

A background image showing two business professionals in a meeting. One person is pointing at a document held by the other. The image is overlaid with a dark teal filter.

CLOUDENSURE

**CLOUD GOVERNANCE
PLATFORM**

GCP Onboarding Guide

Table of Contents

1. Getting Started.....	3
2. Signup with Email Verification	4
3. Adding a GCP Account.....	7
4. Access and API Utilization.....	12
5. Contact us.....	12





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 a GCP account with CloudEnsure

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

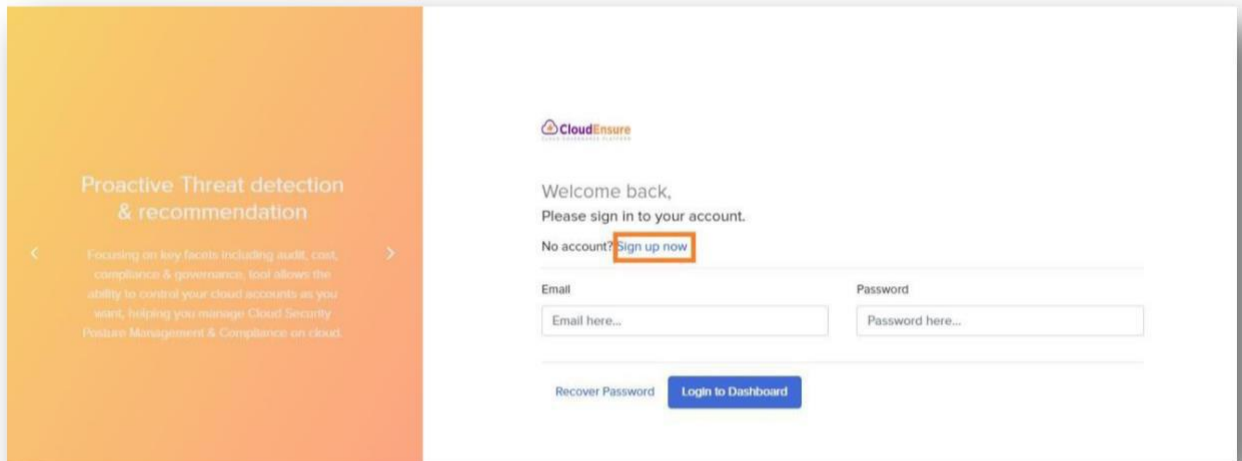
The below listed are pre-requisite details required to Signup & get started with the on-boarding process:

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.

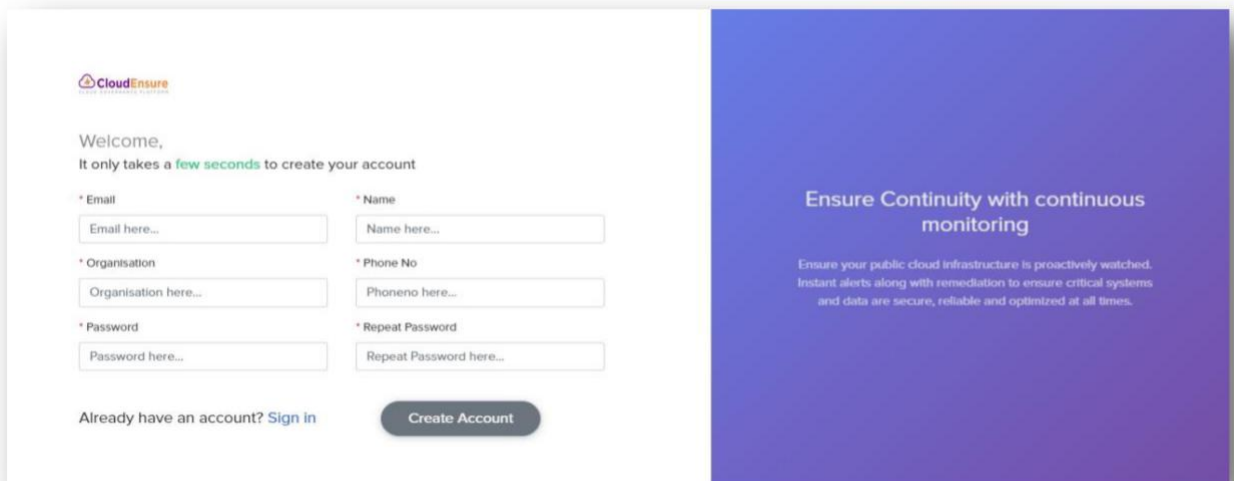


SIGNUP WITH EMAIL VERIFICATION

- 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 screenshot shows a 'User registration' screen with a white background and a blue sidebar on the right. The sidebar contains the text: 'Ensure Continuity with continuous monitoring' and 'Ensure your public cloud infrastructure is proactively watched. Instant alerts along with remediation to ensure critical systems and data are secure, reliable and optimized at all times.'

The main content area is divided into sections:

- Plans:** Shows 'Premium' selected with a checkmark.
- Hosting Type:** Shows 'SaaS'.
- CloudEnsure Product Modules:** A list of modules with checkmarks:
 - AWS Well Architected Review ✓
 - Compliance checks ✓
 - Cost Analytics Dashboard ✓
- Pricing:** A table showing pricing based on AWS account spend:

When you spend	Price
When you spend \$10,000 or less per AWS Account	\$99 per account per month*
When you spend more than \$10,000 per AWS Account	0.99% of your Monthly AWS Account Bill including any credits applied per account*

At the bottom, there are 'Previous' and 'Next' buttons.

- 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

The screenshot shows the 'User registration' screen with a white background and a blue sidebar on the right. The sidebar contains the same text as the previous screenshot: 'Ensure Continuity with continuous monitoring' and 'Ensure your public cloud infrastructure is proactively watched. Instant alerts along with remediation to ensure critical systems and data are secure, reliable and optimized at all times.'

The main content area displays a confirmation message:

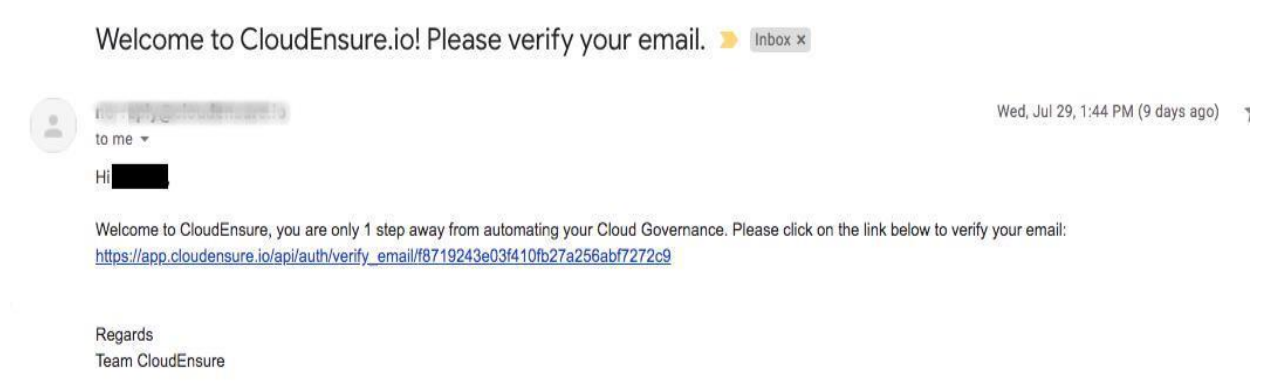
User registration

A Verification email has been sent to your registered email-id. Please click on the verification link to verify your account

Below the message is a 'Login Screen' button.



- 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

Thanks for verifying your email. Your account and subscription has been activated. You may now close this window.

- CloudEnsure Team

- 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 A GCP ACCOUNT

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

1. **GCP Account Name:** This is a reference name provided for ease of access & recognition for the account. This is a given name for each Project ID.
2. **GCP Credentials:** This is a JSON file which is a private key for the service account which is created from the GCP portal and acts as a credential for CloudEnsure in order to read the JSON and onboard a GCP Account.

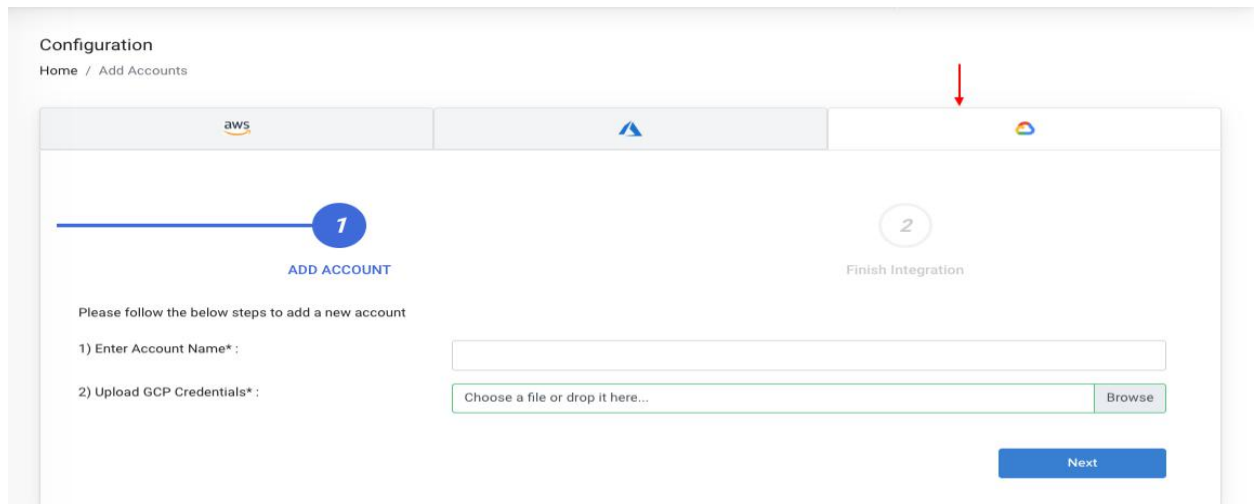
Phase 1: Add New Account (GCP)

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

The screenshot displays the CloudEnsure dashboard interface. On the left is a navigation sidebar with categories like 'AUDIT & GOVERNANCE', 'COST & SAVINGS', 'TRACK ACTIVITY', and 'UPCOMING FEATURES'. The main content area shows a 'Well Architected Audit' summary with four pillars: SECURITY (1535 issues), COST (60 issues), RELIABILITY (134 issues), and OPERATION (234 issues). Below this is a grid of service-specific issue counts, such as API GATEWAY (3 issues), DYNAMODB (12 issues), EC2 (118 issues), GLUE (49 issues), KMS (107 issues), S3 (393 issues), CONFIG, EBS, FIREHOSE, IAM (630 issues), LAMBDA (34 issues), and SNS (6 issues). Each service card includes a bar chart and a dropdown arrow. In the top right corner, a user profile dropdown menu is open, showing options like 'Accounts', 'Users', 'Third Party Integration', 'Policy Configuration', 'Submit Feature Request', 'Profile', and 'Logout'. The user is identified as 'aws Prod_AWS'.



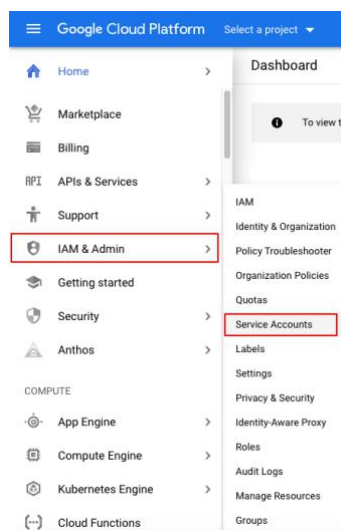
5. Click on top right drop down
6. Click on **Accounts**
7. Click on **“Add New Account”**
8. Select **“GCP”** tab



9. Enter **“Account Name”** & browse for **“GCP credentials”** which should be in JSON format and then click **“Next”**

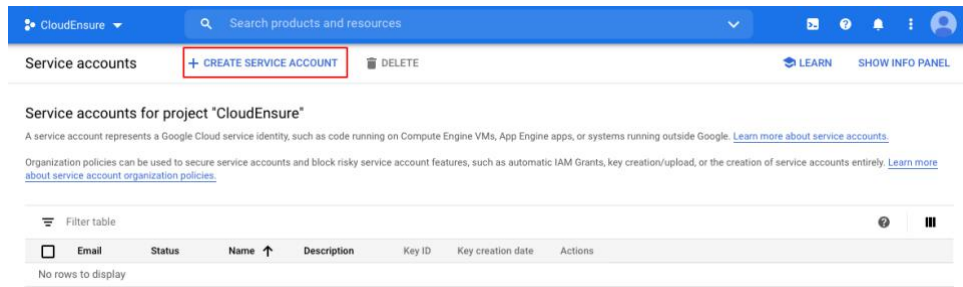
Note: If you don't have a Service Account Created, please follow the below steps

- Login to your GCP Console
- From the menu, select IAM & Admin and then click on Service Accounts





- Click Select a project, choose your project, and click Open.
- Now click on Create Service Account



- Enter a service account name (friendly display name), an optional description

Create service account

1 Service account details — 2 Grant this service account access to project (optional) — 3 Grant users access to this service account (optional)

Service account details

Service account name
Display name for this service account

Service account ID @cloudensure-290208.iam.gserviceaccount.com X C

Service account description
Describe what this service account will do

CREATE CANCEL

- Select a role Viewer and Security Reviewer to grant to the service account and then click Continue

Create service account

1 Service account details — 2 Grant this service account access to project (optional) — 3 Grant users access to this service account (optional)

Service account permissions (optional)

Grant this service account access to CloudEnsure so that it has permission to complete specific actions on the resources in your project. [Learn more](#)

Role: Viewer
Read access to all resources.

Condition: Add condition

+ ADD ANOTHER ROLE

CONTINUE CANCEL



- Now click on Done

Create service account

Service account details —
 Grant this service account access to project (optional) —
 Grant users access to this service account (optional)

Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role ?
Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role ?
Grant users the permission to administer this service account

- Service Account for the project is now successfully created, now in order to create the key, click the 3 dots in the Action column and select Create Key
- Now select JSON and click on CREATE to create a private key for the service account which in turn downloads the JSON key file which should be used to upload in the below section

Service accounts + CREATE SERVICE ACCOUNT [LEARN](#) [SHOW INFO PANEL](#)

Service accounts for project "CloudEnsure"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more about service accounts.](#)

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. [Learn more about service account organization policies.](#)

	Email	Status	Name ↑	Description	Key ID	Key creation date	Actions
<input checked="" type="checkbox"/>	ce-265@cloudensure-290208.iam.gserviceaccount.com	✔	CE	Integration	No keys		⋮
							Edit Disable <input type="button" value="Create key"/> Delete

Each Project under the GCP account has to be added as a new account along with the credentials into CloudEnsure



Phase 2: Creating a Storage Billing Bucket

- Open the Cloud Storage browser in the Google Cloud Console
- Click Create a bucket to open the bucket creation form
- Name your billing bucket and complete all other relevant information for this bucket;
Specify a Name
- Select a Default storage class for the bucket. The default storage class will be assigned by default to all objects uploaded to the bucket. Next, select a location where the bucket data will be permanently stored
- Click Done
- Once the bucket has been created, select Billing from the main menu. Select Billing Export, then select the File Export tab
- Enter the following for the billing bucket:
 - a. Bucket name
 - b. Report prefix - "gcp-report"
 - c. Format (JSON)



ACCESS & API UTILIZATION

CloudEnsure is an agentless tool & has a secure key based access for interacting with GCP Accounts. Only Viewer level access is required fetch metadata about account infrastructure & GCP resources.

The steps mentioned in the Phase 1 emphasizes on how to provide a viewer role to delegate access to the resources that are in GCP accounts that you own.

CONTACT US

Reach out to below IDs for application support & queries

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