

AWS Organizations with SSO, uniform cloudTrail and billing, Admin role that can assume role in other account. - GL

Creating separate AWS accounts to make one organization. Within this Organization we would like one consolidated billing receipt, more uniformed permissions and logs.

Create IAM Admin with MFA to use instead of the Root account due to unrestricted power. An Admin in one account will be able to assume a role and act as an admin in another account to provide support for that department in case their Admin cannot be reached or is out of town. Billing alarms for when account reaches threshold in price limit and create notifications to allow user to decide what action to take.

For more organizational access permission sets will be used with SSO to create a user portal with access to all accounts but with limited permissions.



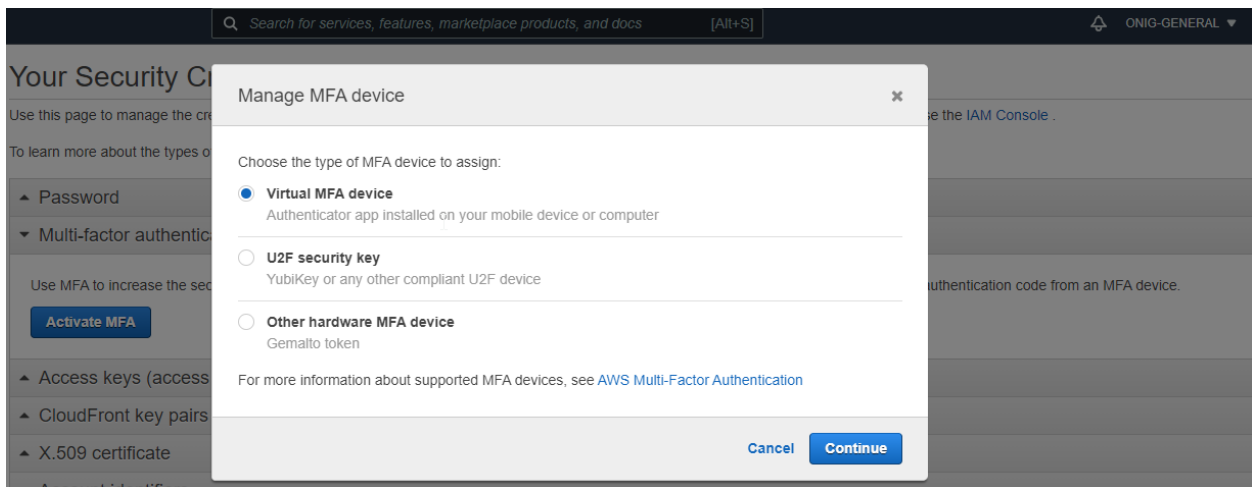
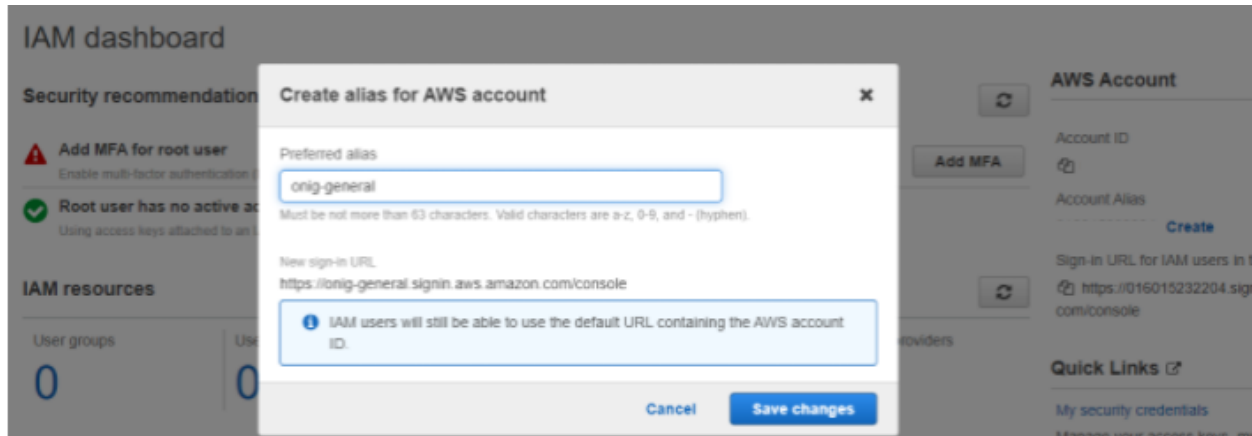
Congratulations!

Thank you for signing up with AWS.

We are activating your account, which should take a few minutes. You will receive an email when this is complete.

[Go to the AWS Management Console](#)

- We can also create an alias for the account for a more readable URL for users. Since it is on the same screen.
- Next step is to secure the account. We need MFA for a second authentication factor in case somebody gets hold of username and password. MFA generates a new code every 30 seconds making it hard to obtain.



Password		
Multi-factor authentication (MFA)		
Use MFA to increase the security of your AWS environments. Signing in to MFA-protected accounts requires a user name, password, and an authentication code from an MFA device.		
Device type	Serial number	Actions
Virtual	arn:aws:iam::-mfa-device	Manage

- To make sure we do not go over AWS service usage an alert needs to be made. By default all the boxes are unchecked. We also need this checked to allow cloudWatch Alarms to monitor it

Home

Billing

Bills

Payments

Credits

Purchase orders

Cost & Usage Reports

Cost Categories

Cost allocation tags

Cost Management

Cost Explorer

Budgets

Budgets Reports

Savings Plans

Preferences

Billing preferences

Preferences

Billing Preferences

☒ **Receive PDF Invoice By Email**

Turn on this feature to receive a PDF version of your invoice by email. Invoices are generally available within the first three days of the month.

Cost Management Preferences

☒ **Receive Free Tier Usage Alerts**

Turn on this feature to receive email alerts when your AWS service usage is approaching, or has exceeded, the AWS Free Tier usage limits. If you wish to receive these alerts at an email address that is not the primary email address associated with this account, please specify the email address below.

Email Address:

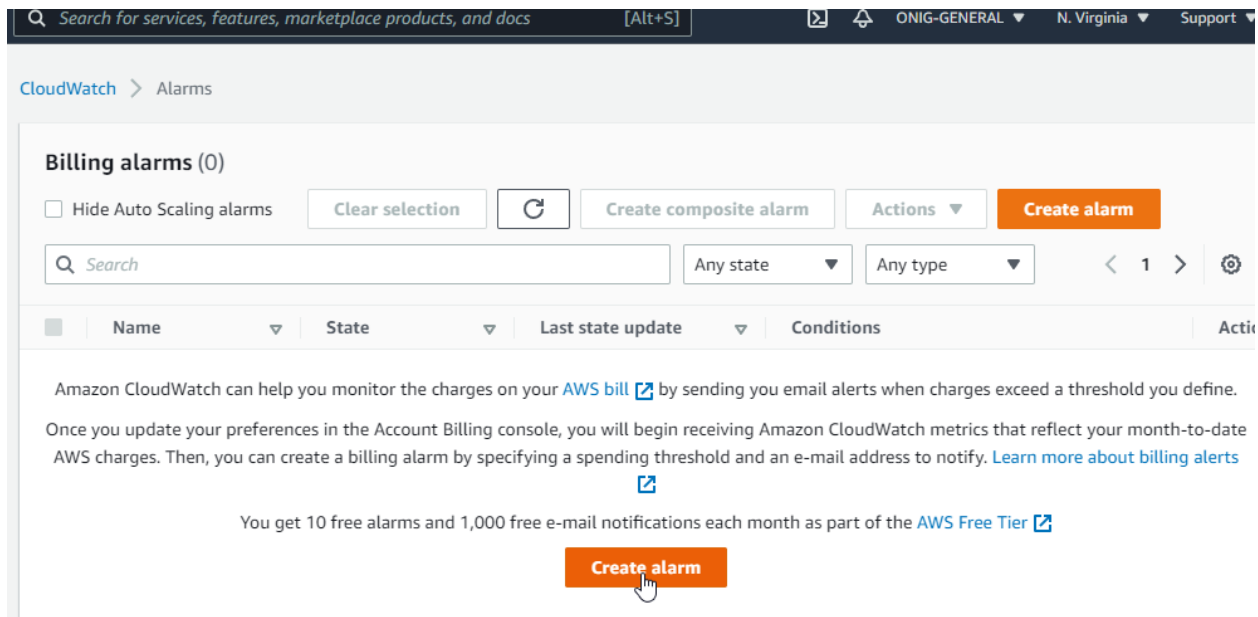
☒ **Receive Billing Alerts**

Turn on this feature to monitor your AWS usage charges and recurring fees automatically, making it easier to track and manage your spending on AWS. You can set up billing alerts to receive email notifications when your charges reach a specified threshold. Once enabled, this preference cannot be disabled. [Manage Billing Alerts](#) or [try the new budgets feature!](#)

► Detailed Billing Reports [Legacy]

Save preferences

- Now we need to make an actual alarm, this will monitor certain metrics and change state based on a condition. In this case, when we exceed free tier we want the alarm to go from OK to ALARM.
- By default we have no alarms.



- This alarm will track the following metric named EstimatedCharges. Specifically, It'll track every 6 hours and if the charge for the account reaches a \$10 quota for the month.

Metric

Edit

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 6 hours.

Namespace

AWS/Billing

Metric name

EstimatedCharges

Currency

USD

Statistic

Maximum

Period

6 hours

Conditions

Threshold type

☒ Static
Use a value as a threshold

☐ Anomaly detection
Use a band as a threshold

Whenever EstimatedCharges is...

Define the alarm condition.

☒ Greater
> threshold

☐ Greater/Equal
≥ threshold

☐ Lower/Equal
≤ threshold

☐ Lower
< threshold

than...

Define the threshold value.

10

USD

Must be a number

► Additional configuration

Cancel

Next

AWS Organizations with SSO, uniform cloudTrail and billing, Admin role that can assume role in other account. - GL 5

Notification

Alarm state trigger

Define the alarm state that will trigger this action.

Remove

☒ **In alarm**

The metric or expression is outside of the defined threshold.

☐ **OK**

The metric or expression is within the defined threshold.

☐ **Insufficient data**

The alarm has just started or not enough data is available.

Select an SNS topic

Define the SNS (Simple Notification Service) topic that will receive the notification.

☐ Select an existing SNS topic

☒ **Create new topic**

☐ Use topic ARN

Create a new topic...

The topic name must be unique.

EstimatedCharges_Exceeded

SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).

Email endpoints that will receive the notification...

Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

onig...l@gmail.com

user1@example.com, user2@example.com

Create topic

Add notification

Type '/' for commands

- We then need to define an alarm state for when the metric is met. In this case below, state will be in ALARM, and we want to notify the owner via email. An SNS topic needs to be made which is a subject or communication channel. Whoever is subscribed to this channel may receive the alert.
- Finally add a name and description to the alarm

Add name and description

Name and description

Alarm name

Alarm description - *optional*

Up to 1024 characters (17/1024)

Cancel Previous Next

- A subscriber must confirm they would like to be added to the channel otherwise they will never receive it.

Search for services, features, marketplace products, and docs [Alt+S]

ONIG-GENERAL N. Virginia

Successfully created alarm EstimatedCharges.

Some subscriptions are pending confirmation

Amazon SNS doesn't send messages to an endpoint until the subscription is confirmed

View SNS Subsc

CloudWatch > Alarms

Billing alarms (1)

☐ Hide Auto Scaling alarms

Clear selection

Refresh

Create composite alarm

Actions

Create

Any state Any type

☐	Name	State	Last state update	Conditions	Actions
☐	EstimatedCharges	Insufficient data	2021-10-13 08:04:03	EstimatedCharges > 10 6 hours	This action sends a message to an SNS topic with an endpoint that is pending confirmation. It will not work as expected until the endpoint is confirmed. Look for a subscription confirmation email or review the topic in SNS. Warning

AWS Notifications <no-reply@sns.amazonaws.com>
to onig.aws+general ▾

8:02 AM (2 minut

You have chosen to subscribe to the topic:

arn:aws:sns:us-east-

4:EstimatedCharges_Exceeded

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):

[Confirm subscription](#)

- Do this for second account*
- The AWS accounts now just need an IAM admin because we do not want to use the Root for safety reasons.
- Create an IAM Admin to act as the account administrator. Since I am going to use the user I will create a password to keep otherwise if assigning may want to autogenerate and allow the target user to generate a new one on fist sign-on.

Services ▾ 🔍 Search for services, features, marketplace products, and docs [Alt+S] ONIG-PRODUCTION ▾ Gl

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 primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type* ☒ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☒ **Password - 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
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

* Required Cancel Next Permissions

- We want to then add a policy with authorizes the users access to services. In this case administrator privilege's.

▼ Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

Create policy

Filter policies ▼

	Policy name ▼	Type	Used as
☒	AdministratorAccess	Job function	None

Permissions
Policy usage
Policy versions

Policy summary
{} JSON

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "*",
7       "Resource": "*"
8     }
9   ]
10 }
  
```

- The policy is written in JSON. In this case it is allowing any action on any resource. By default everything is denied, you must give allow privileges.
- Now we can logout of root and use the admin account from now on. Sign in using the console URL created when we made an account alias. You can check if you're logged into an IAM USER by clicking you username dropdown menu.



Sign in as IAM user

Account ID (12 digits) or account alias

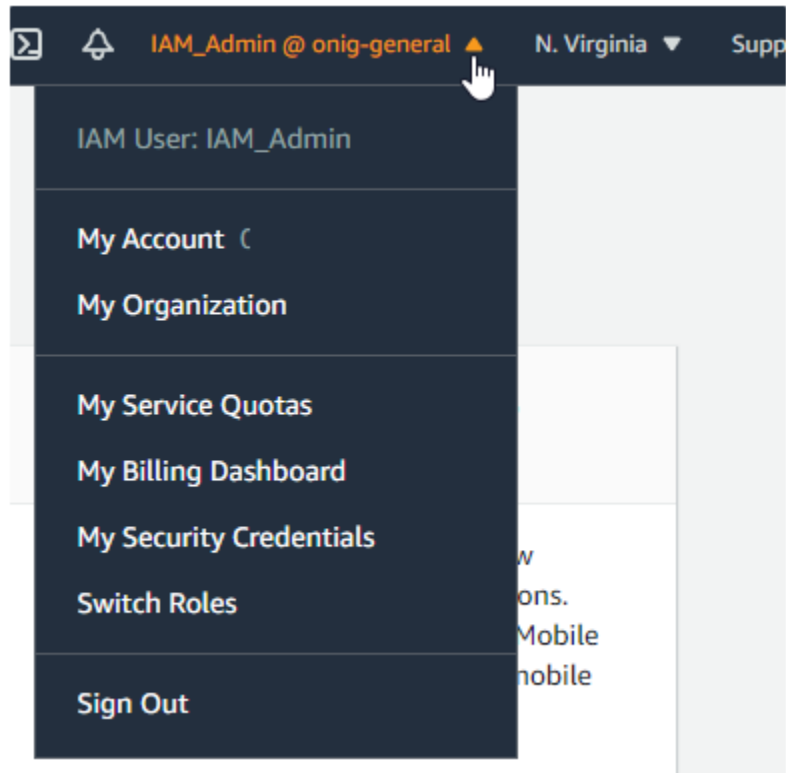
IAM user name

Password

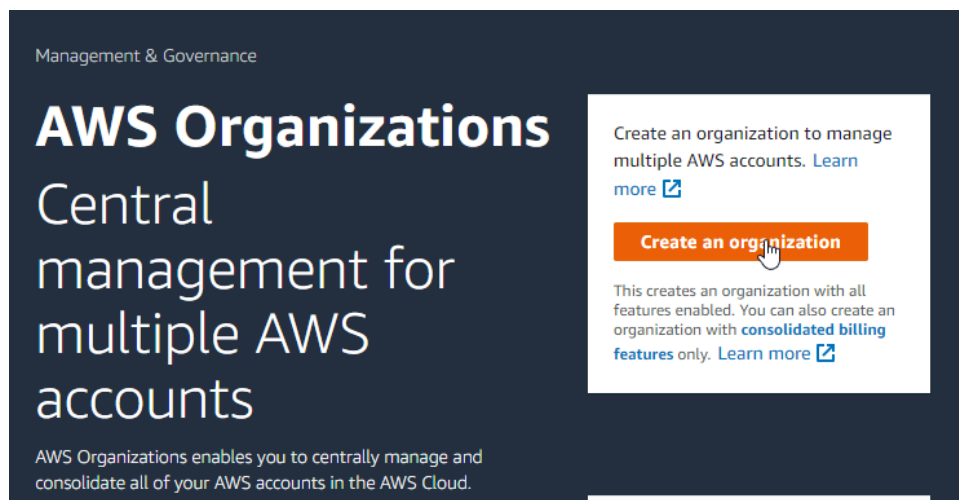
Sign in

[Sign in using root user email](#)

[Forgot password?](#)



- Now we can create an AWS organizations, this way we can merge accounts and have one consolidated bill. Click create and you're all set, this will then be the root account in the organization



AWS Organizations > AWS accounts

AWS accounts

The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS to manage these accounts. [Learn more](#)

Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a unit instead of one at a time.

Find AWS accounts by name, email, or account ID. Find an OU by the name or ID.

Organizational structure

- ▼ ☐ **Root**
r-wm53
 - ☐ **ONIG-GENERAL** **management account**
4 | onig@gmail.com

- We can invite existing accounts to this organization or create accounts from within. If inviting existing you must verify the "management account's" email

Add an AWS account

You can add an AWS account to your organization either by creating an account or by inviting an existing AWS account to join your organization.

☐ Create an AWS account
Create an AWS account that is added to your organization.

☒ Invite an existing AWS account
Send an email request to the owner of the account. If they accept, the account joins the organization.

 **You must verify the management account's email address before you can invite AWS accounts to join your organization.**

Send verification email

Cancel

Send invitation

Add an AWS account

You can add an AWS account to your organization either by creating an account or by inviting an existing AWS account to join your organization

☐ Create an AWS account
Create an AWS account that is added to your organization.

☒ Invite an existing AWS account
Send an email request to the owner of the account. If they accept, the account joins the organization.

Invite an existing AWS account to join your organization

Email address or account ID of the AWS account to invite

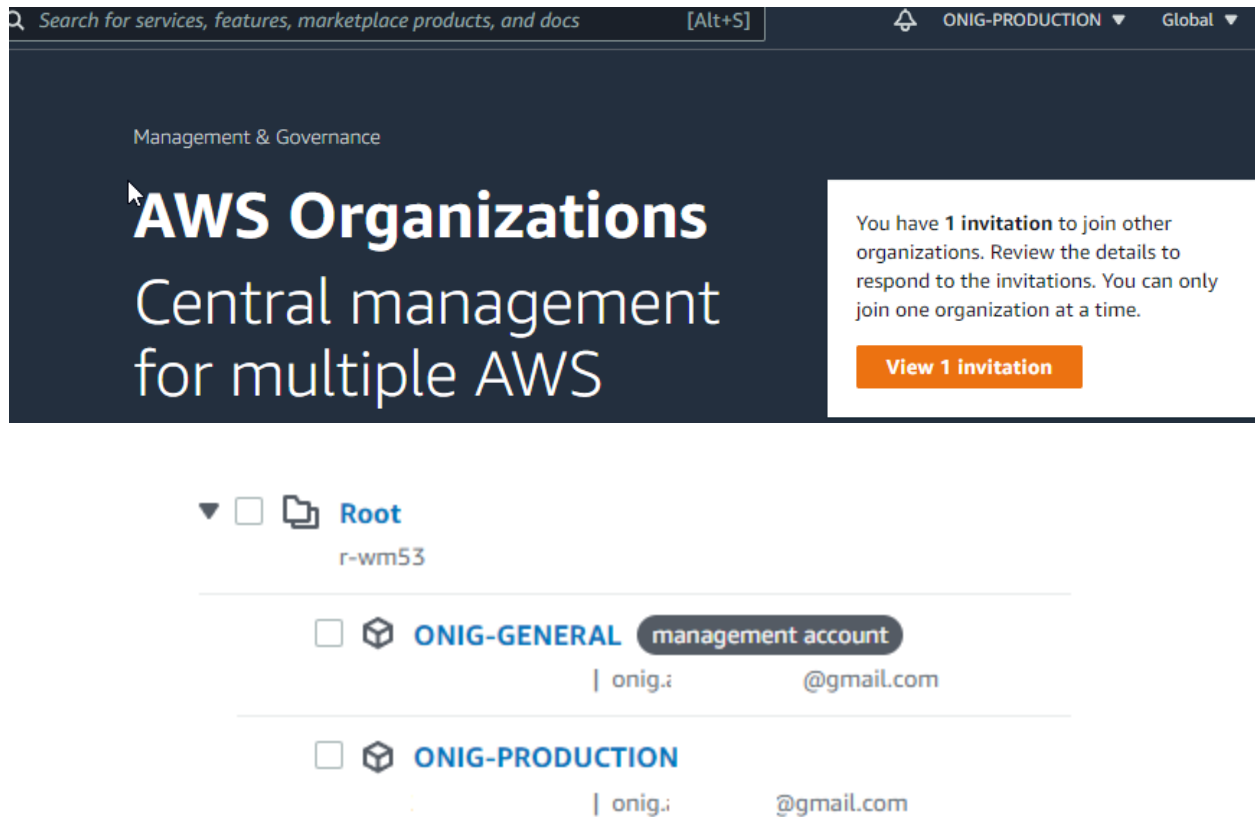
Add another

Message to include in the invitation email message - *optional*

This text is included in the email message sent to the owners of the invited AWS accounts.

Inviting you to the company's organization

- Accept invitation from the other account in AWS Organizations tab



- Because we invited an AWS account this means we need to create a role switching role in order to go into it from another account. If you create an account within the organization then it automatically creates this. All you need is create a role in the invited account (prod), specify another AWS account (general) and input the ID.

Select type of trusted entity

 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web id Cognito provider
--	---	---

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

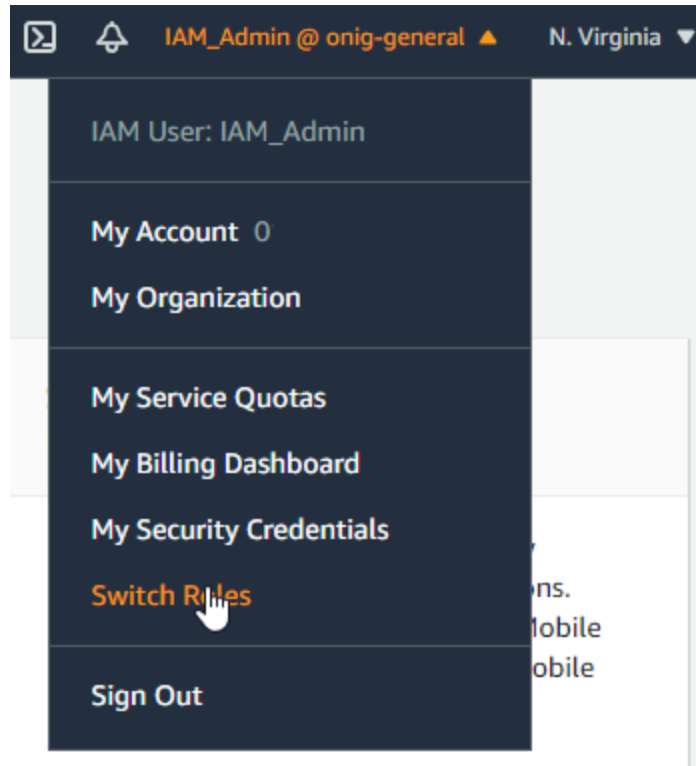
Account ID*	0	
--------------------	--------------------------------	---

Review

Provide the required information below and review this role before you create it.

Role name*	OrganizationAccountAccessRole Use alphanumeric and '+', '@', '-' characters. Maximum 64 characters.
Role description	Admin access Maximum 1000 characters. Use alphanumeric and '+', '@', '-' characters.
Trusted entities	The account 0
Policies	 AdministratorAccess

- So now we can assume a role from the general management account into the prod account. Just need the account ID you want to switch to as well as the name of the role.



Switch Role

Allows management of resources across Amazon Web Services accounts using a single user ID and password. You can switch roles after an Amazon Web Services administrator has configured a role and given you the account and role details. [Learn more.](#)

Account* ⓘ

Role* ⓘ

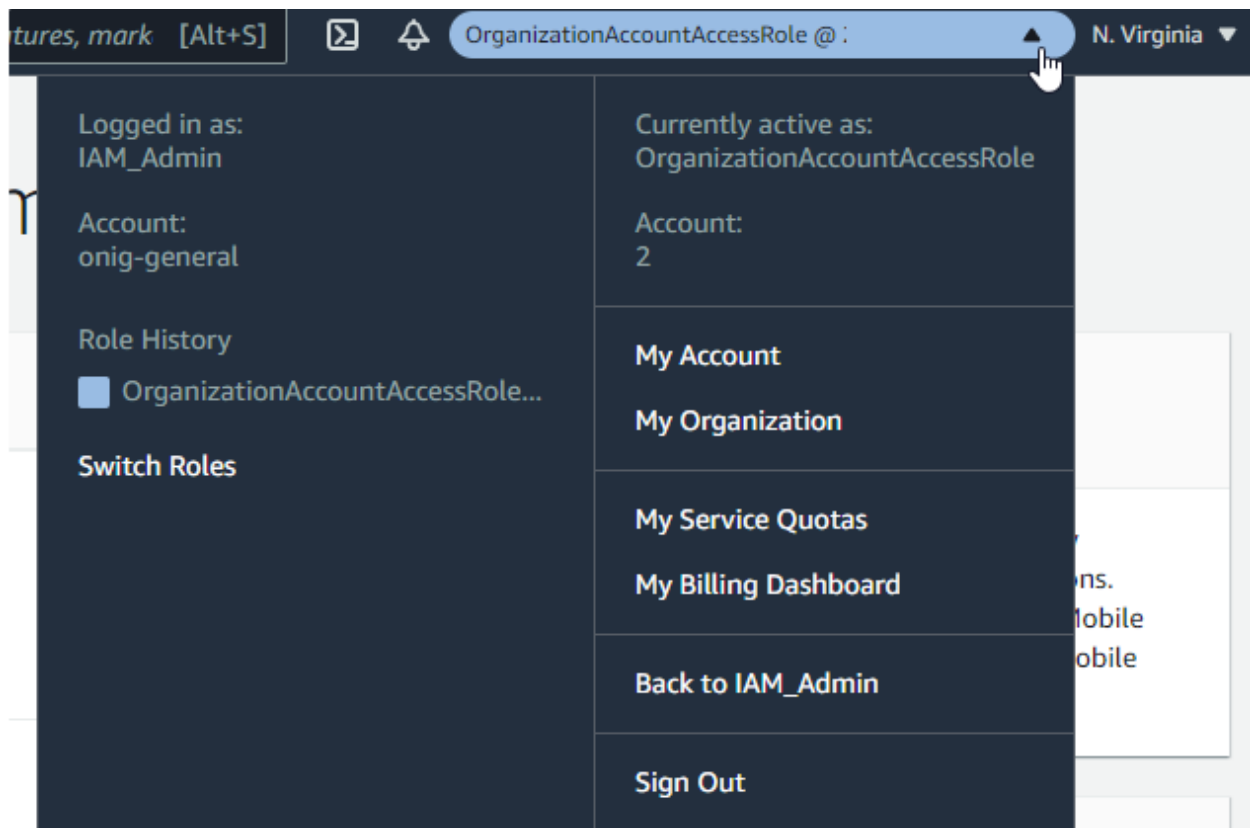
Display Name ⓘ

Color a a a a a a

*Required

[Cancel](#)

[Switch Role](#)



- So we are not going to implement organizational level cloudTrail which will log all the API calls within all the AWS accounts. This way it is located in one S3 bucket making it easy to analyze,
- A trail is a configuration about the logs we want to deliver to the S3 bucket to store for later. Organization trails allows us to use a configuration for all member accounts of a management account in an AWS organization. Therefore we have one unified logging system for a whole account. We can also integrate with cloudWatch logs so we have the ability to monitor trail logs and notify via alarms when an activity occurs.
- 3 types of trails are captured: insight events (unusual volumes of API calls), data events ('GET' to S3 objects) and management events (default, EC2 restarted, who logged in)

Choose trail attributes

Step 1 of 3

General details

A trail created in the console is a multi-region trail. [Learn more](#) 

Trail name

Enter a display name for your trail.

onig-org

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

☒ Enable for all accounts in my organization

To review accounts in your organization, open AWS Organizations. [See all accounts](#) 

Storage location [Info](#)

☒ Create new S3 bucket
Create a bucket to store logs for the trail.

☐ Use existing S3 bucket
Choose an existing bucket to store logs for this trail.

Trail log bucket and folder

Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

cloudtrail-onig-org

Logs will be stored in cloudtrail-onig-org/AWSLogs/o-p5qrh3khar/016015232204

Log file SSE-KMS encryption [Info](#)

☒ Enabled

- Enable cloudWatch logs and a log group, needs an IAM role to give permission.

CloudWatch Logs - *optional*

Configure CloudWatch Logs to monitor your trail logs and notify you when specific activity occurs. Standard CloudWatch and CloudWatch Logs charges apply. [Learn more](#) 

CloudWatch Logs [Info](#)

☒ Enabled

Log group [Info](#)

☒ New

☐ Existing

Log group name

cloudwatchlogs-onig-org

1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.

IAM Role [Info](#)

AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.

☒ New

☐ Existing

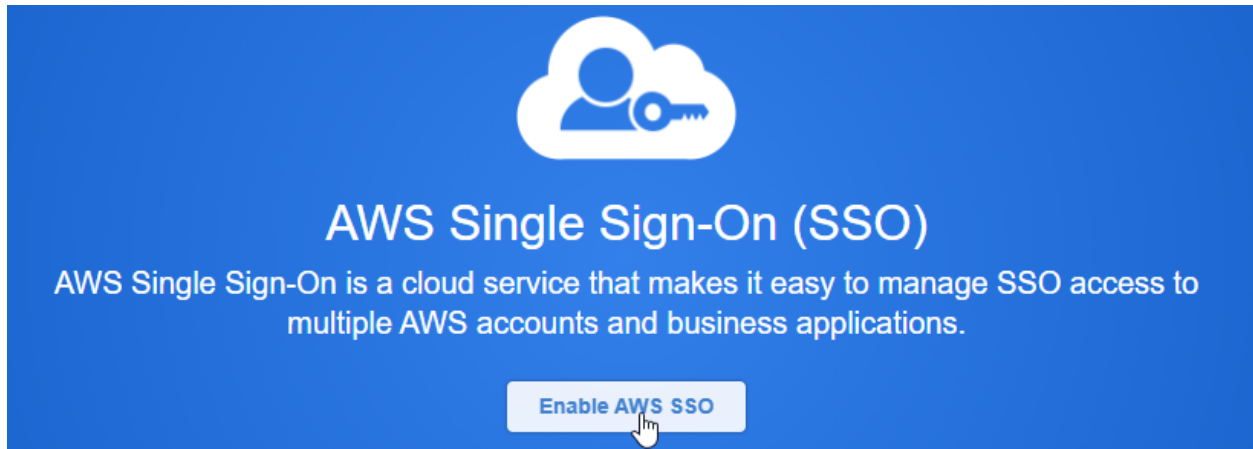
Role name

CloudTrailRoleForOrgAccount

- CloudTrail can be applied to all regions!

Enabling SSO

- We can establish permission sets for groups and users in SSO. This way we can give admin, billing or read only permissions easily for multiple accounts in one organization. We can also give a session duration before it has to be renewed.



- Change the user portal for SSO for a more human readable domain

Customize user portal URL

✕

Customize the URL that your users will use to access their assigned AWS accounts and applications.

User portal URL

You will not be able to change this later.

https://

onig-ssso

.awsapps.com/start ⓘ

Cancel

Save

- We can select the source for our identities, SSO (you administer), Microsoft AD, external IdP (we administer via external IdP)

Change identity source

1

Choose identity source

2

Review

Choose where your identities are sourced

Your identity source is the place where you administer and authenticate identities. You use AWS SSO to manage permissions for identities from your identity source to access AWS accounts, roles, and applications. [Learn more](#)

☒ **AWS SSO**

You will administer all users, groups, credentials, and multi-factor authentication assignments in AWS SSO. Users sign in through the AWS SSO user portal.

☐ **Active Directory**

You will administer all users, groups, and credentials in AWS Managed Microsoft AD, or you can connect AWS SSO to your existing Active Directory using AWS Managed Microsoft AD or AD Connector. Users sign in through the AWS user portal.

☐ **External identity provider**

You will administer all users, groups, credentials, and multi-factor authentication in an external identity provider (IdP). Users sign in through your IdP sign-in page to access the AWS SSO user portal, assigned accounts, roles, and applications.

- Change multi-factor options if needed. Can prompt it on every login, what device MFA is allowed on etc.

Multi-factor authentication

Define the behavior you want to enforce to secure user portal access with multi-factor authentication (MFA). You register MFA devices for users individually through the Users page. [Learn more](#)

Prompt users for MFA

Never (disabled)

Configure

- We want to create an SSO group called billing, and with this we can add users who will be in charge of billing alarms and alerts to have the necessary permissions. We use permission sets which define access levels for the user or group it is assigned to within SSO. This is different to normal IAM because this applies to all the accounts rather than just one. All a user has to do is log into the SSO portal and their credentials are assigned a set of permissions.

AWS SSO > Groups

Groups

With groups you can

[Create group](#)

Group name

☐ Group name

No groups found

Create group

Create group

Group name* Billing_Management

Can contain only alphanumeric characters, or any of the following: . _ - Maximum of 128 characters

Description Billing admins

Can contain only alphanumeric characters, or any of the following: . _ - Maximum of 256 characters

* Required fields

[Cancel](#) [Create](#)

- Once we have a group we can make the user. SSO gives us additional information like contact methods, job info etc.

User details

[View user details](#) [View user groups](#)

Username* John

This username will be required to sign in to the user portal. This cannot be changed later.

Password ☐ Send an email to the user with password setup instructions. [Learn more](#)
☒ Generate a one-time password that you can share with the user. [Learn more](#)

Email address* john@gmail.com

Confirm email address* john@gmail.com

First name* John

Last name* James

Display name* John James

▼ Contact methods (optional)

- Add the user to our billing group

Add user to groups

Users that you add to a group inherit access to AWS accounts, roles, and applications that are assigned to the group.

Create group

Find by group

Name ▲	Description
☒ Billing_Management	Billing admins

- We need to attach some permissions to the group/ user as we cannot do anything at the moment.
- We will create a permission set which can be attached to the SSO group/ user to give permission to the organization
- We will select the billing set

Create new permission set



Select job function policy

[AdministratorAccess](#)

Provides full access to AWS services and resources.

[Billing](#)

Grants permissions for billing and cost management. This includes viewing account usage and viewing and modifying budgets and payment methods.

- When you sign into the user you made via SSO portal you will see everything you have access to
- In this case, we see nothing. And that is because we did not attach the permission sets to the designated accounts. The user John and it's billing group has the permission set but the accounts do not.

You do not have any applications.

- We can go back into SSO and view our AWS Accounts and confirm, no accounts have SSO users or groups attached to them.

AWS Accounts

You can designate which users and groups have SSO access to AWS accounts in your AWS organization. You can also manage permission sets to control the users' level of access to these AWS accounts. [Learn more](#)

AWS organization **Permission sets**

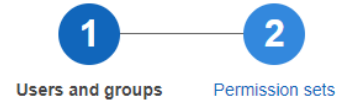
Select one or more AWS accounts in your AWS organization to provide SSO access to users and groups. If you have organized your accounts under organizational units (OUs), you can choose an OU to make account selection easier. [Learn more](#)

Assign users

	AWS account	Permission sets
• All accounts	☐ ONIG-GENERAL #1 onig. @gmail.com	None
▶ Root	☐ onig-DEV #2 i onig.i @gmail.com	None
	☐ ONIG-PRODUCTION # onig @gmail.com	None

- Add group in this case to all the accounts

Assign Users



Select users or groups

You can search for the users and groups that you want to give SSO access to.

Users

Groups

1 group selected | Dese

Select one or more groups to assign to this AWS account.

Group name

Find groups by name

☒ Group name	Description
☒ Billing_Management	Billing admins

- Add permission set to the SSO group

Assign Users



Select permission sets

Permission sets define the level of access that users and groups have to an AWS account. Permission sets are stored in AWS SSO and appear in the AWS account as IAM roles. You can assign more than one permission set to a user. To ensure least privilege access to AWS accounts, users with multiple permission sets on an AWS account must pick a specific permission set when accessing the account and then return to the user portal to pick a different set when necessary. [Learn more](#)

Create new permission set

ARN

Find permission sets by full ARN or permission set ID (i.e., ps-abcdefg123456789).

☒ Permission set	Description	ARN
☒ Billing ↗		arn:aws:sso:::permissionSet/ssoins-7223ed2bc0fdcf2d/ps-69ee6309ea44758c

- Now you should see permission sets attached to the accounts

AWS Accounts

You can designate which users and groups have SSO access to AWS accounts in your AWS organization. You can also manage permission sets to control the users' level of access to these AWS accounts. [Learn more](#)

AWS organization **Permission sets**

Select one or more AWS accounts in your AWS organization to provide SSO access to users and groups. If you have organized your accounts under organizational units (OUs), you can choose an OU to make account selection easier. [Learn more](#)

Assign users to 3 accounts | **Deselect**

	AWS account	Permission sets
• All accounts	☒ ONIG-GENERAL #0 onig. @gmail.com	Billing
▶ Root	☒ onig-DEV #2 onig. @gmail.com	Billing
	☒ ONIG-PRODUCTION #2 onig. @gmail.com	Billing

- Now log back into the SSO console via John

Single Sign-On MFA devices | Sign out

Search


AWS Account (3)

**onig-DEV**
#2 | onig. | @gmail.com
Billing [Management console](#) | [Command line or programmatic access](#)

**ONIG-GENERAL**
#0 | onig. | l@gmail.com

**ONIG-PRODUCTION**
#2 | onig. | @gmail.com

Terms of Use Powered by 