

# ROOT ACCOUNTS IN AWS

by Atomic Badger

2-1-2025

On today's date I asked *ChatGPT* to answer this question.

*What is a root account in AWS? What can it do? How is it typically used by most users? What is it not used for?*

**ChatGPT:**

## **“What is a Root Account in AWS?”**

The **root account** in AWS refers to the original account that is created when signing up for an AWS subscription. It has **unrestricted access** to all AWS resources and services. This account is linked to the email address used for registration.

## **What Can the Root Account Do?**

The AWS root user has **full administrative privileges**, meaning it can:

1. **Manage billing & payments** – View and modify billing settings, create or close AWS accounts.
2. **Change account settings** – Modify security credentials, contact details, and enable/disable multi-factor authentication (MFA).
3. **Access all services & resources** – It has full control over all AWS services without needing additional permissions.
4. **Enable or disable security settings** – Turn on/off features like AWS Organizations, IAM policies, and security tools like AWS Shield.
5. **Create and manage IAM users and roles** – It can delegate permissions to other users through IAM (Identity and Access Management).
6. **Request root-level support** – Certain AWS support requests, like account recovery, require root access.

## **How is it Typically Used by Most Users?**

Most AWS users follow **best practices** and use the root account **only for initial setup and critical administrative tasks**. This includes:

- Setting up IAM roles and users.
- Configuring **multi-factor authentication (MFA)** for security.
- Managing **billing and payments**.

- Enabling **AWS Organizations** for managing multiple AWS accounts.
- **Emergency recovery** if all other access methods fail.

### What is the Root Account *Not* Used For?

Best practices recommend **not** using the root account for:

- **Daily operations** – Instead, users should operate with IAM users that have least privilege access.
- **Running applications or workloads** – The root account should never be used to deploy applications or services.
- **Granting access to others** – Instead, use IAM roles and policies to manage permissions securely.

### Security Best Practices

- **Enable MFA** for root user access.
- **Do not share root account credentials** with anyone.
- **Create IAM users** with necessary permissions instead of using root for daily tasks.
- **Monitor root account activity** using AWS CloudTrail.
- **Lock down root API access** unless absolutely necessary.”