



Getting Started Guide

AWS Management Console



Version 1.0.202610140310

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Management Console: Getting Started Guide

Copyright © 2026 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.

Services or capabilities described in AWS documentation might vary by Region. To see the differences applicable to the AWS European Sovereign Cloud Region, see the [AWS European Sovereign Cloud User Guide](#).

Table of Contents

What is the AWS Management Console?	1
Features of AWS Management Console	1
Individual AWS service consoles	2
Accessing the AWS Management Console	2
Accessing the AWS Management Console with mobile devices	2
Using the AWS Management Console with our new AWS experience	4
Getting started with a service	5
Unified Navigation	6
Accessing the Services menu	6
Searching for products, services, features, and more	7
Searching for AWS products	8
Refining your search	8
Viewing features of a service	9
Launching AWS CloudShell	9
Accessing AWS notifications and Health events	10
Getting support	10
Configuring the AWS Management Console	11
Configuring Unified Settings	11
Configuring visible Regions and services	14
Enabling experimental preview	16
Choosing your Region	18
Favorites	19
Changing your password	24
Changing the language of the AWS Management Console	26
Accessing your AWS information	28
Accessing account information	29
Accessing organization information	30
Accessing service quota information	30
Accessing billing information	30
Signing in to multiple accounts	31
Using recommended actions	32
Features of AWS Recommended Actions	32
Using recommended actions	32
Monitoring with CloudTrail logs	33

AWS Console Home	36
Viewing all AWS services	36
Working with Widgets	36
Managing widgets	37
Chatting with Amazon Q	38
Get started with Amazon Q	38
Example questions	38
AWS User Experience Customization	40
Getting started	41
Prerequisites	41
Accessing UXC settings in the AWS Management Console	41
Accessing UXC settings programmatically	42
API Reference	42
Monitoring with CloudTrail logs	42
UXC data events in CloudTrail	43
UXC management events in CloudTrail	43
UXC event examples	34
Security	45
Identity and Access Management	46
AWS managed policies	56
AWSManagementConsoleBasicUserAccess	56
AWSManagementConsoleAdministratorAccess	57
Policy updates	58
Markdown in AWS	60
Paragraphs, Line Spacing, and Horizontal Lines	60
Headings	61
Text Formatting	61
Links	61
Lists	62
Tables and Buttons (CloudWatch Dashboards)	62
Troubleshooting	64
The page isn't loading properly	64
My browser displays an 'access denied' error when connecting to the AWS Management Console	65
My browser displays timeout errors when connecting to the AWS Management Console	66

I want to change the language of the AWS Management Console but I can't find the language selection menu at the bottom of the page	66
Document history	67

What is the AWS Management Console?

The [AWS Management Console](#) is a web-based application that contains and provides centralized access to all individual AWS service consoles. You can use Unified Navigation in the AWS Management Console to search for services, view notifications, access AWS CloudShell, access account and billing information, and customize your general console settings. The home page of the AWS Management Console is called AWS Console Home. From AWS Console Home, you can manage your AWS applications and access all other individual service consoles. You can also customize AWS Console Home to show other helpful information about AWS and your resources by using widgets. You can add, remove, and rearrange widgets such as **Recently visited**, **AWS Health**, and more.

Topics

- [Features of AWS Management Console](#)
- [Individual AWS service consoles in the AWS Management Console](#)
- [Accessing the AWS Management Console](#)
- [Accessing the AWS Management Console with mobile devices](#)

Features of AWS Management Console

Important features of the AWS Management Console include the following:

- **Navigate to AWS service consoles** – You can use Unified Navigation to access recently visited service consoles, view and add services to your **Favorites** list, access your console settings, and access AWS User Notifications.
- **Search for AWS services and other AWS information** – use Unified Search to search for AWS services and features, and AWS marketplace products.
- **Customize the console** – You can use Unified settings to customize various aspects of the AWS Management Console. This includes the language, default Region, and more.
- **Run CLI commands** – AWS CloudShell is accessible directly from the console. You can use CloudShell to run AWS CLI commands against your favorite services.
- **Access all AWS event notifications** – You can use the AWS Management Console to access notifications from AWS User Notifications and AWS Health.

- **Customize AWS Console Home** – You can completely customize your AWS Console Home experience by using widgets.
- **Create and manage AWS applications** – Manage and monitor the cost, health, security posture, and performance of your applications using myApplications in AWS Console Home.
- **Chat with Amazon Q** – You can get generative artificial intelligence (AI) assistant powered answers to your AWS service questions directly from the console. You can also get connected with a live agent for additional support.

Individual AWS service consoles in the AWS Management Console

Each AWS service has its own individual service console that you can access within the AWS Management Console. Settings you choose in Unified Settings for the AWS Management Console, such as visual mode and default language, are applied to all individual AWS consoles. AWS service consoles offer a wide range of tools for cloud computing, as well as information about your account and about your [billing](#). If you want to know more about a specific service and its console, for example Amazon Elastic Compute Cloud, navigate to its console using Unified Search in the AWS Management Console navigation bar and access the Amazon EC2 documentation from the [AWS Documentation website](#).

When you navigate to an individual AWS service's console, you can still access features of the AWS Management Console using Unified Navigation at the top of console. You can leave feedback for an individual service's console by navigating to that console and choosing **Feedback** in the page's footer.

Accessing the AWS Management Console

You can access the AWS Management Console at <https://eusc-de-east-1.console.amazonaws-eusc.eu/>.

Accessing the AWS Management Console with mobile devices

The [AWS Management Console](#) is designed to work on tablets as well as other kinds of mobile devices:

- Horizontal and vertical space is maximized to show more on your screen.

- Buttons and selectors are larger for a better touch experience.

To access the AWS Management Console on a mobile device, you must use the AWS Console Mobile Application. This app is available for Android and iOS. The Console Mobile Application provides mobile-relevant tasks that are a good companion to the full web experience. For example, you can easily view and manage your existing Amazon EC2 instances and Amazon CloudWatch alarms from your phone. For more information, see [What is the AWS Console Mobile Application?](#) in the *AWS Console Mobile Application User Guide*.

You can download the Console Mobile Application from [Amazon Appstore](#), [Google Play](#), and the [iOS App Store](#).

Using the AWS Management Console with our new AWS experience

Warning

We're currently releasing our new experience to a limited number of customers. You might not be able to access this experience yet.

If you signed up using our [new AWS experience](#), you have access to a simplified version of the AWS Management Console. This version of the AWS Management Console includes the following:

- **Generate your AWS credentials** – You can generate your AWS credentials and use our set up script to let your AI coding tools create AWS resources in your project.
- **Navigate to AWS service consoles** – You can use Unified Navigation to access recently visited service consoles, view and add services to your **Favorites** list, access your console settings, and access AWS User Notifications. Not every AWS service is supported with our new AWS experience. For more information, see [Supported AWS services for Sign up for AWS \(new\)](#).
- **Search for AWS services and other AWS information** – Use Unified Search to search for AWS services and features, and AWS Marketplace products.
- **Menu** – Use the menu to move between the AWS Management Console and AWS Settings, switch between active sessions, and customize the various aspects of the AWS Management Console.
- **Run CLI commands** – Amazon CloudSearch is accessible directly from the console. You can use Amazon CloudSearch to run AWS CLI commands against your favorite services.
- **Access all AWS event notifications** – You can use the AWS Management Console to access notifications from AWS User Notifications and .
- **Chat with Amazon Q** – You can get generative artificial intelligence (AI) assistant powered answers to your AWS service questions directly from the console.

Certain tasks are not supported in the AWS Management Console but are supported in AWS Settings. For more information, see [Compare sign-up options](#).

Getting started with a service in the AWS Management Console

The [AWS Management Console](#) provides multiple ways for navigating to individual service consoles.

To open a console for a service

Do one of the following:

- In the search box on the navigation bar, enter all or part of the name of the service. Under **Services**, choose the service that you want from the list of search results. For more information, see [Searching for products, services, features, and more using Unified Search in the AWS Management Console](#).
- In the **Recently visited services** widget, choose a service name.
- In the **Recently visited services** widget, choose **View all AWS services**. Then, on the **All AWS services** page, choose a service name.
- On the navigation bar, choose **Services** to open a full list of services. Then choose a service under **Recently visited** or **All services**.

Using the AWS Management Console navigation bar via Unified Navigation

This topic describes how to use Unified Navigation. Unified Navigation refers to the navigation bar that acts as the header and footer of the console. You can use Unified Navigation to:

- Search for and access AWS services, features, products, and more.
- Launch AWS Cloudshell.
- Access AWS notifications and AWS Health events.
- Get support from a variety of AWS knowledge sources.
- Configure the AWS Management Console by choosing your default language, visual mode, Region, and more.
- Access account, organization, service quota, and billing information.

Topics

- [Accessing the Services menu in the AWS Management Console](#)
- [Searching for products, services, features, and more using Unified Search in the AWS Management Console](#)
- [Launching AWS CloudShell from the navigation bar in the AWS Management Console](#)
- [Accessing AWS notifications and Health events](#)
- [Getting support](#)
- [Configuring the AWS Management Console using Unified Settings](#)
- [Accessing your AWS account, organization, service quota, and billing information in the AWS Management Console](#)
- [Signing in to multiple accounts](#)
- [AWS Recommended Actions in the AWS Management Console](#)

Accessing the Services menu in the AWS Management Console

You can use the Services menu, next to the search bar to access your recently visited services, view your Favorites list, and view all AWS services. You can also view services by type by choosing a service type, for example **Analytics** or **Application Integration**.

The following procedure describes how to access the **Services** menu.

To access the Services menu

1. Sign in to the [AWS Management Console](#).
2. In the navigation bar, choose **Services** (:::).
3. (Optional) Choose **Recently visited** to view services and applications you recently interacted with.
4. (Optional) Choose **Favorites** to view your Favorites list.
5. (Optional) Choose **All applications** to view your myApplications applications.
6. (Optional) Choose **All services** to view an alphabetical list of all AWS services.
7. (Optional) Choose a service type to view AWS services by type.

Searching for products, services, features, and more using Unified Search in the AWS Management Console

The search box in the navigation bar provides a unified search tool for finding AWS services and features, service documentation, AWS Marketplace products, and more. Just enter a few characters or a question to start generating results from all available content types. Each word you enter further refines your results. The available content types include:

- Services
- Features
- Documents
- Blogs
- Knowledge Articles
- Events
- Tutorials
- Marketplace
- Resources

Note

You can filter your search results to show only resources by performing a focused search. To perform a focused search, enter `/Resources` at the beginning of your query in the search bar and choose **/Resources** from the dropdown menu. Then enter the rest of your query.

Topics

- [Searching for AWS products in the AWS Management Console](#)
- [Refining your search in the AWS Management Console](#)
- [Viewing features of a service in the AWS Management Console](#)

Searching for AWS products in the AWS Management Console

The following procedure details how to search for AWS products using the search tool.

To search for a service, feature, documentation, or AWS Marketplace product

1. In the search box on the navigation bar of the [AWS Management Console](#), enter your query.
2. Choose any link to navigate to your intended destination.

Tip

You can also use your keyboard to quickly navigate to the top search result. First, press **Alt+s** (Windows) or **Option+s** (macOS) to access the search bar. Then start entering your search term. When the intended result appears at the top of the list, press **Enter**. For example, to quickly navigate to the Amazon EC2 console, enter **ec2** and press **Enter**.

Refining your search in the AWS Management Console

You can refine your search by content type and view additional information about search results.

To refine your search to a specific content type

1. In the search box on the navigation bar of the [AWS Management Console](#), enter your query.
2. Choose one of the content types next to your search results.
3. (Optional) To see all results for a specific category:
 - Choose **Show more**. A new tab will open showing the results.
4. (Optional) To view additional information about your search results:
 - a. In the search results, hover your cursor over a search result.
 - b. View the available additional information.

Viewing features of a service in the AWS Management Console

You can view features of a service from within your search results.

To view features of a service

1. In the search box on the navigation bar of the [AWS Management Console](#), enter your query.
2. In the search results, hover your cursor over a service in **Services**.
3. Choose one of the links in **Top features**.

Launching AWS CloudShell from the navigation bar in the AWS Management Console

AWS CloudShell is a browser-based, pre-authenticated shell that you can launch directly from the AWS Management Console navigation bar. You can run AWS CLI commands against services using your preferred shell (Bash, PowerShell, or Z shell).

You can launch CloudShell from the AWS Management Console using one of the following two methods:

- Choose the CloudShell icon in the footer of the console.
- Choose the CloudShell icon on the console navigation bar.

For more information about this service, see the [AWS CloudShell User Guide](#).

For information about the AWS Regions where AWS CloudShell is available, see the [AWS Regional Services List](#). The selection of the Console Region is in sync with the CloudShell Region. If CloudShell isn't available in a selected Region, then CloudShell will operate in the nearest Region.

Accessing AWS notifications and Health events

You can access some of your AWS notifications and view health events from the navigation bar. You can also access AWS User Notifications to view all of your AWS notifications and the AWS Health Dashboard from the navigation bar.

For more information see [What is AWS User Notifications?](#) in the *AWS User Notifications User Guide* and [What is AWS Health?](#) in the *AWS Health User Guide*

The following procedure describes how to access your AWS event information.

To access your AWS event information

1. Sign in to the [AWS Management Console](#).
2. In the navigation bar, choose the bell icon.
3. View your notifications and health events.
4. (Optional) Choose **see all notifications** to navigate to the User Notifications console.
5. (Optional) Choose **see all Health events** to navigate to the AWS Health console.

Getting support

You can get support by choosing the question mark icon in the navigation bar. From the support menu, you can choose to:

- Navigate to the Support Center service console
- View curated knowledge from community articles and the knowledge center on AWS re:Post
- Go to AWS documentation
- Navigate to AWS trainings
- Navigate to the AWS getting started Resource Center
- Leave feedback for any service console you're currently accessing

 Note

This can also be done by choosing **Feedback** in the console footer. The title of the modal that opens shows which console you're currently leaving feedback for

You can also get help anytime in the console, get connected with a live agent, and ask any question about AWS by chatting with AWS Q. For more information, see [???](#).

Configuring the AWS Management Console using Unified Settings

This topic describes how to configure your AWS Management Console using the Unified Settings page to set defaults that apply to all service consoles.

Topics

- [Configuring Unified Settings in the AWS Management Console](#)
- [Configuring visible Regions and services in the AWS Management Console](#)
- [Enabling AWS experimental preview](#)
- [Choosing your Region](#)
- [Favorites in the AWS Management Console](#)
- [Changing your password in the AWS Management Console](#)
- [Changing the language of the AWS Management Console](#)

Configuring Unified Settings in the AWS Management Console

You can configure settings and defaults, such as display, language, and Region, from the AWS Management Console **Unified Settings** page. You can access Unified Settings via the navigation bar in Unified Navigation. The visual mode and default language can also be set directly from the navigation bar. These changes apply to all service consoles.

 Important

To ensure that your settings, favorite services, and recently visited services persist globally, this data is stored in all AWS Regions, including Regions that are disabled by default. These

Regions are Africa (Cape Town), Asia Pacific (Hong Kong), Asia Pacific (Hyderabad), Asia Pacific (Jakarta), Europe (Milan), Europe (Spain), Europe (Zurich), Middle East (Bahrain), and Middle East (UAE). You still need to [manually enable a Region](#) to access it and to create and manage resources in that Region. If you don't want to store this data in all AWS Regions, choose **Reset all** to clear your settings, and then opt out of remembering recently visited services in Settings management.

Topics

- [Accessing Unified Settings in the AWS Management Console](#)
- [Resetting Unified Settings in the AWS Management Console](#)
- [Editing Unified Settings in the AWS Management Console](#)
- [Changing the visual mode of the AWS Management Console](#)

Accessing Unified Settings in the AWS Management Console

The following procedure describes how to access Unified Settings.

To access Unified Settings

1. Sign in to the [AWS Management Console](#).
2. In the navigation bar, choose the gear icon (#).
3. To open the **Unified Settings** page, choose **See all user settings**.

Resetting Unified Settings in the AWS Management Console

You can delete all Unified Settings configurations and restore the default settings by resetting Unified Settings.

Note

This affects multiple areas of AWS, including favorite services in navigation and the Services menu, recently visited services on Console Home widgets and in the AWS Console Mobile Application, and all settings that apply across services, such as default language, default Region, and visual mode.

To reset all Unified Settings

1. Sign in to the [AWS Management Console](#).
2. In the navigation bar, choose the gear icon (#).
3. Open the **Unified Settings** page by choosing **See all user settings**.
4. Choose **Reset all**.

Editing Unified Settings in the AWS Management Console

The following procedure describes how to edit your preferred settings.

To edit Unified Settings

1. Sign in to the [AWS Management Console](#).
2. In the navigation bar, choose the gear icon (#).
3. Open the **Unified Settings** page by choosing **See all user settings**.
4. Choose **Edit** next to your preferred settings:
 - **Localization and default Region:**
 - **Language** lets you select the default language for console text.
 - **Default Region** lets you select a default Region that applies each time you log in. You can select any of the available Regions for your account. You can also select the last used Region as your default.

To learn more about Region routing in the [AWS Management Console](#), see [Choosing a Region](#).

- **Display:**
 - **Visual mode** lets you set your console to light mode, dark mode, or the default display mode of your browser.

Dark mode is a beta feature and might not apply across all AWS service consoles.
 - **Favorites bar display** toggles the **Favorites** bar display between the full service name with its icon or only the service's icon.
 - **Favorites bar icon size** toggles the size of the service icon on the **Favorites** bar display between small (16x16 pixels) and large (24x24 pixels).
- **Settings management:**

- **Remember recently visited services** lets you choose if the AWS Management Console remembers your recently visited services. Turning this off also deletes your recently visited services history, so you will no longer see recently visited services in the Service menu, AWS Console Mobile Application, or on Console Home widgets.

5. Choose **Save changes**.

Changing the visual mode of the AWS Management Console

Your visual mode sets your console to light mode, dark mode, or the default display mode of your browser.

To change the visual mode from the navigation bar

1. Sign in to the [AWS Management Console](#).
2. In the navigation bar, choose the gear icon (#).
3. For **Visual mode**, choose **Light** for light mode, **Dark** for dark mode, or **Browser default** for the default display mode of your browser.

Configuring visible Regions and services in the AWS Management Console

Account administrators can control which AWS Regions and AWS services are visible in the AWS Management Console navigation. These account-level settings are available on the **Account settings** tab of the Unified Settings page. When you hide a Region, it is removed from the Region selector for all users in the account. When you hide a service, it appears as unavailable in a separate section of the Services menu for all users in the account. Hidden services are also grayed out in Unified Search results and in the Recently Visited and Favorites widgets on Console Home.

If a user navigates directly to a hidden Region or service through a URL, they see an overlay that informs them the Region or service is hidden at the account level.

Note

Navigation to the Unified Settings page is always available, so administrators can't lock themselves out of these settings. If a user doesn't have the required permissions, or if the

AWS User Experience Customization service is unavailable, all Regions and services are visible by default.

Topics

- [Prerequisites for configuring visible Regions and services](#)
- [Configuring visible Regions in the AWS Management Console](#)
- [Configuring visible services in the AWS Management Console](#)

Prerequisites for configuring visible Regions and services

To view and change visible Regions and services settings, you need specific IAM permissions.

- To view the settings, you need the `uxc:GetAccountCustomizations` permission.
- To change the settings, you need the `uxc:UpdateAccountCustomizations` permission.

The AWS managed policies `AWSManagementConsoleBasicUserAccess` and `AWSManagementConsoleAdministratorAccess` include these permissions.

For more information, see [???](#).

Configuring visible Regions in the AWS Management Console

You can choose which AWS Regions appear in the Region selector for all users in your account.

To configure visible Regions

1. Sign in to the [AWS Management Console](#).
2. In the navigation bar, choose the gear icon (#).
3. Choose **See all user settings** to open the **Unified Settings** page.
4. Choose the **Account settings** tab.
5. For **Visible Regions**, select the check boxes for the Regions that you want to show, or clear the check boxes for the Regions that you want to hide.
6. Choose **Save changes**.

After you save, hidden Regions are removed from the Region selector for all users in the account.

Configuring visible services in the AWS Management Console

You can choose which AWS services appear in the Services menu for all users in your account.

To configure visible services

1. Sign in to the [AWS Management Console](#).
2. In the navigation bar, choose the gear icon (#).
3. Choose **See all user settings** to open the **Unified Settings** page.
4. Choose the **Account settings** tab.
5. For **Visible services**, select the check boxes for the services that you want to show, or clear the check boxes for the services that you want to hide.
6. Choose **Save changes**.

After you save, hidden services appear as unavailable in a separate section of the Services menu for all users in the account. Hidden services are also grayed out in Unified Search results and in the Recently Visited and Favorites widgets on Console Home.

Enabling AWS experimental preview

AWS experimental preview is an opt-in experience in the AWS Management Console that gives you access to new AWS features that are still being evaluated. AWS uses your feedback to improve features and determine whether they're ready for general availability.

Note

Experimental preview features are subject to change and may be removed.

Topics

- [Enable experimental preview in the console](#)
- [Provide feedback on experimental preview features](#)
- [Opt out of experimental preview in the console](#)

Enable experimental preview in the console

When you enable experimental preview, all features currently in experimental preview are enabled at user level. As new features enter experimental preview, they are also enabled automatically.

To enable experimental preview

1. Log in to the AWS Management Console at <https://eusc-de-east-1.console.amazonaws-eusc.eu/>.
2. In the navigation bar, choose Settings (#).
3. Choose **AWS experimental preview**.
4. On the **AWS experimental preview** page, turn on **Enable preview** to access all experimental preview features.
5. In the pop-up, enter your email address and choose **Submit**. AWS may use this to follow up on feedback you provide.

Provide feedback on experimental preview features

You can provide feedback to help AWS improve experimental features and determine launch readiness.

To provide feedback

1. In the navigation bar, choose Settings (#).
2. Choose **AWS experimental preview**.
3. In the **Features** list, find the feature you want to provide feedback on.
4. In the **Feedback** column, choose **Submit**.
5. Fill out the feedback form, and then choose **Submit**.

Opt out of experimental preview in the console

If you no longer want to use experimental preview features, you can opt out at any time. When you opt out, you opt out of all experimental preview features.

To opt out of experimental preview

1. In the navigation bar, choose Settings (#).

2. Choose **AWS experimental preview**.
3. On the **AWS experimental preview** page, turn off **Enable preview** to opt out.
4. In the pop-up, you can optionally share your reason for opting out.

Choosing your Region

For many services, you can choose an AWS Region that specifies where your resources are managed. Regions are sets of AWS resources located in the same geographical area. You don't need to choose a Region for the [AWS Management Console](#) or for some services, such as AWS Identity and Access Management. To learn more about AWS Regions, see [Managing AWS Regions](#) in the *AWS General Reference*.

Note

If you have created AWS resources but you don't see those resources in the console, the console might be displaying resources from a different Region. Some resources (such as Amazon EC2 instances) are specific to the Region where they were created.

Topics

- [Choosing a Region from the navigation bar in the AWS Management Console](#)
- [Setting the default Region in the AWS Management Console](#)

Choosing a Region from the navigation bar in the AWS Management Console

The following procedure details how you can change your Region from the navigation bar.

To choose a Region from the navigation bar

1. Sign in to the [AWS Management Console](#).
2. In the navigation bar, choose the name of the currently displayed Region.
3. Choose a Region to switch to.

Setting the default Region in the AWS Management Console

The following procedure details how you can change your default Region from the Unified Settings page.

To set your default Region

1. In the navigation bar, choose the gear icon (#).
2. Choose **See all user settings** to navigate to the **Unified Settings** page.
3. Choose **Edit** next to **Localization and default Region**.
4. In **Default Region**, choose a Region.

Note

If you don't select a default Region, the console uses the last Region that you visited. If you sign in with IAM Identity Center, select a specific default Region. The last-visited Region doesn't persist across IAM Identity Center sessions.

5. Choose **Save settings**.
6. (Optional) Choose **Go to new default Region** to immediately go to your new default Region.

Favorites in the AWS Management Console

To access your frequently used services and applications more quickly, you can save their service consoles to a list of **Favorites**. You can add and remove favorites using the AWS Management Console. When you add a service or application to your **Favorites**, it appears on the Favorites quickbar.

Topics

- [Adding favorites in the AWS Management Console](#)
- [Accessing favorites in the AWS Management Console](#)
- [Removing favorites in the AWS Management Console](#)

Adding favorites in the AWS Management Console

You can add services and applications to your favorites from the **Services** menu and the **Recently visited** menu. You can also add services to your favorites by using the search results page from

the search box. Services and applications that you add to your favorites appear in the Favorites quickbar.

Topics

- [Favorites quickbar in the AWS Management Console](#)
- [Adding services to your favorites in the AWS Management Console](#)
- [Adding applications to your favorites in the AWS Management Console](#)

Favorites quickbar in the AWS Management Console

The favorites quickbar appears when you have at least one AWS service or application added to your favorites. The favorites quickbar is located following the navigation bar and is visible in all AWS service consoles, so you can quickly access your favorite services and applications. You can rearrange the order of the services and applications in the favorites quickbar by dragging a service or application to the left or right.

Adding services to your favorites in the AWS Management Console

You can add services to your favorites from the **Services** menu or the search results page from the search box.

Services menu

To add favorites from the Services menu

1. Open the [AWS Management Console](#).
2. In the navigation bar, choose **Services** (:::).
3. (Optional) Add a recently visited service to your favorites:
 - a. In **Recently visited**, hover your cursor over a service.
 - b. Select the star next to the service's name.
4. Choose **All services**.
5. Hover your cursor over your chosen service.
6. Select the star next to the service's name.

Search box

To add favorites from the search box

1. Open the [AWS Management Console](#).
2. Enter the name of a service in the search box.
3. In the search results page, select the star next to the service's name.

Note

After you add a service to your favorites, it's added to the favorites quickbar following the navigation bar.

Adding applications to your favorites in the AWS Management Console

You can add applications to your favorites from the **Services** menu.

To add favorites from the Services menu

1. Open the [AWS Management Console](#).
2. In the navigation bar, choose **Services** (:::).
3. (Optional) Add a recently visited application to your favorites:
 - a. In **Recently visited**, hover your cursor over an application.
 - b. Select the star next to the application's name.
4. Choose **Applications**.
5. Hover your cursor over your chosen application.
6. Select the star next to the application's name.

Note

After you add an application to your favorites, it's added to the favorites quickbar following the navigation bar.

Accessing favorites in the AWS Management Console

You can access services and applications added to your favorites from the **Services** menu, the favorites quickbar, and the **Favorites** widget.

Services menu

To access your favorites from the Services menu

1. Open the [AWS Management Console](#).
2. In the navigation bar, choose **Services** (:::).
3. Choose **Favorites**.
4. View the services and applications you added to your favorites.
5. (Optional) View application resources:
 - a. Select an application.
 - b. (Optional) Select a [view](#).
 - c. View your resources.
 - d. (Optional) Select a filter. You can filter your resources by **Properties** or by **Tags**. For more information, see [Search query syntax reference for Resource Explorer](#) in the *AWS Resource Explorer User Guide*.
 - e. (Optional) Select a resource to view it in the relevant service console.

Tip

You can continue browsing resources where you left off by choosing **Services** (:::). Your applied search filters will also persist.

Favorites quickbar

To access your favorites from the favorites quickbar

1. Open the [AWS Management Console](#).
2. View the services and applications in the favorites quickbar.

Favorites widget

To access your favorites from the Favorites widget

1. Open the [AWS Management Console](#).
2. (Optional) Add the **Favorites** widget if you don't have it:
 - a. Choose the **+ Add widgets** button on the Console Home page.
 - b. In the **Add widgets** menu, drag the **Favorites** widget by using the :: icon and place it on your Console Home page.
3. View the services and applications in the **Favorites** widget.

For more information about widgets, see [the section called "Working with Widgets"](#).

Removing favorites in the AWS Management Console

You can remove services and applications from your favorites using the **Services** menu. You can also remove services by using the search results page from the search bar.

Services menu

To remove favorites from the Services menu

1. Open the [AWS Management Console](#).
2. In the navigation bar, choose **Services**.
3. Choose **Favorites**.
4. Deselect the star next to the service or application.

Search box

Note

Currently, you can only remove services using the search results page from the search bar.

To remove favorites from the search box

1. Open the [AWS Management Console](#).
2. Enter the name of a service in the search box.
3. In the search results page, deselect the star next to the service's name.

Changing your password in the AWS Management Console

You may be able to change your password from the [AWS Management Console](#) depending on your user type and your permissions. The following topic describes how to change your password for each user type.

Topics

- [Root users in the AWS Management Console](#)
- [IAM users in the AWS Management Console](#)
- [IAM Identity Center users in the AWS Management Console](#)
- [Federated identities in the AWS Management Console](#)

Root users in the AWS Management Console

Root users can change their passwords directly from the AWS Management Console. A Root user is the account owner with complete access to all AWS services and resources. You're the root user if you created the AWS account and you sign in using your root user email and password. For more information, see [Root user](#) in the *AWS IAM Identity Center User Guide*.

To change your password as a Root user

1. Sign in to the [AWS Management Console](#).
2. In the navigation bar, choose your account name.
3. Choose **Security credentials**.
4. The options displayed will vary depending on your AWS account type. Follow the instructions shown on the console to change your password.
5. Enter your current password once and your new password twice.

The new password must be at least eight characters long and must include the following:

- At least one symbol
- At least one number
- At least one uppercase letter
- At least one lowercase letter

6. Choose **Change Password** or **Save changes**.

IAM users in the AWS Management Console

IAM users may be able to change their password from the AWS Management Console depending on their permissions. Otherwise, they must use an AWS access portal. An IAM user is an identity within your AWS account that's granted specific custom permissions. You're an IAM user if you didn't create the AWS account and your administrator or help desk employee provided you your sign-in credentials that include an AWS account ID or account alias, an IAM user name, and password. For more information, see [IAM user](#) in the *AWS Sign-In User Guide*.

If you have permissions from the following policy: [AWS: Allows IAM users to change their own console password on the Security credentials page](#), you can change your password from the console. For more information, see [How an IAM user changes their own password](#) in the *AWS Identity and Access Management User Guide*.

If you don't have the requisite permissions to change your password from the AWS Management Console see, [Resetting your AWS IAM Identity Center user password](#) in the *AWS IAM Identity Center User Guide*.

IAM Identity Center users in the AWS Management Console

AWS IAM Identity Center users must change their password from an AWS access portal. For more information, see [Resetting your AWS IAM Identity Center user password](#) in the *AWS IAM Identity Center User Guide*.

An IAM Identity Center user is a user whose AWS account is part of AWS Organizations who signs in through the AWS access portal with a unique URL. These users can be either created directly in the users in IAM Identity Center or in Active directory or another external identity provider. For more information, see [AWS IAM Identity Center user](#) in the *AWS Sign-In User Guide*.

Federated identities in the AWS Management Console

Federated identity users must change their password from an AWS access portal. For more information, see [Resetting your AWS IAM Identity Center user password](#) in the *AWS IAM Identity Center User Guide*.

Federated identity users sign in using an external identity provider (IdP). You're a federated identity if you either:

- Access your AWS account or resources with third party credentials like Login with Amazon, Facebook, or Google.
- Use the same credentials to sign in to corporate systems and AWS services and you use a custom company portal to sign-in to AWS.

For more information, see [Federated identity](#) in the *AWS Sign-In User Guide*.

Changing the language of the AWS Management Console

The AWS Console Home experience includes the Unified Settings page where you can change the default language for AWS services in the AWS Management Console. You can also change the default language quickly from the settings menu from the navigation bar.

Note

The following procedures change the language for all AWS service consoles, but not for AWS documentation. To change the language used for documentation, use the language menu in the upper right of any documentation page.

Topics

- [Supported languages](#)
- [Changing default language from the navigation bar in the AWS Management Console](#)
- [Changing the default language via Unified Settings in the AWS Management Console](#)

Supported languages

The AWS Management Console currently supports the following languages:

- English (US)
- English (UK)
- Bahasa Indonesia
- German
- Spanish
- French
- Japanese
- Italian
- Portuguese
- Korean
- Chinese (Simplified)
- Chinese (Traditional)
- Turkish

Changing default language from the navigation bar in the AWS Management Console

The following procedure details how to change your default language directly from the navigation bar.

To change the default language from the navigation bar

1. Sign in to the [AWS Management Console](#).
2. In the navigation bar, choose the gear icon (#).
3. For **Language**, choose either **Browser default** or the preferred language from the dropdown list.

Changing the default language via Unified Settings in the AWS Management Console

The following procedure details how to change your default language from the Unified Settings page.

To change the default language in Unified Settings

1. Sign in to the [AWS Management Console](#).
2. In the navigation bar, choose the gear icon (#).
3. To open the **Unified Settings** page, choose **See all user settings**.
4. In **Unified Settings**, choose **Edit** next to **Localization and default Region**.
5. To select the language that you want for the console, choose one of the following options:
 - Choose the **Browser default** from the dropdown list, and then choose **Save settings**.

The console text for all AWS services appears in your preferred language that you've set in your browser settings.

Note

The browser default only supports languages supported by the AWS Management Console.

- Choose the preferred language from the dropdown list, and then choose **Save settings**.

The console text for all AWS services appears in your preferred language.

Accessing your AWS account, organization, service quota, and billing information in the AWS Management Console

If you have the necessary permissions, you can access information about your AWS account, service quotas, organization, and billing information from the console.

Note

The AWS Management Console only provides access to account, organization, service quota, and billing information. These services have their own separate consoles. For more information, see the following:

- [Manage your AWS account](#) in the *AWS Account Management Reference Guide*.
- [What is AWS Organizations?](#) in the *AWS Organizations User Guide*.
- [What is Service Quotas?](#) in the *Service Quotas User Guide*.

- [Using the AWS Billing and Cost Management home page](#) in the *AWS Billing User Guide*.

Tip

You can also get more information about any of these topics by asking Amazon Q. For more information, see [Chat with Amazon Q Developer](#).

Topics

- [Accessing account information in the AWS Management Console](#)
- [Accessing organization information in the AWS Management Console](#)
- [Accessing service quota information in the AWS Management Console](#)
- [Accessing billing information in the AWS Management Console](#)

Accessing account information in the AWS Management Console

If you have the necessary permissions, you can access information about your AWS account from the console.

To access your account information

1. Sign in to the [AWS Management Console](#).
2. On the navigation bar, choose your account name.
3. Choose **Account**.
4. View your account information.

Note

If you would like to close your AWS account, see [Close an AWS account](#) in the *AWS Account Management Reference Guide*.

Accessing organization information in the AWS Management Console

If you have the necessary permissions, you can access information about your AWS organizations from the console.

To access organization information

1. Sign in to the [AWS Management Console](#).
2. On the navigation bar, choose your account name.
3. Choose **Organizations**.
4. View your organization information.

Accessing service quota information in the AWS Management Console

If you have the necessary permissions, you can access information about service quotas from the console.

To access service quota information

1. Sign in to the [AWS Management Console](#).
2. On the navigation bar, choose your account name.
3. Choose **Service Quotas**.
4. View and manage your service quota information.

Accessing billing information in the AWS Management Console

If you have the necessary permissions, you can access information about your AWS charges from the console.

To access your billing information

1. Sign in to the [AWS Management Console](#).
2. On the navigation bar, choose your account name.
3. Choose **Billing and Cost Management**.
4. Use the AWS Billing and Cost Management dashboard to find a summary and a breakdown of your monthly spending.

Signing in to multiple accounts

You can sign in to up to five different identities simultaneously in a single web browser in the AWS Management Console. These can be any combination of root, IAM, or federated roles in different accounts or in the same account. Each identity you sign in to opens its own instance of the AWS Management Console in a new tab.

When you enable multi-session support, the console URL contains a subdomain (for example, <https://000000000000-aaaaaaa.us-east-1.console.aws.amazon.com/console/home?region=us-east-1>). Be sure to update your bookmarks and console links.

Note

You must opt-in to multi-session support by choosing **Turn on multi-session** in the account menu in the AWS Management Console, or by choosing **Enable multi-session** on <https://eusc-de-east-1.console.amazonaws-eusc.eu/>. You can opt-out of multi-sessions at any time by choosing **Disable multi-session** on <https://eusc-de-east-1.console.amazonaws-eusc.eu/> or by clearing your browser cookies. Opt-in is browser specific.

To sign in to multiple identities

1. Sign in to the [AWS Management Console](#).
2. In the navigation bar, choose your account name.
3. Choose **Add session** and choose **Sign in**. A new tab will open for you to sign in.

Note

For more information about signing in as a root or IAM user, see [Sign in to the AWS Management Console](#) in the *AWS Sign-in User Guide*.

4. Enter your credentials.
5. Choose **Sign in**. The AWS Management Console loads in this tab as your chosen AWS identity.
6. **(Optional) To federate into additional roles**
 - a. In the AWS IAM Identity Center access portal or your single-sign on (SSO) portal, sign in to the additional role.
 - b. In the AWS Management Console choose your account name.

- c. View the additional sessions that you can choose.

AWS Recommended Actions in the AWS Management Console

AWS Recommended Actions helps you work more efficiently in the AWS Management Console by providing contextual suggestions for completing tasks and implementing best practices. When relevant recommendations are available, a dynamic button appears that you can use to quickly take action based on these suggestions.

Note

AWS Recommended Actions analyzes resource state to provide suggestions but doesn't process user data.

Topics

- [Features of AWS Recommended Actions](#)
- [Using recommended actions](#)
- [Logging AWS Recommended Actions API calls using AWS CloudTrail](#)

Features of AWS Recommended Actions

- **Action recommendations** — Get relevant suggestions based on resource state, best practices, and common usage patterns
- **One-click actions** — Complete recommended actions directly from success messages or resource views
- **Integrated right side panel** — Access an integrated side panel to implement suggestions without disrupting your workflow
- **Multi-service support** — Get recommendations across multiple AWS services

Using recommended actions

To use recommended actions

1. Sign in to the [AWS Management Console](#)

2. Look for the **# Recommended actions** button.

 Note

The recommended actions button can appear anywhere in the AWS Management Console and is only accessible when recommended actions are available.

3. Choose the button to view available actions.
4. Run recommendations directly or through the side panel.

Logging AWS Recommended Actions API calls using AWS CloudTrail

AWS Recommended Actions is integrated with [AWS CloudTrail](#), a service that provides a record of actions taken by a user, role, or an AWS service. CloudTrail captures all API calls for AWS Recommended Actions as events. The calls captured include calls from the AWS Management Console and code calls to the AWS Recommended Actions API operations. Using the information collected by CloudTrail, you can determine the request that was made to AWS Recommended Actions, the IP address from which the request was made, when it was made, and additional details.

CloudTrail is active in your AWS account when you create the account and you automatically have access to the CloudTrail **Event history**. The CloudTrail **Event history** provides a viewable, searchable, downloadable, and immutable record of the past 90 days of recorded management events in an AWS Region. For more information, see [Working with CloudTrail Event history](#) in the *AWS CloudTrail User Guide*. There are no CloudTrail charges for viewing the **Event history**.

For an ongoing record of events in your AWS account past 90 days, create a trail or a [CloudTrail Lake](#) event data store.

AWS Recommended Actions management events in CloudTrail

[Management events](#) provide information about management operations that are performed on resources in your AWS account. These are also known as control plane operations. By default, CloudTrail logs management events.

AWS Recommended Actions logs all AWS Recommended Actions control plane operations as management events.

AWS Recommended Actions event examples

An event represents a single request from any source and includes information about the requested API operation, the date and time of the operation, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so events don't appear in any specific order.

The following example shows a CloudTrail event that demonstrates the operation.

```
{
  "awsRegion": "us-east-2",
  "eventCategory": "Management",
  "eventID": "3510a29e-8070-4cbc-b6a0-9e11f18e26ec",
  "eventName": "ListRecommendedActions",
  "eventSource": "action-recommendations.amazonaws.com",
  "eventTime": "2025-09-03T03:52:02Z",
  "eventType": "AwsApiCall",
  "eventVersion": "1.09",
  "managementEvent": true,
  "readOnly": true,
  "recipientAccountId": "123456789098",
  "requestID": "ec431c91-0315-413d-bdb6-d282fd4f6d83",
  "requestParameters": {
    "context": "*",
    "uxChannel": "EXAMPLE"
  },
  "responseElements": null,
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "EXAMPLE",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROARZDBH75ZCUYWFSTUS:EXAMPLE",
    "arn": "arn:aws:sts::123456789098:assumed-role/EXAMPLE",
    "accountId": "12345678909",
    "accessKeyId": "ASIARZDBEXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROARZDBHEXAMPLE",
        "arn": "arn:aws:iam::12345678909:role/EXAMPLE",
        "accountId": "12345678909",
        "userName": "EXAMPLE"
      }
    }
  },
}
```

```
    "attributes": {
      "creationDate": "2025-09-03T03:52:00Z",
      "mfaAuthenticated": "false"
    },
    "invokedBy": "action-recommendations.amazonaws.com"
  }
}
```

For information about CloudTrail record contents, see [CloudTrail record contents](#) in the *AWS CloudTrail User Guide*.

Using AWS Console Home in the AWS Management Console

This topic describes how to use AWS Console Home, including how to customize your Console Home page. Console Home is the home page of the AWS Management Console. When you first log in to the console, you land on the Console Home page. You can customize your Console Home page using widgets and applications. Widgets let you add custom components that track information about your AWS services and resources. Applications allow you to group your AWS resources and metadata. You can manage applications using myApplications. You can also use Console Home to view a list of all AWS services and chat with Amazon Q.

Topics

- [Viewing all AWS services in AWS Console Home](#)
- [Working with widgets in AWS Console Home](#)
- [Chatting with Amazon Q Developer in AWS Console Home](#)

Viewing all AWS services in AWS Console Home

You can view a list of all AWS services and access their consoles from Console Home.

To access a complete list of AWS services

1. Sign in to the [AWS Management Console](#).
2. Expand the Console Home menu by choosing the hamburger icon (≡).
3. Choose **All services**.
4. Select an AWS service to navigate to its console.

Working with widgets in AWS Console Home

The Console Home dashboard includes widgets that display important information about your AWS environment and provide shortcuts to your services. You can customize your experience by adding and removing widgets, rearranging them, or changing their size.

Managing widgets

You can manage widgets by adding, removing, rearranging, and resizing them. Default widgets can be removed and added again. You can also reset your Console Home to the default layout and request new widgets.

To add a widget

1. On the upper or lower right of the Console Home dashboard, choose the **+Add widgets** button.
2. Choose the **drag indicator**, represented by six vertical dots (::) in the upper left of the widget title bar, and then drag it to your Console Home dashboard.

To remove a widget

1. Choose the **ellipsis**, represented by three vertical dots (:) in the upper right of the widget title bar.
2. Choose **Remove widget**.

To rearrange your widgets

- Choose the **drag indicator**, represented by six vertical dots (::) in the upper left of the widget title bar, and then drag the widget to a new location on your Console Home dashboard.

To resize a widget

- Choose the **resize icon** at the bottom right of the widget, and then drag to resize the widget.

If you want to start over with organizing and setting up your widgets, you can reset the Console Home dashboard to the default layout. This will revert your changes to the Console Home dashboard layout, and restore all the widgets to their default location and size.

To reset the page to the default layout

1. On the upper right of the page, choose the **Reset to default layout** button.
2. To confirm, choose **Reset**.

Note

This will revert all your changes to the layout of the Console Home dashboard.

To request a new widget in the Console Home dashboard

1. On the lower left of the Console Home dashboard, choose **Want to see another widget? Tell us!**

Describe the widget that you want to see added in the Console Home dashboard.

2. Choose **Submit**.

Note

Your suggestions are periodically reviewed and new widgets might be added in future updates to the AWS Management Console.

Chatting with Amazon Q Developer in AWS Console Home

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 Amazon Q any questions about AWS, including questions about AWS architecture, your AWS resources, best practices, documentation, and more. You can also create support cases and receive assistance from a live agent. For more information, see [What is Amazon Q?](#) in the *Amazon Q Developer User Guide*.

Get started with Amazon Q

You can start chatting with Amazon Q in the AWS Management Console, AWS Documentation websites, AWS websites, or the AWS Console Mobile Application by choosing the hexagonal Amazon Q icon. For more information, see [Get started with Amazon Q Developer](#) in the *Amazon Q Developer User Guide*.

Example questions

Following are some example questions you can ask Amazon Q:

- How do I get billing support?

- How do I create an EC2 instance?
- How do I troubleshoot a "Failed to load" error?
- How do I close an AWS account?
- Can you connect me with a person?

AWS User Experience Customization (UXC)

AWS User Experience Customization (UXC) is a utility that lets account administrators customize the visual appearance of the AWS Management Console and manage these settings at the account level.

With UXC, you can customize the following settings:

- **Account color** – You can set a color for your accounts to visually distinguish between them. For example, you can use green for development accounts, yellow for test accounts, and red for production accounts.
- **Service visibility** – You can control which AWS services appear in the console navigation. Service visibility simplifies the AWS Management Console to show only the AWS services that are relevant to your account.
- **Region visibility** – You can control which AWS Regions appear in the Region selector. Region visibility simplifies the AWS Management Console to show only the Regions that are relevant to your account.

If you have not configured a setting, then the default behavior applies: all services and Regions are visible, and no account color is set. You can reset account color to its default by setting the value to "none". You can reset visible services and Regions to their defaults by setting their values to null.

Note

The `visibleServices` and `visibleRegions` settings control only the appearance of services and Regions in the AWS Management Console. They do not restrict access through the AWS Command Line Interface, SDKs, or other APIs.

Topics

- [Getting started with AWS User Experience Customization](#)
- [UXC API Reference](#)
- [Logging AWS User Experience Customization API calls using AWS CloudTrail](#)
- [Security in AWS User Experience Customization](#)

Getting started with AWS User Experience Customization

With UXC, account administrators can configure account customizations for the AWS Management Console.

Prerequisites

Before you begin, you need the following:

- An AWS account
- Appropriate AWS Identity and Access Management (IAM) permissions for UXC. For more information, see [How AWS User Experience Customization works with IAM](#) and [AWS managed policies for the AWS Management Console](#).

Accessing UXC settings in the AWS Management Console

To access account color in the AWS Management Console, see [Accessing account information in the AWS Management Console](#). To access service visibility and Region visibility in the AWS Management Console, see [Configuring the AWS Management Console using Unified Settings](#).

To set an account color in the console

1. Sign in to the [AWS Management Console](#).
2. On the navigation bar, choose your account name.
3. Choose **Account**.
4. In **Account display settings**, choose a color.
5. Choose **Update**.

To set visible Regions in the console

1. Sign in to the [AWS Management Console](#).
2. Open [Unified Settings](#).
3. Choose **Edit** in the **Visible Regions** section.
4. Set your visible Regions to **All available Regions** or **Select Regions** and configure your list.
5. Choose **Save changes**.

To set visible services in the console

1. Sign in to the [AWS Management Console](#).
2. Open [Unified Settings](#).
3. Choose **Edit** in the **Visible services** section.
4. Set your visible services to **All services** or **Select services** and configure your list.
5. Choose **Save changes**.

Accessing UXC settings programmatically

You can also manage account customization settings programmatically or as infrastructure as code. For more information, see the [AWS User Experience Customization API Reference](#) and the [AWS::UXC::AccountCustomization](#) CloudFormation template reference.

UXC API Reference

The [AWS User Experience Customization API Reference](#) contains a complete list of operations supported in UXC.

Logging AWS User Experience Customization API calls using AWS CloudTrail

AWS User Experience Customization is integrated with [AWS CloudTrail](#), a service that provides a record of actions taken by a user, role, or an AWS service. CloudTrail captures API calls for UXC as events, including management events and data events. The calls captured include calls from the UXC console and code calls to the UXC API operations. Using the information collected by CloudTrail, you can determine the request that was made to UXC, the IP address from which the request was made, when it was made, and additional details.

CloudTrail is active in your AWS account when you create the account and you automatically have access to the CloudTrail **Event history**. The CloudTrail **Event history** provides a viewable, searchable, downloadable, and immutable record of the past 90 days of recorded management events in an AWS Region. For more information, see [Working with CloudTrail Event history](#) in the *AWS CloudTrail User Guide*. There are no CloudTrail charges for viewing the **Event history**.

For an ongoing record of events in your AWS account past 90 days, create a trail or a [CloudTrail Lake](#) event data store.

UXC data events in CloudTrail

[Data events](#) provide information about the resource operations performed on or in a resource (for example, reading or writing to an Amazon S3 object). These are also known as data plane operations. Data events are often high-volume activities. By default, CloudTrail doesn't log data events. The CloudTrail **Event history** doesn't record data events.

Additional charges apply for data events. For more information about CloudTrail pricing, see [AWS CloudTrail Pricing](#).

You can log data events for the UXC resource types by using the CloudTrail console, AWS CLI, or CloudTrail API operations. For more information about how to log data events, see [Logging data events with the AWS Management Console](#) and [Logging data events with the AWS Command Line Interface](#) in the *AWS CloudTrail User Guide*.

The following table lists the UXC resource types for which you can log data events. The **Resource type (console)** column shows the value to choose from the **Resource type** list on the CloudTrail console. The **resources.type value** column shows the `resources.type` value, which you would specify when configuring advanced event selectors using the AWS CLI or CloudTrail APIs. The **Data APIs logged to CloudTrail** column shows the API calls logged to CloudTrail for the resource type.

Resource type (console)	resources.type value	Data APIs logged to CloudTrail
UXC account customization	AWS::UXC::AccountCustomization	GetAccountCustomizations

You can configure advanced event selectors to filter on the `eventName`, `readOnly`, and `resources.ARN` fields to log only those events that are important to you. For more information about these fields, see [AdvancedFieldSelector](#) in the *AWS CloudTrail API Reference*.

UXC management events in CloudTrail

[Management events](#) provide information about management operations that are performed on resources in your AWS account. These are also known as control plane operations. By default, CloudTrail logs management events.

AWS User Experience Customization logs the following UXC control plane operations to CloudTrail as management events.

- [UpdateAccountCustomizations](#)

UXC event examples

An event represents a single request from any source and includes information about the requested API operation, the date and time of the operation, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so events don't appear in any specific order.

The following example shows a CloudTrail event that demonstrates the `GetAccountCustomizations` operation.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:jdope",
    "arn": "arn:aws:sts::111122223333:assumed-role/MyRole/jdope",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/MyRole",
        "accountId": "111122223333",
        "userName": "MyRole"
      },
      "attributes": {
        "creationDate": "2026-03-06T15:15:16Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2026-03-06T15:36:13Z",
  "eventSource": "uxc.amazonaws.com",
  "eventName": "GetAccountCustomizations",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.0",
```

```
"userAgent": "aws-sdk-java/2.41.27",
"requestParameters": null,
"responseElements": null,
"requestID": "543db7ab-b4b2-11e9-8925-d139e92a1fe8",
"eventID": "5b2805a5-3e06-4437-a7a2-b5fdb5cbb4e2",
"readOnly": true,
"resources": [
  {
    "accountId": "111122223333",
    "type": "AWS::UXC::AccountCustomization",
    "ARN": "arn:aws:uxc::111122223333:account-customizations"
  }
],
"eventType": "AwsApiCall",
"managementEvent": false,
"recipientAccountId": "111122223333",
"eventCategory": "Data"
}
```

For information about CloudTrail record contents, see [CloudTrail record contents](#) in the *AWS CloudTrail User Guide*.

Security in AWS User Experience Customization

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

Security is a shared responsibility between AWS and you. The 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 .
- **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 UXC. The following topics show you how to configure UXC to meet your security and

compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your UXC resources.

Topics

- [Identity and Access Management for AWS User Experience Customization](#)

Identity and Access Management for AWS User Experience Customization

AWS User Experience Customization (UXC) uses IAM policies to manage access to UXC API Operations.

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 User Experience Customization resources. IAM is an AWS service that you can use with no additional charge.

Topics

- [Audience](#)
- [Authenticating with identities](#)
- [Managing access using policies](#)
- [How AWS User Experience Customization works with IAM](#)
- [Identity-based policy examples for AWS User Experience Customization](#)

Audience

How you use AWS Identity and Access Management (IAM) differs based on your role:

- **Service user** - request permissions from your administrator if you cannot access features (see [Troubleshooting AWS User Experience Customization identity and access](#))
- **Service administrator** - determine user access and submit permission requests (see [How AWS User Experience Customization works with IAM](#))
- **IAM administrator** - write policies to manage access (see [Identity-based policy examples for AWS User Experience Customization](#))

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be authenticated as the AWS account root user, an IAM user, or by assuming an IAM role.

You can sign in as a federated identity using credentials from an identity source like AWS IAM Identity Center (IAM Identity Center), single sign-on authentication, or Google/Facebook credentials. For more information about signing in, see [How to sign in to your AWS account](#) in the *AWS Sign-In User Guide*.

For programmatic access, AWS provides an SDK and CLI to cryptographically sign requests. For more information, see [AWS Signature Version 4 for API requests](#) in the *IAM User Guide*.

AWS account root user

When you create an AWS account, you begin with one sign-in identity called the AWS account *root user* that has complete access to all AWS services and resources. We strongly recommend that you don't use the root user for everyday tasks. For tasks that require root user credentials, see [Tasks that require root user credentials](#) in the *IAM User Guide*.

IAM users and groups

An [IAM user](#) is an identity with specific permissions for a single person or application. We recommend using temporary credentials instead of IAM users with long-term credentials. For more information, see [Require human users to use federation with an identity provider to access AWS using temporary credentials](#) in the *IAM User Guide*.

An [IAM group](#) specifies a collection of IAM users and makes permissions easier to manage for large sets of users. For more information, see [Use cases for IAM users](#) in the *IAM User Guide*.

IAM roles

An [IAM role](#) is an identity with specific permissions that provides temporary credentials. You can assume a role by [switching from a user to an IAM role \(console\)](#) or by calling an AWS CLI or AWS API operation. For more information, see [Methods to assume a role](#) in the *IAM User Guide*.

IAM roles are useful for federated user access, temporary IAM user permissions, cross-account access, cross-service access, and applications running on Amazon EC2. For more information, see [Cross account resource access in IAM](#) 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 defines permissions when associated with an identity or resource. AWS evaluates these policies when a principal makes a request. Most policies are stored in AWS as JSON documents. For more information about JSON policy documents, see [Overview of JSON policies](#) in the *IAM User Guide*.

Using policies, administrators specify who has access to what by defining which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. An IAM administrator creates IAM policies and adds them to roles, which users can then assume. IAM policies define permissions regardless of the method used to perform the operation.

Identity-based policies

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

Identity-based policies can be *inline policies* (embedded directly into a single identity) or *managed policies* (standalone policies attached to multiple identities). To learn how to choose between managed and inline policies, see [Choose 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. Examples include 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. You must [specify a principal](#) in a resource-based policy.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

Other policy types

AWS supports additional policy types that can set the maximum permissions granted by more common policy types:

- **Permissions boundaries** – Set the maximum permissions that an identity-based policy can grant to an IAM entity. For more information, see [Permissions boundaries for IAM entities](#) in the *IAM User Guide*.
- **Service control policies (SCPs)** – Specify the maximum permissions for an organization or organizational unit in AWS Organizations. For more information, see [Service control policies](#) in the *AWS Organizations User Guide*.
- **Resource control policies (RCPs)** – Set the maximum available permissions for resources in your accounts. For more information, see [Resource control policies \(RCPs\)](#) in the *AWS Organizations User Guide*.
- **Session policies** – Advanced policies passed as a parameter when creating a temporary session for a role or federated user. 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 AWS User Experience Customization works with IAM

AWS User Experience Customization (UXC) works with IAM policies to manage access to UXC API Operations.

Before you use IAM to manage access to AWS User Experience Customization (User Experience Customization), learn what IAM features are available to use with User Experience Customization. We recommend you integrate with User Experience Customization through an AWS managed policy, for more information, see [AWS managed policies for the AWS Management Console](#).

Before you use IAM to manage access to User Experience Customization, learn what IAM features are available to use with User Experience Customization.

IAM feature	User Experience Customization support
Identity-based policies	Yes
Resource-based policies	No
Policy actions	Yes

IAM feature	User Experience Customization support
Policy resources	No
Policy condition keys	No
Temporary credentials	Yes
Cross-service principal permissions	No
Service-linked roles	No
Service roles	No

To get a high-level view of how User Experience Customization 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 User Experience Customization

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

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

To view examples of User Experience Customization identity-based policies, see [Identity-based policy examples for AWS User Experience Customization](#).

Policy actions for User Experience Customization

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

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

To see all User Experience Customization actions, refer to the [API Reference](#).

Policy actions in User Experience Customization use the `uxc:` prefix before the action (for example `uxc:GetAccountCustomizations`).

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

```
"Action": [  
    "uxc:GetAccountCustomizations",  
    "uxc:ListServices"  
]
```

To view examples of User Experience Customization identity-based policies, see [Identity-based policy examples for AWS User Experience Customization](#).

Policy resources for User Experience Customization

User Experience Customization does not support policy resources.

Using temporary credentials with User Experience Customization

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

Troubleshooting AWS User Experience Customization identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with User Experience Customization and IAM.

If you receive an error that you're not authorized to perform an action, your policies must be updated to allow you to perform the action.

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

```
User: arn:aws-eusc:iam::123456789012:user/mateojackson is not authorized to perform:  
uxc:GetWidget on resource: my-example-widget because no identity-based policy allows  
the GetWidget action
```

In this case, the policy for the `mateojackson` user must be updated to allow access to the *my-example-widget* resource by using the `uxc:GetWidget` action.

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

After you create your IAM user access keys, you can view your access key ID at any time. However, you can't view your secret access key again. If you lose your secret key, you must create a new access key pair.

Access keys consist of two parts: an access key ID (for example, AKIAIOSFODNN7EXAMPLE) and a secret access key (for example, wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY). Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. Manage your access keys as securely as you do your user name and password.

 Important

Do not provide your access keys to a third party, even to help [find your canonical user ID](#). By doing this, you might give someone permanent access to your AWS account.

When you create an access key pair, you are prompted to save the access key ID and secret access key in a secure location. The secret access key is available only at the time you create it. If you lose your secret access key, you must add new access keys to your IAM user. You can have a maximum of two access keys. If you already have two, you must delete one key pair before creating a new one. To view instructions, see [Managing access keys](#) in the *IAM User Guide*.

To allow others to access User Experience Customization, you must grant permission to the people or applications that need access. If you are using AWS IAM Identity Center to manage people and applications, you assign permission sets to users or groups to define their level of access. Permission sets automatically create and assign IAM policies to IAM roles that are associated with the person or application. For more information, see [Permission sets](#) in the *AWS IAM Identity Center User Guide*.

If you are not using IAM Identity Center, you must create IAM entities (users or roles) for the people or applications that need access. You must then attach a policy to the entity that grants them the correct permissions in User Experience Customization. After the permissions are granted, provide the credentials to the user or application developer. They will use those credentials to access AWS. To learn more about creating IAM users, groups, policies, and permissions, see [IAM Identities](#) and [Policies and permissions in IAM](#) in the *IAM User Guide*.

Identity-based policy examples for AWS User Experience Customization

By default, users and roles don't have permission to get or modify UXC resources. To grant users permission to perform actions on resources, an IAM administrator can create IAM policies. To learn how to create an IAM identity-based policy by using these example JSON policy documents, see [Create IAM policies \(console\)](#) in the *IAM User Guide*.

Topics

- [Policy best practices](#)
- [Read-only access to UXC Account Customizations](#)
- [Full access to UXC Account Customizations](#)

Policy best practices

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

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see [AWS managed policies](#) or [AWS managed policies for job functions](#) in the *IAM User Guide*.
- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see [Policies and permissions in IAM](#) in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as CloudFormation. For more information, see [IAM JSON policy elements: Condition](#) in the *IAM User Guide*.
- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies

adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see [Validate policies with IAM Access Analyzer](#) in the *IAM User Guide*.

- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see [Secure API access with MFA](#) in the *IAM User Guide*.

For more information about best practices in IAM, see [Security best practices in IAM](#) in the *IAM User Guide*.

Read-only access to UXC Account Customizations

The following example shows how to create a policy that allows read-only access to UXC Account Customizations:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "uxc:GetAccountCustomizations",
        "uxc:ListServices"
      ],
      "Resource": "*"
    }
  ]
}
```

Full access to UXC Account Customizations

The following example shows how to create a policy that allows full access to UXC Account Customizations:

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

```
    "Effect": "Allow",
    "Action": [
        "uxc:*"
    ],
    "Resource": "*"
  }
]
```

AWS managed policies for the AWS Management Console

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.

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*.

AWS managed policy: AWSManagementConsoleBasicUserAccess

You can attach `AWSManagementConsoleBasicUserAccess` to your users, groups, and roles.

This policy grants the permissions necessary for non-administrative users of the AWS Management Console. This includes features such as resource discovery, notifications, browser-based shell access, and customized navigation.

Permissions details

This `AWSManagementConsoleBasicUserAccess` is grouped into the following sets of permissions:

- `cloudshell` – Allows principals full access to AWS CloudShell capabilities, including environment creation, session management, and command execution.
- `ec2` – Allows principals to describe Regions enabled for the account in [Unified Navigation](#).
- `notifications` – Allows principals to obtain events from AWS User Notifications.
- `q` – Allows principals to chat with Amazon Q Developer.
- `resource-explorer-2` – Allows principals to search and discover AWS resources using [Unified Search](#).
- `uxc` – Allows principals to read AWS User Experience Customization settings.
- `action-recommendations` – Allows principals to receive contextual action recommendations.
- `account` – Allows principals to retrieve information about the specified account including its account name, account ID, and account creation date and time.

To view the permissions for this policy, see [AWSManagementConsoleBasicUserAccess](#) in the *AWS Managed Policy Reference*.

AWS managed policy:

AWSManagementConsoleAdministratorAccess

You can attach `AWSManagementConsoleAdministratorAccess` to your users, groups, and roles.

This policy grants full access to configure and customize the AWS Management Console. It allows administrators to set account colors, enable user notifications, and configure resource discovery. It also includes permissions from the `AWSManagementConsoleBasicUserAccess` managed policy, which are essential for non-administrative users of the AWS Management Console.

Permissions details

This `AWSManagementConsoleAdministratorAccess` is grouped into the following sets of permissions:

- `cloudshell` – Allows principals full access to AWS CloudShell capabilities, including environment creation, session management, and command execution.
- `ec2` – Allows principals to describe Regions enabled for the account in [Unified Navigation](#).
- `notifications` – Allows principals to access and update notification configurations, events, and feature opt-in status.
- `q` – Allows principals to chat with Amazon Q Developer for AI-assisted support.
- `resource-explorer-2` – Allows principals to search and discover AWS resources using [Unified Search](#).
- `uxc` – Allows principals full access to AWS User Experience Customization settings.
- `action-recommendations` – Allows principals to receive contextual action recommendations.
- `account` – Allows principals to retrieve information about the specified account including its account name, account ID, and account creation date and time.

To view the permissions for this policy, see [AWSManagementConsoleAdministratorAccess](#) in the *AWS Managed Policy Reference*.

AWS Management Console updates to AWS managed policies

View details about updates to AWS managed policies for the AWS Management Console since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the AWS Management Console Document history page.

Change	Description	Date
AWSManagementConsoleBasicUserAccess – Updated policy	Added <code>uxc:GetAccountCustomizations</code> and <code>uxc:ListServices</code> permissions.	March 26, 2026
AWSManagementConsoleAdministratorAccess – Updated policy	Added <code>uxc:GetAccountCustomizations</code> , <code>uxc:UpdateAccountCustomizations</code> , and	March 26, 2026

Change	Description	Date
	<code>uxc:ListServices</code> permissions.	
AWSManagementConso leBasicUserAccess – Updated policy	Updated policy to add permissions to allow users to see account information and receive action recommendations while navigating the AWS Management Console.	December 9, 2025
AWSManagementConso leAdministratorAccess – Updated policy	Updated policy to add permissions to allow users to see account information and receive action recommendations while navigating the AWS Management Console.	December 9, 2025
AWSManagementConso leBasicUserAccess – New policy	Added a new AWS managed policy that grants permissions necessary for basic AWS Management Console navigation, account color viewing, and resource discovery.	August 14, 2025
AWSManagementConso leAdministratorAccess – New policy	Added a new AWS managed policy that provides full access to configure and customize the AWS Management Console.	August 14, 2025
AWS Management Console started tracking changes	AWS Management Console started tracking changes for its AWS managed policies.	August 14, 2025

Using Markdown in the Console

Some services in the AWS Management Console, such as Amazon CloudWatch, support the use of [Markdown](#) in certain fields. This topic explains the types of Markdown formatting supported in the console.

Contents

- [Paragraphs, Line Spacing, and Horizontal Lines](#)
- [Headings](#)
- [Text Formatting](#)
- [Links](#)
- [Lists](#)
- [Tables and Buttons \(CloudWatch Dashboards\)](#)

Paragraphs, Line Spacing, and Horizontal Lines

Paragraphs are separated by a blank line. To make sure that the blank line between the paragraphs renders when it is converted to HTML, add a new line with a non-break space () and then a blank line. Repeat this pair of lines to insert multiple blank lines one after the other, as in the following example:

```
&nbsp;
```

```
&nbsp;
```

To create a horizontal rule that separates the paragraphs, add a new line with three hyphens in a row: ---

```
Previous paragraph.
```

```
---
```

```
Next paragraph.
```

To create a text block with monospace type, add a line with three backticks (`). Enter the text to show in monospace type. Then, add another new line with three backticks. The following example shows text that will be formatted to monospace type when displayed:

```
```
```

This appears in a text box with a background shading.  
The text is in monospace.

```
```
```

Headings

To create headings, use the pound sign (#). A single pound sign and a space indicate a top-level heading. Two pound signs create a second-level heading, and three pound signs create a third-level heading. The following examples show a top-level, second-level, and third-level heading:

```
# Top-level heading
```

```
## Second-level heading
```

```
### Third-level heading
```

Text Formatting

To format text as italic, surround it with a single underscore (_) or asterisk (*) on each side.

```
*This text appears in italics.*
```

To format text as bold, surround it with double underscores or double asterisks on each side.

```
**This text appears in bold.**
```

To format text as strikethrough, surround it with two tildes (~) on each side.

```
~~This text appears in strikethrough.~~
```

Links

To add a text hyperlink, enter the link text surrounded by square brackets ([]), followed by the full URL in parentheses (()), as in the following example:

Choose `[link\_text](http://my.example.com)`.

Lists

To format lines as part of a bulleted list, add them on separate lines that start with with a single asterisk (*) and then a space, as in the following example:

```
Here is a bulleted list:  
* Ant  
* Bug  
* Caterpillar
```

To format lines as part of a numbered list, add them on separate lines that start with with a number, a period (.), and a space, as in the following example:

```
Here is a numbered list:  
1. Do the first step  
2. Do the next step  
3. Do the final step
```

Tables and Buttons (CloudWatch Dashboards)

CloudWatch dashboards text widgets support Markdown tables and buttons.

To create a table, separate columns using vertical bars (|) and rows using new lines. To make the first row a header row, insert a line between the header row and the first row of values. Then, add at least three hyphens (-) for each column in the table. Separate columns using vertical bars. The following example shows Markdown for a table with two columns, a header row, and two rows of data:

```
Table | Header  
----|-----  
Amazon Web Services | AWS  
1 | 2
```

The Markdown text in the previous example creates the following table:

Table	Header
Amazon Web Services	AWS
1	2

In a CloudWatch dashboard text widget, you can also format a hyperlink to appear as a button. To create a button, use `[button:Button text]`, followed by the full URL in parentheses(`( )`), as in the following example:

```
[button:Go to AWS](http://my.example.com)
[button:primary:This button stands out even more](http://my.example.com)
```

Troubleshooting

Consult this section to find solutions to common problems with the AWS Management Console.

You can also diagnose and troubleshoot common errors for some AWS services using Amazon Q Developer. For more information, see [Diagnose common errors in the console with Amazon Q Developer](#) in the *Amazon Q Developer User Guide*.

Topics

- [The page isn't loading properly](#)
- [My browser displays an 'access denied' error when connecting to the AWS Management Console](#)
- [My browser displays timeout errors when connecting to the AWS Management Console](#)
- [I want to change the language of the AWS Management Console but I can't find the language selection menu at the bottom of the page](#)

The page isn't loading properly

- If this problem only occurs occasionally, check your internet connection. Try to connect through a different network, or with or without a VPN, or try using a different web browser.
- If all impacted users are from the same team, it may be a privacy browser extension or security firewall issue. Privacy browser extensions and security firewalls can block access to the domains used by the AWS Management Console. Try turning off these extensions or adjusting firewall settings. To verify issues with your connection, open your browser developer tools ([Chrome](#), [Firefox](#)) and inspect the errors in the **Console** tab. The AWS Management Console uses domains' suffixes including the following list. This list is not exhaustive and can change with time. These domains' suffixes aren't used exclusively by AWS.
 - .a2z.com
 - .amazon.com
 - .amazonaws.com
 - .aws
 - .aws.com
 - .aws.dev
 - .awscloud.com

- .awsplayer.com
- .awsstatic.com
- .cloudfront.net
- .live-video.net

 Warning

Since July 31, 2022, AWS no longer supports Internet Explorer 11. We recommend that you use the AWS Management Console with other supported browsers. For more information, see [AWS News Blog](#).

My browser displays an 'access denied' error when connecting to the AWS Management Console

Recent changes made to the console might affect your access if all of the following conditions are met:

- You access AWS Management Console from a network that is configured to reach AWS service endpoints through VPC endpoints.
- You restrict access to AWS services by either using `aws:SourceIp` or `aws:SourceVpc` global condition key in your IAM policies.

We recommend you review the IAM policies that contain the `aws:SourceIp` or `aws:SourceVpc` global condition key. Apply both `aws:SourceIp` and `aws:SourceVpc` where applicable.

Some AWS Management Console features use dual-stack domains that support both IPv4 and IPv6 connections. If your IAM policy restricts access using `aws:SourceIp` with only IPv4 CIDR blocks, requests might fail when your operating system prefers IPv6 connections (or vice versa). To avoid this, include both IPv4 and IPv6 CIDR blocks in your `aws:SourceIp` condition. For more information, see [aws:SourceIp](#) in the *AWS Identity and Access Management User Guide*.

My browser displays timeout errors when connecting to the AWS Management Console

If there's a service outage in your default AWS Region, your browser might display a 504 Gateway Timeout error when trying to connect to the AWS Management Console. To log in to the AWS Management Console from a different Region, specify an alternate Regional endpoint in the URL. For example, if there's an outage in the us-west-1 (N. California) Region, to access the us-west-2 (Oregon) Region use the following template:

```
https://region.console.aws.amazon.com
```

For more information, see [AWS Management Console service endpoints](#) in the *AWS General Reference*.

To view the status of all AWS services, including the AWS Management Console, see [AWS Health Dashboard](#).

I want to change the language of the AWS Management Console but I can't find the language selection menu at the bottom of the page

The language selection menu has moved to the new Unified Settings page. To change the language of the AWS Management Console, [navigate to the Unified Settings page](#), and then choose the language for the console.

For more information, see [Changing the language of the AWS Management Console](#).

Document history

The following table describes important changes to the *AWS Management Console Getting Started Guide*, beginning in March 2021.

Change	Description	Date
myApplications availability change	myApplications no longer allows creation of new applications. For resource grouping capabilities, explore AWS Resource Groups. Learn more .	July 30, 2026
myApplications availability change	Effective July 30, 2026, myApplications will no longer allow creation of new applications or updates of existing applications. Existing users may continue to access and view their previously created applications. For resource grouping capabilities, explore AWS Resource Groups. Learn more .	June 30, 2026
Page added	New page added to describe AWS experimental preview. For more information, see Enabling AWS experimental preview .	June 15, 2026
Updated AWS managed policies	Updated the AWSManagementConsoleAdministratorAccess and AWSManagementConsoleBasicUserAccess policies with new UXC	March 26, 2026

Change	Description	Date
	permissions. For more information, see ??? .	
Page added	New page added to explain recommended actions. For more information, see ??? .	October 15, 2025
New AWS managed policies	Added two new policies to scope permissions for using, configuring, and customizing the AWS Management Console. • AWSManagementConsoleBasicUserAccess • AWSManagementConsoleAdministratorAccess	August 14, 2025
User Experience Customizations (UXC)	New service available.	August 14, 2025
Page updated	You can now view your applications in myApplications from the Services menu. For more information, see ??? .	July 29, 2025
Page added	New page added to explain multisession feature. For more information, see ??? .	December 6, 2024
Page updated	Changing your password page updated. For more information, see ??? .	June 18, 2024

Change	Description	Date
New pages added	New pages added to describe how to access the Services menu and AWS event notifications. For more information, see ??? and ??? .	June 18, 2024
Page updated	What is the AWS Management Console? page updated. For more information, see ??? .	June 18, 2024
Get support	A new page added to describe how to get support. For more information, see ??? .	June 18, 2024
Unified Navigation and AWS Console Home	New pages added to describe how to work with the console. For more information, see ??? and ??? .	June 18, 2024
Chat with Amazon Q	A new settings page detailing how users can ask AWS questions to Amazon Q Developer. For more information, see Chat with Amazon Q Developer .	May 29, 2024
Configuring Unified Settings	A new settings page for configuring settings and defaults that apply to the current user, including language and region. For more information, see Configuring Unified Settings .	April 6, 2022

Change	Description	Date
New AWS Console Home UI	New AWS Console Home UI, which includes widgets for displaying important usage information and shortcuts to AWS services. For more information, see Working with widgets .	February 25, 2022
Changing the Console language	Choose a different language for the AWS Management Console. For more information, see Changing the language of the AWS Management Console .	April 1, 2021
Launching CloudShell	Open AWS CloudShell from the AWS Management Console and run AWS CLI commands. For more information, see Launching AWS CloudShell .	March 22, 2021