Best practices for the management account

Archived: 2026-04-02 10:40:48 UTC

Follow these recommendations to help protect the security of the management account in AWS Organizations. These recommendations assume that you also adhere to the best practice of using the root user only for those tasks that truly require it.

Topics

Limit who has access to the management account

The management account is key to all the mentioned administrative tasks such as account management, policies, integration with other AWS services, consolidated billing, and so on. Therefore, you should restrict and limit access to the management account only to those admin users who need rights to make changes to the organization.

Review and track who has access

To make sure that you maintain access to the management account, periodically review the personnel within your business who have access to the email address, password, MFA, and phone number associated with it. Align your review with existing business procedures. Add a monthly or quarterly review of this information to verify that only the correct people have access. Ensure that the process to recover or reset access to the root user credentials is not reliant on any specific individual to complete. All processes should address the prospect of people being unavailable.

Use the management account only for tasks that *require* the management account

We recommend that you use the management account and its users and roles for tasks that must be performed only by that account. Store all of your AWS resources in other AWS accounts in the organization and keep them out of the management account. One important reason to keep your resources in other accounts is because Organizations service control policies (SCPs) do not work to restrict any users or roles in the management account. Separating your resources from your management account also helps you to understand the charges on your invoices.

For a list of tasks that must be called from the management account, see Operations you can call from only the organization's management account .

Avoid deploying workloads to the organization’s management account

Privileged operations can be performed within an organization’s management account, and SCPs do not apply to the management account. That's why you should limit the cloud resources and data contained in the management account to only those that must be managed in the management account.

Delegate responsibilities outside the management account for decentralization

Where possible, we recommend delegating responsibilities and services outside the management account. Provide your teams with permissions in their own accounts to manage the needs of the organization, without requiring access to the management account. In addition, you can register multiple delegated administrators for services that support this functionality such as AWS Service Catalog for sharing software across the organization, or CloudFormation StackSets for authoring and deploying stacks.

For more information, see Security Reference Architecture, Organizing Your AWS Environment Using Multiple Accounts, and AWS services that you can use with AWS Organizations for suggestions on registering member accounts as delegated administrator for various AWS services.

For more information about setting up delegated admins, see Enabling a delegated admin account for AWS Account Management and Delegated administrator for AWS Organizations.
