AWS Sign-In
User Guide
AWS Sign-In: User Guide
Copyright © 2022 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is AWS Sign-In?</td>
<td>1</td>
</tr>
<tr>
<td>Terminology</td>
<td>1</td>
</tr>
<tr>
<td>Administrator</td>
<td>1</td>
</tr>
<tr>
<td>Account</td>
<td>1</td>
</tr>
<tr>
<td>Account root user</td>
<td>1</td>
</tr>
<tr>
<td>Credentials</td>
<td>2</td>
</tr>
<tr>
<td>Corporate credentials</td>
<td>2</td>
</tr>
<tr>
<td>Root user credentials</td>
<td>2</td>
</tr>
<tr>
<td>User</td>
<td>2</td>
</tr>
<tr>
<td>Verification code</td>
<td>2</td>
</tr>
<tr>
<td>About user types</td>
<td>2</td>
</tr>
<tr>
<td>Account root user</td>
<td>3</td>
</tr>
<tr>
<td>IAM user</td>
<td>3</td>
</tr>
<tr>
<td>IAM Identity Center user</td>
<td>3</td>
</tr>
<tr>
<td>About sign-in URLs</td>
<td>4</td>
</tr>
<tr>
<td>AWS access portal</td>
<td>4</td>
</tr>
<tr>
<td>IAM user sign-in URL</td>
<td>4</td>
</tr>
<tr>
<td>Federated identities URL</td>
<td>5</td>
</tr>
<tr>
<td>How to sign in to your AWS account</td>
<td>6</td>
</tr>
<tr>
<td>AWS Management Console</td>
<td>6</td>
</tr>
<tr>
<td>AWS access portal</td>
<td>6</td>
</tr>
<tr>
<td>Federated identity</td>
<td>7</td>
</tr>
<tr>
<td>AWS Command Line Interface</td>
<td>7</td>
</tr>
<tr>
<td>Signing in to the AWS Management Console</td>
<td>8</td>
</tr>
<tr>
<td>Signing in as the root user</td>
<td>9</td>
</tr>
<tr>
<td>Signing in as an IAM user</td>
<td>11</td>
</tr>
<tr>
<td>Signing in to the AWS access portal</td>
<td>15</td>
</tr>
<tr>
<td>Requirements</td>
<td>15</td>
</tr>
<tr>
<td>How to sign out of your AWS account</td>
<td>18</td>
</tr>
<tr>
<td>Signing out of the AWS Management Console</td>
<td>18</td>
</tr>
<tr>
<td>Signing out of the AWS access portal</td>
<td>19</td>
</tr>
<tr>
<td>Security best practices</td>
<td>21</td>
</tr>
<tr>
<td>Troubleshooting sign-in issues</td>
<td>22</td>
</tr>
<tr>
<td>My credentials aren't working</td>
<td>22</td>
</tr>
<tr>
<td>I don't have access to the email for my AWS account</td>
<td>23</td>
</tr>
<tr>
<td>My MFA device is lost or stopped working</td>
<td>23</td>
</tr>
<tr>
<td>How can I find my AWS account ID or alias</td>
<td>24</td>
</tr>
<tr>
<td>I can't access the sign-in page</td>
<td>24</td>
</tr>
<tr>
<td>I forgot my root user password for my AWS account</td>
<td>24</td>
</tr>
<tr>
<td>I forgot my IAM user password for my AWS account</td>
<td>27</td>
</tr>
<tr>
<td>I forgot my federated identity password for my AWS account</td>
<td>28</td>
</tr>
<tr>
<td>I forgot my IAM Identity Center password for my AWS account</td>
<td>29</td>
</tr>
<tr>
<td>I need my account verification code</td>
<td>31</td>
</tr>
<tr>
<td>I need to reactivate my suspended AWS account</td>
<td>31</td>
</tr>
<tr>
<td>I need to contact AWS Support for sign-in issues</td>
<td>31</td>
</tr>
<tr>
<td>I need to contact AWS Billing for billing issues</td>
<td>31</td>
</tr>
<tr>
<td>I need help managing my AWS account</td>
<td>31</td>
</tr>
<tr>
<td>Document history</td>
<td>32</td>
</tr>
</tbody>
</table>
What is AWS Sign-In?

This guide helps you determine what kind of information you need to sign in to AWS, such as your user type and sign-in page. Sign in through the AWS Management Console, a web application that comprises and refers to a broad collection of service consoles for managing AWS resources, or your company-specific AWS access portal. For more information about how to sign in to your AWS account, see Signing in to the AWS Management Console (p. 8) or Signing in to the AWS access portal (p. 15).

Looking to solve a sign-in issue? See Troubleshooting sign-in issues (p. 22). If you can’t find what you’re looking for in this guide, contact AWS Support through this form. Include a detailed description of your problem so that we can best help you.

Terminology

Amazon Web Services (AWS) uses common terminology to describe the sign in process. We recommend you read and understand these terms.

Administrator

Also referred to as a AWS account administrator or IAM administrator. The administrator, typically Information Technology (IT) personnel, is an individual who oversees an AWS account. Administrators have a higher level of permissions to the AWS account than other members of their organization. Administrators establish and implement settings for the AWS account. They also create AWS Identity and Access Management (IAM) or IAM Identity Center users. The administrator provides these users with their access credentials and a sign-in URL to sign in to AWS.

Account

A standard AWS account contains both your AWS resources and the identities that can access those resources. Accounts are associated with the account owner’s email address and password.

Note
To sign in to AWS, you need to know which type of AWS user you are. For more information about user types, see About user types (p. 2).

Account root user

Also referred to as the account owner or root user. A root user has complete access to all AWS services and resources in the AWS account. When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is the AWS account root user. You can sign in as the root user using the email address and password that you used to create the account. Root users sign in with the AWS Management Console.

For more information about IAM identities including the root user, see IAM Identities (users, user groups, and roles).

Important
We strongly recommend that you don’t use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform only a few account and service management
tasks. To view the tasks that require you to sign in as the root user, see Tasks that require root user credentials.

Credentials

Also referred to as access credentials or security credentials. Credentials are the information that users provide to AWS to sign in and gain access to AWS resources. Credentials can include an email address, a user name, a user defined password, an account ID or alias, a verification code, and a single use multi-factor authentication (MFA) code. In authentication and authorization, a system uses credentials to identify who is making a call and whether to allow the requested access. In AWS, these credentials are typically the access key ID and the secret access key.

For more information about credentials, see Understanding and getting your AWS credentials.

Note
The type of credentials a user must submit depends on their user type.

Corporate credentials

The credentials that users provide when accessing their corporate network and resources. Your corporate administrator can set up your AWS account to be accessible with the same credentials that you use to access your corporate network and resources. These credentials are provided to you by your administrator or help desk employee.

Root user credentials

The root user credentials are the same credentials used to sign in to the AWS Management Console as the root user.

User

A user is a person or application under an account that makes API calls to AWS products. Each user has a unique name within the AWS account and a set of security credentials that aren’t shared with others. These credentials are separate from the security credentials for the AWS account. Each user is associated with one and only one AWS account.

Verification code

A verification code is a code used to verify your identification during the sign-in process. The delivery methods for verification codes varies. They can be sent via text message or email. Check with your administrator for more information.

About user types

How you sign in to your AWS account depends on what type of AWS user you are. There are a few different types of AWS users. You’re either an account root user, an AWS Identity and Access Management (IAM) user, an IAM Identity Center user, or a federated identity.

Here are some guidelines to help you determine which user type you are:

• If you recently created an AWS account and want to sign in, you’re most likely the root user. For more information, see Account root user (p. 3).
• If you created the AWS account and do not have an administrator managing the account, you’re most likely the root user. For more information, see Account root user (p. 3).
• If you did not create the AWS account and were provided credentials by an administrator or help desk employee, you’re most likely an IAM user. For more information, see IAM user (p. 3).
• If you use the same credentials to sign in to corporate systems and AWS services, you’re most likely an IAM Identity Center user. For more information, see IAM Identity Center user (p. 3).
• If you have been provided with a AWS access portal URL, you’re most likely an IAM Identity Center user. For more information, see IAM Identity Center user (p. 3).
• If you access your AWS account or resources with third party credentials like Login with Amazon, Facebook, or Google, you’re most likely a federated identity. For more information, see Federated identity (p. 7).

Account root user

Also referred to as the account owner or root user. The root user has complete access to all AWS services and resources in the AWS account. When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is the AWS account root user. You can sign in as the root user using the email address and password that you used to create the account. Root users sign in with the AWS Management Console. For step-by-step instructions on how to sign in, see Signing in as the root user (p. 9).

Important
When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the AWS General Reference.

For more information about IAM identities including the root user, see IAM Identities (users, user groups, and roles) and AWS account root user.

IAM user

An IAM user is an entity you create in AWS. These users are the identities within your AWS account with specific custom permissions. IAM users require a name and password which they use to sign in to the AWS Management Console. For step-by-step instructions on how to sign in, see Signing in as an IAM user (p. 11).

For more information about IAM identities including the IAM user, see IAM Identities (users, user groups, and roles) and What is Identity and Access Management?.

IAM Identity Center user

An IAM Identity Center user signs in through the AWS access portal. The AWS access portal, which includes a specific sign-in URL, is provided by your administrator or help desk employee. If you created an IAM Identity Center user for your AWS account, an invitation to join IAM Identity Center was sent to that account’s email address. The specific sign-in URL is included in the email invitation. IAM Identity Center users are not able to sign in through the AWS Management Console. For step-by-step instructions on how to sign in, see Signing in to the AWS access portal (p. 15).

Note
We recommend that you bookmark the specific sign-in URL for the AWS access portal so that you can quickly access it later.
About sign-in URLs

There are a few different types of sign-in URLs for AWS users listed below.

- AWS access portal
- IAM user sign-in URL
- Federated identities URL

AWS access portal

Also referred to as a specific sign-in URL. The AWS access portal is a customizable link for IAM Identity Center users to sign in and access their account. Your administrator or help desk employee should have provided you with a specific sign-in URL like the following examples:

https://d-xxxxxxxxxx.awsapps.com/start

or

https://your_subdomain.awsapps.com/start

If you created an IAM Identity Center user for your AWS account, an invitation to join IAM Identity Center was sent to the email address of the AWS account.

Your specific sign-in URL varies because your administrator can customize it. The specific sign-in URL might begin with the letter D followed by 10 randomized numbers and letters. Your subdomain might also be used in the sign-in URL and may include your company name like the following example:

Note

We recommend that you bookmark the specific sign-in URL for the AWS access portal so that you can quickly access it later.

For more information about the AWS access portal, see Using the AWS access portal.

IAM user sign-in URL

IAM users can access the AWS Management Console with a specific IAM user sign-in URL. The IAM user sign-in URL is created by combining your AWS account ID or alias and signin.aws.amazon.com/console

An example of what an IAM user sign-in URL looks like:

https://account_alias_or_id.signin.aws.amazon.com/console/

If your account ID is 111122223333, your sign-in URL would be:
If you're experiencing issues accessing your AWS account with your IAM user sign-in URL, see Resilience in AWS Identity and Access Management for more information.

**Federated identities URL**

The sign-in URL for federated identities varies. The external identity or external Identity Provider (IdP) determines the sign-in URL for federated identities. The external identity could be Windows Active Directory, Login with Amazon, Facebook, or Google. Contact your administrator for more details on how to sign in as a federated identity.

For more information about federated identities, see About web identity federation.
How to sign in to your AWS account

You can access AWS using the following methods:

- AWS Management Console sign-in page
- AWS access portal sign-in page
- Federated identity
- Programmatic methods like API, AWS Command Line Interface, and SDK (Software Development Kit)

The way you sign in to your AWS account depends on what type of AWS user you are. There are a few different types of AWS users. You can be an account root user, an AWS Identity and Access Management (IAM) user, an AWS IAM Identity Center (successor to AWS Single Sign-On) user, or a federated identity.

AWS Management Console

Root and IAM users sign in through the AWS Management Console. The AWS Management Console provides a web-based user interface that you can use to create and manage your AWS resources. For example, you can start and stop Amazon Elastic Compute Cloud (EC2) instances, create Amazon DynamoDB tables, and create Amazon Simple Storage Service (S3) buckets.

- Root users sign in with:
  - Email address
  - Password
- IAM users sign in with:
  - Account ID or alias
  - User name or email address
  - Password
  - Your account owner or IAM administrator should provide you with your account ID or alias and user name to sign in. They create the account and set your user name. Your user name might be your email address.

For step-by-step directions on how to sign in to the AWS Management Console, see Signing in to the AWS Management Console (p. 8).

For more information about signing in with multi-factor authentication (MFA) devices, see Using MFA devices with your IAM sign-in page.

Important

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the AWS General Reference.

AWS access portal

IAM Identity Center users sign in through the AWS access portal rather than the AWS Management Console. After you sign in through the AWS access portal, you can access your AWS account and
applications. You can access cloud applications such as Office 365, Concur, and Salesforce through the AWS access portal. Your administrator or help desk employee should have provided you a specific sign-in URL like the following examples:

https://d-xxxxxxxxx.awsapps.com/start

or

https://your_subdomain.awsapps.com/start

Alternatively, if you created an IAM Identity Center user for your AWS account, you would have received an email invitation with the specific sign-in URL.

IAM Identity Center users sign in with:

- Corporate user name
- Corporate password
- If prompted for a verification code, check your email and then copy and paste the code into the sign-in page.
- Verification codes are typically sent through email, but the delivery method can vary. Your administrator establishes the security settings that requires users to provide a verification code. Check with your administrator for details.

For step-by-step directions on how to sign in to the AWS access portal, see Signing in to the AWS access portal (p. 15).

For more information about IAM Identity Center, see What is IAM Identity Center?

Federated identity

Federated identities are users that can access secure AWS account resources with external identities. External identities can come from a corporate identity store (such as LDAP or Windows Active Directory) or from a third party (such as Login in with Amazon, Facebook, or Google). Federated identities do not sign in with the AWS Management Console or AWS access portal. The type of external identity in use determines how federated identities sign in.

For more information about federated identities, see About web identity federation.

Administrators must create a custom URL that includes https://signin.aws.amazon.com/federation. For more information, see Enabling custom identity broker access to the AWS Management Console.

Note
Your administrator creates federated identities. Contact your administrator for more details on how to sign in as a federated identity.

AWS Command Line Interface

AWS users can also sign in with the AWS Command Line Interface (AWS CLI). For more information about the AWS CLI, see What is the AWS Command Line Interface.

The following video shows how to sign in to AWS accounts from the AWS CLI with IAM Identity Center credentials.
Signing in to the AWS Management Console

To sign in to the AWS Management Console, choose your user type. The account root user or account owner has unrestricted account access and is associated with the person who created the AWS account. The root user or an IAM administrator then creates other types of users and assigns them access credentials.

If you choose an unintended user type or use credentials that aren't for the user type you select, you might receive an error message similar to the following image. For your security, error messages are generic by design. The error messages don't explicitly state if you've selected the unintended user type or sign-in scenario. If you verify that your sign-in credentials are correct and you receive an error message while attempting to sign in, we recommend that you try to sign in as another user type.

For more information about the different kinds of users, see About user types (p. 2).
For more information about troubleshooting your sign-in issues, see *My credentials aren't working* (p. 22).

The following GIF shows an IAM Identity Center user attempting to sign in to the AWS Management Console. IAM Identity Center users can't sign in with the AWS Management Console. They sign in through the AWS access portal.

For more information on signing in to the AWS Management Console, see the following video.

*How do I sign in to the AWS Management Console?*

**Signing in as the root user**

The root user has complete access to all AWS services and resources in the account. The root user is automatically created when the AWS account is created. The root user creates the AWS account.

**Signing in as a root user**

**Requirements**

Before you sign in to an AWS account as the root user, gather the following information:

- The email address used to create the AWS account
- The password for the root user

**Important**

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see *Tasks that require root user credentials* in the *AWS General Reference*.

**To sign in to an AWS account as the root user**

2. If you have not signed in previously using this browser, the main sign-in page appears. *Root user* is selected by default. Enter the email address associated with your account and choose *Next*. 

![Sign in screen](https://example.com/sign-in.png)
**Note**
If you have previously signed in as a root user in this browser, your browser might remember the email address for the AWS account. If so, you’ll see the screen shown in the next step instead.
If you have signed in previously as an IAM user using this browser, your browser might display the IAM user sign in page instead. To return to the main sign-page, choose Sign in using root user email.

3. You might be prompted to complete a security check as shown in the following image. Complete the security check to move to the next step.

Security check
![Security check image](image)

4. Enter your password and choose Sign in.

Root user sign in

Email: **username@example.com**

Password:  
Forgot password?  
Sign in

Sign in to a different account  
Create a new AWS account

The following animated GIF demonstrates how to successfully sign in to the AWS Management Console as a root user.

![Sign in GIF](image)

For step-by-step directions on how to reset the root user password, see I forgot my root user password for my AWS account (p. 24).
**Signing in as an IAM user**

An IAM user represents the person or service that uses the IAM user to interact with AWS resources. These users are identities within your AWS account that have specific custom permissions. For example, IAM users have permissions to create a directory in AWS IAM Identity Center. IAM user names are unique within a single account. You can use the same user name in multiple accounts. This is why you have to indicate which account you're signing in to.

*For more information about AWS Identity and Access Management, see What is Identity and Access Management? and Identity and Access Management for AWS Account Management.*

**Signing in as an IAM user**

**Requirements**

Gather the following information before you sign in. If you do not have this information, contact the administrator of the AWS account.

- The 12-digit AWS account ID or the account alias
- The user name or email address for your IAM user
  - The IAM user name is created by the account administrator
- The password for your IAM user

**Note**

Your AWS account ID or alias can be found in the AWS Management Console. You must sign in to the AWS Management Console to view your AWS account ID or alias. If you are not signed in the AWS Management Console, contact your administrator for the information. For more information, see Your AWS account ID and its alias.

For more information about signing in as an IAM user with a MFA device, see Using MFA devices with your IAM sign-in page.

If you are an IAM user, you can sign in using either the AWS Management Console or the IAM user sign-in URL.

**To sign in to the AWS Management Console:**

2. If you have not previously signed in using this browser, the main sign-in page appears. Choose IAM user, enter the account ID (12 digits) or alias, and choose Next.

  **Warning**
  
  Do not use your user name or email address in this field. You must use the root user email address, the account ID, or the account alias in this field.
Note
You might not have to enter your account ID or alias if you've previously signed in as the IAM user with your current browser. Your browser might remember this information. If so, you'll see the screen shown in the next step instead.

3. Enter your IAM user name and password and choose Sign in.
Sign in as IAM user

Account ID (12 digits) or account alias

account_alias_or_id

IAM user name

Password

Remember this account

Sign in

Sign in using root user email

Forgot password?

**Note**
Choose **Sign in using root user email** to return to the main sign-in page if you previously signed in as an IAM user for a different AWS account in this browser, or you need to sign in as a root user.

To learn how to sign in to the AWS Management Console as an IAM user, see the following GIF.

For more information about signing in with multi-factor authentication (MFA) devices, see Using MFA devices with your IAM sign-in page.
For step-by-step directions on how to reset the IAM user password, see I forgot my IAM user password for my AWS account (p. 27).

**To sign in with the IAM user sign-in URL:**

1. Open a browser and enter the following sign-in URL, replacing `account_alias_or_id` with the account alias or account ID provided by your administrator:

   ```
   https://account_alias_or_id.signin.aws.amazon.com/console/
   ```

   For example, the following URL represents an account with 111122223333 as the account ID.

   ```
   https://111122223333.signin.aws.amazon.com/console/
   ```

2. Enter your IAM user name and password. Then, choose **Sign in**.

For more information about signing in with multi-factor authentication (MFA) devices, see Using MFA devices with your IAM sign-in page.

For step-by-step directions on how to reset the IAM user password, see I forgot my IAM user password for my AWS account (p. 27).
Signing in to the AWS access portal

AWS IAM Identity Center (successor to AWS Single Sign-On) users can access AWS accounts and business applications by signing in with a specific sign-in URL. This specific sign-in URL for the AWS access portal should have been provided by your administrator or help desk employee.

Requirements

Before you sign in to an AWS account as an IAM Identity Center user, gather the following required information.

- Corporate user name
- Corporate password
- Specific sign-in URL

If you do not have the above information, contact the administrator for the AWS account. If you created an IAM Identity Center user for your AWS account, AWS has already sent an invitation to join IAM Identity Center to the email address of the AWS account.

The specific sign-in URL is formatted like the following.

```
https://d-xxxxxxxxx.awsapps.com/start
```

or

```
https://your_subdomain.awsapps.com/start
```

Your specific sign-in URL might include your company’s subdomain like the following example.

```
https://AnyCompany.awsapps.com/start
```

Note
After you sign in, your AWS access portal session is valid for 8 hours. You are required to sign in again after 8 hours.

To sign in to the AWS access portal

1. In your browser window, paste in the sign-in URL that you were provided through email. Then, press Enter. We recommend that you bookmark this link now so that you can quickly access it later.
2. Sign in using your corporate credentials (like a user name and password). If you are prompted for a verification code, check your email for it. Then copy and paste the code into the sign-in page.

   **Note**
   Verification codes are typically sent through email, but the delivery method might vary. Check with your administrator for details about your verification code.

3. After you sign in, you can access any AWS account and application that appears in the portal. Choose the icon of the application that you want to access. See the following GIF for a tutorial on how to sign in to the AWS access portal as an IAM Identity Center user.
For more information about signing in to the AWS access portal, see [How do I get started with using IAM Identity Center and access the AWS access portal?](#).

For step-by-step directions on how to reset the IAM Identity Center user password, see [I forgot my IAM Identity Center password for my AWS account](#) (p. 29).
How to sign out of your AWS account

The way you sign out of your AWS account depends on what type of AWS user you are. You can be an account root user, an AWS Identity and Access Management (IAM) user, an IAM Identity Center user, or a federated identity.

The root user and IAM users sign in to the AWS Management Console. Both the root user and IAM users follow the same steps when signing out of the AWS Management Console.

IAM Identity Center users sign in to the AWS access portal.

Federated identities should contact their administrator for directions on signing out of their AWS account.

Signing out of the AWS Management Console

To sign out of the AWS Management Console

1. After you’re signed in to the AWS Management Console, you arrive at a page similar to the one shown in the following image. Your account name or IAM user name is shown in the upper right corner.

2. In the navigation bar on the upper right, choose your user name.
3. Select **Sign out** as shown in the following image.

4. You are returned to the AWS Management Console webpage.

**Signing out of the AWS access portal**

**To sign out of the AWS access portal**

1. After you've signed in to the AWS access portal, you arrive at a page similar to the one shown in the following image. Your user name is shown in the upper right corner.
2. When you're ready to sign out, select **sign out**. A tutorial of an IAM Identity Center user signing out is shown in the following animated GIF.

![AWS Sign-in](image)

3. You see the AWS access portal.
Security best practices for account administrators

If you’re an account administrator who has created a new AWS account, we recommend the following steps as a security best practice. For more information, see Security best practices in AWS Identity and Access Management for account administrators.

1. Sign in as the root user to Enable multi-factor authentication (MFA) and create an AWS administrative user in IAM Identity Center if you haven’t already done so. Then, safeguard your root credentials and don’t use them for everyday tasks.

2. Sign in as the AWS account administrator and set up the following identities:
   - Create least-privilege users for other humans.
   - Set up temporary credentials for workloads.
   - Create access keys only for use cases that require long-term credentials.

3. Add permissions to grant access to those identities. You can get started with AWS managed policies and move towards least-privilege permissions.
   - Add permission sets to AWS IAM Identity Center (successor to AWS Single Sign-On) users.
   - Add identity-based policies to IAM roles used for workloads.
   - Add identity-based polices for IAM users for use cases that require long-term credentials.
   - For more information about IAM users, see Security best practices in IAM.

4. Save and share information about How to sign in to your AWS account (p. 6). This information varies, depending on the type of identity you created.
Troubleshooting sign-in issues

Use the information here to help you troubleshoot sign-in and other AWS account issues. For step-by-step directions on signing in to an AWS account, see How to sign in to your AWS account (p. 6).

If you are having trouble signing in to Amazon.com, see Amazon Customer Service instead of this page.

Issues
- My credentials aren't working (p. 22)
- I don't have access to the email for my AWS account (p. 23)
- My MFA device is lost or stopped working (p. 23)
- How can I find my AWS account ID or alias (p. 24)
- I can't access the sign-in page (p. 24)
- I forgot my root user password for my AWS account (p. 24)
- I forgot my IAM user password for my AWS account (p. 27)
- I forgot my federated identity password for my AWS account (p. 28)
- I forgot my IAM Identity Center password for my AWS account (p. 29)
- I need my account verification code (p. 31)
- I need to reactivate my suspended AWS account (p. 31)
- I need to contact AWS Support for sign-in issues (p. 31)
- I need to contact AWS Billing for billing issues (p. 31)
- I need help managing my AWS account (p. 31)

My credentials aren't working

When you can't sign in to the AWS Management Console, try to remember how you previously accessed AWS.

If you don't remember using a password at all

You might have previously accessed AWS without using AWS credentials. This is common for enterprise single sign-on through IAM Identity Center. Accessing AWS this way means that you use your corporate credentials to access AWS accounts or applications without entering your credentials.

- AWS access portal – If an administrator allows you to use credentials from outside AWS to access AWS, you need the URL for your portal. Check your email, browser favorites, or browser history for a URL that includes awsapps.com/start or signin.aws/platform/login.

For example, your custom URL might include an ID or a domain such as https://d-1234567890.awsapps.com/start. If you can't find your portal link, contact your administrator. AWS Support can't help you recover this information.

If you remember your user name and password

You might be on the wrong page. Try signing in on a different page:

- Root user sign-in page – If you created or own an AWS account and need to perform restricted actions, enter your account email address in the AWS Management Console. To learn how to access the root user, see Signing in as a root user (p. 9). If you forgot your root user password, you can reset it. See I forgot my root user password for my AWS account (p. 24) for more information. If you forgot your AWS account email address, check your email inbox for an email from AWS.
I don't have access to the email for my AWS account

When you create an AWS account, you provide an email address and password. These are the credentials for the AWS account root user. If you are not sure of the email address associated with your AWS account, check for saved correspondence from no-reply@amazon.com to any email address for your organization that might have been used to open the AWS account. Ask other members of your team, organization, or family. If someone you know created the account, they can help you get access.

If you know the email address but no longer have access to the email, first try to recover access to the email using one of the following options:

- If you own the domain for the email address, you can restore a deleted email address. Alternatively, you can set up a catch-all for your email account, which "catches all" messages sent to email addresses that no longer exist in the mail server and redirects them to another email address.
- If the email address on the account is part of your corporate email system, we recommend that you contact your IT system administrators. They might be able to help you regain access to the email.

If you're still not able to sign in to your AWS account, you can find alternate support options by contacting AWS Support.

My MFA device is lost or stopped working

If your AWS account root user MFA device is lost, damaged, or not working, you can recover access to your account. IAM users must contact an administrator to deactivate the device. These users cannot recover their MFA device without the administrator’s assistance.
How can I find my AWS account ID or alias

You can find your AWS account ID or alias through the AWS Management Console. Root and IAM users must sign in to the AWS Management Console to locate their account ID or alias. For more information about your AWS account ID and alias and how to find it, see Your AWS account ID and its alias.

If you are an IAM user and you are not signed in, you must ask your administrator for the AWS account ID or alias. You need this information, plus your IAM user name and password, to sign in to your AWS account.

To learn how an administrator can manage your IAM password, see Managing passwords for IAM users.

If you are experiencing issues with your credentials, see I can't sign in because my credentials don't work. You can contact AWS Support with a Billing and Account Support request.

I can't access the sign-in page

If you cannot see your sign-in page, the domain may be blocked by a firewall. Contact your network administrator to add the following domains or URL endpoints to your web-content filtering solution allow-lists depending on what type of user you are and how you sign in.

<table>
<thead>
<tr>
<th>Role</th>
<th>Allow-lists</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root users and IAM users</td>
<td>*.signin.aws.amazon.com</td>
</tr>
<tr>
<td>Amazon.com account sign-in</td>
<td><a href="http://www.amazon.com">www.amazon.com</a></td>
</tr>
</tbody>
</table>
| IAM Identity Center users and first-party application sign-in | • *.awsapps.com (http://awsapps.com/)  
  • *.signin.aws |
To reset the password for an account that you created using AWS Organizations, see Accessing a member account as the root user.

To reset your root user password

1. Use your AWS email address to begin signing in to the AWS Management Console as the root user. Then, choose Next.

2. Choose Forgot password?

3. Complete the password recovery steps. An example of a password recovery page is shown in the following image.
4. After you complete the password recovery steps, you receive a message that further instructions have been sent to the email address associated with your AWS account as shown in the following image.

An email with a link to reset your password is sent to the email used to create the AWS account.

**Note**
The email will come from an address ending in @amazon.com or aws.amazon.com.

5. Select the link provided in the AWS email to reset your AWS root user password.
I forgot my IAM user password for my AWS account

To change your IAM user password, you must have the proper permissions. For more information about resetting your IAM user password, see How an IAM user changes their own password. If you do not have these permissions, only the IAM administrator can reset an IAM user password. IAM users should contact their IAM administrator to reset their password.
I forgot my federated identity password for my AWS account

Federated identities sign in to access AWS accounts with external identities. The type of external identity in use determines how federated identities sign in. Your administrator creates federated identities. Check with your administrator for more details on how to reset your password.
I forgot my IAM Identity Center password for my AWS account

If you are an IAM Identity Center user and you have lost or forgotten the password for your AWS account, you can reset your password. You must know the email address used for the IAM Identity Center account and have access to it. A link to reset your password is sent to your AWS account email.

To reset your IAM Identity Center user password

1. Use your AWS access portal URL link and enter your IAM Identity Center user name. Then, choose Next.

2. Select Forgot password as shown in the following image.
3. Complete the password recovery steps.

4. After you complete the password recovery steps, you receive the following message confirming that you've been sent an email message that you can use to reset your password.

An email with a link to reset your password is sent to the email associated with the IAM Identity Center user account. Select the link provided in the AWS email to reset your IAM Identity Center user password. The link directs you to a new webpage to create a new IAM Identity Center user password. After creating a new password, you receive confirmation that the password reset was successful.
I need my account verification code

If you provided your account email address and password, AWS sometimes requires you to provide a one-time verification code. To retrieve the verification code, check the email that is associated with your AWS account for a message from Amazon Web Services. The email address ends in @amazon.com or @aws.amazon.com. Follow the directions in the message. If you don't see the message in your account, check your spam and junk folders. If you no longer have access to the email, see I don't have access to the email for my AWS account (p. 23).

I need to reactivate my suspended AWS account

If your AWS account is suspended and you want to reinstate it, see How can I reactivate my suspended AWS account?

I need to contact AWS Support for sign-in issues

If you tried everything, you can get help from AWS Support by completing the Billing and Account Support request.

I need to contact AWS Billing for billing issues

If you can't sign in to your AWS account and would like to contact AWS Billing for billing issues, you can do so through a Billing and Account Support request.

I need help managing my AWS account

If you need help changing a credit card for your AWS account, reporting fraudulent activity, or closing your AWS account, see Troubleshooting other issues with AWS accounts.
# Document history

The following table describes important additions to the AWS Sign-In documentation. We also update the documentation frequently to address the feedback that you send us.

- **Latest major documentation update:** August 31, 2022

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>New guide</td>
<td>This is the first release of the AWS Sign-In User Guide.</td>
<td>August 31, 2022</td>
</tr>
</tbody>
</table>