

# AWS ASSOCIATE SET-UP

---

DEVOPSANDBEYOND

# Project

---

ABC Consulting has hired devopsandbeyond to build a scalable static hosting environment. This environment will use both windows and linux based web servers.

- Billing Alerts
- IAM configuration
- SAND-VPC

[https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial\\_billing.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_billing.html)

# IAM Account Configuration

---

## Tasks

- Create accounting group
- Create a billing user AWS account.
- Create admin User
- Create custom URL
- Test logins

# Steps

---

[Step 1: Enable Access to Billing Data on Your AWS Test Account](#)

[Step 2: Create IAM Policies That Grant Permissions to Billing Data](#)

[Step 3: Attach Billing Policies to Your Groups](#)

[Step 4: Test Access to the Billing Console](#)

Once you've completed the core tasks, you're ready to test the policy. Testing ensures that the policy works the way you want it to.

# Create billybiller

User name\*

billybiller@accounting.nodomain

[+ Add another user](#)

## Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type\*

☐

**Programmatic access**

Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☒

**AWS Management Console access**

Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password\*

☐

Autogenerated password

☒

Custom password

••••••••

☐

Show password

Require password reset

☐

User must create a new password at next sign-in

# Accounting Group

Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom perm

Group name

accounting

Create policy

Refresh

To grant your IAM users and roles access to your account billing information and tools, the root user must follow the steps to enable billing access in [this procedure](#)

Filter: Policy type ▾

Q billing

	Policy name ▾	Type	Attachments ▾	Description
<input checked="" type="checkbox"/>	▶ Billing	Job function	0	Grants permissions for billing and cost management. This includes

# Enable IAM Under Account Settings

## ▼ Account Settings

Edit 

**Account Id:** 057134241828

**Seller:** AWS Inc.

**Account Name:** David Benna

**Password:** \*\*\*\*\*

My Account

My Organization

My Billing Dashboard

My Security Credentials

Sign Out

## ▼ Contact Information

Edit

Please note that updating your contact information on this page will not update the information displayed on your PDF Invoices. If you wish to update the billing address information associated with your Invoice, please edit it through the Payment Methods page, located [here](#).

## ▼ IAM User and Role Access to Billing Information

You can give IAM users and federated users with roles permissions to access billing information. This includes access to Account Settings, Payment Methods, and Report pages. You control which users and roles can see billing information by creating IAM policies. For more information, see [Controlling Access to Your Billing Information](#).

☒ **Activate IAM Access**

Update

Cancel

# Test Billy Biller

## Welcome to Identity and Access Management

IAM users sign-in link:

<https://awsandbeyond.signin.aws.amazon.com/console>



| [Customize](#)

Copy to clipboard

## IAM Resources

Users: 3

Groups: 3









Customer Managed Policies: 0

Roles: 4

Identity Providers: 0

## Security Status

 4 out of 5 complete.

- |   |                                   |   |
|---|-----------------------------------|---|
|  | Delete your root access keys      |  |
|  | Activate MFA on your root account |  |
|  | Create individual IAM users       |  |
|  | Use groups to assign permissions  |  |



# Create auditor@security.nodomain

## Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name\*

[+ Add another user](#)

## Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type\*

☐

**Programmatic access**

Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☒

**AWS Management Console access**

Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password\*

☒

Autogenerated password

☐

Custom password

Require password reset

☐

User must create a new password at next sign-in

# IAM Study Links

---

## **IAM AWS LABS: (each is a link)**

- [Tutorial: Delegate Access to the Billing Console](#)
- [Tutorial: Delegate Access Across AWS Accounts Using IAM Roles](#)
- [Tutorial: Create and Attach Your First Customer Managed Policy](#)
- [Tutorial: Enable Your Users to Configure Their Own Credentials and MFA Settings](#)

# Create auditing group

Group name

auditing

Create policy

Refresh

A group can have no more than 10 policies attached. You must deselect one or more policies to finish creating the group. [Learn more](#)

Filter: Policy type


readonly

Policy name

Type

Attachments

Description

- ☒ ▶  AmazonDynamoDBReadOnlyAccess
- ☒ ▶  AmazonEC2ContainerRegistryReadOnly

AWS managed

0

Provides read only access t

AWS managed

0

Provides read-only access t

# Test Access

- Create custom URL
- Test billybiller and your gmail login

The screenshot shows the AWS IAM console interface. At the top is a navigation bar with the AWS logo and links to various services: Services, Resource Groups, EC2, Route 53, S3, VPC, CloudFormation, IAM, and CloudWatch. On the left is a sidebar with a search bar and a list of navigation items: Dashboard (highlighted), Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area is titled 'Welcome to Identity and Access Management'. It includes a section for 'IAM users sign-in link:' with the URL 'https://awsandbeyond.signin.aws.amazon.com/console' circled in yellow. To the right of this link is a 'Customize' link and a tooltip that says 'Click here to remove the alias', also circled in yellow. Below the sign-in link is a section for 'IAM Resources' showing counts for Users (5), Groups (4), Roles (4), and Identity Providers (0). At the bottom is a 'Security Status' section with a progress bar indicating '4 out of 5 complete'. It contains a list of security tasks: 'Delete your root access keys' (checked), 'Activate MFA on your root account' (warning icon), and 'Create individual IAM users' (checked).

aws Services ▾ Resource Groups ▾ EC2 Route 53 S3 VPC CloudFormation IAM CloudWatch

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

## Welcome to Identity and Access Management

IAM users sign-in link:

<https://awsandbeyond.signin.aws.amazon.com/console>

[Customize](#) Click here to remove the alias

### IAM Resources

Users: 5 Roles: 4

Groups: 4 Identity Providers: 0

Customer Managed Policies: 0

### Security Status

4 out of 5 complete.

✓	Delete your root access keys	▼
⚠	Activate MFA on your root account	▼
✓	Create individual IAM users	▼

Feature S

Additional

IAM best pr

IAM docum

Web Identit