Configure ISE 3.2 EAP-TLS with Microsoft Azure Active Directory

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

- Network Diagram
- Procedure
- Configurations
  - ISE Configuration
  - Configure the Certificate Authentication Profile
  - User Configuration

Verify

- ISE Verification

Troubleshoot

- Enable Debugs on ISE
- Log Snippets

Introduction

This document describes how to configure and troubleshoot authorization policies in ISE based on Azure AD group membership with EAP-TLS or TEAP.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Identity Services Engine (ISE)
- Microsoft Azure AD, subscription, and apps
- EAP-TLS authentication

Components Used

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

- Cisco ISE 3.2
- Microsoft Azure AD

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.

Background Information

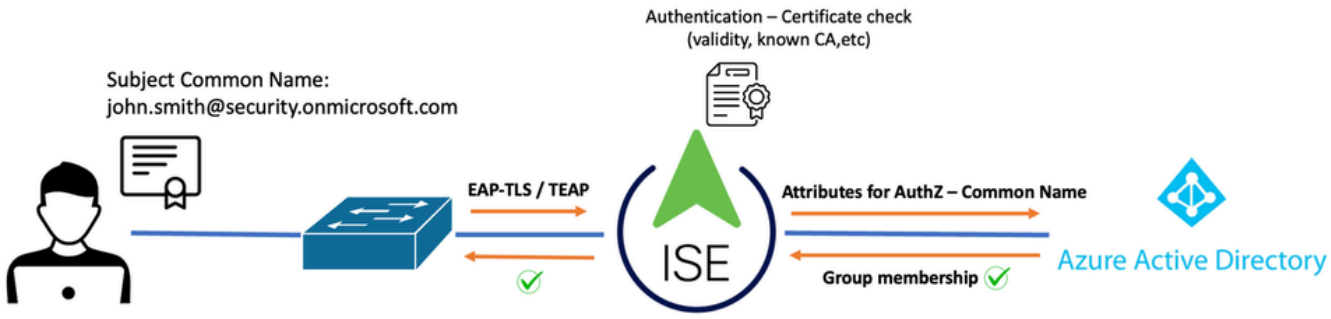
In ISE 3.0 it is possible to leverage the integration between ISE and Azure Active Directory (AAD) to authenticate the users based on Azure AD groups and attributes through Resource Owner Password Credentials (ROPC) communication. With ISE 3.2, you can configure certificate-based authentication and users can be authorized based on azure AD group memberships and other attributes. ISE queries Azure through graph API to fetch groups and attributes for the authenticated user, it uses the certificate's Subject Common Name (CN) against User Principal name (UPN) on the Azure side.

Note: The certificate-based authentications can be either EAP-TLS or TEAP with EAP-TLS as the inner method. Then, you can select attributes from Azure Active Directory and add them to the Cisco ISE dictionary. These attributes can be used for authorization. Only user authentication is supported.

Configure

Network Diagram

The next image provides an example of a network diagram and traffic flow:



Procedure

1. The certificate is sent to ISE through EAP-TLS or TEAP with EAP-TLS as the inner method.
2. ISE evaluates the user's certificate (validity period, trusted CA, CRL, and so on.)
3. ISE takes the certificate subject name (CN) and performs a look-up to the Microsoft Graph API to fetch the user's groups and other attributes for that user. This is referred to as User Principal name (UPN) on the Azure side.
4. ISE Authorization policies are evaluated against the user's attributes returned from Azure.

Note: You must configure and grant the Graph API permissions to ISE app in Microsoft Azure as shown below:

API / Permissions name	Type	Description
Microsoft Graph (3)		
Group.Read.All	Application	Read all groups
User.Read	Delegated	Sign in and read user profile
User.Read.All	Application	Read all users' full profiles

Configurations

ISE Configuration

Note: ROPC functionality and Integration between ISE with Azure AD is out of the scope of this document. It is important that groups and user attributes are added from Azure. See the configuration guide.

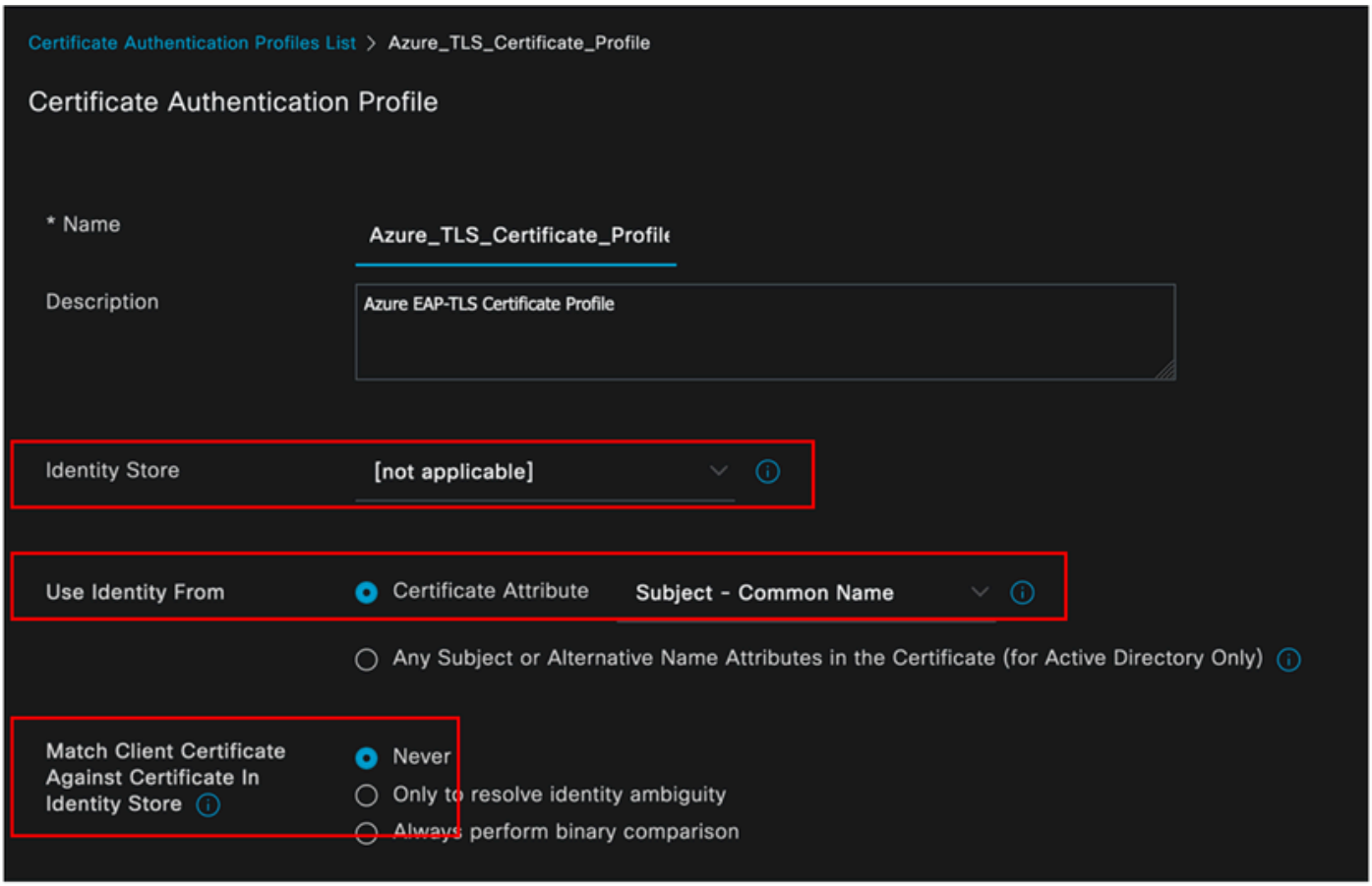
Configure the Certificate Authentication Profile



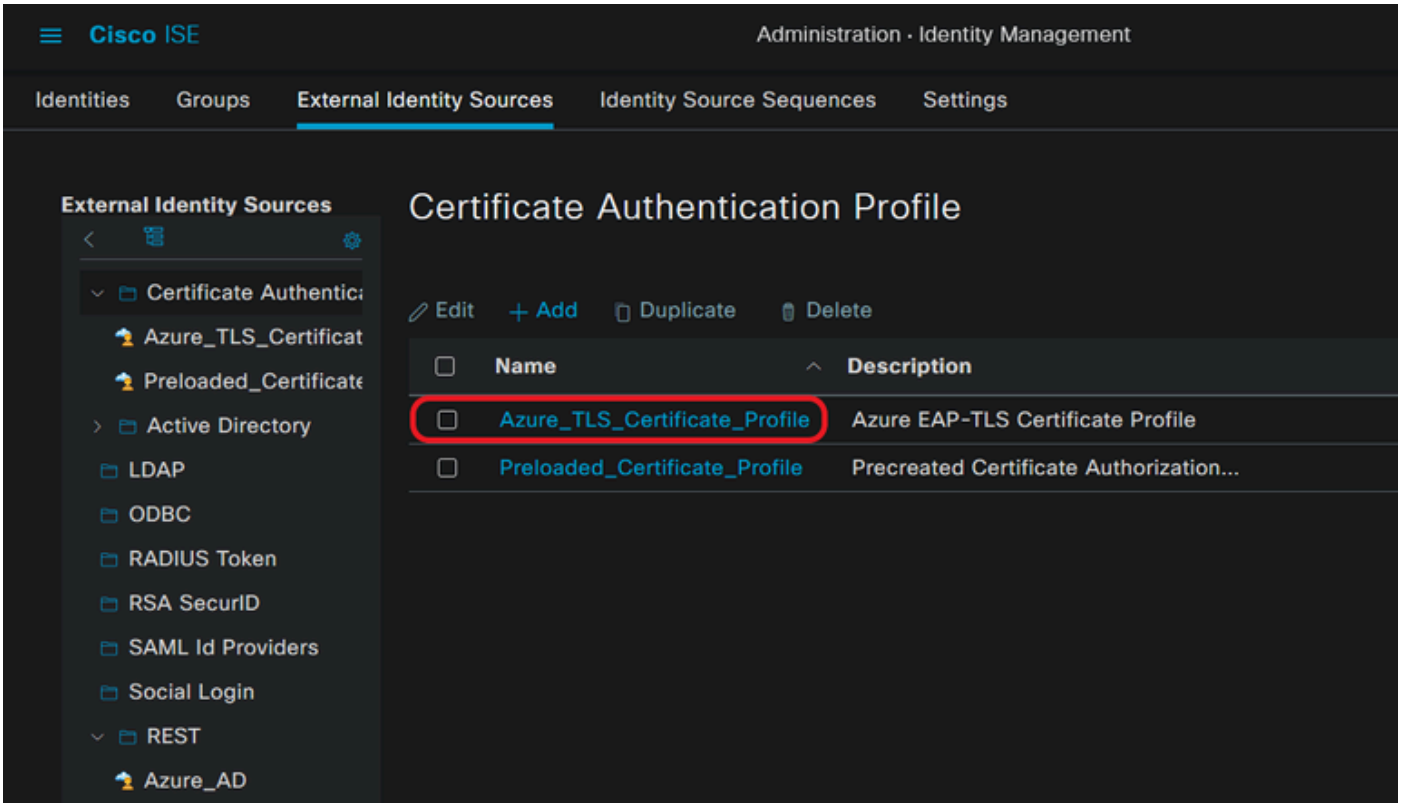
Step 1. Navigate to the Menu icon located in the upper left corner and select **Administration > Identity Management > External Identity sources**.

Step 2. Select **Certificate Authentication** Profile and then click on **Add**.

Step 3. Define the name. Set the **Identity Store** as [Not applicable], and select Subject – Common Name on **Use Identity From** field. Select Never on Match **Client Certificate against Certificate in Identity Store** Field.



Step 4. Click **Save**:



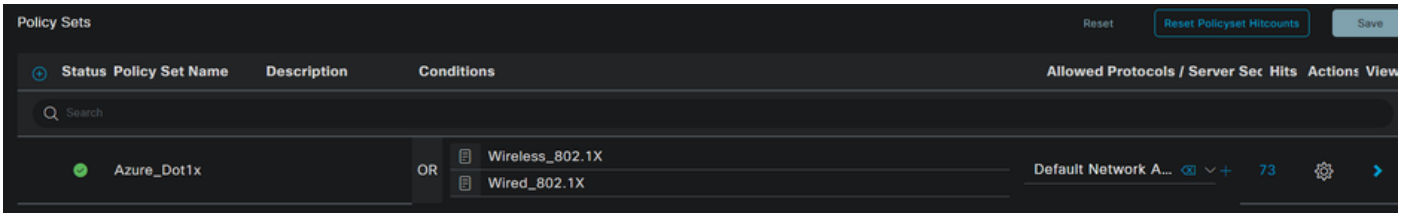
Step 5. Navigate to the Menu icon



located in the upper left corner and select **Policy > Policy Sets**.

Step 6. Select the plus

icon to create a new policy set. Define a name and select Wireless 802.1x or wired 802.1x as conditions. The Default Network Access option is used in this example:

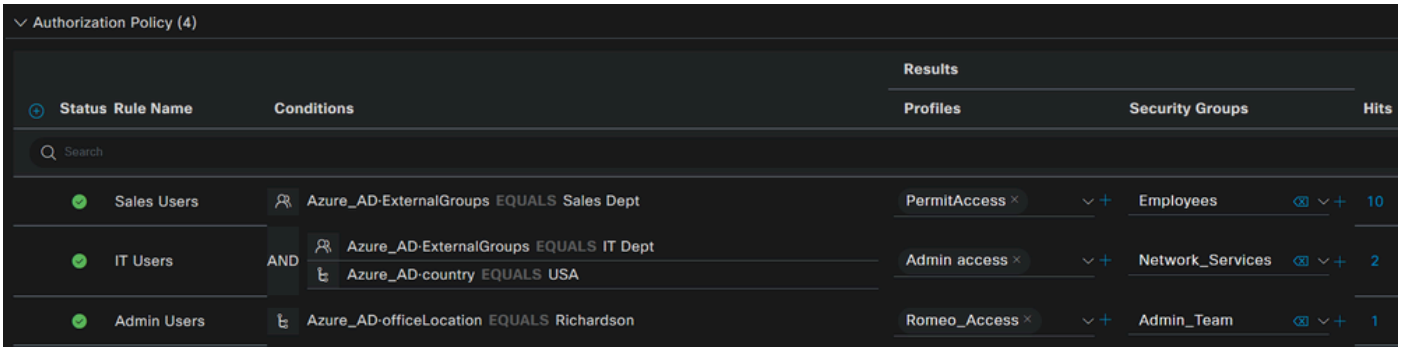


Step 7. Select the arrow
next to Default Network Access to configure Authentication and Authorization Policies.

Step 8. Select the Authentication Policy option, define a name and add EAP-TLS as Network Access EAPAuthentication, it is possible to add TEAP as Network Access EAPTunnel if TEAP is used as the authentication protocol. Select the Certificate Authentication Profile created on step 3 and click **Save**.

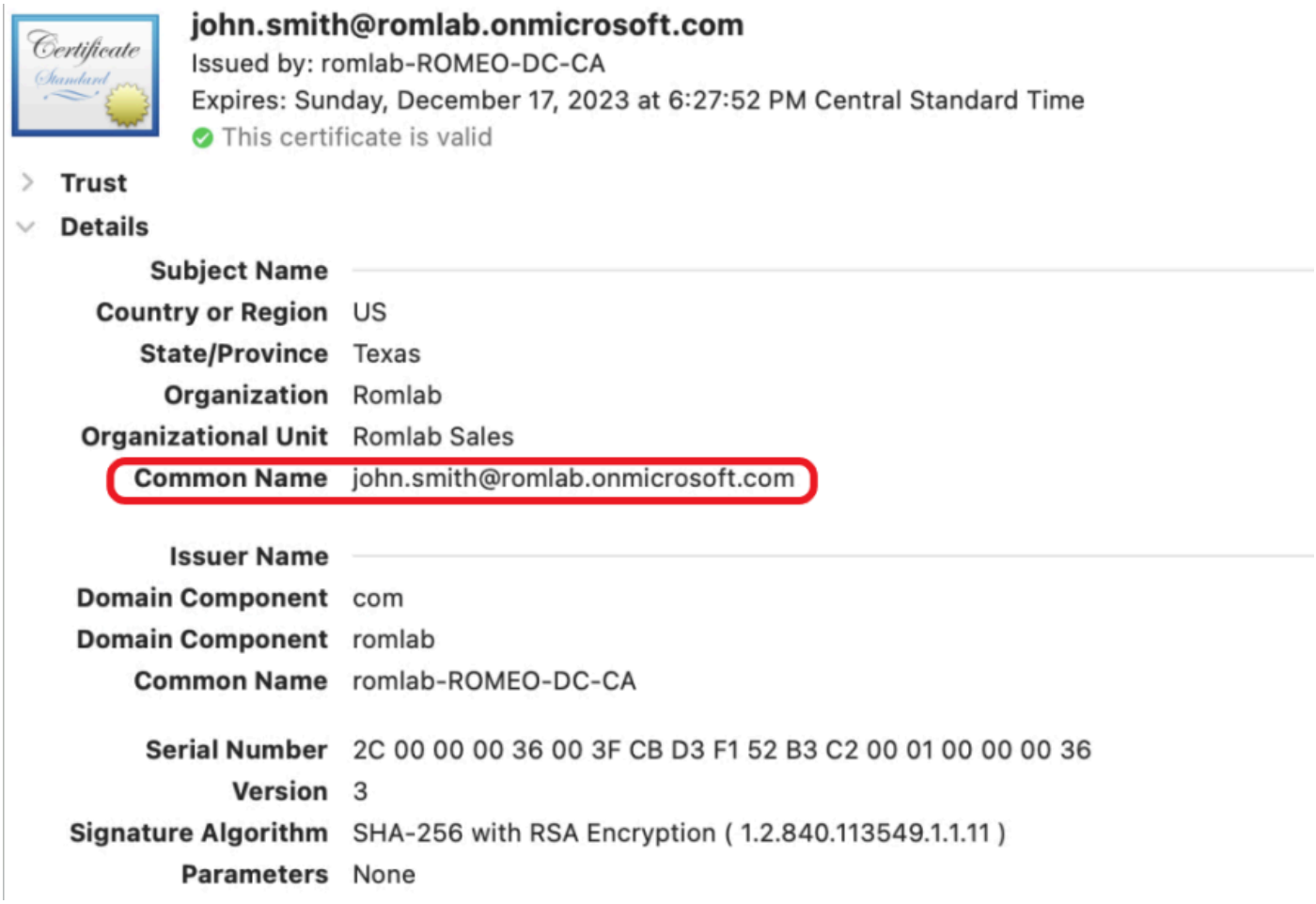


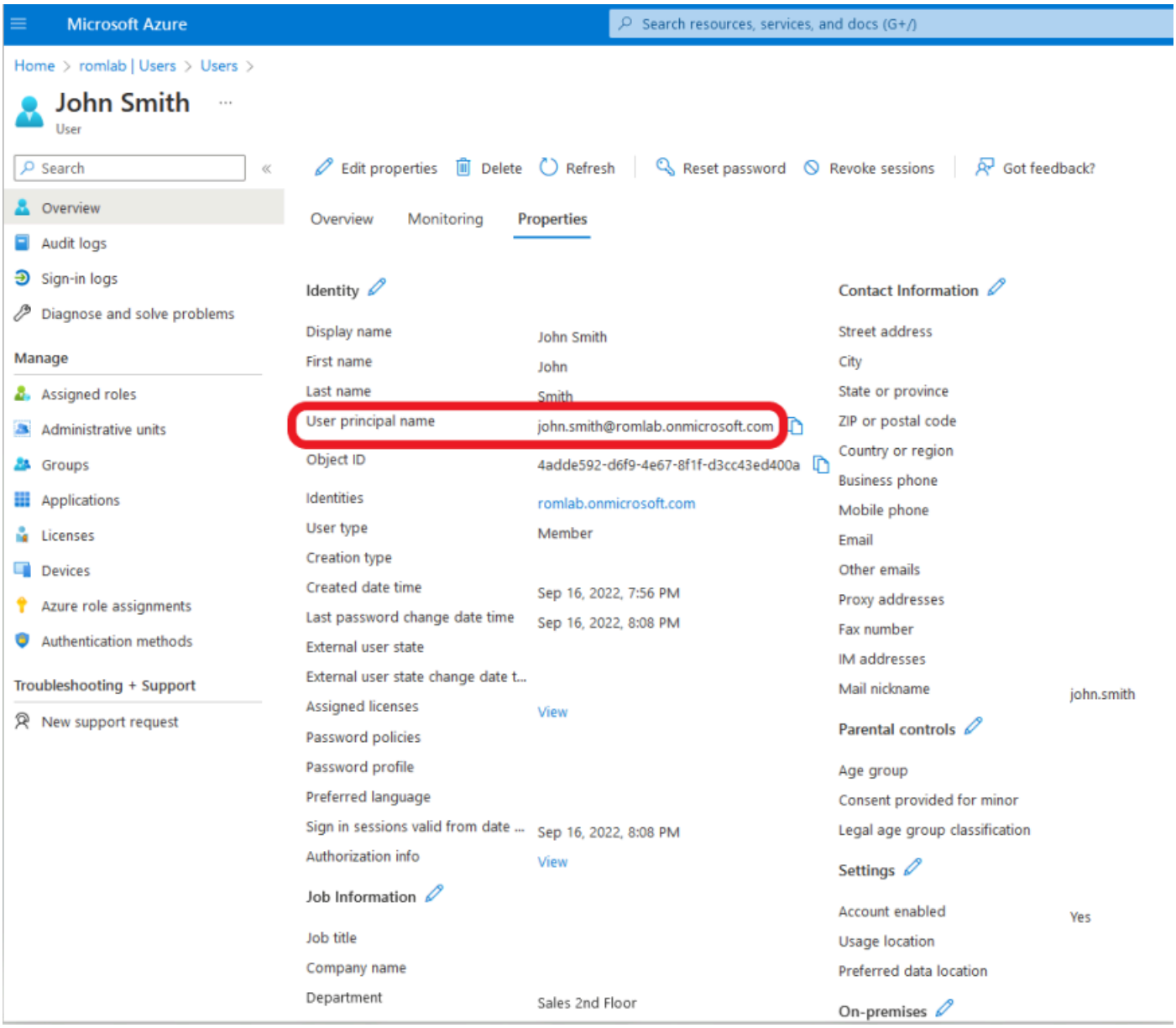
Step 9. Select the Authorization Policy option, define a name and add Azure AD group or user attributes as a condition. Choose the profile or security group under Results, depends on the use case, then click **Save**.



User Configuration

The Subject Common Name (CN) from the user certificate must match the User Principal Name (UPN) on the Azure side in order to retrieve AD group Membership and user attributes that be used in authorization rules. For the authentication to be successful, the root CA and any intermediate CAs certificates must be in ISE Trusted Store.



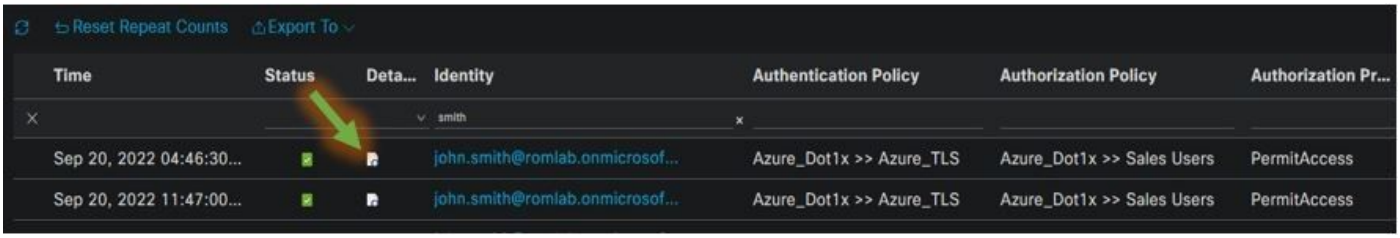


Verify

ISE Verification

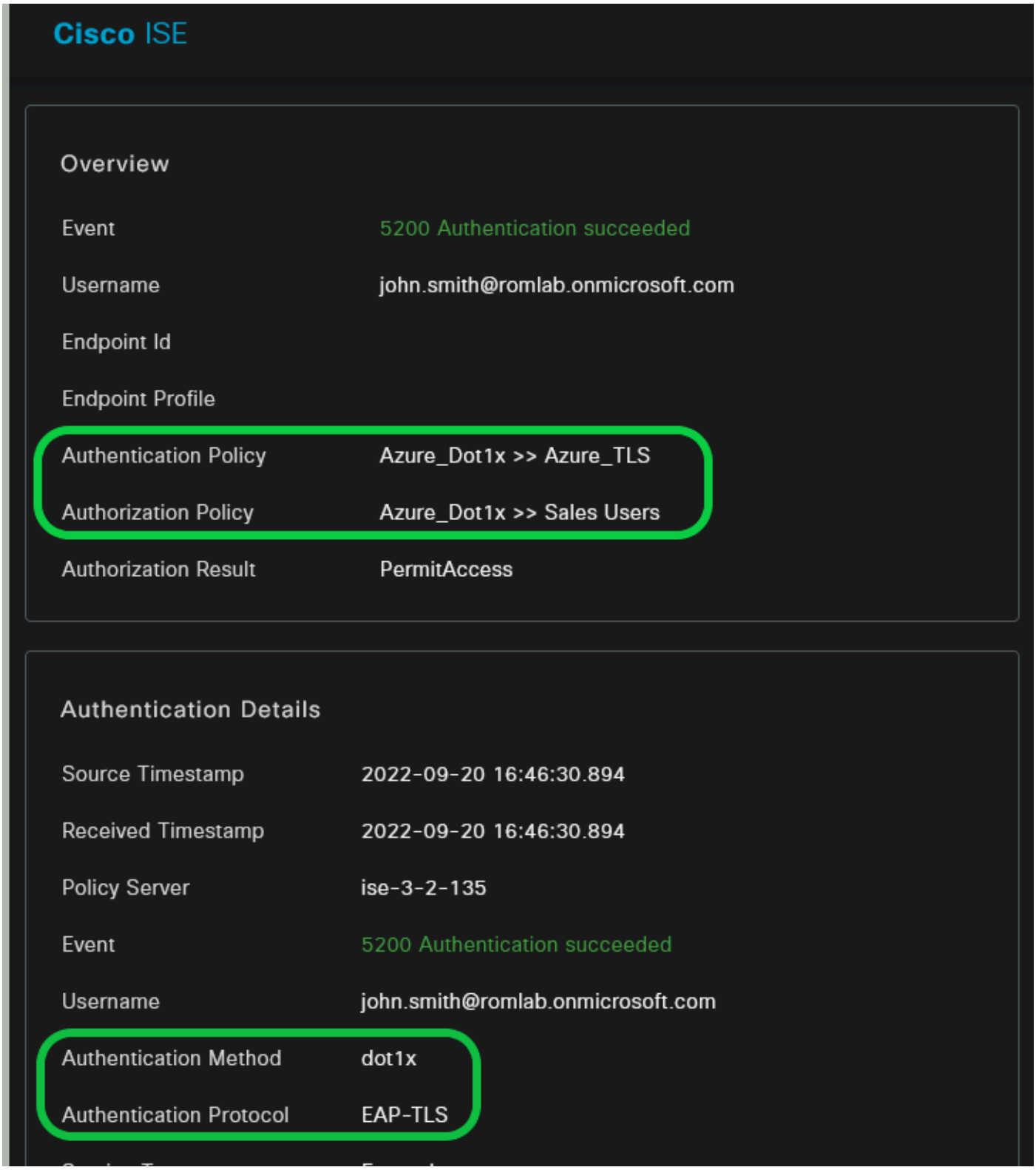
In the Cisco ISE GUI, click the Menu icon

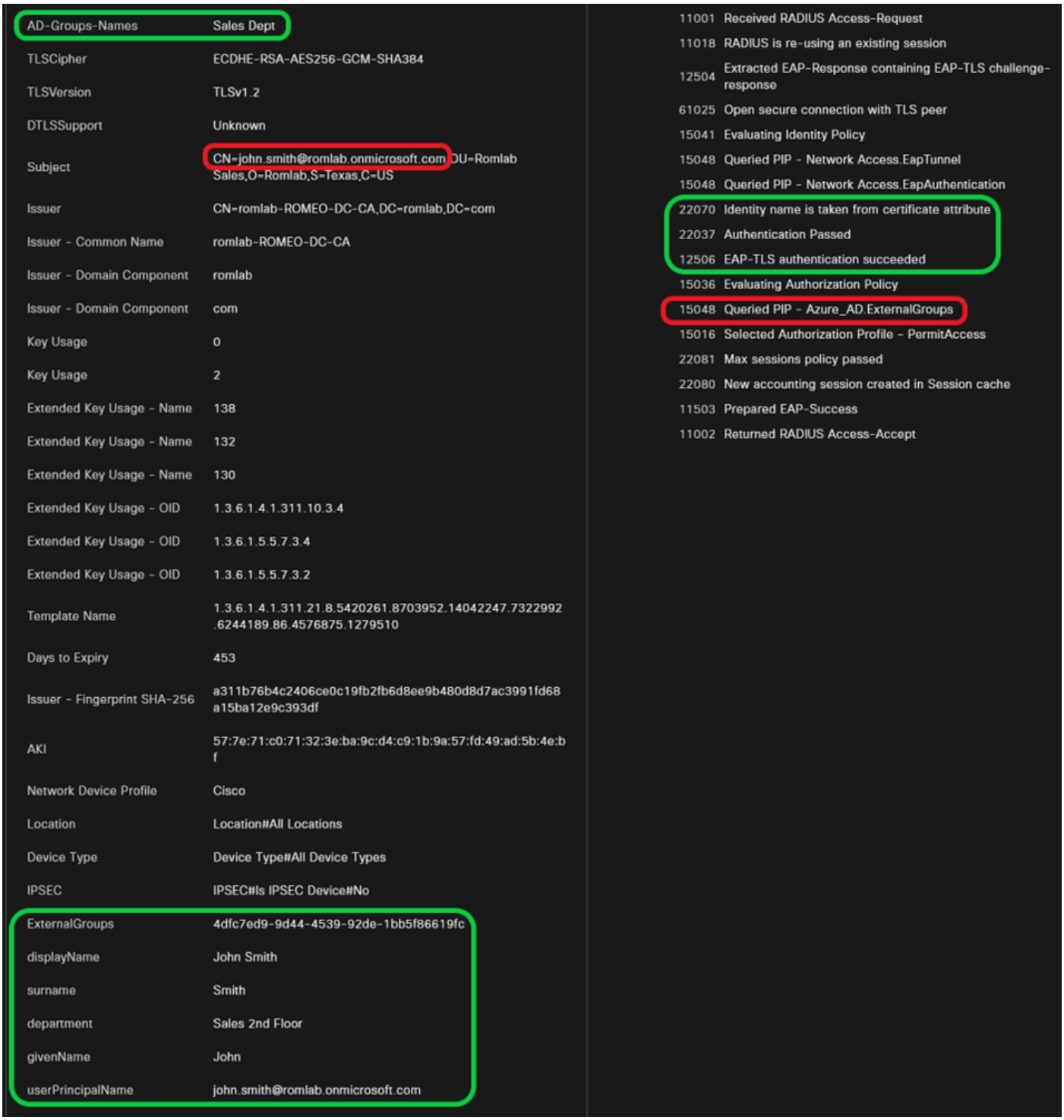
and choose **Operations > RADIUS > Live Logs for network authentications (RADIUS)**.



Click the magnifier icon in the Details column to view a detailed authentication report and confirm if the flow works as expected.

1. Verify Authentication/Authorization policies.
2. Authentication method/protocol.
3. User’s subject name taken from the certificate.
4. User groups and other attributes fetched from Azure directory.


Cisco ISE
Overview
Event
5200 Authentication succeeded
Username
john.smith@romlab.onmicrosoft.com
Endpoint Id
Endpoint Profile
Authentication Policy
Azure_Dot1x >> Azure_TLS
Authorization Policy
Azure_Dot1x >> Sales Users
Authorization Result
PermitAccess
Authentication Details
Source Timestamp
2022-09-20 16:46:30.894
Received Timestamp
2022-09-20 16:46:30.894
Policy Server
ise-3-2-135
Event
5200 Authentication succeeded
Username
john.smith@romlab.onmicrosoft.com
Authentication Method
dot1x
Authentication Protocol
EAP-TLS



Troubleshoot

Enable Debugs on ISE

Navigate to **Administration > System > Logging > Debug Log Configuration** to set the next components to the specified level.

Node	Component Name	Log Level	Log Filename
PSN	rest-id-store	Debug	rest-id-store.log

PSN	runtime-AAA	Debug	prrt-server.log

Note: When you are done with troubleshooting, remember to reset the debugs. To do so, select the related node and click **Reset to Default**.

Log Snippets

The next excerpts show the last two phases in the flow, as mentioned earlier in the network diagram section.

1. ISE takes the certificate subject name (CN) and performs a look-up to the Azure Graph API to fetch user's groups and other attributes for that user. This is referred to as User Principal name (UPN) on Azure side.
2. ISE Authorization policies are evaluated against the user attributes returned from Azure.

Rest-id logs:

```
2022-09-20 16:46:30,424 INFO  [http-nio-9601-exec-10] cisco.ise.ropc.controllers.ClientCredController -::- UPN:
john.smith@romlab.onmicrosoft.com , RestIdStoreName: Azure_AD, Attrname: ExternalGroups,city,companyName,country,department,
displayName,employeeId,givenName,officeLocation,state,surname,userPrincipalName

2022-09-20 16:46:30,424 DEBUG [http-nio-9601-exec-10]ise.ropc.providers.cache.IdpKeyValueCacheInitializer -::::- Found access token

2022-09-20 16:46:30,424 DEBUG [http-nio-9601-exec-10] ise.ropc.providers.azure.AzureIdentityProviderFacade -::- User Lookup by UPN
john.smith@romlab.onmicrosoft.com

2022-09-20 16:46:30,425 DEBUG [http-nio-9601-exec-10]ise.ropc.providers.azure.AzureIdentityProviderFacade -::- Lookup url
https://graph.microsoft.com/v1.0/users/john.smith@romlab.onmicrosoft.com?$select=ExternalGroups,city,companyName,country,depart
ment,displayName,employeeId,givenName,officeLocation,state,surname,userPrincipalName

2022-09-20 16:46:30,425 DEBUG [http-nio-9601-exec-10]cisco.ise.ropc.utilities.HttpClientWrapper -::- Start building http client for uri
https://graph.microsoft.com/v1.0/users/john.smith@romlab.onmicrosoft.com?$select=ExternalGroups
,city,companyName,country,department,displayName,employeeId,givenName,officeLocation,state,surname,userPrincipalName

2022-09-20 16:46:30,660 DEBUG [http-nio-9601-exec-10] ise.ropc.providers.azure.AzureIdentityProviderFacade -::- UserAttribute size 11

2022-09-20 16:46:30,661 DEBUG [http-nio-9601-exec-10] cisco.ise.ropc.utilities.HttpClientWrapper -::- Start building http client for uri
https://graph.microsoft.com/v1.0/users/john.smith@romlab.onmicrosoft.com/transitiveMemberOf/microsoft.graph.group

2022-09-20 16:46:30,876 DEBUG [http-nio-9601-exec-10][[]] ise.ropc.providers.azure.AzureIdentityProviderFacade -::- UserGroups size 1
```

Prrt logs:

```
2022-09-20 16:46:30,182 DEBUG  [Thread-759][[]] cisco.cpm.prrt.impl.PrRTCpmBridge -::::- ---- Running Authorization Policy ----

2022-09-20 16:46:30,252 DEBUG  [Thread-759][[]] cisco.cpm.prrt.impl.PrRTCpmBridge -::::- setting sessionCache attribute
CERTIFICATE.Subject - Common Name to john.smith@romlab.onmicrosoft.com

2022-09-20 16:46:30,253 DEBUG  [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::- [RestIdentityProviderPIP] has been called
by PIP manager: dictName: Azure_AD attrName: Azure_AD.ExternalGroups context: NonStringifiableExecutionContext inputs:

2022-09-20 16:46:30,408 DEBUG  [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::- checking attrList
ExternalGroups,city,companyName,country,department,displayName,employeeId,givenName,officeLocation,state,surname,userPrincipalNa
me

2022-09-20 16:46:30,408 DEBUG  [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::-  Username from the Context
john.smith@romlab.onmicrosoft.com

2022-09-20 16:46:30,880 DEBUG  [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::-  userAttr size 11
...
2022-09-20 16:46:30,881 DEBUG  [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::-  userAttr update in context & map, Key :
Azure_AD.department value Sales 2nd Floor

2022-09-20 16:46:30,881 DEBUG  [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::-  userAttr update in context & map, Key :
Azure_AD.displayName value John Smith
2022-09-20 16:46:30,881 DEBUG  [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::-  userAttr update in context & map, Key :
Azure_AD.givenName value John
2022-09-20 16:46:30,881 DEBUG  [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::-  userAttr update in context & map, Key :
Azure_AD.surname value Smith

2022-09-20 16:46:30,881 DEBUG  [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::-  userAttr update in context & map, Key :
Azure_AD.userPrincipalName value john.smith@romlab.onmicrosoft.com

2022-09-20 16:46:30,881 DEBUG  [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::-  userGroup 1

2022-09-20 16:46:30,882 DEBUG  [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::- Group value  4dfc7ed9-9d44-4539-92de-
1bb5f86619fc group name Sales Dept
```