

Microsoft Azure Active Directory를 사용하여 Cisco ISE 3.2 EAP-TLS 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[설정](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 Azure AD 그룹 구성원 자격 및 EAP-TLS 또는 TEAP를 인증 프로토콜로 사용하는 기타 사용자 특성을 기반으로 ISE에서 권한 부여 정책을 구성하고 문제를 해결하는 방법에 대해 설명합니다.

기고자: Emmanuel Cano, Security Consulting Engineer 및 Romeo Migisha, Technical Consulting Engineer

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Identity Services Engine(ISE)
- Microsoft Azure AD, 구독 및 앱
- EAP-TLS 인증

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE 3.2
- Microsoft Azure AD

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

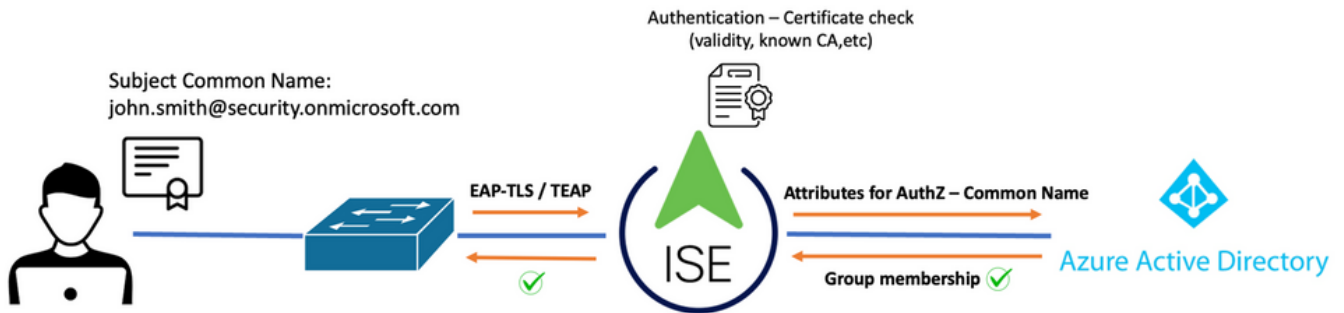
ISE 3.0에서는 ISE와 Azure Active Directory(AAD) 간의 통합을 활용하여 ROPC(Resource Owner Password Credentials) 통신을 통해 Azure AD 그룹 및 특성을 기반으로 사용자를 인증할 수 있습니다. ISE 3.2에서는 인증서 기반 인증을 구성할 수 있으며 사용자는 azure AD 그룹 멤버십 및 기타 특성을 기반으로 인증될 수 있습니다. ISE는 그래프 API를 통해 Azure에 쿼리하여 인증된 사용자의 그룹 및 특성을 가져오고, Azure 측의 UPN(User Principal Name)에 대해 인증서의 CN(Subject Common Name)을 사용합니다.

참고: 인증서 기반 인증은 EAP-TLS 또는 EAP-TLS를 내부 방법으로 사용하는 TEAP일 수 있습니다. 그런 다음 Azure Active Directory에서 특성을 선택하고 Cisco ISE 사전에 추가할 수 있습니다. 이러한 특성은 권한 부여에 사용할 수 있습니다. 사용자 인증만 지원됩니다.

구성

네트워크 다이어그램

다음 이미지는 네트워크 다이어그램 및 트래픽 흐름의 예를 제공합니다



절차:

1. 인증서는 EAP-TLS 또는 EAP-TLS가 포함된 TEAP를 통해 ISE에 내부 방법으로 전송됩니다.
2. ISE는 사용자의 인증서(유효 기간, 신뢰할 수 있는 CA, CRL 등)를 평가합니다.
3. ISE는 CN(Certificate Subject Name)을 사용하여 Microsoft Graph API를 조회하여 사용자의 그룹 및 해당 사용자에 대한 기타 특성을 가져옵니다. 이를 Azure 측에서 UPN(User Principal Name)이라고 합니다.
4. ISE 권한 부여 정책은 Azure에서 반환된 사용자의 특성에 대해 평가됩니다.

참고: 아래 표시된 대로 Microsoft Azure의 ISE 앱에 Graph API 권한을 구성하고 부여해야 합니다.


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

설정

ISE 구성

참고: ROPC 기능 및 ISE와 Azure AD 간의 통합은 이 문서의 범위를 벗어납니다. 그룹 및 사용자 특성은 Azure에서 추가해야 합니다. [여기서](#) 컨피그레이션 가이드를 참조하십시오.

인증서 인증 프로파일 구성

1단계. 탐색 메뉴 아이콘  왼쪽 위 모서리에 위치한 다음 **관리 > 신원 관리 > 외부 ID 소스**.

2단계. 선택 **인증서 인증** 프로필을 작성한 다음 **추가**.

3단계. 이름을 정의하고 **ID 저장소** [Not applicable](해당 없음)로 입력하고 Subject - Common Name on(주체 - 공통 이름)을 선택합니다. **ID 사용 위치** 필드. 일치하지 않음 선택 **ID 저장소의 인증서에 대한 클라이언트 인증서 필드**.

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

4단계. 클릭 저장

Cisco ISE Administration · Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

External Identity Sources


- External Identity Sources
 - Certificate Authentication Profiles
 - Azure_TLS_Certificate_Profile
 - Preloaded_Certificate_Profile
 - Active Directory
 - LDAP
 - ODBC
 - RADIUS Token
 - RSA SecurID
 - SAML Id Providers
 - Social Login
 - REST
 - Azure_AD

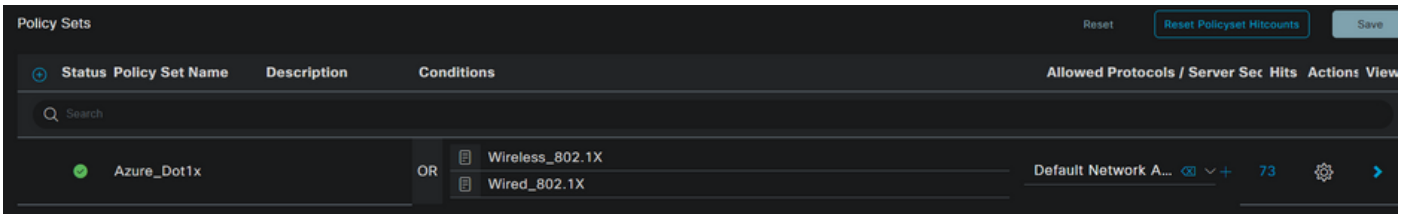
Certificate Authentication Profile

Edit + Add Duplicate Delete

Name	Description
<u>Azure_TLS_Certificate_Profile</u>	Azure EAP-TLS Certificate Profile
Preloaded_Certificate_Profile	Precreated Certificate Authorization...

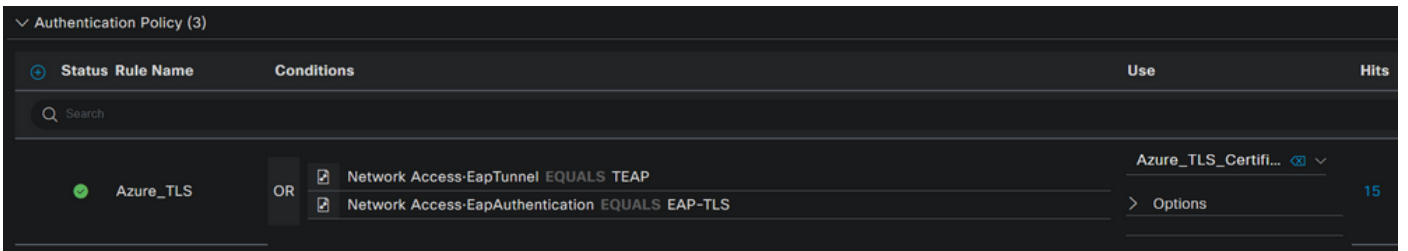
5단계. 탐색 메뉴 아이콘  왼쪽 위 모서리에 위치한 다음 Policy(정책) > Policy Sets(정책 집합)

6단계. 더하기 선택  새 정책 집합을 만드는 아이콘입니다. 이름을 정의하고 조건으로 Wireless 802.1x 또는 wired 802.1x를 선택합니다. 이 예에서는 Default Network Access 옵션을 사용합니다

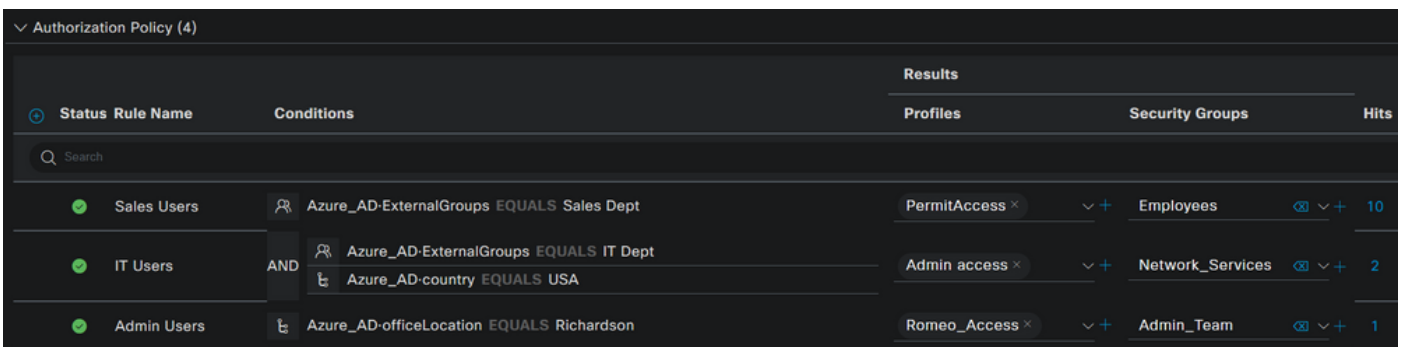


7단계. 화살표 선택 ➔ Default Network Access(기본 네트워크 액세스) 옆의 인증 및 권한 부여 정책을 구성합니다.

8단계. Authentication Policy(인증 정책) 옵션을 선택하고 이름을 정의하고 EAP-TLS를 Network Access EAPAuthentication으로 추가합니다. TEAP가 인증 프로토콜로 사용되는 경우 TEAP를 Network Access EAPPunnel로 추가할 수 있습니다. 3단계에서 생성한 인증서 인증 프로필을 선택하고 저장.



9단계. 권한 부여 정책 옵션을 선택하고, 이름을 정의하고, 조건으로 Azure AD 그룹 또는 사용자 특성을 추가합니다. Results(결과)에서 활용 사례에 따라 달라지는 프로필 또는 보안 그룹을 선택한 다음 저장.



사용자 컨피그레이션

권한 부여 규칙에 사용되는 AD 그룹 구성원 및 사용자 특성을 검색하려면 사용자 인증서의 주체 CN(공용 이름)이 Azure 측의 UPN(사용자 계정 이름)과 일치해야 합니다. 인증에 성공하려면 루트 CA 및 중간 CA 인증서가 ISE Trusted Store에 있어야 합니다.



john.smith@romlab.onmicrosoft.com

Issued by: romlab-ROME0-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-ROME0-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

다음을 확인합니다.

ISE 확인

Cisco ISE GUI에서 메뉴 아이콘을 클릭합니다. ≡ 선택 **Operations(운영) > RADIUS > Live Logs for network authentications (RADIUS)**(네트워크 인증을 위한 라이브 로그).

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

자세한 인증 보고서를 보고 흐름이 예상대로 작동하는지 확인하려면 Details 열에서 돋보기 아이콘을 클릭합니다.

1. 인증/권한 부여 정책 확인
2. 인증 방법/프로토콜

- 3. 인증서에서 가져온 사용자의 주체 이름
- 4. Azure 디렉터리에서 가져온 사용자 그룹 및 기타 특성

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		

문제 해결

ISE에서 디버깅 활성화

탐색 Administration(관리) > System(시스템) > Logging(로깅) > Debug Log Configuration(디버그 로그 구성) 을 눌러 다음 구성 요소를 지정된 레벨로 설정합니다.

노드 구성 요소 이름	로그 레벨	로그 파일 이름
PSN ID 저장소	디버그	rest-id-store.log
PSN 런타임 AAA	디버그	prrt-server.log

참고: 트러블슈팅이 완료되면 디버깅을 재설정해야 합니다. 이렇게 하려면 관련 노드를 선택하고 "Reset to Default(기본값으로 재설정)"를 클릭합니다.

로그 조각

다음 발췌문은 앞서 네트워크 다이어그램 섹션에서 언급한 것처럼 흐름의 마지막 두 단계를 보여줍니다.

1. ISE는 CN(인증서 주체 이름)을 사용하여 Azure Graph API를 조회하여 사용자의 그룹 및 해당 사용자에 대한 기타 특성을 가져옵니다. 이를 Azure 측에서 UPN(User Principal Name)이라고 합니다.
2. ISE 권한 부여 정책은 Azure에서 반환된 사용자의 특성에 대해 평가됩니다.

Rest-id 로그:

```
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,department,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
```

포트 로그:

```
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
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.