Configure ISE 3.0 REST ID with Azure Active Directory

Contents

Introduction

This document describes Cisco ISE 3.0 integration with Azure AD implemented through REST Identity service with Resource Owner Password Credentials.

Background Information

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

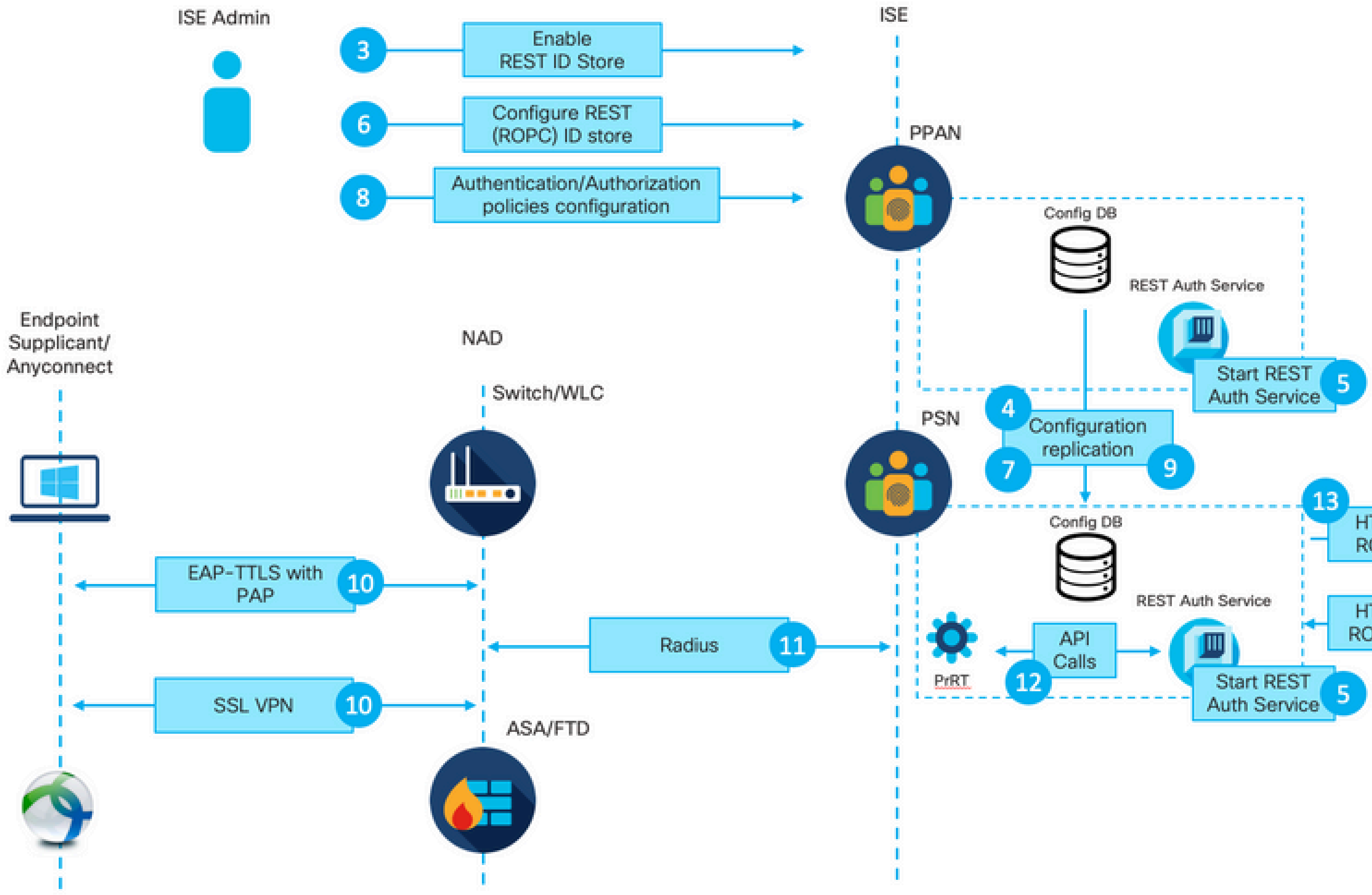
- WS-C3850-24P with s/w 16.9.2
- ASAv with 9.10 (1)
- Windows 10.0.18363

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 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:

- 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, the user password has to be provided to the Microsoft identity platform in 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 the final Authentication/Authorization result. Either Access-Accept with attributes from the 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.

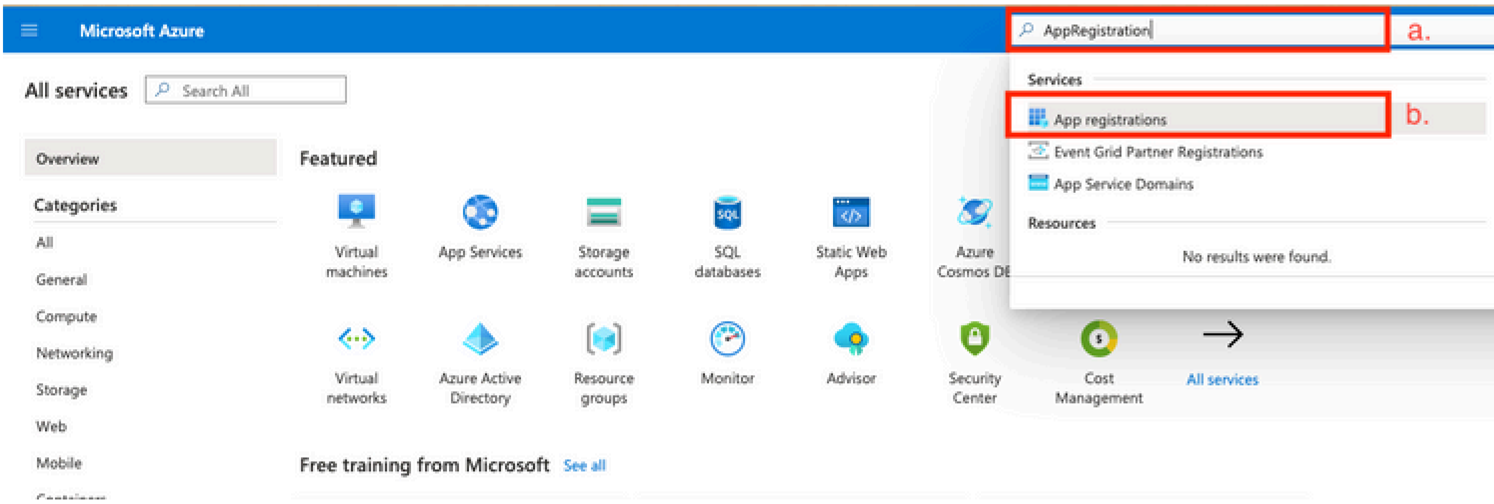
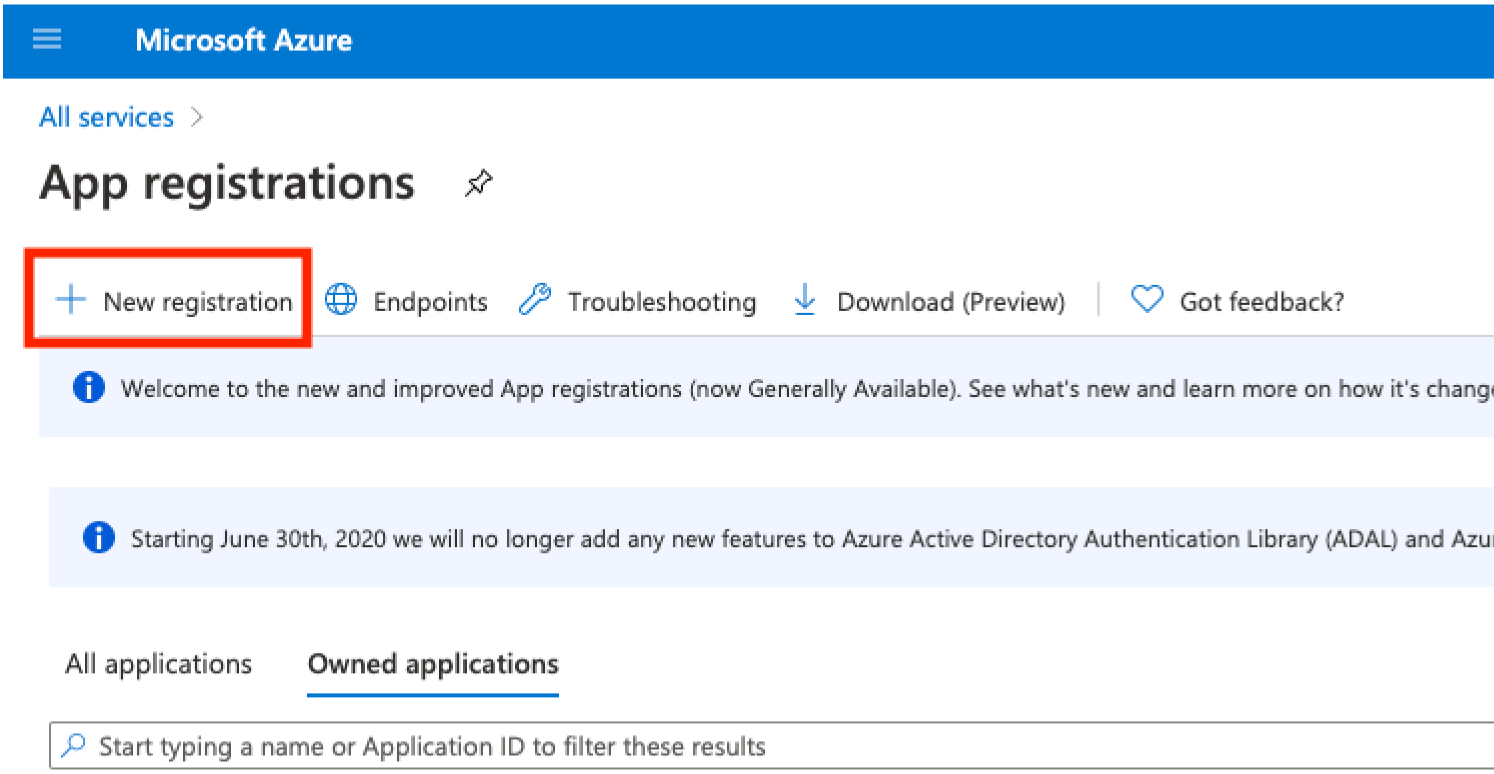


Figure 2.

a. Type AppRegistration in the Global search bar.

b. Click on the App registration service.

2. Create a new App Registration.



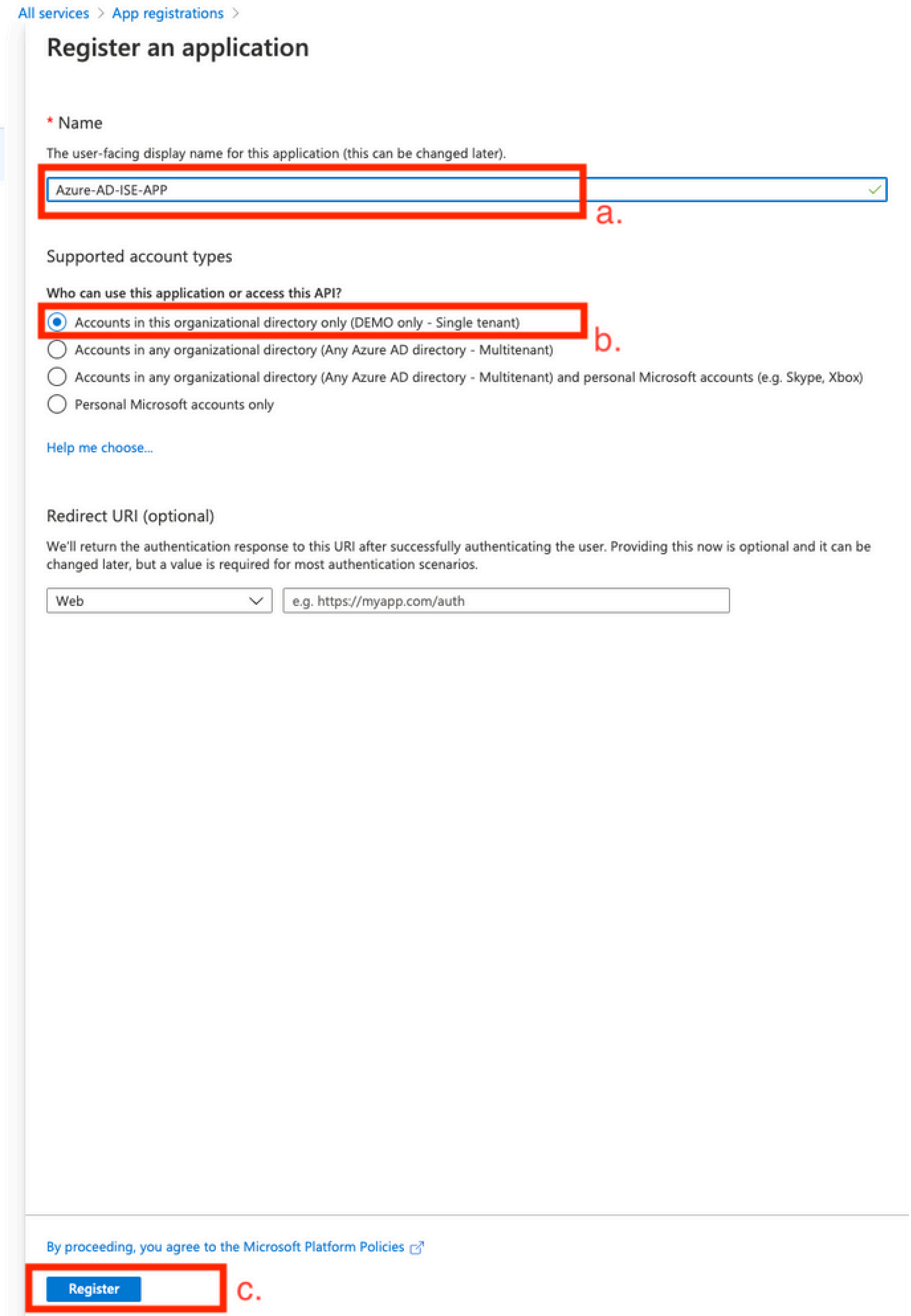
Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's chang

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

All applications
Owned applications
Start typing a name or Application ID to filter these results

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

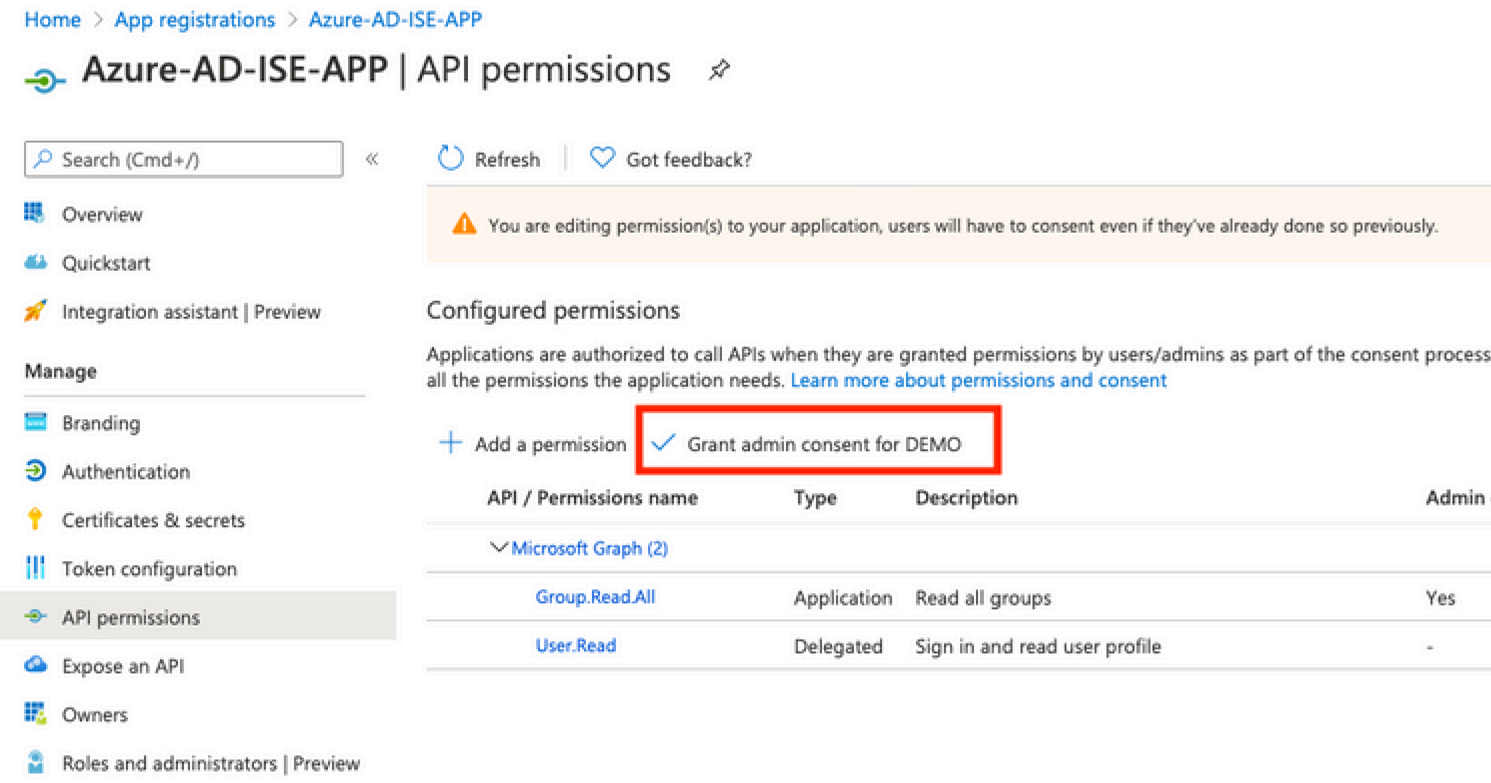
By proceeding, you agree to the Microsoft Platform Policies

Figure 4.

Define the name of the A

: User group data can be fetched from Azure AD in multiple ways with the help of different API permission. The method described in this example is proven to be successful in the Cisco TAC lab. Use other API permissions in case your Azure AD administrator recommends it.

16. Grant admin consent for API permissions.



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

Azure-AD-ISE-APP | API permissions

Search (Cmd+/)

- Overview
- Quickstart
- Integration assistant | Preview

Manage

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

Refresh | Got feedback?

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

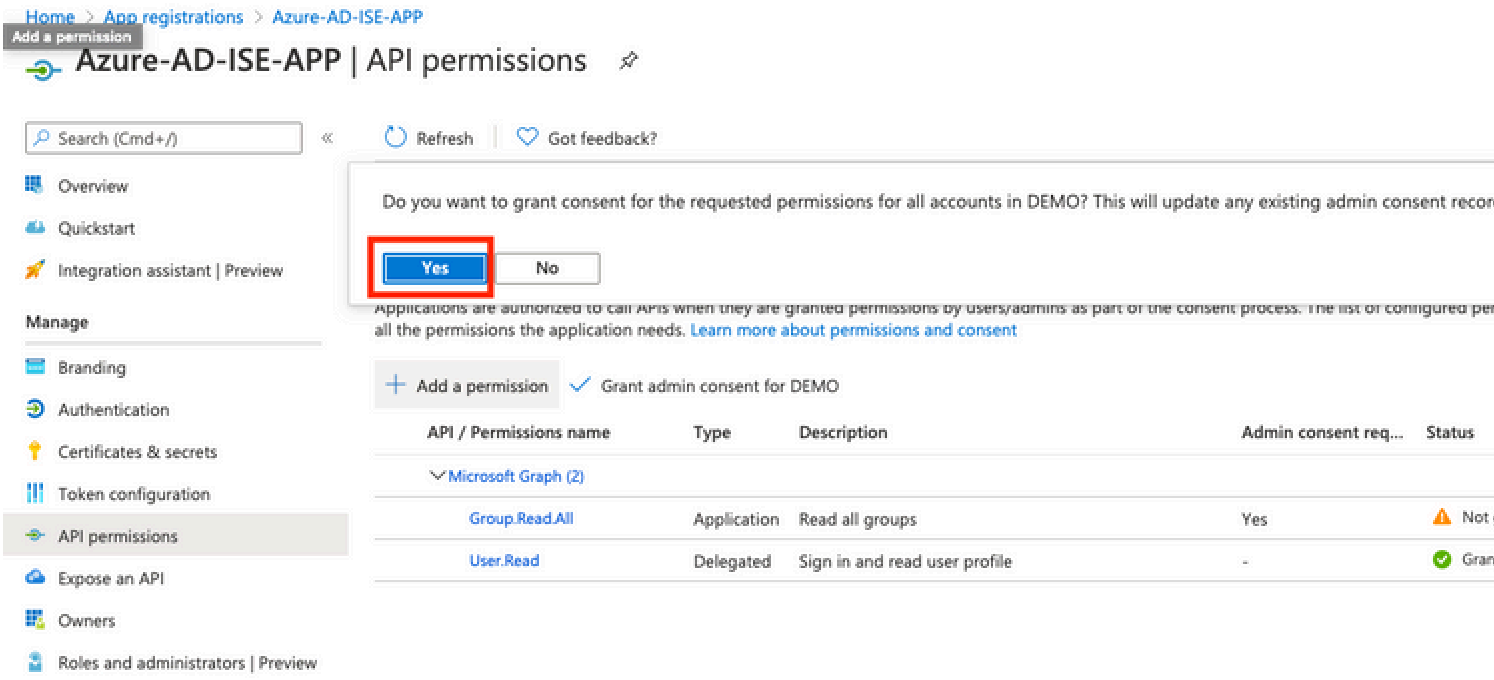
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process
all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for DEMO

API / Permissions name	Type	Description	Admin
Microsoft Graph (2)			
Group.Read.All	Application	Read all groups	Yes
User.Read	Delegated	Sign in and read user profile	-

Figure 17.

17. Confirm Grant consent for Admin.



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

Add a permission

Azure-AD-ISE-APP | API permissions

Search (Cmd+/)

- Overview
- Quickstart
- Integration assistant | Preview

Manage

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

Refresh | Got feedback?

Do you want to grant consent for the requested permissions for all accounts in DEMO? This will update any existing admin consent recor

Yes No

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured pe
all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for DEMO

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (2)				
Group.Read.All	Application	Read all groups	Yes	⚠ Not
User.Read	Delegated	Sign in and read user profile	-	✓ Gran

Figure 18.

At this point, you can consider integration fully configured on the Azure AD side.

Configure ISE for Integration

1. Navigate to Identity Management settings.

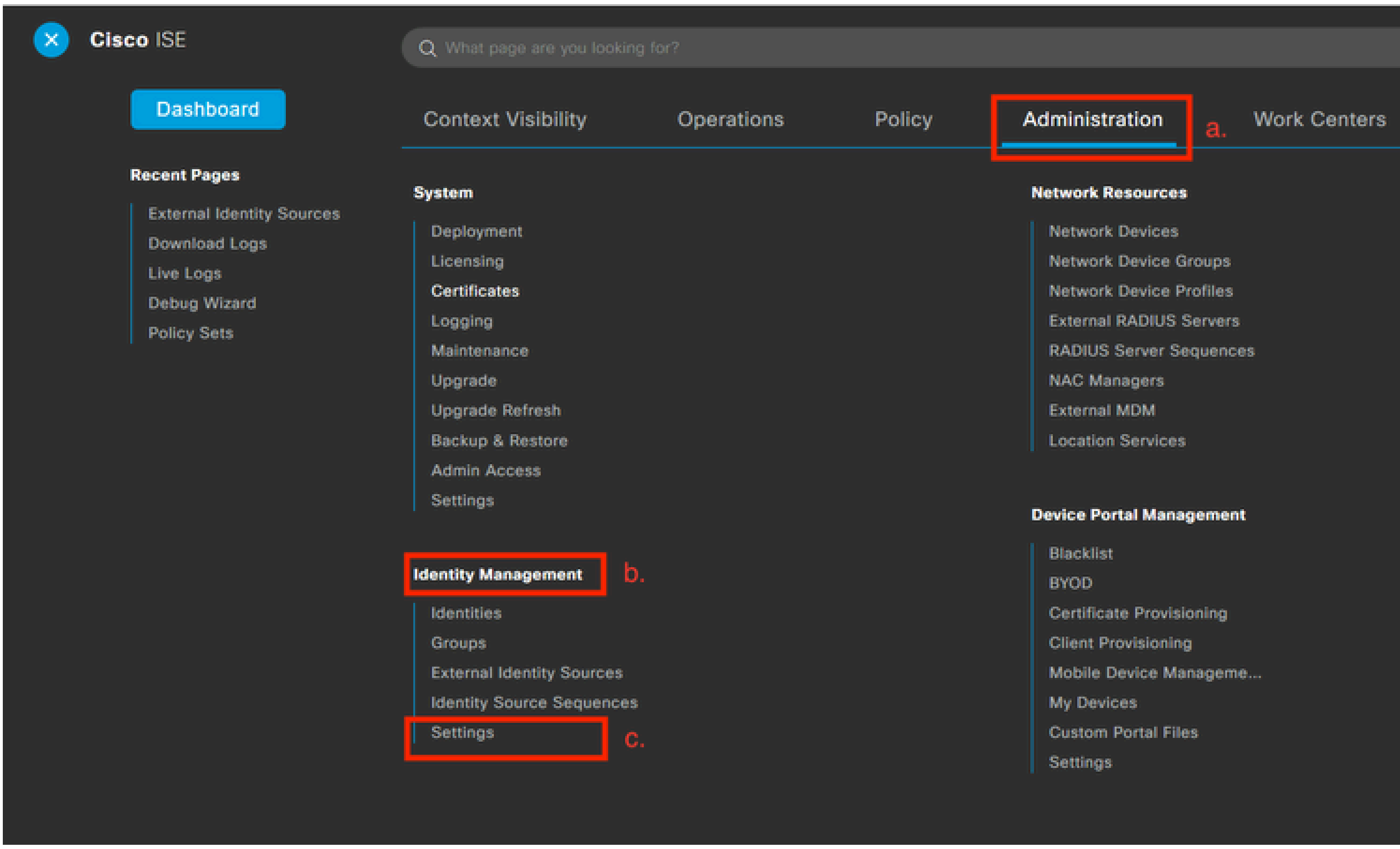


Figure 19.

Navigate to Administration > Identity Management> Settings .

2. Enable REST ID service (disabled by default).

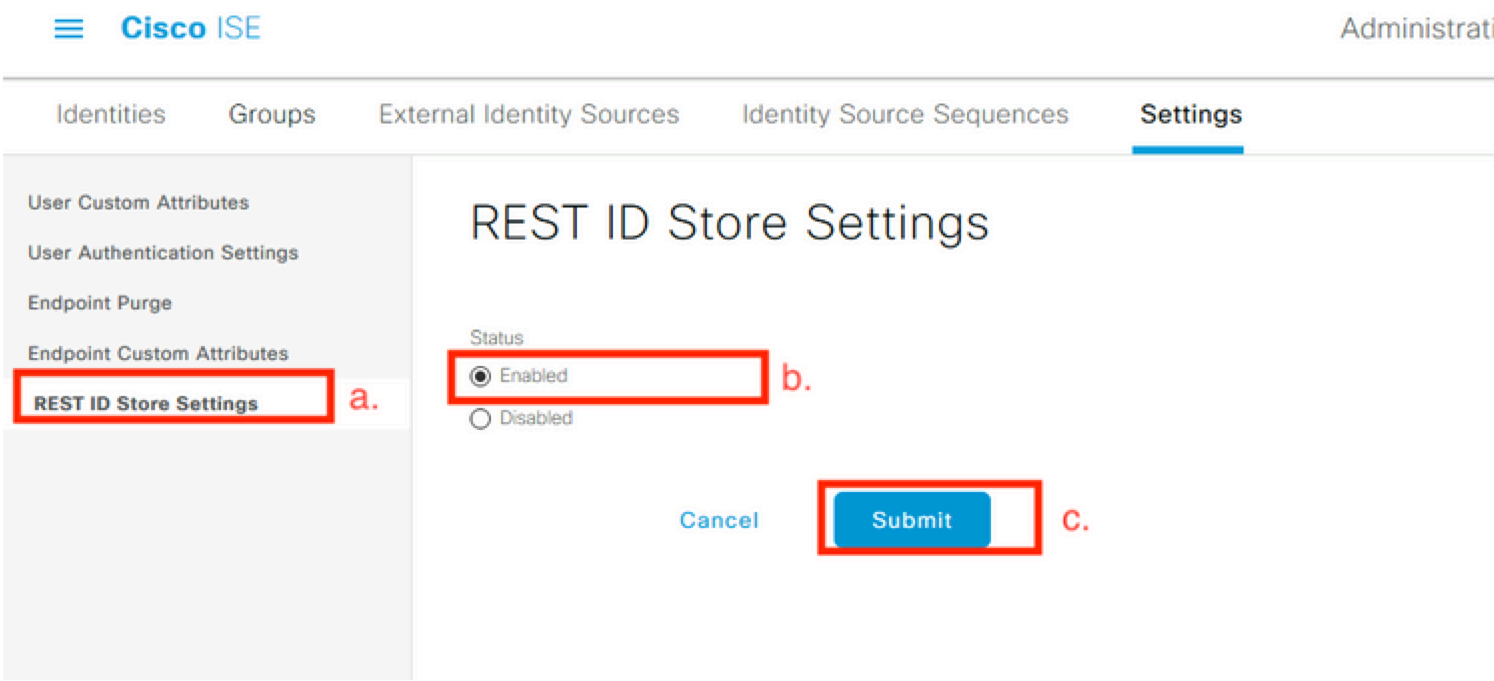


Figure 20.

Navigate to REST ID Store Settings and change the status of REST ID Store Settings in order to Enable, then Submit your changes.

3. Create a REST ID store.

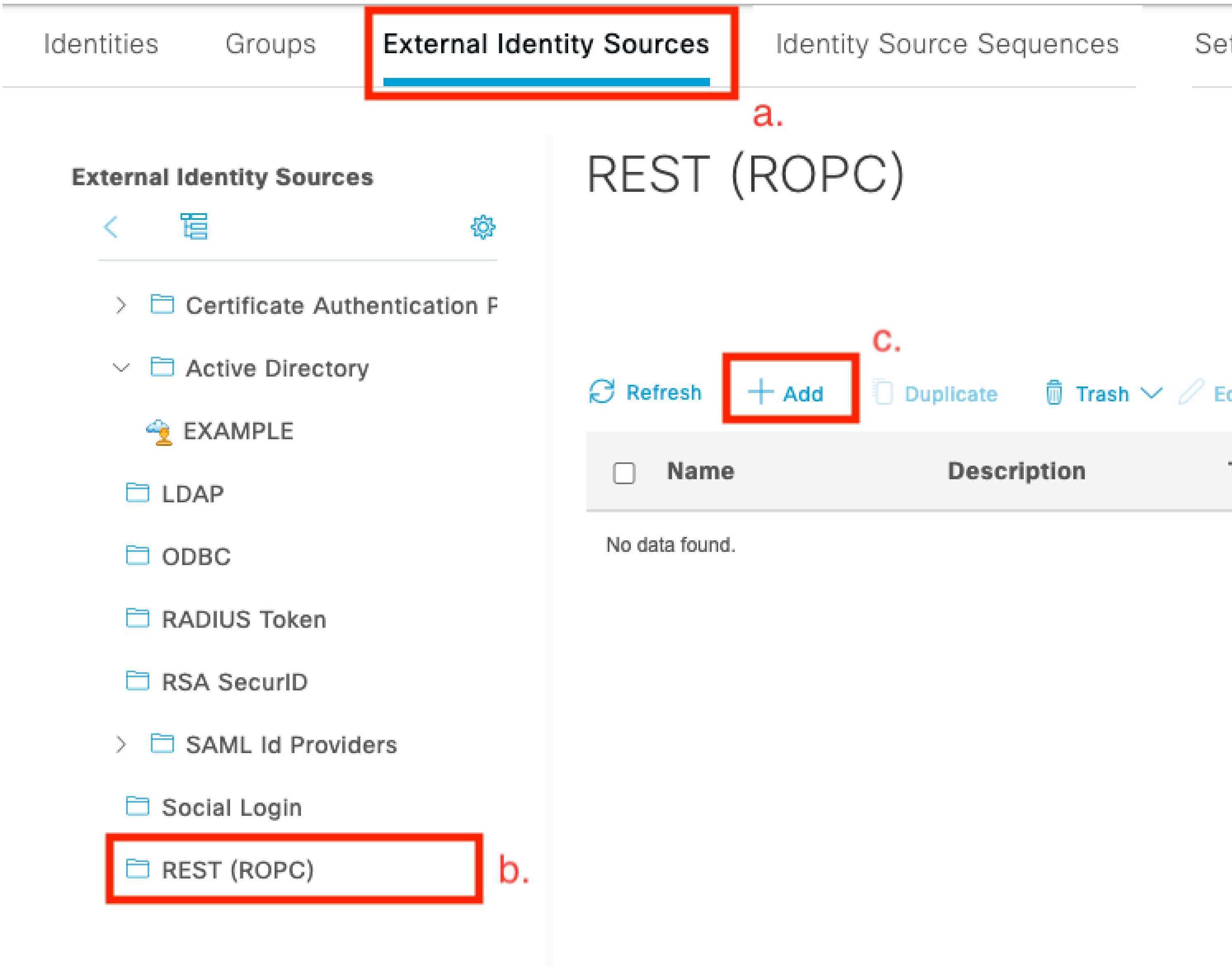
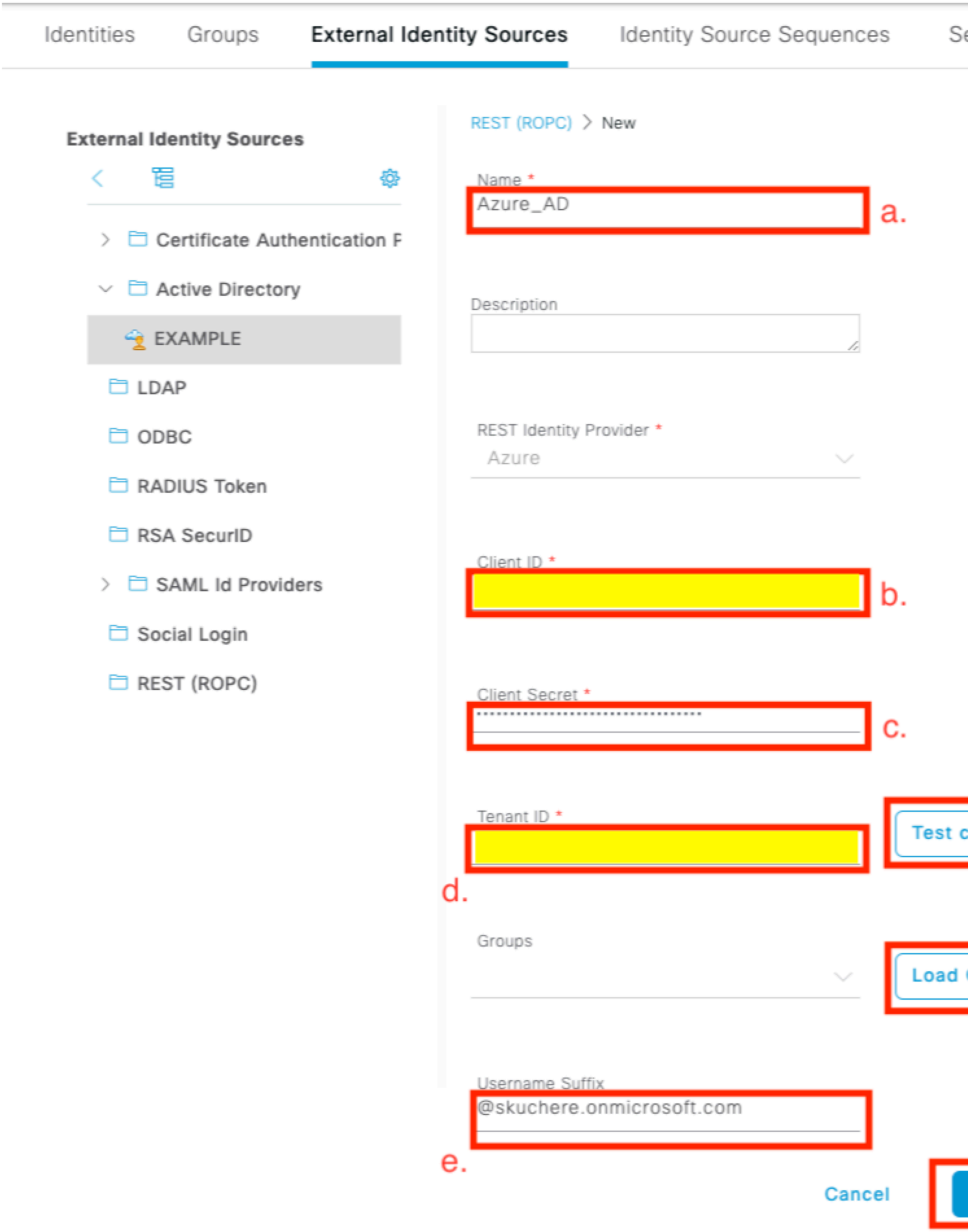


Figure 21.

Switch to the External Identity Sources tab, click on REST (ROPC) sub-tab, and click **Add**.

4. Configure the REST ID store.



External Identity Sources

REST (ROPC) > New

Name * Azure_AD

a.

Description

REST Identity Provider * Azure

Client ID * [redacted]

b.

Client Secret * ••

c.

Tenant ID * [redacted]

d.

Groups

Username Suffix @skuchere.onmicrosoft.com

e.

Figure 22.

a. Define the ID store name. Later this name can be found in the list of ISE dictionaries when you configure authorization policies. Also, this name is displayed in the list of ID stores available in the Authentication Policy settings and in the list of ID stores available in the Identity Store sequence configuration.

b. Provide client ID (taken from Azure AD in Step 8. of the Azure AD integration configuration section).

c. Provide client secret (taken from Azure AD in Step 7. of the Azure AD integration configuration section).

d. Provide Tenant ID (taken from Azure AD in Step 8. of the Azure AD integration configuration section).

e. Configure username Sufix - by default ISE PSN uses a username supplied by the end-user, which is provided in the sAMAccountName format (short username, for example, bob); in such case, Azure AD does not be able to locate the user. Username Sufix is the value added to the username supplied by the user in order to bring the username to the UPN format.

> **Note**: ROPC is limited to User authentication since it relies on the Username attribute during authentication. Device objects in Azure AD do not have Username attributes.

f. Press on Test connection in order to confirm that ISE can use provided App details in order to establish a connection with Azure AD.

g. Press on Load Groups in order to add groups available in the Azure AD to REST ID store. The example here shows how admin experience looks like.

> **Note**: Please be aware of the defect Cisco bug ID CSCvx00345, as it cause groups not to load. The defect is fixed in ISE 3.0 patch 2.

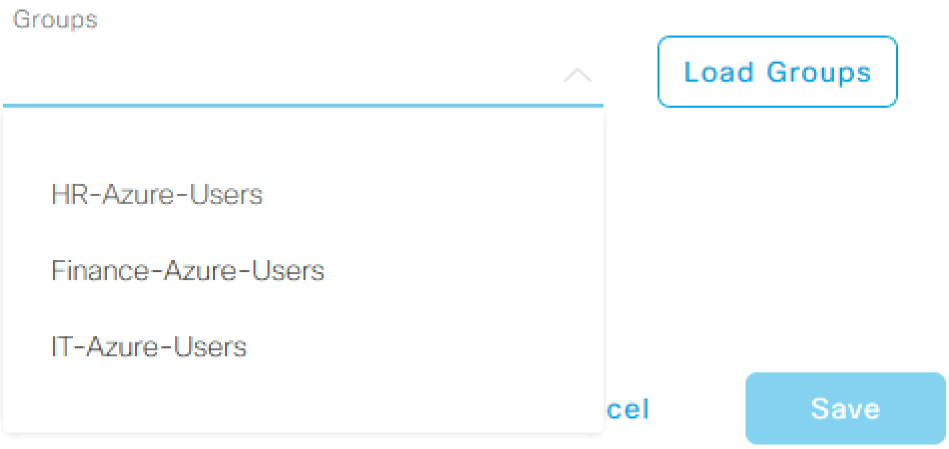


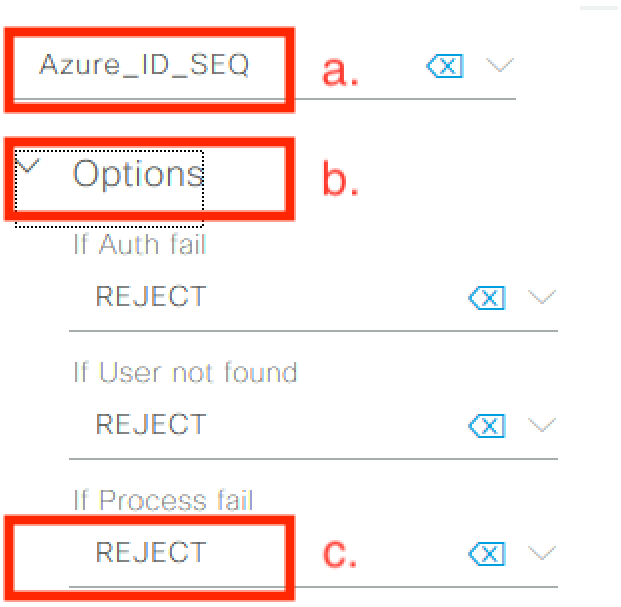
Figure 23.

h. Submit your changes.

5. At this step, consider the creation of a new Identity Store Sequence, which includes a newly created REST ID store.

6. At the moment when the REST ID store or Identity Store sequence which contains it assigned to the authentication policy, Change a default action for Process Failure from DROP to REJECT as shown in the

image.



Azure_ID_SEQ

Options

If Auth fail

REJECT

If User not found

REJECT

If Process fail

REJECT

Figure 24.

a. Locate Authentication policy that uses the REST ID store.

b. Open Options drop-down list.

c. The change default action for Process Failed from DROP to REJECT.

This is needed in order to avoid PSN marked as dead on the NADs side at a time when specific failures happen within the REST ID store like:

- The user is not a member of any group in Azure AD.
- The user password has to be changed.

7. Add REST ID store dictionary into Authorization policy.

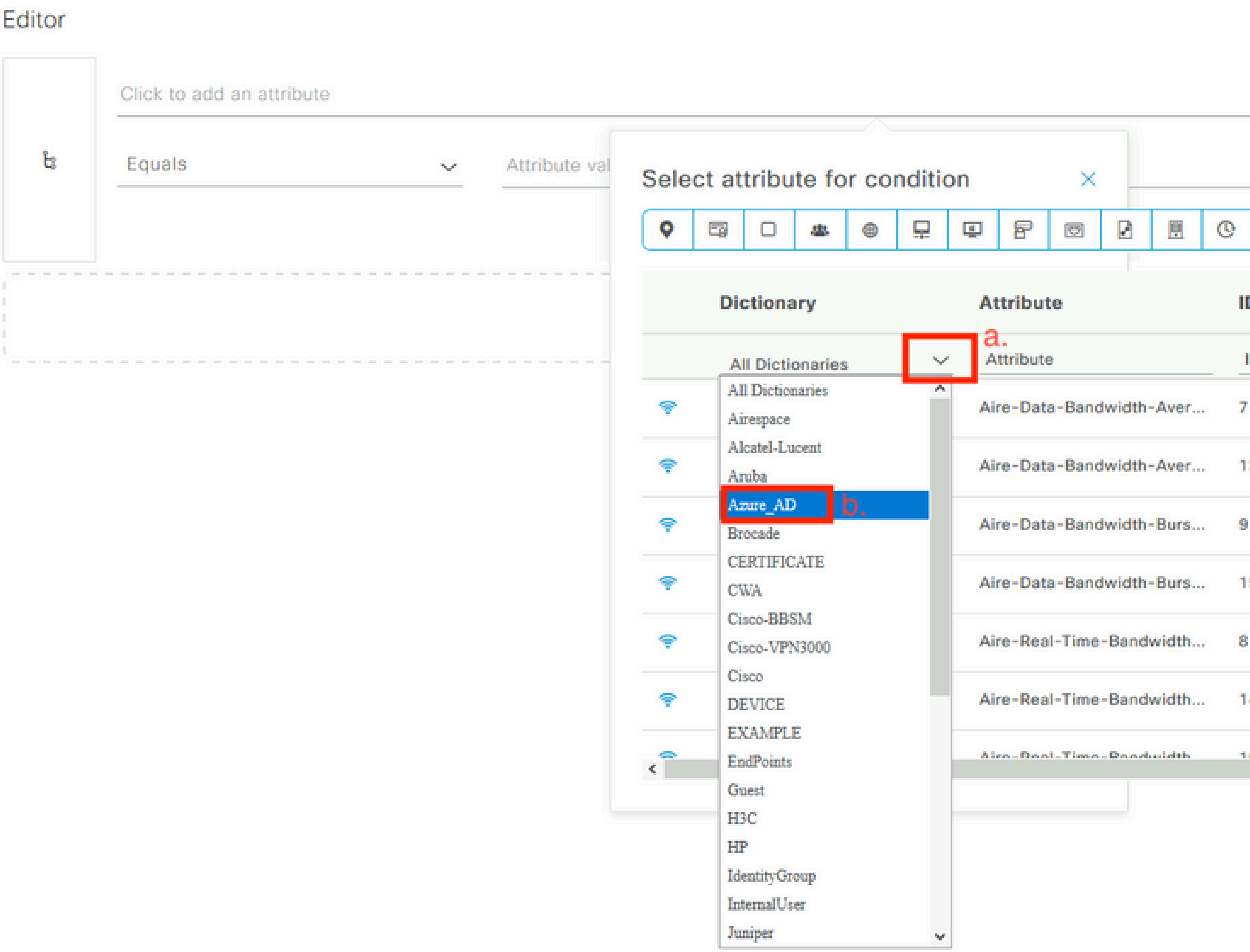
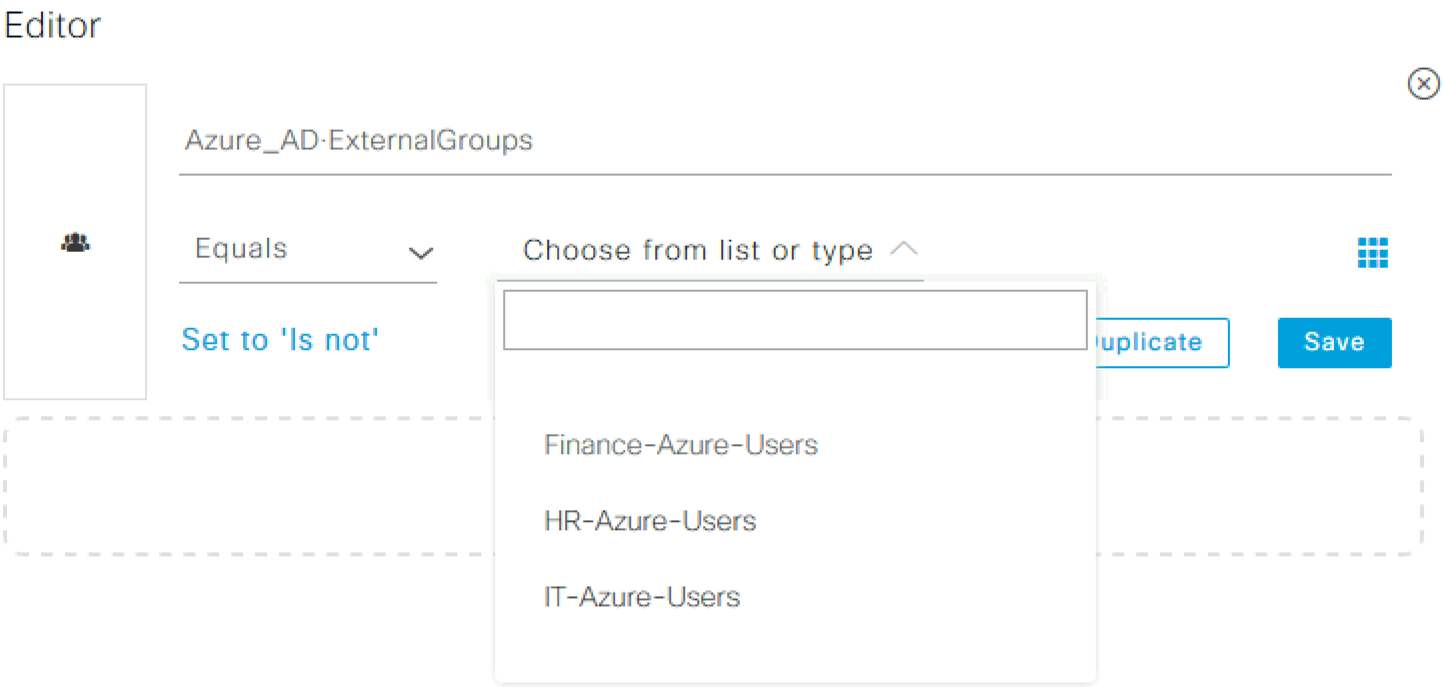


Figure 25.

a. Open All Dictionary drop-down list.

b. Locate the dictionary named in the same way as your REST ID store.

8. Add external identity groups (As of ISE 3.0, the only attribute available in the REST ID store dictionary is an external Group).



Editor

Azure_AD·ExternalGroups

Equals

Choose from list or type

Finance-Azure-Users

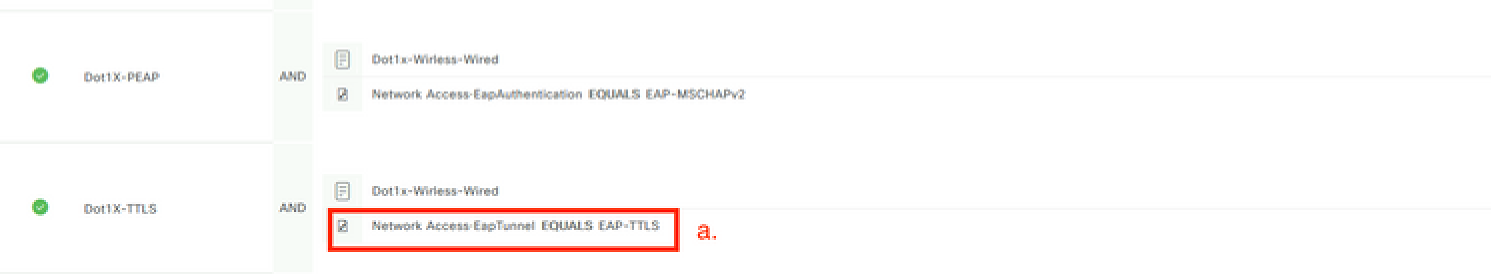
HR-Azure-Users

IT-Azure-Users

Figure 26.

ISE Policy Examples for Different Use Cases

In the case of Dot1x authentication, the EAP Tunnel condition from the Network Access dictionary can be used to match EAP-TTLS attempts as shown in the image.



Dot1X-PEAP AND
Dot1x-Wirless-Wired
Network Access·EapAuthentication EQUALS EAP-MSCHAPv2

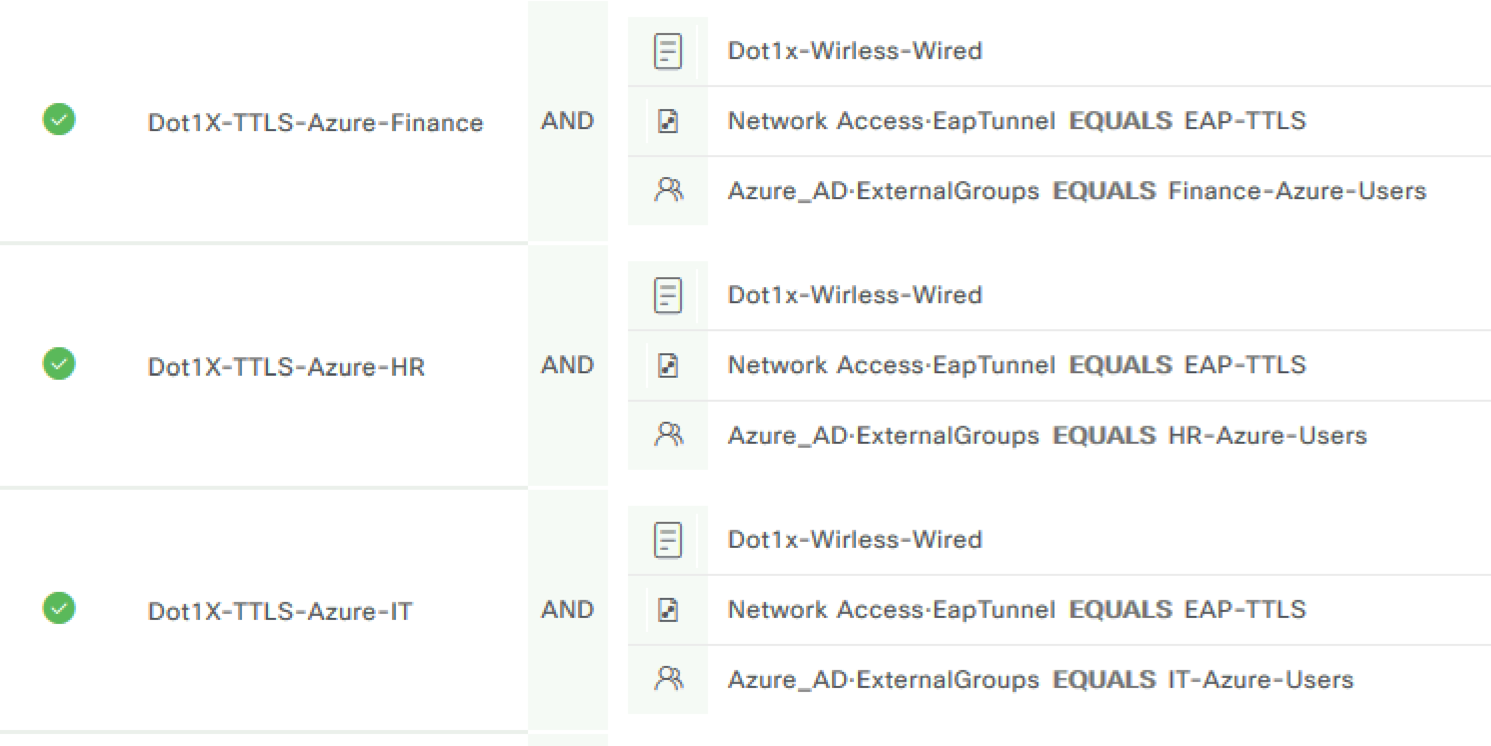
Dot1X-TTLS AND
Dot1x-Wirless-Wired
Network Access·EapTunnel EQUALS EAP-TTLS

Figure 27.

a. Define EAP Tunnel EQUAL to EAP-TTLS to match attempts that need to be forwarded to the REST ID store.

b. Select in REST ID store directly or Identity Store Sequence, which contains it in the Use column.

Inside of individual authorization policies, external groups from Azure AD can be used along with EAP Tunnel type:

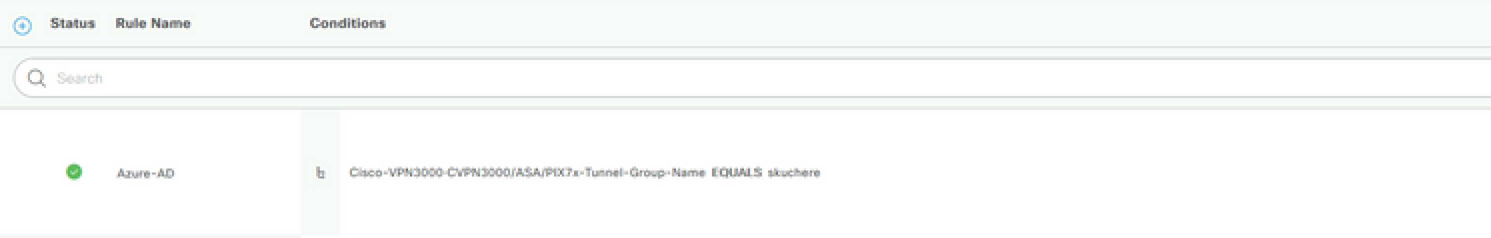


Status	Rule Name		Conditions
✓	Dot1X-TTLS-Azure-Finance	AND	Dot1x-Wirless-Wired Network Access·EapTunnel **EQUALS** EAP-TTLS Azure_AD·ExternalGroups **EQUALS** Finance-Azure-Users
✓	Dot1X-TTLS-Azure-HR	AND	Dot1x-Wirless-Wired Network Access·EapTunnel **EQUALS** EAP-TTLS Azure_AD·ExternalGroups **EQUALS** HR-Azure-Users
✓	Dot1X-TTLS-Azure-IT	AND	Dot1x-Wirless-Wired Network Access·EapTunnel **EQUALS** EAP-TTLS Azure_AD·ExternalGroups **EQUALS** IT-Azure-Users

Figure 28.

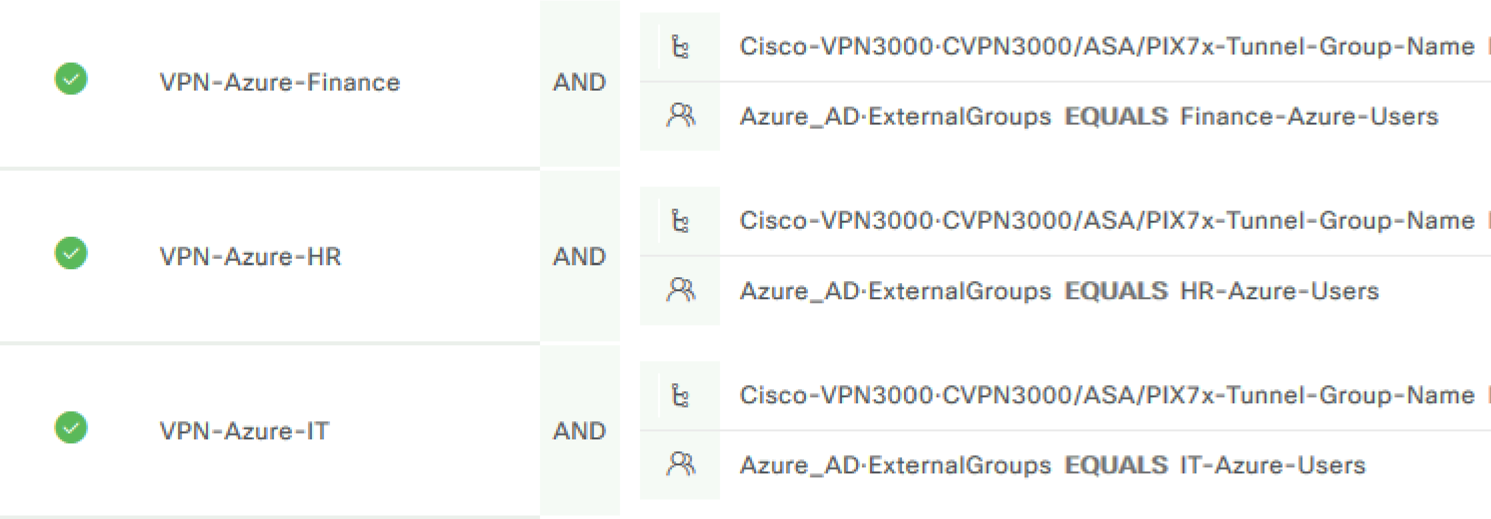
For VPN based flow, you can use a tunnel-group name as a differentiator:

Authentication policy:



Status	Rule Name	Conditions
✓	Azure-AD	Cisco-VPN3000·CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS skuchere

Authorization policies:



Status	Rule Name		Conditions
✓	VPN-Azure-Finance	AND	Cisco-VPN3000·CVPN3000/ASA/PIX7x-Tunnel-Group-Name Azure_AD·ExternalGroups **EQUALS** Finance-Azure-Users
✓	VPN-Azure-HR	AND	Cisco-VPN3000·CVPN3000/ASA/PIX7x-Tunnel-Group-Name Azure_AD·ExternalGroups **EQUALS** HR-Azure-Users
✓	VPN-Azure-IT	AND	Cisco-VPN3000·CVPN3000/ASA/PIX7x-Tunnel-Group-Name Azure_AD·ExternalGroups **EQUALS** IT-Azure-Users

Figure 29.

Verify

Use this section to confirm that your configuration works properly.

1. Confirm that REST Auth Service runs on the ISE node.

In order to check this you, need to execute the **show application status ise** command in the Secure Shell (SSH) shell of a target ISE node:

<#root>

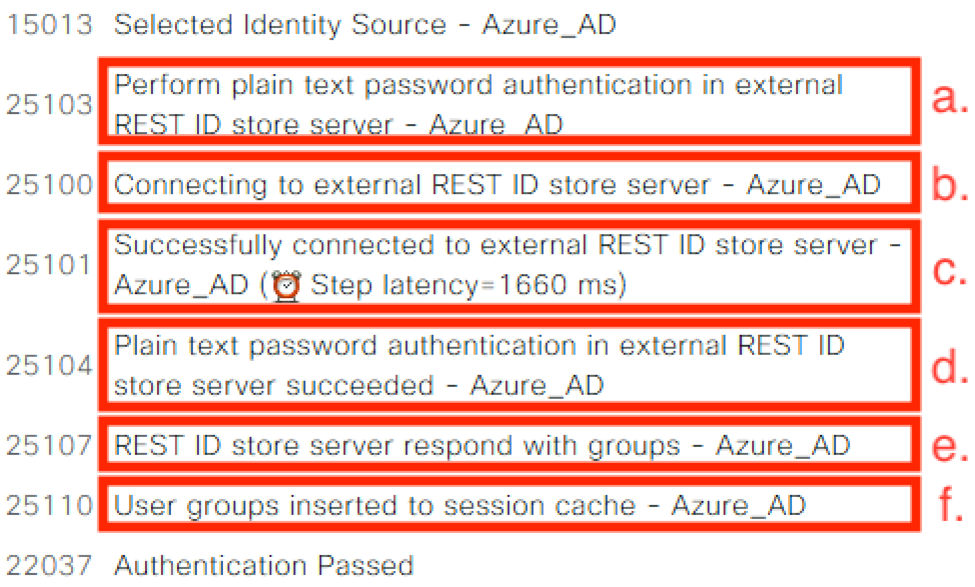
```
skuchere-ise30-1/admin# show application status ise

ISE PROCESS NAME STATE PROCESS ID
--------------------------------------------------------------------
Database Listener running 101790
Database Server running 92 PROCESSES
Application Server running 39355
Profiler Database running 107909
ISE Indexing Engine running 115132
AD Connector running 116376
M&T Session Database running 107694
M&T Log Processor running 112553
Certificate Authority Service running 116226
EST Service running 119875
SXP Engine Service disabled
Docker Daemon running 104217
TC-NAC Service disabled
pxGrid Infrastructure Service disabled
pxGrid Publisher Subscriber Service disabled
pxGrid Connection Manager disabled
pxGrid Controller disabled
PassiveID WMI Service disabled
PassiveID Syslog Service disabled
PassiveID API Service disabled
PassiveID Agent Service disabled
PassiveID Endpoint Service disabled
PassiveID SPAN Service disabled
DHCP Server (dhcpd) disabled
DNS Server (named) disabled
ISE Messaging Service running 104876
ISE API Gateway Database Service running 106853
ISE API Gateway Service running 110426
Segmentation Policy Service disabled

REST Auth Service running 63052


SSE Connector disabled
```

2. Verify that the REST ID store is used at the time of the authentication (check the Steps. section of the detailed authentication report).



```
15013  Selected Identity Source - Azure_AD
25103  Perform plain text password authentication in external
       REST ID store server - Azure_AD
25100  Connecting to external REST ID store server - Azure_AD
25101  Successfully connected to external REST ID store server -
       Azure_AD (⏰ Step latency=1660 ms)
25104  Plain text password authentication in external REST ID
       store server succeeded - Azure_AD
25107  REST ID store server respond with groups - Azure_AD
25110  User groups inserted to session cache - Azure_AD
22037  Authentication Passed
```

a. PSN starts Plain text authentication with selected REST ID store.

b. Connection established with Azure Cloud.

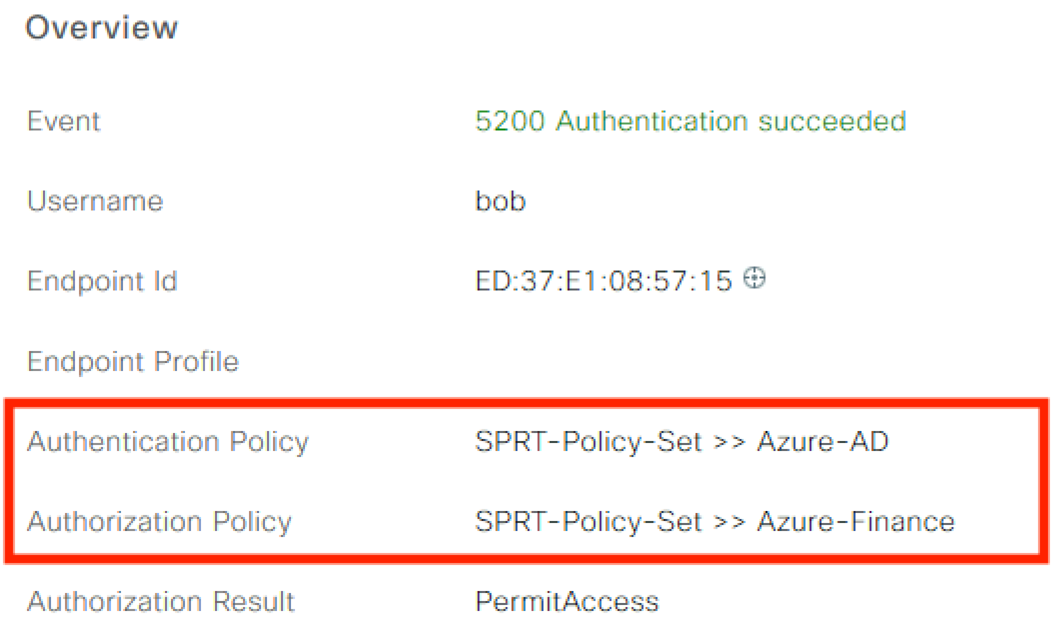
c. Actual authentication step - pay attention to the latency value presented here. In case if all your authentications with the Aure Cloud struggle from significant latency, this affects the other ISE flow, and as a result, the entire ISE deployment becomes unstable.

d. Confirmation of successful authentication.

e. Confirmation of group data presented in response.

f. Session context populated with user group data. For more details about the ISE session management process, consider a review of this article - link.

3. Confirm that expect Authentication/Authorization policies are selected (for this investigate Overview section of the detailed authentication report).



Overview

Event	5200 Authentication succeeded
Username	bob
Endpoint Id	ED:37:E1:08:57:15 ⊕
Endpoint Profile	
Authentication Policy	SPRT-Policy-Set >> Azure-AD
Authorization Policy	SPRT-Policy-Set >> Azure-Finance
Authorization Result	PermitAccess

Figure 30.

Troubleshoot

This section provides the information you can use to troubleshoot your configuration.

Issues with REST Auth Service

In order to troubleshoot any issues with REST Auth Service, you need to start with the review of the **ADE.log** file. Support bundle location - **/support/adeos/ade**

A search keyword for REST Auth Service is - **ROPC-control**.

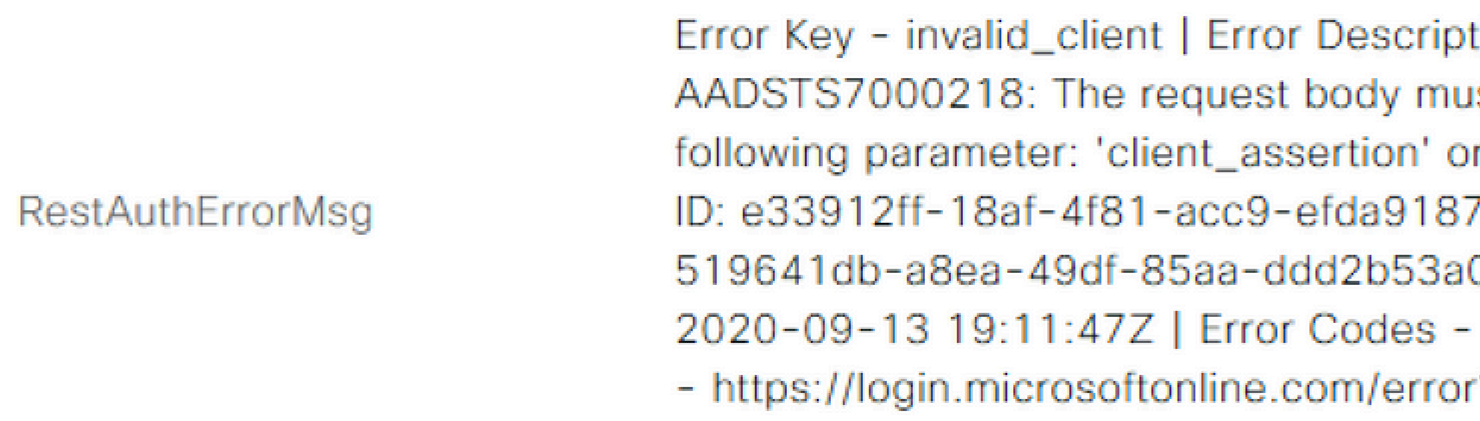
This example shows how REST Auth Service starts:

```
2020-08-30T11:15:38.624197+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] St
2020-08-30T11:15:39.217794+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] in
2020-08-30T11:15:39.290301+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Im
2020-08-30T11:15:39.291858+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Do
2020-08-30T11:15:39.293768+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Lo
2020-08-30T11:15:39.359490+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Er
2020-08-30T11:15:42.789242+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Lo
2020-08-30T11:15:42.830411+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Do
2020-08-30T11:15:42.832131+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Se
2020-08-30T11:15:42.844051+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] in
2020-08-30T11:15:53.479968+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Co
2020-08-30T11:15:55.325973+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Co
2020-08-30T11:15:57.103245+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Co
2020-08-30T11:15:57.105752+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Cr
2020-08-30T11:15:57.278374+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Co
```

In cases when service fails to start or it goes down unexpectedly, it always makes sense to start by review the **ADE.log** around a problematic timeframe.

Issues with REST ID Authentication

In the case of authentication failures when the REST ID store is used, you always need to start from a detailed authentication report. In the Other Attributes area, you are able to see a section - **RestAuthErrorMsg** which contains an error returned by Azure cloud:



RestAuthErrorMsg

Error Key - invalid_client | Error Descript
AADSTS7000218: The request body mus
following parameter: 'client_assertion' or
ID: e33912ff-18af-4f81-acc9-efda9187
519641db-a8ea-49df-85aa-ddd2b53a0
2020-09-13 19:11:47Z | Error Codes -
- https://login.microsoftonline.com/error

Figure 31.

Work with the Log Files

In ISE 3.0 due to the Controlled Introduction of REST ID feature, debugs for it enabled by default.
All REST ID related logs are stored in ROPC files which can be viewed over CLI:

```
skuchere-ise30-1/admin# sh logging application | i ropc
755573 Oct 04 2020 09:10:29 ropc/ropc.log

skuchere-ise30-1/admin# sh logging application ropc/ropc.log
23:49:31.449 [http-nio-9601-exec-6] DEBUG c.c.i.r.c.ROPCController - Starting ROPC auth flow
23:49:31.788 [http-nio-9601-exec-6] DEBUG c.c.i.r.u.ScimUtility - Found user and pass in the SCIM filte
```

On ISE 3.0 with the installed patch, notice that the filename is rest-id-store.log and not ropc.log. The previous search example provided works because the folder name did not change.

Or those files can be extracted from the ISE support bundle.

Here are a couple of log examples that show different working and non-working scenarios:

1. Certificate error when the Azure Graph is not trusted by the ISE node. This error can be seen when groups do not load in the REST ID store setting.

```
20:44:54.420 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start proxy load for URI 'https:

20:44:54.805 [http-nio-9601-exec-7] ERROR c.c.i.r.p.a.AzureIdentityProviderFacade - Couldn't fetch appli
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: No trusted certificate f
at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
at sun.security.ssl.SSLSocketImpl.fatal(SSLSocketImpl.java:1946)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:316)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:310)
at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1639)
```

This issue indicates that the Microsoft graph API certificate is not trusted by ISE. ISE 3.0.0.458 does not have a DigiCert Global Root G2 CA installed in the trusted store. This is documented in the defect

- Cisco bug ID CSCvv80297 To address this issue you need to install DigiCert Global Root G2 CA in ISE trusted store and mark it as trusted for Cisco services.

The certificate can be downloaded from here - https://www.digicert.com/kb/digicert-root-certificates.htm

2. Wrong application secret.

```
10:57:53.200 [http-nio-9601-exec-1] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tru
10:57:54.205 [http-nio-9601-exec-1] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Stat
10:57:54.206 [http-nio-9601-exec-1] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.InvalidApplicationAuthException: AADSTS7000215: Invalid client se
Trace ID: 99cc29f7-502a-4aaa-b2cf-1daeb071b900
Correlation ID: a697714b-5ab2-4bd1-8896-f9ad40d625e5
Timestamp: 2020-09-29 09:01:36Z - Error Codes: [7000215]
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateApplication(AzureIdentityP
```

3. Wrong APP ID.

```
21:34:36.090 [http-nio-9601-exec-4] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tru
21:34:36.878 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Stat
21:34:36.879 [http-nio-9601-exec-4] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.InvalidApplicationAuthException: AADSTS700016: Application with i
Trace ID: 6dbd0fdd-0128-4ea8-b06a-5e78f37c0100
Correlation ID: eced0c34-fcc1-40b9-b033-70e5abe75985
Timestamp: 2020-08-31 19:38:34Z - Error Codes: [700016]
```

4. User not found.

```
10:43:01.351 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Stat
10:43:01.352 [http-nio-9601-exec-2] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_grant","error_desc
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

5. User password expired - typically can happen for the newly created user as the password defined by Azure admin needs to be changed at the time of the login to Office365.

```
10:50:55.096 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Stat
10:50:55.097 [http-nio-9601-exec-4] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_grant","error_desc
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.GeneratedMethodAccessor53.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

6. Groups cannot be loaded due to wrong API permissions.

```
12:40:06.624 [http-nio-9601-exec-9] ERROR c.c.i.r.u.RestUtility - Error response in 'GET' request. Statu
"error": {
"code": "Authorization_RequestDenied",
"message": "Insufficient privileges to complete the operation.",
"innerError": {
"date": "2020-08-30T10:43:59",
"request-id": "da458fa4-cc8a-4ae8-9720-b5370ad45297"
}
}
}'
```

7. Authentication fails when ROPC is not allowed on the Azure side.

```
11:23:10.824 [http-nio-9601-exec-2] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tru
11:23:11.776 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Stat
11:23:11.777 [http-nio-9601-exec-2] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_client","error_desc
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.GeneratedMethodAccessor53.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

8. Authentication fails since the user does not belong to any group on the Azure side.

```
21:54:55.976 [http-nio-9601-exec-5] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tru
21:54:57.312 [http-nio-9601-exec-5] ERROR c.c.i.r.p.a.AzureROPCFlow - Missing claims in the id token: "n
21:54:57.313 [http-nio-9601-exec-5] ERROR c.c.i.r.c.ROPCController - Server Error
com.cisco.ise.ROPC.entities.exceptions.JsonParseException: Json exception: Missing claims in the id toke
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.validateIdTokenPayload(AzureROPCFlow.java:93)
```

9. Succesful user authentication and group retrieval.

```
11:46:03.035 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Starting ROPC auth flow
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.ScimUtility - Found user and pass in the SCIM filter
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Getting the right ROPC handler for
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Getting user groups from handler
11:46:03.038 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start building http client
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start proxy load for URI 'https:
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start check if host is bypass
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Iterating bypass hosts '192.168.
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Proxy server found with address
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start adding proxy credentials t
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - No credentials found for proxy
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - Created SSLContext with TLSv1.2
11:46:03.041 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tru
11:46:04.160 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - The ROPCHandlerResponse is: {
"schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:User" ],
"userName" : "username",
"name" : {
"formatted" : "bob"
},
"displayName" : "bob",
"groups" : [ {
"value" : "17db2c79-fb87-4027-ae13-88eb5467f25b"
} ],
"roles" : [ ]
}
```