# **Configure ISE 3.0 REST ID with Azure Active Directory**

# Contents

Introduction Prerequisites Requirements Components Used Configure High-Level Flow Overview Configure Azure AD for Integration Configure ISE for Integration ISE Policy Examples for Different Use Cases Verify Troubleshoot Issues with REST Auth Service Issues with REST ID Authentication Work with the Log Files

# 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.

Microsoft Azure									a.		×	
All services P Search All							Services		_	Marketplace		1
							App registration	5	b.		No results were found.	
Overview	Featured						Event Grid Partn	er Registrations		Documentation	No secolo const	
Categories	٠	6	-	SQL		1	App Service Dor	nains		Resource Groups	No results were found.	
All	Virtual	App Services	Storage	SQL	Static Web	Azure	Resources	No results were found.			No results were found.	
General	machines		accounts	databases	Apps	Cosmos De						
Compute	<b>~</b> ~~				•		0	$\rightarrow$				r!
Networking	<b>N N</b>		( )	0		•	•	/				
Storage	Virtual networks	Azure Active Directory	Resource groups	Monitor	Advisor	Security Center	Cost Management	All services				
Web												
Mobile	Free training	from Microsof	See all									

## Figure 2.

- a. Type AppRegistration in the Global search bar.
- b. Click on the App registration service.
- 2. Create a new App Registration.

All services >	
App registrations 🖉	
+ New registration 🔀 Endpoints 🖉 Troubleshooting 🞍 Download (Preview) 🛛 🛇 Got feedback?	
(i) Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed. $ ightarrow$	
3 Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We w	ill con
All applications Owned applications	
Start typing a name or Application ID to filter these results	

Figure 3.

3. Register a new App.

## **Register an application**

#### \* Name

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

 $\sim$ 

Azure-AD-ISE-APP	✓
Supported account types	- a.
Who can use this application or access this API?	
<ul> <li>Accounts in this organizational directory only (DEMO only - Single tenant)</li> </ul>	h
<ul> <li>Accounts in any organizational directory (Any Azure AD directory - Multitenant)</li> </ul>	- D.
<ul> <li>Accounts in any organizational directory (Any Azure AD directory - Multitenant) and</li> </ul>	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 ♂

Register

C.

### 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.

#### All services > App registrations > Azure-AD-ISE-APP Azure-AD-ISE-APP Ż Search (Cmd+/) ~ Overview f Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). oQuickstart ∧ Essentials 💉 Integration assistant | Preview : Azure-AD-ISE-APP Display name Application (client) ID : Manage Directory (tenant) ID Branding Object ID Authentication Certificates & secrets 🚯 Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azu Token configuration API permissions Call APIs Expose an API Owners Roles and administrators | Preview Manifest Support + Troubleshooting Build more powerful apps with rich user and business data Þ Troubleshooting from Microsoft services and your own company's data sources Rew support request View API permissions

## 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 🔗					
	♡ Got feedback?					
<ul> <li>Overview</li> <li>Quickstart</li> </ul>	Overview 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.					
🚀 Integration assistant   Preview	Certificates					
Manage	Certificates can be used as secrets to prove the application's identity whe	n requesting a token. Al	so can be referred to as public keys.			
E Branding	↓ Upload certificate					
Authentication	Thumborint St	art date	Fynires			
📍 Certificates & secrets	- Humppink St	art dute	Lopica			
Token configuration	No certificates have been added for this application.					
API permissions						
Expose an API	Client secrets					
Owners	A secret string that the application uses to prove its identity when request	ting a token. Also can b	e referred to as application password.			
Roles and administrators   Preview						
0 Manifest	+ New client secret					
Support + Troubleshooting	Description	Expires	Value			

#### Figure 6.

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

All :	I services > App registrations > Azure-AD-ISE-APP					
1	Azure-AD-ISE-APP	Certificates & secret	S ☆			
٩	Search (Cmd+/) «	♡ Got feedback?				
8	Overview	Add a client secret				
<b>43</b>	Quickstart	Description				
*	Integration assistant   Preview	Secret for ISE Azure APP	a.			
Mar	nage	Expires				
A.418	Branding	O In 2 years				
Э	Authentication	Never	b.			
•	Certificates & secrets					
Ш	Token configuration	Add Cancel				
<del>.</del>	API permissions	С.				
۵	Expose an API	Client secrets				
4	Owners	A secret string that the application u	ises to prove its identity when requesting a token. Also can be referred to as application password.			
2	Roles and administrators   Preview					
0	Manifest	+ 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).

Home > App registrations > Azure-AD-	ISE-APP			
🔶 Azure-AD-ISE-APP	Certificates & secrets 🛛 🖈			
	♡ Got feedback?			
Overview	Copy the new client secret value. You won't be able to retrieve it after	r you perform another ope	ation or leave this blade.	
Quickstart				
🚀 Integration assistant   Preview	Credentials enable confidential applications to identify themselves to the scheme). For a higher level of assurance, we recommend using a certific	ne authentication service cate (instead of a client s	when receiving tokens at a web addressable location (using an HTTf ecret) as a credential.	25
Manage				
E Branding	Certificates			
Authentication	Certificates can be used as secrets to prove the application's identity wi	hen requesting a token. A	lso can be referred to as public keys.	
📍 Certificates & secrets	Upload certificate			
Token configuration	Thumbprint	Start date	Expires	
API permissions	No certificates have been added for this application.			
Expose an API				
Owners				
Roles and administrators   Preview	Client secrets			
III Manifest	A secret string that the application uses to prove its identity when requ	esting a token. Also can	be referred to as application password.	
Support + Troubleshooting	+ New client secret			
Troubleshooting	Description	Expires	Value	Copy to clipboard
New support request	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**.



#### sign in users in 5 minu

#### Figure 9.

9. Enable ROPC for the App.

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

∋ Azure-AD-ISE-AP	P   Authentication ⇒ d.
₽ Search (Cmd+/)	Save X Discard Of Got feedback?
Overview	Got a second to give us some feedback? →
🍊 Quickstart	
🚀 Integration assistant   Preview	Platform configurations
Manage	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.
🔤 Branding	· · · · · · · ·
	+ Add a platform
Certificates & secrets	
Token configuration	Supported account types
API permissions	Who can use this application or access this API?
🚳 Expose an API	<ul> <li>Accounts in this organizational directory only (DEMO only - Single tenant)</li> </ul>
Owners	Accounts in any organizational directory (Any Azure AD directory - Multitenant)
Roles and administrators   Preview	Help me decide
0 Manifest	🛕 Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft
Support + Troubleshooting	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.
P Troubleshooting	Advanced settings b.
New support request	Default client type ①
	Treat application as a public client. Required for the use of the following flows where a redirect URI is not used:
	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.

# Azure-AD-ISE-APP | Token configuration 🔗

۶	Search (Cmd+/) «	♡ Got feedback?				
18	Overview	Optional claims				
<b>6</b> 3	Quickstart	- Optional claims are used to configure additional information which is returned in one or more tokens. Learn more 🖂				
R	Integration assistant   Preview	+ Add optional claim + Add groups claim b.				
Ma	nage					
	Branding	Claim ↑.	Description			
Э	Authentication					
Ŷ	Certificates & secrets	groups	Optional formatting for group claims			
11	Token configuration a.					
<del>.</del> .	API permissions					
2	Expose an API					
é	Owners					
	Roles and administrators   Preview					
0	Manifest					
Su	oport + Troubleshooting					
ß	Troubleshooting					
2	New support request					

## Figure 11.

- a. Navigate to Token configuration.
- b. Press on Add groups claim.
- 11. Define group types which need to be added