

Configurare ISE 3.2 EAP-TLS con Microsoft Azure Active Directory

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare e risolvere i problemi relativi ai criteri di autorizzazione in ISE in base all'appartenenza al gruppo Azure AD con EAP-TLS o TEAP.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Identity Services Engine (ISE)
- Microsoft Azure AD, sottoscrizione e app
- EAP-TLS autenticazione

Componenti usati


Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISE 3.2
- Microsoft Azure AD

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

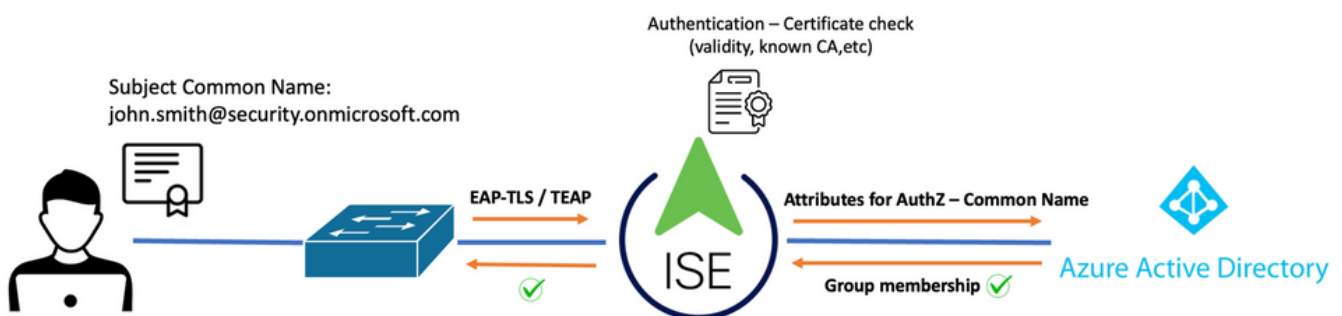
In ISE 3.0 è possibile sfruttare l'integrazione tra ISE e Azure Active Directory (AAD) per autenticare gli utenti in base ai gruppi e agli attributi di Azure AD tramite la comunicazione ROPC (Resource Owner Password Credentials). Con ISE 3.2 è possibile configurare l'autenticazione basata su certificati e autorizzare gli utenti in base all'appartenenza ai gruppi di Azure AD e ad altri attributi. ISE esegue query su Azure tramite l'API del grafico per recuperare gruppi e attributi per l'utente autenticato. Utilizza il nome comune del soggetto (CN) del certificato in base al nome dell'entità utente (UPN) sul lato Azure.

 Nota: le autenticazioni basate sui certificati possono essere EAP-TLS o TEAP con EAP-TLS come metodo interno. È quindi possibile selezionare gli attributi da Azure Active Directory e aggiungerli al dizionario Cisco ISE. Questi attributi possono essere utilizzati per l'autorizzazione. È supportata solo l'autenticazione utente.

Configurazione


Esempio di rete

Nell'immagine seguente viene illustrato un esempio di diagramma di rete e di flusso del traffico



Procedura:


1. Il certificato viene inviato all'ISE tramite EAP-TLS o TEAP con EAP-TLS come metodo interno.
2. ISE valuta il certificato dell'utente (periodo di validità, CA attendibile, CRL e così via).
3. ISE acquisisce il nome del soggetto del certificato (CN) ed esegue una ricerca nell'API di Microsoft Graph per recuperare i gruppi e altri attributi dell'utente. Questo nome è noto come UPN (User Principal Name) nel lato di Azure.
4. I criteri di autorizzazione ISE vengono valutati in base agli attributi dell'utente restituiti da Azure.

 Nota: è necessario configurare e concedere le autorizzazioni dell'API Graph per l'app ISE in Microsoft Azure, come mostrato di seguito:

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

Configurazioni

Configurazione di ISE

 Nota: la funzionalità ROPC e l'integrazione tra ISE e Azure AD non rientrano nell'ambito di questo documento. È importante aggiungere gruppi e attributi utente da Azure. Vedere [qui la guida alla configurazione](#).

Configurare il profilo di autenticazione del certificato



Passaggio 1. Passa a l'icona Menu nell'angolo superiore sinistro e selezionare Amministrazione > Gestione delle identità > Origini identità esterne.

Passaggio 2. Seleziona Autenticazione certificato Profilo, quindi fare clic su Aggiungi.

Passaggio 3. Definire il nome, Impostare il Archivio identità come [Non applicabile], quindi selezionare Oggetto - Nome comune in Usa identità da campo. Selezionare Mai in corrispondenza Certificato client rispetto al certificato nell'archivio identità Campo.

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

Passaggio 4. Fare clic su Salva

Cisco ISE Administration - Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Certificate Authentication Profile

External Identity Sources

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

Edit + Add Duplicate Delete

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

Passaggio 5. Passa a l'icona Menu

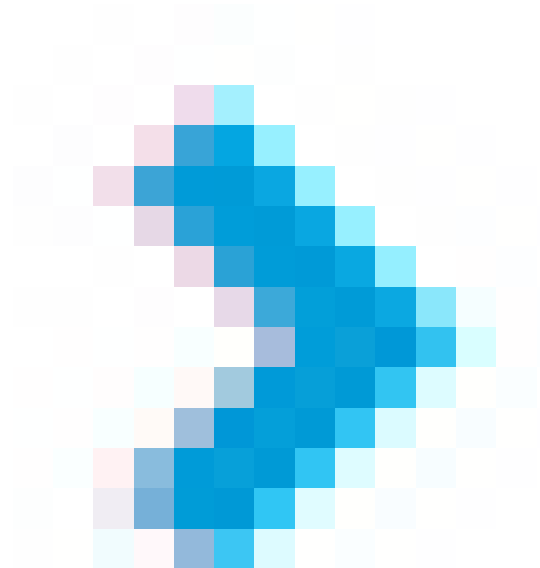
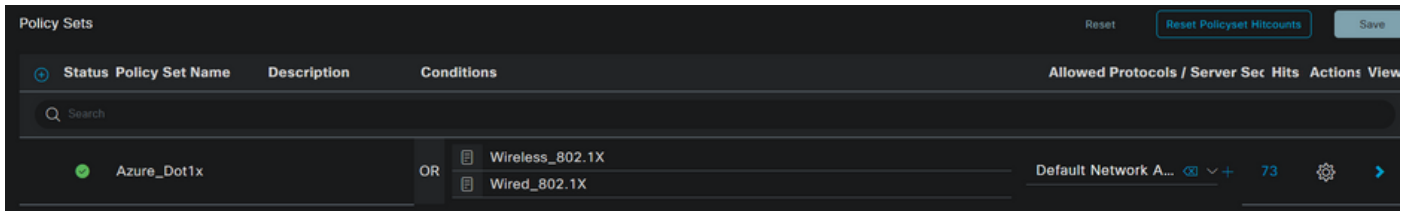


nell'angolo superiore sinistro e selezionare Criterio > Set di criteri.

Passaggio 6. Selezionare il segno più

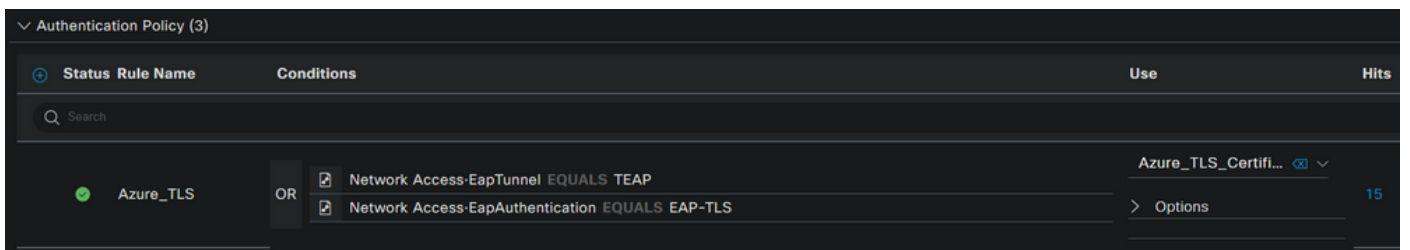


per creare un nuovo set di criteri. Assegnare un nome e selezionare Wireless 802.1x o Wireless 802.1x come condizioni. In questo esempio viene utilizzata l'opzione Accesso alla rete predefinito



Passaggio 7. Selezionare la freccia accanto a Accesso alla rete predefinito per configurare i criteri di autenticazione e autorizzazione.

Passaggio 8. Selezionare l'opzione Authentication Policy (Criterio di autenticazione), definire un nome e aggiungere EAP-TLS come Network Access EAPAuthentication (Autenticazione EAPA accesso alla rete). È possibile aggiungere TEAP come Network Access EAPTunnel se TEAP viene utilizzato come protocollo di autenticazione. Selezionare il profilo di autenticazione certificato creato al passaggio 3 e fare clic su Salva.



Passaggio 9. Selezionare l'opzione Criteri di autorizzazione, definire un nome e aggiungere gli attributi utente o del gruppo di Azure AD come condizione. Scegliere il profilo o il gruppo di protezione in Risultati, in base allo Use Case, quindi fare clic su Salva.

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

Configurazione utente.

Il nome comune del soggetto (CN) del certificato utente deve corrispondere al nome dell'entità utente (UPN) sul lato Azure per recuperare l'appartenenza al gruppo AD e gli attributi utente da utilizzare nelle regole di autorizzazione. Affinché l'autenticazione abbia esito positivo, la CA radice e gli eventuali certificati delle CA intermedie devono trovarsi nell'archivio attendibile ISE.



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

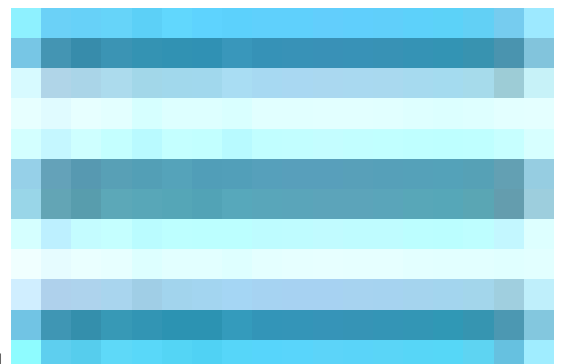
Troubleshooting + Support New support request

Overview Monitoring **Properties**

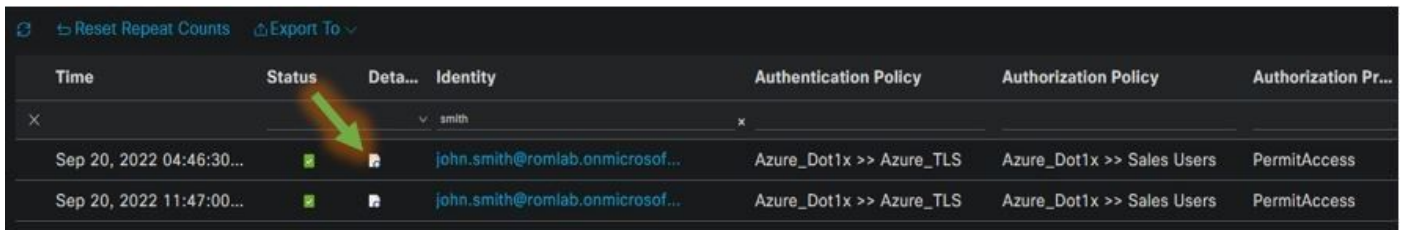
Identity		Contact Information	
Display name	John Smith	Street address	
First name	John	City	
Last name	Smith	State or province	
User principal name	john.smith@romlab.onmicrosoft.com	ZIP or postal code	
Object ID	4adde592-d6f9-4e67-8f1f-d3cc43ed400a	Country or region	
Identities	romlab.onmicrosoft.com	Business phone	
User type	Member	Mobile phone	
Creation type		Email	
Created date time	Sep 16, 2022, 7:56 PM	Other emails	
Last password change date time	Sep 16, 2022, 8:08 PM	Proxy addresses	
External user state		Fax number	
External user state change date t...		IM addresses	
Assigned licenses	View	Mail nickname	john.smith
Password policies		Parental controls	
Password profile		Age group	
Preferred language		Consent provided for minor	
Sign in sessions valid from date ...	Sep 16, 2022, 8:08 PM	Legal age group classification	
Authorization info	View	Settings	
Job Information		Account enabled	Yes
Job title		Usage location	
Company name		Preferred data location	
Department	Sales 2nd Floor	On-premises	

Verifica


Verifica ISE



Nell'interfaccia utente di Cisco ISE, fare clic sull'icona Menu e scegliere Operazioni > RADIUS > Live Log per le autenticazioni di rete (RADIUS).



The screenshot shows a table with the following columns: Time, Status, Deta..., Identity, Authentication Policy, Authorization Policy, and Authorization Pr... The table contains two rows of log entries. A green arrow points to a magnifying glass icon in the 'Deta...' column of the first row.

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

Fare clic sull'icona della lente di ingrandimento nella colonna Dettagli per visualizzare un report di autenticazione dettagliato e verificare se il flusso funziona come previsto.

1. Verifica criteri di autenticazione/autorizzazione
2. Metodo/protocollo di autenticazione
3. Nome soggetto utente ricavato dal certificato
4. Gruppi di utenti e altri attributi recuperati dalla directory di Azure

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		
TLS cipher	ECDHE-RSA-AES256-GCM-SHA384		11001 Received RADIUS Access-Request
TLSVersion	TLSv1.2		11018 RADIUS is re-using an existing session
DTLSSupport	Unknown		12504 Extracted EAP-Response containing EAP-TLS challenge-response
Subject	CN=john.smith@romlab.onmicrosoft.com OU=Romlab Sales,O=Romlab,S=Texas,C=US		61025 Open secure connection with TLS peer
Issuer	CN=romlab-ROME0-DC-CA,DC=romlab,DC=com		15041 Evaluating Identity Policy
Issuer - Common Name	romlab-ROME0-DC-CA		15048 Queried PIP - Network Access.EapTunnel
Issuer - Domain Component	romlab		15048 Queried PIP - Network Access.EapAuthentication
Issuer - Domain Component	com		22070 Identity name is taken from certificate attribute
Key Usage	0		22037 Authentication Passed
Key Usage	2		12506 EAP-TLS authentication succeeded
Extended Key Usage - Name	138		15036 Evaluating Authorization Policy
Extended Key Usage - Name	132		15048 Queried PIP - Azure_AD.ExternalGroups
Extended Key Usage - Name	130		15016 Selected Authorization Profile - PermitAccess
Extended Key Usage - OID	1.3.6.1.4.1.311.10.3.4		22081 Max sessions policy passed
Extended Key Usage - OID	1.3.6.1.5.5.7.3.4		22080 New accounting session created in Session cache
Extended Key Usage - OID	1.3.6.1.5.5.7.3.2		11503 Prepared EAP-Success
Template Name	1.3.6.1.4.1.311.21.8.5420261.8703952.14042247.7322992.6244189.86.4576875.1279510		11002 Returned RADIUS Access-Accept
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		


Risoluzione dei problemi

Abilita debug su ISE

Passa a Amministrazione > Sistema > Registrazione > Configurazione registro di debug per impostare i componenti successivi al livello specificato.

Nodo	Nome componente	Livello log	Nome file di log

PSN	rest-id-store	Debug	rest-id-store.log
PSN	runtime-AAA	Debug	port-server.log

 Nota: al termine della risoluzione dei problemi, ripristinare i debug. A tale scopo, selezionare il nodo correlato e fare clic su "Ripristina valori predefiniti".

Registra frammenti

Gli estratti successivi mostrano le ultime due fasi del flusso, come accennato in precedenza nella sezione diagramma reticolare.

1. ISE acquisisce il nome soggetto del certificato (CN) ed esegue una ricerca nell'API di Azure Graph per recuperare i gruppi e altri attributi dell'utente. Questo nome è noto come UPN (User Principal Name) sul lato Azure.
2. I criteri di autorizzazione ISE vengono valutati in base agli attributi dell'utente restituiti da Azure.

Log ID residuo:

```

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

```

Registri porte:

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

2022-09-20 16:46:30,252 DEBUG [Thread-759][()] cisco.cpm.pr.rt.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.pr.rt.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.pr.rt.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.pr.rt.pip.RestIdentityProviderPIP -::::- Username from the Context
john.smith@romlab.onmicrosoft.com

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

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).