aws

User Guide

AWS Setup

AWS Setup: User Guide

Table of Contents

Overview **1**
..... 1
..... 1
Terminology **2**
..... 2
Administrator 2
Account 2
Credentials 2
Corporate credentials 3
Profile 3
User 3
Root user credentials 3
Verification code 3
AWS users and credentials **4**
Root user 4
IAM Identity Center user 5
Federated identity 5
IAM user 5
AWS Builder ID user 6
Prerequisites and considerations **7**
AWS account requirements 7
IAM Identity Center considerations 8
Active Directory or external IdP 8
AWS Organizations 9
IAM roles 10
Next-generation firewalls and secure web gateways 10
Using multiple AWS accounts 10
Part 1: Set up a new AWS account **13**
Step 1: Sign up for an AWS account 13
Step 2: Sign in as the root user 15
To sign in as the root user 15
Step 3: Activate MFA for your AWS account root user 16
Part 2: Create an administrative user in IAM Identity Center **17**
Step 1: Enable IAM Identity Center 17

Step 2: Choose your identity source 18
Connect Active Directory or another IdP and specify a user 19
Use the default directory and create a user in IAM Identity Center 21
Step 3: Create an administrative permission set 22
Step 4: Set up AWS account access for an administrative user 23
Step 5: Sign in to the AWS access portal with your administrative credentials 25
Troubleshooting AWS account creation issues 27
I didn't receive the call from AWS to verify my new account 27
I get an error about "maximum number of failed attempts" when I try to verify my AWS account by phone 28
It's been more than 24 hours and my account isn't activated 28

Overview

This guide provides instructions to create a new AWS account and set up your first administrative user in AWS IAM Identity Center following the latest security best practices.

An AWS account is required to access AWS services and serves as two basic functions:

- **Container** – An AWS account is a container for all the AWS resources you can create as an AWS customer. When you create an Amazon Simple Storage Service (Amazon S3) bucket or Amazon Relational Database Service (Amazon RDS) database to store your data, or an Amazon Elastic Compute Cloud (Amazon EC2) instance to process your data, you are creating a *resource* in your account. Every resource is uniquely identified by an Amazon Resource Name (ARN) that includes the account ID of the account that contains or owns the resource.
- **Security boundary** – An AWS account is the basic security boundary for your AWS resources. Resources that you create in your account are available only to users who have credentials for that same account.

  Among the key resources you can create in your account are *identities*, such as IAM users and roles, and federated identities, such as users from your enterprise user directory, a web identity provider, the IAM Identity Center directory, or any other user that accesses AWS services by using credentials provided through an identity source. These identities have credentials that someone can use to sign in, or *authenticate* to AWS. Identities also have permission policies that specify what the person who signed in is authorized to do with the resources in the account.

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 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.

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.

Profile

When you sign up for an AWS Builder ID, you create a profile. Your profile includes the contact information you provided and the ability to manage multi-factor authentication (MFA) devices and active sessions. You can also learn more about privacy and how we handle your data in your profile. For more information about your profile and how it relates to an AWS account, see AWS Builder ID and other AWS credentials.

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 not 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.

Root user credentials

The root user credentials are the same credentials used to sign in to the AWS Management Console as the root user. For more information on the root user, see Root user.

Verification code

A verification code verifies your identity during the sign-in process using multi-factor authentication (MFA). The delivery methods for verification codes vary. They can be sent via text message or email. Check with your administrator for more information.

AWS users and credentials

When you interact with AWS, you specify your AWS *security credentials* to verify who you are and whether you have permission to access the resources that you're requesting. AWS uses security credentials to authenticate and authorize requests.

For example, if you want to download a protected file from an Amazon Simple Storage Service (Amazon S3) bucket, your credentials must allow that access. If your credentials show you aren't authorized to download the file, AWS denies your request. However, security credentials aren't required to download files in publicly shared Amazon S3 buckets.

Root user

Also referred to as the account owner or account root user. As the root user, you have complete access to all AWS services and resources in your 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 to the AWS Management Console as the root user using the email address and password that you used to create the account. For step by step instructions on how to sign in, see Sign in to the AWS Management Console as 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 don't 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 *IAM User Guide*.

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

IAM Identity Center user

An IAM Identity Center user signs in through the AWS access portal. The AWS access portal or 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 user was sent to the email address of the AWS account. The specific sign-in URL is included in the email invitation. IAM Identity Center users cannot sign in through the AWS Management Console. For step by step instructions on how to sign in, see Sign in to the AWS access portal.

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

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

Federated identity

A federated identity is a user who can sign in using a well-known external identity provider (IdP), such as Login with Amazon, Facebook, Google, or any other OpenID Connect (OIDC)-compatible IdP. With web identity federation, you can receive an authentication token, and then exchange that token for temporary security credentials in AWS that map to an IAM role with permissions to use the resources in your AWS account. You do not sign in with the AWS Management Console or AWS access portal. Instead, the external identity in use determines how you sign in.

For more information, see Sign in as a federated identity.

IAM user

An IAM user is an entity you create in AWS. This user is an identity within your AWS account that is granted specific custom permissions. Your IAM user credentials consist of a name and password used to sign in to the AWS Management Console. For step by step instructions on how to sign in, see Sign in to the AWS Management Console as an IAM user.

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

AWS Builder ID user

As an AWS Builder ID user, you specifically sign in to the AWS service or tool that you want to access. An AWS Builder ID user complements any AWS account you already have or want to create. An AWS Builder ID represents you as a person, and you can use it to access AWS services and tools without an AWS account. You also have a profile where you can see and update your information. For more information, see To sign in with AWS Builder ID.

Prerequisites and considerations

Before you begin the set up process, review the account requirements, consider whether you'll need more than one AWS account, and understand the requirements for setting up your account for administrative access in IAM Identity Center.

AWS account requirements

To sign up for an AWS account, you need to provide the following information:

- **An account name** – The name of the account appears in several places, such as on your invoice, and in consoles such as the Billing and Cost Management dashboard and the AWS Organizations console.

  We recommend that you use an account naming standard so that the account name can be easily recognized and distinguished from other accounts you might own. If it's a company account, consider using a naming standard such as *organization-purpose-environment* (for example, *AnyCompany-audit-prod*). If it's a personal account, consider using a naming standard such as *first name-last name-purpose* (for example, *paulo-santos-testaccount*).
- **An email address** – This email address is used as the sign-in name for the account's root user, and is required for account recovery, such as forgetting the password. You must be able to receive messages sent to this email address. Before you can perform certain tasks, you must verify that you have access to the email account.

  > **Important**
  >
  > If this account is for a business, we recommend that you use a corporate distribution list (for example, `it.admins@example.com`). Avoid using an individual's corporate email address (for example, `paulo.santos@example.com`). This helps ensure that your company can access the AWS account if an employee changes positions or leaves the company. The email address can be used to reset the account's root user credentials. Be sure that you protect access to this distribution list or address.
- **A phone number** – This number can be used when confirmation of account ownership is required. You must be able to receive calls at this phone number.

> **Important**
>
> If this account is for a business, we recommend using a corporate phone number instead of a personal phone number. This helps ensure that your company can access the AWS account if an employee changes positions or leaves the company.

- **A multi-factor authentication device** – To secure your AWS resources, enable multi-factor authentication (MFA) on the root user account. In addition to you regular sign-in credentials, a secondary authentication is required when MFA is activated, providing an extra layer of security. For more information about MFA, see What is MFA? in the *IAM User Guide*.
- *AWS Support plan* – You will be asked to choose one of the available plans during the account creation process. For a description of the available plans, see Compare AWS Support plans.

IAM Identity Center considerations

The following topics provide guidance for setting up IAM Identity Center for specific environments. Understand the guidance that applies to your environment before you proceed to Part 2: Create an administrative user in IAM Identity Center.

Topics

- Active Directory or external IdP
- AWS Organizations
- IAM roles
- Next-generation firewalls and secure web gateways

Active Directory or external IdP

If you're already managing users and groups in Active Directory or an external IdP, we recommend that you consider connecting this identity source when you enable IAM Identity Center and choose your identity source. Doing this before you create any users and groups in the default Identity Center directory will help you avoid the additional configuration that's required if you change your identity source later.

If you want to use Active Directory as your identity source, your configuration must meet the following prerequisites:

- If you're using AWS Managed Microsoft AD, you must enable IAM Identity Center in the same AWS Region where your AWS Managed Microsoft AD directory is set up. IAM Identity Center stores the assignment data in the same Region as the directory. To administer IAM Identity Center, you might need to switch to the Region where IAM Identity Center is configured. Also, note that the AWS access portal uses the same access URL as your directory.
- Use an Active Directory residing in your management account:

  You must have an existing AD Connector or AWS Managed Microsoft AD directory set up in AWS Directory Service, and it must reside within your AWS Organizations management account. You can connect only one AD Connector or one AWS Managed Microsoft AD at a time. If you need to support multiple domains or forests, use AWS Managed Microsoft AD. For more information, see:

  - Connect a directory in AWS Managed Microsoft AD to IAM Identity Center in the *AWS IAM Identity Center User Guide*.
  - Connect a self-managed directory in Active Directory to IAM Identity Center in the *AWS IAM Identity Center User Guide*.
- Use an Active Directory residing in the delegated admin account:

  If you plan to enable IAM Identity Center delegated admin and use Active Directory as your IAM identity source, you can use an existing AD Connector or AWS Managed Microsoft AD directory set up in AWS directory residing in the delegated admin account.

  If you decide to change IAM Identity Center source from any other source to Active Directory, or change it from Active Directory to any other source, the directory must reside in (be owned by) the IAM Identity Center delegated administrator member account if one exists; otherwise, it must be in the management account.

AWS Organizations

Your AWS account must be managed by AWS Organizations. If you haven't set up an organization, you don't have to. When you enable IAM Identity Center, you will choose whether to have AWS create an organization for you.

If you've already set up AWS Organizations, make sure that all features are enabled. For more information, see Enabling all features in your organization in the *AWS Organizations User Guide*.

To enable IAM Identity Center, you must sign in to the AWS Management Console by using the credentials of your AWS Organizations management account. You can't enable IAM Identity

Center while signed in with credentials from an AWS Organizations member account. For more information, see Creating and managing an AWS Organization in the *AWS Organizations User Guide*.

IAM roles

If you've already configured IAM roles in your AWS account, we recommend that you check whether your account is approaching the quota for IAM roles. For more information, see IAM object quotas.

If you're nearing the quota, consider requesting a quota increase. Otherwise, you might experience problems with IAM Identity Center when you provision permission sets to accounts that have exceeded the IAM role quota. For information about how to request a quota increase, see Requesting a quota increase in the *Service Quotas User Guide*.

Next-generation firewalls and secure web gateways

If you filter access to specific AWS domains or URL endpoints by using a web content filtering solution such as NGFWs or SWGs, you must add the following domains or URL endpoints to your web-content filtering solution allow-lists.

Specific DNS domains

- *.awsapps.com (http://awsapps.com/)
- *.signin.aws

Specific URL endpoints

- https://*[yourdirectory]*.awsapps.com/start
- https://*[yourdirectory]*.awsapps.com/login
- https://*[yourregion]*.signin.aws/platform/login

Using multiple AWS accounts

AWS accounts serve as the fundamental security boundary in AWS. They serve as a resource container that provides a useful level of isolation. The ability to isolate resources and users is a key requirement to establishing a secure, well governed environment.

Separating your resources into separate AWS accounts helps you support the following principles in your cloud environment:

- **Security control** – Different applications can have different security profiles that require different control policies and mechanisms. For example, it's easier to talk to an auditor and be able to point to a single AWS account that hosts all elements of your workload that are subject to Payment Card Industry (PCI) Security Standards.
- **Isolation** – An AWS account is a unit of security protection. Potential risks and security threats should be contained within an AWS account without affecting others. There could be different security needs due to different teams or different security profiles.
- **Many teams** – Different teams have different responsibilities and resource needs. You can prevent teams from interfering with each other by moving them to separate AWS accounts.
- **Data isolation** – In addition to isolating the teams, it's important to isolate the data stores to an account. This can help limit the number of people that can access and manage that data store. This helps contain exposure to highly private data and therefore can help in compliance with the European Union's General Data Protection Regulation (GDPR).
- **Business process** – Different business units or products may have completely different purposes and processes. With multiple AWS accounts, you can support a business unit's specific needs.
- **Billing** – An account is the only true way to separate items at a billing level. Multiple accounts help separate items at a billing level across business units, functional teams, or individual users. You can still get all of your bills consolidated to a single payer (using AWS Organizations and consolidated billing) while having line items separated by AWS account.
- **Quota allocation** – AWS service quotas are enforced separately for each AWS account. Separating workloads into different AWS accounts prevents them from consuming quotas for each other.

All of the recommendations and procedures described in this guide are in compliance with the AWS Well-Architected Framework. This framework is intended to help you design a flexible, resilient, and scalable cloud infrastructure. Even when you are starting small, we recommend that you proceed in compliance with the guidance in the framework. Doing so can help you scale your environment securely and without impacting your ongoing operations as you grow.

Before you start adding multiple accounts, you'll want to develop a plan to manage them. For that, we recommend that you use AWS Organizations, which is a free AWS service, to manage all of the AWS accounts in your organization.

AWS also offers AWS Control Tower, which adds layers of AWS managed automation to Organizations and automatically integrates it with other AWS services like AWS CloudTrail, AWS Config, Amazon CloudWatch, AWS Service Catalog, and others. These services can incur additional costs. For more information, see AWS Control Tower pricing.

Part 1: Set up a new AWS account

These instructions will help you create an AWS account and secure the root user credentials. Complete all steps before proceeding to Part 2: Create an administrative user in IAM Identity Center.

Topics

- Step 1: Sign up for an AWS account
- Step 2: Sign in as the root user
- Step 3: Activate MFA for your AWS account root user

Step 1: Sign up for an AWS account

1. Open https://portal.aws.amazon.com/billing/signup.
2. Choose **Create an AWS account**.

   > **Note**
   >
   > If you signed in to AWS recently, choose **Sign in to the Console**. If the option **Create a new AWS account** isn't visible, first choose **Sign in to a different account**, and then choose **Create a new AWS account**.

3. Enter your account information, and then choose **Continue**.

   Be sure that you enter your account information correctly, especially your email address. If you enter your email address incorrectly, you can't access your account.

4. Choose **Personal** or **Professional**.

   The difference between these options is only in the information that we ask you for. Both account types have the same features and functions.

5. Enter your company or personal information based on the guidance provided in AWS account requirements.
6. Read and accept the AWS Customer Agreement.
7. Choose **Create Account and Continue**.

At this point, you'll receive an email message to confirm that your AWS account is ready to use. You can sign in to your new account by using the email address and password you provided during sign up. However, you can't use any AWS services until you finish activating your account.

8. On the **Payment Information** page, enter the information about your payment method. If you want to use an address that's different than the one you used to create the account, choose **Use a new address** and enter the address you want used for billing purposes.
9. Choose **Verify and Add**.

> **Note**
>
> If your contact address is in India, your user agreement for your account is with AISPL, a local AWS seller in India. You must provide your CVV as part of the verification process. You might also have to enter a one-time password, depending on your bank. AISPL charges your payment method 2 INR as part of the verification process. AISPL refunds the 2 INR after it completes verification.

10. To verify your phone number, choose your country or region code from the list, and enter a phone number where you can be called in the next few minutes. Enter the CAPTCHA code, and submit.
11. The AWS automated verification system calls you and provides a PIN. Enter the PIN using your phone and then choose **Continue**.
12. Select an AWS Support plan.

    For a description of the available plans, see Compare AWS Support plans.

    A confirmation page appears that indicates that your account is being activated. This usually takes only a few minutes but can sometimes take up to 24 hours. During activation, you can sign in to your new AWS account. Until activation is complete, you might see a **Complete Sign Up** button. You can ignore it.

    AWS sends a confirmation email message when account activation is complete. Check your email and spam folder for the confirmation email message. After you receive this message, you have full access to all AWS services.

Step 2: Sign in as the root user

When you first 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.

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 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 *IAM User Guide*.

To sign in as the root user

1. Open the AWS Management Console at https://console.aws.amazon.com/.

   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 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**.

2. If you have not signed in previously using this browser, the main sign-in page appears. If you are the account owner, choose **Root user**. Enter your AWS account email address associated with your account and choose **Next**.
3. You might be prompted to complete a security check. Complete this to move to the next step. If you cannot complete the security check, try listening to the audio or refreshing the security check for a new set of characters.
4. Enter your password and choose **Sign in**.

Step 3: Activate MFA for your AWS account root user

To enhance the security of your root user credentials, we recommend that you follow the security best practice to activate multi-factor authentication (MFA) for your AWS account. Because the root user can perform sensitive operations in your account, adding this additional layer of authentication helps you to better secure your account. Multiple types of MFA are available.

For instructions about activating MFA for the root user, see Enabling MFA devices for users in AWS in the *IAM User Guide*.

Part 2: Create an administrative user in IAM Identity Center

After you complete Part 1: Set up a new AWS account, the following steps will help you set up AWS account access for an administrative user, which will be used to perform daily tasks.

> **Note**
>
> This topic provides the minimum required steps to successfully set up administrator access for an AWS account and create an administrative user in IAM Identity Center. For additional information, see Getting started in the *AWS IAM Identity Center User Guide*.

Topics

- Step 1: Enable IAM Identity Center
- Step 2: Choose your identity source
- Step 3: Create an administrative permission set
- Step 4: Set up AWS account access for an administrative user
- Step 5: Sign in to the AWS access portal with your administrative credentials

Step 1: Enable IAM Identity Center

> **Note**
>
> If you did not activate multi-factor authentication (MFA) for your root user, complete Step 3: Activate MFA for your AWS account root user before you proceed.

To enable IAM Identity Center

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

3. Under **Enable IAM Identity Center**, choose **Enable**.
4. IAM Identity Center requires AWS Organizations. If you haven't set up an organization, you must choose whether to have AWS create one for you. Choose **Create AWS organization** to complete this process.

   AWS Organizations automatically sends a verification email to the address that is associated with your management account. There might be a delay before you receive the verification email. Verify your email address within 24 hours.

> **Note**
>
> If you are using a multi-account environment, we recommend that you configure delegated administration. With delegated administration, you can limit the number of people who require access to the management account in AWS Organizations. For more information, see Delegated Administration in the *AWS IAM Identity Center User Guide*.

Step 2: Choose your identity source

Your identity source in IAM Identity Center defines where your users and groups are managed. You can choose one of the following as your identity source:

- **IAM Identity Center directory** – When you enable IAM Identity Center for the first time, it is automatically configured with an IAM Identity Center directory as your default identity source. This is where you create your users and groups and assign their level of access to your AWS accounts and applications.
- **Active Directory** – Choose this option if you want to continue managing users in either your AWS Managed Microsoft AD directory using AWS Directory Service or your self-managed directory in Active Directory (AD).
- **External identity provider** – Choose this option if you want to manage users in an external identity provider (IdP) such as Okta or Azure Active Directory.

After you enable IAM Identity Center, you must choose your identity source. The identity source that you choose determines where IAM Identity Center searches for users and groups that need single sign-on access. After you choose your identity source, you'll create or specify a user and assign them administrative permissions to your AWS account.

Important

If you're already managing users and groups in Active Directory or an external identity provider (IdP), we recommend that you consider connecting this identity source when you enable IAM Identity Center and choose your identity source. This should be done before you create any users and groups in the default Identity Center directory and make any assignments. If you're already managing users and groups in one identity source, changing to a different identity source might remove all user and group assignments that you configured in IAM Identity Center. If this occurs, all users, including the administrative user in IAM Identity Center, will lose single sign-on access to their AWS accounts and applications.

Topics

- Connect Active Directory or another IdP and specify a user
- Use the default directory and create a user in IAM Identity Center

Connect Active Directory or another IdP and specify a user

If you're already using Active Directory or an external identity provider (IdP), the following topics will help you connect your directory to IAM Identity Center.

You can connect an AWS Managed Microsoft AD directory, a self-managed directory in Active Directory, or an external IdP with IAM Identity Center. If you plan to connect an AWS Managed Microsoft AD directory or a self-managed directory in Active Directory, make sure that your Active Directory configuration meets the prerequisites in Active Directory or external IdP.

Note

As a security best practice, we strongly recommend that you enable multi-factor authentication. If you plan to connect an AWS Managed Microsoft AD directory or a self-managed directory in Active Directory and you're not using RADIUS MFA with AWS Directory Service, enable MFA in IAM Identity Center. If you plan to use an external identity provider, note that the external IdP, not IAM Identity Center, manages MFA settings. MFA in IAM Identity Center is not supported for use by external IdPs. For more information, see Enable MFA in the *AWS IAM Identity Center User Guide*.

AWS Managed Microsoft AD

1. Review the guidance in Connect to a Microsoft Active Directory.
2. Follow the steps in Connect a directory in AWS Managed Microsoft AD to IAM Identity Center.
3. Configure Active Directory to synchronize the user to whom you want to grant administrative permissions into IAM Identity Center. For more information, see Synchronize an administrative user into IAM Identity Center.

Self-managed directory in Active Directory

1. Review the guidance in Connect to a Microsoft Active Directory.
2. Follow the steps in Connect a self-managed directory in Active Directory to IAM Identity Center.
3. Configure Active Directory to synchronize the user to whom you want to grant administrative permissions into IAM Identity Center. For more information, see Synchronize an administrative user in IAM Identity Center.

External IdP

1. Review the guidance in Connect to an external identity provider.
2. Follow the steps in How to connect to an external identity provider.
3. Configure your IdP to provision users into IAM Identity Center.

> **Note**
>
> Before you set up automatic, group-based provisioning of all your workforce identities from your IdP into IAM Identity Center, we recommend that you synchronize the one user to whom you want to grant administrative permissions into IAM Identity Center.

Synchronize an administrative user into IAM Identity Center

After you connect your directory to IAM Identity Center, you can specify a user to whom you want to grant administrative permissions, and then synchronize that user from your directory into IAM Identity Center.

1. Open the IAM Identity Center console.

2. Choose **Settings**.
3. On the **Settings** page, choose the **Identity source** tab, choose **Actions**, and then choose **Manage Sync**.
4. On the **Manage Sync** page, choose the **Users** tab, and then choose **Add users and groups**.
5. On the **Users** tab, under **User**, enter the exact user name and choose **Add**.
6. Under **Added Users and Groups**, do the following:

    a. Confirm that the user to whom you want to grant administrative permissions is specified.

    b. Select the check box to the left of the user name.

    c. Choose **Submit**.
7. In the **Manage sync** page, the user that you specified appears in the **Users in sync scope** list.
8. In the navigation pane, choose **Users**.
9. On the **Users** page, it might take some time for the user that you specified to appear in the list. Choose the refresh icon to update the list of users.

At this point, your user doesn't have access to the management account. You will set up administrative access to this account by creating an administrative permission set and assigning the user to that permission set.

Next step: Step 3: Create an administrative permission set

Use the default directory and create a user in IAM Identity Center

When you enable IAM Identity Center for the first time, it is automatically configured with an IAM Identity Center directory as your default identity source. Complete the following steps to create a user in IAM Identity Center.

1. Sign in to the AWS Management Console as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.
2. Open the IAM Identity Center console.
3. Follow the steps in Add users to create a user.

    When you specify the user details, you can either send an email with the password setup instructions (this is the default option) or generate a one-time password. If you send an email, make sure that you specify an email address that you can access.

4. After you add the user, return to this procedure. If you kept the default option to send an email with the password setup instructions, do the following:

   a. You'll receive an email with the subject **Invitation to join AWS Single Sign-On**. Open the email and choose **Accept invitation**.

   b. On the **New user sign up** page, enter and confirm a password, and then choose **Set new password**.

   > **Note**
   >
   > Make sure to save your password. You'll need it later to Step 5: Sign in to the AWS access portal with your administrative credentials.

At this point, your user doesn't have access to the management account. You will set up administrative access to this account by creating an administrative permission set and assigning the user to that permission set.

Next step: Step 3: Create an administrative permission set

Step 3: Create an administrative permission set

Permission sets are stored in IAM Identity Center and define the level of access that users and groups have to an AWS account. Perform the following steps to create a permission set that grants administrative permissions.

1. Sign in to the AWS Management Console as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.
2. Open the IAM Identity Center console.
3. In the IAM Identity Center navigation pane, under **Multi-account permissions**, choose **Permission sets**.
4. Choose **Create permission set**.
5. For **Step 1: Select permission set type**, on the **Select permission set type** page, keep the default settings and choose **Next**. The default settings grant full access to AWS services and resources using the **AdministratorAccess** predefined permission set.

> **Note**
>
> The predefined **AdministratorAccess** permission set uses the **AdministratorAccess** AWS managed policy.

6. For **Step 2: Specify permission set details**, on the **Specify permission set details** page, keep the default settings and choose **Next**. The default setting limits your session to one hour.
7. For **Step 3: Review and create**, on the **Review and create** page, do the following:
    1. Review the permission set type and confirm that it is **AdministratorAccess**.
    2. Review the AWS managed policy and confirm that it is **AdministratorAccess**.
    3. Choose **Create**.

Step 4: Set up AWS account access for an administrative user

To set up AWS account access for an administrative user in IAM Identity Center, you must assign the user to the **AdministratorAccess** permission set.

1. Sign in to the AWS Management Console as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.
2. Open the IAM Identity Center console.
3. In the navigation pane, under **Multi-account permissions**, choose **AWS accounts**.
4. On the **AWS accounts** page, a tree view list of your organization appears. Select the check box next to the AWS account to which you want to assign administrative access. If you have multiple accounts in your organization, select the check box next to the management account.
5. Choose **Assign users or groups**.
6. For **Step 1: Select users and groups**, on the **Assign users and groups to "*AWS-account-name*"** page, do the following:
    1. On the **Users** tab, select the user to whom you want to grant administrative permissions.

        To filter the results, start typing the name of the user that you want in the search box.
    2. After you confirm that the correct user is selected, choose **Next**.
7. For **Step 2: Select permission sets**, on the **Assign permission sets to "*AWS-account-name*"** page, under **Permission sets**, select the **AdministratorAccess** permission set.

8. Choose **Next**.
9. For **Step 3: Review and Submit**, on the **Review and submit assignments to "*AWS-account-name*"** page, do the following:

    1. Review the selected user and permission set.
    2. After you confirm that the correct user is assigned to the **AdministratorAccess** permission set, choose **Submit**.

    > **Important**
    >
    > The user assignment process might take a few minutes to complete. Leave this page open until the process successfully completes.

10. If either of the following applies, follow the steps in Enable MFA to enable MFA for IAM Identity Center:

    - You're using the default Identity Center directory as your identity source.
    - You're using an AWS Managed Microsoft AD directory or a self-managed directory in Active Directory as your identity source and you're not using RADIUS MFA with AWS Directory Service.

    > **Note**
    >
    > If you're using an external identity provider, note that the external IdP, not IAM Identity Center, manages MFA settings. MFA in IAM Identity Center is not supported for use by external IdPs.

When you set up account access for the administrative user, IAM Identity Center creates a corresponding IAM role. This role, which is controlled by IAM Identity Center, is created in the relevant AWS account, and the policies specified in the permission set are attached to the role.

Step 5: Sign in to the AWS access portal with your administrative credentials

Complete the following steps to confirm that you can sign in to the AWS access portal by using the credentials of the administrative user, and that you can access the AWS account.

1. Sign in to the AWS Management Console as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.
2. Open the AWS IAM Identity Center console at https://console.aws.amazon.com/singlesignon/.
3. In the navigation pane, choose **Dashboard**.
4. On the **Dashboard** page, under **Settings summary**, copy the AWS access portal URL.
5. Open a separate browser, paste the AWS access portal URL that you copied, and press **Enter**.
6. Sign in by using either of the following:
   - If you're using Active Directory or an external identity provider (IdP) as your identity source, sign in by using the credentials of the Active Directory or IdP user that you assigned to the **AdministratorAccess** permission set in IAM Identity Center.
   - If you're using the default IAM Identity Center directory as your identity source, sign in by using the user name that you specified when you created the user and the new password you specified for the user.
7. After you are signed in, an **AWS account** icon appears in the portal.
8. When you select the **AWS account** icon, the account name, account ID, and email address associated with the account appear.
9. Choose the name of the account to display the **AdministratorAccess** permission set, and select the **Management Console** link to the right of **AdministratorAccess**.

   When you sign in, the name of the permission set to which the user is assigned appears as an available role in the AWS access portal. Because you assigned this user to the `AdministratorAccess` permission set, the role will appear in the AWS access portal as: `AdministratorAccess/`*`username`*
10. If you are redirected to the AWS Management Console, you successfully finished setting up administrative access to the AWS account. Proceed to step 10.
11. Switch to the browser that you used to sign into the AWS Management Console and set up IAM Identity Center, and sign out from your AWS account root user.

> **Important**
>
> We strongly recommend that you adhere to the best practice of using the credentials of the administrative user when you sign in to the AWS access portal, and that you don't use the root user credentials for your everyday tasks.

To allow other users to access your accounts and applications, and to administer IAM Identity Center, create and assign permission sets only through IAM Identity Center.

Troubleshooting AWS account creation issues

Use the information here to help you troubleshoot issues related to creating an AWS account.

Issues

- I didn't receive the call from AWS to verify my new account
- I get an error about "maximum number of failed attempts" when I try to verify my AWS account by phone
- It's been more than 24 hours and my account isn't activated

I didn't receive the call from AWS to verify my new account

When you create an AWS account, you must provide a phone number on which you can receive either an SMS text message or a voice call. You specify which method to use to verify the number.

If you don't receive the message or call, verify the following:

- You entered the correct telephone number and selected the correct country code during the sign-up process.
- If you're using a mobile phone, be sure that you have a cellular signal to receive SMS text messages or calls.
- The information that you entered for your payment method is correct.

If you didn't receive an SMS text message or call to complete the identity verification process, AWS Support can help you to activate your AWS account manually. Use the following steps:

1. Be sure that you can be reached at the telephone number that you provided for your AWS account.
2. Open the AWS Support console, and then choose **Create case**.
   a. Choose **Account and billing support**.
   b. For **Type**, select **Account**.
   c. For **Category**, select **Activation**.
   d. In the **Case description** section, provide a date and time when you can be reached.
   e. In the **Contact options** section, select **Chat** for **Contact methods**.

f. Choose **Submit**.

> **Note**
>
> You can create a case with AWS Support even if your AWS account isn't activated.

I get an error about "maximum number of failed attempts" when I try to verify my AWS account by phone

AWS Support can help you to manually activate your account. Follow these steps:

1. Sign in to your AWS account using the email address and password that you specified when creating your account.
2. Open the AWS Support console , and then choose **Create case**.
3. Choose **Account and Billing Support**.
4. For **Type**, select **Account**.
5. For **Category**, select **Activation**.
6. In the **Case description** section, provide a date and time when you can be reached.
7. In the **Contact options** section, select **Chat** for **Contact methods**.
8. Choose **Submit**.

AWS Support will contact you and attempt to manually activate your AWS account.

It's been more than 24 hours and my account isn't activated

Account activation can sometimes be delayed. If the process takes more than 24 hours, check the following:

- **Finish the account activation process.**

  If you closed the window for the sign-up process before you added all the necessary information, open the registration page. Choose **Sign in to an existing AWS account**, and sign in using the email address and password you chose for the account.
- **Check the information associated with your payment method.**

In the AWS Billing and Cost Management console, check Payment Methods for errors.

- **Contact your financial institution.**

  Sometimes financial institutions reject authorization requests from AWS. Contact the institution associated with your payment method, and ask them to approve authorization requests from AWS. AWS cancels the authorization request as soon as it's approved by your financial institution, so you aren't charged for the authorization request. Authorization requests might still appear as a small charge (usually 1 USD) on statements from your financial institution.
- **Check your email and spam folder for requests for additional information.**
- **Try a different browser.**
- **Contact AWS Support.**

  Contact AWS Support for help. Mention any troubleshooting steps that you already tried.

> **Note**
>
> Don't provide sensitive information, such as credit card numbers, in any correspondence with AWS.