Configure ISE 3.0 REST ID with Azure Active Directory

Contents

Introduction

This document describes how to configure and troubleshoot Identity Services Engine (ISE) 3.0 integration with Microsoft (MS) Azure Active Directory (AD) implemented through Representational State Transfer (REST) Identity (ID) service with the help of Resource Owner Password Credentials (ROPC).

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of these topics:

- ISE
- MS Azure AD
- Understanding of ROPC protocol implementation and limitations; link

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ISE Version 3.0
- MS Azure AD
- WS-C3850-24P with s/w 16.9.2

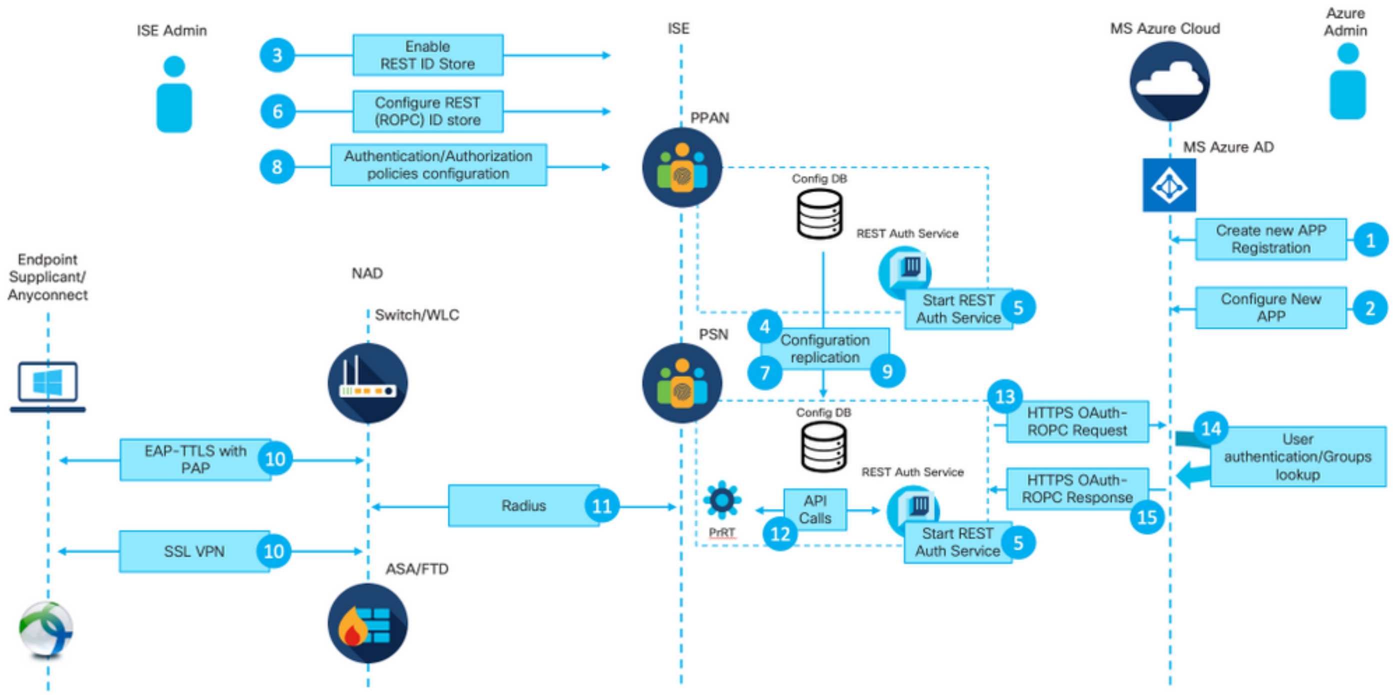
- ASAv with 9.10 (1)
- Windows 10.0.18363

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

ISE REST ID functionality is based on the new service introduced in ISE 3.0 - REST Auth Service. This service is responsible for communication with Azure AD over Open Authorization (OAuth) ROPC exchanges in order to perform user authentication and group retrieval. REST Auth Service is disabled by default, and after the administrator enables it, it runs on all ISE nodes in the deployment. Since REST Auth Service communication with the cloud happens when at the time of the user authentication, any delays on the path might bring additional latency into Authentication/Authorization flow. This latency is outside of ISE control, and any implementation of REST Auth has to be carefully planned and tested to avoid impact to other ISE services.

High-Level Flow Overview



1. Azure cloud administrator creates a new application (App) Registration. Details of this App are later used on ISE in order to establish a connection with the Azure AD.

2. Azure cloud admin has to configure the App with:

Figure 1.

- Create a Client Secret
- Enable ROPC
- Add group claims
- Define Application Programming Interface (API) permissions

3. ISE admin turns on the REST Auth Service. It needs to be done before any other action can be

executed.

4. Changes are written into the configuration database and replicated across the entire ISE deployment.

5. REST Auth Service starts on all the nodes.

6. ISE Admin configures the REST ID store with details from Step 2.

7. Changes are written into the configuration database and replicated across the entire ISE deployment.

8. ISE admin creates a new Identity store sequence or modifies the one that already exists and configures authentication/authorization policies.

9. Changes are written into the configuration database and replicated across the entire ISE deployment.

10. Endpoint initiates authentication. As per ROPC protocol specification, user password has to be provided to the Microsoft identity platform in a clear text over an encrypted HTTP connection; due to this fact, the only available authentications options supported by ISE as of now are:

- Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) with Password Authentication Protocol (PAP) as the inner method
- AnyConnect SSL VPN authentication with PAP

11. Exchange with ISE Policy Service Node (PSN) over Radius.

12. Process Runtime (PrRT) sends a request to REST ID service with user details (Username/Password) over internal API.

13. REST ID service sends OAuth ROPC request to Azure AD over HyperText Transfer Protocol Secure (HTTPS).

14. Azure AD performs user authentication and fetches user groups.

15. Authentication/Authorization result returned to ISE.

After point 15, the authentication result and fetched groups returned to PrRT, which involves policy evaluation flow and assign final Authentication/Authorization result. Either Access-Accept with attributes from authorization profile or Access-Reject returned to Network Access Device (NAD).

Configure Azure AD for Integration

1. Locate AppRegistration Service as shown in the image.

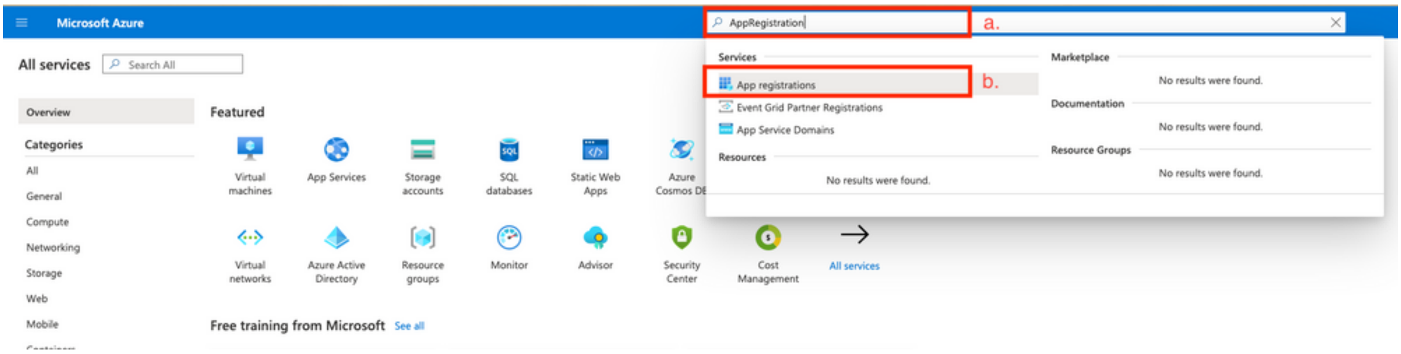
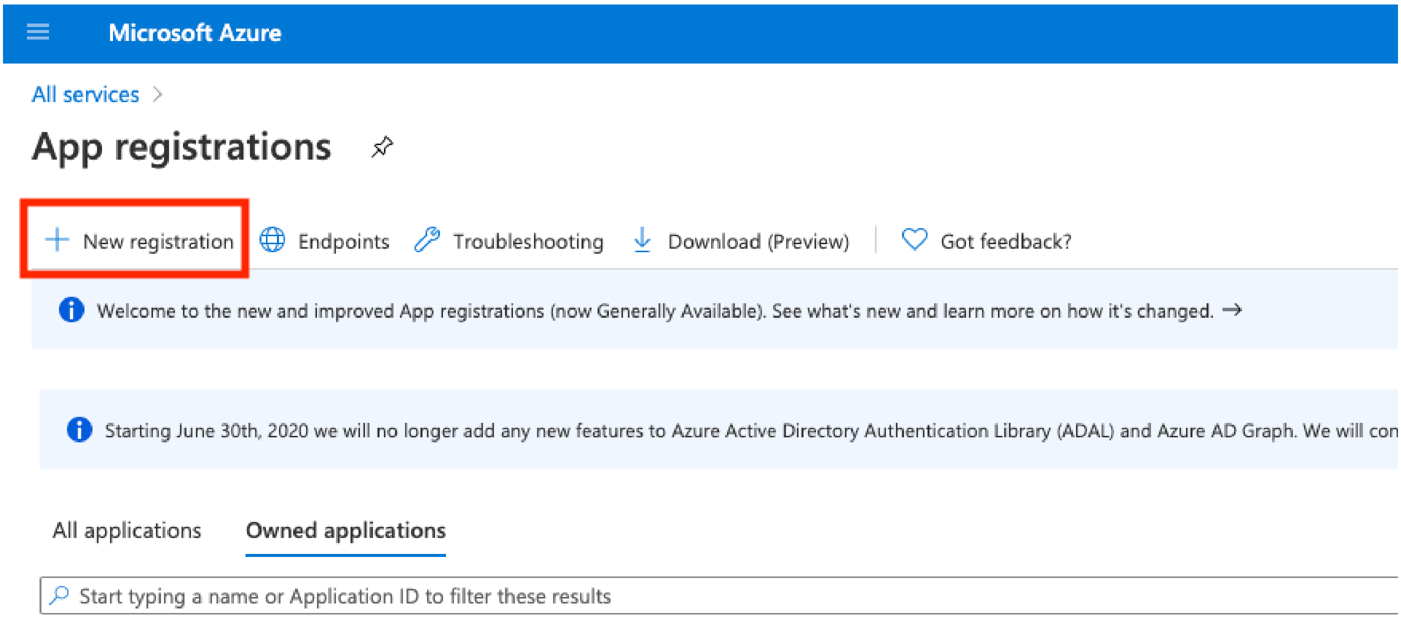


Figure 2.

a. Type AppRegistration in the Global search bar.

b. Click on the App registration service.

2. Create a new App Registration.

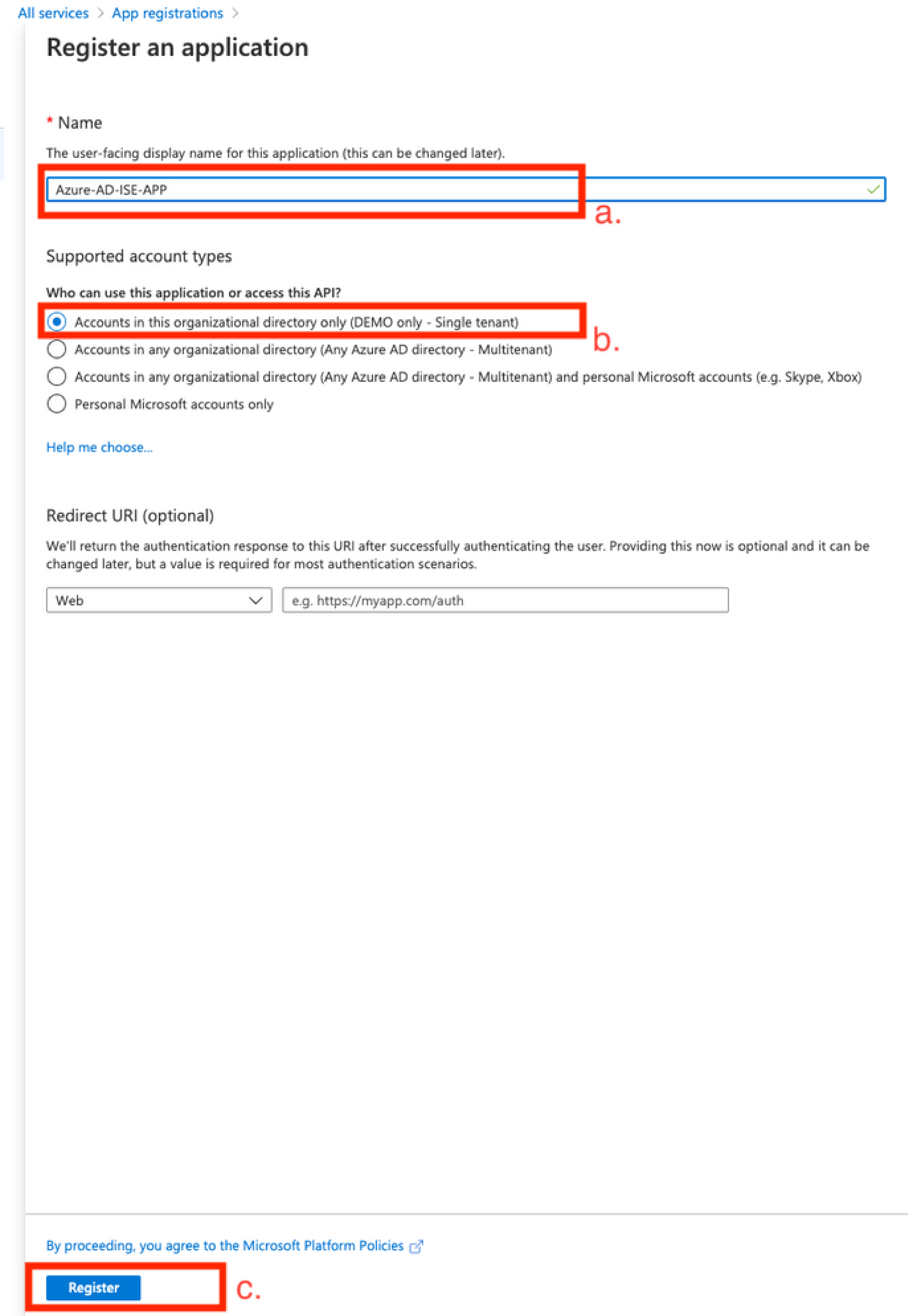


Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will con

Figure 3.

3. Register a new App.



All services > App registrations >

Register an application

* Name

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

Azure-AD-ISE-APP

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (DEMO only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

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

e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies

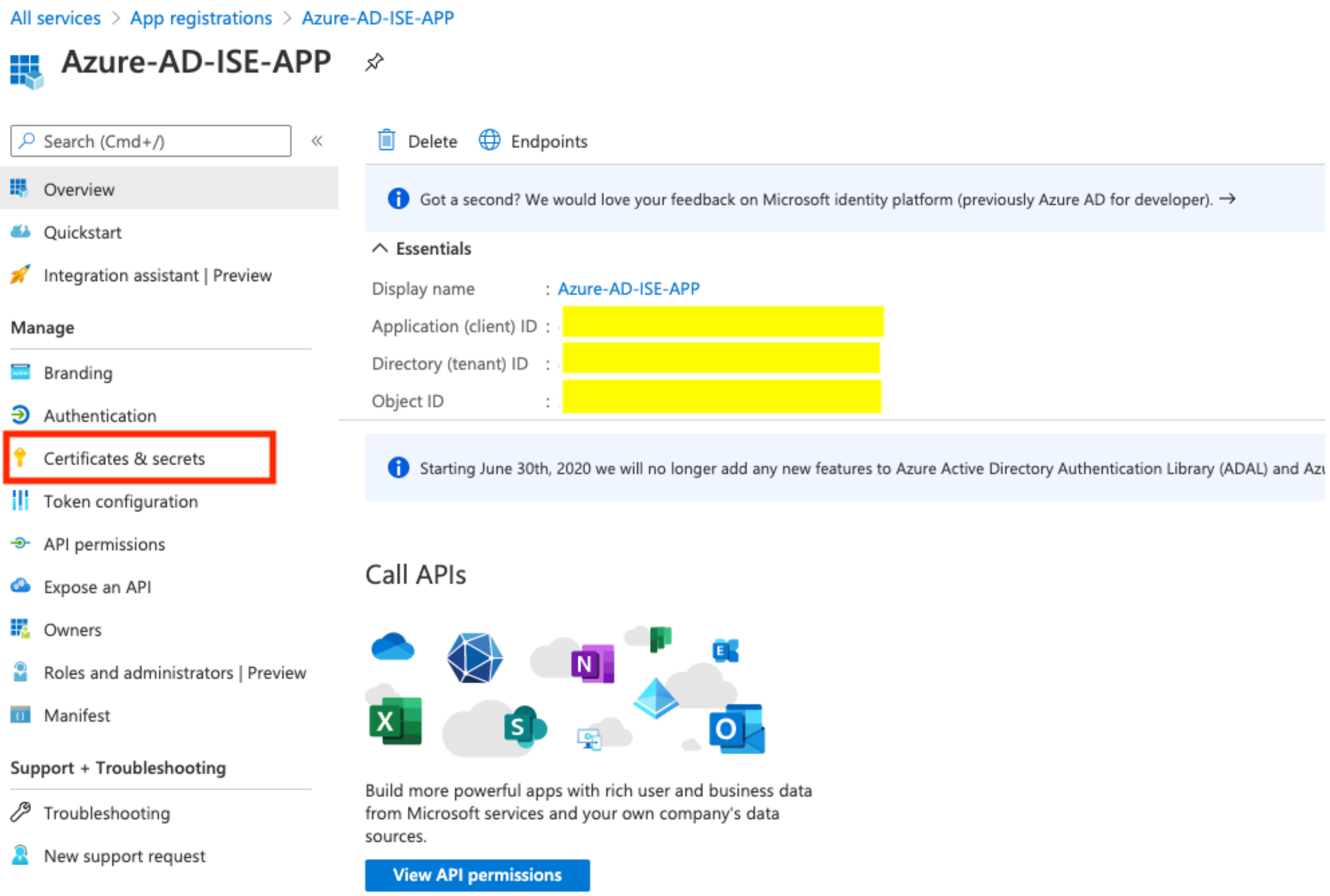
Figure 4.

a. Define the name of the App.

b. Define which accounts can use new applications.

c. Press the Register button.

4. Navigate to **Certificate & secrets**.



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name : Azure-AD-ISE-APP

Application (client) ID : [redacted]

Directory (tenant) ID : [redacted]

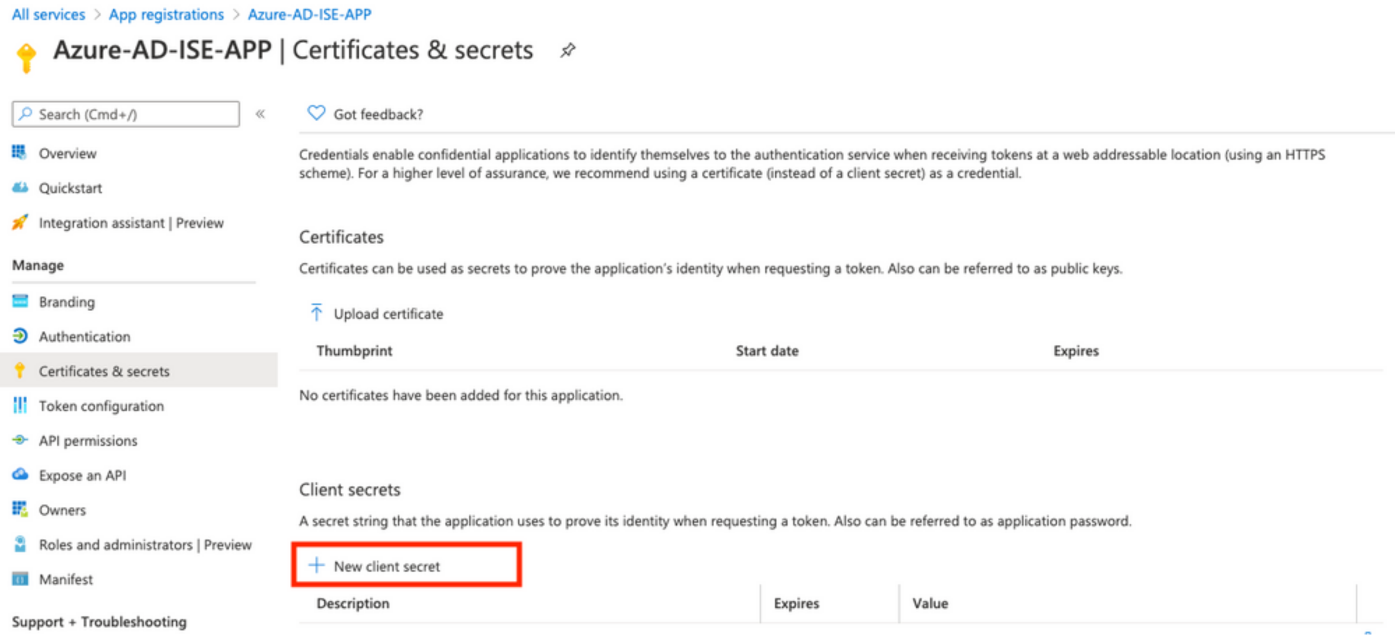
Object ID : [redacted]

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azu

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Figure 5.

5. Create **New client secret** as shown in the image.



All services > App registrations > Azure-AD-ISE-APP

Azure-AD-ISE-APP | Certificates & secrets

Search (Cmd+/)

- Overview
- Quickstart
- Integration assistant | Preview

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

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.

Certificates

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	Start date	Expires

No certificates have been added for this application.

Client secrets

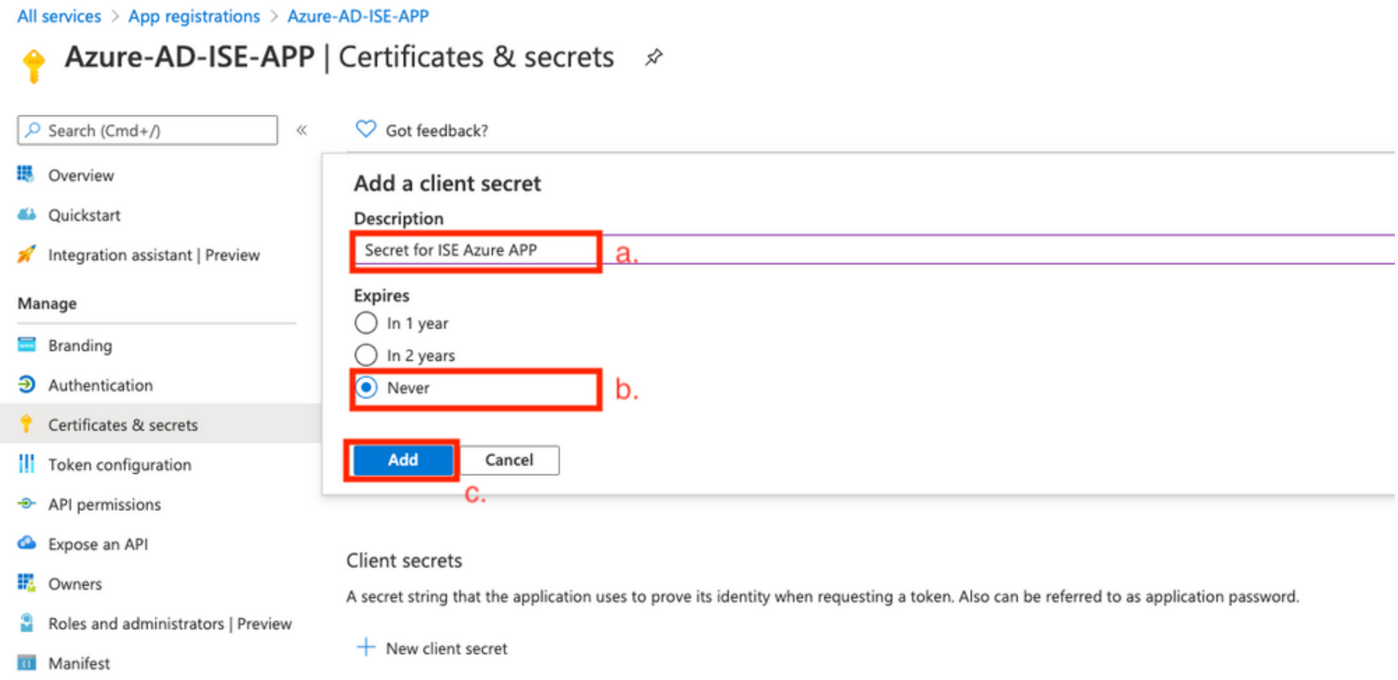
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value

Figure 6.

6. Configure the **client secret** as shown in the image.



All services > App registrations > Azure-AD-ISE-APP

Azure-AD-ISE-APP | Certificates & secrets

Search (Cmd+/)

- Overview
- Quickstart
- Integration assistant | Preview

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- Owners
- Roles and administrators | Preview
- Manifest

Got feedback?

Add a client secret

Description

Secret for ISE Azure APP

a.

Expires

○ In 1 year

○ In 2 years

● Never

b.

Add Cancel

c.

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.

+ New client secret

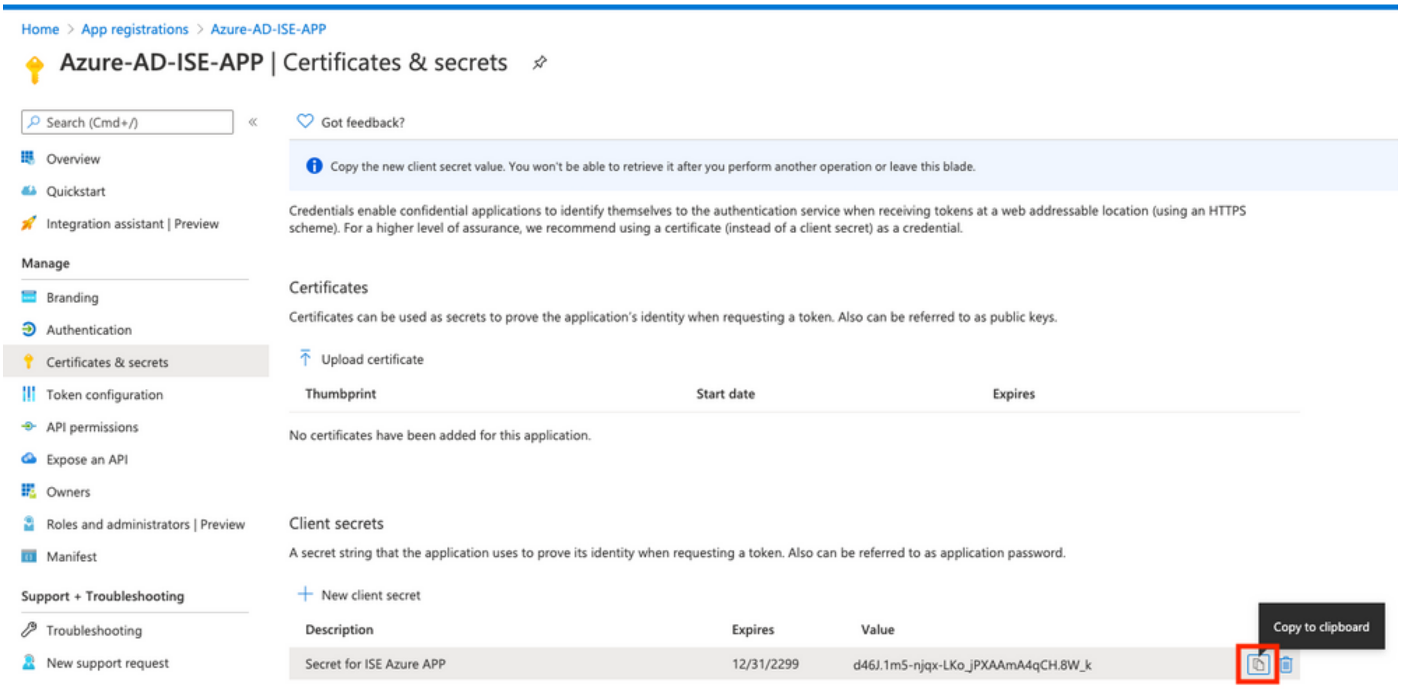
Figure 7.

a. Define the description of a new secret.

b. Choose the expiration period.

c. Click the **Add** button.

7. Copy and save the secret value (it later needs to be used on ISE at the time of the integration configuration).



Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

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.

Certificates

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

Thumbprint	Start date	Expires

No certificates have been added for this application.

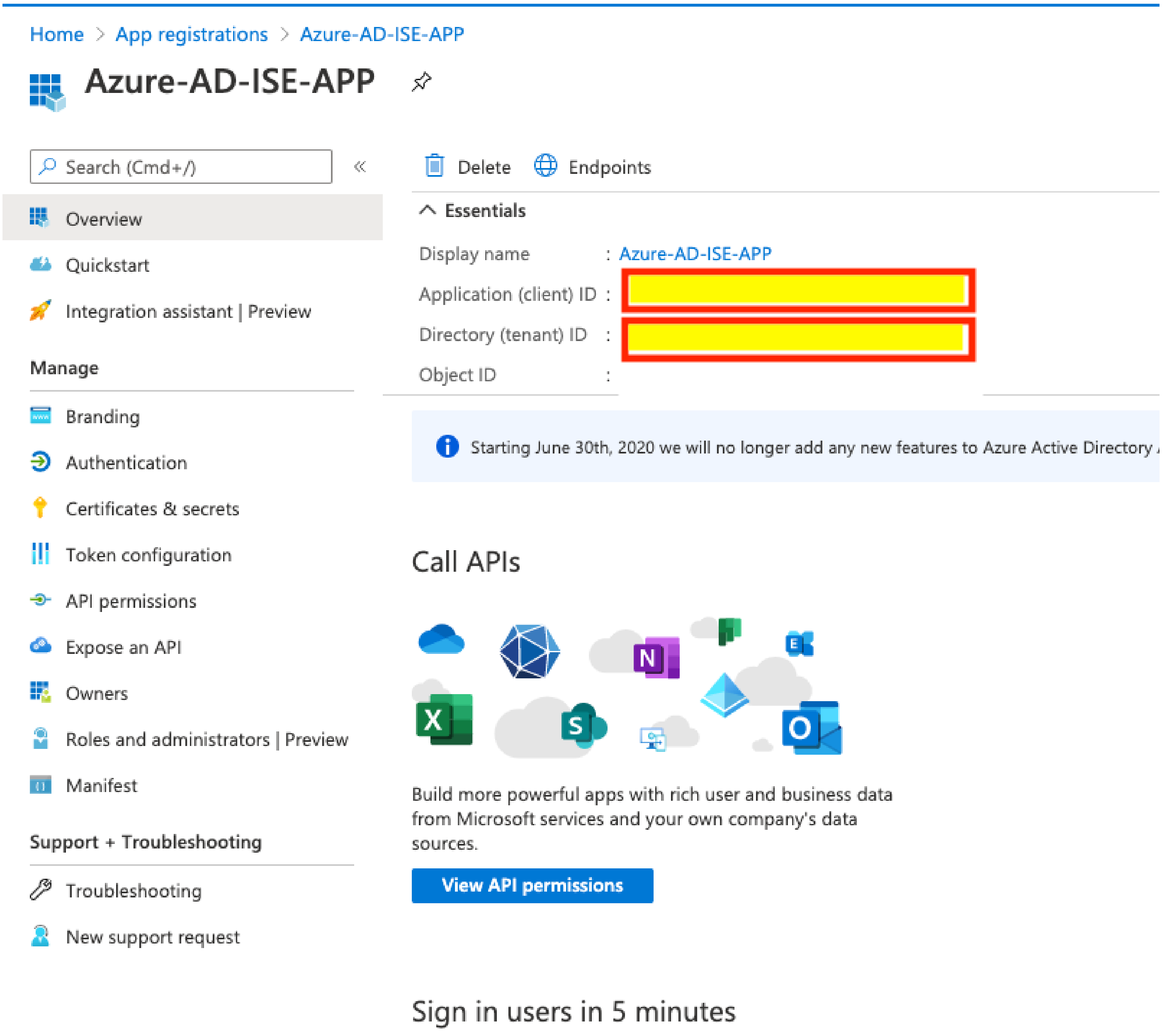
Client secrets

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
Secret for ISE Azure APP	12/31/2299	d46J.1m5-njqx-LKo_jPXAAmA4qCH.8W_k

Figure 8.

8. Navigate back to the **Overview** tab in order to copy the **App ID** and **Tenant ID**.



Display name : Azure-AD-ISE-APP

Application (client) ID : [redacted]

Directory (tenant) ID : [redacted]

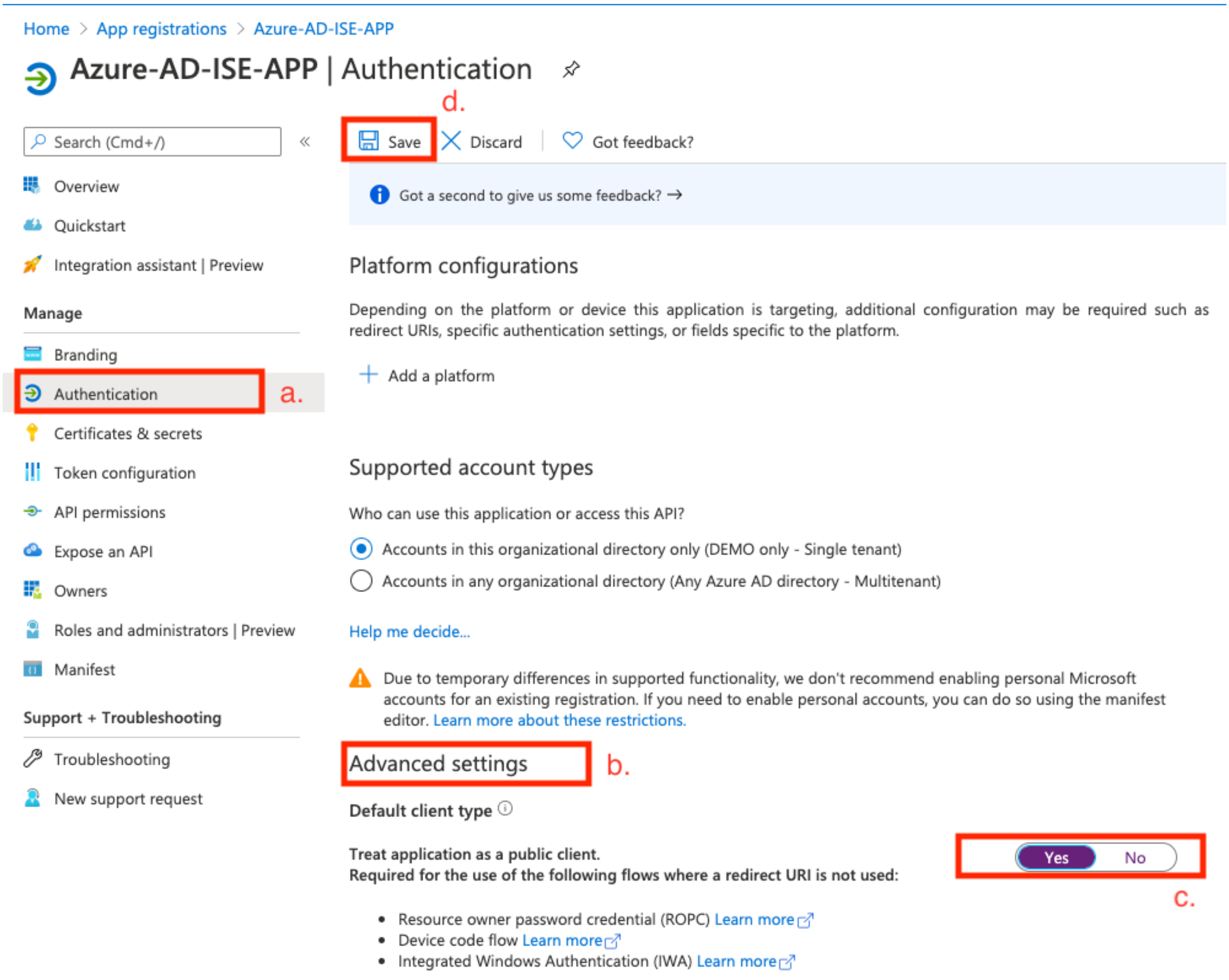
Object ID :

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Figure 9.

9. Enable ROPC for the App.



Home > App registrations > Azure-AD-ISE-APP

Azure-AD-ISE-APP | Authentication

Search (Cmd+/)

Save | Discard | Got feedback?

- Overview
- Quickstart
- Integration assistant | Preview

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Got a second to give us some feedback? →

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

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (DEMO only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - 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.

Advanced settings

Default client type

Treat application as a public client.
Required for the use of the following flows where a redirect URI is not used: [✓ Yes] No

- Resource owner password credential (ROPC) Learn more
- Device code flow Learn more
- Integrated Windows Authentication (IWA) Learn more

Figure 10.

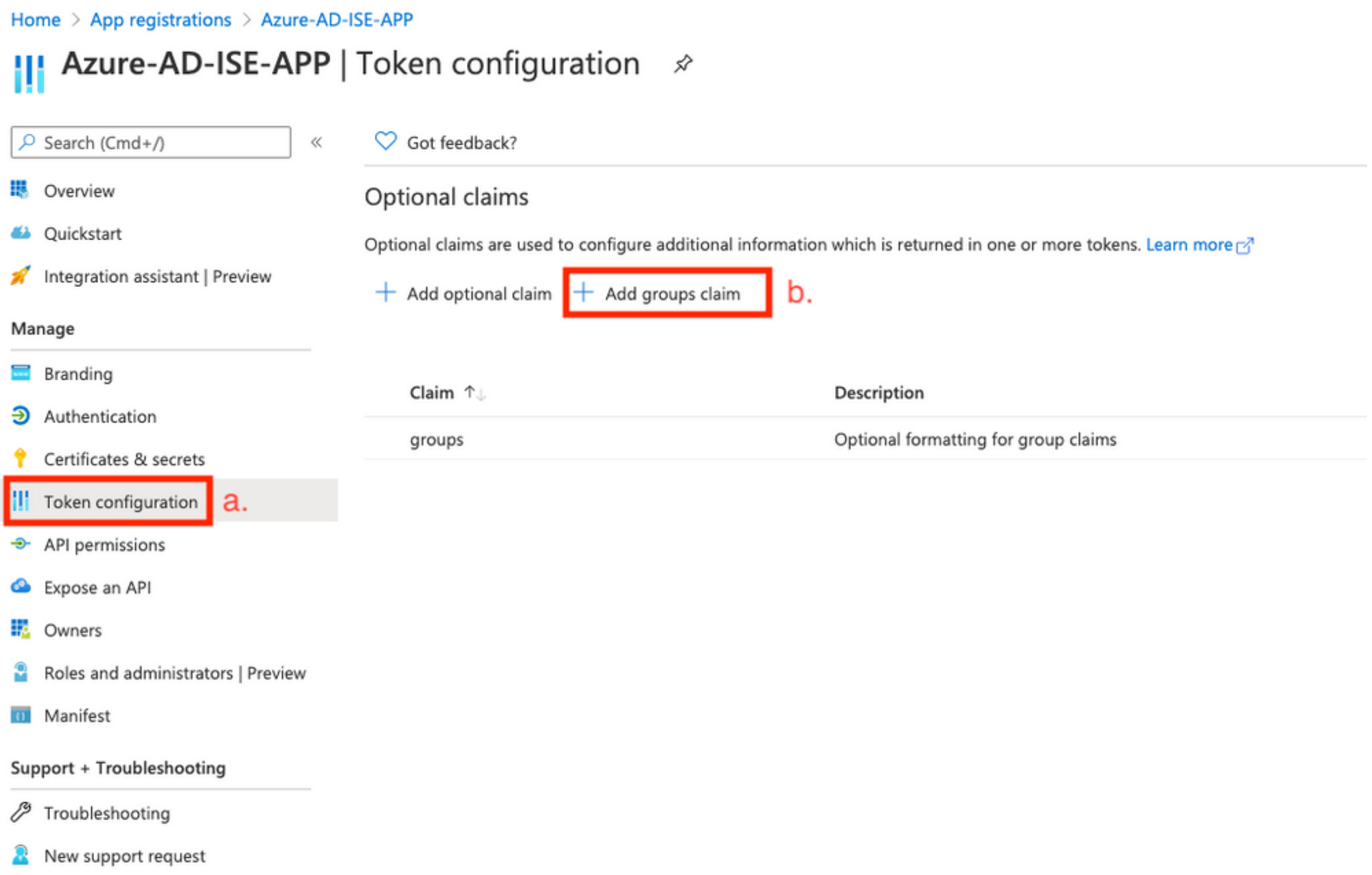
a. Navigate to the **Authentication** tab.

b. Locate the Advanced settings section.

c. Select **Yes** for - Treat application as a public client.

d. Click the **Save** button.

10. **Add group claims** to the App.



Home > App registrations > Azure-AD-ISE-APP

Azure-AD-ISE-APP | Token configuration

Search (Cmd+/)

- Overview
- Quickstart
- Integration assistant | Preview

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration a.
- API permissions
- Expose an API
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Got feedback?

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

+ Add optional claim + Add groups claim b.

Claim ↑↓	Description
groups	Optional formatting for group claims

Figure 11.

a. Navigate to Token configuration.

b. Press on - **Add groups claim**.

11. Define group types which need to be added