AWS account root user - AWS Identity and Access Management

Archived: 2026-04-05 16:09:43 UTC

When you first create an Amazon Web Services (AWS) account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user*. The email address and password that you used to create your AWS account are the credentials you use to sign in as your root user.

- Use the root user only to perform the tasks that require root-level permissions. For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials.
- Follow the root user best practices for your AWS account.
- If you're having trouble signing in, see Sign in to the AWS Management Console.

Important

We strongly recommend that you don't use the root user for your everyday tasks and that you follow the root user best practices for your AWS account. 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.

While MFA is enforced for root users by default, it requires customer action to add MFA during the initial account creation or as prompted during sign-in. For more information about using MFA to protect the root user, see Multi-factor authentication for AWS account root user.

Centrally manage root access for member accounts

To help you manage credentials at scale, you can centrally secure access to root user credentials for member accounts in AWS Organizations. When you enable AWS Organizations, you combine all your AWS accounts into an organization for central management. Centralizing root access lets you remove root user credentials and perform the following privileged tasks on member accounts.

Remove member account root user credentials

> After you centralize root access for member accounts, you can choose to delete root user credentials from member accounts in your Organizations. You can remove the root user password, access keys, signing certificates, and deactivate multi-factor authentication (MFA). New accounts you create in Organizations have no root user credentials by default. Member accounts can't sign in to their root user or perform password recovery for their root user unless account recovery is enabled.

Perform privileged tasks that require root user credentials

Some tasks can only be performed when you sign in as the root user of an account. Some of these Tasks that require root user credentials can be performed by the management account or delegated administrator for IAM. To learn more about taking privileged actions on member accounts, see Perform a privileged task.

Enable account recovery of the root user

If you need to recover root user credentials for a member account, the Organizations management account or delegated administrator can perform the **Allow password recovery** privileged task. The person with access to the root user email inbox for the member account can reset the root user password to recover root user credentials. We recommend deleting root user credentials once you complete the task that requires access to the root user.

Tasks that require root user credentials

We recommend that you configure an administrative user in AWS IAM Identity Center to perform daily tasks and access AWS resources. However, you can perform the tasks listed below only when you sign in as the root user of an account.

To simplify managing privileged root user credentials across member accounts in AWS Organizations, you can enable centralized root access to help you centrally secure highly privileged access to your AWS accounts. Centrally manage root access for member accounts lets you centrally remove and prevent long-term root user credential recovery, improving account security in your organization. After you enable this feature, you can perform the following privileged tasks on member accounts.

- Remove member account root user credentials to prevent account recovery of the root user. You can also allow password recovery to recover root user credentials for a member account.
- Remove a misconfigured bucket policy that denies all principals from accessing an Amazon S3 bucket.
- Delete an Amazon Simple Queue Service resource-based policy that denies all principals from accessing an Amazon SQS queue.

Account Management Tasks

- Change your AWS account settings. Standalone AWS accounts that are not part of AWS Organizations require root credentials to update the email address, root user password, and root user access keys. Other account settings, such as account name, contact information, alternate contacts, payment currency preference, and AWS Regions, don't require root user credentials.

  Note

  AWS Organizations, with all features enabled, can be used to manage member account settings centrally from the management account and delegated admin accounts. Authorized IAM users or IAM roles in both the management account and delegated admin accounts can close member accounts and update the root email addresses, account names, contact information, alternate contacts, and AWS Regions of member accounts.

- Close your AWS account. Standalone AWS accounts that are not part of AWS Organizations require root credentials to close the account. With AWS Organizations, you can close the member accounts centrally from the management account and delegated admin accounts.
- Restore IAM user permissions. If the only IAM administrator accidentally revokes their own permissions, you can sign in as the root user to edit policies and restore those permissions.

Billing Tasks

- Activate IAM access to the Billing and Cost Management console.
- Some Billing tasks are limited to the root user. See Managing an AWS account in AWS Billing User Guide for more information.
- View certain tax invoices. An IAM user with the aws-portal:ViewBilling permission can view and download VAT invoices from AWS Europe, but not AWS Inc. or Amazon Internet Services Private Limited (AISPL).

AWS KMS Task

- In the event that an AWS Key Management Service key becomes unmanageable, an administrator can recover it by contacting Support; however, Support responds to your root user's primary phone number for authorization by confirming the ticket OTP.

Additional resources

For more information about the AWS root user, see the following resources:

- For help with root user issues, see Troubleshoot issues with the root user.
- To centrally manage root user email addresses in AWS Organizations, see Updating the root user email address for a member account in the *AWS Organizations User Guide*.

The following articles provide additional information about working with the root user.

- What are some best practices for securing my AWS account and its resources?
- How can I create an EventBridge event rule to notify me that my root user was used?
- Monitor and notify on AWS account root user activity
- Monitor IAM root user activity
