderabad)
- Asia Pacific (Jakarta)
- Asia Pacific (Melbourne)
- Europe (Milan)
- Europe (Spain)
- Europe (Zurich)
- Middle East (Bahrain)
- Middle East (UAE)
- Israel (Tel Aviv)

Amazon Q Developer rename - Summary of changes

On April 30, 2024, Amazon CodeWhisperer became a part of Amazon Q Developer. This section points you to the parts of this guide where you can find documentation for features that you are accustomed to using through CodeWhisperer.

As you transition from using CodeWhisperer to using Amazon Q Developer, you may consider the following changes to be most significant:

- The [administrative setup](#) at the professional tier (Amazon Q Developer Pro) is different than it was for CodeWhisperer Professional.
- You can [chat with Amazon Q Developer](#) in the AWS Management Console, and on the AWS documentation and marketing websites.

The following familiar features of CodeWhisperer are available as part of Amazon Q Developer, with a few changes:

- Coding suggestions [in a third-party IDE](#)
- Coding suggestions [in the context of another AWS service](#)
- Suggestions [at the command line](#)
- [Customizations](#)
- [Security scans](#)
- [Dashboard](#)

Document history for Amazon Q Developer User Guide

The following table describes the document history for the *Amazon Q Developer User Guide*. For notifications about updates to this documentation, you can subscribe to the RSS feed.

Change	Description	Date
<u>CodeWhisperer endpoint needed for IDE VPC access</u>	<u>Access from a Amazon VPC</u> must include both q and codewhisperer endpoints.	July 18, 2024
<u>New endpoint</u>	Endpoints can now <u>use the string q instead of codewhisperer</u> .	July 12, 2024
<u>Customizations are GA</u>	The <u>customizations</u> feature is generally available.	July 10, 2024
<u>Chatting about customizations (Preview)</u>	In Preview, you can use the <u>customizations</u> feature to ask questions related to your codebase.	July 10, 2024
<u>Updated managed policy: AmazonQFullAccess</u>	Additional permissions have been added to the <u>AmazonQFullAccess</u> policy.	July 9, 2024
<u>New managed policy: AmazonQDeveloperAccess</u>	The <u>AmazonQDeveloperAccess</u> managed policy provides full access to enable interactions with Amazon Q Developer, without administrator access.	July 9, 2024
<u>Updated Amazon Q Developer admin policy</u>	The <u>policy for empowering Amazon Q Developer administrators has been</u>	June 19, 2024

updated to include
sso>ListProfiles .

Trusted access section

A [new section](#) more clearly explains how a Amazon Q Developer administrator can share settings with member accounts.

June 19, 2024

Updated setup procedures

There's an improved [Getting started](#) chapter that includes support for [account instances](#).

June 6, 2024

Updated code examples

The [code examples](#) now include C and C++, and have improved examples for C#.

June 6, 2024

Updated managed policy: AmazonQFullAccess

Additional permissions have been added to the [AmazonQFullAccess](#) policy.

April 30, 2024

New service-linked role: AWSServiceRoleForUserSubscriptions

The [AWSServiceRoleForUserSubscriptions](#) service-linked role provides access for User Subscriptions to your IAM Identity Center resources to automatically update your subscriptions.

April 30, 2024

New service-linked role: AWSServiceRoleForAmazonQDeveloper

The [AWSServiceRoleForAmazonQDeveloper](#) service-linked role grants permission to access and emit data, and to create reports.

April 30, 2024

<u>New managed policy: AWSServiceRoleForUserSubscriptionPolicy</u>	The <u>AWSServiceRoleForUserSubscriptionPolicy</u> allows principals to track IAM Identity Center directory and AWS Organizations changes.	April 30, 2024
<u>New managed policy: AWSServiceRoleForAmazonQDeveloperPolicy</u>	The <u>AWSServiceRoleForAmazonQDeveloperPolicy</u> allows Amazon Q Developer to call CloudWatch and CodeGuru on your behalf.	April 30, 2024
<u>GA release</u>	Amazon Q Developer is available for general audiences.	April 30, 2024
<u>Amazon CodeWhisperer merge</u>	Amazon CodeWhisperer is now a part of Amazon Q Developer.	April 30, 2024
<u>New guide name</u>	This service and accompanying user guide have been renamed Amazon Q Developer.	March 29, 2024
<u>New permission</u>	The <u>ListConversations action</u> is required to chat with Amazon Q in the console.	March 5, 2024
<u>New data protection topic</u>	Amazon Q now uses content for <u>service improvement purposes</u> .	January 25, 2024
<u>New topic</u>	Added instructions for how to <u>add Amazon Q to Slack and Microsoft Teams channels</u> that are configured with AWS Chatbot.	January 18, 2024

Preview release

This is the initial preview
release of the *Amazon Q*
Developer User Guide.

November 28, 2023