

Cisco ISE 3.2 EAP-TLS configureren met Microsoft Azure Active Directory

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

In dit document wordt beschreven hoe u autorisatiebeleid in ISE kunt configureren en oplossen op basis van Azure AD-groepslicidmaatschap en andere gebruikerskenmerken met EAP-TLS of TEAP als verificatieprotocollen.

Bijgedragen door Emmanuel Cano, Security Consulting Engineer en Romeo Migisha, Technical Consulting Engineer

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Identity Services Engine (ISE)
- Microsoft Azure AD, abonnement en apps
- EAP-TLS verificatie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ISE-lijnkaart 3.2
- Microsoft Azure AD

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

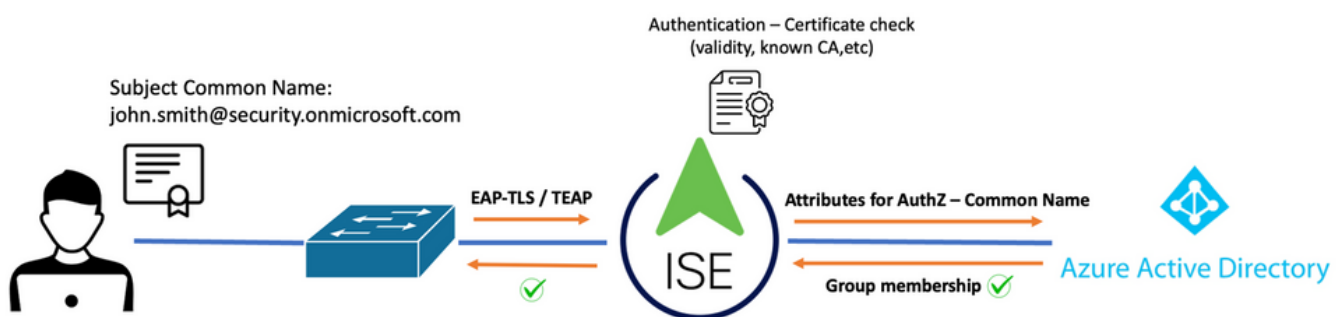
In ISE 3.0 kan gebruik worden gemaakt van de integratie tussen ISE en Azure Active Directory (AAD) om gebruikers te verifiëren op basis van Azure AD-groepen en -kenmerken via ROPC-communicatie (Resource Owner Password Credentials). Met ISE 3.2 kunt u op certificaat gebaseerde verificatie configureren en kunnen gebruikers worden geautoriseerd op basis van azure AD-groepslidmaatschap en andere kenmerken. ISE vraagt Azure via grafiek API om groepen en attributen voor de geauthenticeerde gebruiker op te halen, het gebruikt de onderwerpsnaam (Onderwerp Common Name, CN) van het certificaat tegen Gebruiker Principal Name (UPN) aan de Azure-kant.

Opmerking: de op certificaten gebaseerde verificaties kunnen EAP-TLS of TEAP zijn met EAP-TLS als binnenmethode. Vervolgens kunt u kenmerken selecteren uit Azure Active Directory en deze toevoegen aan het Cisco ISE-woordenboek. Deze eigenschappen kunnen voor vergunning worden gebruikt. Alleen gebruikersverificatie wordt ondersteund.

Configureren

Netwerkdigram

Het volgende beeld verstrekt een voorbeeld van een netwerkdigram en een verkeersstroom



Procedure:

1. Het certificaat wordt naar ISE verzonden via EAP-TLS of TEAP met EAP-TLS als binnenmethode.
2. ISE evalueert het gebruikerscertificaat (geldigheidsperiode, vertrouwde CA, CRL enzovoort).
3. ISE neemt de certificaatonderwerpsnaam (CN) en voert een raadpleging uit naar de Microsoft Graph API om de gebruikersgroepen en andere kenmerken voor die gebruiker te halen. Dit staat bekend als User Principal Name (UPN) aan de kant van Azure.
4. ISE-autorisatiebeleid wordt beoordeeld aan de hand van de gebruikerskenmerken die door Azure zijn geretourneerd.

Opmerking: U moet de Graph API-rechten configureren en verlenen aan de ISE-app in Microsoft Azure, zoals hieronder wordt getoond:

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

Configuraties

ISE-configuratie

Opmerking: ROPC-functionaliteit en integratie tussen ISE en Azure AD valt buiten het bereik van dit document. Het is belangrijk dat groepen en gebruikerskenmerken worden toegevoegd van Azure. Zie [hier](#) de configuratiehandleiding.

Het profiel voor certificaatverificatie configureren

Stap 1. Naar navigeren het menu-pictogram  in de linkerbovenhoek en selecteer **Administratie > Identiteitsbeheer > Externe identiteitsbronnen**.

Stap 2. Kiezen **Certificaatverificatie Profiel** en klik op **Toevoegen**.

Stap 3. Bepaal de naam, Stel de **Identity Store** als [Niet van toepassing], en selecteer **Onderwerp - Gemeenschappelijke naam op Identiteit gebruiken van** veld. Selecteer nooit op overeenkomst **Clientcertificaat tegen certificaat in Identity Store** Veld.

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

Stap 4. Klik op Opslaan

Cisco ISE Administration · Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

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

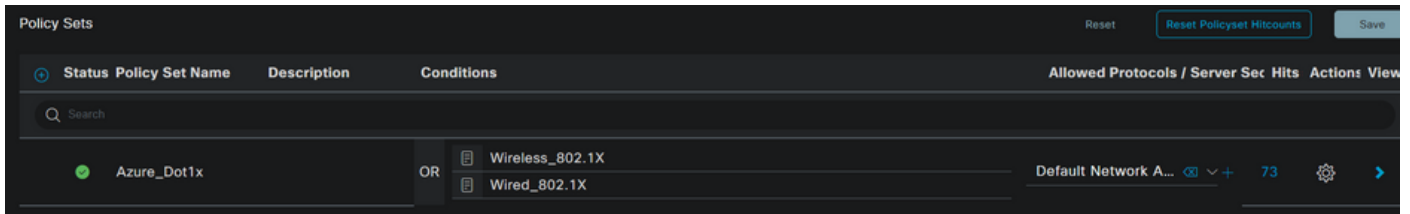
Edit + Add Duplicate Delete


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

Stap 5. Naar navigeren het menu-pictogram  in de linkerbovenhoek en selecteer **Beleid > Beleidssets**.

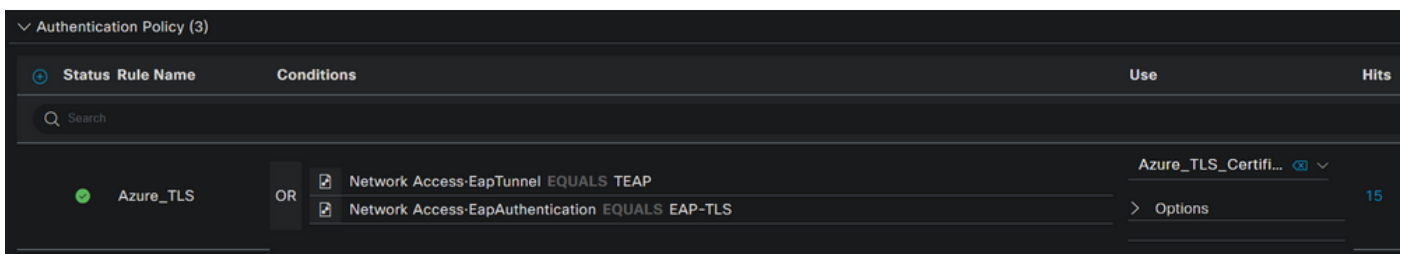
Stap 6. Selecteer de plus  pictogram om een nieuwe beleidsset te maken. Definieer een naam

en selecteer Wireless 802.1x of bekabeld 802.1x als voorwaarden. De optie Standaard netwerktoegang wordt in dit voorbeeld gebruikt

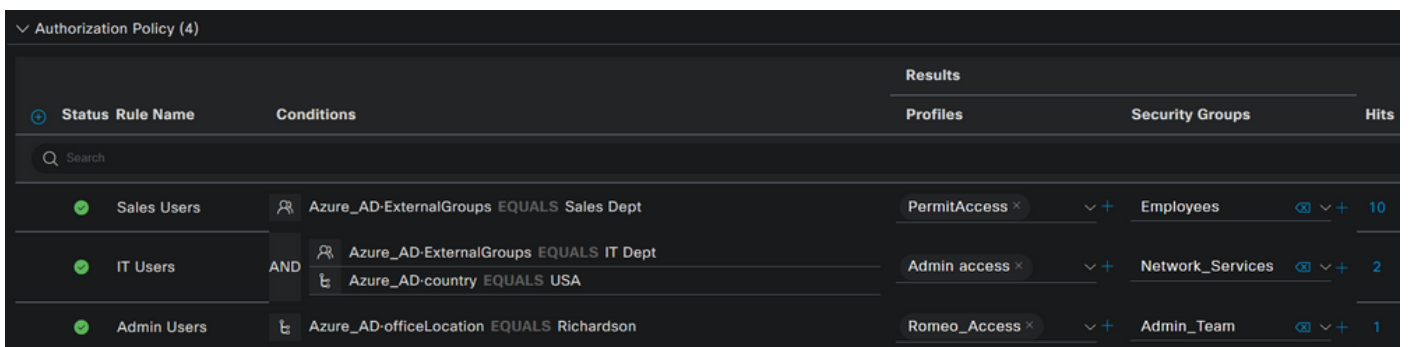


Stap 7. Selecteer de pijl  naast Default Network Access om verificatie- en autorisatiebeleid te configureren.

Stap 8. Selecteer de optie Verificatiebeleid, definieer een naam en voeg EAP-TLS toe als EAP-Authenticatie voor netwerktoegang. Het is mogelijk om TEAP toe te voegen als EAP-Tunnel voor netwerktoegang als TEAP wordt gebruikt als verificatieprotocol. Selecteer het certificaatverificatieprofiel dat in stap 3 is gemaakt en klik op **Opslaan**.



Stap 9. Selecteer de optie Autorisatiebeleid, definieer een naam en voeg Azure AD-groep of gebruikerskenmerken als voorwaarde toe. Kies het profiel of de beveiligingsgroep onder Resultaten, hangt af van de gebruikscase en klik vervolgens op **Opslaan**.



Gebruikersconfiguratie.

De onderwerpnaam (CN) uit het gebruikerscertificaat moet overeenkomen met de hoofdnaam van de gebruiker (UPN) aan de kant van Azure om het lidmaatschap van de AD-groep en gebruikerskenmerken op te halen die in de machtigingsregels worden gebruikt. De authenticatie kan alleen succesvol zijn als de root-CA en alle tussenliggende CA's-certificaten zich in de ISE Trusted Store bevinden.



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

Verifiëren

ISE-verificatie

Klik in de Cisco ISE GUI op het pictogram Menu  en kiezen **Operations > RADIUS > Live logs voor netwerkverificatie (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

Klik in de kolom Details op het pictogram vergrootglas om een gedetailleerd verificatierapport te bekijken en te bevestigen of de stroom werkt zoals verwacht.

1. Verifieer het verificatie-/autorisatiebeleid
2. Verificatiemethode/protocol

3. Onderwerpnaam van de gebruiker overgenomen van het certificaat
4. Gebruikersgroepen en andere kenmerken gehaald uit 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	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		

Problemen oplossen

Debugs inschakelen op ISE

Naar navigeren **Beheer > Systeem > Vastlegging > Configuratie debug-log** om de volgende onderdelen op het opgegeven niveau in te stellen.

Knooppunt	Naam van component	Logniveau	Logbestandsnaam
PSN	winkel voor ruilhandel	Debuggen	rest-id-store.log
PSN	runtime-AAA	Debuggen	prtserver.log

Opmerking: wanneer u klaar bent met probleemoplossing, vergeet niet de debugs opnieuw in te stellen. Hiertoe selecteert u het betreffende knooppunt en klikt u op "Standaard opnieuw

instellen".

Logs-fragmenten

De volgende uittreksels tonen de laatste twee fasen in de stroom, zoals eerder vermeld in de sectie van het netwerkdiagram.

1. ISE neemt de certificaatonderwerpnaam (CN) en voert een opzoekactie uit naar de Azure Graph API om gebruikersgroepen en andere kenmerken voor die gebruiker te halen. Dit staat bekend als User Principal Name (UPN) aan Azure-zijde.
2. ISE-autorisatiebeleid wordt beoordeeld aan de hand van de gebruikerskenmerken die door Azure zijn geretourneerd.

logbestanden van rest-id's:

```
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
```

Printerlogboeken:

```
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
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.