CLOUDENSURE

CLOUD GOVERNANCE PLATFORM

Azure Onboarding Guide

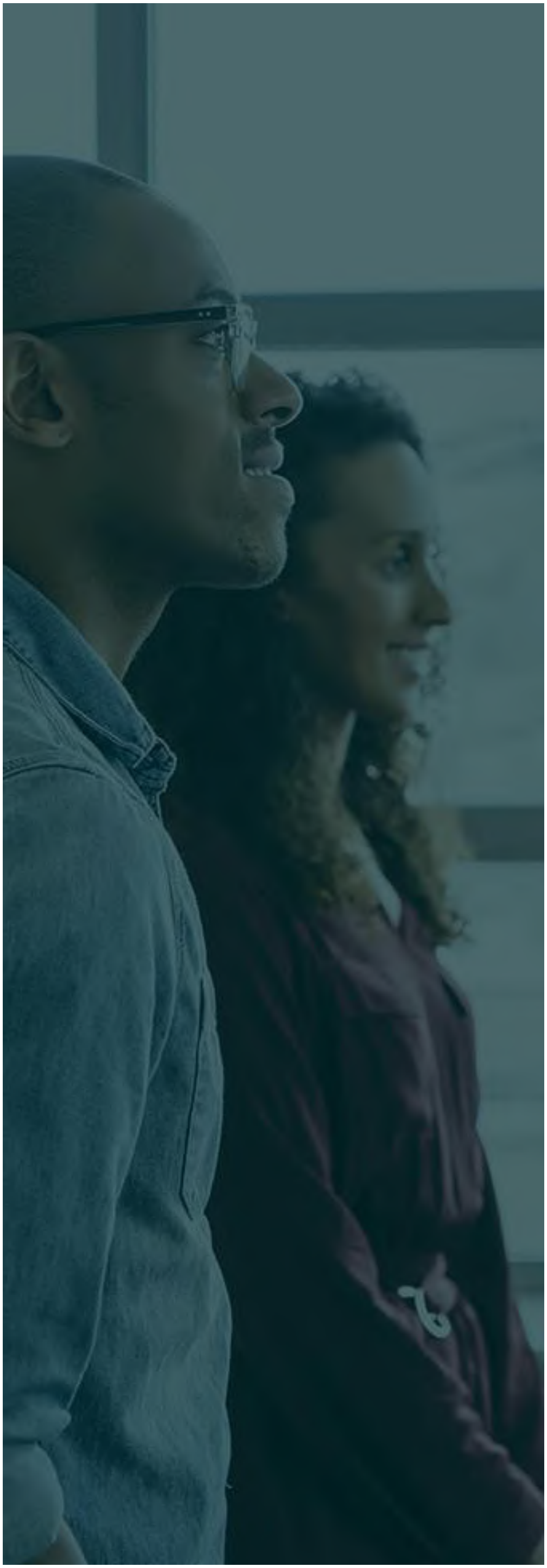


Table of Contents

GET 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 and the ability to drill down on various aspects based on need.

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
- Onboarding Azure Account

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/ distribution list accessible to desired personnel only. For example, CTO@xyz.com where xyz would be your org name/ID. 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:**

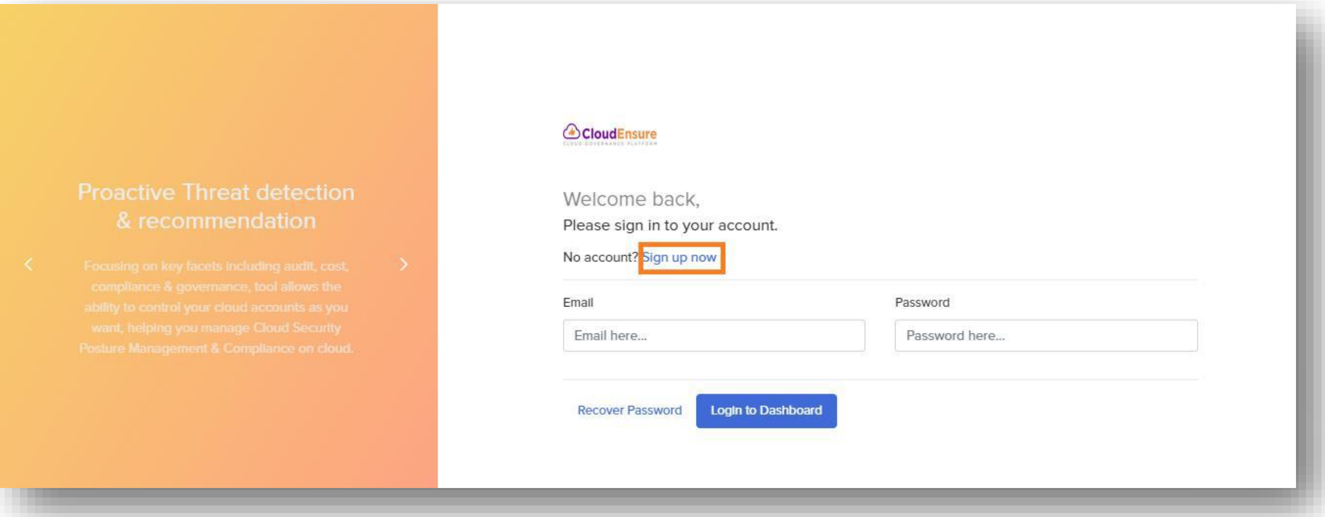
At this point we don't verify the registered phone number. However, we recommend this to be a service phone number. In upcoming feature releases:

1. We will send notifications for business critical findings.

2. We will use these numbers for OTP for MFA.

SIGNUP WITH EMAIL VERIFICATION

- Open https://app.cloudensure.io in your browser.
- Click on Signup as depicted below:



Proactive Threat detection & recommendation

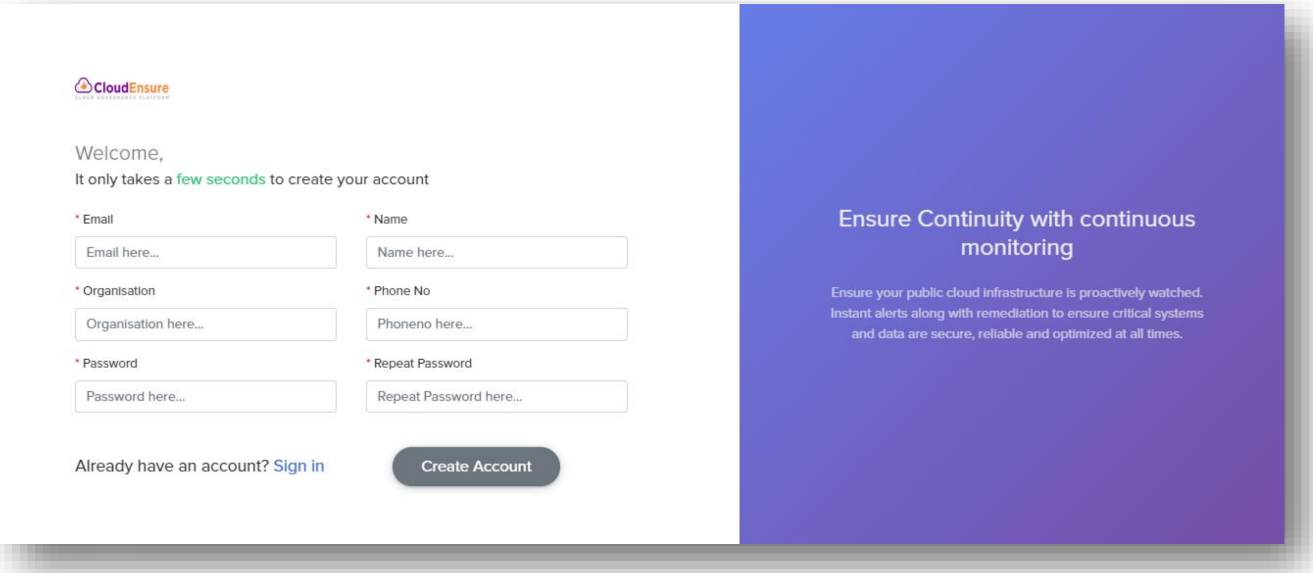
Focusing on key facets including audit, cost, compliance & governance, tool allows the ability to control your cloud accounts as you want, helping you manage Cloud Security Posture Management & Compliance on cloud.

Welcome back,

Please sign in to your account.

No account? Sign up now

- Enter the required details and click on **Next:**



Welcome,

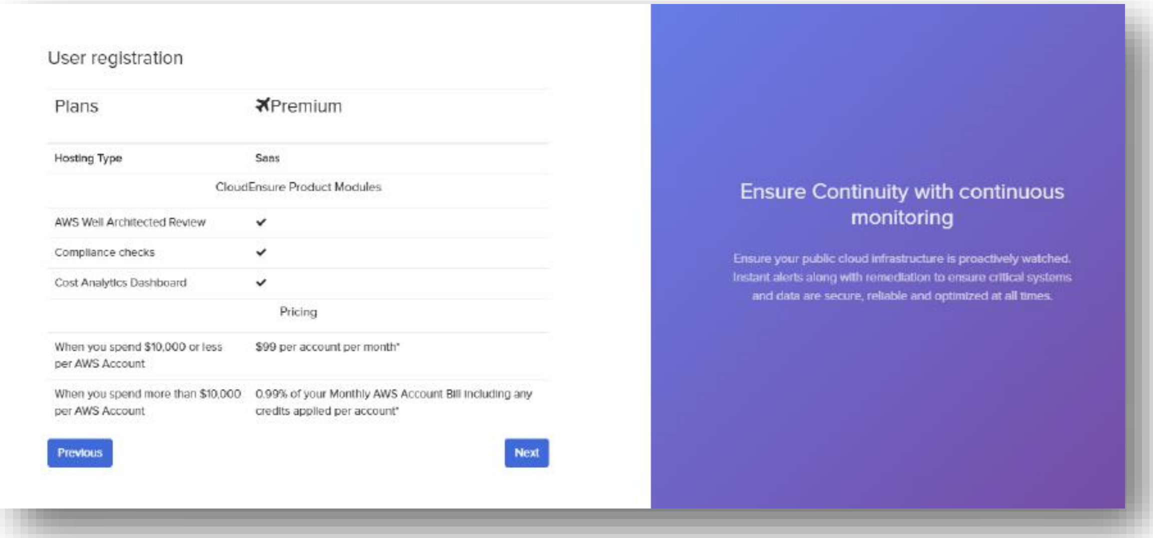
It only takes a few seconds to create your account

Already have an account? Sign in

Ensure Continuity with continuous monitoring

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 next screen will show the available & applicable plan details.
- Click on **Next**



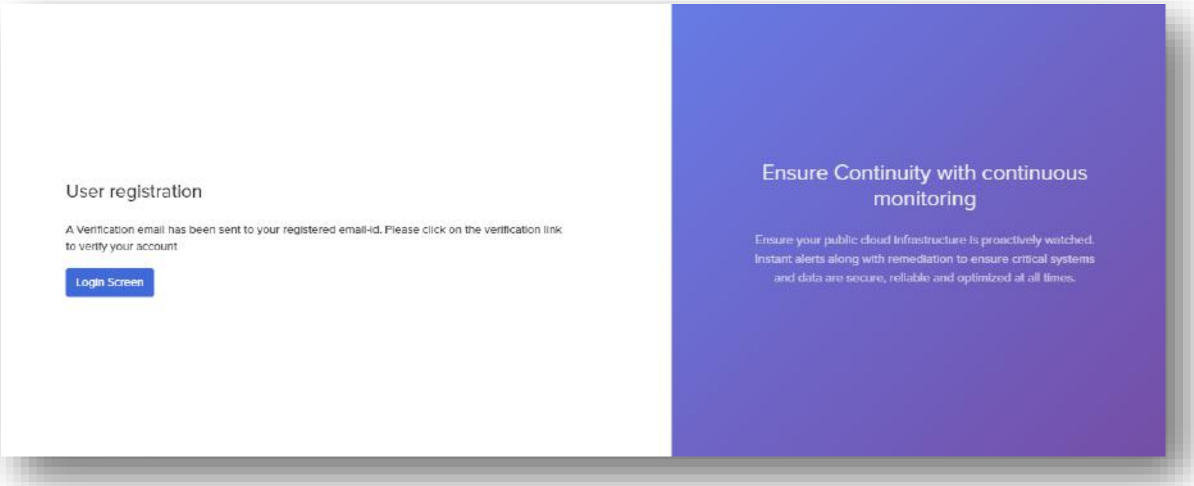
User registration

Plans	✈Premium
Hosting Type	Saas
CloudEnsure Product Modules	
AWS Well Architected Review	✓
Compliance checks	✓
Cost Analytics Dashboard	✓
Pricing	
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*

Ensure Continuity with continuous monitoring

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 final screen will display a confirmation message suggesting that a verification link has been sent to mail ID provided by you.



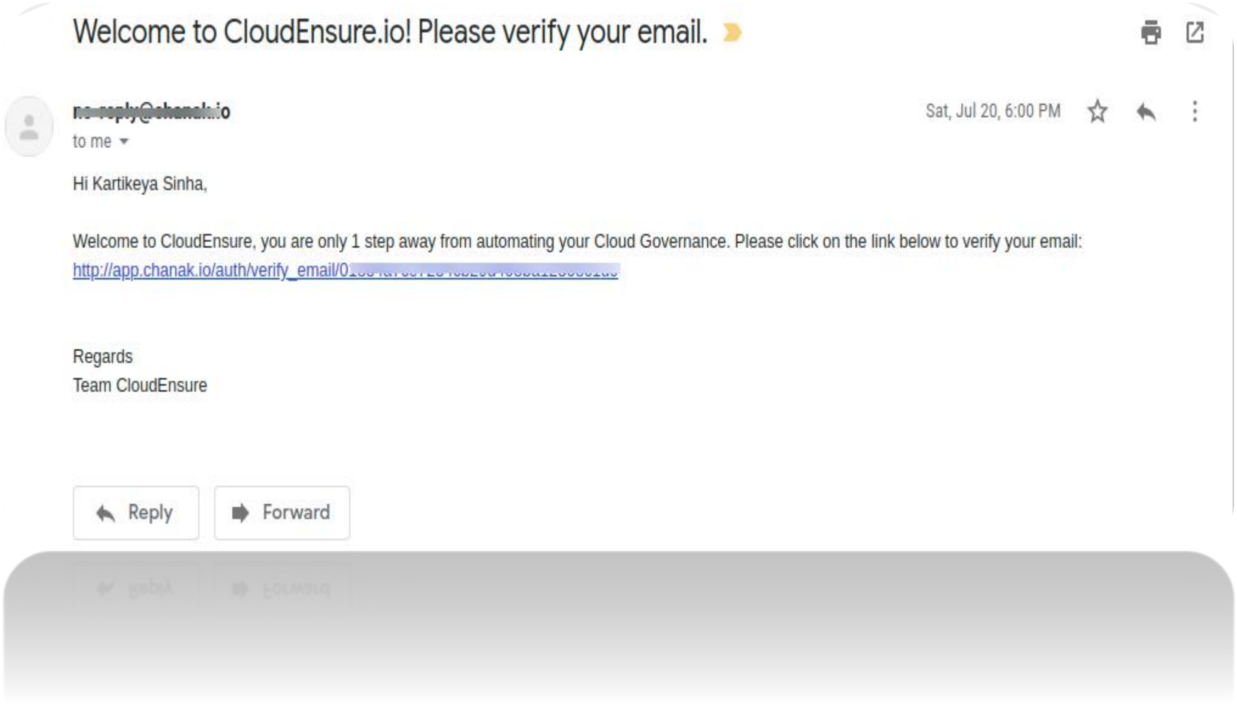
User registration

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

Ensure Continuity with continuous monitoring

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.

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



Welcome to CloudEnsure.io! Please verify your email.

[redacted]
to me

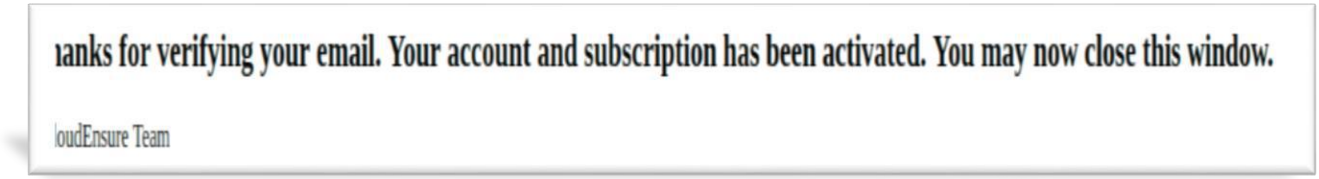
Sat, Jul 20, 6:00 PM

Hi Kartikeya Sinha,

Welcome to CloudEnsure, you are only 1 step away from automating your Cloud Governance. Please click on the link below to verify your email:
http://app.chanak.io/auth/verify_email/0[redacted]

Regards
Team CloudEnsure

- Upon clicking the link, you will get a confirmation message as depicted below:



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

loudEnsure Team

- This completes the signup and email verification process.
- You will now be able to login and add account in CloudEnsure application.

ADD ACCOUNT

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

1. **Reference Azure 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. **Domain Name:**

This is an Azure Active Directory domain-name, specific to the organization. This does not add any permissions for our (CloudEnsure Team) access. This is needed for authentication purposes only.

3. **Tenant Id:**

This is Azure Active directory ID. This is needed for authentication purposes.

4. **Application Id:**

This is a new service principle to be created for CloudEnsure connections only. This is a Unique identity created for CloudEnsure application in Azure AD.

5. **Secret Key:**

This is a secret key associated with the service principle to be created for CloudEnsure app in specific. The secret key provides the expiry configuration option as (1 year, 2 years, Never). This can be set as per organization norms and can be renewed after the desired period (recommended option is “1 Year”)

Note: Both application ID and Secret key should be available **only** to the person onboarding the account to CloudEnsure. On CloudEnsure side Secret-key is encrypted by application using **AES 256-bit** format before storing in DB. Only Azure Admin can remove the key or the application as and when desired to revoke access for CloudEnsure.

Refer the section “**Register Application**” for registering the application in your azure account & obtaining the above details

Below listed steps to be followed to on-board an Azure account on CloudEnsure Application:

Phase 1

1. Open **https://app.cloudensure.io**

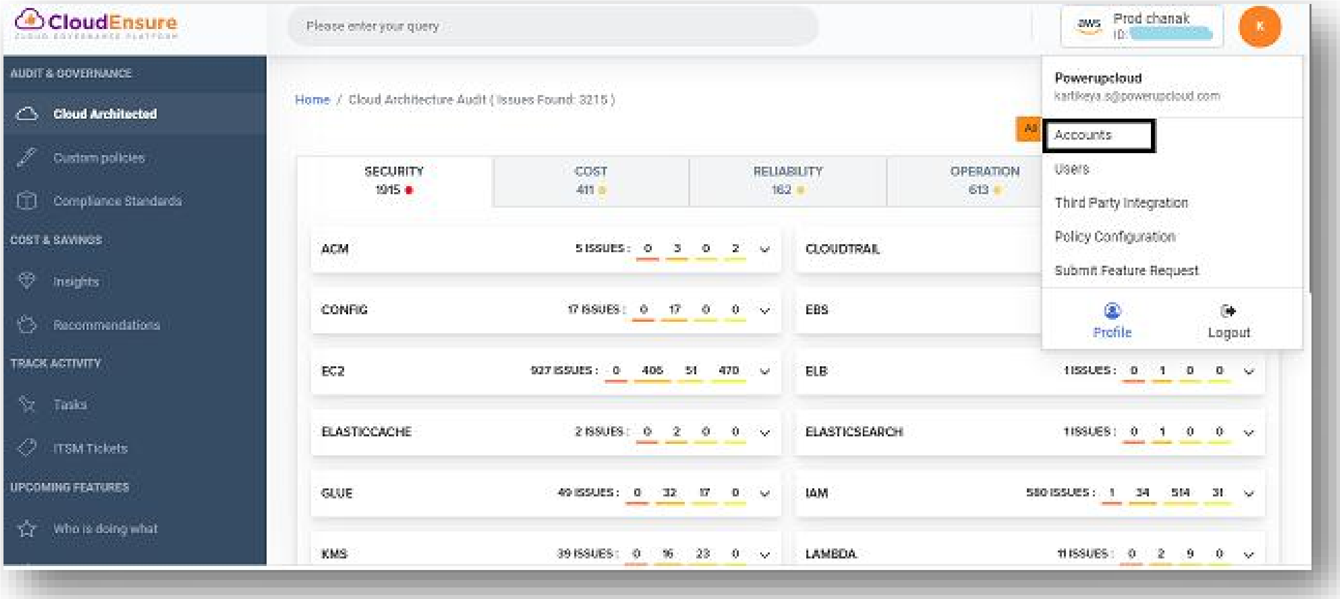
2. Enter **Username** with valid credentials. (Email ID)

3. Enter **Password** with valid credentials. (Minimum eight Characters)

4. Click on Login, you will be taken to the CloudEnsure landing page.

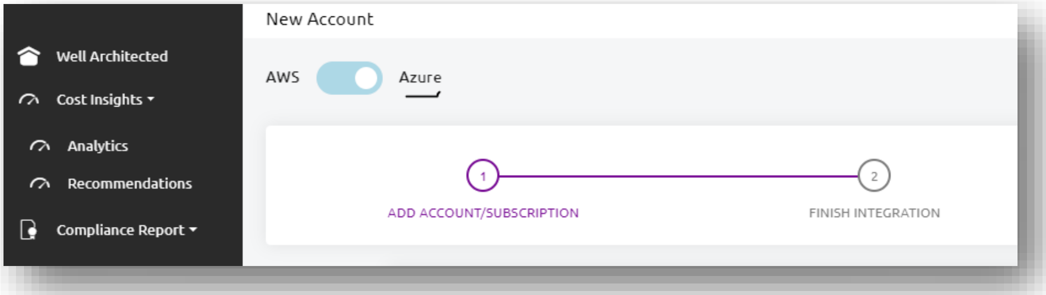
5. Click on top right drop down.

6. Click on **Accounts**:

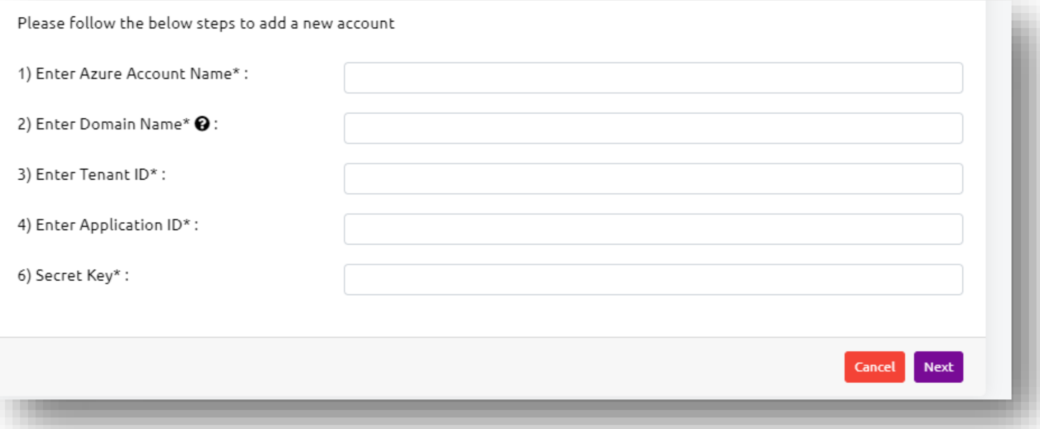


7. Click on the “**Add New Account**” button on the next page.

8. Click on the **Toggle** button to choose **Azure Account**



9. Follow the steps shown in the app or Refer "Register Application" section for detailed steps
10. Enter the required details:
    1. Azure account name
    2. Domain Name
    3. Tenant ID
    4. Application ID
    5. Secret key


Please follow the below steps to add a new account

1) Enter Azure Account Name* :

2) Enter Domain Name* ❓ :

3) Enter Tenant ID* :

4) Enter Application ID* :

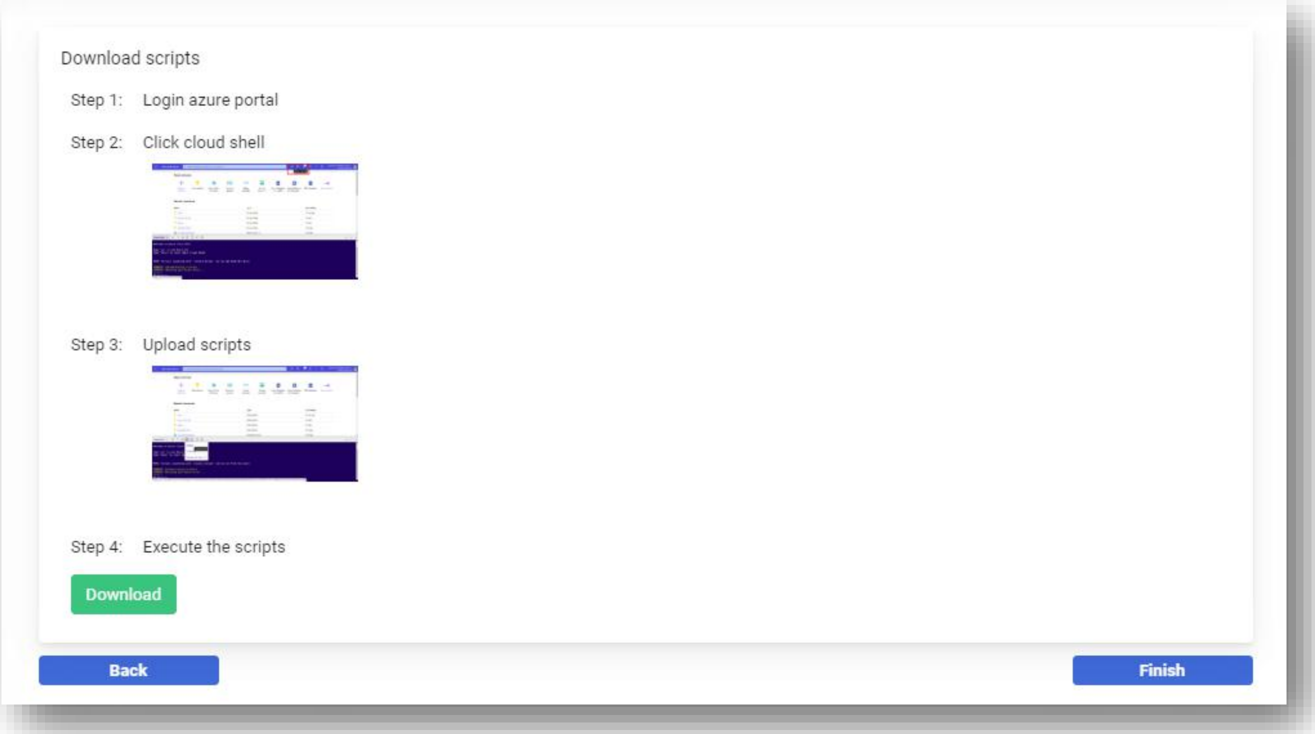
6) Secret Key* :

11. Click on **Next.**

Phase 2,

You would require logging into the Azure Portal and perform the below listed steps to complete the registration & onboarding process.

1. Click on cloud shell.
2. Download the scripts from the CloudEnsure portal
3. Go to “PowerShell →Upload” section & upload the scripts
4. Execute the scripts
5. Click on **Finish** button, your account is on-boarded



Download scripts

Step 1: Login azure portal

Step 2: Click cloud shell

Step 3: Upload scripts

Step 4: Execute the scripts

Note: The script assigns the App created for CloudEnsure to all the subscriptions in the Azure account. To assign App to only specific subscriptions refer to the “*Register Application*” section in the document.

Below listed is the Script to be executed: Replace **Tenant ID** and **App credentials** in the script.

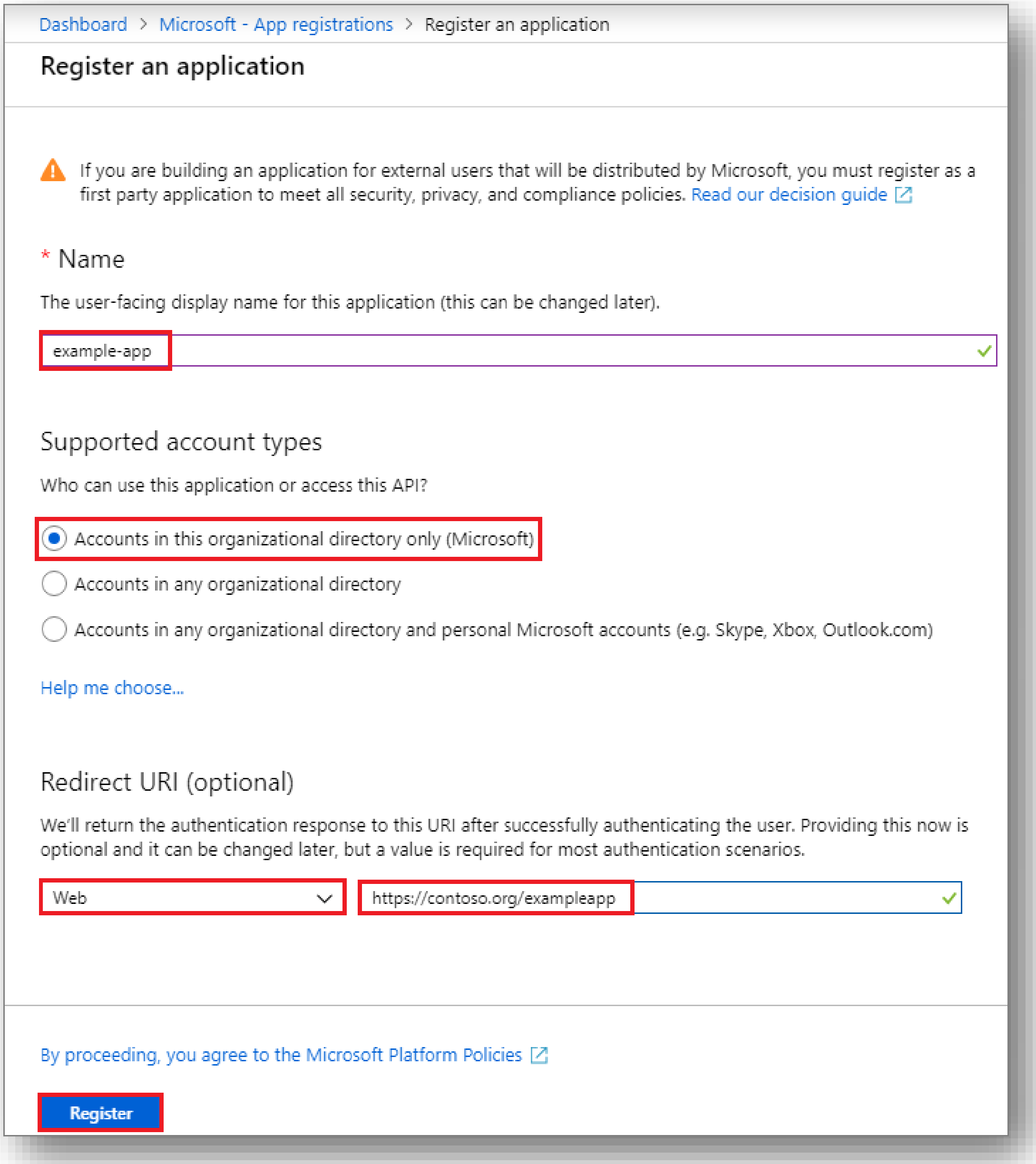
```
$listOfSubscriptions = Get-AzureRmSubscription -TenantId <TenantId>
$AppId = ""
$appKey = "<app key>"
$allApps = Get-AzureRmADServicePrincipal
Foreach ($app in $allApps)
{
    if($app.ApplicationId -eq $appKey)
    {
        $AppId = $app.Id.ToString()
        break
    }
}
if($AppId -eq ''){
    '~~~~~~~~~~~~~~~~~Specified application not found~~~~~~~~~~~~~~~~~'
}Else{
        $listOfSubscriptionsAlreadyAdded = New-Object System.Collections.ArrayList
        Foreach ($subscription in $listOfSubscriptions)
        {
            if($subscription.State -eq 'Enabled' -and !$listOfSubscriptionsAlreadyAdded.Contains($subscription.Id)){
                '~~~~~~~~~~~~~~~ assigning Reader role at ' + $subscription + ' ~~~~~~~~~~'
                New-AzureRmRoleAssignment -ObjectId $AppId -RoleDefinitionName "Reader" -Scope
/subscriptions/$subscription
                '~~~~~~~~~ done assigning Reader role at ' + $subscription + ' ~~~~~~~~~~'


            }
        }
        '~~~~~~~~~~~~~~You have successfully completed subscriptions configuration~~~~~~~~~~~~~~'
}
```

REGISTER APPLICATION

This section will guide you to access all relevant details required to Onboard Azure account by helping you register the CloudEnsure application in your azure account portal.

- Sign in to your Azure Account through the Azure portal
- Select **Azure Active Directory**
- Select **App registrations**
- Select **New registration**
- Name the application
- Select a supported account type, which determines who can use the application
- Under **Redirect URI**, select **Web** for the type of application you want to create
- Enter the URL where the access token is sent to you. You can't create credentials for a Native application. You can't use that type for an automated application. After setting the values
- Select **Register**.



Dashboard > Microsoft - App registrations > Register an application

Register an application

⚠ If you are building an application for external users that will be distributed by Microsoft, you must register as a first party application to meet all security, privacy, and compliance policies. Read our decision guide

* Name

The user-facing display name for this application (this can be changed later).

example-app ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Microsoft)

○ Accounts in any organizational directory

○ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Help me choose...

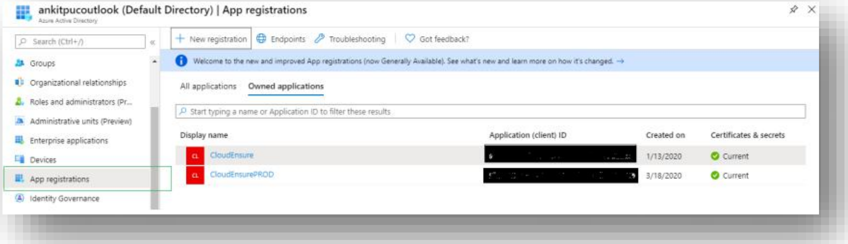
Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | https://contoso.org/exampleapp ✓

By proceeding, you agree to the Microsoft Platform Policies

- If you have already registered click on the registered app name.



ankitpucoutlook (Default Directory) | App registrations

Azure Active Directory

Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed. →

All applications | Owned applications

Start typing a name or Application ID to filter these results

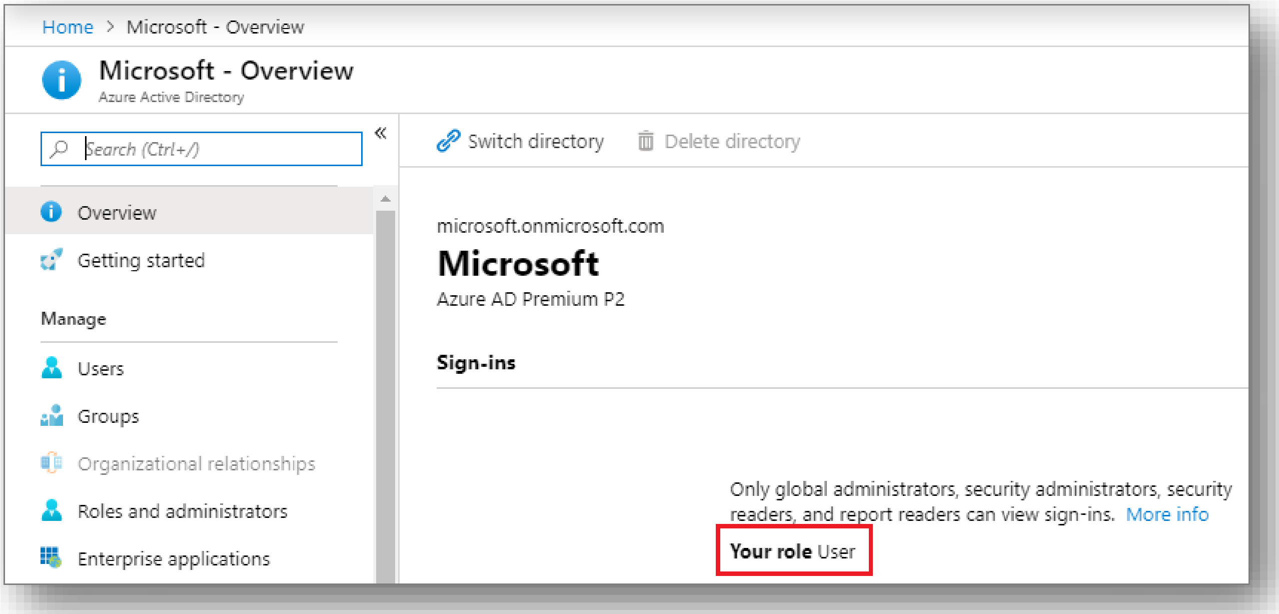
Display name	Application (client) ID	Created on	Certificates & secrets
CL CloudEnsure	[redacted]	1/13/2020	✓ Current
CL CloudEnsurePROD	[redacted]	3/18/2020	✓ Current

Permissions for registering an app

You must have sufficient permissions to register an application with your Azure AD tenant, and assign a role to the application in your Azure subscription.

Check Azure AD permissions

- Select **Azure Active Directory**.
- Note your role. If you have the **User** role, you must make sure that non-administrators can register applications.



Home > Microsoft - Overview

Microsoft - Overview

Azure Active Directory

microsoft.onmicrosoft.com

Microsoft

Azure AD Premium P2

Sign-ins

Only global administrators, security administrators, security readers, and report readers can view sign-ins. More info

Your role User

- In the left pane, select **User settings**.
- Check the **App registrations** setting. This value can only be set by an administrator. If set to **Yes**, any user in the Azure AD tenant can register an app.

Azure subscription permissions

In your Azure subscription, your account must have “`Microsoft.Authorization/*/Write`” access to assign a role to an AD app.

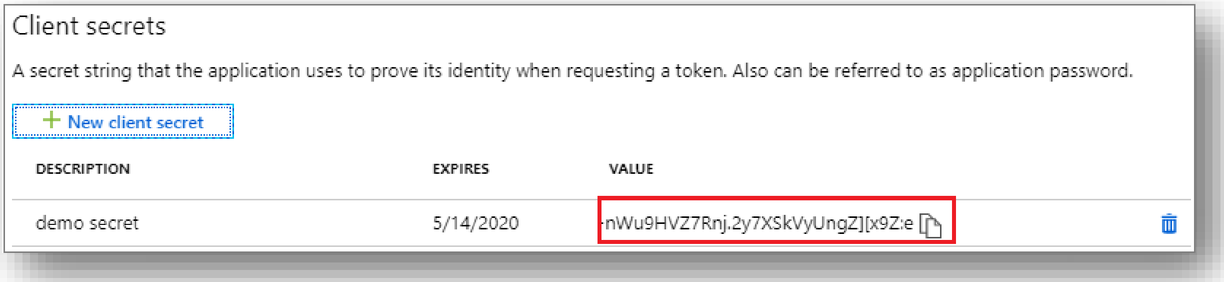
This action is granted through the any of the below roles

- Owner role
- User Access Administrator role

Minimum role permissions required are that for a Contributor role to enable remediation’s from the tool.

Certifications & Secrets

- Select **Azure Active Directory**.
- From **App registrations** in Azure AD, select your application.
- Select **Certificates & secrets**.
- Select **Client secrets -> New client secret**.
- Provide a description of the secret, and a duration. When done, select **Add**.
- After saving the client secret, the value of the client secret is displayed.
- Copy this value because you won't be able to retrieve the key later (or)
- You will provide the key value with the application ID to sign in as the application. Store the key value where your application can retrieve it.



Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

DESCRIPTION	EXPIRES	VALUE
demo secret	5/14/2020	-nWu9HVZ7Rnj.2y7XSkVyUngZ][x9Z:e

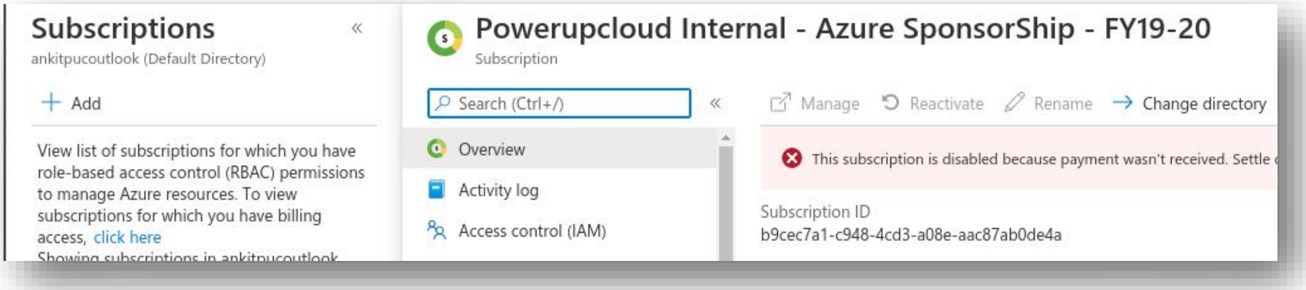
- Click on the registered app name in the **app registration** under **Active Directory**.

Assign App to Subscriptions

The App registered should be assigned to one or more subscriptions. To do the same follow the below steps.

To Assign Subscription by manual process:

1. Click on the Subscriptions name in the azure portal.



Subscriptions

ankitpucoutlook (Default Directory)

View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have billing access, click here

Showing subscriptions in ankitpucoutlook

Powerupcloud Internal - Azure SponsorShip - FY19-20

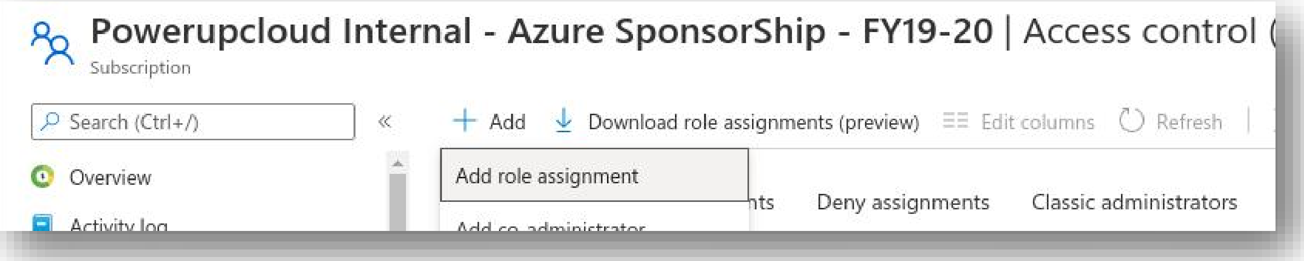
Subscription

This subscription is disabled because payment wasn't received. Settle

Subscription ID
b9cec7a1-c948-4cd3-a08e-aac87ab0de4a

2. Select the Access Control (IAM) section in the left pane.

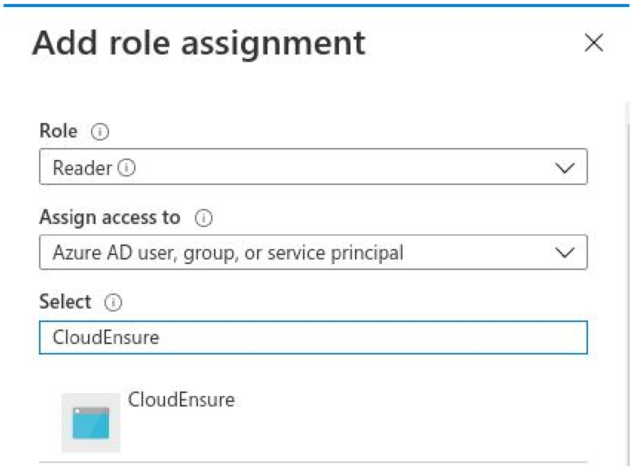
3. Click on Add - > Role Assignment.



Powerupcloud Internal - Azure SponsorShip - FY19-20 | Access control (

Subscription

4. Select Role as Reader and Assign Access to Option as Azure AD user, group or service principal. Select the App registered for CloudEnsure and click on Save.



Add role assignment

Role: Reader

Assign access to: Azure AD user, group, or service principal

Select: CloudEnsure

CloudEnsure

5. Repeat the steps to assign App to multiple subscriptions.

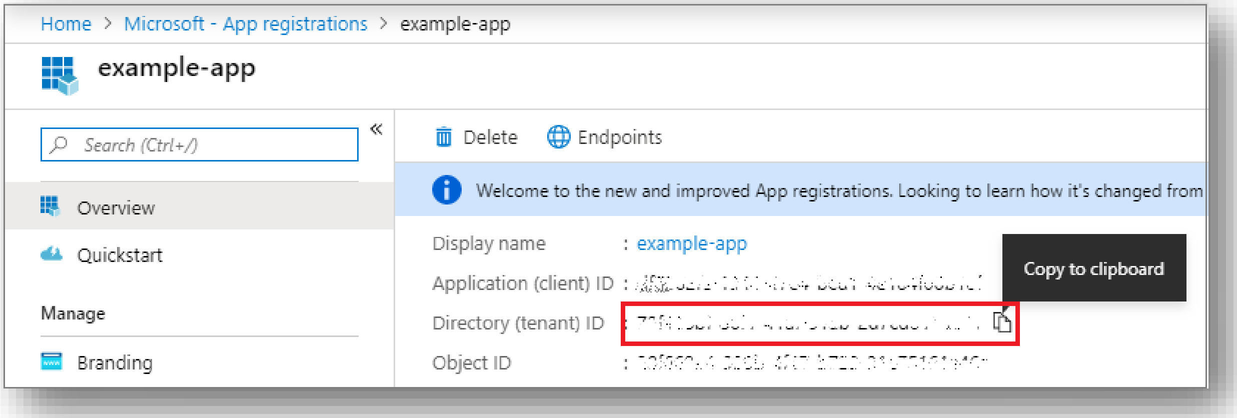
Assign App to Subscription using shell script:

- Download the script from the CloudEnsure portal and execute the script to assign the app to all the subscriptions.

Tenant ID & Application ID

To get the Tenant ID and Application ID values, use the following steps:

1. From **App registrations** in Azure AD, select your application.
2. Copy the Directory (tenant) ID and store it in your application code.



Welcome to the new and improved App registrations. Looking to learn how it's changed from

Display name : example-app

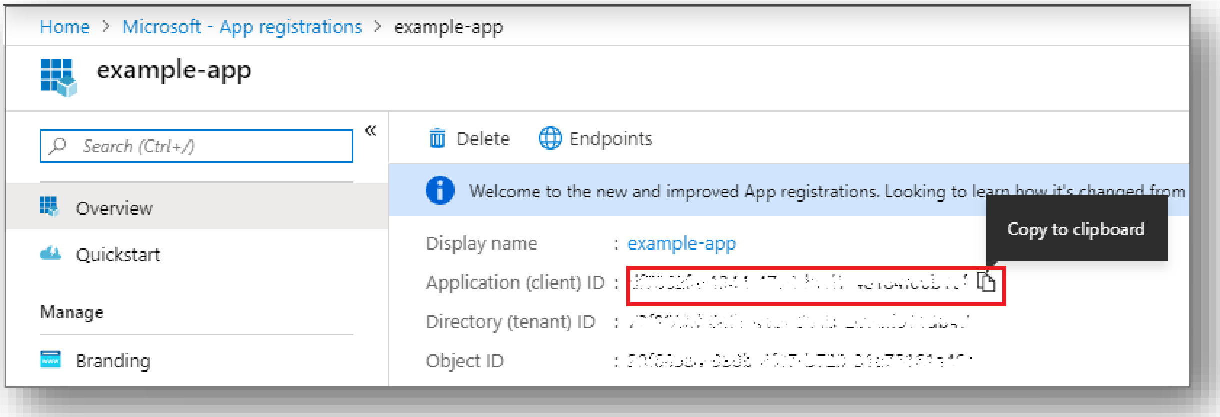
Application (client) ID : [redacted]

Directory (tenant) ID : [redacted]

Object ID : [redacted]

Note: The directory (tenant) ID can also be found in the default directory overview page.

3. Copy the **Application ID**



Home > Microsoft - App registrations > example-app

example-app

Search (Ctrl+/)

Overview

Quickstart

Manage

Branding

Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn how it's changed from

Copy to clipboard

Display name : example-app

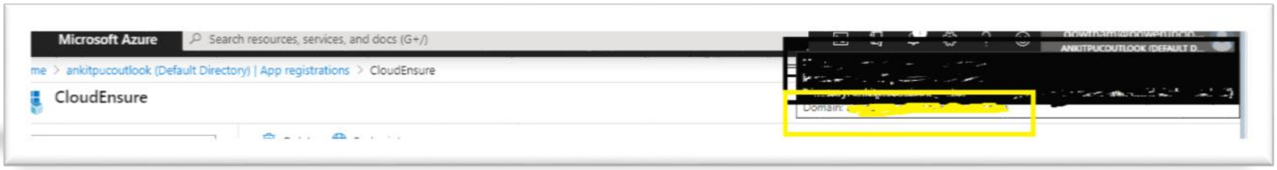
Application (client) ID : [redacted]

Directory (tenant) ID : [redacted]

Object ID : [redacted]

Domain Name

Select the Domain Name from the profile section. Place the cursor on the profile as depicted in the below image.



Microsoft Azure

Search resources, services, and docs (G+/)

me > ankitpucoutlook (Default Directory) | App registrations > CloudEnsure

CloudEnsure

[redacted]

ANKITPUCOUTLOOK (DEFAULT D...

Domain: [redacted]

Post following these steps you will have all the required information for adding an account in CloudEnsure Application.

1. Domain Name
2. Tenant ID
3. Application ID
4. Secret Key

PowerShell Script:

CloudEnsure will share a script that will assign infra-level(CMDB-level), read-only (Azure - ‘Reader’) permissions to all the subscriptions in the account.

ACCESS & API UTILIZATION

CloudEnsure is an agentless tool & has a secure key based access for interacting with Azure Accounts. Only Application level access is required with reader access to fetch metadata about account infrastructure & resources. No User level access is required whatsoever.

CloudEnsure does allow for restricted subscription access ensuring information of only the required subscriptions are accessed by the tool & other subscriptions are not used or called upon.

The tool utilizes & consumes below listed API's on Azure:

1. Azure Active Directory Graph API
2. Azure Rest APIs
3. Azure Resource Usage API
4. Azure Resource RateCard API

The list of API’s consumed by CloudEnsure platform keeps evolving as the product is continuously updated based on threat trends and industry best practices. However, we don’t pro-actively send notification to customers for updated API calls. Also, the new API’s are within the scope of above acquired permissions.

On-Demand, CloudEnsure will be able to provide a list of all Read API calls in use. On a two days-notice, we can share all the APIs being used at any point in time.

For the Remediation’s to work & only if the client has opted for one-click remediation’s below listed permission will have to be enabled.

- Azure Active Directory Graph API like Azure Rest API to have write access.

CONTACT US

Reach out to below IDs for support & queries:

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