

Display name

:

Portals-ContraMind

Home > Portals-ContraMind

Portals-ContraMind | Branding & properties

Search

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Name *

Portals-ContraMind

Logo

None provided

Upload new logo

Select a file

Home page URL

e.g. https://example.com

Terms of service URL

e.g. https://example.com/termsofservice

Privacy statement URL

e.g. https://example.com/privacystatement

Service management reference

Internal notes

Add information relevant to the management of this application.

Publisher domain

ayman.ws

Update domain

This domain will appear on the application's consent screen.

Learn more about publisher domain

Publisher verification

Application (client) ID: ebe21e1e-5db3-460d-9b22-417687ce8a87

Object ID: e68250f3-f721-498f-a1d5-a42f661c14fd

Directory (tenant) ID: 2af26d74-7a26-4d6b-899c-ff09267d9b46

Supported account types : [Multiple organizations](#)

Web

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

<https://8103ac6b-c2ec-453b-b704-b562d25d30d7-00-1ntd620e4kt76.spock.replit.dev/api/auth/microsoft/callback>

Portals-Contramind | Authentication

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

[+](#) Add a platform

Web

Redirect URIs

Quickstart

Docs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

https://8103ac6b-c2ec-453b-b704-b562d25d30d7-00-1ntd620e4kt76.spock.replit.dev/api/auth/micros

Add URI

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://example.com/logout

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens](#).

Select the tokens you would like to be issued by the authorization endpoint:



- ☐ Access tokens (used for implicit flows)
- ☐ ID tokens (used for implicit and hybrid flows)


Supported account types

Who can use this application or access this API?

- ☐ Accounts in this organizational directory only (AYMAN HAMDAN CONSULTANCY WLL only - Single tenant)
- ☒ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

[Help me decide...](#)

 Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#) 

 Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. [Add MPN ID to verify publisher](#) 

Advanced settings

Allow public client flows

Enable the following mobile and desktop flows:

Yes

No

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#) 
- No keyboard (Device Code Flow) [Learn more](#) 
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#) 

App instance property lock

Configure the application instance modification lock. [Learn more](#) 

[Configure](#)

Save

Discard

Microsoft Azure

Home > Portals-ContraMind

Portals-ContraMind | Certificates & secrets

Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting

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

Copilot

Got feedback?

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (1)

Client secrets (0)

Federated credentials (0)

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Description	Start date	Expires	Certificate ID
EDBDEE544E079B346BA36CDABE22F...	CN=4c5d7cf8-9f44-42e9-842f-78828...	08/03/2025	07/03/2026	f7193f8c-6953-4494-... <div></div>

Add or remove favorites by pressing Cmd+Shift+F

Application ID URI <api://2af26d74-7a26-4d6b-899c-ff09267d9b46/74e946d7-ee04-475c-999a-0d245ce490c1>:

Scopes : api://2af26d74-7a26-4d6b-899c-ff09267d9b46/74e946d7-ee04-475c-999a-0d245ce490c1/user_impersonation

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Portals-ContraMind

Portals-ContraMind | Expose an API

Search

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Application ID URI :

api://2af26d74-7a26-4d6b-899c-ff09267d9b46/74e9...

Edit

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app roles assignable to application type. [Go to App roles.](#)

+ Add a scope

Scopes	Copied	Admins and users	Admin consent display ...	User consent display na...	State
api://2af26d74-7a26-4d6b-899c-ff09267d9b46/74e94...		Access Portals-ContraMind	Access Portals-ContraMind	Access Portals-ContraMind	Enabled

Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

+ Add a client application

Client Id	Scopes
No client applications have been authorized	

Managed application in local directory [Portals-ContraMind](#)

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home >

Portals-ContraMind | Overview

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Security

Activity

Troubleshooting + Support

Properties

P

Name

Portals-ContraMind

Application ID

ebe21e1e-5db3-460d-9b22-...

Object ID

0668c00e-b4cd-4fc7-8ad3-f0...

Getting Started

1. Assign users and groups

Provide specific users and groups access to the applications

[Assign users and groups](#)

2. Provision User Accounts

You'll need to create user accounts in the application

[Learn more](#)

3. Conditional Access

Secure access to this application customizable access policy.

[Create a policy](#)

What's New

Sign in charts have moved!

The new Insights view shows sign in info along with other useful application data. [View insights](#)

Delete Application has moved to Properties

You can now delete your application from the Properties page. [View properties](#)

Getting started has moved to Overview

The Getting Started page has been replaced by the steps above