Configure ISE 3.2 EAP-TLS with Microsoft Azure Active Directory

Contents

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

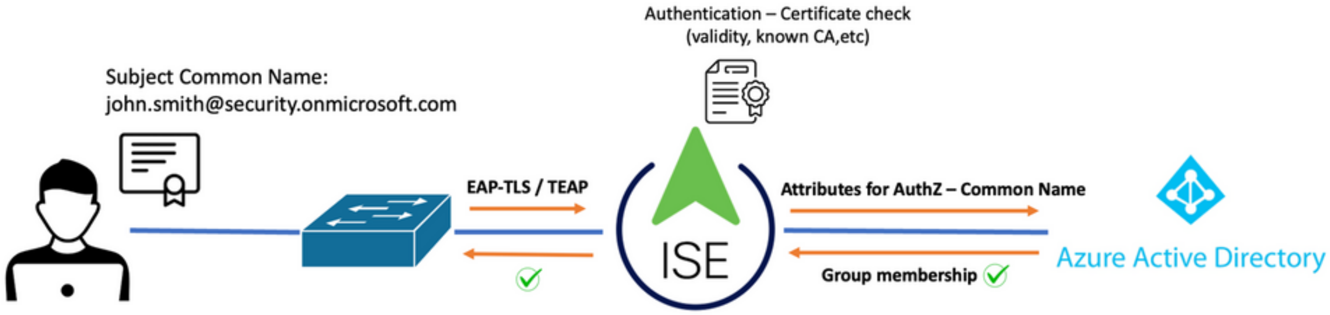
In ISE 3.0 it is possible to leverage the integration between ISE and Azure Active Directory (AAD) to authenticate the users based on Azure AD groups and attributes through Resource Owner Password Credentials (ROPC) communication. With ISE 3.2, you can configure certificate-based authentication and users 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

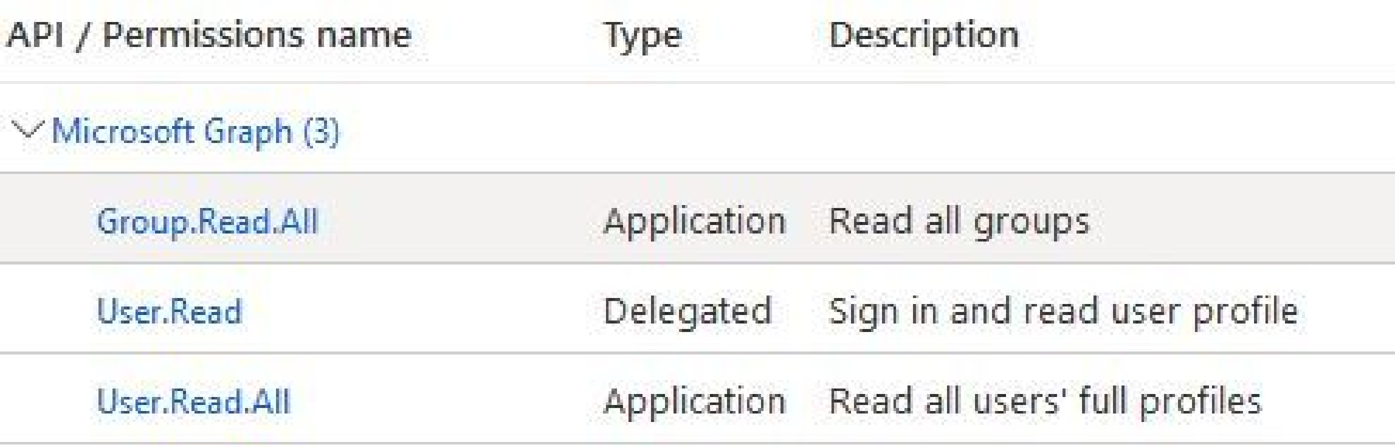
The next image provides an example of a network diagram and traffic flow


Authentication – Certificate check
(validity, known CA,etc)
Subject Common Name:
john.smith@security.onmicrosoft.com
EAP-TLS / TEAP
ISE
Attributes for AuthZ – Common Name
Group membership
Azure Active Directory

<u>Procedure</u>:

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

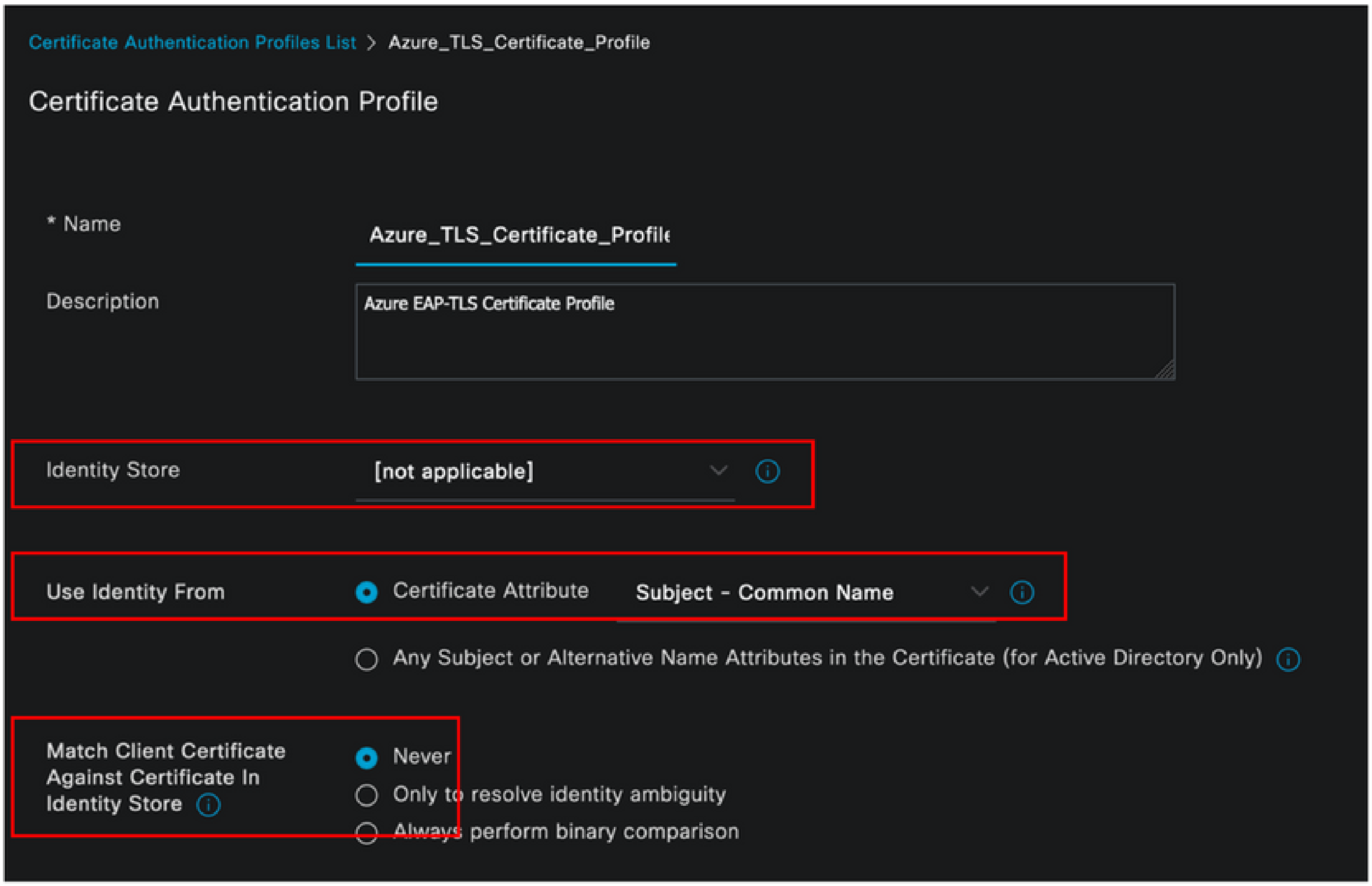
Note: ROPC functionality and Integration between ISE with Azure AD is out of the scope of this document. It is important that groups and user attributes are added from Azure. See configuration guide here.

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.


Certificate Authentication Profiles List > Azure_TLS_Certificate_Profile

Certificate Authentication Profile

* Name: Azure_TLS_Certificate_Profile

Description: Azure EAP-TLS Certificate Profile

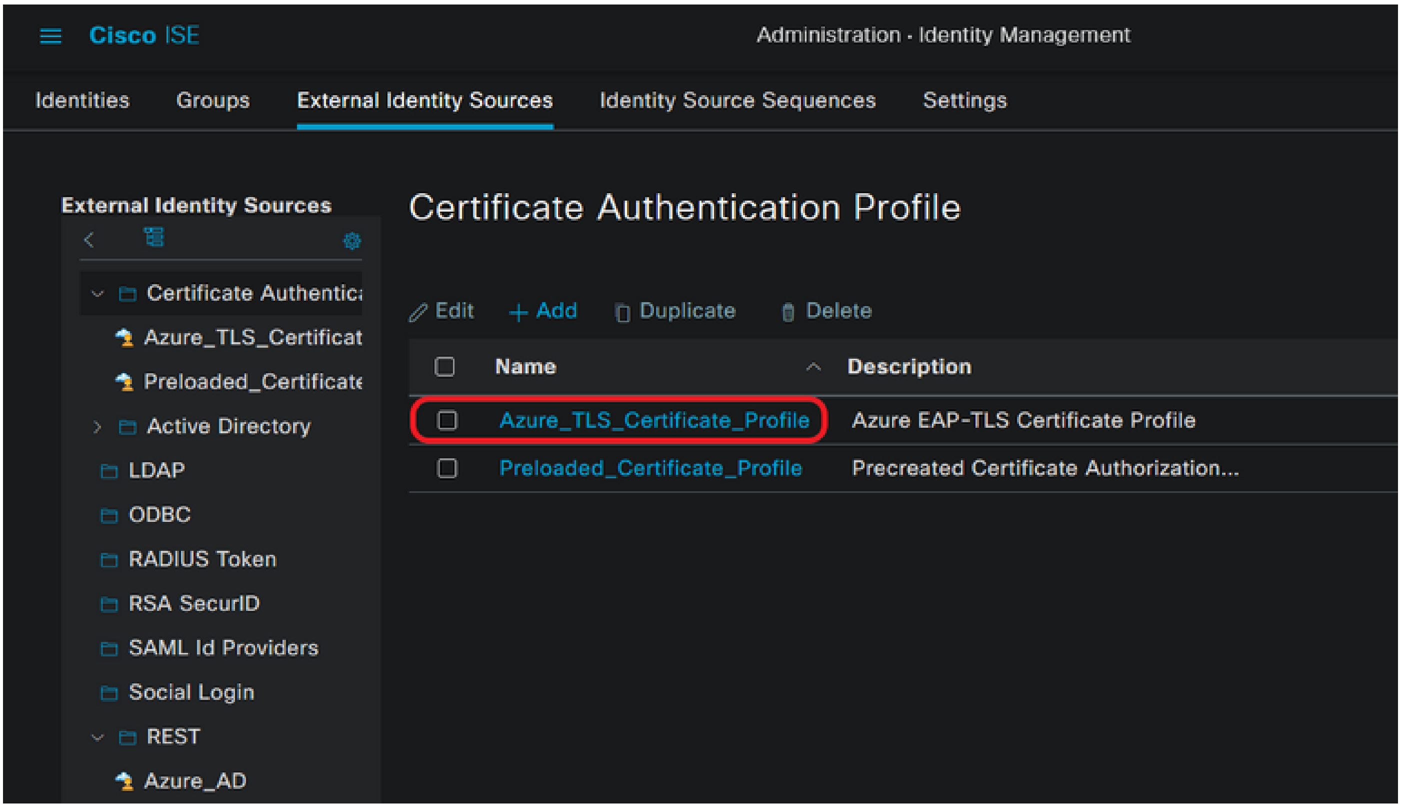
Identity Store: [not applicable]

Use Identity From: ● Certificate Attribute Subject - Common Name

○ Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate In Identity Store:
● Never
○ Only to resolve identity ambiguity
○ Always perform binary comparison

Step 4. Click on **Save**



Certificate Authentication Profile

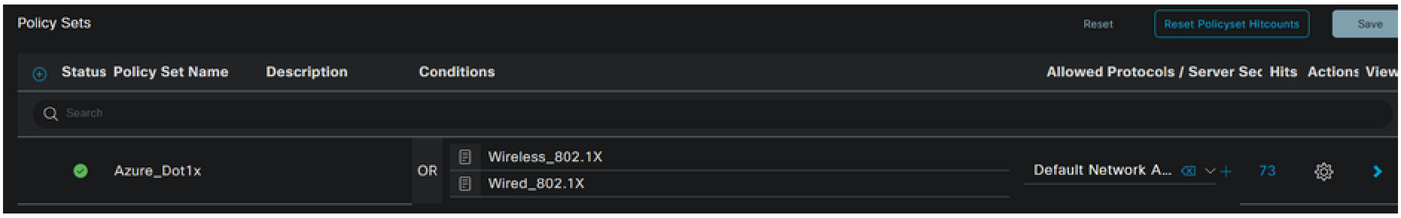
	Name	Description
□	Azure_TLS_Certificate_Profile	Azure EAP-TLS Certificate Profile
□	Preloaded_Certificate_Profile	Precreated Certificate Authorization...

Step 5. Navigate to the Menu icon

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

Step 6. Select the plus

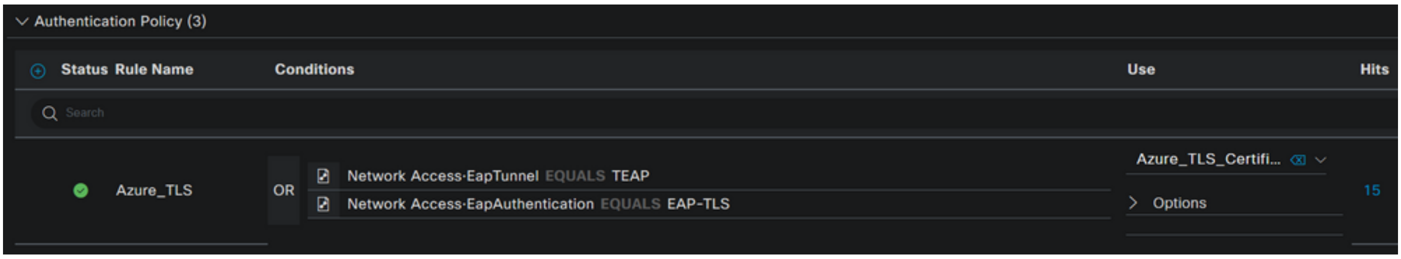
icon to create a new policy set. Define a name and select Wireless 802.1x or wired 802.1x as conditions. The Default Network Access option is used in this example



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sec	Hits	Actions	View
●	Azure_Dot1x		OR Wireless_802.1X Wired_802.1X	Default Network A...	73	⚙	›

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

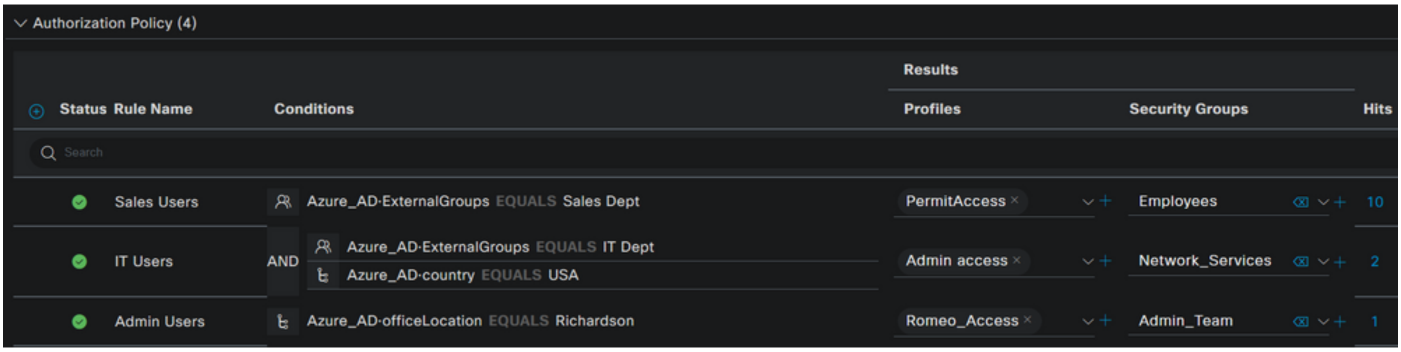
Step 8. Select the Authentication Policy option, define a name and add EAP-TLS as Network Access EAPAuthentication, it is possible to add TEAP as Network Access EAPTunnel if TEAP is used as the authentication protocol. Select the Certificate Authentication Profile created on step 3 and click on **Save**.



Authentication Policy (3)

Status	Rule Name		Conditions	Use	Hits
●	Azure_TLS	OR	Network Access·EapTunnel EQUALS TEAP Network Access·EapAuthentication EQUALS EAP-TLS	Azure_TLS_Certifi... Options	15

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, and then click **Save**.

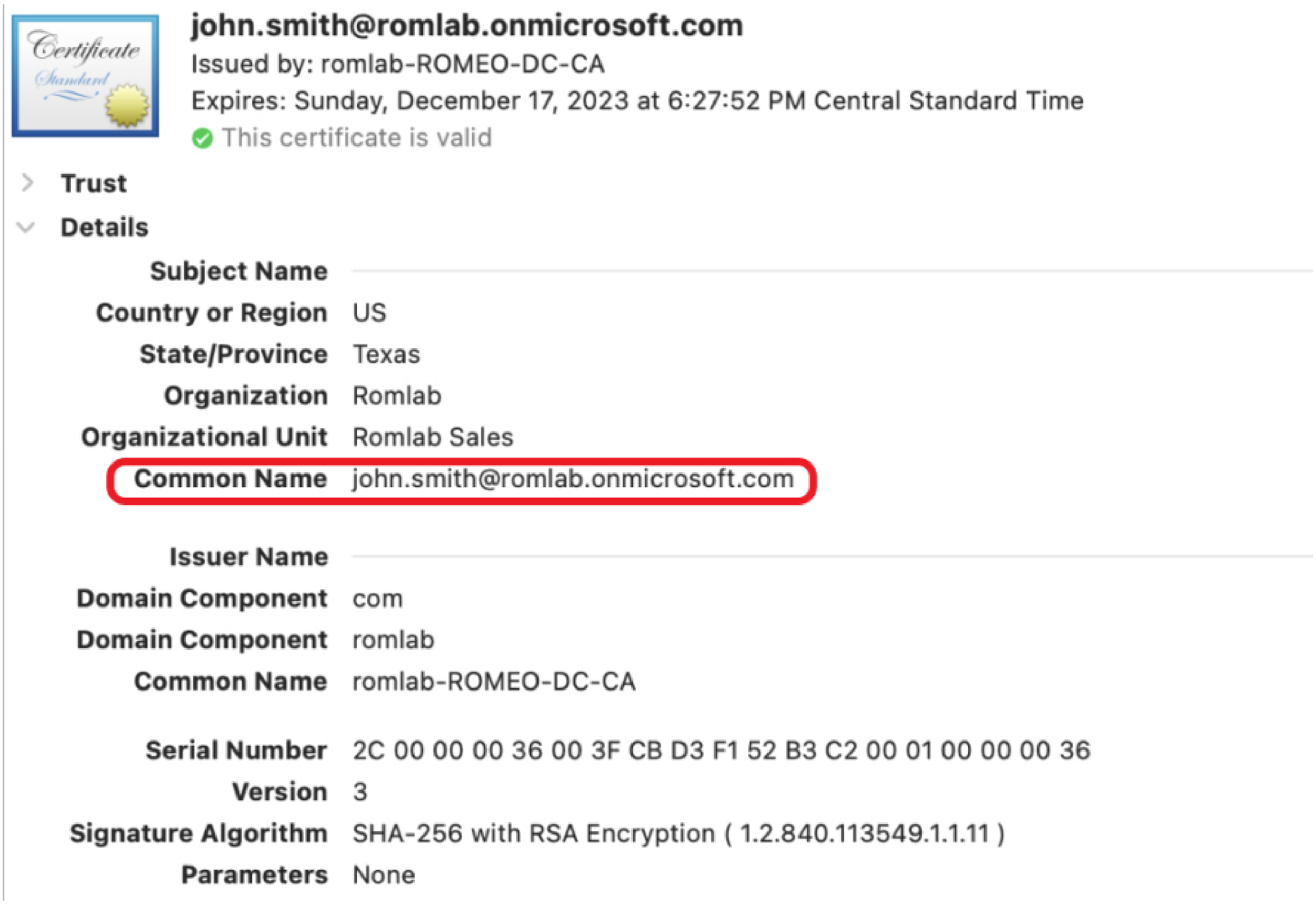


Authorization Policy (4)

				Results		
Status	Rule Name		Conditions	Profiles	Security Groups	Hits
●	Sales Users		Azure_AD·ExternalGroups EQUALS Sales Dept	PermitAccess	Employees	10
●	IT Users	AND	Azure_AD·ExternalGroups EQUALS IT Dept Azure_AD·country EQUALS USA	Admin access	Network_Services	2
●	Admin Users		Azure_AD·officeLocation EQUALS Richardson	Romeo_Access	Admin_Team	1

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.

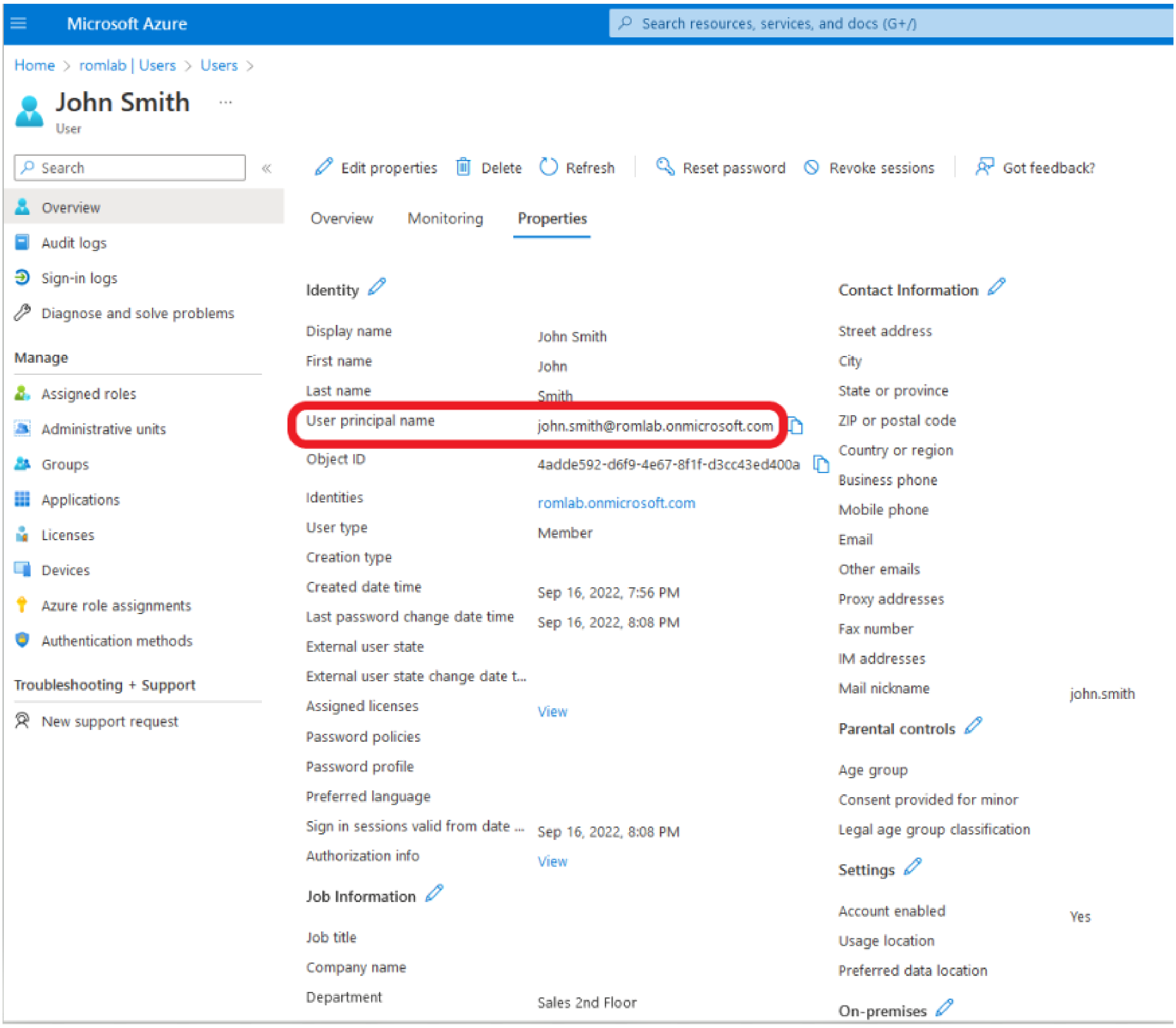


john.smith@romlab.onmicrosoft.com
Issued by: romlab-ROMEO-DC-CA
Expires: Sunday, December 17, 2023 at 6:27:52 PM Central Standard Time
✓ This certificate is valid

> Trust

⌄ Details

Subject Name	
Country or Region	US
State/Province	Texas
Organization	Romlab
Organizational Unit	Romlab Sales
Common Name	john.smith@romlab.onmicrosoft.com
Issuer Name	
Domain Component	com
Domain Component	romlab
Common Name	romlab-ROMEO-DC-CA
Serial Number	2C 00 00 00 36 00 3F CB D3 F1 52 B3 C2 00 01 00 00 00 36
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	None



Identity

Display name John Smith

First name John

Last name Smith

User principal name john.smith@romlab.onmicrosoft.com

Object ID 4adde592-d6f9-4e67-8f1f-d3cc43ed400a

Identities romlab.onmicrosoft.com

User type Member

Creation type

Created date time Sep 16, 2022, 7:56 PM

Last password change date time Sep 16, 2022, 8:08 PM

External user state

External user state change date t...

Assigned licenses View

Password policies

Password profile

Preferred language

Sign in sessions valid from date ... Sep 16, 2022, 8:08 PM

Authorization info View

Job Information

Job title

Company name

Department Sales 2nd Floor

Contact Information

Street address

City

State or province

ZIP or postal code

Country or region

Business phone

Mobile phone

Email

Other emails

Proxy addresses

Fax number

IM addresses

Mail nickname john.smith

Parental controls

Age group

Consent provided for minor

Legal age group classification

Settings

Account enabled Yes

Usage location

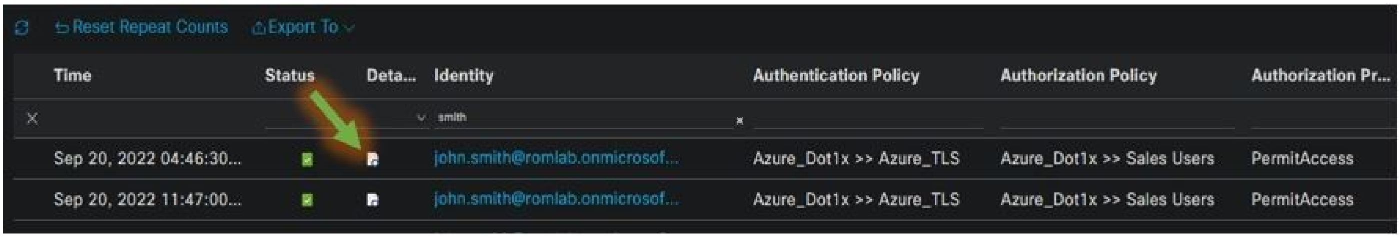
Preferred data location

On-premises

Verify

ISE verification

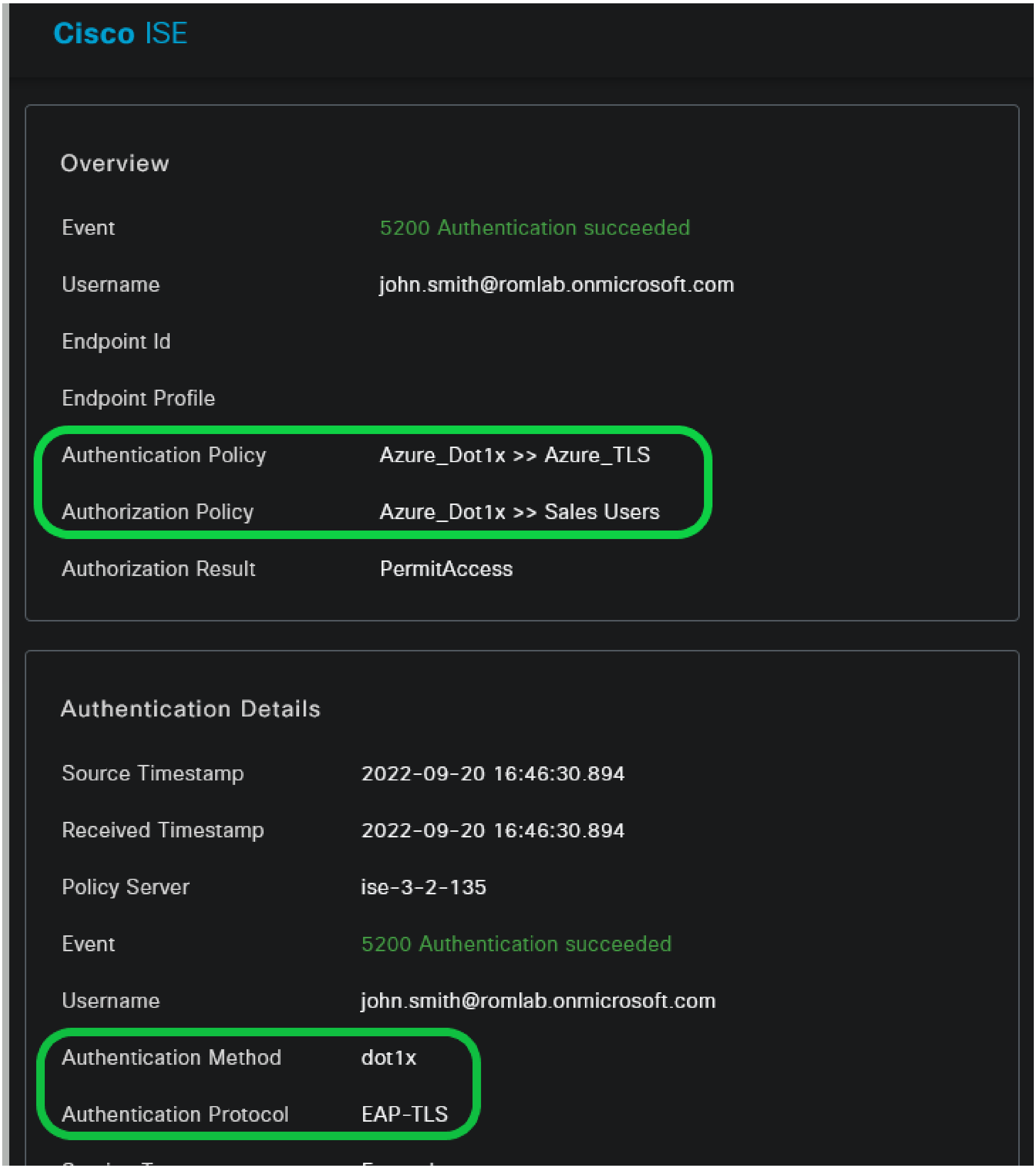
In the Cisco ISE GUI, click the Menu icon and choose **Operations > RADIUS > Live Logs for network authentications (RADIUS).**



Time	Status	Deta...	Identity	Authentication Policy	Authorization Policy	Authorization Pr...
			smith			
Sep 20, 2022 04:46:30...	✓		john.smith@romlab.onmicrosof...	Azure_Dot1x >> Azure_TLS	Azure_Dot1x >> Sales Users	PermitAccess
Sep 20, 2022 11:47:00...	✓		john.smith@romlab.onmicrosof...	Azure_Dot1x >> Azure_TLS	Azure_Dot1x >> Sales Users	PermitAccess

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



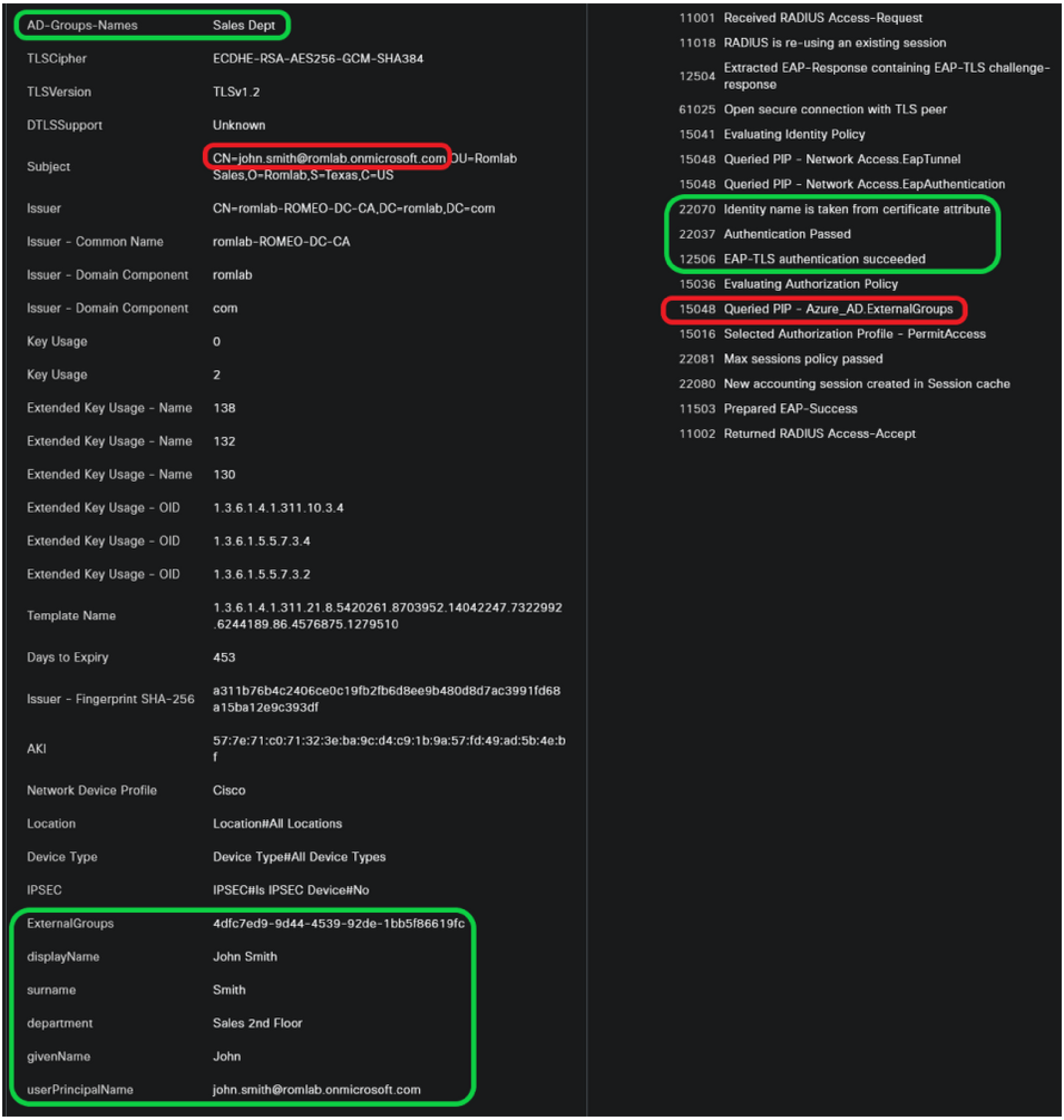
Cisco ISE

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



AD-Groups-Names	Sales Dept
TLSCipher	ECDHE-RSA-AES256-GCM-SHA384
TLSVersion	TLSv1.2
DTLSSupport	Unknown
Subject	CN=john.smith@romlab.onmicrosoft.com,OU=Romlab Sales,O=Romlab,S=Texas,C=US
Issuer	CN=romlab-ROMEO-DC-CA,DC=romlab,DC=com
Issuer - Common Name	romlab-ROMEO-DC-CA
Issuer - Domain Component	romlab
Issuer - Domain Component	com
Key Usage	0
Key Usage	2
Extended Key Usage - Name	138
Extended Key Usage - Name	132
Extended Key Usage - Name	130
Extended Key Usage - OID	1.3.6.1.4.1.311.10.3.4
Extended Key Usage - OID	1.3.6.1.5.5.7.3.4
Extended Key Usage - OID	1.3.6.1.5.5.7.3.2
Template Name	1.3.6.1.4.1.311.21.8.5420261.8703952.14042247.7322992.6244189.86.4576875.1279510
Days to Expiry	453
Issuer - Fingerprint SHA-256	a311b76b4c2406ce0c19fb2fb6d8ee9b480d8d7ac3991fd68a15ba12e9c393df
AKI	57:7e:71:c0:71:32:3e:ba:9c:d4:c9:1b:9a:57:fd:49:ad:5b:4e:bf
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
ExternalGroups	4dfc7ed9-9d44-4539-92de-1bb5f86619fc
displayName	John Smith
surname	Smith
department	Sales 2nd Floor
givenName	John
userPrincipalName	john.smith@romlab.onmicrosoft.com

```
11001  Received RADIUS Access-Request
11018  RADIUS is re-using an existing session
12504  Extracted EAP-Response containing EAP-TLS challenge-
       response
61025  Open secure connection with TLS peer
15041  Evaluating Identity Policy
15048  Queried PIP - Network Access.EapTunnel
15048  Queried PIP - Network Access.EapAuthentication
22070  Identity name is taken from certificate attribute
22037  Authentication Passed
12506  EAP-TLS authentication succeeded
15036  Evaluating Authorization Policy
15048  Queried PIP - Azure_AD.ExternalGroups
15016  Selected Authorization Profile - PermitAccess
22081  Max sessions policy passed
22080  New accounting session created in Session cache
11503  Prepared EAP-Success
11002  Returned RADIUS Access-Accept
```

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

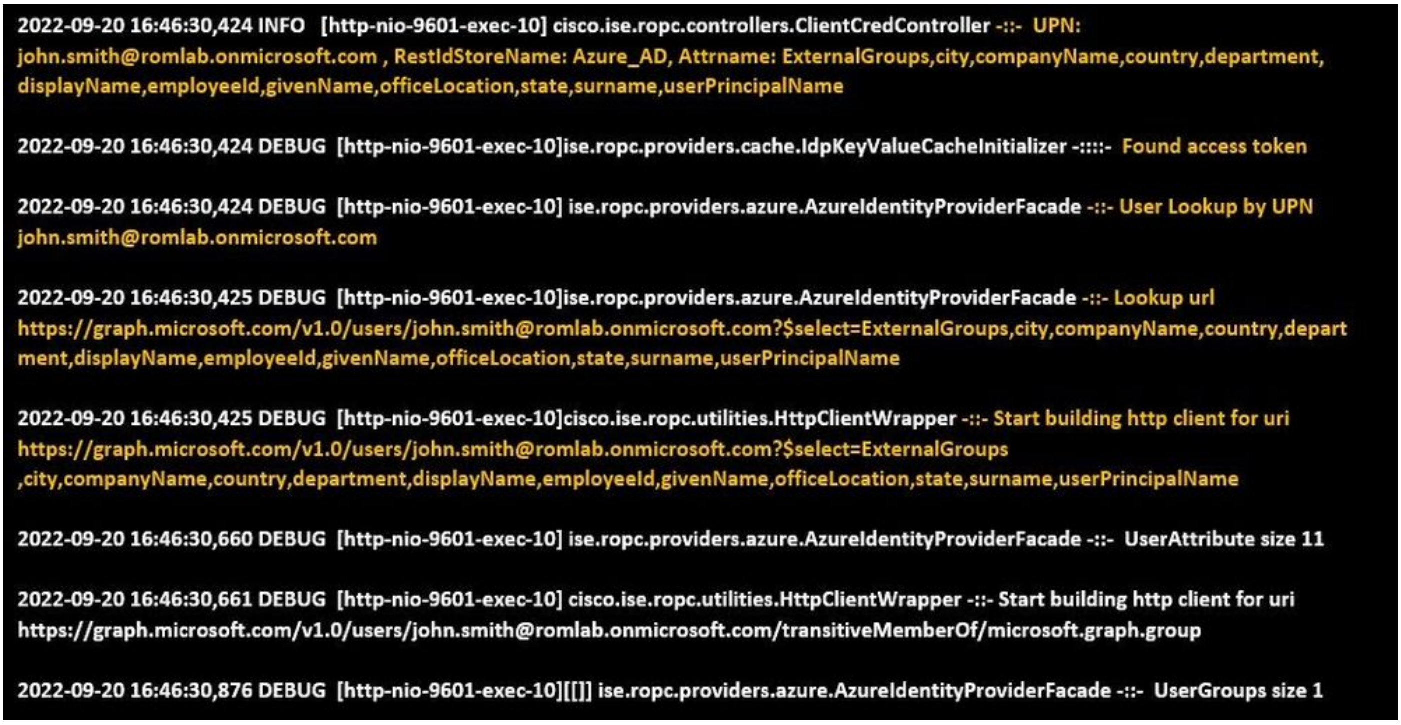
Note: When you are done with troubleshooting, remember to reset the debugs. To do so select the related node and click "Reset to Default".

Logs Snippets

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

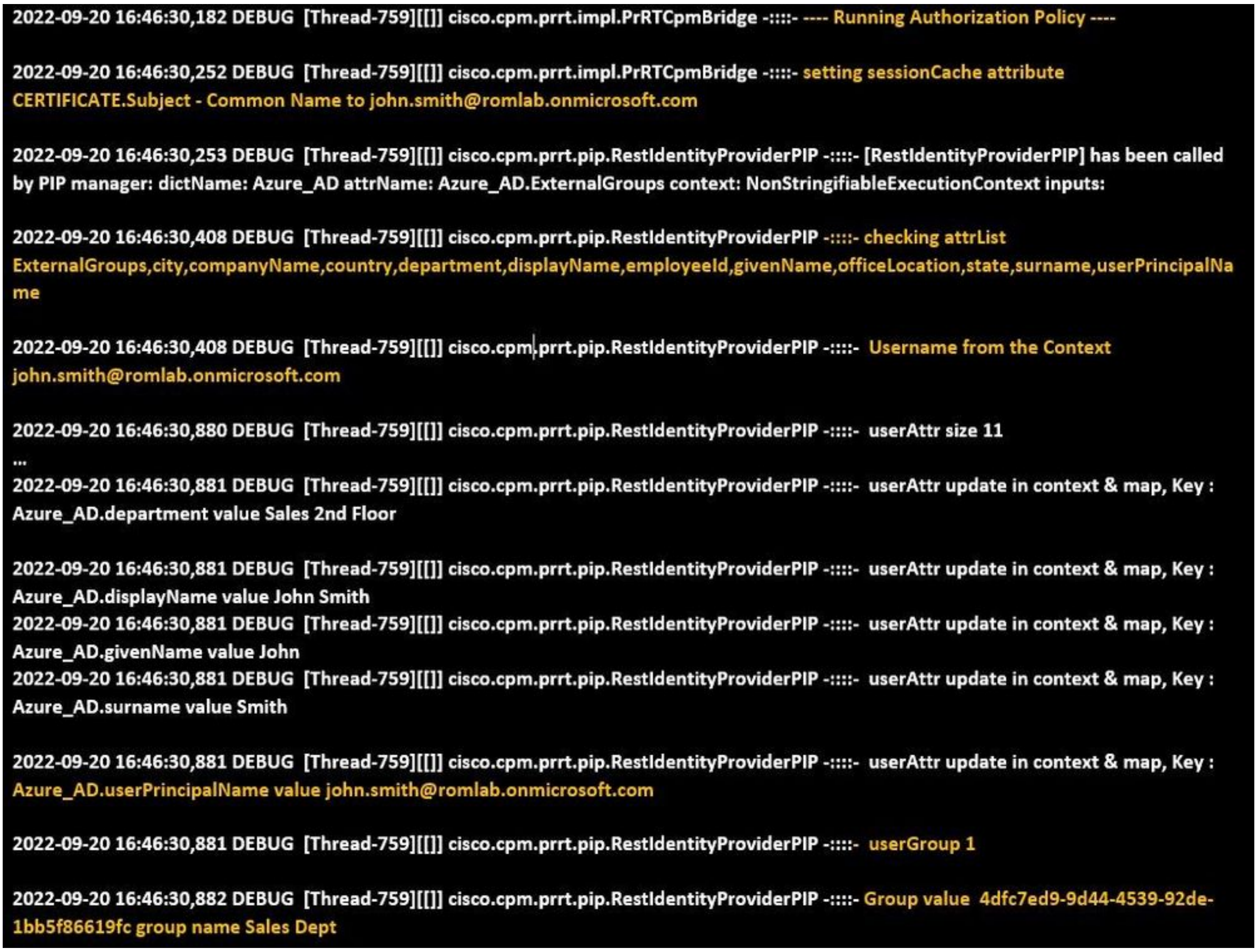
1. ISE takes the certificate subject name (CN) and performs a look-up to the Azure Graph API to fetch user's groups and other attributes for that user. This is referred to as User Principal name (UPN) on Azure side.
2. ISE Authorization policies are evaluated against the user's attributes returned from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