

Konfigurieren von Cisco ISE 3.2 EAP-TLS mit Microsoft Azure Active Directory

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie Autorisierungsrichtlinien in ISE auf der Grundlage der Azure AD-Gruppenmitgliedschaft und anderer Benutzerattribute mit EAP-TLS oder TEAP als Authentifizierungsprotokolle konfigurieren und Fehler in diesen Richtlinien beheben.

Beitrag von Emmanuel Cano, Security Consulting Engineer, und Romeo Migisha, Technical Consulting Engineer

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Identity Services Engine (ISE)
- Microsoft Azure AD, Abonnement und Apps
- EAP-TLS authentifizierung

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ISE 3.2
- Microsoft Azure AD

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

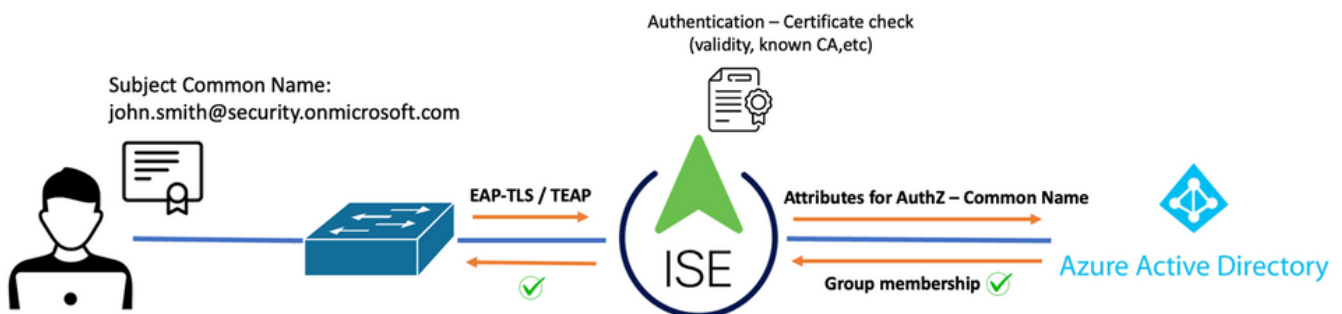
In ISE 3.0 ist es möglich, die Integration zwischen ISE und Azure Active Directory (AAD) zu nutzen, um die Benutzer basierend auf Azure AD-Gruppen und -Attributen über die ROPC-Kommunikation (Resource Owner Password Credentials) zu authentifizieren. Mit ISE 3.2 können Sie eine zertifikatbasierte Authentifizierung konfigurieren, und Benutzer können basierend auf Azure AD-Gruppenmitgliedschaften und anderen Attributen autorisiert werden. ISE fragt Azure über eine Grafik-API ab, um Gruppen und Attribute für den authentifizierten Benutzer abzurufen. Dabei wird der Common Name (CN) des Zertifikats mit dem UPN (User Principal Name) auf Azure-Seite verglichen.

Hinweis: Bei den zertifikatbasierten Authentifizierungen kann es sich entweder um EAP-TLS oder um TEAP mit EAP-TLS als interner Methode handeln. Anschließend können Sie Attribute aus Azure Active Directory auswählen und sie dem Cisco ISE-Wörterbuch hinzufügen. Diese Attribute können für die Autorisierung verwendet werden. Nur die Benutzerauthentifizierung wird unterstützt.

Konfigurieren

Netzwerkdiagramm

Das nächste Bild zeigt ein Netzwerkdiagramm und einen Verkehrsfluss.



Vorgehensweise:

1. Das Zertifikat wird über EAP-TLS oder TEAP mit EAP-TLS als interner Methode an die ISE gesendet.
2. Die ISE wertet das Zertifikat des Benutzers aus (Gültigkeitsdauer, vertrauenswürdige Zertifizierungsstelle, Zertifikatsperrliste usw.).
3. Die ISE sucht anhand des Zertifikatssubjektnamens (CN) nach der Microsoft Graph-API, um die Benutzergruppen und andere Attribute für diesen Benutzer abzurufen. Dies wird auf der Azure-Seite als Benutzerprinzipalname (User Principal Name, UPN) bezeichnet.
4. ISE-Autorisierungsrichtlinien werden anhand der von Azure zurückgegebenen Benutzerattribute ausgewertet.

Hinweis: Sie müssen die Graph API-Berechtigungen für die ISE-App in Microsoft Azure konfigurieren und erteilen, wie unten gezeigt:

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

Konfigurationen

ISE-Konfiguration

Hinweis: Die ROPC-Funktionalität und die Integration zwischen der ISE und Azure AD werden in diesem Dokument nicht behandelt. Es ist wichtig, dass Gruppen und Benutzerattribute von Azure hinzugefügt werden. Siehe Konfigurationsleitfaden [hier](#).

Konfigurieren des Zertifikatauthentifizierungsprofils

Schritt 1: Navigieren Sie zu das Menü-Symbol  in der linken oberen Ecke befindet, und wählen Sie **Administration > Identity Management > Externe Identitätsquellen**.

Schritt 2: Auswählen **Authentifizierung von Zertifikaten** Profil erstellen und dann auf klicken **Hinzufügen**

Schritt 3: Definieren Sie den Namen, legen Sie den **Identitätsspeicher** als [Nicht zutreffend] aus, und wählen Sie Subject - Common Name on **Identität verwenden von** feld. Nie zuordnen auswählen **Clientzertifikat für Zertifikat im Identitätsspeicher** Feld.

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

Schritt 4: Klicken Sie **Speichern**

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

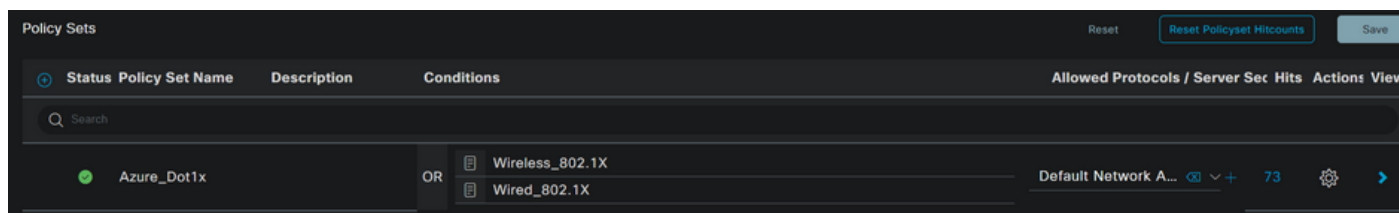
Edit + Add Duplicate Delete

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

Schritt 5: Navigieren Sie zu das Menü-Symbol  in der linken oberen Ecke befindet, und wählen Sie **Richtlinie > Richtliniensätze**.

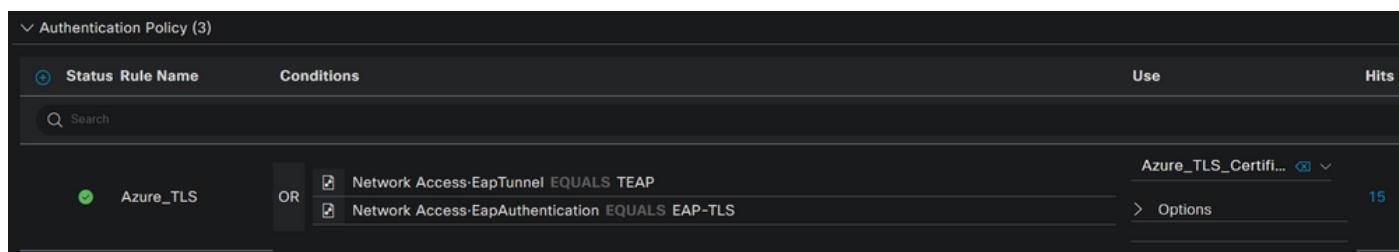
Schritt 6: Wählen Sie das Plus  um einen neuen Richtliniensatz zu erstellen. Definieren Sie

einen Namen, und wählen Sie als Bedingungen Wireless 802.1x oder kabelgebundene 802.1x-Verbindungen aus. In diesem Beispiel wird die Option Default Network Access (Standard-Netzwerkzugriff) verwendet

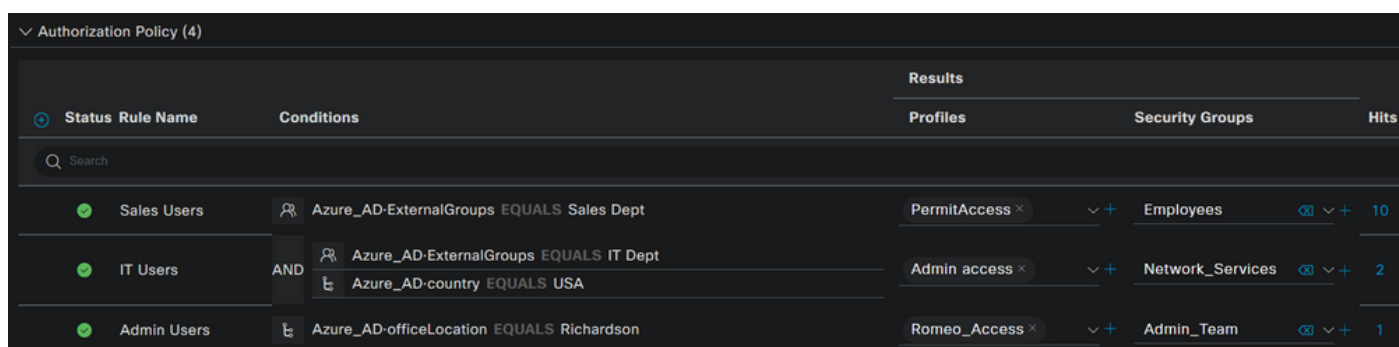


Schritt 7. Pfeil auswählen ➔ neben Standard-Netzwerkzugriff, um Authentifizierungs- und Autorisierungsrichtlinien zu konfigurieren.

Schritt 8: Wählen Sie die Authentifizierungsrichtlinie Option, definieren Sie einen Namen und fügen Sie EAP-TLS als Network Access EAPAuthentication, es ist möglich, TEAP als Network Access EAPTunnel hinzuzufügen, wenn TEAP als Authentifizierungsprotokoll verwendet wird. Wählen Sie das in Schritt 3 erstellte Zertifikatauthentifizierungsprofil aus, und klicken Sie auf **Speichern**.



Schritt 9. Wählen Sie die Option Autorisierungsrichtlinie aus, definieren Sie einen Namen, und fügen Sie Azure AD-Gruppen- oder Benutzerattribute als Bedingung hinzu. Wählen Sie das Profil oder die Sicherheitsgruppe unter "Ergebnisse" aus, hängt vom Anwendungsfall ab, und klicken Sie dann auf **Speichern**.



Benutzerkonfiguration.

Der Common Name (CN) des Antragstellers aus dem Benutzerzertifikat muss mit dem UPN (User Principal Name) auf Azure-Seite übereinstimmen, damit die AD-Gruppenmitgliedschaft und die Benutzerattribute abgerufen werden können, die in Autorisierungsregeln verwendet werden. Damit die Authentifizierung erfolgreich ist, müssen sich die Stammzertifizierungsstelle und alle zwischengeschalteten Zertifizierungsstellenzertifikate im vertrauenswürdigen ISE-Speicher befinden.



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

Überprüfung

ISE-Verifizierung

Klicken Sie in der Cisco ISE-GUI auf das Menü-Symbol  und wählen **Vorgänge > RADIUS > Live-Protokolle für Netzwerkauthentifizierungen (RADIUS)**.

Reset Repeat Counts Export To

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

Klicken Sie in der Spalte "Details" auf das Lupensymbol, um einen detaillierten Authentifizierungsbericht anzuzeigen und zu überprüfen, ob der Fluss wie erwartet funktioniert.

1. Überprüfen von Authentifizierungs-/Autorisierungsrichtlinien
2. Authentifizierungsmethode/Protokoll

3. Dem Zertifikat entnommener Benutzername

4. Benutzergruppen und andere Attribute aus Azure-Verzeichnis abgerufen

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		

Fehlerbehebung

Debuggen auf ISE aktivieren

Navigieren Sie zu **Administration > System > Protokollierung > Konfiguration des Debug-Protokolls**, um die nächsten Komponenten auf die angegebene Ebene zu setzen.

Knoten	Komponentenname	Protokollstufe	Protokolldateiname
PSN	Ruhestandslager	Fehlersuche	rest-id-store.log
PSN	Laufzeit-AAA	Fehlersuche	prrt-server.log

Hinweis: Wenn Sie mit der Fehlerbehebung fertig sind, sollten Sie die Fehlerbehebungen zurücksetzen. Wählen Sie dazu den entsprechenden Knoten aus und klicken Sie auf "Reset

to Default".

Protokolle Ausschnitte

Die nächsten Auszüge zeigen die letzten beiden Phasen im Fluss, die bereits im Netzwerkdiagrammabschnitt erwähnt wurden.

1. ISE verwendet den Zertifikatssubjektnamen (CN) und führt eine Suche in der Azure Graph-API durch, um Benutzergruppen und andere Attribute für diesen Benutzer abzurufen. Dies wird auf Azure-Seite als Benutzerprinzipalname (UPN) bezeichnet.
2. ISE-Autorisierungsrichtlinien werden anhand der von Azure zurückgegebenen Benutzerattribute ausgewertet.

REST-ID-Protokolle:

```
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.IpdKeyValueCacheInitializer -:- 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
```

Port-Protokolle:

```
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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.