

使用Microsoft Azure Active Directory配置Cisco ISE 3.2 EAP-TLS

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

简介

本文档介绍如何根据Azure AD组成员身份和其他用户属性，将EAP-TLS或TEAP作为身份验证协议，在ISE中配置授权策略并进行故障排除。

作者：安全咨询工程师Emmanuel Cano和技术咨询工程师Romeo Migisha

先决条件

要求

Cisco 建议您了解以下主题：

- 身份服务引擎 (ISE)
- Microsoft Azure AD、订阅和应用
- EAP-TLS 身份验证

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ISE 3.2
- Microsoft Azure AD

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

在ISE 3.0中，可以利用ISE与Azure Active Directory(AAD)之间的集成，通过资源所有者密码凭证(ROPC)通信根据Azure AD组和属性对用户进行身份验证。使用ISE 3.2，您可以配置基于证书的身份验证，用户可以根据Azure AD组成员身份和其他属性获得授权。ISE通过图形API查询Azure以获

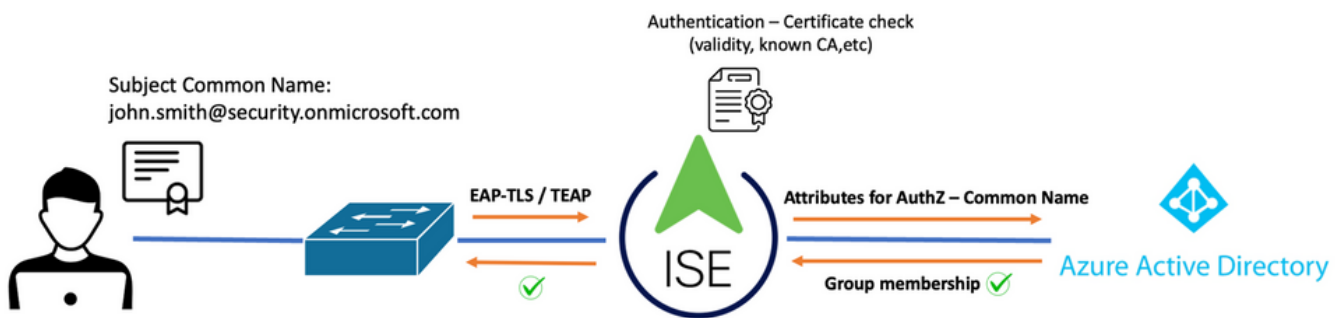
取经过身份验证的用户的组和属性，它根据Azure端的用户主体名称(UPN)使用证书的使用者公用名(CN)。

注意：基于证书的身份验证可以是EAP-TLS或将EAP-TLS作为内部方法的TEAP。然后，您可以从Azure Active Directory选择属性并将其添加到思科ISE词典。这些属性可用于授权。仅支持用户身份验证。

配置

网络图

下图提供了网络图和流量传输的示例



步骤:

1. 证书通过EAP-TLS或TEAP发送到ISE，EAP-TLS作为内部方法。
2. ISE评估用户的证书（有效期、受信任CA、CRL等。）
3. ISE获取证书使用者名称(CN)并执行查找Microsoft Graph API以获取用户的组以及该用户的其它属性。这在Azure端称为用户主体名称(UPN)。
4. ISE授权策略根据从Azure返回的用户属性进行评估。

注意：您必须在Microsoft Azure中配置并授予ISE应用的图形API权限，如下所示：


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

配置

ISE 配置

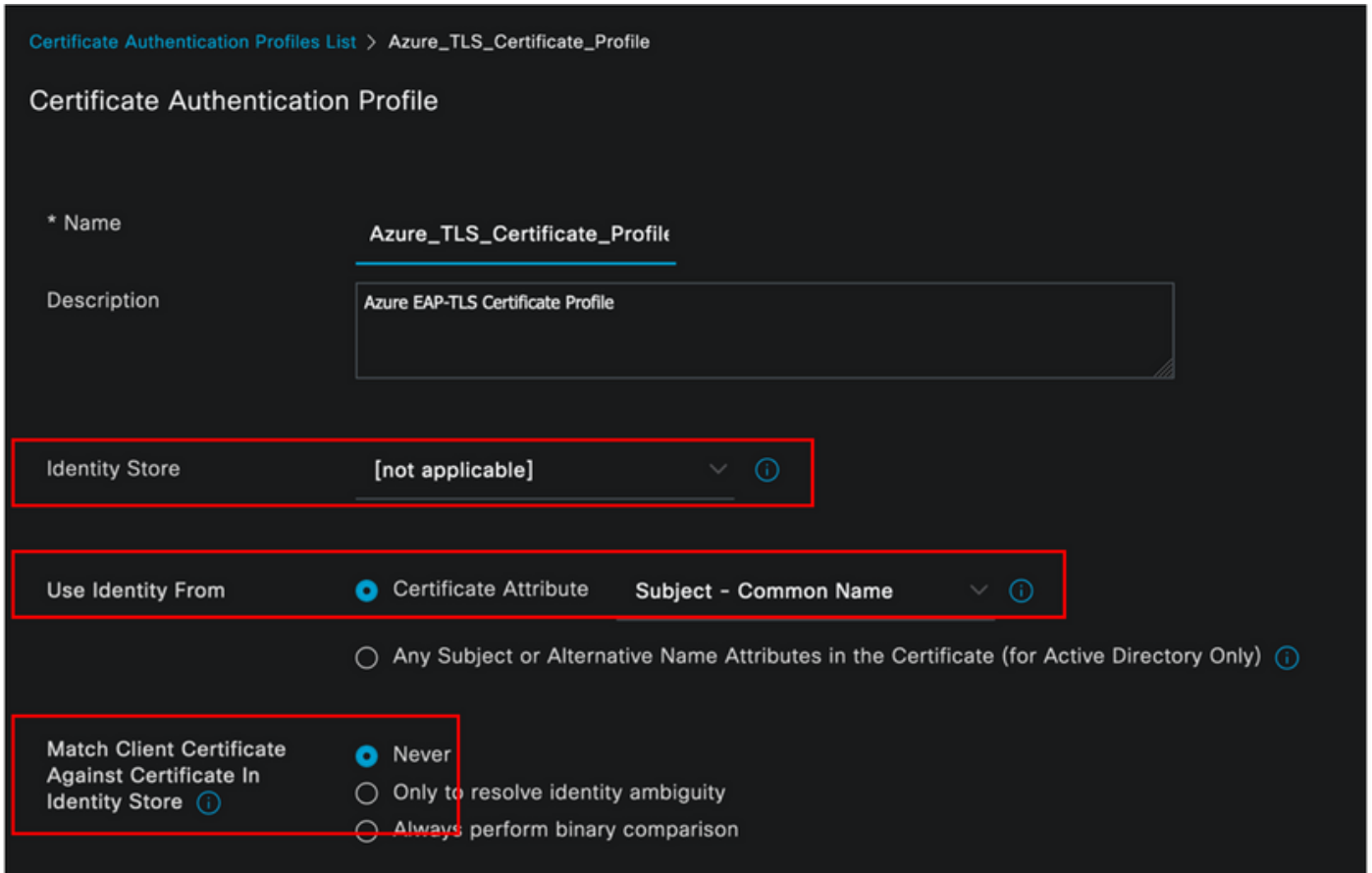
注意:ROPC功能和ISE与Azure AD之间的集成不在本文档的讨论范围之内。从Azure添加组和用户属性很重要。请参阅此处的[配置指南](#)。

配置证书身份验证配置文件

步骤1: 导航至 Menu图标  位于左上角，然后选择 **管理>身份管理>外部身份源**。

第二步： 选择 **证书身份验证** 创建配置文件，然后单击 **添加**。

第三步： 定义名称，设置 **身份库** 设置为[不适用]，并选择“主题 — 公用名称”使用来自的身份 字段。选择Never on Match **根据身份库中的证书创建客户端证书** 字段。



Certificate Authentication Profiles List > Azure_TLS_Certificate_Profile

Certificate Authentication Profile

* Name

Description

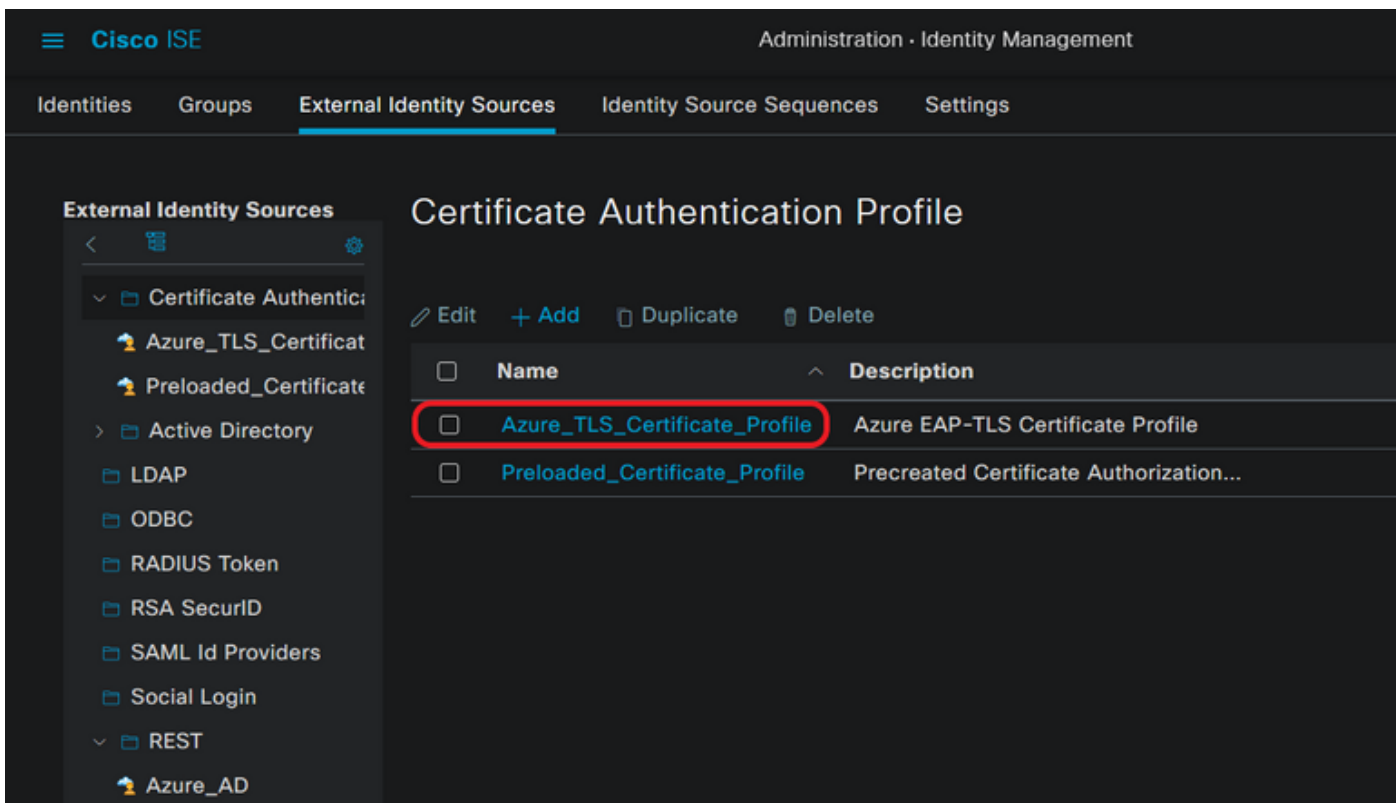
Identity Store


Use Identity From Certificate Attribute Directory Object Directory Object (for Active Directory Only) Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)


Subject - Common Name

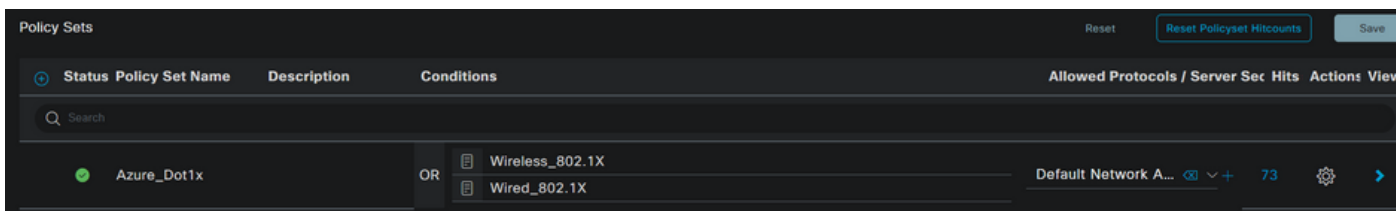
Match Client Certificate Against Certificate In Identity Store Never Only to resolve identity ambiguity Always perform binary comparison

第四步： 点击 **保存**



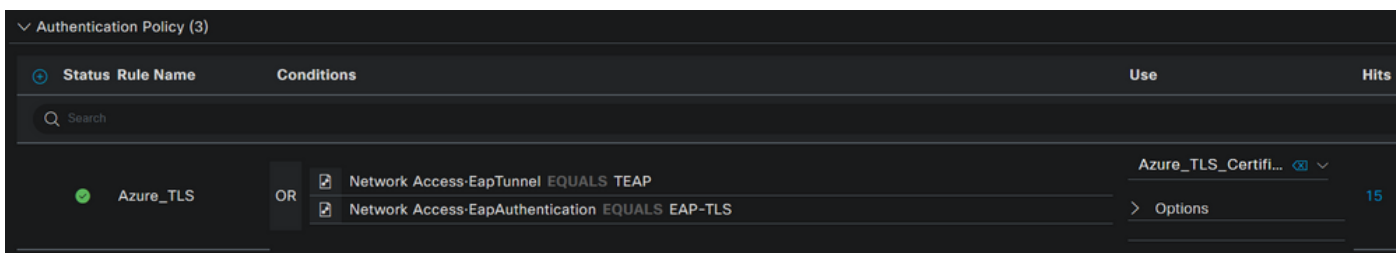
第五步： 导航至 Menu图标  位于左上角，然后选择 **策略>策略集**。

第六步： 选择加号  图标以创建新的策略集。定义名称并选择无线802.1x或有线802.1x作为条件。本示例中使用了Default Network Access选项



步骤 7. 选择箭头  在Default Network Access旁边，配置身份验证和授权策略。

步骤 8 选择Authentication Policy选项，定义名称并添加EAP-TLS作为网络访问EAPAuthentication，如果将TEAP用作身份验证协议，则可以添加TEAP作为网络访问EAPTunnel。选择在步骤3中创建的证书身份验证配置文件，然后单击 **保存**。



步骤 9 选择“授权策略”选项，定义名称并将Azure AD组或用户属性添加为条件。在“结果”(Results)下选择配置文件或安全组，具体取决于使用案例，然后单击 **保存**。

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

用户配置.

用户证书的主题公用名(CN)必须与Azure端上的用户主体名称(UPN)匹配，才能检索在授权规则中使用的AD组成员身份和用户属性。为使身份验证成功，根CA和任何中间CA证书必须位于ISE受信任库中。



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

Microsoft Azure

Search resources, services, and docs (G+)

Home > romlab | Users > Users >

John Smith ...
User

Search << Edit properties Delete Refresh Reset password Revoke sessions Got feedback?

Overview Audit logs Sign-in logs Diagnose and solve problems

Manage

- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Troubleshooting + Support

- New support request

Overview Monitoring **Properties**

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

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	

Job Information

Job title	
Company name	
Department	Sales 2nd Floor

验证

ISE验证

在Cisco ISE GUI中，点击Menu图标 选择 Operations > RADIUS > Live Logs for network authentications(RADIUS)。

Time	Status	Deta...	Identity	Authentication Policy	Authorization Policy	Authorization Pr...
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

点击“详细信息”(Details)列中的放大镜图标，以查看详细的身份验证报告，并确认流是否按预期运行。

1. 验证身份验证/授权策略
2. 身份验证方法/协议

3. 从证书中获取的用户使用者名称
4. 从Azure目录获取的用户组和其他属性

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	11001	Received RADIUS Access-Request
TLSCipher	ECDHE-RSA-AES256-GCM-SHA384	11018	RADIUS is re-using an existing session
TLSVersion	TLSv1.2	12504	Extracted EAP-Response containing EAP-TLS challenge-response
DTLSSupport	Unknown	61025	Open secure connection with TLS peer
Subject	CN=john.smith@romlab.onmicrosoft.com OU=Romlab Sales,O=Romlab,S=Texas,C=US	15041	Evaluating Identity Policy
Issuer	CN=romlab-ROME0-DC-CA,DC=romlab,DC=com	15048	Queried PIP - Network Access.EapTunnel
Issuer - Common Name	romlab-ROME0-DC-CA	15048	Queried PIP - Network Access.EapAuthentication
Issuer - Domain Component	romlab	22070	Identity name is taken from certificate attribute
Issuer - Domain Component	com	22037	Authentication Passed
Key Usage	0	12506	EAP-TLS authentication succeeded
Key Usage	2	15036	Evaluating Authorization Policy
Extended Key Usage - Name	138	15048	Queried PIP - Azure_AD.ExternalGroups
Extended Key Usage - Name	132	15016	Selected Authorization Profile - PermitAccess
Extended Key Usage - Name	130	22081	Max sessions policy passed
Extended Key Usage - OID	1.3.6.1.4.1.311.10.3.4	22080	New accounting session created in Session cache
Extended Key Usage - OID	1.3.6.1.5.5.7.3.4	11503	Prepared EAP-Success
Extended Key Usage - OID	1.3.6.1.5.5.7.3.2	11002	Returned RADIUS Access-Accept
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:b f		
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		

故障排除

在ISE上启用调试

导航至 **管理>System >记录>调试日志配置** 将下一个组件设置为指定的级别。

节点	组件名称	日志级别	日志文件名
PSN	rest-id-store	调试	rest-id-store.log
PSN	运行时AAA	调试	prrt-server.log

注意：完成故障排除后，请记住重置调试。为此，请选择相关节点，然后单击“重置为默认值”。

日志片段

下面的摘录显示了流程的最后两个阶段，如前面的网络图部分所述。

1. ISE获取证书使用者名称(CN)并执行对Azure Graph API的查找，以获取用户的组以及该用户的其它属性。这在Azure端称为用户主体名称(UPN)。
2. ISE授权策略根据从Azure返回的用户属性进行评估。

Rest-id日志:

```
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
```

打印日志:

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

2022-09-20 16:46:30,252 DEBUG [Thread-759][()] cisco.cpm.prvt.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.prvt.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.prvt.pip.RestIdentityProviderPIP -::::- checking attrList
ExternalGroups,city,companyName,country,department,displayName,employeeId,givenName,officeLocation,state,surname,userPrincipalName

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

2022-09-20 16:46:30,880 DEBUG [Thread-759][()] cisco.cpm.prvt.pip.RestIdentityProviderPIP -::::- userAttr size 11
...
2022-09-20 16:46:30,881 DEBUG [Thread-759][()] cisco.cpm.prvt.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.prvt.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.prvt.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.prvt.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.prvt.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.prvt.pip.RestIdentityProviderPIP -::::- userGroup 1

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

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。