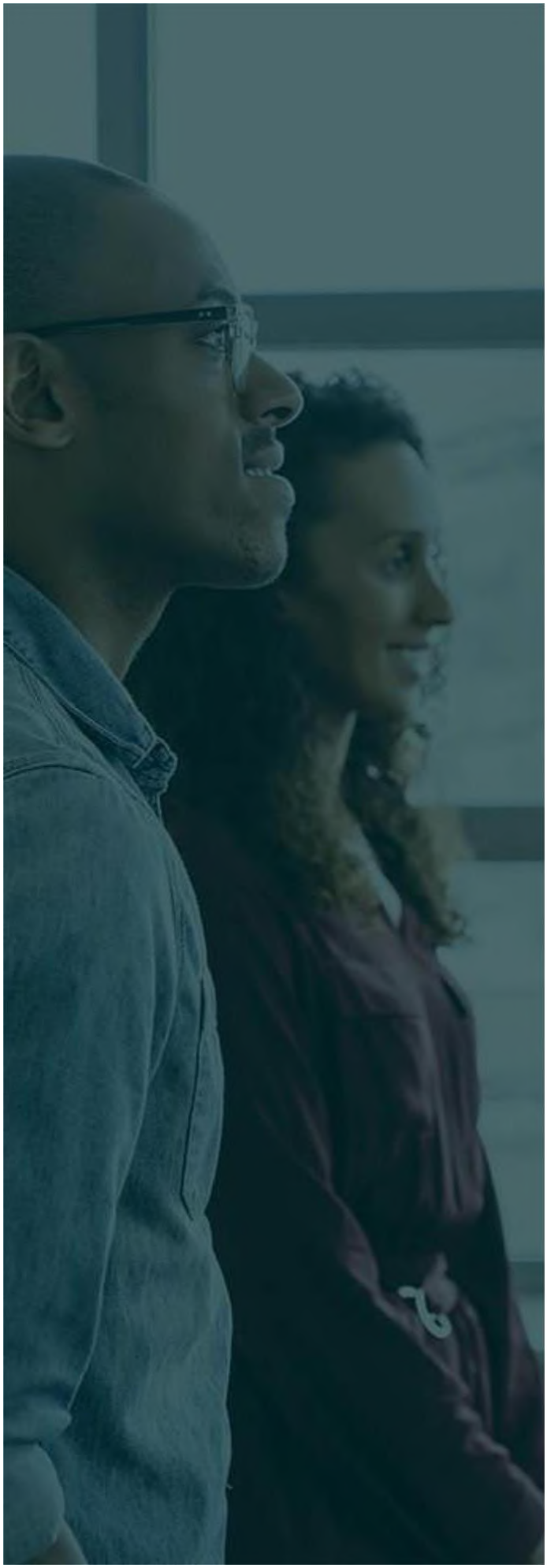
CLOUDENSURE

CLOUD GOVERNANCE PLATFORM

AWS Onboarding Guide



CloudEnsure
CLOUD GOVERNANCE PLATFORM

aws

Table of Contents

GETTING STARTED

CloudEnsure is an autonomous cloud governance platform built to manage multi-cloud environments – available both in SaaS & Enterprise versions. The tool performs real-time compliance checks on all your cloud accounts at a single stop, giving you, a bird's eye view of your cloud portfolio.

To start using CloudEnsure, following are the steps which must be completed:

- Signup of the root user with CloudEnsure
- Email verification of the above user
- Adding an AWS account with CloudEnsure

Once the above steps are completed, the root user can login to CloudEnsure and explore different modules available.

The below listed are pre-requisite details required to Signup & get started with the on- boarding process:

1. **Name:** This is a generic user information for root user. This can be the name of CTO, or a generic name. This should be indicative of who has access to the email and phone number used for registration.

2. **Organization Name:** We recommend this to be OU or BU or Revenue-Stream name. This can follow a naming convention & be something like **OrgName-BusinessUnitName**. This is generic root account user information.

3. **Email ID:** This ID is used for validation. We recommend this to be a group email-id accessible to one person at a time. For example, CTO@xyz.com. This ensures that this is easily transferrable internally from customer's side. The same ID is also used for admin activities such as root account password resets and account closure etc. Notification alerts
   & updates will be sent to the same ID.

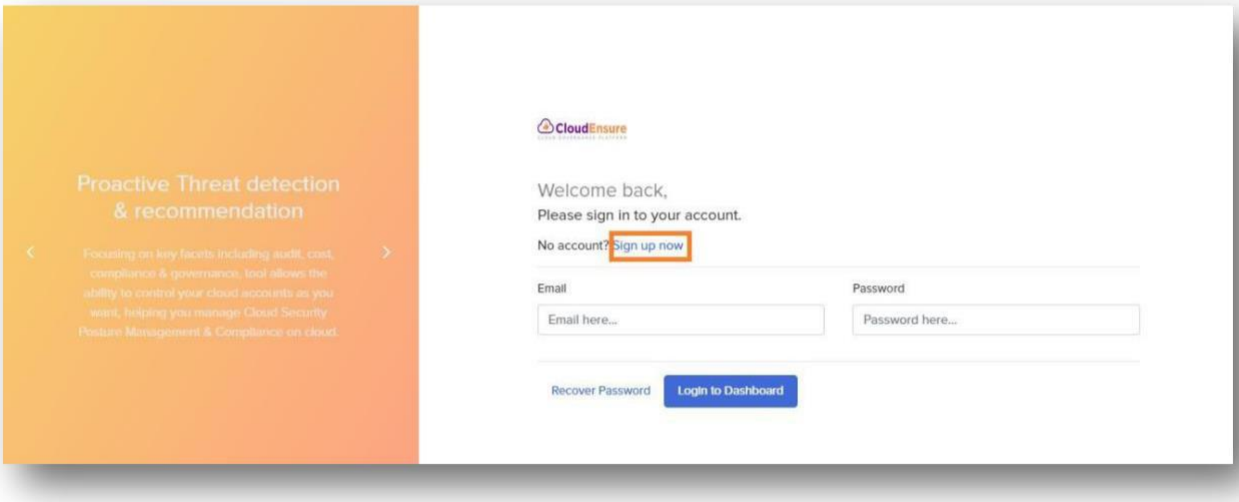
4. **Phone Number:** At this point we don't verify the registered phone number.

   However, we recommend this to be a service phone number. **In upcoming feature releases:**

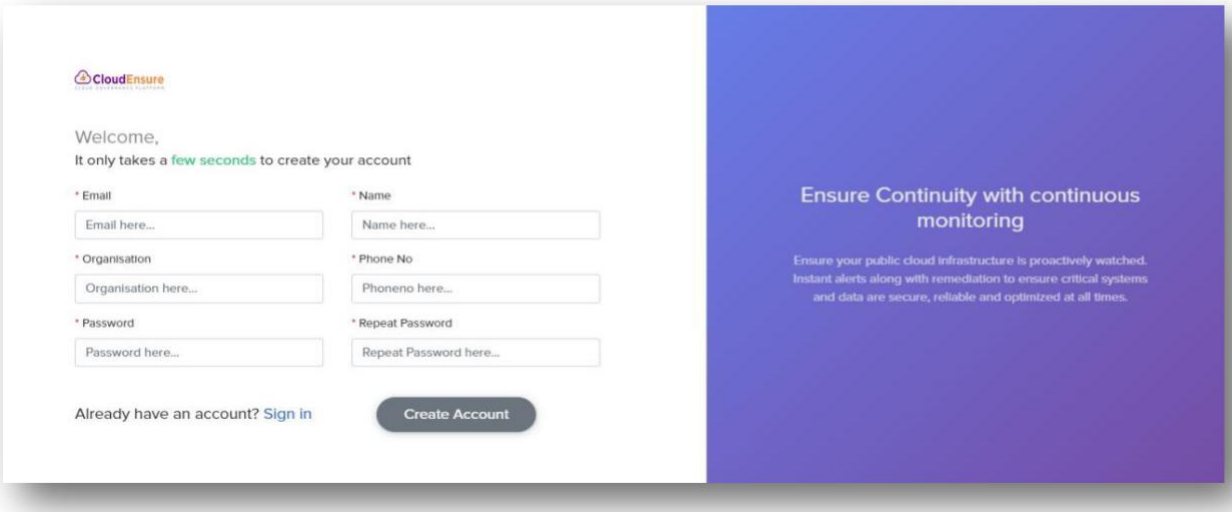
   - We will send notifications for business-critical findings.
   - We will use these numbers for OTP for MFA.

SIGNUP WITH EMAIL VERIFICATION

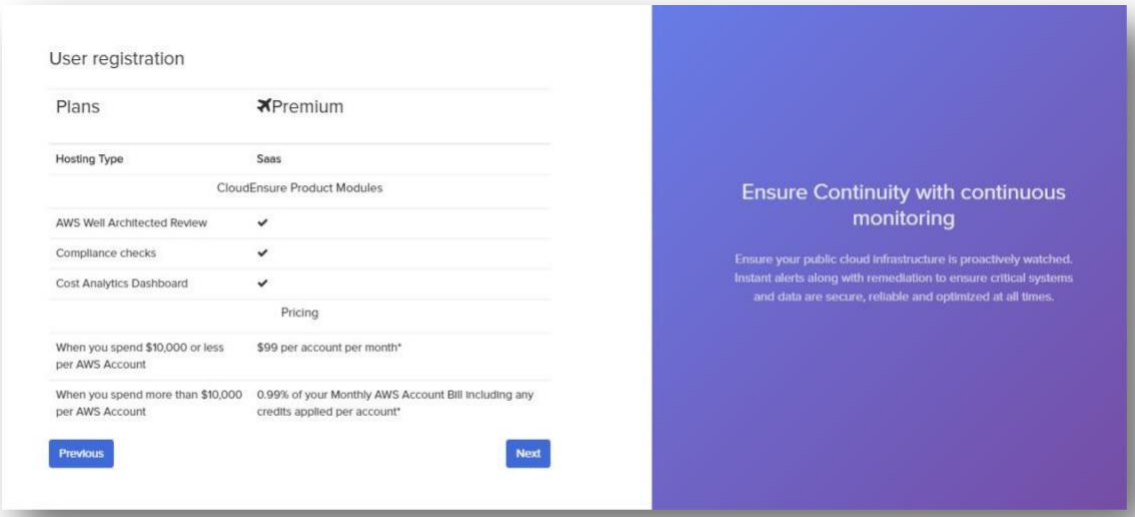
- Open https://app.cloudensure.io in your browser
- Click on **Sign up now** as shown below



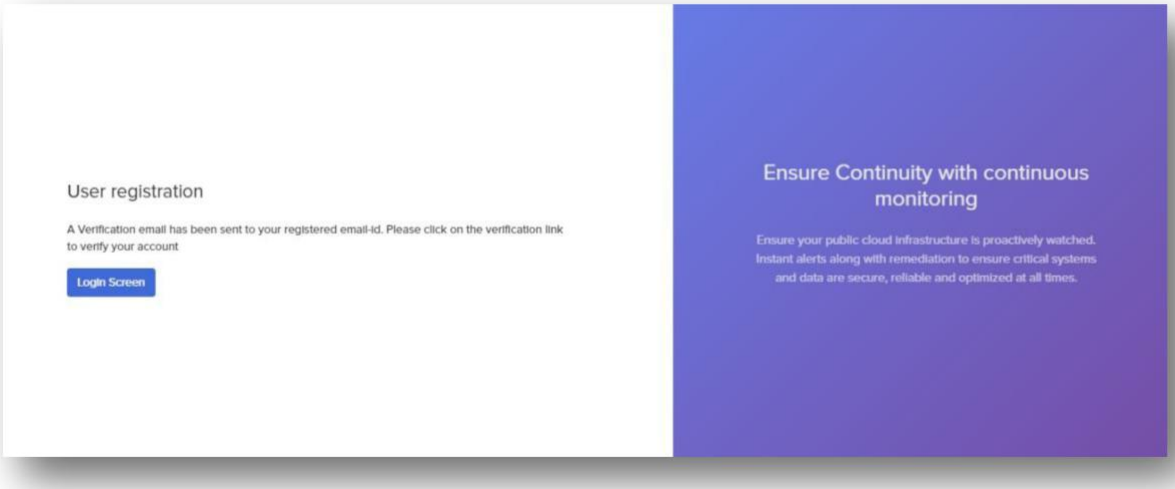
- Enter the required (mandatory) details and click on **Create Account**



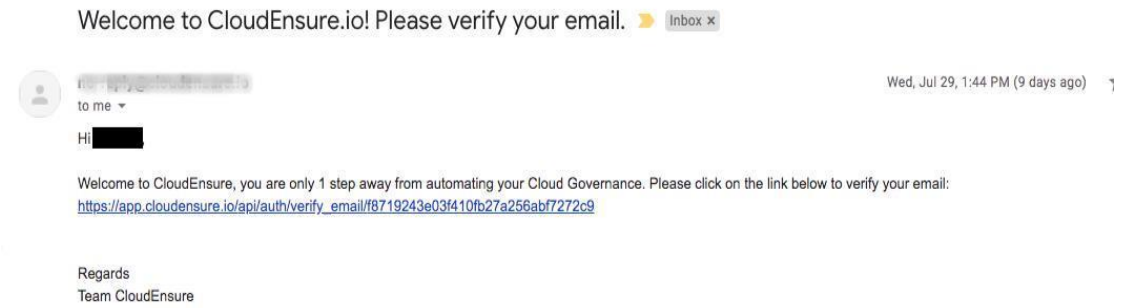
- The next screen will show the plan and its related details. Click on **Next**



- The final screen will show you a confirmation message that a verification link has been sent to your mail id which was used during the account creation



- Open your mail & verify your account using the verification link in the mail received from CloudEnsure



- Upon clicking the verification link, you will get a confirmation message as shown below

- This completes the signup and email verification process
- You will now have the authorization to login and add account(s) in the CloudEnsure application

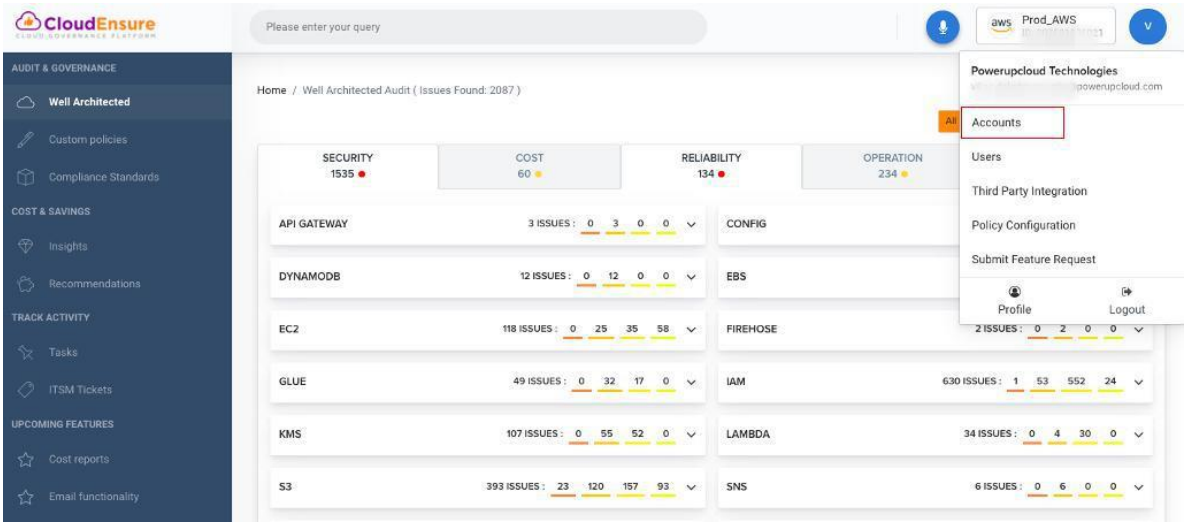
ADDING AN AWS ACCOUNT

The below listed are pre-requisite details required to add an account in the CloudEnsure application:

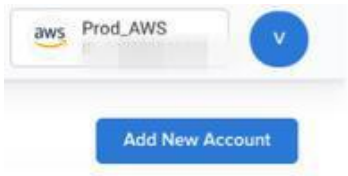
1. **AWS Account Name:** This is a reference name provided for ease of access & recognition for the account. This is a given name for each application ID. One root user account in CloudEnsure can onboard multiple cloud accounts for centralized governance.
2. **AWS Account ID:** A 12-digit number, such as 123456789012, that uniquely identifies an AWS account.
3. **Role-ARN:** An Amazon Resource Name (ARN) is a file naming convention used to identify a particular resource in the Amazon Web Services (AWS). Role - ARNs, are specific to AWS and is required for gaining role-based access.

Phase 1: Add New Account (AWS)

1. Open **https://app.cloudensure.io**
2. Enter **Username** with valid credentials (Email ID)
3. Enter **Password** with valid credentials (Minimum eight Characters)
4. Click on Login, you will be redirected to the CloudEnsure landing page

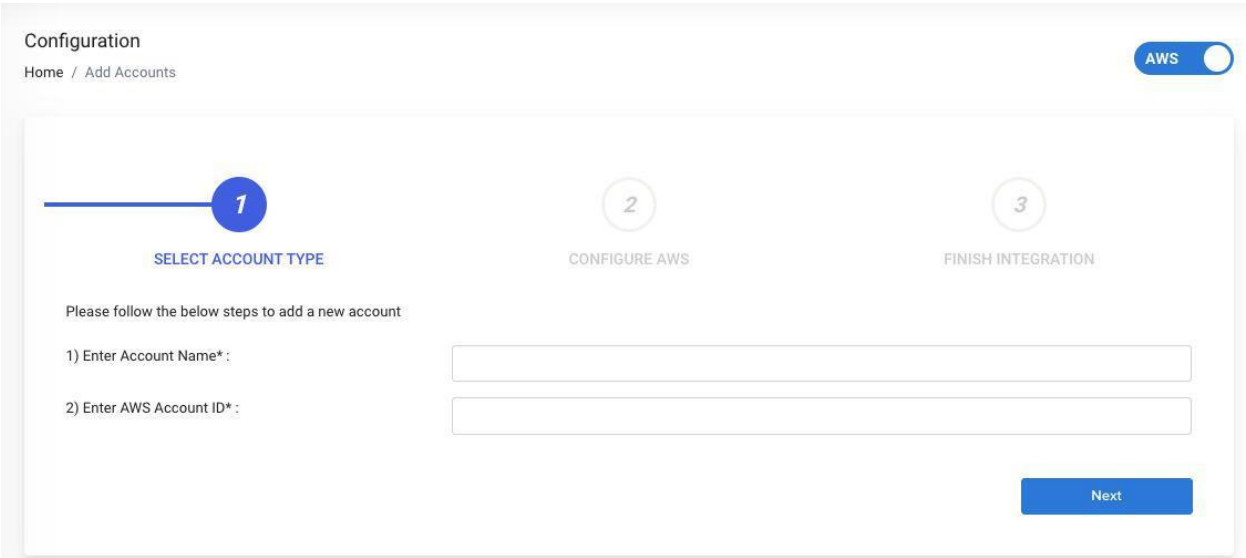


5. Click on top right drop down
6. Click on **Accounts**
7. Click on **“Add New Account”**



8. Select “**AWS**” using toggle button.

9. Enter “**Account Name**” & “**AWS Account ID**”, then click “**Next**”



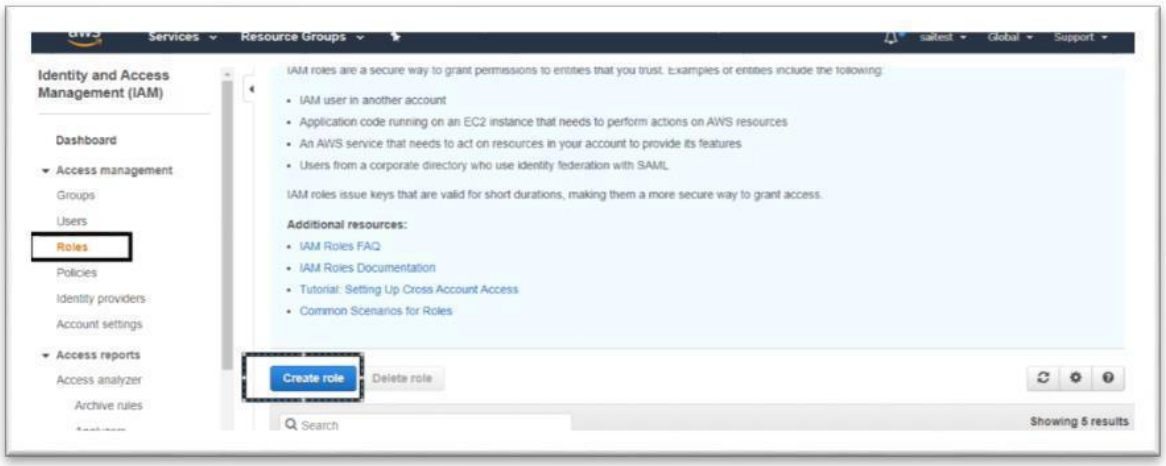
Note: If you don't have AWS ID, please follow the below steps.

- Log in to your AWS Account.
- Click on the username dropdown at the top of the navigation bar.
- Click on My Account
- You can see your Account ID

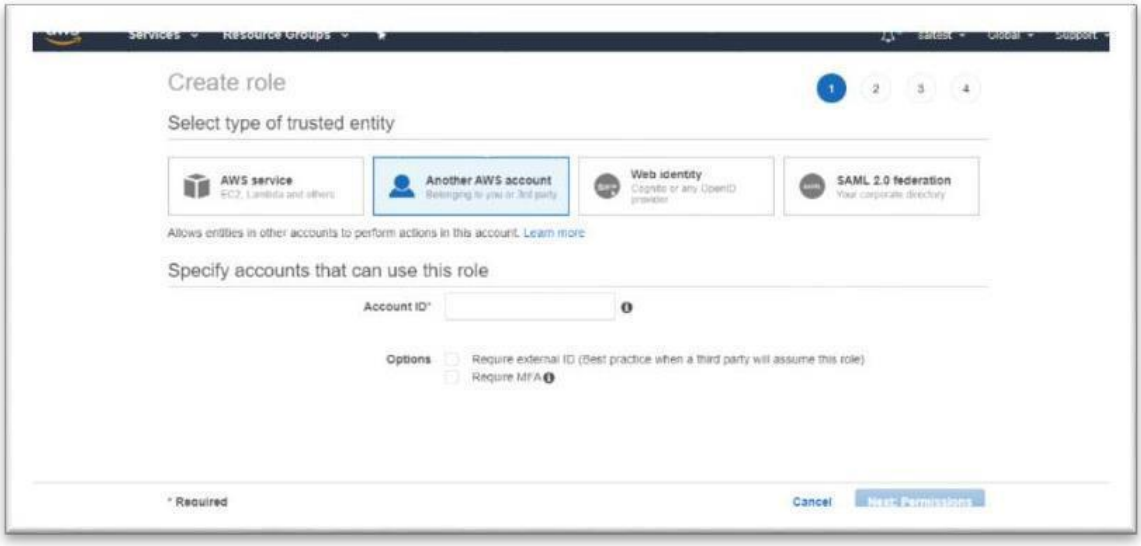
- Copy your Account ID and paste it in "AWS Account Id" field of CloudEnsure application

Phase 2 – Configuring AWS Access

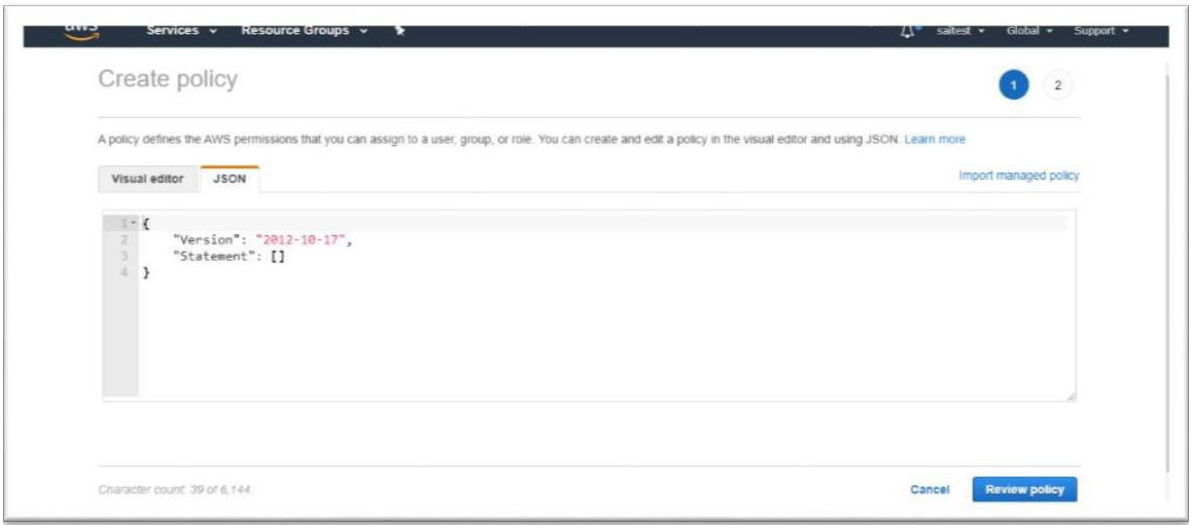
1. Go to your ***AWS Console***
2. Select ***IAM Service***
3. Click on Roles - **Create Role**



4. Select type of trusted entity as "***Another Aws Account***"
5. Now under specify accounts under this role
6. Enter 025012189825 in ***Account ID*** field
7. Click on ***Next***



8. Click on ***Create Policy***
9. Click on ***JSON***. Now from the CloudEnsure copy & paste the JSON code to the JSON in the AWS Account.
10. Click on "***Review policy*** "

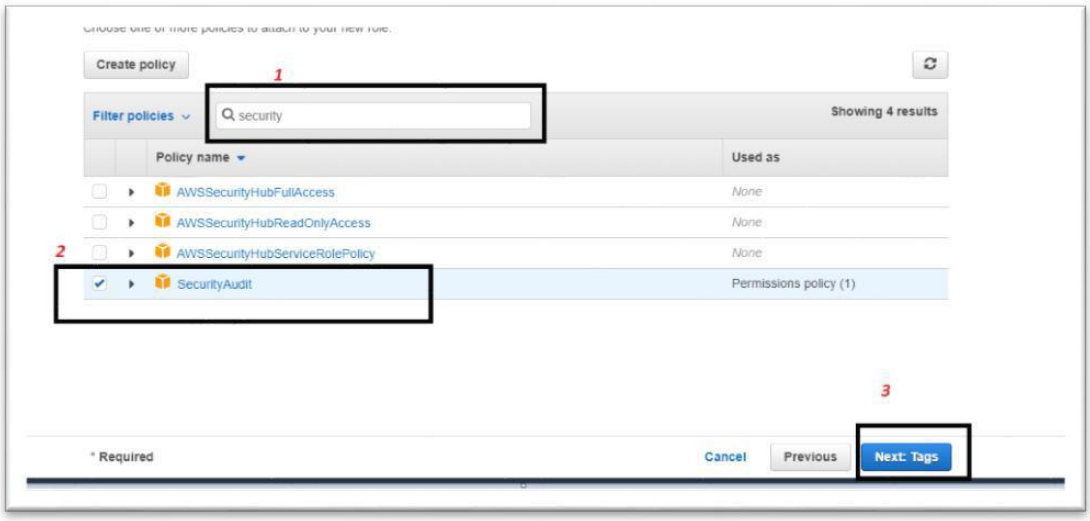


Custom Policy JSON:

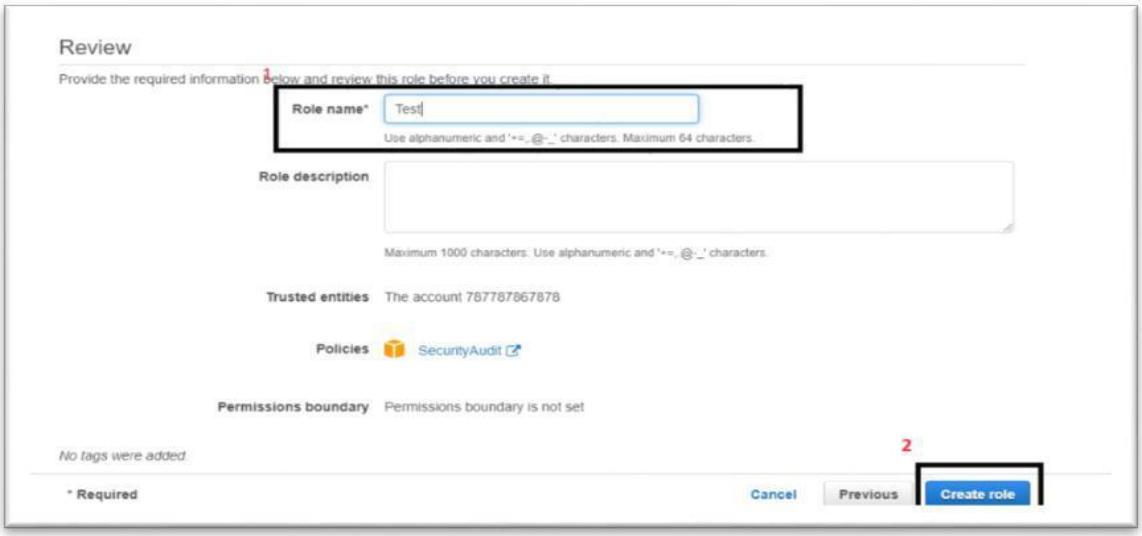
```
{
   {
    "Version": "2012-10-17",
     "Statement": [
       {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
         "lambda:GetFunction",
         "backup:GetBackupVaultAccessPolicy",
         "backup:ListBackupPlans",
         "kms:GetKeyRotationStatus",
         "glue:GetDataCatalogEncryptionSettings",
         "glue:GetSecurityConfigurations",
         "kms:GetKeyPolicy",
         "support:DescribeTrustedAdvisorChecks",
         "SNS:ListSubscriptions",
         "secretsmanager:DescribeSecret",
         "mq:ListBrokers",
         "servicequotas:GetServiceQuota",
         "cloudwatch:GetMetricStatistics",
         "SNS:GetSubscriptionAttributes",
         "backup:ListBackupVaults",
         "sts:AssumeRole",
         "ce:GetCostAndUsage",
         "ce:GetCostForecast",
         "ce:GetReservationCoverage",
         "ce:GetReservationPurchaseRecommendation",
         "ce:GetReservationUtilization",
         "ce:GetRightsizingRecommendation",
         "ce:GetSavingsPlansCoverage",
         "ce:GetSavingsPlansPurchaseRecommendation",
         "ce:GetSavingsPlansUtilization",
         "ce:GetSavingsPlansUtilizationDetails",
         "pricing:GetAttributeValues",
         "secretsmanager:GetSecretValue",
         "mq:DescribeBroker",
         "xray:GetEncryptionConfig",
         "athena:GetQueryExecution",
         "kms:DescribeKey",
         "support:DescribeSeverityLevels",
         "apigateway:GET",
         "es:ListElasticsearchVersions",
         "support:RefreshTrustedAdvisorCheck",
         "support:DescribeTrustedAdvisorCheckResult"
          ],
         "Resource": "*"
       }
     ]
  }
```

Note: This custom policy consists of read and list related permissions that is required for Access and API utilization which is further discussed.

11. Now under filters Search for "***Security Audit***" attach that policy (Select the check box)



12. Click on ***Next***
13. Add "***Tags***" if required
14. Provide the name of the "***Role***"
15. Click on "***Create Role***"



15. Now copy your ***Role-ARN*** Number
16. Redirect back to the Cloud Ensure application. Click on ***Next***
17. Paste the copied ***Role ARN*** Number
18. Click on ***Save***

ACCESS & API UTILIZATION

CloudEnsure is an agentless tool & has a secure key based access for interacting with AWS Accounts. Only Application level access is required with role-based access to fetch metadata about account infrastructure & AWS resources.

No User level access is required whatsoever. Basically, CloudEnsure uses Role-ARN to create a temporary security credentials that is used to access AWS resources and infrastructure for that role.

The steps mentioned in the Phase 2 emphasizes on how to create a role to delegate access to the resources that are in AWS accounts that you own. By setting up cross-account access in this way, there is no need to create individual IAM users in each account.

The two major steps for the role-based access include,

a. Creation of the role
b. Granting access to the role using the custom policies and security audit policies

Note:

The 'Role' should have these policies attached (Covered in Phase 2)

1. Security Audit Policy
2. Custom Policy (read and list permissions – available in the Configure AWS step in the tool)

CONTACT US

Reach out to below IDs for application support & queries

- support@cloudensure.io
- sales@cloudensure.io